В.С. Викторова, А.С. Степанянц

Модели и методы расчета надежности технических систем

Москва 2013

Книга содержит основные понятия и определения теории надежности и описание моделей и методов анализа надежности технических систем. Изложены методы расчета показателей надежности, использующие основные формулы теории вероятностей и комбинаторики. Рассмотрен класс логико-вероятностных моделей и методы получения и преобразования формального описания структур систем, в т.ч. блок-схемы надежности, деревья отказов. Рассмотрены вопросы марковского моделирования надежности и вычислительные схемы расчета показателей надежности восстанавливаемых и невосстанавливаемых систем. Дан обзор подходов к анализу видов и последствий отказов. Приводятся примеры расчетов с привлечением современных средств автоматизации анализа надежности. Книга предназначена для инженеров и научных работников, специализирующихся в области проектного анализа надежности технических систем.

СОДЕРЖАНИЕ

Оглавление

Предисловие

Как самостоятельное научное направление теория надежности зародилась в США через несколько лет после окончания Второй Мировой войны, когда американцы начали военные действия в Кореи, далеко от стационарных баз, где можно было бы отремонтировать или заменить отказавшую военную технику. Для решения проблемы надежности в Институте Радиоинженеров США(IRE) была создана секция надежности и контроля качества, которая стала выпускать ежеквартальные журналы и, начиная с 1954г., созывать ежегодные симпозиумы по надежности. В это же время вопросам надежности технических объектов стало уделяться должное внимание и в Советском Союзе. Уже в 1954 г. вышел первый сборник переводов зарубежных материалов, затрагивающих вопросы надежности, под ред. академика В.И. Сифорова. Возможности советской системы по быстрой мобилизации интеллектуальных и материальных ресурсов в нужном направлении дали свои плоды. Была сформирована группа специалистов (в основном военных из Академии Жуковского), которые возглавили работы в Москве: Б.В. Васильев, Г.В. Дружинин, В.А. Кузнецов, Б.Р. Левин, И.И. Морозов, М.А. Синица, К.Ф. Цветаев. В 1958 г. состоялась Первая Всесоюзная конференция по надежности. Ленинградскими специалистами уже в 1959г. в первом отечественном отделе надежности (в одном из Ленинградских НИИ Судпрома) была выпущена первая книжка - «Основы теории и расчета надежности (авторы книги – одни из основоположников отечественной школы надежности: И.М. Маликов, А.М. Половко, Н.А. Романов и П.А. Чукреев). А в 1959г. в декабре проходила уже Вторая Всесоюзная конференция по надежности, главным организатором которой было НТО им. А.С. Попова. Был создан специальный объединенный отдел надежности всех оборонных министерств под руководством замечательного ученого и организатора – Якова Михайловича Сорина, в котором работал тогда еще молодой специалист, а ныне крупный ученый, автор всемирно известного справочника по теории надежности, Игорь Алексеевич Ушаков. Выдающиеся теоретические результаты работы этих ученых и их высочайшая практическая ценность позволили доказать ряду тогдашних главных конструкторов ошибочность мнения о том, что “считают надежность те, кто ее не умеет делать”. В 60-х годах почти одновременно в СССР и США были выпущены две книги, заложившие теоретический фундамент анализа надежности, “Математические методы в теории надежности” и “Mathematical Theory of Reliability”. Авторами первой книги были выдающиеся советские математики, “классики при жизни” – Б.В. Гнеденко, Ю.К. Беляев, А.Д. Соловьев, руководители кафедры и лаборатории теории вероятностей МГУ. Академик, заведующий кафедрой теории вероятностей МГУ Борис Владимирович Гнеденко – ученый, классические результаты которого в

теории экстремальных величин, в статистике и теории массового обслуживания известны во всем мире. Доктор физико-математических наук, профессор Александр Дмитриевич Соловьев – известный ученый, крупнейший специалист по асимптотическим методам теории надежности. Доктор физико-математических наук, профессор Юрий Константинович Беляев - ученик А.Н. Колмогорова, выдающийся ученый, специализирующийся на статистических методах оценки показателей надежности и методах контроля качества. Вторая книга была написана профессором Калифорнийского университета Р. Барлоу и профессором университета Флориды, сотрудником научной лаборатории фирмы Boeing Ф. Прошаном. За вклад в развитие теории надежности они были удостоены премии фон Неймана Американского Общества Исследования Операций.

Дальнейшее развитие отечественной теории надежности связано с именами многих выдающихся ученых. Среди них, адмирал Игорь Алексеевич Рябинин – один из создателей логико-вероятностного направления теории надежности, родившегося в связи с необходимостью построения адекватных моделей надежности многоэлементных, высокорезервированных корабельных систем, Геннадий Николаевич Черкесов, автор оригинальных работ по анализу надежности систем с временным резервированием, Илья Борисович Герцбах, написавший одну из лучших книг по моделям систем с профилактическим обслуживанием, ученики Б.В. Гнеденко Владимир Семенович Королюк и Игорь Николаевич Коваленко, получившие очень интересные теоретические результаты в области надежности и массового обслуживания, Георгий Васильевич Дружинин, автор одной из первых отечественных монографий по теории надежности “Надежность устройств автоматики”, выпущенной в 1964г, и организатор научного семинара по надежности, в котором принимали участие все ведущие специалисты страны, Борис Степанович Сотсков, один из основателей направления, связанного с физикой отказов элементов и устройств автоматики и вычислительной техники, и многие другие.

Читателю, который хочет более подробно ознакомиться с историей становления отечественной научной школы надежности, можно порекомендовать прочесть замечательный исторический обзор И.А. Ушакова, помещенный им на форуме Гнеденко по web адресу http://www.gnedenko-forum.org/history.htm.

Современными российскими специалистами ведутся теоретические исследования во всех разделах теории надежности. Широко известными являются работы Акуловой Л.Г., Можаева А.С., Рябинина И.А., Ушакова И.А., Филина Б.П. (логико-вероятностные методы), Лубкова Н.В., Половко А.М., Рыкова В.В., Ушакова И.А., Шубинского И.Б. (марковские, полумарковские случайные процессы), Калашникова В.В., Соловьева А.Д., (асимптотические методы - полумарковские, регенерирующие процессы, теория восстановления), Буянова Б.Б., Калашникова

В.В., Кузнецова Н.Ю., Лубкова Н.В. (ускорение статистического моделирования), Волика Б.Г., Рябинина И.А., Ушакова И.А. (анализ эффективности и техногенной безопасности), Петрухина Б.П. (прогнозирование безотказности электронной элементной базы) и многих других.

Данная книга ориентирована на изложение моделей и методов проектного анализа надежности сложных технических систем. Опыт, приобретенный авторами в ходе выполнения этих проектов, показывает, что существует признанный порядок и состав этапов проектного анализа надежности. Это - определение структуры системы и расчет характеристик безотказности и ремонтопригодности ее элементов; проведение анализа видов и последствий отказов (чаще всего на уровне типовых элементов замены); анализ надежности на системном уровне с учетом различных видов резервирования, особенностей функционирования, обслуживания, ремонтов. Характерной особенностью выполнения проектных исследований в данной области является использование специализированного программного обеспечения анализа надежности. Программное обеспечение анализа надежности коммерческого уровня (Windchill Quality Solutions, Isograph, RAM Commander…), содержит стандартный набор модулей, поддерживающих проведение проектного анализа систем. К ним относятся блок-схемы надежности, деревья отказов/деревья событий, модуль марковского моделирования. В соответствии с этим делением и структурирован материал книги. В главе 1 даны общие положения и введение в моделирование надежности. Глава 2 посвящена моделям анализа надежности резервированных последовательно-параллельных и мостиковых систем, использующим основные формулы теории вероятностей событий. В главе 3 изложены базовые понятия логико-вероятностных методов анализа надежности. В главе 4 описаны аппараты деревьев отказов, деревьев событий, приводятся многочисленные примеры построения деревьев отказов монотонных и немонотонных систем, рассмотрено применение диаграмм двоичных решений при программной реализации деревьев отказов, дан критический обзор моделей отказов по общей причине. Глава 5 посвящена марковскому моделированию надежностного поведения систем. В главе 6 рассмотрен современный аппарат анализа надежности сложных систем, основанный на агрегировании логико-вероятностных и марковских моделей надежности, динамические деревья отказов. В главе 7 обсуждаются подходы к проведению на ранних стадиях проектирования качественного и предварительного количественного анализа видов и последствий отказов.

Приложение 1 содержит основные формулы теории вероятностей событий, используемые при расчетах показателей надежности. В приложении 2 приведены основные положения и соотношения алгебры логики .В приложении 3 рассмотрены способы вычисления показателя средней наработки на отказ.

Книга будет полезна студентам и аспирантам, соответствующих специальностей, сотрудникам отделов надежности, проводящим анализ конкретных систем и знакомым с основами теории надежности, молодым специалистам, которые начали свое знакомство с надежностью не с изучения теоретических основ, а с использования специализированного программного обеспечения анализа надежности. Мы надеемся, что эта книга поможет создавать адекватные модели анализа надежности исследуемых систем, корректно задавать параметры модели, правильно интерпретировать полученные результаты.

Глава 1. Введение в моделирование надежности сложных систем

1.1. Основные термины и понятия

Для однозначности толкования основных понятий теории надежности в 1989 году (дата последнего издания - 01.07.2002) был утвержден государственный стандарт, регламентирующий терминологию теории надежности: ГОСТ27.002-89 “НАДЕЖНОСТЬ В ТЕХНИКЕ. Основные понятия, термины и определения”. Расширенный и тематически упорядоченный перечень терминов и определений, применяемых в теории надежности, приведен в справочнике [1]. Основными понятиями теории надежности являются

- *объект* - техническое изделие определенного целевого назначения, рассматриваемое в периоды проектирования, производства, испытаний и эксплуатации
- *система* - объект, представляющий собой совокупность элементов, взаимодействующих в процессе выполнения определенного круга задач и взаимосвязанных функционально
- *элемент системы* – объект, представляющий собой простейшую часть системы, отдельные части которого не представляют самостоятельного интереса в рамках конкретного рассмотрения
- *надежность* – свойство объекта сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения, обслуживания, ремонтов, хранения и транспортировки. Надежность – это сложное свойство, включающее (в зависимости от назначения и условий применения) такие свойства, как безотказность, долговечность, ремонтопригодность и сохраняемость
- *безотказность* – свойство объекта непрерывно сохранять работоспособность в течение некоторой наработки
- *долговечность* – свойство объекта сохранять работоспособность до наступления предельного состояния с перерывами на ТО и ремонт
- *ремонтопригодность* – свойство объекта, заключающееся в его приспособленности к предупреждению и обнаружению отказов и повреждений, к восстановлению работоспособности и исправности в процессе ТО и ремонта
- *сохраняемость* – свойство объекта непрерывно сохранять работоспособность в течение (и после) хранения и (или) транспортировки

- *исправность* – состояние объекта, при котором он соответствует всем требованиям нормативно-технической документацию. Неисправность – не соответствует хотя бы одному требованию
- *работоспособность* – состояние объекта, при котором он способен выполнять заданные функции, сохраняя значения основных параметров в пределах, установленных нормативно-технической документацией. Неработоспособность – состояние объекта, при котором он не выполняет хотя бы одну функцию.
- *отказ* – событие, заключающееся в нарушении работоспособности объекта
- *восстановление* – процесс обнаружения и устранения отказа
- *восстанавливаемый (невосстанавливаемый) объект*– объект, работоспособность которого в случае возникновения отказа подлежит (не подлежит) восстановлению в рассматриваемых условиях

Кроме надежности технические объекты могут характеризоваться и другими свойствами, определяющими их работоспособность. К ним относятся: живучесть, эффективность и безопасность. Вопросам сравнительного анализа этих свойств посвящены работы доктора технических наук, профессора Волика Б.Г [2-5]. Надежность, живучесть эффективность и безопасность определяют разные стороны изменений работоспособности объекта. Одни основываются на анализе источников нарушений работоспособности, другие – на анализе их последствий. Источники – различаются на внутренние и внешние источники. К внутренним относятся отказы технических средств объекта, ошибки в программах функционирования и эксплуатации, нарушения координации протекающих в объекте процессов, ошибки управляющего и обслуживающего персонала. Внешние - это случайные и/или преднамеренные воздействия на объект, способные нарушить его работоспособность. Надежность характеризует поведение объекта по отношению к внутренним источникам, живучесть – по отношению к внешним.

Живучесть – свойство объекта выполнять заданные функции, хотя бы в минимальном допустимом объёме, при внешних неблагоприятных воздействиях на него не предусмотренных заданными штатными условиями применения по назначению.

Последствия нарушений работоспособности по существу являются источником какого-либо ущерба той надсистемы, элементом которой является рассматриваемый объект. Несмотря на многообразие возможных последствий нарушений работоспособности, их можно обобщить в две принципиально различные группы (А и Б):

А. Потери целевой отдачи объекта. Это частичное или полное невыполнение предписанных функций, финансовые или материальные потери.

Б. Потери здоровья или жизни персонала и населения, попадающих в зону действия поражающих факторов объекта, ущерб окружающей среде сверх установленных норм.

Последствия группы А определяют свойство названное эффективностью, а группы Б – безопасностью

Эффективность – свойство объекта обеспечивать, на заданном интервале времени эксплуатации, целевую отдачу не ниже заданного уровня.

Эффективность может выступать индикатором сравнения конкурирующих вариантов объекта.

Безопасность – свойство объекта не допускать выхода в область возможного нахождения производственного персонала и/или населения поражающих для их жизни и здоровья факторов, а также факторов, наносящих ущерб окружающей среде сверх установленных норм.

1.2 Общие положения анализа надежности

На современном этапе развития теории надежности четко выделились четыре основных направления.

1. Разработка моделей и методов анализа надежности систем.

Модели анализа надежности делятся на два класса: *динамические*, когда происходящие события, отказы рассматриваются как процессы, развивающиеся во времени; *статические*, в которых состояния системы определяются наборами работоспособных и неработоспособных элементов в момент времени t.

В рамках динамических моделей применяются:

- моделирование систем марковскими, полумарковскими процессами [1,6-13]
- методы теории восстановления, полумарковских и регенерирующих процессов (в основном, используются асимптотические результаты либо для системы в целом, либо для отдельных резервированных звеньев) [1, 6, 14-17]
- статистическое имитационное моделирование (Монте Карло) [12, 16, 18-21]

В рамках статических моделей анализ надежности проводится следующими методами:

- метод, использующий основные формулы теории вероятностей (вероятность суммы и произведения событий, формула полной вероятности) и комбинаторики; применяется,

главным образом, для последовательно-параллельных, параллельно-последовательных структурных надежностных схем и схем m из n [1, 6, 7, 9, 11, 15]

- методы, основанные на записи логических условий, интересующих исследователя функций через состояния элементов системы с последующим применением теории алгебры логики (логико-вероятностные методы, используемые в деревьях отказов, схемах функциональной целостности, блок-схемах надежности) [22-30]

2. Подготовка исходных данных для системных моделей надежности:

- прогнозирование безотказности, включающее расчет надежности элементной базы на основе физики отказов элементов и статистических испытаний [31-40]
- прогнозирование ремонтопригодности, т.е. определение средних времен восстановления для стандартных операций обслуживания и ремонтов [41]
- анализ видов, последствий и критичности отказов, в процессе которого выявляются возможные типы отказов элементов, их частотные характеристики, степень влияния этих отказов на систему в целом [42, 43]

3. Управление надежностью систем на основе испытаний и эксплуатации [44-48]:

- разработка методов и организация определительных и контрольных испытаний на надежность
- проведение испытаний с целью приработки
- организация ускоренных испытаний на надежность
- статистический анализ функций распределения наработки до отказа и времени восстановления
- статистическая оценка показателей надежности по результатам испытаний и эксплуатации и последующая коррекция проектных решений
- обоснование и коррекция сроков и объемов технического обслуживания, количества ЗИП и ремонтного персонала

4. Автоматизация анализа надежности

Задача адекватного моделирования надежности систем сложной структуры может быть решена только с помощью автоматизации, причем, программное обеспечение анализа надежности должно включать в себя всю совокупность методов как статических, так и динамических моделей, поддержку прогнозирования безотказности, ремонтопригодности, анализа видов и последствий отказов.

Наиболее развитыми и известными отечественными программными средствами анализа надежности и безопасности являются: АРБИТР (ПК АСМ СЗМА) – программный комплекс автоматизированного структурно-логического моделирования и расчета надежности и безопасности систем; Автоматизированная система расчета надежности (АСРН-2000, 2002), реализующая стандартизованные модели безотказности радиоэлектронной элементной базы; АСОНИКА-К – программное обеспечение расчета надежности на основе методов статистического моделирования, содержащее также модели безотказности радиоэлектронной элементной базы; УНИВЕРСАЛ – программное обеспечение анализа надежности и безопасности, использующее полумарковское моделирование.

Лидерами зарубежных программных продуктов являются Isograph (Англия, США), ITEM iQRAS (Англия, США), RAM Commander (Израиль), Windchill Quality Solutions (Relex) (США). Это интегрированные программные средства, включающие различные методы анализа, реализующие разнообразные формы задания моделей (графы, деревья отказов, деревья событий, блок-схемы надежности), содержащие обширные базы исходных данных, имеющие развитый графический интерфейс пользователя, исчерпывающе документированные, имеющие как локальную, так и сетевую конфигурации, сопрягаемые по импорту-экспорту с базами данных, текстовыми редакторами, электронными таблицами, логистическим ПО, САПР. Ознакомится с возможностями современных программ анализа надежности можно в работах [30, 49-56]

Современный период развития техники характеризуется разработкой и внедрением сложных технических систем и комплексов. Создаются и успешно применяются полностью автоматизированные технологические комплексы. При разработке, испытаниях и эксплуатации таких комплексов особое значение имеют вопросы прогнозирования и обеспечения надежности. Важность этой проблемы обусловлена тем, что надежность в сложившихся представлениях определяется не только как одно из основных свойств системы, характеризующее её способность выполнять заданные функции. «Надежностным поведением» определяется техническая эффективность и безопасность функционирования систем. Авторы книги участвовали в решении вопросов анализа и обеспечения надежности и технической эффективности ряда проектов. В частности, проект по объектам уничтожения химического оружия (2002-2006гг), проекты по технологическому комплексу Штокмановского газоконденсатного месторождения (2005-2006гг, 2010-2012гг), проекты по модернизации кольцевого газопровода Московской Области (2007-2008гг) и по газопроводу Сахалин – Хабаровск - Владивосток (2008-2009гг) проекты по самолетам SSJ100 (2006-2011гг) и МС-21 (2011-2013гг). Требования к надежности подобных систем разнообразны и высоки. Здесь и требования по качественному анализу видов и последствий

отказов и отказоустойчивости, высокие требования по показателям надежности и коэффициенту сохранения эффективности, требования по показателям контролепригодности (полноте и глубине контроля, достоверности контроля).

Можно выделить три взаимодополняющих подхода к обеспечению надежности и технической эффективности проектируемых систем: повышение надежности элементной базы, введение резервирования, обеспечение многоуровневого характера функционирования.

Первый подход предполагает использование высоконадежных элементов, изготовленных в соответствие с современными технологиями и проверенных и отобранных на заданных режимах работы, защиту элементов от внешних вредных воздействий (климатических, механических, радиационных…), снижение нагрузок на элементы.

Если мероприятия первого подхода оказываются недостаточными и надежность комплектующих элементов не обеспечивает требуемую надежность системы, то применяют *резервирование*.

Резервирование - это метод повышения надежности системы путем введения дополнительных элементов и функциональных возможностей сверх минимально необходимых для нормального выполнения системой возложенных на нее функций.

В [1] выделены пять видов резервирования: структурное, временное, информационное, функциональное, нагрузочное. Структурное резервирование это метод повышения надежности объекта, предусматривающий использование избыточных элементов, входящих в физическую структуру объекта. Ещё одним способом обеспечения показателей надежности (в частности, коэффициента сохранения эффективности) является разработка систем с многоуровневым характером функционирования при возникновении отказов. Многоуровневость функционирования с надежностностных позиций означает, что при возникновении отказов система не остается на том же, например, 100%-ом уровне производительности, что имеет место в резервированных системах, и не снижает уровень производительности до 0% (отказ системы), а переключается на промежуточные, как правило, дискретные уровни, снижая свою эффективность (производительность).

В книге будут рассмотрены вопросы анализа надежности систем со структурным резервированием и с многоуровневым функционированием.

1.3. Основные показатели надежности технических объектов

Показатель надежности – техническая характеристика, количественным образом определяющая одно или несколько свойств, составляющих надежность объекта. Показатель надежности количественно характеризует, в какой степени данному объекту или данной группе объектов присущи определенные свойства, обуславливающие надежность. Показатели надежности могут иметь размерность или быть безразмерными. Исследуемые в рамках теории надежности объекты можно разделить на два больших класса – восстанавливаемые и невосстанавливаемые. Следует иметь в виду, что эти понятия относительные и зависят от выполняемых объектом функций и режимов работы. Одно и то же изделие - компьютер может рассматриваться как невосстанавливаемый объект, если он используется в системе управления ракеты, летящей на Марс, или как восстанавливаемый объект, если он работает в локальном режиме и используется для проведения бухгалтерских расчетов. Под восстановлением объекта понимается не только ремонт той или иной его части, но и их замена, а возможно, и полная замена всего объекта.

Показатели надежности также можно разделить на два класса – показатели надежности невосстанавливаемых и восстанавливаемых объектов.

Определения показателей надежности обычно дают в двух формах: вероятностной и статистической. Вероятностная форма обычно бывает удобнее при априорных аналитических расчетах надежности. Статистическая – при экспериментальном исследовании надежности технических объектов.

Важным понятием, присутствующим во многих формулировках показателей надежности, является *наработка.* Наработка это продолжительность или объем работы объекта, т.е. наработка может измеряться не только в единицах времени, но и единицах выработки продукции, пройденном расстоянии и пр. Например, в одном из зарубежных стандартов по расчету надежности устройств военно-морской техники частотные показатели имеют размерность 1/милю.

Модели и методы, представленные в данной книге, ориентированы на анализ по отношению к внезапным отказам, т.е. отказам, характеризующимся скачкообразным изменением значений одного или нескольких основных параметров объекта. Постепенные отказы, характеризующиеся постепенным изменением значений одного или нескольких основных параметров объекта, в данной книге не рассматриваются.

При определении показателей будем использовать следующие обозначения:

ξ_1 – случайная наработка объекта до первого отказа.

$\xi_1^{(i)}$ – реализация случайной величины ξ_1 для i-го объекта.

$F_1(t) = P(\xi_1<t)$ – распределение времени до первого отказа

$n(t)$ – число отказавших объектов к моменту времени t.

$N(t)$ – число работоспособных объектов к моменту времени t.

$\Delta n(t,t')$ – число объектов, отказавших на интервале времени (t,t').

1.3.1. Показатели надежности невосстанавливаемых объектов

Будем приводить вероятностную и статистическую формы представления показателей. Статистические показатели будем обозначать как и вероятностные но с “крышечкой” сверху. При статистическом представлении будем рассматривать схему, когда несколько объектов работают до отказа. В этом случае статистические показатели имеют простое частотное толкование и с ростом числа испытываемых объектов будут сходиться в пределе к аналогичным вероятностным показателям.

1. *Вероятность безотказной работы* объекта на интервале времени от 0 до t

$$P(t) = P(0,t) = \mathrm{Prob}(\xi_1 \geq t) = 1 - F_1(t) \ . \tag{1.1}$$

Вероятность безотказной работы определяется как вероятность того, что объект проработает безотказно в течение заданного времени (наработки) t при начале работы в нулевой момент времени:

Статистический показатель (точечная оценка) вероятности безотказной работы определяется как отношение числа объектов, безотказно проработавших до момента времени t, к числу объектов, исправных в начальный момент времени

$$\hat{P}(t) = \frac{N(t)}{N(0)}. \tag{1.2}$$

2. *Вероятность отказа объекта* на интервале времени от 0 до t

$$Q(t) = Q(0,t) = \mathrm{Prob}(\xi_1 < t) = F_1(t) = 1 - P(t) \ . \tag{1.3}$$

$$\hat{Q}(t) = \frac{n(t)}{N(0)} = 1 - \hat{P}(t) \tag{1.4}$$

3. *Вероятность безотказной работы объекта на интервале времени от t до t_0*

$$P(t, t+t_0) = \ \mathrm{Prob}(\xi_1 \geq t + t_0 / \xi_1 \geq t) = P(0, t+t_0)/P(0,t) = P(t+t_0)/P(t), \tag{1.5}$$

т.е. $P(t, t+t_0)$ - есть условная вероятность того, что случайная наработка объекта до отказа окажется больше величины $t+t_0$ при условии, что объект уже проработал безотказно до момента времени t.

При статистической интерпретации это есть отношение числа объектов, проработавших до момента времени $t+t_0$, к числу объектов, исправных к моменту t

$$\hat{P}(t, t+t_0) = N(t+t_0)/N(t) \tag{1.6}$$

4. *Плотность распределения отказов*

$$f(t) = \frac{d}{dt}F(t) = \frac{d}{dt}Q(t) = -\frac{d}{dt}P(t) \tag{1.7}$$

Статистическая плотность определяется как отношение числа отказов в интервале $(t,t+\Delta t)$ к произведению числа исправных объектов в начальный момент времени t=0 на длительность интервала Δt

$$\hat{f}(t) = \frac{n(t, t+\Delta t) - n(t)}{N(0)\Delta t} = \frac{N(t) - N(t, t+\Delta t)}{N(0)\Delta t} = \frac{\Delta n(t, t+\Delta t)}{N(0)\Delta t} \tag{1.8}$$

5. *Интенсивность отказов* объекта в момент времени t

$$\lambda(t) = \frac{1}{1-F(t)}\frac{d}{dt}F(t) = \frac{f(t)}{P(t)} \tag{1.9}$$

$\lambda(t)$ – условная плотность вероятности отказа объекта к моменту времени t при условии, что до этого момента времени отказа объекта не было.

Статистическое определение показателя

$$\hat{\lambda}(t) = \frac{n(t, t+\Delta t) - n(t)}{N(t)\Delta t} = \frac{N(t) - N(t, t+\Delta t)}{N(t)\Delta t} = \frac{\Delta n(t, t+\Delta t)}{N(t)\Delta t} \tag{1.10}$$

На рис.1.1. показана так называемая “ваннообразная” кривая, иллюстрирующая поведение интенсивности отказов на всех основных периодах жизни технических объектов. Период приработки, на котором выявляются и устраняются ошибки проектирования и производственные недостатки, имеет убывающую $\lambda(t)$. Для моделирования этого этапа следует применять функции распределения с убывающей условной плотностью, например, распределение Вейбулла с параметром формы < 1. Период нормальной эксплуатации, при котором отказы вызываются случайными факторами и имеют постоянную интенсивность, адекватно описывается экспоненциальным распределением. В период старения, обусловленный износом оборудования,

наблюдается возрастание λ(t). Здесь применяют “стареющие” распределения с возрастающей функцией интенсивности, например, распределение Вейбулла с параметром формы > 1.

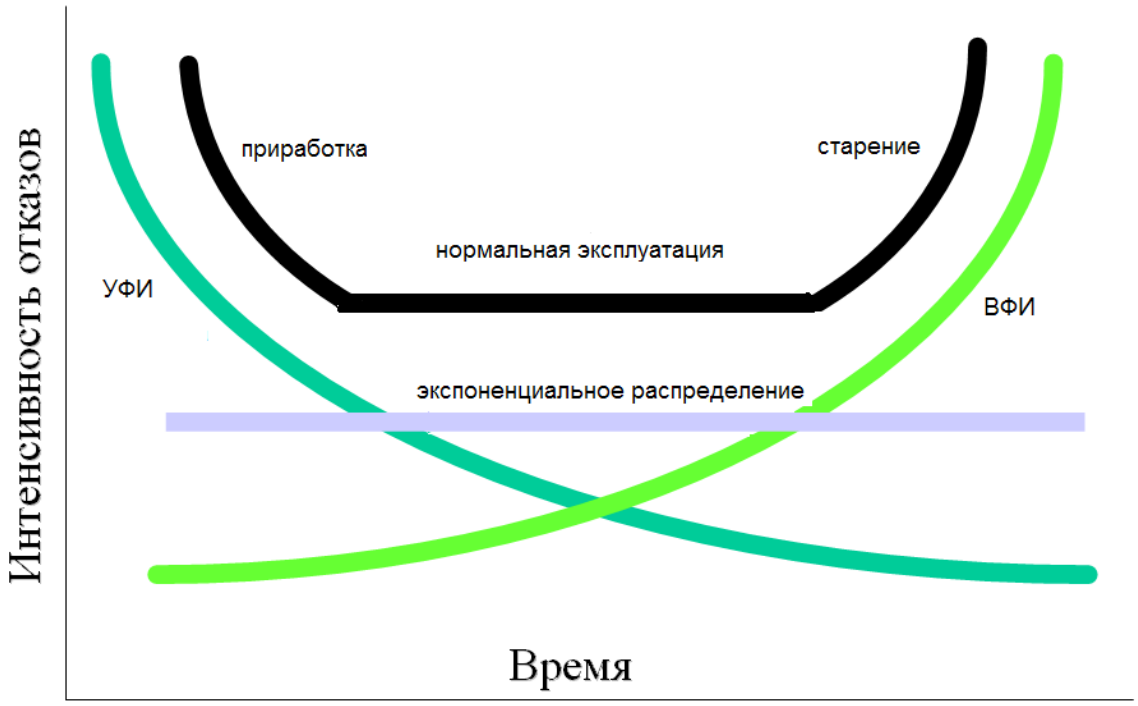


Рис.1.1. “Ваннообразная” кривая (ВФИ – возрастающая функция интенсивности, УФИ – убывающая функции интенсивности)

6. *Средняя наработка объекта до первого отказа* (математическое ожидание случайной наработки до первого отказа)

$$T_1 = M[\xi_1] = \int_0^\infty \tau f(\tau)dx = \int_0^\infty \tau dQ(\tau) = \int_0^\infty P(\tau)d\tau \qquad (1.11)$$

$$\hat{T}_1 = \frac{1}{N(0)} \sum_{i=1}^{N(0)} \xi_1^i \qquad (1.12)$$

Показатели (1.1÷1.12) характеризуют случайное время появления первого отказа, поэтому они получили название – *показатели безотказности.*

7. *Гамма- процентная наработка до отказа* T_γ

Иногда бывает важно узнать значение наработки до отказа объекта, которая гарантируется с заданной вероятностью γ. Очевидно, что величина T_γ определяется как корень уравнения P(t)= γ.

Используя формулу (1.9) можно записать $\lambda(t) = -\frac{\frac{d}{dt}P(t)}{P(t)}$. Это соотношение позволяет выразить вероятность безотказной работы через интенсивность отказов. Для этого поменяем левую и правую части местами и возьмем от них интеграл в пределах от нуля до t: $\int_0^t \frac{dP(\tau)}{P(\tau)} = -\int_0^t \lambda(\tau)d\tau$.

Отсюда получаем $\ln(P(t)) = -\int_0^t \lambda(\tau)d\tau$ и далее

$$P(t) = e^{-\int_0^t \lambda(\tau)d\tau} \tag{1.13}$$

Полученное выражение (1.13) справедливо для любых распределений случайного времени работы до отказа. Иногда это соотношение называют “основным законом надежности”. Для экспоненциального распределения (1.13) преобразуется к виду

$$P(t) = e^{-\lambda t} \tag{1.14}$$

На основании (1.13), выражение для средней наработки до отказа (1.11) можно записать в виде

$$T_1 = \int_0^\infty e^{-\int_0^t \lambda(\tau)d\tau} dt \tag{1.15}$$

Для экспоненциального распределения имеем

$$T_1 = \frac{1}{\lambda} \tag{1.16}$$

1.3.2. Показатели надежности восстанавливаемых объектов

Все приведенные выше показатели безотказности могут быть применены и для исследования надежности восстанавливаемых объектов. Однако так как функционирование восстанавливаемых объектов имеет свои особенности, то для характеристики этих особенностей вводятся специальные показатели.

1. *Средняя наработка между отказами T.*

Процесс функционирования восстанавливаемого объекта представляет собой последовательность чередующихся случайных интервалов работы (ξ_k) и простоя (θ_k) (рис 1.2.). Простои наступают после отказа объекта, когда над ним проводятся восстановительные операции. Восстановление работоспособности может быть как полным (замена на аналогичный новый объект), так и частичным (например, ремонт только неисправной части).

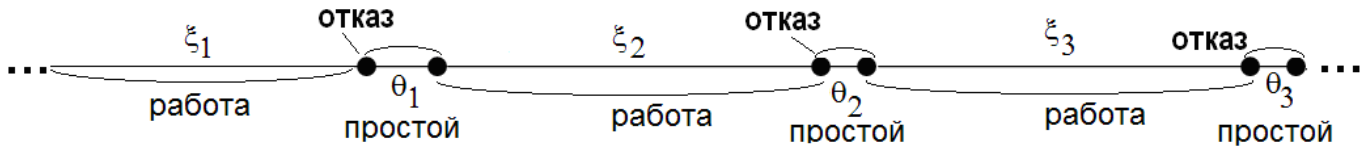


Рис.1.2. Стационарный участок функционирования восстанавливаемого объекта

В общем случае, при неполном восстановлении случайные времена ξ_k работы после k-1-го восстановления и до k-го отказа имеют разное распределение с плотностями $f_k(t)$. В этом случае средняя наработка между отказами T вычисляется как

$$T = \lim_{k\to\infty} M[T_k] = \lim_{k\to\infty} \frac{1}{k}\sum_{i=1}^{k} T_i \ , \qquad (1.17)$$

где каждая из средних наработок объекта от момента окончания k-1-го восстановления до k-го отказа определяется как

$$T_k = M[\xi_k] = \int_0^\infty t f_k(t)dt \qquad (1.18)$$

Или статистически

$$\hat{T}_k = \frac{1}{N(0)}\sum_{i=1}^{N(0)} \xi_k^i \qquad (1.19)$$

Если мы будем описывать процесс функционирования восстанавливаемого объекта с полным восстановлением его работоспособности, то в этом случае величины ξ_k и θ_k взаимно независимы и их распределение не зависит от k. В этом случае вычисления показателя средней наработки между отказами (1.17, 1.18) упрощаются, а процесс $\{\xi,\theta\}$ носит название альтернирующего процесса.

2. *Среднее время восстановления* $\tau_в$ или математическое ожидание случайного времени восстановления θ:

$$\tau_в = M[\theta] = \int_0^\infty t g(t)dt = \int_0^\infty t dG(t) = \int_0^\infty (1-G(t))dt \ . \qquad (1.20)$$

Здесь G(t) – функция распределения случайного времени восстановления, g(t) – плотность распределения времени восстановления

Статистическое определение

$$\hat{\tau}_в = \frac{1}{N(0)} \sum_{i=1}^{N(0)} \theta^i \ . \qquad (1.21)$$

3. *Интенсивность восстановления* объекта

$$\mu(t) = \frac{1}{1-G(t)} \frac{d}{dt} G(t) = \frac{g(t)}{1-G(t)} \qquad (1.22)$$

$\mu(t)$ – условная плотность восстановления объекта в момент времени t при условии, что до этого момента времени восстановление объекта не произошло.

Статистическое определение:

$$\hat{\mu}(t) = \frac{\Delta n_в(t, t+\Delta t)}{N_в(t)\Delta t} \ , \qquad (1.23)$$

т.е. $\hat{\mu}(t)$ определяется как отношение числа восстановленных объектов в интервале $(t,t+\Delta t)$ ($\Delta n_в(t,t+\Delta t)$) к произведению числа еще не восстановленных объектов к моменту времени t ($N_в(t)$) на длительность интервала Δt.

4. Важной количественной характеристикой потока отказов восстанавливаемого объекта в момент времени t является показатель - *параметр потока отказов ω(t)*. Этот показатель определяется как производная по времени от среднего числа отказов на интервале (0,t) – $N_{ср}(t)$:

$$\omega(t) = \frac{dN_{ср}(t)}{dt}. \qquad (1.24)$$

Статистическое определение

$$\hat{\omega}(t) = \frac{\Delta n(t, t+\Delta t)}{N_0 \Delta t} \ , \qquad (1.25)$$

где N_0 – количество работоспособных объектов в момент времени t.

Выражение (1.24) не является расчетной формулой. Вопрос аналитического определения показателя ω(t) будет рассмотрен при изучении логико-вероятностных и марковских моделей анализа надежности.

Существует ряд комплексных показателей надежности восстанавливаемых объектов, характеризующих их свойства безотказности и ремонтопригодности. Важнейшими из них являются показатели готовности и оперативной готовности.

1. *Коэффициент готовности $K_г(t)$.*

$K_г(t)$ – есть вероятность застать объект в работоспособном состоянии в произвольный момент времени t. На практике обычно используется асимптотическое значение показателя, обозначаемое как $K_г$ и называемое стационарным коэффициентом готовности:

$$K_г = \lim_{t\to\infty} K_г(t) = \frac{T}{T + \tau_в}, \tag{1.26}$$

т.е. стационарный коэффициент готовности определяется как отношение средней наработки между отказами к сумме средней наработки между отказами и среднего времени восстановления.

Вопрос аналитического определения нестационарного коэффициента готовности будет подробно рассмотрен при изучении марковских и логико-вероятностных моделей надежности.

Статистическое определение показателя

$$\hat{K}_г(t) = \frac{N_t}{N(0)}, \tag{1.27}$$

где N_t – число объектов работоспособных в момент времени t.

2. *Коэффициент оперативной готовности $K_{ог}(t,t_0)$.*

$K_{ог}(t,t_0)$ – вероятность того, что объект окажется работоспособным в произвольный момент времени t и далее проработает безотказно в течение интервала времени (t,t_0).

$$K_{ог}(t,t_0) = K_г(t)P(t,t_0). \tag{1.28}$$

Статистическое определение

$$\hat{K}_г(t,t_о) = \frac{N(t,t_0)}{N(0)}, \tag{1.29}$$

где $N(t,t_0)$ – число объектов исправных в момент t и безотказно проработавших в интервале (t,t_0).

3. *Коэффициент технического использования $K_{ти}$*

$$K_{ти} = \frac{T}{T + \tau_в + \tau_п} \tag{1.30}$$

Показатель аналогичен стационарному коэффициенту готовности, но учитывает не только время ремонта, но и простои объекта, связанные с техническими осмотрами и профилактическим обслуживанием $\tau_п$.

При проведении анализа надежности необходимо помнить, что коэффициент готовности является “точечным” показателем, определяющим надежность объекта в заданный момент времени, в отличии от вероятности безотказной работы, характеризующей надежность на интервале. Для демонстрации этого факта на рис 1.3. приведена временная эпюра работы 10

устройств, поставленных на испытание. Показатели коэффициент готовности и вероятность безотказной работы определяются каждый час в течение 10 часов.

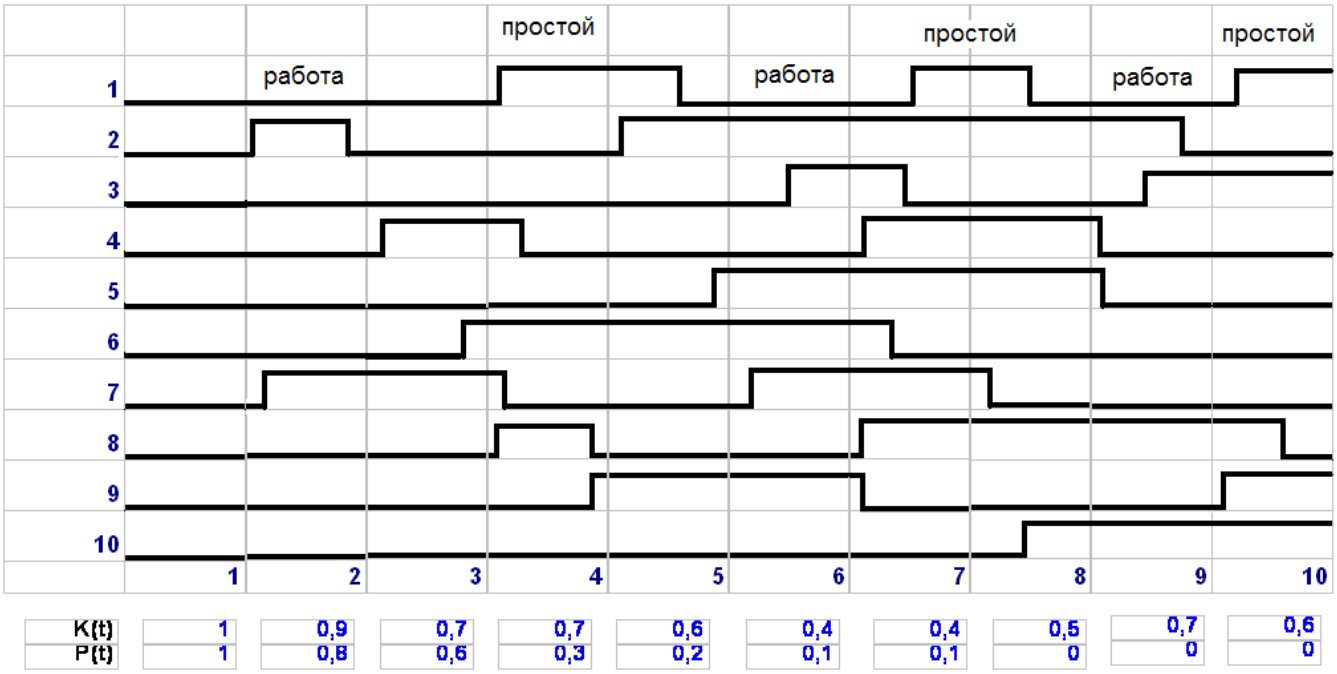


Рис 1.3. Статистическое определение коэффициента готовности и вероятности безотказной работы.

4. *Средняя наработка на отказ* $T_{на.}$

В нормативной (например, ГОСТ 27.002-89, ГОСТ 27.003-90) и справочной литературе [1] приводится определение ещё одного показателя, а именно средняя наработка на отказ ($T_{на}$), который регламентируется как один из основных показателей безотказности для восстанавливаемых объектов,

$$T_{на}(t_н) = \frac{t_н}{M\{n(t_н)\}}, \qquad (1.31)$$

т.е., отношение суммарной наработки объекта ($t_н$) к математическому ожиданию числа отказов $n(t_н)$ за эту наработку.

Статистическое определение

$$\hat{T}_{на}(t_н) = \frac{t_н}{n(t_н)}. \qquad (1.32)$$

Этот показатель внесен в нормативную литературу в начале 80-х годов не в качестве дополнительного показателя, характеризующего какую-либо особенность применения объекта,

которую не отражают другие показатели, а взамен показателя средней наработки между отказами. Приведём результаты критического анализа показателя $T_{на}$.

- показатель $T_{на}$ является функцией наработки, поэтому нормировать и вычислять его необходимо на заданной наработке, т.е. правильно обозначать его не $T_{на}$, а $T_{на}(t_н)$.
- сравним наработку на отказ с другими наработками, фигурирующими в определениях показателей. Средняя наработка до отказа (T_1) характеризует только наработки до первого отказа. Так как все показатели в нормативной документации определены для полностью исправного начального состояния объекта, то для распределений с неубывающей функцией интенсивности отказов средняя наработка до первого отказа будет наибольшей. Средняя наработка между отказами (Т) не охватывает наработки до первого отказа, а усредняет (на бесконечности) наработки после первого отказа. Для распределений с неубывающей функцией интенсивности отказов средняя наработка между отказами будет наименьшей. Отметим, что все резервированные структуры имеют возрастающую функцию интенсивности отказов. Средняя наработка на отказ ($T_{на}(t_н)$) включает в общем случае и наработку до отказа и наработки между отказами. Таким образом, из приведенных объяснений должно следовать следующее соотношение между показателями: $T_1 \geq T_{на}(t_н) \geq T$. Причем, оно верно и для убывающих распределений наработки до отказа, только с переменой символов больше или равно на меньше или равно. Но это не выполняется, что будет продемонстрировано на примерах.
- методов вычисления $T_{на}(t_н)$ нет ни в одном известном литературном источнике. Имеется в виду, что нет четко сформулированного способа получения значений показателя и примеров его вычисления для резервированных восстанавливаемых структур. Связано это с тем, что наработка на заданном календарном времени функционирования объекта является случайной величиной.
- практически всегда, когда нормируется или вычисляется показатель $T_{на}$ имеется в виду показатель Т – средняя наработка между отказами, а иногда – средняя наработка до отказа T_1.
- при $t_н \to \infty$ $T_{на}(t_н) \to T$, именно поэтому (возможно и не понимая) говорят и пишут $T_{на}$, хотя определяют его асимптотическое (стационарное) значение, равное Т.
- при $t_н \to 0$ показатель $T_{на}(t_н)$ растет, в том числе до бесконечности.
- статистическое определение допустимо лишь в предположении эргодичности (т.е. замены наблюдений за множеством однотипных объектов на длительные наблюдения за одним

объектом). Причем, для получения приемлемой точности оценки, необходима хорошая статистика (число отказов не должно быть малым). Представительная статистика может быть получена только при достаточно длительных наблюдениях, что опять же приводит к большим величинам $t_н$, а значит полученное значение $\hat{T}_{на}(t_н)$ будет близко к средней наработке между отказами T.

Показатель средняя наработка на отказ ($T_{на}(t_н)$) если и должен присутствовать в нормативной литературе, то только в качестве специального показателя для объектов с заданной строго определённой наработкой (по истечении которой объект снимается с эксплуатации, даже если не закончено выполнение им определённого задания). Авторам подобные объекты не известны. *Из основных показателей он должен быть убран, а показатель средняя наработка между отказами введен в список основных показателей надежности.*

Ещё раз подчеркнем, что практически всегда записывается в требованиях и оценивается при проектном анализе показатель средняя наработка между отказами, а называют её средней наработкой на отказ! При этом никогда не указывают наработку, на которой необходимо определить среднюю наработку на отказ.

В зарубежной нормативной и технической литературе показателя аналогичного $T_{на}(t_н)$ нет. В зарубежных стандартах и специальной литературе присутствуют показатели MTTF – среднее время до отказа и показатель MTBF- среднее время между отказами. MTTF определяется также как и T_1 – средняя наработка до отказа. Показатель MTBF равен сумме средней наработки между отказами и среднего времени восстановления $MTBF = T + \tau_в$.

Примеры вычисления показателя средней наработки на отказ даны в приложении 3.

5. *Коэффициент сохранения эффективности $К_{с.\ эф.}(t)$.*

Отношение значения показателя эффективности использования объекта по назначению за определенную продолжительность эксплуатации к номинальному значению этого показателя, вычисленному при условии, что отказы объекта в течение того же периода не возникают. Этот показатель характеризует степень влияния отказов объекта на эффективность применения его по назначению. Содержание понятия эффективности и точный смысл показателя эффективности при нормировании $К_{с.\ эф.}(t)$ определяются техническим заданием и вводятся в нормативно-техническую и проектную документацию.

$$К_{с.\ эф.}(t) = М\{Э(t)\}/Эн(t) . \qquad (1.33)$$

1.4. Основные аналитические методы анализа надежности систем

В книге будут излагаться три основных аналитических метода оценки надежности систем:

- метод, использующий основные теоремы теории вероятностей случайных событий (см. приложение 1) и комбинаторные формулы
- логико-вероятностные методы
- метод марковских процессов.

Основными визуальными способами представления надежностной модели системы являются блок-схемы надежности, деревья отказов. Для расчетов по блок-схемам используются, в основном, формулы и логико-вероятностные методы. При применении деревьев отказов используются логико-вероятностные методы. Кроме того, известны и применяются способы визуального задания модели в виде графов связи [57] и схем функциональной целостности [28, 29]. Графы связи в основном применяются для задания моделей надежности и пропускной способности сетевых структур. Недостатком графов связи является (если говорить о классическом их применении) невозможность представления структур с повторяющимися элементами, структур m из n и немонотонных моделей[1]. Классические блок-схемы практически имеют те же недостатки, однако принципиально позволяют отображать и учитывать повторяющиеся элементы в разных частях схемы. Эти недостатки в основном определяются тем, что, во-первых, было принято в узлах, куда входит несколько связей, реализовывать по умолчанию логическую функцию ИЛИ. А, во-вторых, не предусматривается одновременного присутствия на схеме как прямых, так и инверсных выходов с блоков и схемы в целом. Деревья отказов не имеют ограничений на представление любой логической функции отказов/работоспособности. Но строить деревья достаточно сложно, вид представления абсолютно не похож на функциональную схему, можно строить одну и ту же логическую функцию несколькими разными способами, а поэтому проверять правильность (особенно другому человеку) ещё сложнее, чем строить. Схемы функциональной целостности являются очень удобным способом визуального задания моделей, объединяющим лучшие стороны блок-схем и деревьев отказов. Они существенно расширяют возможности представления моделей как раз за счет того, что снимают указанные выше ограничения графов и блок-схем.

Перечисленные способы представления структур в классическом варианте ориентированы на применение статических моделей и для расчетов используются два первых метода, а именно,

[1] Пояснения по повторяющимся элементам и немонотонным логико-вероятностным моделям будут даны в главах 2 и 4 соответственно

метод, использующий три основные теоремы теории вероятности случайных событий и логико-вероятностные методы. В общем случае, же в программных продуктах, используют логико-вероятностные методы, а формулы теории вероятностей применяют лишь при “ручных” расчетах не очень многоразмерных и сложных структур. И самое главное, логико-вероятностные методы (имеется в виду бинарная алгебра логики и для элементов и для системы в целом) не выходят за рамки трех основных теорем теории вероятностей событий и поэтому ничего дополнительно учесть не позволяют. Можно сказать, что они являются формальным аппаратом применения этих трех теорем.

Необходимо отметить, что логико-вероятностные методы позволяют моделировать только системы с нагруженным резервированием и независимым функционированием элементов. Вычисляются только мгновенные показатели в момент времени t. Для учета каких-либо зависимостей, вычисления показателей не только мгновенных, но и интервальных, показателей, определяемых на бесконечности (типа средних наработок), применяются другие методы, в частности, методы марковского моделирования, которые будут рассмотрены в главе 5.

Глава 2. Метод анализа надежности, использующий основные теоремы теории вероятностей случайных событий

2.1 Анализ надежности последовательно-параллельных невосстанавливаемых систем

Приведем ряд терминов, используемых при анализе надежности резервированных систем. Определение терминов взято из [1].

Основной (рабочий) элемент – элемент основной физической структуры системы, минимально необходимый для выполнения возложенных на нее задач.

Резервный элемент – элемент, предназначенный для обеспечения работоспособности системы в случае отказа основного элемента.

Общее резервирование – резервирование, при котором резервируется система в целом.

Раздельное резервирование – резервирование, при котором резервируются отдельные компоненты системы.

Нагруженный резерв – резервный элемент, находящийся в том же режиме, что и основной.

Ненагруженный резерв – резервный элемент, практически не несущий нагрузок.

Облегченный резерв – резервный элемент, находящийся в менее нагруженном режиме, чем основной.

Начнем наше рассмотрение с простейших схем нагруженного резервирования, так называемых последовательно-параллельных структур (систем). Удобной графической интерпретацией последовательно-параллельных структур являются блок-схемы надежности (в зарубежной литературе – reliability block diagram или RBD). Эта визуальная модель представляет надежностные взаимосвязи между компонентами и не всегда соответствует реальному соединению элементов системы. Расчет показателей надежности в рамках этих моделей может осуществляться различными методами – формульными, логико-вероятностными, интегральными соотношениями, статистическим моделированием. В данном разделе мы будем рассматривать простейший метод расчета показателей надежности (безотказности) невосстанавливаемых последовательно-параллельных систем, основанный на использовании соотношений теории вероятностей, полученных из теорем полной вероятности и теорем сложения и умножения вероятностей.

Хотя метод ориентирован на произвольное распределение случайного времени возникновения отказов элементов, мы ограничимся рассмотрением экспоненциального случая. Для

одного “экспоненциального” элемента формулы основных показателей безотказности сведены в таблицу 2.1.

Таблица 2.1. Основные показатели безотказности элемента с экспоненциально распределенной наработкой до отказа.

наименование показателя	аналитическое выражение
Вероятность безотказной работы на интервале (0,t)	$e^{-\lambda t}$
Вероятность отказа на интервале (0,t)	$1-e^{-\lambda t}$
Плотность распределения случайной наработки до отказа	$\lambda e^{-\lambda t}$
Интенсивность отказов	Λ
Средняя наработка до отказа	$1/\lambda$

1. *Последовательное соединение элементов*

Последовательное соединение элементов представляет собой неизбыточную структуру без резервирования. Отказ каждого из элементов приводит к отказу системы в целом. Блок-схема надежности последовательного соединения n элементов представлена на рис.2.1.

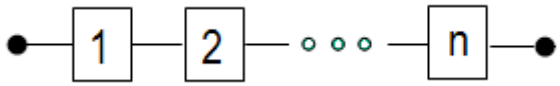


Рис. 2.1. Блок-схема надежности последовательного соединения.

Вероятность безотказной работы P(t) для последовательного соединения определяется как произведение вероятностей безотказной работы ее элементов $p_i(t)$

$$P(t) = p_1(t)p_2(t)...p_n(t) = \prod_{i=1}^{n} p_i(t). \qquad (2.1)$$

Для экспоненциального случая:

$$P(t) = e^{-\lambda_1 t} \cdot e^{-\lambda_2 t} \cdot ... \cdot e^{-\lambda_n t} = e^{-(\lambda_1+\lambda_2+...+\lambda_n)t} . \qquad (2.2)$$

Интенсивность отказов определяется как сумма интенсивностей отказов элементов системы:

$$\lambda(t) = -\frac{P'(t)}{P(t)} = \lambda_1 + \lambda_2 + ... + \lambda_n = \lambda_\Sigma . \qquad (2.3)$$

Средняя наработка до отказа есть

$$T = \int_0^\infty P(t)dt = \int_0^\infty e^{-\lambda_\Sigma t}dt = -\frac{1}{\lambda_\Sigma} e^{-\lambda_\Sigma t}\Big|_0^\infty = \frac{1}{\lambda_\Sigma} . \qquad (2.4)$$

2. *Параллельное соединение элементов*

Параллельное соединение элементов представляет собой избыточную структуру с нагруженными (активными) резервными элементами, показанную на блок-схеме рис.2.2

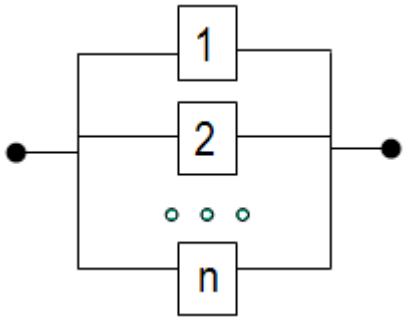


Рис.2.2. Параллельное соединение элементов.

Одновременно работают все n элементов. Система работоспособна пока работает хотя бы один элемент из n. Отказом системы является отказ всех n ее элементов. Тогда вероятность отказа системы Q(t) будет равна произведению вероятностей отказа ее элементов $q_i(t)$:

$$Q(t) = \prod_{i=1}^{n} q_i(t). \tag{2.5}$$

Вероятность безотказной работы:

$$P(t) = 1 - \prod_{i=1}^{n} (1 - p_i(t)). \tag{2.6}$$

И для равнонадежных элементов

$$P(t) = 1 - (1 - p(t))^n = 1 - (q(t))^n. \tag{2.7}$$

Рассмотрим частные случаи параллельного соединения из двух и трех элементов.

3. *Дублированная схема*

Вероятность безотказной работы дублированной схемы может быть представлена через произведение вероятностей независимых событий отказа ее элементов

$$P(t) = 1 - (1 - p_1(t))(1 - p_2(t)) \tag{2.8}$$

или как сумма вероятностей совместных событий их исправной работы

$$P(t) = p_1(t) + p_2(t) - p_1(t)p_2(t). \tag{2.9}$$

При экспоненциальном распределении получаем

$$P(t) = e^{-\lambda_1 t} + e^{-\lambda_2 t} - e^{-(\lambda_1 + \lambda_2)t}. \tag{2.10}$$

Наработка до отказа есть

$$T = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} - \frac{1}{\lambda_1 + \lambda_2}. \qquad (2.11)$$

И при равнонадежных элементах имеем

$$P(t) = 2e^{-\lambda t} - e^{-2\lambda t} \ . \qquad (2.12)$$

$$\lambda(t) = \frac{2\lambda e^{-\lambda t} - 2\lambda e^{-2\lambda t}}{2e^{-\lambda t} - e^{-2\lambda t}} = \frac{2\lambda - 2\lambda e^{-\lambda t}}{2 - e^{-\lambda t}}. \qquad (2.13)$$

$$T = \frac{3}{2\lambda}. \qquad (2.14)$$

Исследование выражения (2.13) показывает, что интенсивность отказов дублированной схемы, состоящей из элементов с постоянными интенсивностями отказов, является функцией времени, при больших временах стремящейся к λ одного элемента ($\lambda(0) = 0; \lambda(t) \underset{t\to\infty}{\to} \lambda$). График $\lambda(t)$ дублированной схемы показан на рис.2.3.

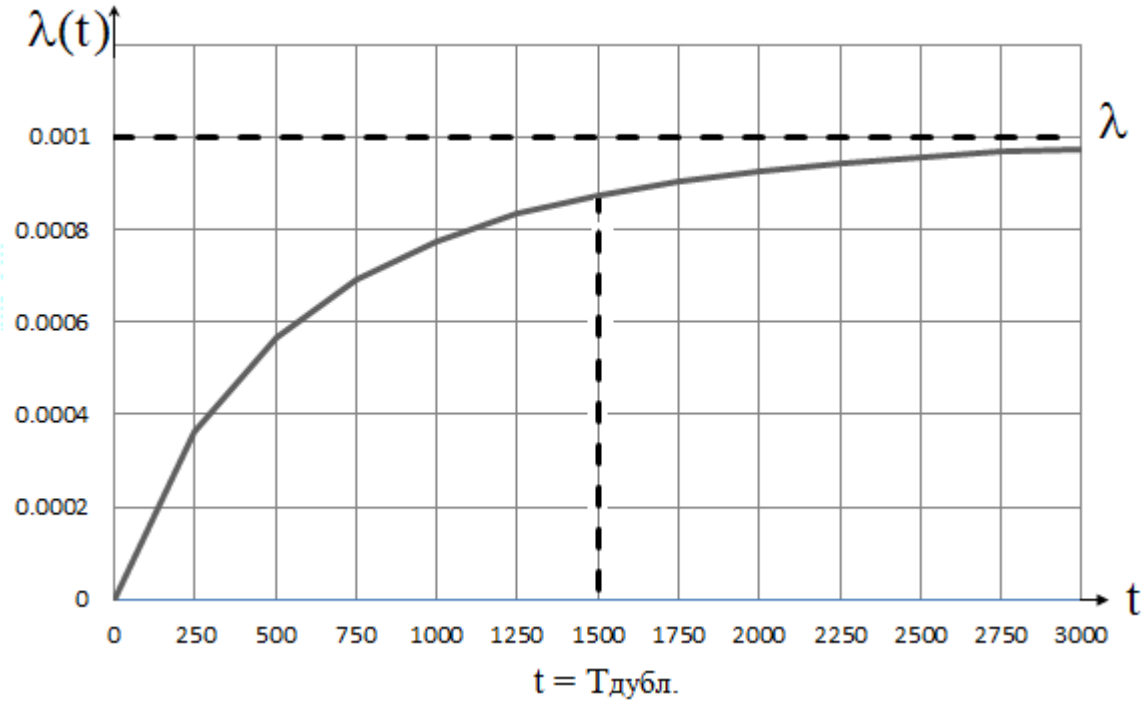


Рис.2.3. Зависимость от времени интенсивности отказов дублированной схемы.

4. *Троированная схема*

Троированная схема имеет три параллельно работающих нагруженных элемента. Отказ схемы происходит при отказе всех трех элементов.

Вероятность безотказной работы равна

$$P(t) = 1-(1-p_1(t))(1-p_2(t))(1-p_3(t)) \tag{2.15}$$

или

$$P(t) = p_1(t) + p_2(t) + p_3(t) - p_1(t)p_2(t) - p_1(t)p_3(t) - p_2(t)p_3(t) + p_1(t)p_2(t)p_3(t) \tag{2.16}$$

Для экспоненциального случая и равнонадежных элементов

$$P(t) = 3e^{-\lambda t} - 3e^{-2\lambda t} + e^{-3\lambda t} \tag{2.17}$$

Средняя наработка до отказа

$$T = \frac{11}{6\lambda} \tag{2.18}$$

5. *Схемы "m из n"*

Рассмотрим общий случай схем параллельного соединения n элементов – схему "m из n". Такая схема считается работоспособной пока работают хотя бы m элементов из n. Отказом схемы является отказ минимум n-m+1 ее элементов, т.е. n-m+1**,** n-m+2, …, n:

Рассмотрим общую процедуру вычисления показателей надежности, основанную на формировании подмножества состояний работоспособности или подмножества состояний отказа множества всех возможных состояний схемы, отличающихся различными комбинациями работоспособных и отказавших элементов. Всего имеем n+1 событие A_0, A_1, … A_n, из которых n-m+1 событие соответствует работоспособности схемы (i=0÷n-m), а m событий соответствуют отказу схемы (i=n-m+1÷n). Каждое событие формируется из C_n^i комбинаций i отказавших и n-i работоспособных элементов:

Очевидно, что события A_0, A_1, … A_n составляют полную группу несовместных событий. Тогда вероятность безотказной работы P(t) и вероятность отказа Q(t) могут быть вычислены как сумма вероятностей возникновения соответствующих событий:

$$P(t) = P(A_0 \bigcup A_1 ... \bigcup A_i ... \bigcup A_m) = \sum_{i=0}^{n-m} C_n^i p^{n-i} q^i \tag{2.19}$$

$$Q(t) = P(A_{m+1} \bigcup A_{m+2} ... \bigcup A_n) = \sum_{i=n-m+1}^{n} C_n^i p^{n-i} q^i \tag{2.20}$$

Если m < (n+1)/2, то вероятность безотказной работы целесообразно вычислять как 1-Q(t).

Таблица.2.2. Формулы для расчета вероятности безотказной работы схем “m из n”

	n = 1	n = 2	n = 3	n = 4	n = 5
m = 2	$1-q^2$				
m = 3	$1-q^3$	p^3+3p^2q			
m = 4	$1-q^4$	$1-(4pq^3+q^4)$	p^4+4p^3q		
m = 5	$1-q^5$	$1-(5pq^4+q^5)$	$p^5+5p^4q+10p^3q^2$	p^5+5p^4q	
m = 6	$1-q^6$	$1-(6pq^5+q^6)$	$1-(15p^2q^4+6pq^5+q^6)$	$p^6+6p^5q+15p^4q^2$	p^6+6p^5q

6. *Мажоритарная схема ”2 из 3”*

Наиболее распространенной конфигурацией схем “m из n” является конфигурация “2 из 3”. Часто эта конфигурация используется в информационных системах (аналоговых или дискретных), в которых происходит сравнение значений выходных сигналов и выбор правильного значения по большинству. Такие схемы получили название мажоритарных (рис.2.4).

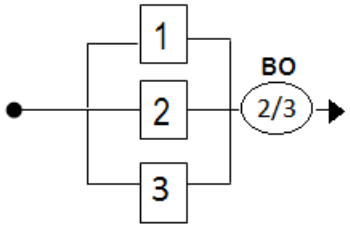


Рис. 2.4. Блок-схема надежности мажоритарной структуры “2 из 3”

Предполагается, что в мажоритарных схемах присутствует специальное устройство, называемое восстанавливающим органом (ВО), который и осуществляет операцию выбора уровня (значения) выходного сигнала схемы. В общем случае ВО не обладает идеальной надежностью, что должно быть учтено при составлении выражений для вычисления показателей надежности. Так как отказ ВО сразу приводит к отказу всей схемы, то вероятность безотказной работы определяется как произведение вероятностей безотказной работы параллельного соединения “2 из 3” и восстанавливающего органа:

$$P(t) = P_{2/3}(t)*P_{BO}(t), \tag{2.21}$$

где

$$P_{2/3}(t) = p^3 + 3p^2q = 3p^2 - 2p^3. \tag{2.22}$$

Пусть $P_{BO}(t) = 1$, тогда для экспоненциального распределения

$$P(t) = 3e^{-2\lambda t} - 2e^{-3\lambda t}; \quad T = \frac{5}{6}\lambda. \tag{2.23}$$

Значение средней наработки до отказа мажоритарной схемы оказалось хуже не только троированной и дублированной схемы, но и хуже, чем наработка одного нерезервированного элемента. Таким образом, применение мажоритарных структур *без восстановления* целесообразно лишь с точки зрения повышения достоверности выходной информации на коротких интервалах времени.

7. *Расчет средней наработки до отказа*

Рассмотрим случай резервированных структур “1 из n”, состоящих из равнонадежных экспоненциально распределенных элементов: $T = \int_0^\infty P(t)dt = \int_0^\infty [1-(1-e^{-\lambda t})^n]dt.$

Применим процедуру, описанную в [15]. Сделаем замену переменных $1 - e^{-\lambda t} = x; t = \frac{1}{\lambda}\ln\frac{1}{1-x}; \; dt = \frac{dx}{\lambda(1-x)}.$

Тогда средняя наработка до отказа для схем “1 из n” будет определена как

$$T = \frac{1}{\lambda}\int_0^1 \frac{1-x^n}{1-x}dx = \frac{1}{\lambda}\int_0^1 (1 + x + ... + x^{n-1})dx = \frac{1}{\lambda}(1 + \frac{1}{2} + ... + \frac{1}{n}) \tag{2.24}$$

А средняя наработка до отказа для схем “m из n” равна

$$T = \frac{1}{\lambda}\left(\frac{1}{n} + \frac{1}{n-1} + \frac{1}{n-2}... + \frac{1}{m}\right). \tag{2.25}$$

В таблицу сведены выражения для средних наработок до отказа основных видов схем “m из n”, полученные по формулам (2.24 ,2.25).

Таблица 2.3. Формулы для расчета средних наработок до отказа схем “m из n”.

	m = 1	m = 2	m = 3	m = 4	m = 5
n = 2	$\frac{3}{2\lambda}$				
n = 3	$\frac{11}{6\lambda}$	$\frac{5}{6\lambda}$			
n = 4	$\frac{25}{12\lambda}$	$\frac{13}{12\lambda}$	$\frac{7}{12\lambda}$		
n = 5	$\frac{137}{60\lambda}$	$\frac{77}{60\lambda}$	$\frac{47}{60\lambda}$	$\frac{9}{20\lambda}$	
n = 6	$\frac{147}{60\lambda}$	$\frac{29}{20\lambda}$	$\frac{57}{60\lambda}$	$\frac{37}{60\lambda}$	$\frac{11}{30\lambda}$

8. *Расчет надежности сложных последовательно-параллельных невосстанавливаемых систем*

Реальные высоконадежные системы обычно представляют собой совокупность произвольно соединенных резервированных схем. Если как сами схемы, так и их соединения между собой есть рассмотренные выше конфигурации (дублированные, троированные, “m из n”), то такие системы называют сложными последовательно-паралельными системами. Для расчета показателей безотказности таких систем применяется процедура последовательного расчета звеньев по приведенным выше формулам и замене резервированного звена одним элементом с известной вероятностью безотказной работы. Эта процедура повторяется до тех пор, пока система не будет сведена к известной последовательно-параллельной конфигурации. Поясним применение процедуры на примере расчета сложной системы, показанной на рис.2.5. На первом этапе расчета выделим звено последовательного соединения (A) и два дублированных звена (B и C). Для них по известным формулам (2.1,2.9) рассчитаем вероятности безотказной работы (P_A,P_B,P_C) и заменим эти звенья на эквивалентные элементы A, B, C. . На втором этапе последовательное соединение элементов 4 и B и 7 и C заменим на эквивалентные элементы D и E с соответствующими вероятностями безотказной работы P_D и P_E . Для полученной простой последовательно-параллельной схемы на третьем этапе записываем выражение для системной вероятности безотказной работы.

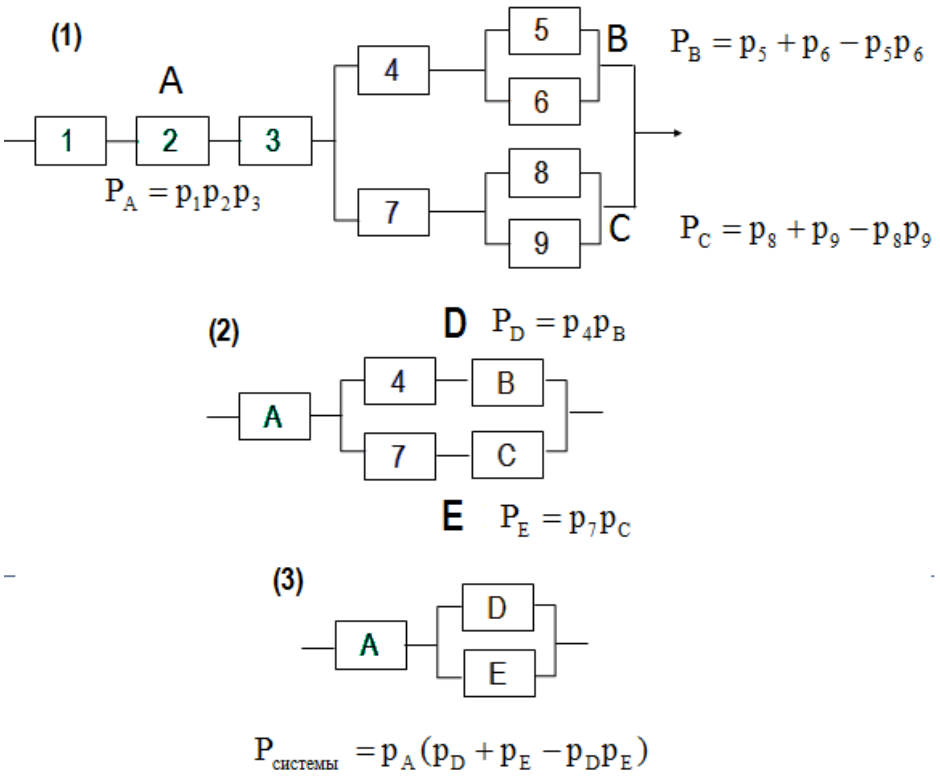


Рис2.5. Этапы расчета сложной последовательно-параллельной системы

2.2. Расчет надежности невосстанавливаемых сложных резервированных структур

1. *Расчет надежности мостиковых схем*

Рассмотрим схему передачи сигнала между источником А и приемником В в сети мобильной телефонной связи с ретрансляторами. Функциональная схема сети представлена на рис.2.6.

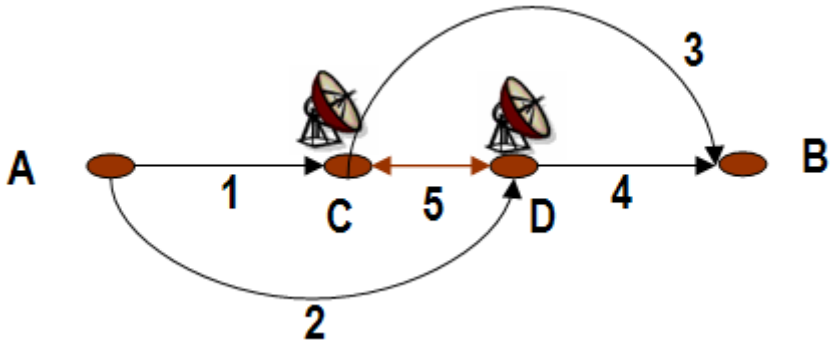


Рис.2.6. Функциональная схема МТС с ретрансляторами.

При отсутствии связи между ретрансляторами сигнал может быть передан по маршрутам: 1,3; 2,4. Введение двухсторонней связи (5) между ретрансляторами C и D позволило передать информацию между узлами A и B по следующим маршрутам: 1,3; 2,4; 1,5,4; 2,5,3.

На рис. 2.7 приведен пример еще одной сложной схемы - подсистемы формирования и подачи пара на турбины энергетического блока АЭС [30]. Подсистема состоит из установки поддержания вакуума в секциях главного конденсатора (1), секции главного конденсатора левого и правого каналов (2, 3), конденсатных насосов левого и правого каналов (5, 6), перемычки между каналами (4), питательных насосов левого и правого каналов (7, 8), блоков питательных клапанов левого и правого каналов (9, 10), парогенераторов левого и правого каналов (11, 12, 13, 14), турбогенератора (15).

Наличие перемычки (4) позволяет обеспечить работу конденсатного насоса одного канала на питательный насос другого. Для обеспечения нормального функционирования турбогенератора достаточным является нахождение в работе любых двух (из четырех) парогенераторов.

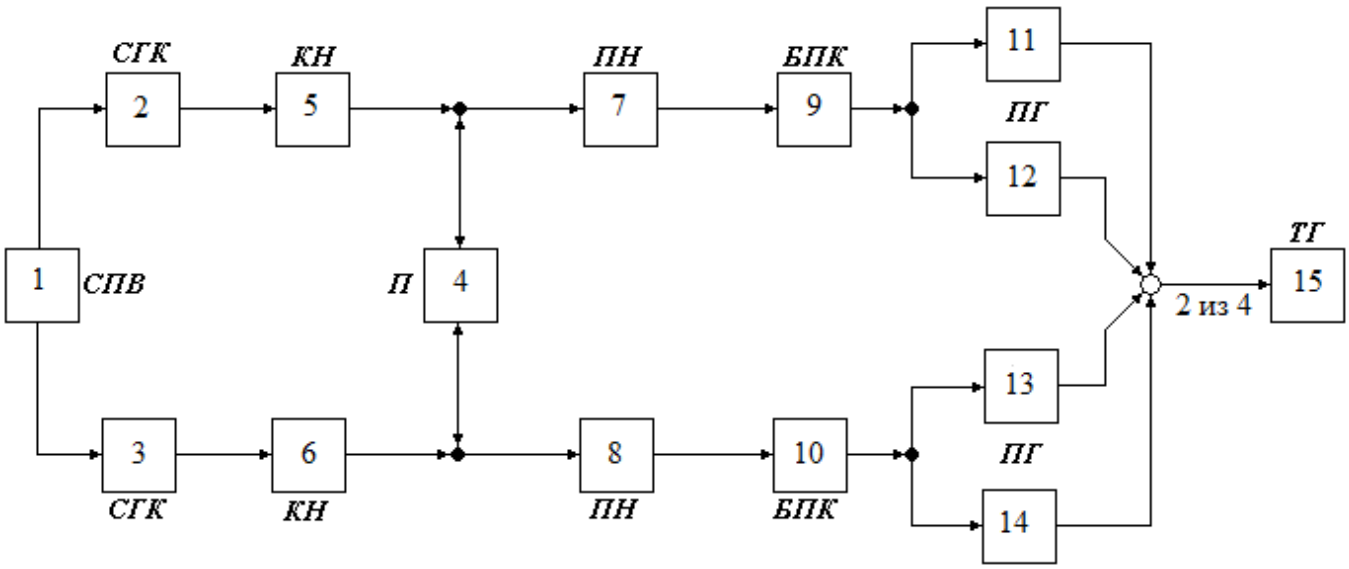


Рис.2.7. Функциональная схема фрагмента ядерной энергетической установки.

Рассмотренные схемы не могут быть представлены последовательно-параллельным соединением в смысле надежности. Характерной особенностью этих схем является наличие перемычки между каналами, что позволяет при отказе последовательного фрагмента одного канала работать, используя аппаратуру другого канала.

Схемы подобного рода получили название *мостиковых схем* или просто “мостика”.

Блок-схемы надежности ретрансляционной сети и фрагмента ядерной энергетической установки представлены на рис.2.8 и 2.9 соответственно.

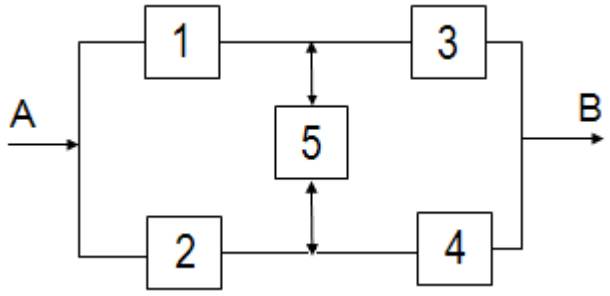


Рис.2.8 Блок-схема надежности МТС с ретрансляторами.

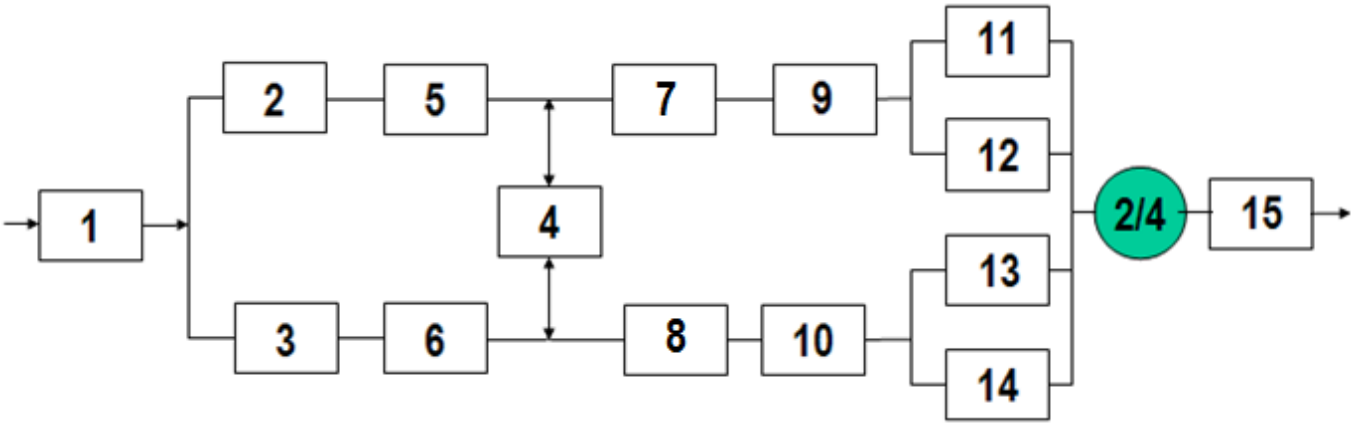
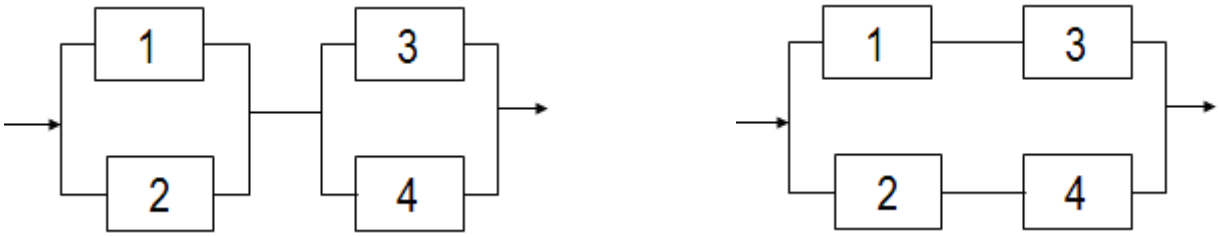


Рис.2.9. Блок-схема надежности фрагмента ядерной энергетической установки

При расчете мостиковых структур используется метод разложения относительно особого элемента, основанный на формуле полной вероятности (см. приложение 1). Сформируем полную группа событий относительно перемычки “мостика” (элемент 5). Событие B_1 - перемычка не отказала; событие B_2 - перемычка отказала. Для определения вероятности события безотказной работы “мостика” (А) при условии B_1 и B_2 рассматриваются его преобразованные схемы. Если реализовалось условие B_1, то мостиковая схема преобразуется в последовательное соединение двух дублированных структур, как это показано на рис.2.10.а. Если реализовалось условие B_2, то мостиковая схема преобразуется в дублированную структуру, верхний канал которой состоит из последовательного соединения элементов 1 и 3, а нижний – 2 и 4 (см. рис.2.10.б). Тогда выражение для вероятности безотказной работы мостиковой схемы имеет вид

$$P(A) = P(B_1)P(A/B_1) + P(B_2)P(A/B_2) = p_5[(1 - q_1q_2)(1 - q_3q_4)] + (1-p_5)[1 – (1-p_1p_3)(1-p_2p_4)] \quad (2.26)$$



а). Элемент 5 (перемычка) работоспособен

б). Элемент 5 (перемычка) отказал

Рис.2.10. Преобразование схемы “мостика”.

Идея метода разложения может быть применена не только для одного, но и для группы особых элементов. В этом случае рассматриваются все комбинации состояний работоспособности и отказа элементов группы. Если для всех комбинаций анализируемая схема сводится к последовательно-параллельному соединению, то расчет надежности производится по известным формулам, основанным на теоремах о вероятности суммы и произведения случайных событий. Если при каких-либо комбинациях схема не сводится к последовательно-параллельному соединению, то снова выбирается особый элемент или группа и проводится операция разложения. Процесс выбора и разложения относительно особого элемента повторяется вплоть до сведения схемы к последовательно-параллельному соединению.

Рассмотрим резервированную двухканальную систему с двумя однонаправленными перемычками между верхним и нижним каналом. Блок-схема надежности системы, набранная в модуле RBD Windchill Quality Solutions, показана на рис. 2.11.

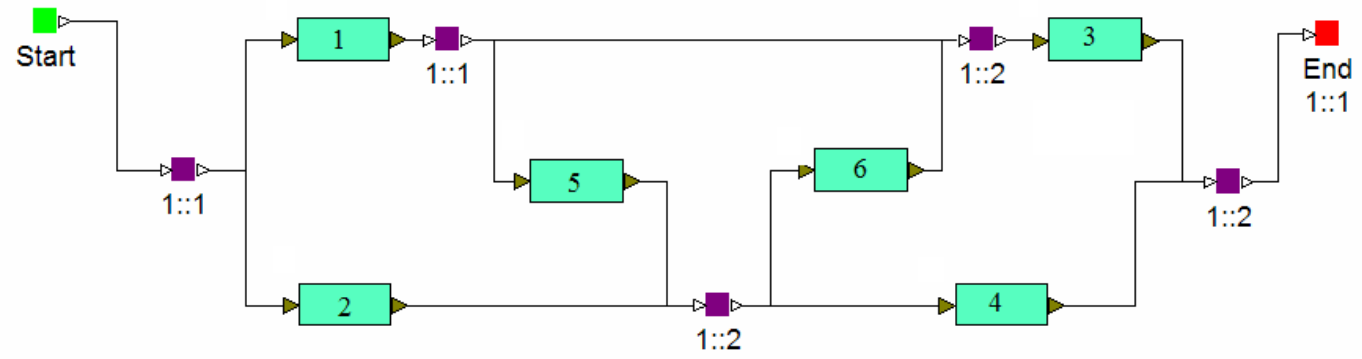


Рис.2.11. Блок-схема надежности двухканальной системы с однонаправленными пермычками.

Перемычка 1 формируется из элемента 5 и обеспечивает резервирование элемента 3 элементом 4. Перемычка 2 формируется из элемента 6 и обеспечивает резервирование элемента 4

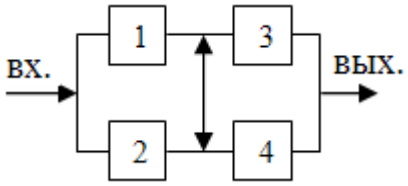
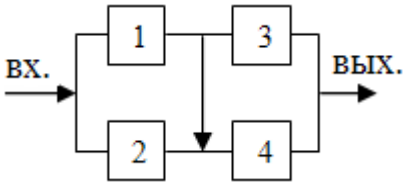
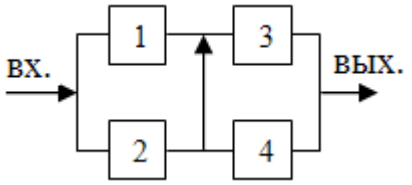
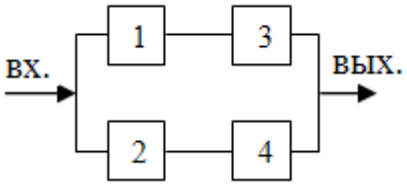
элементом 3. Все элементы системы равнонадежны (p-вероятность безотказной работы элемента, q – вероятность отказа).

В качестве группы особых элементов выберем две перемычки – элементы 5 и 6. Полная группа событий относительно этих элементов будет $\{B_1,B_2,B_3,B_4\}$:

$$B_1 = A_5 \cdot A_6; \quad B_2 = A_5 \cdot \overline{A}_6; \quad B_3 = \overline{A}_5 \cdot A_6; \quad B_4 = \overline{A}_5 \cdot \overline{A}_6,$$

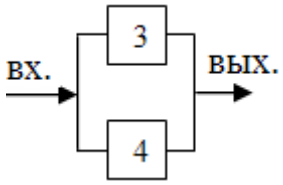
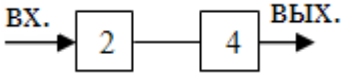
где A_i – событие работоспособности i – го элемента, $\overline{A}_i$ – событие отказа i – го элемента.

Результат первой итерации разложения приведен ниже

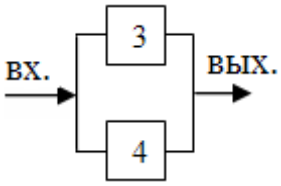
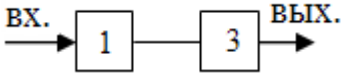
№ схемы	Событие	Полученная схема	Вероятность безотказной работы схемы
Схема 1	Событие B_1 $P(B_1) = p^2$		$P_1=(1-q^2)^2$
Схема 2	Событие B_2 $P(B_2) = pq$		Необходимо дальнейшее разложение
Схема 3	Событие B_3 $P(B_3) = qp$		Необходимо дальнейшее разложение
Схема 4	Событие B_4 $P(B_4) = q^2$		$P_4=1-(1-p^2)^2$

Схемы 2 и 3 не являются последовательно-параллельным соединением, поэтому необходимо проведение еще одной итерации разложения.

Схему 2 разложим по элементу 1. Событие B_{21} – элемент 1 работает, B_{22} – элемент 1 отказал.

№ схемы	Событие	Полученная схема	Вероятность безотказной работы схемы
Схема 2.1	Событие B_{21} $P(B_{21}) = p$		$P_{21}=(1-q^2)$
Схема 2.2	Событие B_{22} $P(B_{22}) = q$		$P_{22}=p^2$

Схему 3 разложим по элементу 2. Событие B_{31} – элемент 2 работает, B_{32} – элемент 2 отказал.

№ схемы	Событие	Полученная схема	Вероятность безотказной работы схемы
Схема 3.1	Событие B_{31} $P(B_{31}) = p$		$P_{31}=(1-q^2)$
Схема 3.2	Событие B_{32} $P(B_{32}) = q$		$P_{32}=p^2$

И окончательно, вероятность безотказной работы двухканальной схемы с двумя однонаправленными перемычками будет:

$$P=P(B_1)P_1+P(B_{21})P_{21}+P(B_{22})P_{22}+ P(B_{31})P_{31}+P(B_{32})P_{32}+ P(B_4)P_4\,. \qquad (2.27)$$

2. *Расчет надежности схем с повторяющимися элементами*

Иногда при анализе надежности приходится учитывать элемент, отказ которого приводит к отказу сразу нескольких частей анализируемой системы. Классическим примером такой ситуации являются отказы источников питания, одновременно приводящие к неработоспособности значительных частей системы в целом. В блок-схемах надежности такой элемент учитывается с помощью “повторяющегося блока” (“повторяющегося элемента”), который может присутствовать в разных ветвях блок-схемы, физически являясь одним элементом.

ассмотрим схему раздельного питания нижнего и верхнего каналов двух дублированных структур (рис.2.12). Если мы сформируем группу особых элементов из источников питания $П_1$ и $П_2$, то схема сведется к последовательно-параллельным соединениям, показанным на рис.2.13 и

соответствующим работоспособности $П_1$ и $П_2$ (2.13.а) работоспособности $П_1$ и отказу $П_2$ (2.13.б), работоспособности $П_2$ и отказу $П_1$ (2.13.в).

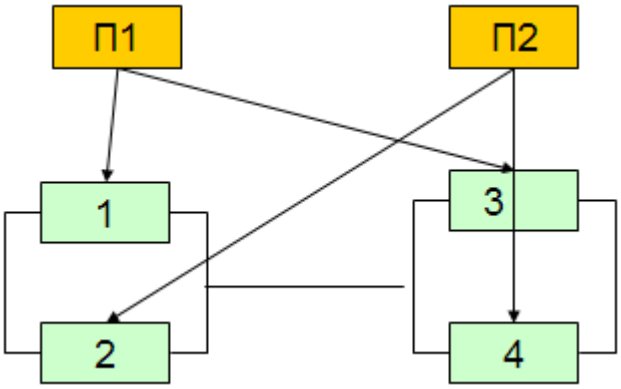
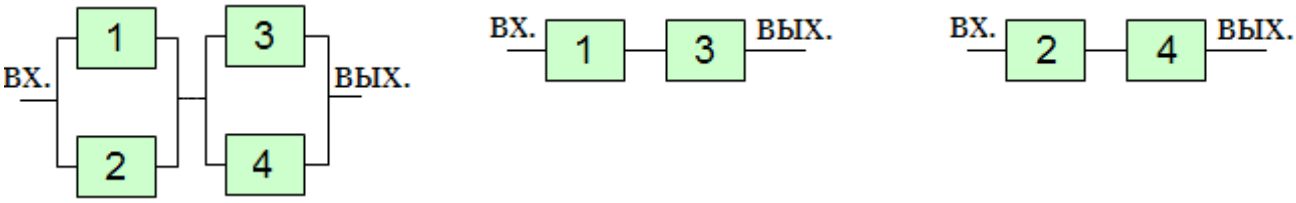


Рис.2.12. Схема раздельного питания нижнего и верхнего каналов дублированных структур



а) Источники питания $П_1$ и $П_2$ работоспособны.

б). Источник питания $П_1$ работоспособен, $П_2$- отказал.

в). Источник питания $П_2$ работоспособен, $П_1$ отказал.

Рис. 2.13. Преобразованная схема раздельного питания.

Вероятность безотказной работы схемы раздельного питания будет

$$P = P_{п1}P_{п2}(1-q_1q_2)(1-q_3q_4) + P_{п1}Q_{п2}p_1p_3 + P_{п2}Q_{п1}p_2p_4, \qquad (2.28)$$

На рис.2.14 приведена зависимость от времени вероятности безотказной работы схемы, рассчитанная с учетом и без учета повторяющихся элементов (источников питания). График показывает, что приближенный расчет без учета повторяющихся элементов занижает вероятность безотказной работы схемы по сравнению с точным значением, рассчитанным по (2.28).

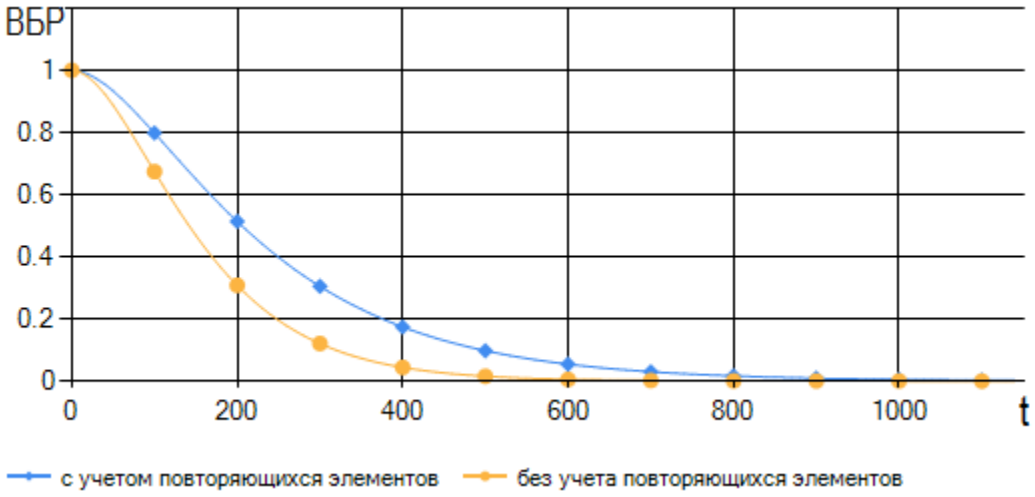


Рис.2.14. График зависимости от времени вероятности безотказной работы схемы раздельного питания

2.3. Сравнение основных схем нагруженного резервирования

Проведем сравнение основных схем нагруженного резервирования по показателю вероятности безотказной работы (ВБР). Рассмотрим следующие схемы: дублированную, троированную, мажоритарную “2 из 3” и мостиковую. Будем предполагать, что все схемы состоят из одинаковых равнонадежных невосстанавливаемых элементов. Базой для сравнения будет служить неизбыточная схема, состоящая из одного элемента.

На рис. 2.15 представлены зависимости ВБР резервированных схем от ВБР элемента (p). График показывает, что схемы “1 из n” (дублированная, троированная) оказываются лучшими на всем диапазоне изменения p. Мажоритарные и мостиковые схемы показывают улучшение вероятности безотказной работы только при $p>0.5$. При ненадежных элементах ($p<0.5$) эти схемы оказываются хуже неизбыточной стрктуры из одного элемента. В точке $p=0.5$ вероятность безотказной работы мажоритарной и мостиковой схем равняется 0.5, т.е. вероятности безотказной работы одного элемента. Этот факт можно использовать при тестировании специализированного программного обеспечения для расчетов надежности.

На рис.2.16 представлены зависимости ВБР резервированных структур от времени. Зависимости построены для случая равнонадежных экспоненциально распределенных элементов схем при $\lambda=0.002$ 1/ч. Поведение схем исследовано на интервале времени равном одному году (8760 часов). График демонстрирует преимущество дублированной и троированной схем на всем временном диапазоне. Мажоритарные и мостиковые схемы показывают улучшение показателя вероятности безотказной работы по сравнению с одним элементом лишь на интервалах времени t

< ln(2)/λ или t < 0.69/λ. При t > 0.69/λ ВБР мажоритарной и мостиковой схем оказываются хуже ВБР одного элемента. Отметим, что точка t = 0.69/λ лежит на временной оси левее точек средней наработки до отказа как одного элемента (1/λ), так и мажоритарной схемы (5/6λ).

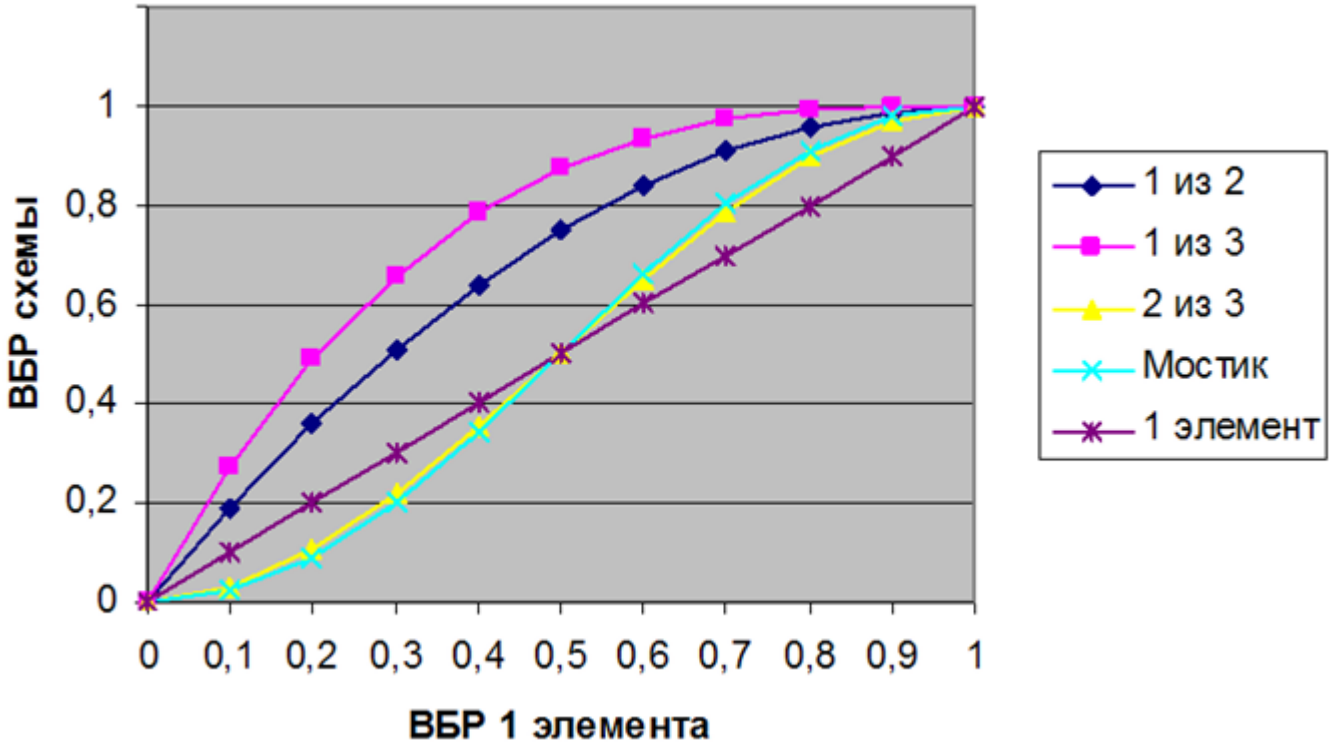


Рис.2.15 Зависимость ВБР резервированных схем от ВБР одного элемента

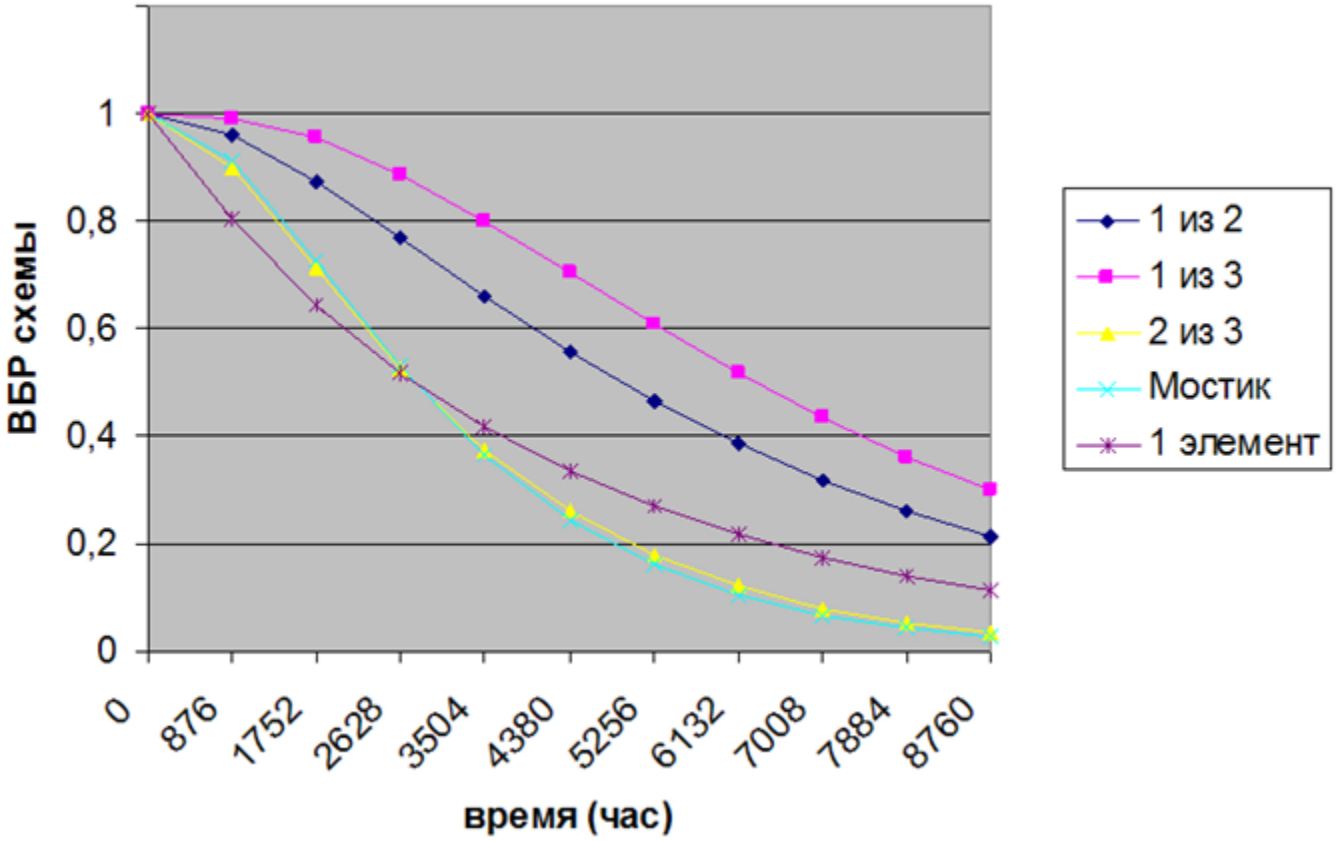


Рис.2.16. Зависимость ВБР резервированных схем от времени

В заключении отметим, что в параллельных резервированных структурах резервные элементы работают наравне с рабочим, поэтому эффективность любых схем нагруженного резервирования достаточно мала. Для экспоненциально распределенных элементов, исходя из формулы $T_{1\,\text{из}\,n} = \frac{1}{\lambda}(1+\frac{1}{2}+...+\frac{1}{n})$, показано, что повышение наработки схемы с нагруженным резервированием в 10 раз требует подключения ~ 10000 элементов, а повышение наработки в 100 раз требует подключения почти 10^{40} элементов. Для “стареющих” элементов такое положение только усугубляется. Поэтому в системах без восстановления часто применяют ненагруженный режим работы резервных элементов. Такой вид резервирования получил название ненагруженное (пассивное) резервирование или резервирование замещением. В западной литературе по отношению к ненагруженному резерву применяется термин standby**.**

Классическая схема ненагруженного резервирования состоит из одного рабочего элемента и нескольких резервных элементов, которые последовательно подключаются на место отказавшего рабочего. Резервные элементы находятся в ненагруженном состоянии (не расходуют свой ресурс и не могут отказывать). Схема работает до отказа последнего резервного элемента.

Очевидно, что случайная (ξ_Σ) и средняя (T_Σ) наработка до отказа такой схемы определяется суммированием соответствующих наработок всех ее элементов: $\xi_\Sigma = \sum_{i=1}^{n} \xi_i$; $T_\Sigma = M\left\{\sum_{i=1}^{n} \xi_i\right\} = \sum_{i=1}^{n} T_i$.

Чтобы увеличить в 10 раз среднюю наработку схемы, надо увеличить в 10 раз число резервных элементов. Для увеличения наработки в 100 раз, резерв надо увеличить в 100 раз и т.д. Таким образом, средняя наработка до отказа схем резервирования замещением растет линейно от числа резервных элементов.

Если элементы, находящиеся в резерве, могут отказывать, но с меньшей вероятностью (интенсивностью), чем при работе в основном канале, то такой вид резервирования называется облегченным. Вероятность отказа облегченного резервного элемента q находится в диапазоне $0<q<q_{рабочего}$. После отказа рабочего элемента и последующего включения резерва в основной канал $q = q_{рабочего}$.

Статические модели надежности, рассматриваемые в данной главе, не позволяют описывать надежностное поведение схем ненагруженного и облегченного резервирования. Это связано с тем, что в рамках этих моделей невозможно описать последовательность событий отказа рабочего элемента и последующего включение резерва в рабочую конфигурацию. Эта последовательность может быть смоделирована с помощью динамических моделей, например интегральных соотношений, описанных в [1, 7, 9], и марковских процессов, которые будут рассмотрены в пятой главе настоящей книги.

2.4. Сравнение схем раздельного и поканального нагруженного резервирования

Часто в процессе проектирования высоконадежных систем перед разработчиками встает вопрос о выборе “масштаба” резервирования. Альтернативы здесь таковы – раздельное (поэлементное) резервирование, общее (поканальное) резервирование:

1. *Раздельное (поэлементное) резервирование.*

Общий случай схемы раздельного поэлементного резервирования представлен на рис.2.17. Имеем n рабочих элементов, к каждому из которых добавляются m резервных элементов, работающих в нагруженном режиме. Полученные параллельные схемы работают по критерию “1 из m”. Вероятность безотказной работы такой схемы раздельного резервирования есть

$$P_1(t) = \prod_{i=1}^{n} (1 - (1 - p_i(t))^m) \qquad (2.29)$$

Случайная наработка до отказа $\xi_{1\Sigma}$ схемы раздельного резервирования определяется как

$$\xi_{1\Sigma} = \min_{1\le j\le n} \max_{1\le i\le m} \xi_{ij} \qquad (2.30)$$

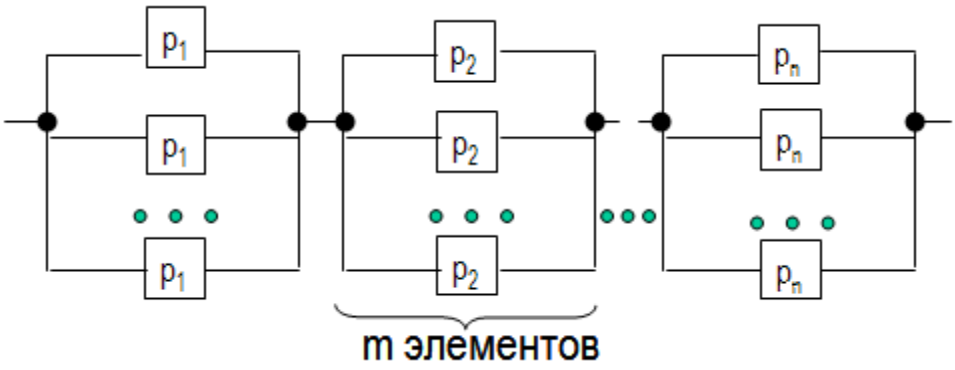


Рис.2.17. Схема раздельного, поэлементного резервирования

2. *Общее (поканальное) резервирование*

Общий случай схемы поканального резервирования представлен на рис.2.18. Имеем один рабочий канал, представляющий собой последовательное соединение n элементов. К рабочему каналу добавляются m резервных каналов, работающих в нагруженном режиме. Полученная параллельная схема работает по критерию “1 из m” каналов.

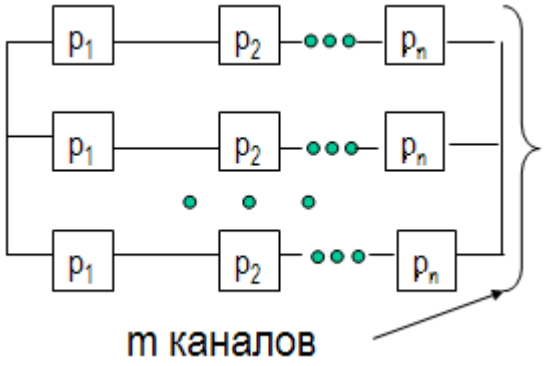


Рис.2.18. Схема поканального резервирования.

Вероятность безотказной работы схемы поканального резервирования есть

$$P_2(t) = 1 - [1 - \prod_{i=1}^{n} p_i(t)]^m \qquad (2.31)$$

Случайная наработка до отказа $\xi_{2\Sigma}$ схемы поканального резервирования определяется как

$$\xi_{2\Sigma} = \max_{1\le i\le m} \min_{1\le j\le n} \xi_{ij} \qquad (2.32)$$

В [10], используя известное соотношение математического анализа (min max ≥ max min), показано, что случайная наработка до отказа схем поэлементного резервирования превосходит случайную наработку при поканальном резервировании. А, следовательно, схемы поэлементного раздельного резервирования являются более предпочтительными по показателям вероятности безотказной работы и средней наработки до отказа:

$$P_1(t) = P\{\xi_{1\Sigma} \geq t\} \geq P_2(t) = P\{\xi_{2\Sigma} \geq t\}\ , \tag{2.33}$$

$$T_1(t) = M\{\xi_{1\Sigma}\} \geq T_2(t) = M\{\xi_{2\Sigma}\}\ . \tag{2.34}$$

Необходимо отметить, что при проектировании высоконадежных систем выбор окончательного решения по кратности и “масштабу” резервирования обычно проводится с учетом многих факторов (сложность технической реализации, весо-габаритные характеристики, стоимость и пр.). Поэтому поэлементное резервирование не всегда используется в реальных проектах.

2.5. Специальные случаи применения блок-схем надежности

Блок-схемы являются компактным, удобным для человеческого восприятия визуальным представлением различных моделей надежности резервированных структур. Именно поэтому все специализированное программное обеспечение анализа надежности коммерческого уровня (Windchill Quality Solutions, Isograph, A.L.D. …) обязательно содержит модуль блок-схем надежности (англо-язычный термин – Reliability Block Diagram – RBD). Наиболее развитые программы, например Windchill Quality Solutions, содержат расширения классических блок-схем надежности, называемые фазовыми диаграммами и блок-схемами потокового и электрического типа.

1. Фазовые диаграммы.

Фазовые диаграммы применяются для моделирования надежностного поведения систем, работающих в многофазном режиме. С точки зрения анализа надежности это означает, что система может иметь различные надежностные характеристики в каждой фазе. Может изменяться как техническая структура системы, так и параметры надежности ее элементов.

Для описания модели фазовых диаграмм необходимо задать

- общее количество фаз, их длительность и очередность
- конфигурацию системы в каждой фазе
- вид и параметры функций распределения случайных наработок до отказа элементов системы в каждой фазе

Конфигурация системы задается в виде блок-схем надежности.

Вектор распределения вероятностей состояний системы на конец i-ой фазы является вектором начальных состояний для i+1-ой фазы.

Поясним работу фазовых диаграмм на простом примере бортовой вычислительной системы.

Бортовая вычислительная система, состоящая из трех компьютеров ($БВ_i$), работает в двухфазном режиме. Первая фаза – управление взлетом летательного аппарата. Вторая фаза – управление полетом (рис.2.19). Длительность первой фазы T_1, второй T_2. При взлете, для повышения достоверности выходной информации три компьютера работают по мажоритарному принципу “2 из 3”. В полете конфигурация меняется на “1 из 3”. Вибрация при взлете приводит к повышению интенсивностей отказов электроники по сравнению со штатным режимом полета. Поэтому интенсивности отказов компьютеров на первой фазе выше, чем на второй $(\lambda_1 > \lambda_2)$.

Вероятность безотказной работы на момент окончания второй фазы, с учетом того, что она может начаться как из трех, так и из двухмашинной конфигурации, вычисляется как

$$P(0, T_1 + T_2) = e^{-3\lambda_1 T_1}(1-(1-e^{-\lambda_2 T_2})^3) + 3e^{-2\lambda_1 T_1}(1-e^{-\lambda_1 T_1})(1-(1-e^{-\lambda_2 T_2})^2). \quad (2.35)$$

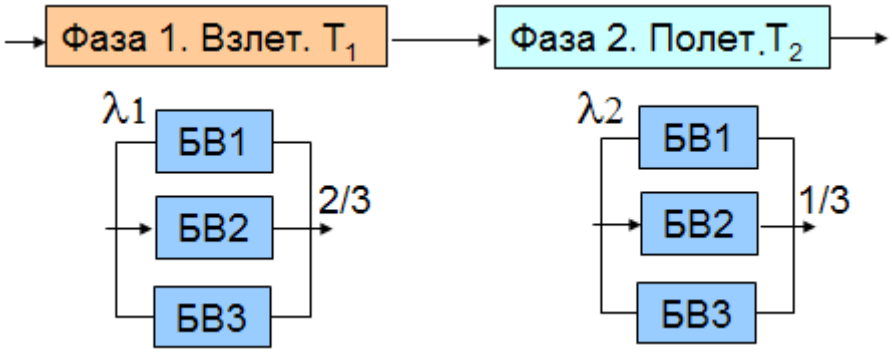


Рис.2.19 Фазовая диаграмма бортовой вычислительной системы

2. *Расширение блок-схем надежности для расчета производительности*

Для ответа на вопрос о том, насколько полно удовлетворяет система заданным на нее требованиям, оказывается недостаточным проведение расчетов только показателей надежности. Часто мерой соответствия системы своему назначению являются показатели технической эффективности, например, средняя производительность. Для расчета показателей производительности на блок-схемах надежности помимо обычных исходных данных (вид и параметры функций распределения случайных наработок до отказа блоков) необходимо задать дополнительные данные. К ним относятся средняя производительность каждого блока и требуемая производительность на выходе системы. В зависимости от правила, по которому потоки

продукции суммируются на входе и делятся на выходе узлов различают электрические и потоковые блок-схемы для расчета пропускной способности (производительности).

Правило электрической схемы. На входе узлов электрической схемы производительности от всех работоспособных выходов суммируются. На каждый выход из узла к блокам передается все то, что суммировалось на входе

Правило потоковой схемы. На входе узлов потоковой блок-схемы производительности от всех работоспособных выходов суммируются. На каждый выход из узла к блокам передается 1/n того, что суммировалось на входе (n-число выходов из узла).

Эффективность (мера соответствия своему назначению) входного узла всегда равна 100% как для электрической, так и потоковой блок-схемы.

Производительность любого узла всегда меньше или равна 100%

Выходная производительность i-го блока есть $C_{iвых}=\min\{C_{iвх}, C_i\}$, где $C_{iвх}$ – входная производительность i-го блока; C_i – производительность i-го блока.

Рассмотрим примеры расчета производительности.

Пример.1. Электрическая схема расчета производительности.

На рис. 2.20 приведена блок-схема резервированной структуры “1 из 4. Все элементы системы равнонадежны ($К_г(t)$ – коэффициент готовности элемента). Если элемент невосстанавливаемый, то коэффициент готовности элемента равен вероятности его безотказной работы. При распределении производительности по электрическому принципу входные 100% непосредственно передаются на каждый из четырех блоков, т.е. $C_{вх}$ = 100%. Блоки имеют 30% процентную производительность. На выходном узле суммируется производительность от каждого исправного блока. Тогда показатель средней производительности на интервале времени (0,t) рассчитывается следующим образом:

$$C(t) = К_г^4(t)\cdot 100\% + 4К_г^3(t)(1-К_г(t))\cdot 90\% + 6К_г^2(t)(1-К_г(t))^2\cdot 60\% + 4К_г(t)(1-К_г(t))^3\cdot 30\% \quad (2.36)$$

Пример 2. Потоковая схема расчета производительности.

Если для схемы (рис. 2.20) распределение производительности осуществляется по потоковому принципу, то входные 100% поровну разделяются между входами каждого из четырех блоков ($C_{вх}$ = 25%). Выходы блоков равны 25% ($C_{iвых}=\min\{25, 30\}$, i=1÷4). На выходном узле суммируется производительность от каждого исправного блока. Показатель средней производительности на интервале времени (0,t) есть

$$C(t) = К_г^4(t)\cdot 100\% + 4К_г^3(t)(1-К_г(t))\cdot 75\% + 6К_г^2(t)(1-К_г(t))^2\cdot 50\% \quad (2.37)$$

Член, соответствующий работоспособному состоянию схемы из одного работающего и трех отказавших блоков ($4К_г(t)(1-К_г(t))^3 \cdot 25\%$), не включен в (2.37), так как система не обеспечивает в этом состоянии требуемую производительность 30%.

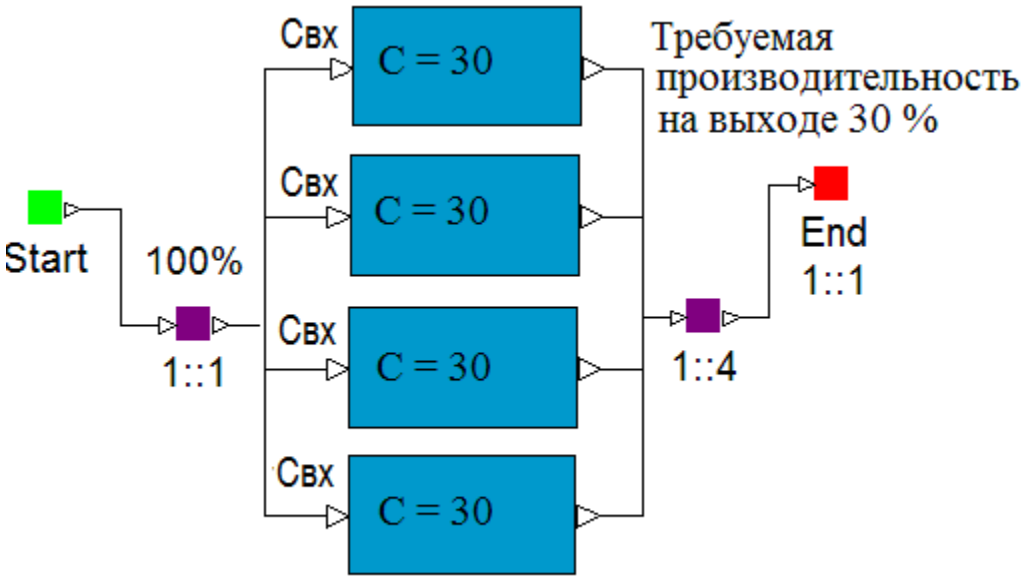


Рис.2.20. Блок-схема расчета производительности

Глава 3. Логико-вероятностные методы анализа надежности структурно-сложных систем

Под структурно-сложной системой с точки зрения анализа надежности будем понимать систему, состоящую из произвольного количества произвольно соединенных звеньев с нагруженным резервированием (параллельно-последовательных, мостиковых). В предыдущих лекциях были рассмотрены два метода исследования надежности структурно-сложных систем: метод декомпозиции и агрегировании последовательно-параллельных структур, метод разложения относительно особого элемента. При большом количестве элементов и межэлементных связей проведение расчетов надежности этими методами является крайне сложной задачей. Автоматизация расчетов позволяет решить проблему анализа надежности структурно-сложных систем. Для осуществления автоматизации необходимо иметь общее формальное описание “надежностного поведения” анализируемой системы. В качестве такого описания была выбрана алгебра логики (см. приложение 2). Метод анализа надежности сложных систем, при котором их структура описывается средствами математического аппарата бинарной алгебры логики, а количественная оценка надёжности производится с помощью теории вероятностей, получил название *логико-вероятностного метода*.

3.1. Этапы применения логико-вероятностного метода

Применение логико-вероятностных методов для определения значений вероятностных показателей надежности в момент времени t для системы, состоящей из n элементов, осуществляется в несколько этапов:

- конструирование логической функции работоспособности системы
- преобразование логической функции к форме перехода к замещению
- получение расчетной вероятностной формулы

1. Конструирование логической функции работоспособности (неработоспособности) системы

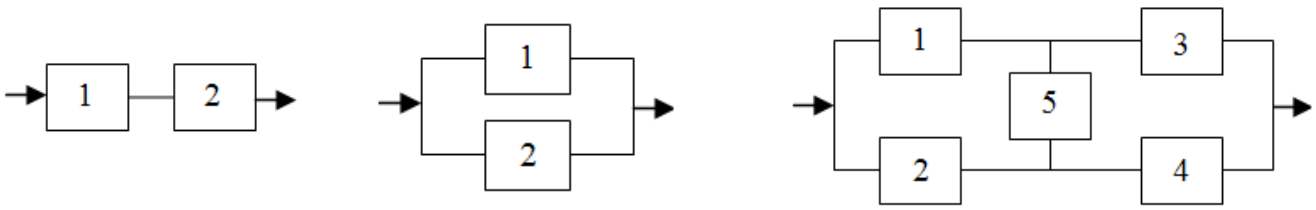
Делается предположение о том, что как сама система, так и составляющие ее элементы могут находится только в двух состояниях – работоспособности и отказа, причем отказы элементов предполагаются независимыми. Тогда, исходя из условий работоспособности (неработоспособности) системы, можно сконструировать логическую функцию ее работоспособности $S(\mathbf{x})$ (неработоспособности $\overline{S}(x)$)

$$S(\mathbf{x}) = \begin{cases} 1, \text{ когда система работоспособна} \\ 0, \text{ когда система отказала.} \end{cases} \quad (3.1)$$

Аргументом функции S является вектор-строка x логических переменных x_i, $i=\overline{1,n}$, таких что

$$x_i = \begin{cases} 1, \text{ когда элемент i работоспособен} \\ 0, \text{ когда элемент i отказал} \end{cases} \quad (3.2)$$

Например, если за исходное описание системы принять блок-схемы надежности, то для системы, состоящей из двух последовательно соединенных в смысле надежности элементов (отказ каждого является отказом системы в целом) (рис.3.1.а), $S(x) = x_1 x_2$, а $\overline{S}(x) = \overline{x}_1 \vee \overline{x}_2$. Функция работоспособности дублированной системы, в которой одиночные отказы элементов не приводят к ее отказу (рис.3.1.б), равна $S(x) = x_1 \vee x_2$, неработоспособности - $\overline{S}(x) = \overline{x}_1 \wedge \overline{x}_2$. Для мостиковой структуры (рис.3.1.в) $S(x) = x_1x_3 \vee x_2x_4 \vee x_1x_4x_5 \vee x_2x_3x_5$, $\overline{S}(x) = \overline{x}_1\overline{x}_2 \vee \overline{x}_3\overline{x}_4 \vee \overline{x}_1\overline{x}_4\overline{x}_5 \vee \overline{x}_2\overline{x}_3\overline{x}_5$. Эти функции построены достаточно формально – они отражают наличие хотя бы одной связи (пути) между входом и выходом надежностной схемы системы. Путь работоспособен, если работоспособны все входящие в него элементы, следовательно, для каждого пути формируется элементарная конъюнкция соответствующих переменных. Тогда функция работоспособности есть дизъюнкция всех элементарных конъюнкций, соответствующих возможным путям от входа к выходу. Для систем небольшой размерности запись подобных логических выражений не представляет труда, для сложных систем, состоящих из большого числа компонентов, требуются специальные алгоритмы прохода схемы и формирования путей.



а). б). в).

Рис. 3.1. Блок-схемы надежности.

2. *Преобразование логической функции к форме перехода к замещению*

Полученная на первом этапе форма логической функции S(X) называется *исходной*. Работая только с исходной функцией работоспособности (неработоспособности), мы не сможем достигнуть конечной цели – получить из S(x) вероятностное аналитическое выражение (P(S(x)=1) для расчета показателей надежности. Например, если заменить соответствующими вероятностями логические

переменные в выражении функции работоспособности для параллельных систем “1 из n”, то, очевидно, можно получить значение большее единицы. Поэтому исходную форму необходимо преобразовать в одну из специальных форм, называемых *формами перехода к замещению* (ФПЗ). Если S(x) представлена в ФПЗ, то при замещении логических переменных вероятностями, а логических операций арифметическими, мы получим точное значение вычисляемого показателя надежности.

Формами перехода к замещению являются совершенная дизъюнктивная нормальная форма (СДНФ), бесповторная форма в базисе конъюнкция-отрицание, дизъюнкция ортогональных форм в базисе конъюнкция-отрицание (ОФПЗ) [9]. Достаточно подробное описание формальных методов получения ФПЗ дано в [59, 60]. Примеры ФПЗ для резервированной структуры “1 из 3” есть в приложении 2. Алгоритмы получения СДНФ хорошо формализуемы, а, следовательно, достаточно легко переводятся в программные коды, однако форма представления является громоздкой. Бесповторная форма в базисе конъюнкция-отрицание является более компактным представлением логической функции, но алгоритмы ее получения, основанные на последовательном применении операций поглощения, склеивания и правила де-Моргана (см. приложение 2), ориентированы на использование человеком, а не на машинную реализацию.

Наиболее удобными для автоматизации являются различные способы представления исходной логической функции S(X) в виде дизъюнкции ортогональных конъюнкций Y_i: $S(x) = Y_1 \vee Y_2 \vee ... \vee Y_m$, $Y_i \wedge Y_j = 0$ для $i \neq j$. Условия ортогональности конъюнкций и независимости логических переменных в каждой конъюнкции позволяют применять к этой форме теорему суммы несовместных событий, что и обеспечивает корректность прямой замены логических переменных соответствующими вероятностями.

Для преобразования логической функции к ОФПЗ разработан алгоритм “разрезания”, описанный в [59,60] и основанный на теореме разложения логической функции на единичную и нулевую составляющие по аргументу x_i:

$$S(x_1, x_2, ...x_i, ...x_n) = x_i S(x_1, x_2, ...1, ...x_n) \vee \bar{x}_i S(x_1, x_2, ...0, ...x_n), \qquad (3.3)$$

Обычно для получения ОФПЗ требуется выполнить последовательность “разрезаний” по нескольким логическим аргументам. Причем, выбор этих аргументов достаточно произволен и рекомендацией здесь является выбор аргумента по числу наибольших вхождений в функцию.

В [9] приведен пример использования алгоритма разрезания на примере получения ОФПЗ для логической функции работоспособности мостиковой схемы (рис 3.1.в):

$$S(x) = x_1(x_3 \vee x_4 x_5) \vee x_2(x_4 \vee x_3 x_5) \qquad (3.4)$$

Разрезание по x_5 дает

$$S(x) = x_5(x_1(x_3 \vee x_4) \vee x_2(x_3 \vee x_4)) \vee \bar{x}_5(x_1x_3 \vee x_2x_4) \quad (3.5)$$

Применяя правило де-Моргана к каждой из ортогональных конъюнкций, получаем ОФПЗ в виде

$$S(x) = x_5(\overline{\bar{x}_1\bar{x}_2\bar{x}_3\bar{x}_4}) \vee \bar{x}_5(\overline{\overline{x_1x_3}\ \ \overline{x_2x_4}}) \quad (3.6)$$

Основным недостатком изложенного алгоритма является то, что он ориентирован на человека, который выбирает элементы разложения, видит оставшиеся логические конструкции и принимает решение о продолжении “разрезания” или применении правила де Моргана. Такую последовательность действий чрезвычайно трудно запрограммировать. Поэтому в современных развитых программных системах, например в Windchill Quality Solutions, применяют принципиально иной подход, а именно диаграммы двоичных решений (Binary Decision Diagram –BDD), которые описаны в разделе 4.6.

3. *Получение расчетной вероятностной формулы*

После приведения исходной логической функции работоспособности (неработоспособности) к любой из рассмотренных ФПЗ, получение расчетной формулы для вероятности истинности в момент времени t логической функции системы не представляет труда. Для этого надо логическую переменную x_i заменить соответствующей вероятностью $p_i = P(x_i = 1)$, $\bar{x}_i$ - вероятностью $q_i = P(x_i = 0)$, логическую операцию дизъюнкции $\vee$ – арифметической операцией сложения, конъюнкцию $\wedge$ – умножением, операцию логического отрицания $\bar{y}$ - вычитанием из единицы: 1- P(y=1). Вычисляемая таким образом вероятностная характеристика является коэффициентом готовности ($К_г$) (коэффициентом простоя=1-$К_г$) для систем с восстановлением элементов. Для систем без восстановления элементов вероятность истинности в момент времени t будет являться вероятностью безотказной работы (отказа) на интервале (0,t).

Так, исходя из ОФПЗ мостиковой схемы (3.6), получаем

$$P(S(x) = 1) = p_5(1 - q_1q_2)(1 - q_3q_4) + q_5(1 - (1 - p_1p_3)(1 - p_2p_4)) \quad (3.7)$$

Полученная формула идентична выражению (2.26), которое получено методом разложения относительно особого элемента.

3.2. Расчет показателей надежности на основе теоремы сложения вероятностей совместных событий

При автоматизации рассмотренного в предыдущих разделах подхода к определению показателей надежности, основанного на преобразовании логических функций работоспособности в форму перехода к замещению, возникают определенные трудности, связанные с разработкой алгоритмов получения бесповторных ортогональных форм. В связи с этим в рамках логико-вероятностных методов создаются другие подходы, порождающие более регулярные алгоритмы оценки показателей надежности. Одним из них является подход, основанный на теореме сложения вероятностей совместных событий реализации минимальных путей (сечений). Для системы произвольной структуры *минимальным путем* (МП) называется минимальное множество работоспособных элементов, которое обеспечивает работоспособное состояние системы:

группа элементов Π_j есть минимальный путь

а) если элементы множества Π_j работоспособны, то система работоспособна независимо от состояния других элементов

б) никакое подмножество Π_j не удовлетворяет первому условию

Минимальным сечением (МС) в системе произвольной структуры называется минимальное множество элементов, отказ которых приводит к отказу системы:

группа элементов C_i называется минимальным сечением

а) если откажут все элементы сечения, то система откажет независимо от состояния других элементов

б) никакое подмножество C_i не удовлетворяет первому условию.

Логическую функцию работоспособности $S(x)$ (неработоспособности $\overline{S}(x)$) системы можно представить в ДНФ, в которой элементарная конъюнкция $\Pi_j(C_j)$ составляется из элементов, входящих в j-й минимальный путь (i-е сечение):

$$S(x) = \bigvee_{j=1}^{r} \Pi_j \tag{3.8}$$

$$\overline{S}(x) = \bigvee_{i=1}^{l} C_j \tag{3.9}$$

События реализации минимальных путей (сечений) системы в общем случае являются совместными событиями. Поэтому, применяя теорему сложения вероятностей совместных событий, можно записать:

$$R = P\{\bigvee_{j=1}^{r} \Pi_j = 1\} = \sum_{j=1}^{r} P\{\Pi_j\} - \sum_{i=1}^{r-1}\sum_{j>i} P\{\Pi_i \wedge \Pi_j\} + \sum_{i=1}^{r-2}\sum_{j>i}\sum_{k>j} P\{\Pi_i \wedge \Pi_j \wedge \Pi_k\} - \ldots$$
$$+ (-1)^{r-1} P\{\Pi_1 \wedge \Pi_2 \ldots \wedge \Pi_r\} = 1 - \sum_{i=1}^{l} P\{C_i\} + \sum_{i=1}^{l-1}\sum_{j>i} P\{C_i \wedge C_j\} - \ldots + (-1)^{l-1} P\{C_1 \wedge C_2 \ldots \wedge C_l\} \quad (3.10)$$

Здесь $\{\Pi_j\}$- событие, состоящее в безотказной работе всех элементов пути Π_j; $\{C_i\}$- событие, состоящее в отказе всех элементов сечения C_i; r – число минимальных путей, l – число минимальных сечений; R-вычисляемый показатель надежности (коэффициент готовности для восстанавливаемых систем, вероятность безотказной работы для систем без восстановления).

Например, для мостиковой схемы без восстановления по формуле (3.10) получаем следующее выражение для вероятности безотказной работы

$$\begin{aligned} R = P\{S(x) = 1\} &= P\{x_1x_3\} + P\{x_2x_4\} + P\{x_1x_4x_5\} + P\{x_2x_3x_5\} \\ &- P\{x_1x_3x_2x_4\} - P\{x_1x_3x_4x_5\} - P\{x_1x_2x_3x_5\} - P\{x_1x_2x_4x_5\} - P\{x_2x_3x_4x_5\} - P\{x_1x_2x_3x_4x_5\} \\ &+ P\{x_1x_2x_3x_4x_5\} + P\{x_1x_2x_3x_4x_5\} + P\{x_1x_2x_3x_4x_5\} + P\{x_1x_2x_3x_4x_5\} \\ &- P\{x_1x_2x_3x_4x_5\} \end{aligned}, \quad (3.11)$$

где $P\{x_i,x_j,\ldots x_k\}=p_ip_j\ldots p_k$; p_i – вероятность безотказной работы i-го элемента.

Если S(x) содержит достаточно большое количество конъюнкций (путей, сечений), то время счета по (3.10) резко возрастает. Здесь следует отметить, что выражение для R представляет собой знакопеременный ряд. Если его последовательно наращивать, каждый раз останавливаясь перед сменой знака, то будем получать оценки. Если остановились перед знаком минус, то получаем верхнюю оценку соответствующей вероятности (работоспособности – по путям, отказа – по сечениям). Если остановились перед знаком плюс, то получаем нижнюю оценку. Причем, получаемые оценки стремятся к точному значению при увеличении членов (т.е. разность между верхней и нижней оценкам уменьшается). *Это свойство может быть использовано при программной реализации метода.* Особенно актуально проведение оценок, а не точных вычислений, для сложных систем с большим количеством минимальных путей (сечений) и достаточно надежными элементами. Поэтому современное программное обеспечение для расчетов надежности (например, Windchill Quality Solutions) предоставляет возможность пользователю управлять процессом вычисления по формуле (3.10), ограничивая кратность пересечения конъюнкций.

3.3. Приближенная оценка надежности монотонных структур

Все изученные нами резервированные системы с нагруженным резервом (последовательно-параллельные, мостиковые) являются системами с *монотонной структурой*. Для них характерно следующее: отказ любого из элементов приводит к ухудшению надежности или отказу всей системы, а восстановление любого из элементов не может привести к ухудшению надежности системы. В [6] дано строгое определение понятия монотонности

$$\begin{cases} S(1,1,...1) = 1 \\ S(0,0,...0) = 0 \\ \text{если } x_i \geq y_i, \text{ то } S(x_1, x_2, ...x_n) \geq S(y_1, y_2, ...y_n) \end{cases} \quad (3.12)$$

Для таких систем можно получать приближенные оценки вероятности безотказной работы (отказа).

Для надежности систем с монотонной структурой, состоящих из независимых элементов, справедливы оценки по минимальным путям и сечениям (оценки Эзари-Прошана):

$$\prod_{k=1}^{l} P\{C_k(x) = 1\} \leq P\{S(x) = 1\} \leq 1 - \prod_{j=1}^{r} (1 - P\{\Pi_j(x) = 1\}) \quad (3.13)$$

где Π_j– логическая функция работоспособности j-го пути, C_k- логическая функция работоспособности k-го сечения, r (l) – общее количество путей (сечений).

Обоснование справедливости оценок по минимальным путям и минимальным сечениям дано в [6].

Вычислим верхнюю и нижнюю оценки Эзари-Прошана мостиковой схемы (рис.3.1.в).

1. Верхняя оценка вероятности безотказной работы мостиковой схемы по минимальным путям.

$$\begin{aligned} &\Pi_1 = x_1 \cdot x_3;\ P(\Pi_1 = 1) = p_1 p_3 = P_1 \\ &\Pi_2 = x_2 \cdot x_4;\ P(\Pi_2 = 1) = p_2 p_4 = P_2 \\ &\Pi_3 = x_1 \cdot x_4 \cdot x_5;\ P(\Pi_3 = 1) = p_1 p_4 p_5 = P_3 \\ &\Pi_4 = x_2 \cdot x_3 \cdot x_5;\ P(\Pi_4 = 1) = p_2 p_3 p_5 = P_4 \end{aligned} \quad . \quad (3.14)$$

$$P = 1 - \prod_{i=1}^{4} (1 - P_i) = 1 - (1 - p_1 p_3)(1 - p_2 p_4)(1 - p_1 p_4 p_5)(1 - p_2 p_3 p_5),$$

что соответствует параллельному соединению всех минимальных путей мостиковой схемы (рис.3.2.а).

2. Нижняя оценка вероятности безотказной работы мостиковой схемы по минимальным сечениям.

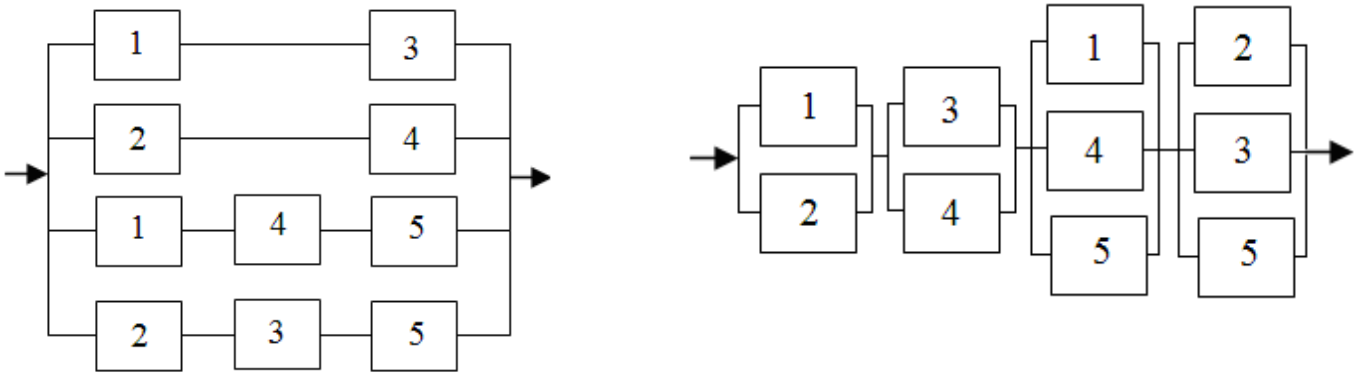
$$
\begin{aligned}
&C_1 = x_1 + x_2;\ P(C_1 = 1) = 1 - (1 - p_1)(1 - p_2) = P_1 \\
&C_2 = x_3 + x_4;\ P(C_2 = 1) = 1 - (1 - p_3)(1 - p_4) = P_2 \\
&C_3 = x_1 + x_4 + x_5;\ P(C_3 = 1) = 1 - (1 - p_1)(1 - p_4)(1 - p_5) = P_3 \\
&C_4 = x_2 + x_3 + x_5;\ P(C_4 = 1) = 1 - (1 - p_2)(1 - p_3)(1 - p_5) = P_4
\end{aligned}
\quad . \qquad (3.15)
$$

$$
P = \prod_{i=1}^{4} P_i
$$

что соответствует последовательному соединению всех минимальных сечений мостиковой схемы (рис.3.2.б).

В таблицу 3.1 сведены значения оценок Эзари-Прошана вероятности безотказной работы мостиковой схемы из равнонадежных элементов. Оценки вычислены при варьировании вероятности безотказной работы элементов в пределах от 0.01 до 0.99. Вычисления показывают, что нижняя оценка по сечениям, тем точнее, чем более надежны элементы схемы.

Очевидно, что если бы пути и сечения не содержали бы повторяющихся элементов, то оценка Эзари-Прошана давала бы точное значение вычисляемого показателя.



а). Параллельное соединение путей б). Последовательное соединение сечений

Рис.3.2. Представление мостиковой схемы через минимальные пути и сечения.

Таблица 3.1. Поведение оценок Эзари-Прошана для мостиковой схемы

ВБР элементов (p_i=p)	Оценка ВБР по сечениям (нижняя)	Точное значение ВБР	Оценка ВБР по путям (верхняя)
0,01	0,00000035	***0,0002***	***0,0002***
0,1	0,0026	0,0202	0,0219
0,5	0,4307	0,5	0,5697
0,9	0,9781	0,9798	0,99926
0,99	***0,9998***	***0,9998***	0,9999934

3.4.Об оценке показателей надежности восстанавливаемых систем логико-вероятностными методами

В общем случае показатели надежности (в частности, безотказности) систем с восстановлением отказавших элементов логико-вероятностными методами не вычисляются. Напомним, что логико-вероятностные методы позволяют вычислять лишь мгновенные показатели (показатели в момент времени t), а именно коэффициент готовности и параметр потока отказов. Для многоуровневых логико-вероятностных моделей функционирования вычисляемыми показателями являются вероятность застать систему в момент времени t в заданном логическим выражением подмножестве состояний и параметр потока переходов в это или дополнительное подмножество состояний. То есть, для систем с независимыми отказами и восстановлением элементов принципиально могут вычисляться лишь показатели - коэффициент готовности и параметр потока отказов. Для вычисления коэффициента готовности системы в полученное логическое выражение в виде формы замещения вместо переменных подставляются коэффициенты готовности, простоя. Вычислению параметра потока отказов в логико-вероятностных моделях будут посвящены отдельные разделы, так как этот вопрос до последнего времени был проработан слабо и авторами монографии в 2007-2011 г.г. были получены новые результаты. Остановимся отдельно на условии независимости отказов для восстанавливаемых систем, которое с теоретической точки зрения позволяет применять логико-вероятностное моделирование. Восстановление значительно расширяет возможные нарушения условий независимости отказов, которые теперь уже связаны не только с физикой процессов отказов в элементах, как в невосстанавливаемых системах, а и с различными особенностями восстановления. Такими особенностями являются, например, стратегии восстановления, ограничения на число бригад, ЗИП, характеристики (и сама возможность) отказов элементов в состояниях неработоспособности системы. В главе 5 (марковские модели надежности) приведен пример последовательной восстанавливаемой системы, отказ которой наступает после отказа любого одного элемента. Если при восстановлении отказавшего элемента и системы отказы других элементов невозможны (т.к. система не функционирует), то это означает несовместность отказов элементов (а значит зависимость!) и нельзя применять теорему произведения вероятностей независимых событий. Таким образом, произведение коэффициентов готовности всех элементов даст неверный результат. Но оценка через произведение даёт нижнее (худшее) значение

готовности и, более того, если произведение даст значение большее 0,9, то погрешностью можно пренебречь (по неготовности – единицы процентов, по готовности – менее 1 процента).

Итак, логико-вероятностные методы принципиально позволяют определять коэффициент готовности для систем с независимыми процессами отказов и восстановления элементов. Для элементов по заданным функциям распределения наработки до отказа и функциям распределения времени восстановления вычисляются коэффициент готовности и параметр потока отказов (нестационарные, стационарные), через которые определяются надежностные показатели для системы. При экспоненциальных распределениях наработки до отказа и времени восстановления элемента, значения коэффициента готовности и параметра потока отказов записываются в явном формульном виде. Если эти распределения неэкспоненциальные, то значения указанных показателей для элементов могут быть получены численными методами, в частности, статистическим моделированием.

Остановимся на многоуровневых моделях. Многоуровневые модели позволяют представить пространство состояний системы большим, чем два (работоспособность/неработоспособность системы), количеством классов состояний. Это даёт возможность отразить состояния со сниженными уровнями эффективности функционирования, состояния с различной критичностью отказов. Одним из основных показателей надежности является коэффициент сохранения эффективности, и именно многоуровневые модели позволяют его определять. Логико-вероятностное моделирование в этом случае требует применения немонотонных логических функций. А именно, необходимо определить класс состояний соответствующий сниженному уровню эффективности функционирования. Логическое выражение для этого класса должно содержать в каждой конъюнкции, как работоспособные элементы, так и отказавшие, что и является критерием немонотонности. Вычисление распределения вероятностей застать систему в момент времени t в каждом классе состояний является обычной задачей, не отличающейся от вычисления коэффициента готовности/простоя.

В многоуровневых моделях функционирования систем среднее (по уровням) значение интегральной эффективности E(0,t) на интервале (0,t) может быть представлено так:

$$E(0,t) = \sum_i \int_0^t Pr_i(\tau) h_i d\tau + \sum_{i,j} \int_0^t \omega_{i,j}(\tau) h_{i,j} d\tau, \qquad (3.16)$$

где $Pr_i(\tau)$ – вероятность застать систему в момент τ в i-м состоянии;

$\omega_{i,j}(\tau)$– параметр потока переходов из i-го состояния в j-е в момент τ;

h_i – доход (потери) в единицу времени от пребывания системы в состоянии i;

$h_{i,j}$ – единовременные доходы (потери) за переход.

Первый интеграл определяет среднее время пребывания системы на интервале (0,t) в каждом из состояний умноженное на доход в единицу времени пребывания в этих состояниях. А второй интеграл - среднее число переходов между выделенными состояниями, взвешенное доходами (потерями) от каждого перехода. Если, например, при некоторых отказах повреждается «соседнее» оборудование (связанное с отказавшим по технологической цепи или расположенное рядом) или теряется находящийся в технологической обработке объект (изделие, вещество, информация, …), то параметр потока отказов позволит оценить потери.

Известная традиционная оценка средней эффективности E(t) в момент времени t по выражению (3.17) в таком случае даст слишком оптимистический результат без учета единовременных потерь:

$$E(t) = \sum_i Pr_i(t) \cdot E_i(t), \qquad (3.17)$$

где $E_i(t)$ – эффективность в состоянии i (в частности, $E_i(t)$ может быть равно h_i и тогда (3.17) даст ожидаемый доход, например, производительность, в момент времени t).

Основной и, пожалуй, единственной трудностью применения логико-вероятностных методов является размерность анализируемой системы. Разработки методов и алгоритмов получения логического описания, преобразование этого описания в специальную форму, пригодную для расчета, начались более 50 лет назад и продолжаются в настоящее время. Все эти разработки в основном направлены на преодоление “проклятия размерности”. Причем если более ранние работы представляли собой в большей степени «человеческий» (т.е. ориентированный на “ручные” расчеты) метод, алгоритм, то в настоящее время можно говорить об ориентации методов и особенно алгоритмов на применение вычислительной техники. Примером такого машинно-ориентированного алгоритма является алгоритм получения ортогональной формы логического выражения, использующий способ описания и прохода деревьев отказа с помощью бинарных деревьев. Для “ручного” расчета он сложен и громоздок, но в машинной реализации достаточно эффективен. Этот алгоритм весьма своеобразно использует метод разложения по элементам системы. В разделе 4.6 приведен алгоритм и продемонстрировано его применение.

Эффективным способом решения проблем размерности в задачах анализа надежности является декомпозиция структуры системы или логического описания. При декомпозиции можно выделить:

1. Односвязную декомпозицию структуры, когда выделяемые подсистемы (звенья, модули и пр.) связываются друг с другом только через две свои вершины, причем одна вершина

является входом (ребра связей в нее только входят), а другая – выходом (ребра связей из нее только выходят), т.е. имеем последовательное соединение подсистем. Каждая из подсистем может представлять собой резервированную структуру с некоторой логической функцией в выходной вершине (или элементе). В данном способе нет сложностей с вычислением и агрегированием показателей надежности, безопасности, технической эффективности.

2. Многосвязную декомпозицию, когда выделяемые подсистемы могут иметь любое число входов и выходов. Сохраняются лишь следующие ограничения (ацикличность связей):
   a. Все входные вершины подсистемы L^k являются либо головными, либо связаны с другими (не входящими в L^k) элементами посредством входящих в L^k ребер;
   b. Все выходные вершины являются либо конечными, либо связаны с другими элементами посредством исходящих из L^k ребер.

   Сложностей в этом способе много, как в выделении таких подсистем, так и в агрегировании некоторых показателей (например, параметра потока отказов). Но эффективность его может оказаться очень высокой при решении проблем размерности, и при учете особенностей «надежностного поведения» (см. пример ниже).

3. Декомпозицию, связанную с разложением по полной группе событий относительно выделенных элементов, блоков, … .
4. Логическую декомпозицию. В этом способе, не предусматриваются какие-либо преобразования исходной структуры системы. На более простые части разбивается сама задача надежностного моделирования. Это достигается разделением общего логического критерия работоспособности, отказа на несколько частных и установлении их связи (лучше арифметической) с системной функцией. Одним из способов агрегирования показателей может быть применение теоремы суммирования вероятностей совместных событий, что позволит получать двухсторонние оценки показателей.

Способы декомпозиции, особенно приведенные в п.п. 1 и 3, известны [23, 26, 28] и широко применяются, но преимущественно для вычисления коэффициента готовности (простоя).

Рассмотрим пример многосвязной декомпозиции структурно сложной схемы, показанной на рис.3.3.

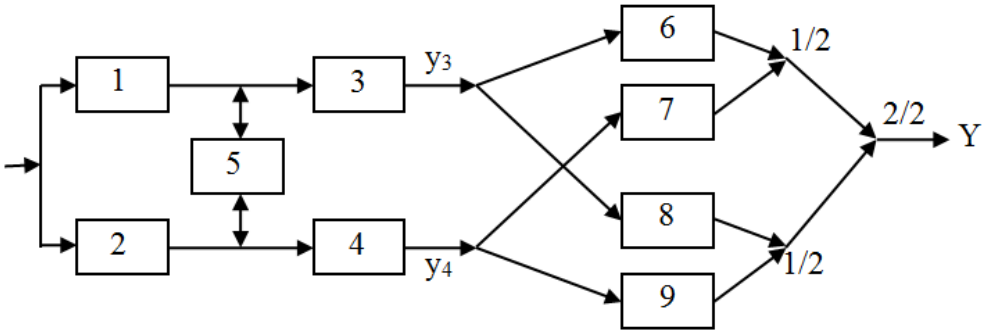


Рис.3.3. Структурно-сложная схема, допускающая многосвязную декомпозицию.

Проведем структурную многосвязную декомпозицию этой схемы. «Разрезаем» блок-схему на две части по выходам блоков 3 и 4 (y_3, y_4) и рассматриваем все комбинации с выходами y_3, y_4, обеспечивающими работоспособность всей структуры. А именно

$$Z_1 = y_3 \cdot y_4 = x_3 \cdot x_4 \cdot [x_5 \cdot (x_1 + x_2) + \bar{x}_5 \cdot x_1 \cdot x_2] = x_3 \cdot x_4 \cdot [x_5 \cdot (x_1 + \bar{x}_1 \cdot x_2) + \bar{x}_5 \cdot x_1 \cdot x_2]$$

$$Z_2 = \bar{y}_3 \cdot y_4 = x_4 \cdot [x_3 \cdot \bar{x}_1 \cdot x_2 \cdot \bar{x}_5 + \bar{x}_3 \cdot (x_2 + x_1 \cdot x_5)] = x_4 \cdot [x_3 \cdot \bar{x}_1 \cdot x_2 \cdot \bar{x}_5 + \bar{x}_3 \cdot (x_2 + \bar{x}_2 \cdot x_1 \cdot x_5)]$$

$$Z_3 = y_3 \cdot \bar{y}_4 = x_3 \cdot [x_4 \cdot x_1 \cdot \bar{x}_2 \cdot \bar{x}_5 + \bar{x}_4 \cdot (x_1 + x_2 \cdot x_5)] = x_3 \cdot [x_4 \cdot x_1 \cdot \bar{x}_2 \cdot \bar{x}_5 + \bar{x}_4 \cdot (x_1 + \bar{x}_1 \cdot x_2 \cdot x_5)]].$$

После декомпозиции структура в соответствии с теоремой полной вероятности принимает вид

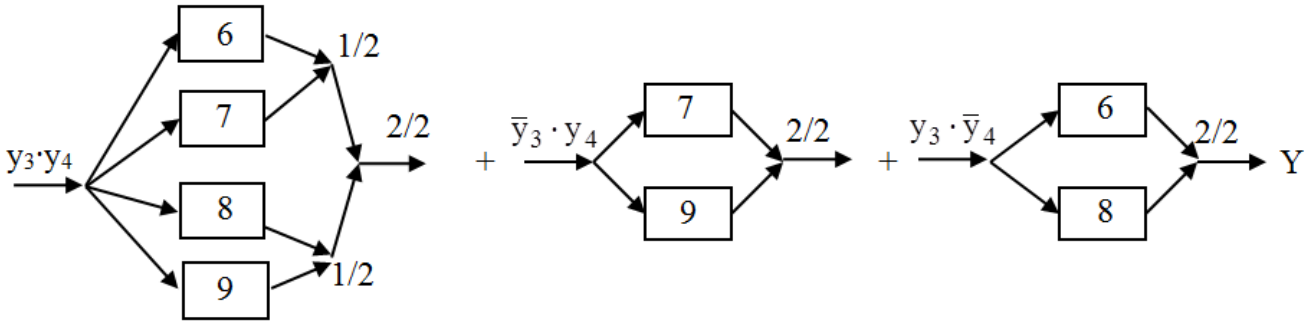


Рис.3.4. Декомпозиция структурно-сложной схемы.

И окончательно получаем:

$$Y = Z_1 \cdot [(x_6 + x_7) \cdot (x_8 + x_9)] + Z_2 \cdot x_7 \cdot x_9 + Z_3 \cdot x_6 \cdot x_8 =$$
$$Z_1 \cdot [(x_6 + \bar{x}_6 \cdot x_7) \cdot (x_8 + \bar{x}_8 \cdot x_9)] + Z_2 \cdot x_7 \cdot x_9 + Z_3 \cdot x_6 \cdot x_8 .$$

3.5. Вычисление параметра потока отказов в логико-вероятностных моделях.

Большинство работ по методам и алгоритмам оценки показателей надежности, безопасности систем в классе логико-вероятностного моделирования посвящены вычислениям вероятности выполнения (истинности) некоторой логической функции, определенной на булевских переменных (элементах системы), в частности, коэффициента готовности/простоя. Важным показателем, характеризующим переходы системы, например, из состояния работоспособности в состояние неработоспособности, является параметр потока отказов. Этот показатель необходимо вычислять при исследовании эффективности, безопасности, риска эксплуатации систем. Параметр потока отказов определяется как производная по времени от математического ожидания числа отказов. Поэтому среднее значение числа отказов (а в общем случае числа интересующих исследователя переходов) можно определить интегрированием на заданном интервале времени параметра потока отказов (параметра потока переходов в интересующее подмножество состояний). Параметр потока отказов и среднее число отказов являются основными показателями, если одной (основной) из составляющих потерь являются единовременные потери при переходе в некоторое подмножество отказов. Отметим также, что с использованием параметра потока отказов можно оценивать такой основной показатель надежности как вероятность безотказной работы на заданном интервале времени для восстанавливаемых систем, который непосредственно не может быть получен в логико-вероятностных моделях.

Известный метод вычисления параметра потока отказов, основывающийся на формуле вероятности объединения совместных событий (3.10), приводит к значительным затратам времени и даже к невозможности получения точного значения при больших размерностях задачи из-за переборного характера алгоритма. Авторами разработан менее трудоемкий метод вычисления параметра потока отказов систем большой размерности. Изложим известный и предлагаемый методы. Напомним, что коэффициент готовности (простоя) системы определяется на основе знания минимальных путей (Π_j), минимальных сечений (C_i) по следующим выражениям:

$$P\{S(x,t)=1\} = P\{\bar{S}(x,t)=0\} = P\{\bigvee_{j=1}^{r}\Pi_j=1\} = 1 - P\{\bigvee_{i=1}^{l}C_i=1\}, \quad (3.18)$$

$$P\{S(x,t)=0\} = P\{\bar{S}(x,t)=1\} = P\{\bigvee_{i=1}^{l}C_{ij}=1\} = 1 - P\{\bigvee_{j=1}^{r}\Pi_j=1\}, \quad (3.19)$$

где P{.} - вероятность наступления в момент **t** заключенного в скобки события.

Для вычисления коэффициента готовности (простоя) системы предложено большое число методов и алгоритмов. Основной направленностью этих разработок является стремление повысить эффективность преобразований логических выражений (3.8) и /или (3.9) для получения вероятностей (3.18) и /или (3.19). Проблема заключается в экспоненциальном росте вычислительной сложности при росте размерности системы (числа элементов, числа минимальных путей, сечений). Так, при вычислении коэффициента простоя по (3.19) с применением метода, использующего формулу вероятности объединения совместных событий, имеем следующее выражение

$$Q(t) = \sum_{i_1=1}^{l} P\{C_{i_1}\} - \sum_{i_1=1}^{l-1}\sum_{i_2>i_1}^{l} P\{C_{i_1} \wedge C_{i_2}\} + \sum_{i_1=1}^{l-2}\sum_{i_2>i_1}^{l-1}\sum_{i_3>i_2}^{l} P\{C_{i_1} \wedge C_{i_2} \wedge C_{i_3}\} - \ldots + \\ + (-1)^{l-1} P\{C_1 \wedge C_2 \wedge \ldots \wedge C_l\} \qquad (3.20)$$

Число слагаемых в правой части (3.20) будет $2^l - 1$. Сложной задачей является также алгоритмизация нахождения пересечений символьных подмножеств путей, сечений. Например, тестовый пример корабельной электроэнергетической системы, известный под названием «задача №35 И.А. Рябинина» [23,71], имеет 15 элементов, 31 минимальное сечение и 92 минимальных пути ($2^{31} > 2 \cdot 10^9$). В программных продуктах, реализующих этот метод вычисления показателей надежности (например, программа Risk Spectrum фирмы RELCON, Швеция), вынуждены отказываться от получения точных значений показателей и ограничиваться приближенными, которые при невысоких надежностях элементов дают слишком грубую оценку. Отметим весьма эффективные (в постановке (3.18), (3.19)) методы вычисления коэффициента готовности (простоя) систем, предложенные в [28, 57, 61-65].

Параметр потока отказов системы есть ожидаемое число появления отказа системы в момент времени t (т.е. на (t, t+Δt) при Δt→0), что означает возникновение по крайней мере одного сечения в момент времени t. Пусть e_i – событие появления i-го сечения в (t, t+Δt), где $e_i(t+\Delta t)$ – конъюнкция n_i переменных (элементов), образующих сечение C_i. Появление e_i на Δt означает (при ординарном потоке отказов), что в момент t неработоспособными были ($n_i - 1$) элементов сечения C_i (это событие обозначим e_i'), и произошел отказ на Δt одного (работоспособного в момент t) элемента. Вероятность появления на Δt сечения e_i определится по формуле полной вероятности так

$$P\{e_i\} = w_i^*(t) \cdot \Delta t = \sum_{j_i=1}^{n_i} [w_{j_i}(t) \cdot \prod_{g_i \neq j_i}^{n_i} Q_{g_i}(t)] \cdot \Delta t \ , \qquad (3.21)$$

где $w_{j_i}(t), Q_{g_i}(t)$ - параметр потока отказов и коэффициент простоя (неготовность) элементов j_i, g_i в момент времени t; $w_i^*(t)$ – параметр потока отказов, обусловленный появлением сечения C_i.

Известный метод [26] вычисления параметра потока отказов ω_S также основывается на формуле (3.20):

$$\omega_S \cdot \Delta t = P\{(S(x,t)=1) \wedge (\bigcup_{i=1}^{l} e_i)\} = P\{\bigcup_{i=1}^{l} e_i\} - P\{(S(x,t)=0) \wedge (\bigcup_{i=1}^{l} e_i)\} = (\omega_{S1} - \omega_{S2}) \cdot \Delta t \qquad (3.22)$$

$$\omega_{S1} \cdot \Delta t = \sum_{i_1=1}^{l} P\{e_{i_1}\} - \sum_{i_1=1}^{l-1} \sum_{i_2>i_1}^{l} P\{e_{i_1} \bigcap e_{i_2}\} + \sum_{i_1=1}^{l-2} \sum_{i_2>i_1}^{l-1} \sum_{i_3>i_2}^{l} P\{e_{i_1} \bigcap e_{i_2} \bigcap e_{i_3}\} - \ldots + (-1)^{l-1} P\{e_1 \bigcap e_2 \bigcap \ldots \bigcap e_l\}, \qquad (3.23)$$

$$\omega_{S2} \cdot \Delta t = \sum_{i=1}^{l} \Big[\sum_{j \neq i}^{l} P\{C_j \wedge e_i\} - \sum_{\substack{j_1=1 \\ j_1 \neq i}}^{l-1} \sum_{j_2=j_1+1}^{l} P\{C_{j_1} \wedge C_{j_2} \wedge e_i\} + \ldots + (-1)^{l-2} \cdot P\{C_1 \wedge \ldots \wedge C_{i-1} \wedge C_{i+1} \wedge \ldots \wedge C_l \wedge e_i\} \Big] -$$
$$- \sum_{i_1=1}^{l-1} \sum_{i_2=i_1+1}^{l} \Big[\sum_{j \neq i_1, i_2}^{l} P\{C_j \wedge (e_{i_1} \bigcap e_{i_2})\} - \sum_{\substack{j_1=1 \\ j_1, j_2 \neq i_1, i_2}}^{l-1} \sum_{j_2=j_1+1}^{l} P\{C_{j_1} \wedge C_{j_2} \wedge (e_{i_1} \bigcap e_{i_2})\} + \ldots + (-1)^{l-3} \cdot P\{C_1 \wedge C_2 \wedge \ldots \wedge C_{i_1-1} \wedge C_{i_1+1} \wedge \ldots \wedge C_{i_2-1} \wedge C_{i_2+1} \wedge \ldots \wedge C_l \wedge (e_{i_1} \bigcap e_{i_2})\} \Big] +$$
$$\ldots + \sum_{j=1}^{l} (-1)^{l-1} \cdot P\{C_j \wedge (e_1 \bigcap \ldots \bigcap e_{j-1} \bigcap e_{j+1} \bigcap \ldots \bigcap e_l)\} \qquad (3.24)$$

Событие $\{C_{j_1} \wedge C_{j_2} \wedge (e_{i_1} \bigcap e_{i_2})\}$ означает, что в момент t система находилась в отказе по причине реализации двух сечений C_{j_1}, C_{j_2}, и за Δt произошел отказ общего для сечений C_{i_1}, C_{i_2} элемента (т.е. на (t, t+Δt) появились сечения i_1 и i_2). Если такого элемента нет, то вероятность события появления сразу двух (и более) сечений на Δt равна нулю. Общий член равен

$$P\{C_{j_1} \wedge C_{j_2} \wedge \ldots \wedge \ldots \wedge C_{j_U} \wedge (e_{i_1} \bigcap e_{i_2} \bigcap \ldots \bigcap e_{i_G})\} = \omega_{GU}(t) \cdot \Delta t \cdot \prod_{1\ldots U}^{1\ldots G} Q(t), \qquad (3.25)$$

где $\omega_{GU}(t)$ - параметр потока группы элементов общих для G сечений и не входящих в U из остальных (l – G); $\prod_{1\ldots U}^{1\ldots G} Q(t)$ - произведение коэффициентов простоя всех элементов входящих в G сечений и U сечений из остальных (l – G), за исключением тех элементов, которые используются при вычислении $\omega_{GU}(t)$ ($\omega_{GU}(t)$ вычисляется по формуле аналогичной (3.5), если её применить для группы общих элементов, входящих в G сечений). При этом в произведении каждый элемент

учитывается только один раз. Вычисления параметра потока отказов по (3.21-3.24) ещё более трудоёмкая задача (более чем в 3 раза), чем коэффициента готовности (простоя) по (3.20).

В [63] предложен метод рекурсивного наращивания переменных для вычисления коэффициента готовности (простоя). Суть его в следующем. Пусть

$$\begin{aligned} p^{(k)} &= P\{S(x_1, x_2, ..., x_k; t) = 1 / x_{k+1} = 1, x_{k+2} = 1, ..., x_n = 1\} \\ r^{(k)} &= P\{S(x_1, x_2, ..., x_k; t) = 1 / x_{k+1} = 0, x_{k+2} = 1, ..., x_n = 1\} \end{aligned} \tag{3.26}$$

Вычисления проводятся по формуле

$$p^{(k+1)} = R_{k+1}(t) \cdot p^{(k)} + Q_{k+1}(t) \cdot r^{(k)} \tag{3.27}$$

где $R_{k+1}(t) = 1 - Q_{k+1}(t) = P\{x_{k+1}(t) = 1\}$, $p^{(0)} = 1$. Последовательно вычисляя $p^{(1)}, p^{(2)}, ..., p^{(n)}$, на последнем n-ом шаге рекурсии получим коэффициент готовности системы. Отметим, что определять с помощью логико-вероятностных преобразований и вычислений необходимо только $r^{(k)}$, т.к. $p^{(k+1)}$ определяются по (3.27).

Подход рекурсивного наращивания переменных (3.26, 3.27) применим и для вычисления параметра потока отказов. Пусть

$$\begin{aligned} \omega^{(k)}(t) \cdot \Delta t &= P\Big\{ (S(x, t) = 1) \wedge \Big(\bigcup_{i=1}^{l} e_i'\Big) / x_{k+1} = x_{k+2} = \ldots = x_n = 1 \Big\} \\ v^{(k)}(t) \cdot \Delta t &= P\Big\{ (S(x, t) = 1) \wedge \Big(\bigcup_{i=1}^{l} e_i'\Big) / x_{k+1} = 0, x_{k+2} = \ldots = x_n = 1 \Big\} \end{aligned} \tag{3.28}$$

Утверждение.

Параметр потока отказов системы рекурсивно вычисляется следующим образом

$$\omega^{(k+1)}(t) = R_{k+1}(t) \cdot \omega^{(k)}(t) + Q_{k+1}(t) \cdot v^{(k)}(t) + P^{x_{k+1}}_{\text{предотк}}(t) \cdot \omega_{k+1}(t), \quad \omega^{(0)}(t) = 0, \tag{3.29}$$

где $P^{x_{k+1}}_{\text{предотк}}(t) = (p^{(k)} - r^{(k)})$, k =(0,1, …, n-1)

Доказательство. На (k+1) шаге рекурсии элементы x_{k+2}, …, x_n системы абсолютно надежны и рассматривается полная группа несовместных событий относительно элемента x_{k+1}:

- элемент x_{k+1} в момент t работоспособен. Вероятность этого события $R_{k+1}(t)$, а параметр отказов системы равен $\omega(k)$ в соответствии с первым выражением (3.28);
- элемент x_{k+1} в момент t неработоспособен. Вероятность этого события $Q_{k+1}(t)$, а параметр отказов системы равен $v(k)$ в соответствии со вторым выражением (3.28);
- элемент x_{k+1} отказывает на $(t,t+\Delta t)$. Вероятность этого события $\omega_{k+1}(t) \cdot \Delta t$ (т.е. параметр потока отказов равен $\omega_{k+1}(t)$). А для того, чтобы при отказе элемента x_{k+1} система перешла в состояние неработоспособности необходимо, чтобы она находилась в таком предотказовом подмножестве

состояний, в котором элемент x_{k+1} работоспособен, но его отказ переводит систему в отказ. Вероятность такого подмножества предотказовых состояний обозначим $P^{x_{k+1}}_{\text{предотк}}(t)$. В [66] доказывается, что

$$P^{x_i}_{\text{предотк}}(t) = R_{\text{сист}}(t)/\{x_i = 1\} - R_{\text{сист}}(t)/\{x_i = 0\} \qquad (3.30)$$

где $R_{\text{сист}}(t)/\{A\}$ - условный коэффициент готовности системы, при условии А.

С учетом (3.30) на (k+1) шаге рекурсии $P^{x_{k+1}}_{\text{предотк}}(t) = p^{(k)} - r^{(k)}$.

В соответствии с формулой полной вероятности получаем (3.29).

Отметим, что (3.30) является значимостью i-го элемента по Бирнбауму, Рябинину [26,67].

Метод вычисления параметра потока отказов (3.28), (3.29) (как и коэффициента готовности, простоя (3.26), (3.27)) можно применять для вычислений, не декомпозируя систему. Но для преодоления проблем размерности, повышения быстродействия численных алгоритмов целесообразно проводить декомпозицию системы. В этом случае алгоритм вычисления параметра потока с использованием рассмотренных способов декомпозиции таков:

- все последовательные, параллельные и **k** из **m** надежностные группы элементов «укрупняются» в один элемент с вычисленным по ниже приведенным выражениям (3.31 - 3.33, 3.35) параметром потока отказов (а для коэффициента готовности, простоя - по известным формулам последовательного, параллельного и **k** из **m** соединения).
- оставшаяся структура (возможно, после нескольких итераций «укрупнения») называется в литературе «неприводимой». Вычисления параметра потока отказов в этом случае проводятся по (3.28, 3.29). Причем элементам наибольшее число раз входящим в различные конъюнкции (лучше в минимальные пути), различным перемычкам в графах связи, блок-схемах надежности, целесообразно присвоить наибольшие номера. Тогда вычисления на первых шагах рекурсии (пока эти элементы рассматриваются как работоспособные в соответствии с первым выражением (3.28)) оказываются достаточно простыми по формулам последовательно-параллельных соединений. При формализации этапа получения минимальных путей, сечений можно воспользоваться алгоритмом, предложенным в [57, 68], который позволяет выделять элементы, “делающие” надежностную структуру «неприводимой».

Параметр потока отказов для последовательных, параллельных и **(k** из **m)** структур имеет вид:

– m параллельно соединенных элементов, когда для работоспособности требуется один (1 из m)

$$\omega_{1\,\text{из}\,m}\{t\} = \sum_{j=1}^{m}[w_j(t)\cdot\prod_{g\neq j}^{m}Q_g(t)] \tag{3.31}$$

– m последовательно соединенных элементов, когда для работоспособности требуются все m (m из m)

$$\omega_{m\,\text{из}\,m}\{t\} = \sum_{j=1}^{m}[w_j(t)\cdot\prod_{g\neq j}^{m}R_g(t)] \tag{3.32}$$

– m параллельно соединенных элементов, когда для работоспособности требуются k элементов (k из m)

$$\omega_{k\,\text{из}\,m}\{t\} = \sum_{i_1<i_2<\ldots<i_{m-k}}^{m}Q_{i_1}\cdot Q_{i_2}\cdot\ldots\cdot Q_{i_{m-k}}\cdot\Big[\sum_{j=1,\,j\neq i_1,i_2,\ldots i_{m-k}}^{m}[w_j(t)\cdot\prod_{g=1,\,g\neq j,i_1,i_2,\ldots i_{m-k}}^{m}R_g(t)]\Big], \tag{3.33}$$

где $R_i(t),\quad Q_i(t)=1-R_i(t),\ \omega_i(t)$ - коэффициент готовности, коэффициент простоя, параметр потока отказов элемента i.

Выражения (3.31) – (3.33) могут быть получены из (3.22) – (3.24), либо непосредственно из

$$\omega_S = P\{(S(x,t)=1)\wedge(\bigcup_{i=1}^{l}e_i')\}. \tag{3.34}$$

Схемы резервирования **k** из **m** часто осуществляются из **m** одинаковых элементов, тогда выражение (3.33) примет вид

$$\omega_{k\,\text{из}\,m}\{t\} = C_m^{m-k}\cdot Q^{m-k}(t)\cdot k\cdot w(t)\cdot R^{k-1}(t), \tag{3.35}$$

где C_m^{m-k} - число сочетаний из **m** элементов по **(m – k)**.

Запишем выражение для параметра потока отказов, если применять декомпозицию системы разложением по элементу. Из (3.29) следует

$$\omega_S(t) = K_x(t)\cdot\omega_A(t) + (1-K_x(t))\cdot\omega_B(t) + (K_A(t)-K_B(t))\cdot\omega_x(t), \tag{3.36}$$

где $K_x(t)$ – коэффициент готовности элемента x, по которому осуществляется разложение;

$\omega_x(t)$ - параметр потока отказов элемента x, по которому осуществляется разложение;

$K_A(t)$, $K_B(t)$, – коэффициенты готовности системы при x=1 и x=0, соответственно;

$\omega_A(t)$, $\omega_B(t)$ – параметры потока отказов системы при x=1 и x=0, соответственно.

Общий способ вычисления $r^{(k)}$ и $\nu^{(k)}$ состоит в следующем. На каждом шаге рекурсии значения x_i, указанные в условии, подставляются в логические выражения (3.8), (3.9) и полученные выражения преобразуются в вероятностные функции относительно коэффициента готовности и параметра потока отказов (на данном шаге). При "ручном" расчете можно также изображать получаемую структуру, тогда все возможности использования для расчетов формул (3.31 – 3.33, 3.35, 3.36), применяя декомпозицию и агрегирование, будут видны. Отметим, что в общем случае при вычислении $r^{(k)}$ и $\nu^{(k)}$ на некоторых шагах может понадобиться рекурсия для данного шага, если получаемые логические выражения не будут соответствовать схемам, сводящимся к последовательным и параллельным соединениям. В этом случае на данном шаге решается как бы новая задача с полученным логическим описанием, в котором меньшее число переменных и меньшее число членов в логической форме.

Пример.

Рассмотрим классическую «неприводимую» мостиковую структуру (рис.3.1.в) и проведем вычисление параметра потока отказов двумя изложенными методами.

$C_1 = \bar{1}\cdot\bar{2};\ C_2 = \bar{3}\cdot\bar{4};\ C_3 = \bar{1}\cdot\bar{5}\cdot\bar{4};\ C_4 = \bar{2}\cdot\bar{5}\cdot\bar{3}$ (вместо элементов x_i пишем только индексы, символ конъюнкции заменяем на символ умножения).

1. Приведем расчет по (3.22) – (3.25).

$$\omega_{S1} = (\omega_1\cdot Q_2 + \omega_2\cdot Q_1) + (\omega_3\cdot Q_4 + \omega_4\cdot Q_3) + (\omega_1\cdot Q_5\cdot Q_4 + \omega_5\cdot Q_1\cdot Q_4 + \omega_4\cdot Q_1\cdot Q_5) +$$
$$(\omega_2\cdot Q_5\cdot Q_3 + \omega_5\cdot Q_2\cdot Q_3 + \omega_3\cdot Q_2\cdot Q_5) - \omega_1\cdot Q_2\cdot Q_5\cdot Q_4 - \omega_2\cdot Q_1\cdot Q_5\cdot Q_3 - \quad (3.37)$$
$$\omega_4\cdot Q_1\cdot Q_5\cdot Q_3 - \omega_3\cdot Q_2\cdot Q_5\cdot Q_4 - \omega_5\cdot Q_1\cdot Q_2\cdot Q_3\cdot Q_4.$$

В ω_{S1} вошли все e_i (соответствующие C_i -м) – первые четыре скобки, и пересечения по два e_i, e_j (пересечение $e_1 \cap e_2$ не имеет общих элементов, поэтому для этого события параметр потока отказов равен нулю).

$$\omega_{S2} = [(\omega_1\cdot Q_2 + \omega_2\cdot Q_1)\cdot Q_3\cdot Q_4 + \omega_2\cdot Q_1\cdot Q_5\cdot Q_4 + \omega_1\cdot Q_2\cdot Q_5\cdot Q_3]_1 - [\omega_2\cdot Q_1\cdot Q_3\cdot Q_5\cdot Q_4 +$$
$$\omega_1\cdot Q_2\cdot Q_5\cdot Q_3\cdot Q_4]_2 + [(\omega_3\cdot Q_4 + \omega_4\cdot Q_3)\cdot Q_1\cdot Q_2 + \omega_3\cdot Q_1\cdot Q_5\cdot Q_4 + \omega_4\cdot Q_2\cdot Q_5\cdot Q_3]_3 -$$
$$[\omega_3\cdot Q_1\cdot Q_2\cdot Q_5\cdot Q_4 + \omega_4\cdot Q_1\cdot Q_2\cdot Q_5\cdot Q_3]_4 + [(\omega_4\cdot Q_5 + \omega_5\cdot Q_4)\cdot Q_1\cdot Q_2 + (\omega_1\cdot Q_5 + \omega_5\cdot Q_1)\cdot$$
$$Q_3\cdot Q_4 + (\omega_1\cdot Q_4 + \omega_4\cdot Q_1)\cdot Q_2\cdot Q_5\cdot Q_3]_5 - [\omega_5\cdot Q_1\cdot Q_2\cdot Q_3\cdot Q_4 + \omega_4\cdot Q_1\cdot Q_2\cdot Q_5\cdot Q_3 +$$
$$\omega_1\cdot Q_3\cdot Q_4\cdot Q_2\cdot Q_5]_6 + [(\omega_3\cdot Q_5 + \omega_5\cdot Q_3)\cdot Q_1\cdot Q_2 + (\omega_2\cdot Q_5 + \omega_5\cdot Q_2)\cdot Q_3\cdot Q_4 + \quad (3.38)$$
$$(\omega_2\cdot Q_3 + \omega_3\cdot Q_2)\cdot Q_1\cdot Q_5\cdot Q_4]_7 - [\omega_5\cdot Q_1\cdot Q_2\cdot Q_3\cdot Q_4 + \omega_3\cdot Q_1\cdot Q_2\cdot Q_5\cdot Q_4 +$$
$$\omega_2\cdot Q_1\cdot Q_3\cdot Q_5\cdot Q_4]_8 - [\omega_1\cdot Q_3\cdot Q_4\cdot Q_2\cdot Q_5 + \cancel{\omega_1\cdot Q_3\cdot Q_4\cdot Q_2\cdot Q_5} - \cancel{\omega_1\cdot Q_3\cdot Q_4\cdot Q_2\cdot Q_5}]_9 -$$
$$[\omega_2\cdot Q_1\cdot Q_3\cdot Q_5\cdot Q_4 + \cancel{\omega_2\cdot Q_1\cdot Q_3\cdot Q_5\cdot Q_4} - \cancel{\omega_2\cdot Q_1\cdot Q_3\cdot Q_5\cdot Q_4}]_{10} - [\omega_4\cdot Q_1\cdot Q_2\cdot Q_5\cdot Q_3 +$$

$\omega_4 \cdot Q_1 \cdot Q_2 \cdot Q_5 \cdot Q_3 - \omega_4 \cdot Q_1 \cdot Q_2 \cdot Q_5 \cdot Q_3]_{11} - \omega_3 \cdot Q_1 \cdot Q_2 \cdot Q_5 \cdot Q_4 + \omega_3 \cdot Q_1 \cdot Q_2 \cdot Q_5 \cdot Q_4 -$

$\omega_3 \cdot Q_1 \cdot Q_2 \cdot Q_5 \cdot Q_4]_{12} - [\omega_5 \cdot Q_1 \cdot Q_2 \cdot Q_3 \cdot Q_4 + \omega_5 \cdot Q_1 \cdot Q_2 \cdot Q_3 \cdot Q_4 - \omega_5 \cdot Q_1 \cdot Q_2 \cdot Q_3 \cdot Q_4]_{13}$

В ω_{S2} вошли события: $e_1 \Lambda C_i$ – первая квадратная скобка (обозначим $[\ldots]_1$); $e_1 \Lambda C_i \Lambda C_j$ – вторая квадратная скобка (событие $C_3\ \Lambda C_4$ содержит отказ всех элементов системы, поэтому параметр для него равен нулю); $e_2 \Lambda C_i$, $e_3 \Lambda C_i$, $e_4 \Lambda C_i$, - квадратные скобки 3, 5, 7, соответственно; $e_2 \Lambda C_i \Lambda C_j$, $e_3 \Lambda C_i \Lambda C_j$, $e_4 \Lambda C_i \Lambda C_j$ - квадратные скобки 4, 6, 8, соответственно;

$e_1 \cap e_3 \Lambda C_2$, $e_1 \cap e_3 \Lambda C_4$, $e_1 \cap e_3 \Lambda C_2 \Lambda C_4$ – квадратная скобка 9; $e_1 \cap e_4 \Lambda C_2$, $e_1 \cap e_4 \Lambda C_3$, $e_1 \cap e_4 \Lambda C_2 \Lambda C_3$ – квадратная скобка 10; $e_2 \cap e_3 \Lambda C_1$, $e_2 \cap e_3 \Lambda C_4$, $e_2 \cap e_3 \Lambda C_1 \Lambda C_4$ – квадратная скобка 11; $e_2 \cap e_4 \Lambda C_1$, $e_2 \cap e_4 \Lambda C_3$, $e_2 \cap e_4 \Lambda C_1 \Lambda C_3$ - – квадратная скобка 12; $e_3 \cap e_4 \Lambda C_1$, $e_3 \cap e_4 \Lambda C_2$, $e_3 \cap e_4 \Lambda C_1 \Lambda C_2$ – квадратная скобка 13.

Пересечения e_i по три и четыре сечения для ω_{S1} и ω_{S2} не имеют общих элементов (поэтому их составляющая параметра потока отказов равна нулю). Но проделать все эти пересечения надо (и человеку, и машине).

Запишем окончательное выражение для параметра потока отказов в соответствии с (3.22) следующим образом:

$$\begin{aligned}\omega_{\text{системы}} = \omega_{S1} - \omega_{S2} = &[\omega_1 \cdot (Q_2 + Q_4 \cdot Q_5 - Q_2 \cdot Q_4 \cdot Q_5 - Q_2 \cdot Q_3 \cdot Q_4 - Q_2 \cdot Q_3 \cdot Q_5 - \\ &Q_3 \cdot Q_4 \cdot Q_5 + 2 \cdot Q_2 \cdot Q_3 \cdot Q_4 \cdot Q_5)] + [\omega_2 \cdot (Q_1 + Q_3 \cdot Q_5 - Q_1 \cdot Q_3 \cdot Q_5 - Q_1 \cdot Q_3 \cdot Q_4 - \\ &Q_1 \cdot Q_4 \cdot Q_5 - Q_3 \cdot Q_4 \cdot Q_5 + 2 \cdot Q_1 \cdot Q_3 \cdot Q_4 \cdot Q_5)] + [\omega_1 \cdot (Q_2 + Q_4 \cdot Q_5 - Q_2 \cdot Q_4 \cdot Q_5 - \\ &Q_2 \cdot Q_3 \cdot Q_4 - Q_2 \cdot Q_3 \cdot Q_5 - Q_3 \cdot Q_4 \cdot Q_5 + 2 \cdot Q_2 \cdot Q_3 \cdot Q_4 \cdot Q_5)] + [\omega_3 \cdot (Q_4 + Q_2 \cdot Q_5 - \\ &Q_2 \cdot Q_4 \cdot Q_5 - Q_1 \cdot Q_2 \cdot Q_4 - Q_1 \cdot Q_4 \cdot Q_5 - Q_1 \cdot Q_2 \cdot Q_5 + 2 \cdot Q_1 \cdot Q_2 \cdot Q_4 \cdot Q_5)] + [\omega_4 \cdot (Q_3 + \\ &Q_1 \cdot Q_5 - Q_1 \cdot Q_3 \cdot Q_5 - Q_1 \cdot Q_2 \cdot Q_3 - Q_2 \cdot Q_3 \cdot Q_5 - Q_1 \cdot Q_2 \cdot Q_5 + 2 \cdot Q_1 \cdot Q_2 \cdot Q_3 \cdot Q_5)] + \\ &[\omega_5 \cdot (Q_1 \cdot Q_4 + Q_2 \cdot Q_3 - Q_1 \cdot Q_2 \cdot Q_4 - Q_1 \cdot Q_3 \cdot Q_4 - Q_1 \cdot Q_2 \cdot Q_3 - Q_2 \cdot Q_3 \cdot Q_4 + \\ &2 \cdot Q_1 \cdot Q_2 \cdot Q_3 \cdot Q_4)]\end{aligned} \tag{3.39}$$

2. Вычислим теперь параметр потока отказов предлагаемым методом, предварительно получив выражения для условных коэффициентов готовности (простоя) в соответствии с (3.26), (3.27).

Логическую функцию работоспособности для вычисления запишем через пути

$$S(x, t) = \left\{ \bigvee_{j=1}^{4} A_j \right\} = 1, \quad A_1 = 1 \cdot 3;\ A_2 = 2 \cdot 4;\ A_3 = 1 \cdot 5 \cdot 4;\ A_4 = 2 \cdot 5 \cdot 3.$$

$$p^{(1)} = R_1 \cdot p^{(0)} + Q_1 \cdot r^{(0)} = R_1 \cdot 1 + Q_1 \cdot 1 = 1 \quad (r^{(0)} = P\{S(x) = 1 / x_1 = 0, x_2 = x_3 = x_4 = x_5 = 1\} = 1),$$

$$p^{(2)} = R_2 \cdot p^{(1)} + Q_2 \cdot r^{(1)} = R_2 \cdot 1 + Q_2 \cdot P\{S(x) = S(x_1) = 1 / x_2 = 0, x_3 = x_4 = x_5 = 1\} = R_2 + Q_2 \cdot R_1,$$

$$p^{(3)} = R_3 \cdot p^{(2)} + Q_3 \cdot r^{(2)} = R_3 \cdot (R_2 + Q_2 \cdot R_1) + Q_3 \cdot r^{(2)} = R_3 \cdot (R_2 + Q_2 \cdot R_1) + Q_3 \cdot P\{S(x) =$$

$$S(x_1, x_2) = 1 / x_3 = 0, x_4 = x_5 = 1\} = R_3 \cdot (R_2 + Q_2 \cdot R_1) + Q_3 \cdot (R_2 + Q_2 \cdot R_1) = R_2 + Q_2 \cdot R_1,$$

$$p^{(4)} = R_4 \cdot p^{(3)} + Q_4 \cdot r^{(3)} = R_4 \cdot (R_2 + Q_2 \cdot R_1) + Q_4 \cdot P\{S(x) = S(x_1, x_2, x_3) = 1 / x_4 = 0, x_5 = 1\} = \qquad (3.40)$$

$$R_4 \cdot (R_2 + Q_2 \cdot R_1) + Q_4 \cdot R_3 \cdot (R_2 + Q_2 \cdot R_1) = (R_2 + Q_2 \cdot R_1) \cdot (R_4 + Q_4 \cdot R_3),$$

$$R_{\text{системы}} = P\{S(x,t)=1\} = p^{(5)} = R_5 \cdot p^{(4)} + Q_5 \cdot r^{(4)} = R_5 \cdot (R_2 + Q_2 \cdot R_1) \cdot (R_4 + Q_4 \cdot R_3) +$$

$$Q_5 \cdot P\{S(x) = S(x_1, x_2, x_3, x_4) = 1 / x_5 = 0\} = R_5 \cdot (R_2 + Q_2 \cdot R_1) \cdot (R_4 + Q_4 \cdot R_3) +$$

$$Q_5 \cdot (1 - (1 - R_1 \cdot R_3) \cdot (1 - R_2 \cdot R_4))$$

Найдем параметр потока отказов в соответствии с (3.28), (3.29).

$$\omega^{(1)} = R_1 \cdot \omega^{(0)} + Q_1 \cdot v^{(0)} + \omega_1 \cdot (p^{(0)} - r^{(0)}) = R_1 \cdot 0 + Q_1 \cdot P\{(S(x, t) = 1) \wedge$$

$$(\bigcup_{i=1}^{4} e_i^{'}) / x_1 = 0, x_2 = \ldots = x_5 = 1\} + \omega_1 \cdot (1 - 1) = 0;$$

$$\omega^{(2)} = R_2 \cdot \omega^{(1)} + Q_2 \cdot v^{(1)} + \omega_2 \cdot (p^{(1)} - r^{(1)}) = R_2 \cdot 0 + Q_2 \cdot P\{(S(x, t) = 1) \wedge$$

$$(\bigcup_{i=1}^{4} e_i^{'}) / x_2 = 0, x_3 = x_4 = x_5 = 1\} + \omega_2 \cdot (1 - R_1) = Q_2 \cdot \omega_1 + \omega_2 \cdot (1 - R_1) = Q_2 \cdot \omega_1 + \omega_2 \cdot Q_1;$$

$$\omega^{(3)} = R_3 \cdot \omega^{(2)} + Q_3 \cdot v^{(2)} + \omega_3 \cdot (p^{(2)} - r^{(2)}) = R_3 \cdot (Q_2 \cdot \omega_1 + \omega_2 \cdot Q_1) +$$

$$Q_3 \cdot P\{(S(x, t) = 1) \wedge (\bigcup_{i=1}^{4} e_i^{'}) / x_3 = 0, x_4 = x_5 = 1\} + \omega_3 \cdot (R_2 + Q_2 \cdot R_1 - R_2 - Q_2 \cdot R_1) = \qquad (3.41)$$

$$R_3 \cdot (Q_2 \cdot \omega_1 + \omega_2 \cdot Q_1) + Q_3 \cdot (Q_2 \cdot \omega_1 + \omega_2 \cdot Q_1) = Q_2 \cdot \omega_1 + \omega_2 \cdot Q_1;$$

$$\omega^{(4)} = R_4 \cdot \omega^{(3)} + Q_4 \cdot v^{(3)} + \omega_4 \cdot (p^{(3)} - r^{(3)}) = R_4 \cdot (Q_2 \cdot \omega_1 + \omega_2 \cdot Q_1) +$$

$$Q_4 \cdot P\{(S(x, t) = 1) \wedge (\bigcup_{i=1}^{4} e_i^{'}) / x_4 = 0, x_5 = 1\} + \omega_4 \cdot (R_2 + Q_2 \cdot R_1 - R_3 \cdot (R_2 + Q_2 \cdot R_1))$$

$$= R_4 \cdot (Q_2 \cdot \omega_1 + \omega_2 \cdot Q_1) + Q_4 \cdot (\omega_3 \cdot (1 - Q_1 \cdot Q_2) + R_3 \cdot (\omega_1 \cdot Q_2 + \omega_2 \cdot Q_1)) + \omega_4 \cdot Q_3 \cdot (R_2 + Q_2 \cdot R_1);$$

$$\omega_{\text{системы}} = \omega^{(5)} = R_5 \cdot \omega^{(4)} + Q_5 \cdot v^{(4)} + \omega_5 \cdot (p^{(4)} - r^{(4)}) = R_5 \cdot [R_4 \cdot (Q_2 \cdot \omega_1 + \omega_2 \cdot Q_1) +$$

$$Q_4 \cdot [\omega_3 \cdot (1 - Q_1 \cdot Q_2) + R_3 \cdot (\omega_1 \cdot Q_2 + \omega_2 \cdot Q_1)] + \omega_4 \cdot Q_3 \cdot (R_2 + Q_2 \cdot R_1)] + Q_5 \cdot [(\omega_3 \cdot R_1 +$$

$$\omega_1 \cdot R_3) \cdot (1 - R_2 \cdot R_4) + (\omega_2 \cdot R_4 + \omega_4 \cdot R_2) \cdot (1 - R_1 \cdot R_3)] +$$

$$\omega_5 \cdot [(R_2 + Q_2 \cdot R_1) \cdot (R_4 + Q_4 \cdot R_3) - (1 - (1 - R_1 \cdot R_3) \cdot (1 - R_2 \cdot R_4))]$$

Прокомментируем вычисление некоторых $r^{(k)}$ и $\nu^{(k)}$.

$r^{(0)} = P\{S(x) = 1 / x_1 = 0, x_2 = x_3 = x_4 = x_5 = 1\} = 1$ - при условном событии в момент t неработоспособности x_1 и работоспособности остальных элементов, $S(x) = 1$ является достоверным событием и искомая вероятность равна 1.

$\nu^{(0)} \cdot \Delta t = P\{(S(x, t) = 1) \wedge (\bigcup_{i=1}^{4} e_i^{'}) / x_1 = 0, x_2 = \ldots = x_5 = 1\}$ - при работоспособности в момент t элементов 2 – 5 отказа системы быть не может (т.е. $\bigcup_{i=1}^{4} e_i$ - невозможное событие), поэтому $\nu^{(0)} = 0$.

$r^{(1)} = P\{S(x,t) = S(x_1,t) = 1 / x_2 = 0, x_3 = x_4 = x_5 = 1\} = R_1$- при отказавшем элементе x_2 и работоспособным $x_3 – x_5$ (подставив их в S(x), записанную через пути A_i), получаем

$S(x) = x_1$, поэтому $r^{(1)} = R_1$.

$\nu^{(1)} \cdot \Delta t = P\{(S(x, t) = 1) \wedge (\bigcup_{i=1}^{4} e_i^{'}) / x_2 = 0, x_3 = x_4 = x_5 = 1\} = \omega_1 \cdot \Delta t$ - подставляя $x_2 = 0$, $x_3 = x_4 = x_5 = 1$ в пути $A_i(t)$ и сечения C_i $(t+\Delta t)$, получаем $S(x) = x_1$, $e_1(t+\Delta t) = \bar{x}_1 \cdot 1 = \bar{x}_1$, остальные $e_i = 0$. Чтобы в $t+\Delta t$ произошел отказ x_1, надо, чтобы в момент t он был работоспособен, поэтому $e_1(t) = x_1$. Итак, $\nu^{(1)} = \omega_1$.

$r^{(2)} = P\{S(x) = S(x_1, x_2) = 1 / x_3 = 0, x_4 = x_5 = 1\} = R_2 + Q_2 \cdot R_1$ - подставим значения переменных в условии в S(x,t), выраженное через пути. Получим $S(x,t) = S(x_1,x_2,t) = x_1+x_2$, что сразу позволяет записать $r^{(2)} = R_2 + Q_2 \cdot R_1$ (параллельное соединение x_1 и x_2).

$\nu^{(2)} \cdot \Delta t = P\{(S(x, t) = 1) \wedge (\bigcup_{i=1}^{4} e_i^{'}) / x_3 = 0, x_4 = x_5 = 1\} = Q_2 \cdot \omega_1 + \omega_2 \cdot Q_1$ - выражение для S(x,t) (с учетом условия) уже получено, а при подстановке условия в сечения, которые должны появиться в момент $(t, t+\Delta t)$, имеем $e_1(t, t+\Delta t) = C_1(t, t+\Delta t) = \bar{x}_1 \cdot \bar{x}_2$. Чтобы в $(t, t+\Delta t)$ реализовалось это сечение, необходима реализация в момент t события $e_1^{'}(t) = x_1 \cdot \bar{x}_2 + x_2 \cdot \bar{x}_1$. $(S(x,t) = x_1+x_2) \wedge (e_1^{'}(t) = x_1 \cdot \bar{x}_2 + x_2 \cdot \bar{x}_1) = x_1 \cdot \bar{x}_2 + x_2 \cdot \bar{x}_1$, поэтому $\nu^{(2)} = Q_2 \cdot \omega_1 + \omega_2 \cdot Q_1$ (что можно было записать сразу по виду S(x,t) для параллельного соединения в соответствие с (3.31)).

Если в $\omega_{системы}$ (3.41) заменить все R_i на $(1-Q_i)$ и привести подобные, то получим (3.39).

Вывод по примеру.

При расчете известным методом по (3.22) – (3.25) было сделано следующее число L шагов преобразований логического описания (логическое описание состояло из 4-х сечений):

– для вычисления ω_{S1}: $L(\omega_{S1}) = (C_4^1=4)+(C_4^2=6)+(C_4^3=4)+(C_4^4=1)=15.$ (3.42)

В (3.42) первая скобка равна числу членов первой суммы в выражении для ω_{S1} (3.23) и соответствует первым четырем круглым скобкам в (3.37). Вторая скобка в (3.42) равна числу членов второй (двойной) суммы для ω_{S1} в (3.23) и соответствует оставшимся пяти слагаемым (с минусом; шестое слагаемое равно нулю) в (3.37). Остальные две скобки в (3.42) соответствуют

числу членов третьей (тройной) суммы и последнему слагаемому для ω_{S1} в (3.23). В (3.37) составляющие от этих преобразований отсутствуют, т.к. они равны нулю.

– для вычисления ω_{S2} (в соответствии с (3.38)):

$$L(\omega_{S2}) = [(C_4^1=4)\cdot(C_3^1+C_3^2+C_3^3=7)]_1+[(C_4^2=6)\cdot(C_2^1+C_2^2=3)]_2+[(C_4^3=4)\cdot(C_1^1=1)]_3 = 50. \quad (3.43).$$

В первых круглых скобках в каждом из трех слагаемых, определяемых квадратными скобками, число появления одного, двух и трех e_i (сечений) на Δt, соответственно. А вторые круглые скобки – число возможных комбинации наличия остальных сечений в момент t.

В результате выполнения ряда шагов могут получаться пустые множества, поэтому формульные составляющие от таких шагов равны нулю. Ещё раз подчеркнем, что все эти шаги надо проделать, в том числе те, которые дадут нулевой результат.

Таким образом, общее число шагов L = 65.

При расчете предлагаемым методом ((3.28), (3.29) с учетом (3.26), (3.27)) переборных комбинаторных шагов нет. Здесь шагами расчета являются рекурсивные итерации наращивания переменных. Для рассматриваемого примера было проделано 5 шагов вычисления $r^{(k)}$ ($r^{(0)}$,…, $r^{(4)}$) и 5 шагов вычисления $\nu^{(k)}$ ($\nu^{(0)}$, …, $\nu^{(4)}$).

Форма представления конечного результата в предлагаемом методе более экономная и более удобная для анализа (приближение к конечному результату происходит лишь суммированием составляющих рекурсивных итераций).

3.6. Метод вычисления параметра потока отказов в немонотонных моделях

Остановимся на особенностях вычисления параметра потока переходов в заданное логическим немонотонным выражением подмножество состояний. Напомним, что немонотонные логико-вероятностные модели систем обязательно содержат как работоспособные, так и неработоспособные наборы элементов. Немонотонные модели формализуют некоторые, можно сказать «промежуточные», состояния системы, в которых обязательно присутствуют как отказавшие наборы элементов, так и работоспособные. На рис.3.5 приведен вид надежностной модели в виде графа состояний и переходов некоторой системы. На рисунке стрелки от состояний с меньшими номерами к состояниям с большими – это потоки отказов элементов, а стрелки от состояний с большими номерами к состояниям с меньшими – это потоки восстановления элементов (если нумерация состояний такова, что состояния с большей кратностью отказов имеют и больший номер).

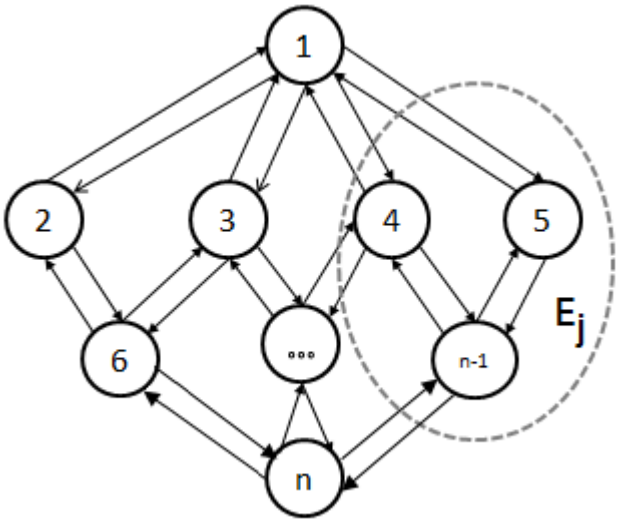


Рис. 3.5. Граф переходов между состояниями системы.

Пусть обведенные состояния 4, 5, n-1 определяют класс (подмножество) состояний системы, в которых эффективность функционирования составляет уровень E_j. Тогда переходы в это подмножество состояний определяются как потоком отказов по стрелкам из состояний с меньшими номерами в соответствующие состояния данного подмножества, так и параметром восстановления - по стрелкам из состояний с большими номерами в соответствующие состояния с меньшими номерами данного класса состояний. Отметим, что в классе монотонных двухуровневых моделей всё множество состояний разделено на два подмножества, одно соответствует работоспособности системы, другое – отказу. Разделяющая эти два подмножества линия является незамкнутой и переходы из одного подмножества в другое определяются одним потоком либо отказов, либо восстановления.

Логическая функция $Y(E_j)$, выделяющая класс состояний, эквивалентных промежуточному уровню E_j, может быть разделена на две составляющие A и $\overline{B}$, объединенных конъюнкцией

$$Y(E_j) = A \wedge \overline{B}, \tag{3.44}$$

где A – логическое выражение работоспособности части структуры системы, необходимой для обеспечения уровня не ниже E_j; $\overline{B}$ - логическое выражение неработоспособности части структуры системы, не позволяющей системе работать на уровне выше E_j.

Предлагается вычисление параметра потока переходов из подмножества состояний $\overline{Y}(E_j)$ в подмножество $Y(E_j)$ проводить следующим образом:

1. Выражение (3.44) необходимо представить в дизъюнктивной нормальной форме (ДНФ), где каждая конъюнкция будет содержать как работоспособные в момент времени t элементы (из составляющей A выражения (3.44); обычно в виде минимальных путей), так и неработоспособные элементы (из составляющей $\overline{B}$ выражения (3.44); обычно в виде минимальных сечений). Элементы составляющих помечаются, чтобы для одних записывать параметр потока восстановлений (для элементов составляющей A), а для других (для элементов составляющей $\overline{B}$) – параметр потока отказов.

2. Пусть K_i – событие появления в (t, t+Δt) i-й конъюнкции, содержащей одно сечение из $\overline{B}$ и один путь из A, т.е. i-я конъюнкция имеет вид $K_i = C_i \wedge A_i$, причем в C_i и A_i нет общих элементов. Появление K_i на Δt означает (при ординарном потоке отказов, восстановления):

а) в момент t неработоспособными были $(n_i - 1)$ элементов сечения C_i (n_i число элементов сечения C_i) и произошел отказ на Δt одного (работоспособного в момент t) элемента; при этом все элементы пути A_i – работоспособны;

б) в момент t работоспособными были $(h_i - 1)$ элементов пути A_i (h_i число элементов пути A_i) и произошло восстановление одного (неработоспособного в момент t) элемента; при этом все элементы сечения C_i – неработоспособны. Тогда вероятность появления на Δt конъюнкции K_i определится по формуле полной вероятности так

$$P\{K_i\} = w_i^*(t)\cdot\Delta t = \prod_{r=1}^{h_i} R_r(t)\cdot\sum_{j_i=1}^{n_i}[w_{j_i}(t)\cdot\prod_{g_i\neq j_i}^{n_i} Q_{g_i}(t)]\cdot\Delta t + \prod_{r=1}^{n_i} Q_r(t)\cdot\sum_{j_i=1}^{h_i}[\psi_{j_i}(t)\cdot\prod_{g_i\neq j_i}^{h_i} R_{g_i}(t)]\cdot\Delta t, \quad (3.45)$$

где $w_{j_i}(t)$ - параметр потока отказов и восстановления элементов j_i;

$\psi_{j_i}(t)$ - параметр потока восстановления элементов j_i;

$Q_r(t),\ Q_{gi}(t)$ - коэффициент простоя (неготовность) элементов r, g_i в момент времени t;

$R_r(t),\ R_{gi}(t)$ - коэффициент готовности элементов r, g_i в момент времени t;

$w_i^*(t)$ – параметр потока переходов, обусловленный появлением конъюнкции K_i.

3. Итак, имеем описание подмножества состояний, куда осуществляется переход в виде

$$Y(E_j) = K_1 \vee K_2 \vee \cdots \vee K_s \ . \quad (3.46)$$

Далее вычисления можно проводить либо в соответствии с выражениями (3.22 – 3.25) (которые реализуют формулу (3.20), с заменой сечений C_i на конъюнкции K_i, содержащие и сечения и пути, необходимые для перехода в искомое подмножество состояний). Для каждого набора K_i вычисления проводятся по (3.45). Либо можно применить рекурсивную процедуру (3.28,

3.29) (запишем выражения для этой процедуры ещё раз, чтобы выделить немонотонную функцию $Y(E_j)$). Выражения для параметра потока отказов той части логического критерия, которая связана с отказами будут иметь вид

$$\omega^k(t)\cdot\Delta t = P\{(Y(E_j, x, t)=1) \wedge (\bigcup_{i=1}^{l} e_i) / x_{k+1} = x_{k+2} = \ldots = x_n = 1\}$$
$$v^k(t)\cdot\Delta t = P\{(Y(E_j, x, t)=1) \wedge (\bigcup_{i=1}^{l} e_i) / x_{k+1} = 0, x_{k+2} = \ldots = x_n = 1\} \quad (3.47)$$

где x_i – i-ый элемент системы (x_i =1 – работоспособность, x_i =0 – отказ i-го элемента); $Y(E_j, x,t)$ =1 – логическая функция перехода в искомое подмножество; e_i – событие появления i-го сечения отказа либо пути восстановления работоспособности в (t, t+Δt); ω^k, ν^k – условный параметр потока отказов системы на k шаге рекурсии.

А выражения для параметра потока восстановления составляющих логического критерия, связанных с работоспособностью элементов примут вид

$$\psi^k(t)\cdot\Delta t = P\{(Y(E_j, x, t)=0) \wedge (\bigcup_{i=1}^{r} \eta_i) / x_{k+1} = 0, x_{k+2} = \ldots = x_n = 1\}$$
$$\varphi^k(t)\cdot\Delta t = P\{(Y(E_j, x, t)=0) \wedge (\bigcup_{i=1}^{r} \eta_i) / x_{k+1} = x_{k+2} = \ldots = x_n = 1\} \quad (3.48)$$

$$\psi^{k+1}(t) = Q_{k+1}(t)\cdot\psi^k(t) + R_{k+1}(t)\cdot\varphi^k(t) + (p^k - r^k)\cdot\psi_{k+1}(t), \quad \psi^0(t) = 0 \quad (3.49)$$

где ψ^k, φ^k - условные параметры потока восстановления системы на k-ом шаге рекурсии; ψ_{k+1} - параметр потока восстановления элемента k +1; η - множество минимальных путей попадания в состояния, определяемые логической функцией $Y(E_j)$.

В выражениях (3.47 – 3.49) параметры потока отказов (ω(t)) и потока восстановления элемента (ψ(t)), в предположении экспоненциальных распределений наработки до отказа и времени восстановления, имеют вид:

$$\omega(t) = \frac{\mu\lambda}{\lambda+\mu} + \frac{\lambda^2}{\lambda+\mu}\exp\{-(\lambda+\mu)t\} \quad (3.50)$$

$$\psi(t) = \frac{\lambda\mu}{\lambda+\mu}(1-\exp\{-(\lambda+\mu)t \quad (3.51)$$

где λ – интенсивность отказов элемента, μ - интенсивность восстановления элемента.

Таким образом, осуществляя преобразования и вычисления в соответствии с подпунктами 1 – 3, получим параметр потока переходов в заданное немонотонным логическим выражением (3.44) подмножество состояний.

Алгоритм вычисления следующий:

- для интересующего исследователя подмножества состояний системы записывается логическое выражение (3.44), которое затем преобразуется к виду (3.46)
- вычисляются численные значения параметров потока отказов и восстановления для каждого элемента системы по (3.50), (3.51) и их коэффициенты готовности, простоя
- проводятся вычисления либо по (3.22-3.24), где для каждой конъюнкции K_i и пересечения конъюнкций (пересечение также будет конъюнкцией), параметр потока определяется по (3.45).
- либо вычисления проводятся для условных конъюнкций по (3.47 – 3.49) также с использованием (3.45), где вид условных конъюнкций последовательно с шагами рекурсии определяется состояниями элементов, стоящими в условиях выражений (3.47, 3.48).

Практическое применение методологии анализа надежности многоуровневых систем с оценкой показателей вероятностей пребывания на каждом уровне эффективности функционирования, параметров переходов между уровнями и средних времён пребывания на уровне осуществлялось при техническом проектировании вариантов развития Кольцевого Газопровода Московской области (КГМО). По вычисленным выше указанным показателям оценивался основной показатель - коэффициент сохранения эффективности газоснабжения [69, 70].

Глава 4. Деревья отказов, деревья событий

4.1. Основные положения методологии деревьев отказов

Методология деревьев отказов начала развиваться с 1962 г., когда впервые была применена в Bell Telephone Laboratories для анализа надежности систем управления запуском ракет “Минитмен”. Дальнейшее развитие методологии связано с исследованиями надежности и безопасности, проводимыми компанией Boeing. В настоящее время методология качественного и количественного анализа деревьев отказов является стандартом де факто для исследований надежности и безопасности в таких важнейших областях как авиастроение, атомная энергетика, космическая промышленность, нефтегазовая отрасль, объекты уничтожения химического оружия.

Деревья отказов (Fault Tree) представляют собой визуализацию логико-вероятностных моделей теории надежности. В классическом варианте, с точки зрения учитываемых в модели факторов “надежностного поведения” исследуемых объектов и применяемого математического аппарата, деревья отказов ничем не отличаются от логико-вероятностных методов. Единственным отличием данной методологии является формальное представление логики возникновения отказа системы при возникновении отказов ее элементов и, возможно, влиянии внешних факторов в виде деревьев. Причем, сама методология построения дерева отказов основывается на, так называемой, дедуктивной логике исследований, когда интересующее исследователя нежелательное событие является вершиной дерева (вершинным событием (Top Event)), и выявляются все причины, которые могут привести к данному нежелательному событию. То есть, на каждом уровне рассмотрения событий задается вопрос “каким образом это может произойти?”. При визуальном представлении в виде дерева аргументы логической функции заменяются базовыми событиями, а операции дизъюнкции $\vee$ и конъюнкции $\wedge$ логическими вершинами (операторами) OR (ИЛИ), AND (И) соответственно. В таблице 4.1 перечислены наиболее распространенные вершины и базовые события деревьев отказов. Первоначально деревья содержали только логические вершины OR и AND, что полностью повторяло логико-вероятностные монотонные модели. Такие деревья называют *классическими или когерентными деревьями отказов*.

Аналогично логико-вероятностным методам, в которых может быть сконструирована как функция работоспособности, так и функция отказа исследуемого объекта, вершинное событие дерева может соответствовать как отказу, так и работоспособности. В последнем случае термин “дерево отказов” заменяют на “дерево успехов”. На рис.4.1 а и б показаны классические деревья отказа и успеха объекта, выполняющего две функции. Отказом объекта считается невыполнение

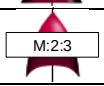
хотя бы одной функции (4.1.а). Если обе функции выполняются, объект считается работоспособным (4.1.б).

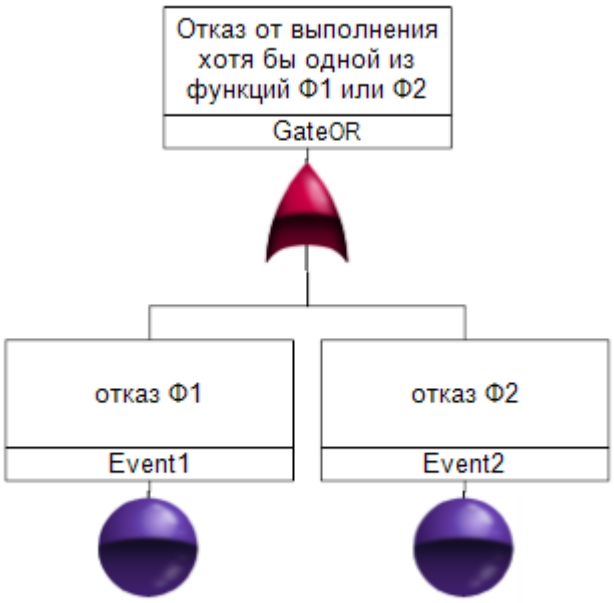
Дальнейшее развитие методологии деревьев отказов связано с добавлением логического оператора NOT (НЕ), что аналогично немонотонной логико-вероятностной теории. Например, на рис.4.1.в показано *некогерентное дерево*, соответствующее выполнению объектом только функции Ф2 и отказу Ф1. Введение оператора XOR (исключающее ИЛИ) позволяет обобщить этот случай и отобразить событие работы только одной из двух функций, либо Ф1, либо Ф2 (рис 4.1.г). Возможность выделения определенных функций с помощью некогерентных деревьев позволяет строить многоуровневые модели надежности, т.е. учитывать несколько уровней эффективности (производительности) функционирования, и определять показатели эффективности. Кроме того, становится возможным выделять состояния отказа разной степени критичности.

В последнее время деревья отказов стали активно применяться в анализе безопасности. Так, деревья отказов являются основной утвержденной МАГАТЭ[2] методологией при проведении вероятностного анализа безопасности атомных станций. Набор вершин OR, AND, XOR, NOT, NOR, NAND, получивших название *статические вершины*, не позволяет проводить полноценный анализ безопасности, так как с их помощью нельзя описать развертывание во времени моделируемой ситуации. Проблема решается введением *динамических вершин* (см. таблицу 4.1). Важнейшей из динамических вершин является PAND (приоритетное И). С помощью приоритетного И можно отобразить последовательность возникновения отказов. Так, если нас интересует вероятность того, что отказ Ф1 возникнет раньше Ф2, то имеем дерево отказов, приведенное на рис. 4.1.д. Деревья, в которые входят операторы, учитывающие развитие процесса возникновения базовых событий во времени, называются *динамическими деревьями отказов.* Динамические деревья реализуются с помощью марковских процессов и будут подробно описаны после изложения марковских моделей надежности в главе 6.

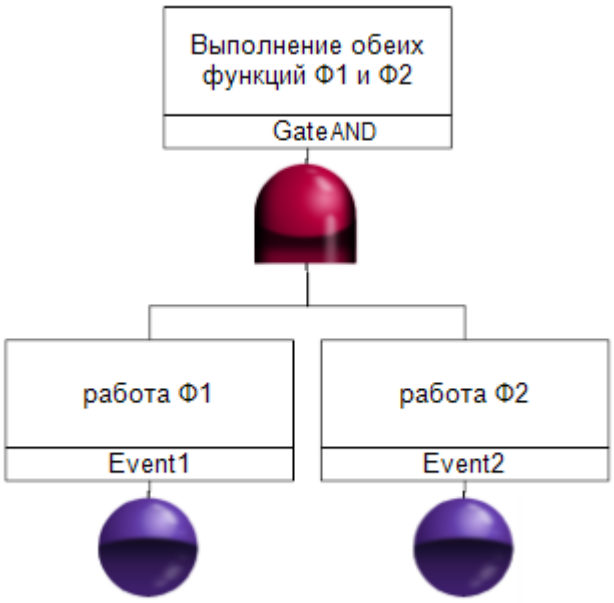
[2] МАГАТЭ (IAEA) – Международное Агентство по Атомной Энергетике

Таблица 4.1. Обозначение вершин и событий деревьев отказов

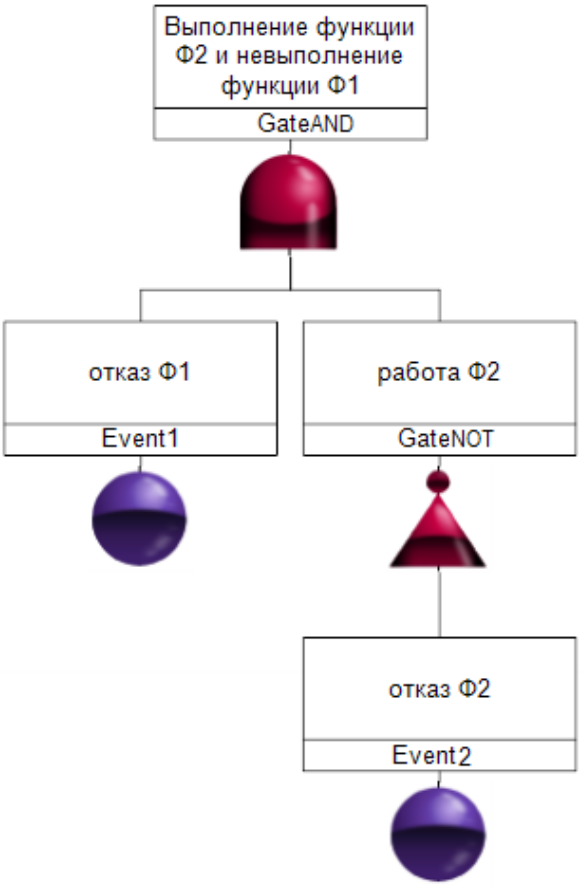
вершина	название	описание
	AND	логическое И
	OR	логическое ИЛИ
	NAND	логическое И-НЕ
	NOR	логическое ИЛИ-НЕ
	NOT	логическое НЕ
	VOTING (k/n)	m:n голосование (выбор входов по критерию m из n)
	INHIBIT	логическое И с запрещающим входом (ингибиторное И)
	XOR	исключающее ИЛИ
	PRIORITY AND (PAND)	приоритетное И (динамический оператор)
	FDEP	функциональная зависимость (динамический оператор)
	SPARE	гибридное резервирование (динамический оператор)
	SEQ	последовательность возникновения событий (динамический оператор)
	TRANSFER	разбивает дерево на поддеревья, располагаемые на разных листах (вспомогательный оператор)
	REMARKS	ввод комментариев (вспомогательный оператор)
событие	название	описание
	BASIC	базовое событие
	BASIC Repeated Event	повторяющееся базовое событие
	UNDEVELOPED	сложное (составное) базовое событие
	UNDEVELOPED Repeated Event	повторяющееся сложное базовое событие



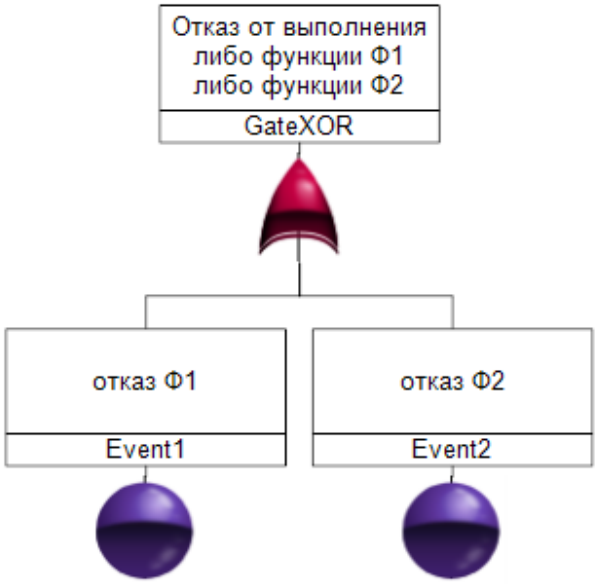
а). Когерентное дерево отказов.



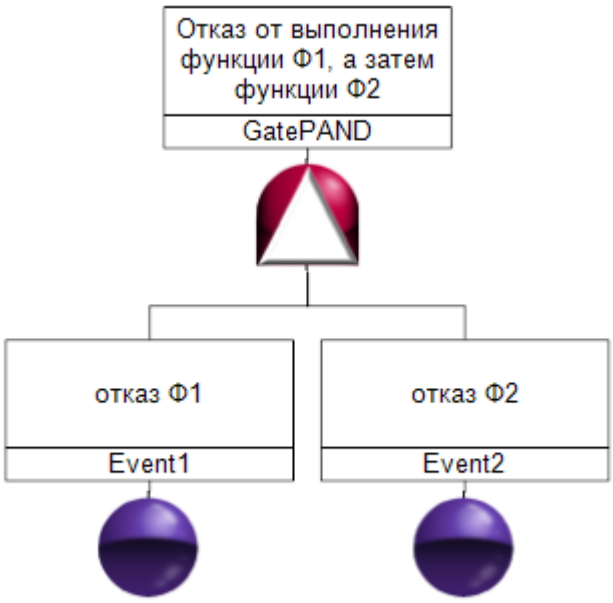
б). Когерентное дерево успехов.



в). Некогерентное дерево отказа Ф1 и работы Ф2.



г). Некогерентное дерево отказа одной и работы другой функции.



д.) Дерево отказов функции Ф1, а затем Ф2.

Рис.4.1. Деревья объекта, выполняющего две функции Ф1 и Ф2.

4.2. Подходы к построению деревьев отказов структурно сложных систем

Процесс построения дерева достаточно эвристичен, а его результат во многом зависит от знаний и квалификации аналитика. Описывая логику, приводящую к возникновению вершинного события, можно строить различные деревья. Однако логические функции, соответствующие этим деревьям, должны быть эквивалентны, с точки зрения получаемого результата. Приведем примеры построения когерентных (монотонных) и некогерентных (немонотонных) деревьев отказов и успехов. Начнем с построения деревьев отказов мостиковой схемы (рис.3.1.в). Несмотря на кажущуюся простоту мостиковой схемы, на ее примере можно продемонстрировать три основных подхода к построению деревьев структурно-сложных схем. Первый подход основан на перечислении минимальных сечений (путей) схемы и, следовательно, пригоден только для систем небольшой размерности. Второй более универсальный подход основан на обратном проходе всех узлов схемы, начиная с выходного. При проходе для каждого узла определяется логика его отказа (работоспособности). Третий подход основан на применении принципа разложения относительно выделенных элементов. Последовательное разложение дерева на несовместные составляющие позволяет проводить анализ достаточно сложных систем. Так, для построения дерева отказов известной “35 задачи” И.А. Рябинина [71] достаточно проведение трех итераций разложения.

На рис.4.2 показано дерево отказов мостиковой схемы, построенное на основе априорного знания набора минимальных сечений {1,2}, {3,4}, {1,4,5}, {1,3,5}. На рисунках 4.3 и 4.4 соответственно приведены деревья отказов и успехов мостика. Эти деревья построены на основе прохода узлов схемы от выхода к входу. Дерево на рис. 4.5 построено на основе разложения относительно перемычки мостика (элемент 5). Здесь и далее представленные деревья набраны в модуле FTA анализа Windchill Quality Solutions. При наборе деревьев помимо стандартных базовых событий и логических операторов используются повторяющиеся события (repeated events) (см. табл.4.1). Повторяющиеся базовые события аналогично повторяющимся элементам блок схем учитывают возможность присутствия одного и того же события в разных ветвях дерева. Например, в дереве (рис.4.2) отказ элемента 1 (повторяющееся базовое событие event 16) приведет к тому, что соответствующие входы гейтов 14 и 16 одновременно примут значение true (истинна).

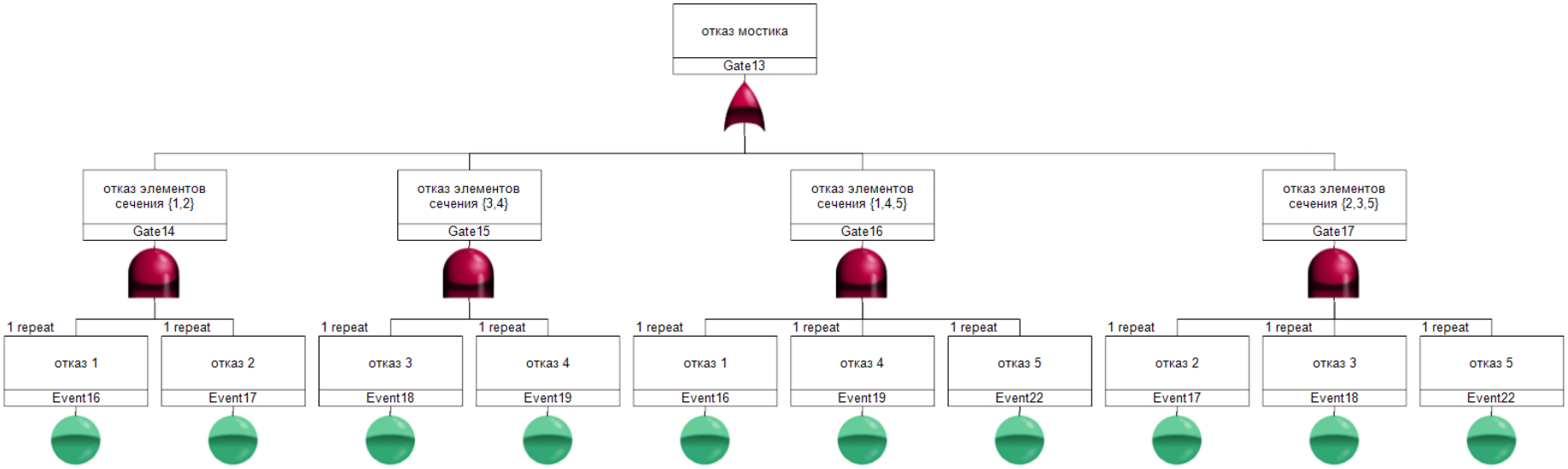


Рис.4.2. Дерево отказов мостика, построенное на основе перечисления сечений.

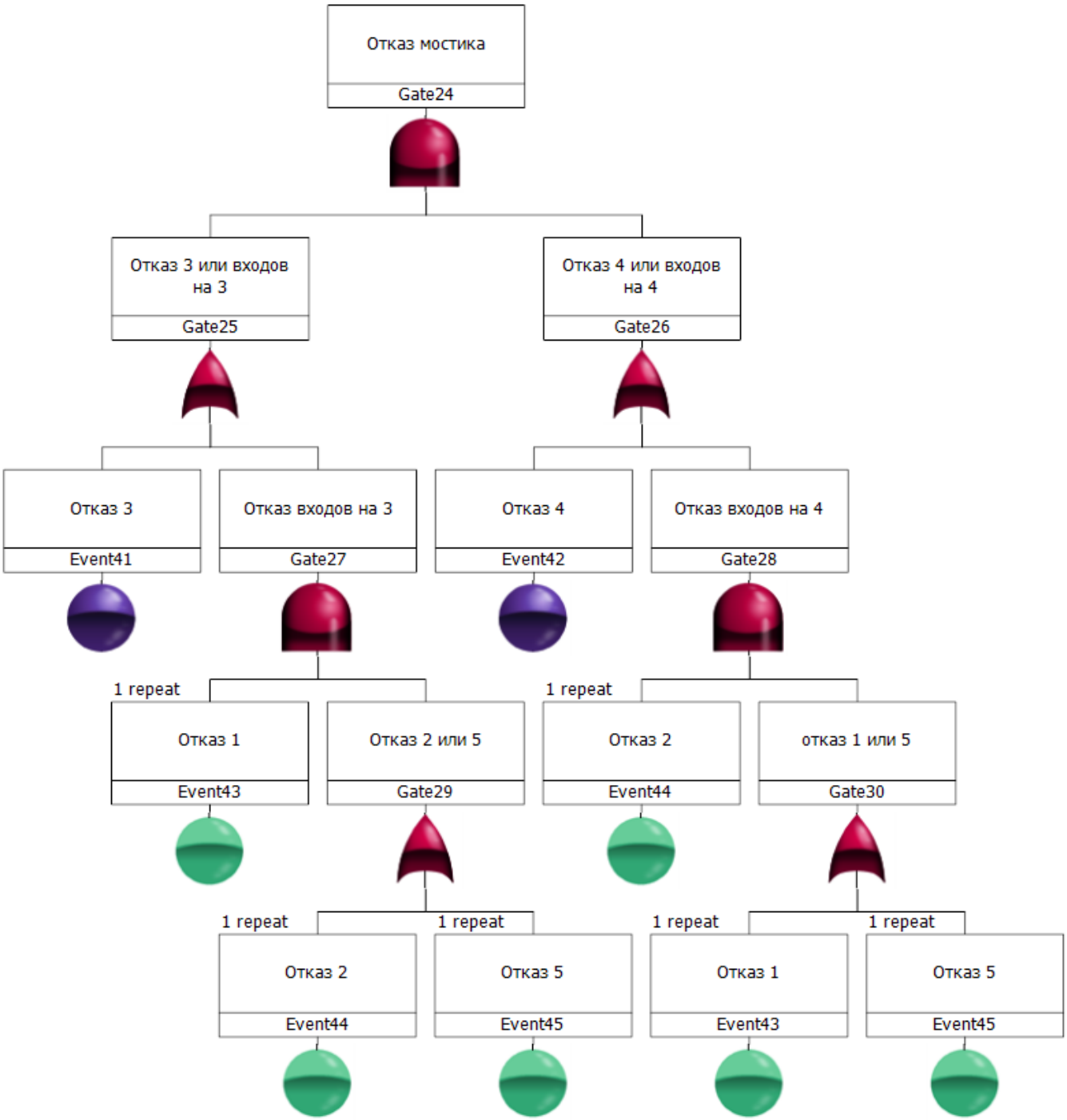


Рис.4.3. Дерево отказов мостика, построенное на основе прохода узлов схемы от выхода к входу.

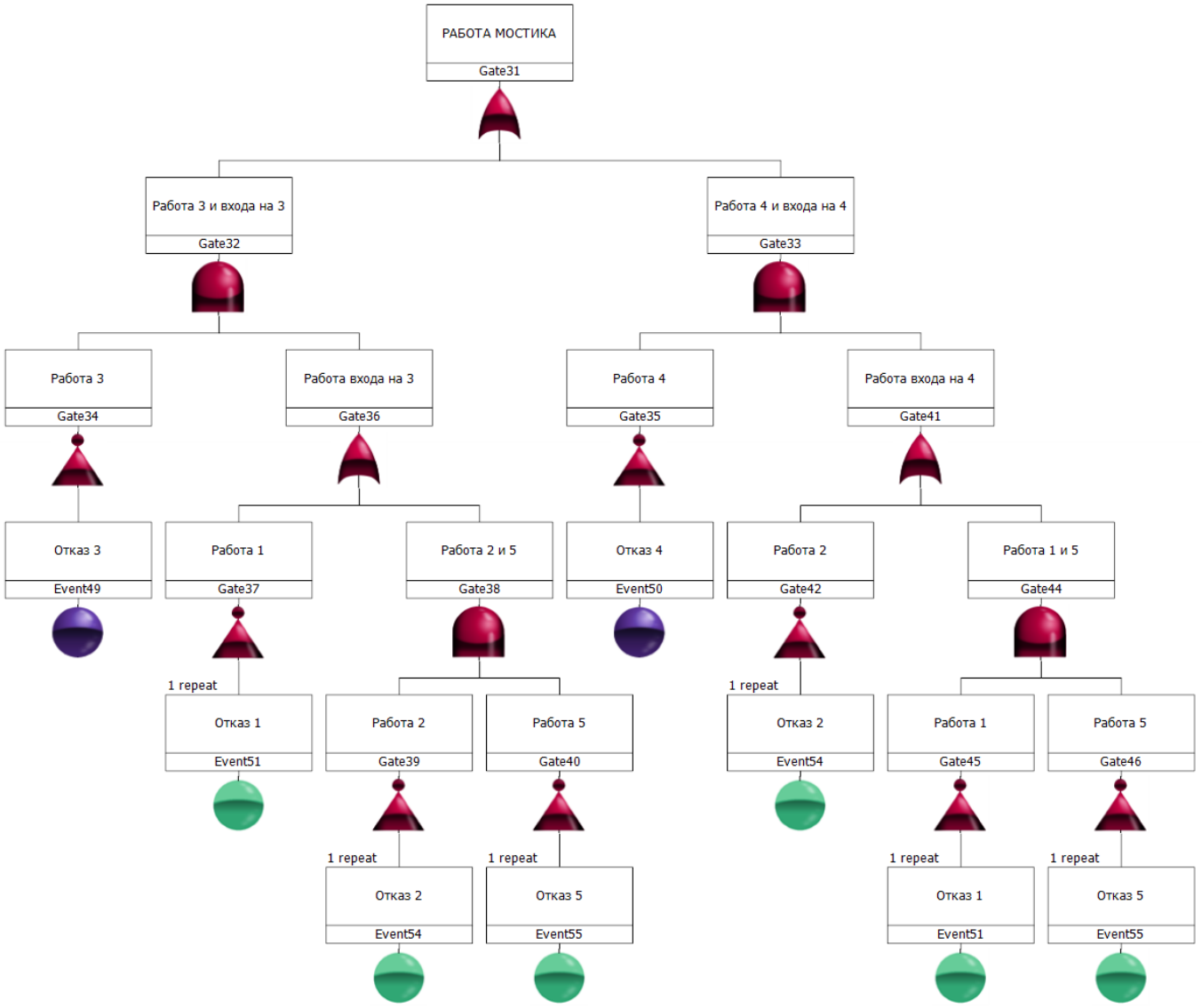


Рис.4.4. Дерево успехов мостика, построенное на основе прохода узлов схемы от выхода к входу

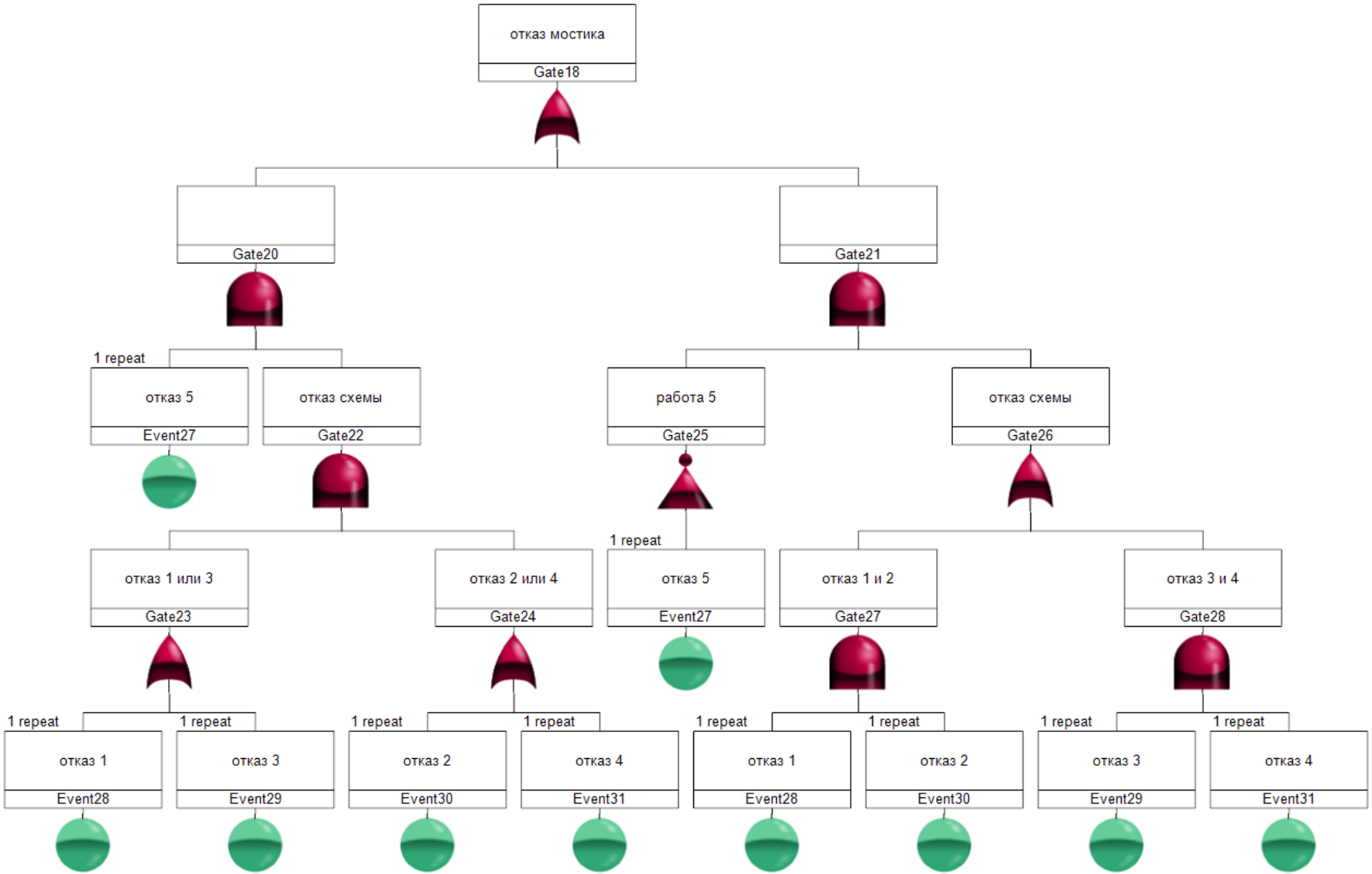


Рис.4.5. Дерево отказов мостика, построенное на основе разложения относительно перемычки (элемент 5).

.

4.3. Формализованное представление логики развития опасных ситуаций в виде деревьев

Деревья отказов являются одной из наиболее распространенных моделей для графического представления причинно-следственных взаимосвязей и проведения качественного и количественного анализа развития ситуаций. Наиболее часто такие задачи возникают при анализе безопасности. В этом случае опасная ситуация соотносится вершинному событию дерева, а базовые события возможным отказам оборудования, неправильным действиям человека, неблагоприятным воздействиям окружающей среды и пр. Рассмотренные в предыдущем разделе подходы к построению деревьев для схем с заданной надежностной структурой применимы и в случаях моделирования логики возникновения опасных ситуаций:

Ситуация 1.Разрыв бака технологической установки

Рассмотрим описанную в [26] технологическую установку, состоящую из бака и насоса, подающего в него жидкость (рис.4.6). Установку включает человек. Имеется два устройства, предотвращающие опасную ситуацию, связанную с переполнением бака: таймер и сирена. Таймер служит для размыкания контактора по истечении определенного интервала времени. Сирена при переполнении бака дает звуковой сигнал человеку на отключение (размыкание выключателя). Разрыв бака может произойти, как из-за отказов элементов бака, так и из-за превышения давления жидкости в баке. Превышение допустимого уровня давления может произойти, если контактор и выключатель надолго замкнуты. Дерево разрыва бака технологической установки показано на рис.4.7. Для описания логики событий, приводящих к разрыву, достаточно вершин И и ИЛИ, поэтому дерево является когерентным (монотонным).

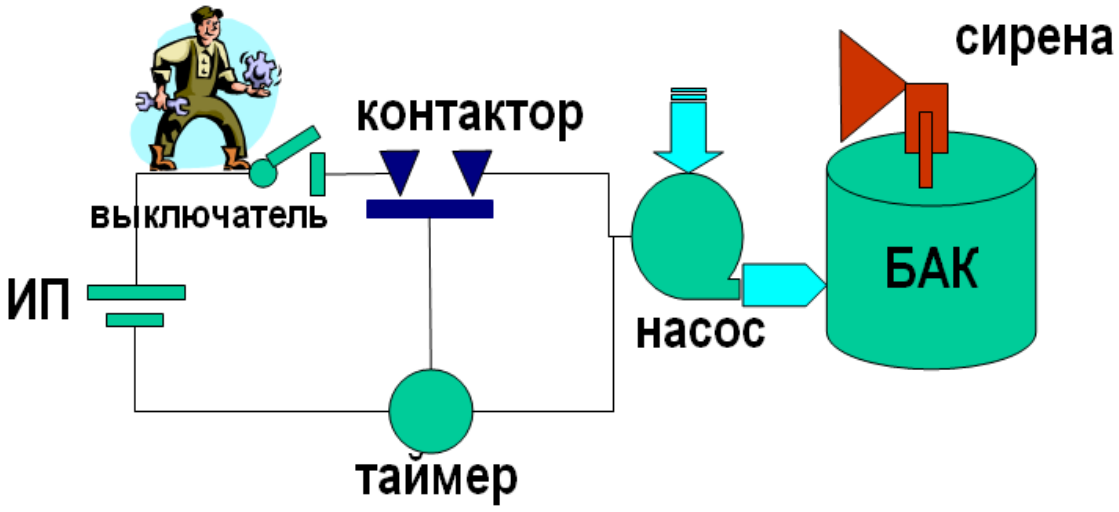


Рис.4.6. Блок технологической установки.

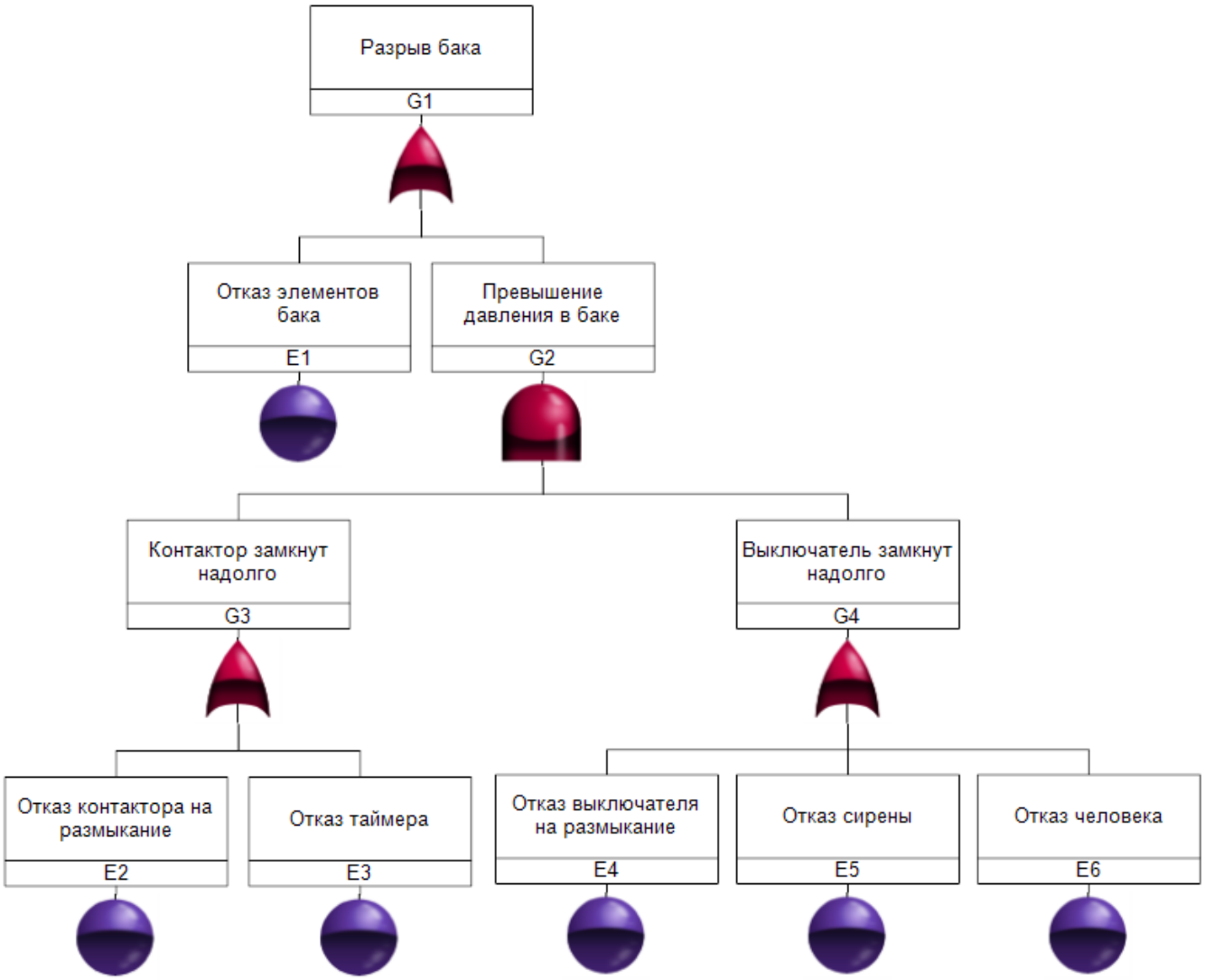


Рис.4.7. Дерево разрыва бака технологической установки

Ситуация 2. Авария на участке железной дороги.

Рассмотрим знаменитый пример, описывающий ситуацию возникновения аварии на железной дороге. Этот пример был предложен А.С. Можаевым в процессе проведения верификации трех программных средств анализа надежности АРБИТР, Relex, Risk Spectrum [30].. Пример демонстрирует возможности этих программ по заданию и исследованию немонотонных логико-вероятностных моделей.

На рис.4.8 приведена функциональная схема участка железной дороги, возможная авария на котором может произойти по причинам – излома рельса и/или возникновение предмета на рельсах. Если произошли события излома рельса и безотказной работы системы индикации излома рельса, то зеленый разрешающий сигнал светофора изменяется на запрещающий красный сигнал. Если

машинист не допустит ошибки и увидит предмет на рельсах и/или красный сигнал светофора, то он включит систему торможения поезда. Тогда, при условии безотказной работы системы торможения, железнодорожная авария будет предотвращена. Немонотонность логико-вероятностной модели возникает по причине того, что нежелательное событие “возникновение предмета на рельсах” приводит к снижению вероятности возникновения аварии при несрабатывании светофора.

Построим дерево отказов, описывающее эту ситуацию. Применим принцип разложения и построим несовместные ветви дерева, соответствующие событиям

- есть излом рельса и предмет на рельсах (в этом случае авария возникает при “отказе” человека или тормозной системы)
- есть излом рельса и нет предмета на рельсах (в этом случае авария возникает при “отказе” человека или тормозной системы или светофора)
- нет излома и есть предмет на рельсах (в этом случае авария возникает при “отказе” человека или тормозной системы).

Дерево аварии участка железной дороги показано на рис.4.9. Полученное дерево оказалось достаточно наглядным, хотя и громоздким. Более компактное представление этой же ситуации представлено на дереве рис.4.10. Оба дерева эквивалентны, но чтобы построить компактное дерево надо обладать достаточным опытом.

Некогерентное дерево успехов, вершинным событием которого является “безопасное состояние участка железной дороги” приведено на рис.4.11.

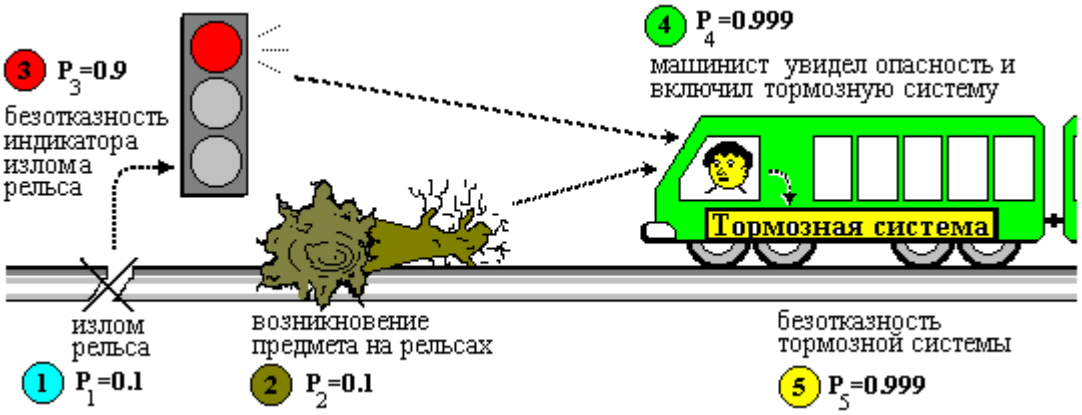


Рис.4.8. Аварийная ситуация на железной дороге.

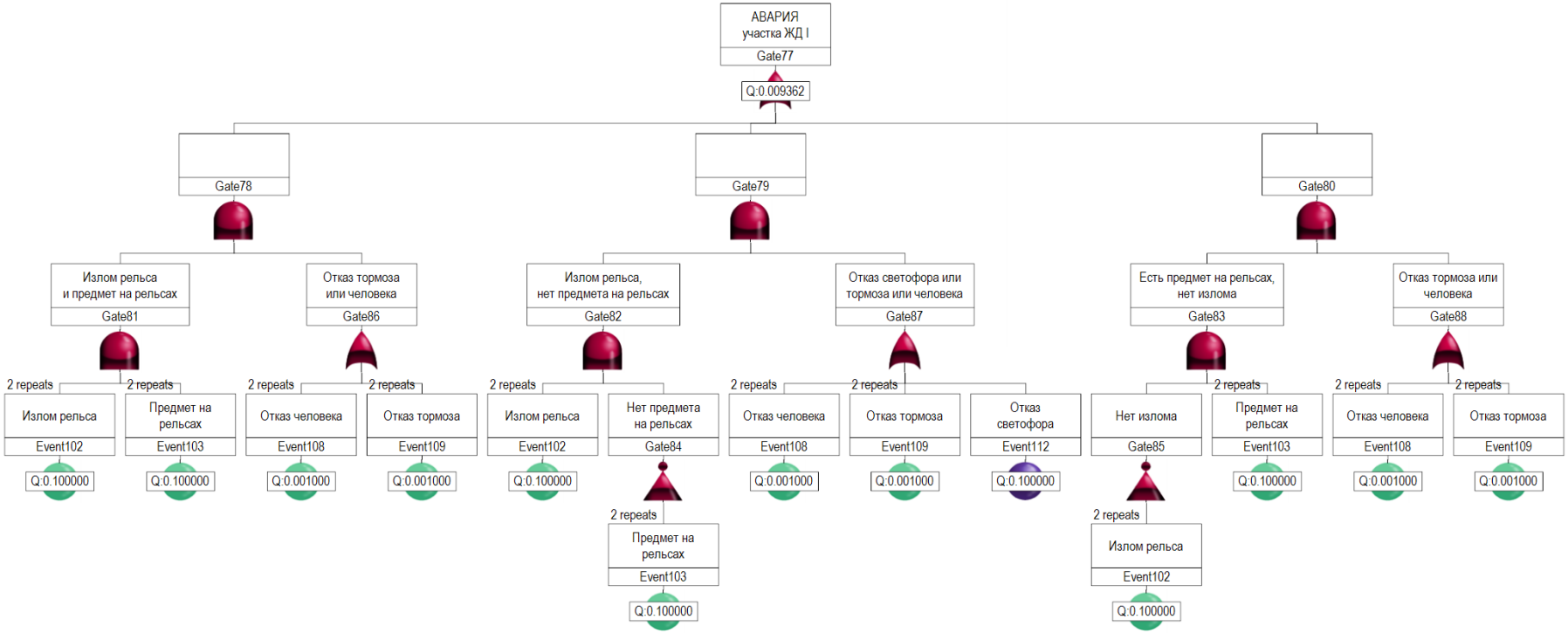


Рис.4.9. Дерево отказов (I) аварийной ситуация на железной дороге.

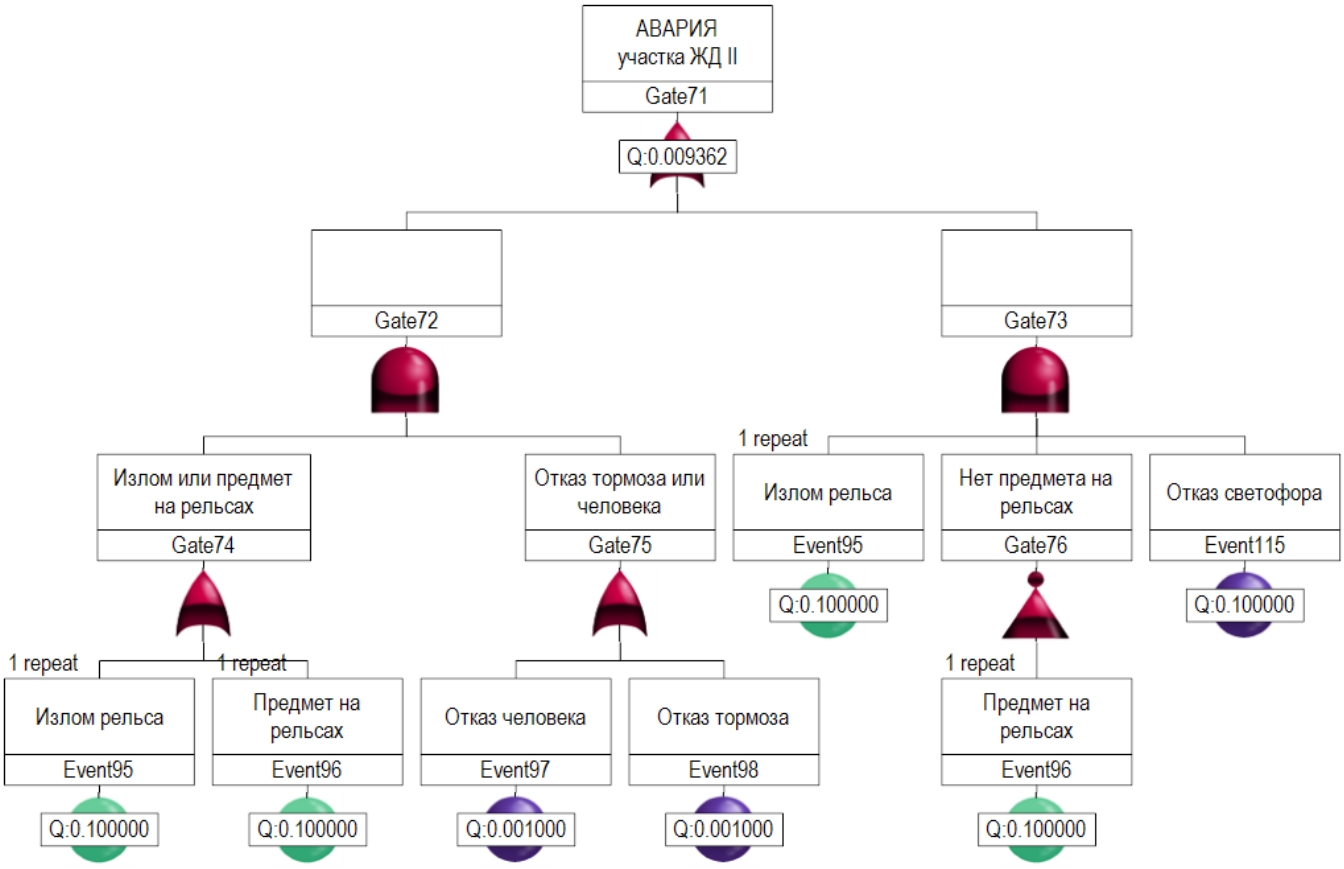


Рис.4.10. Дерево отказов (II) аварийной ситуация на железной дороге.

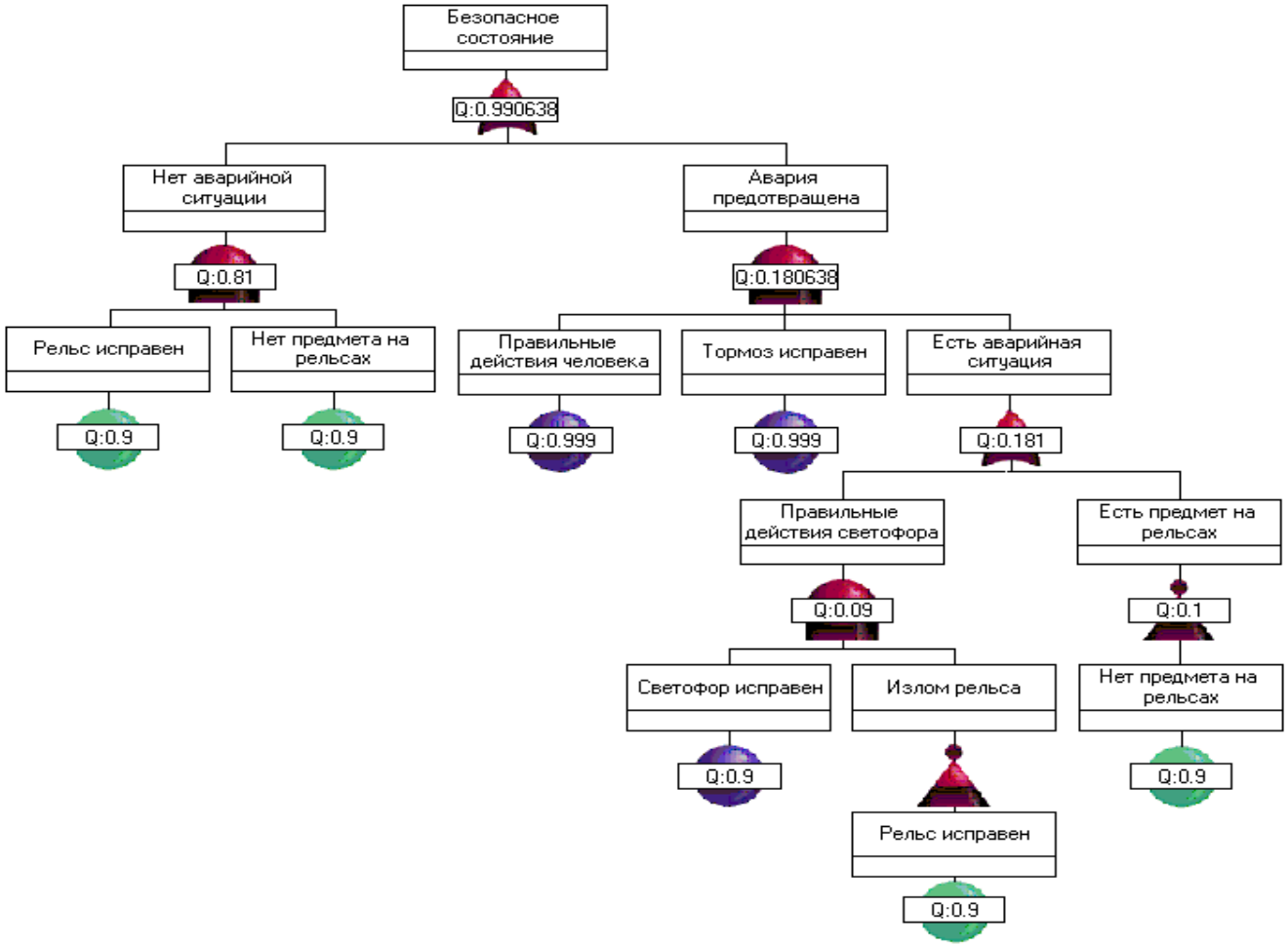


Рис.4.11. Дерево безопасности участка железной дороги

4.4. Деревья отказов, использующие вспомогательные статические вершины

Для облегчения задания логики дерева и более компактного его представления введены две дополнительные статические вершины

- вершина ингибитор (INHIBIT)
- вершина выбора входов по критерию “m из n” (VOTING m:n)

Ингибитор полностью повторяет логику вершины логического И (AND), однако один из входов определен как условие (Conditional Event), запрещающее или разрешающее срабатывание вершины при истинности всех остальных входов. Все входы ингибитора, кроме условия, могут быть как базовыми событиями, так и выходами других логических вершин дерева. Использование ингибитора улучшает читаемость дерева. На рис.4.12 приведено дерево, отображающее логику возникновения пожара при наличии источника воспламенения и горючих материалов. Условное

событие соответствует наличию кислорода в воздухе, без которого невозможен процесс горения. Пример взят из on-line справки программы Windchill Quality Solutions.

Рис.4.12. Дерево отказов с вершиной INHIBIT.

Логика выбора входов по критерию “m из n” может быть достаточно просто реализована с помощью классических вершин И (AND), ИЛИ (OR) и перечисления сечений (путей). Однако чтобы облегчить набор дерева и сделать его более компактным, была введена вершина VOTING m:n. Рассмотрим пример моделирования надежности трехъярусной структуры, показанной на рис.4.13. Отказом структуры является отказ более трех выходов. Дерево работоспособности структуры показано на рис.4.14. Если бы мы не использовали в качестве вершинного события этого дерева VOTING 5:8, то нам необходимо было бы сформировать все 56 путей схемы (C_8^5) и объединить их с помощью вершины ИЛИ (OR). При построении дерева также были использованы вершины-переходники (TRANSFER). Каждая TRANSFER вершина раскрывается вложенным деревом.

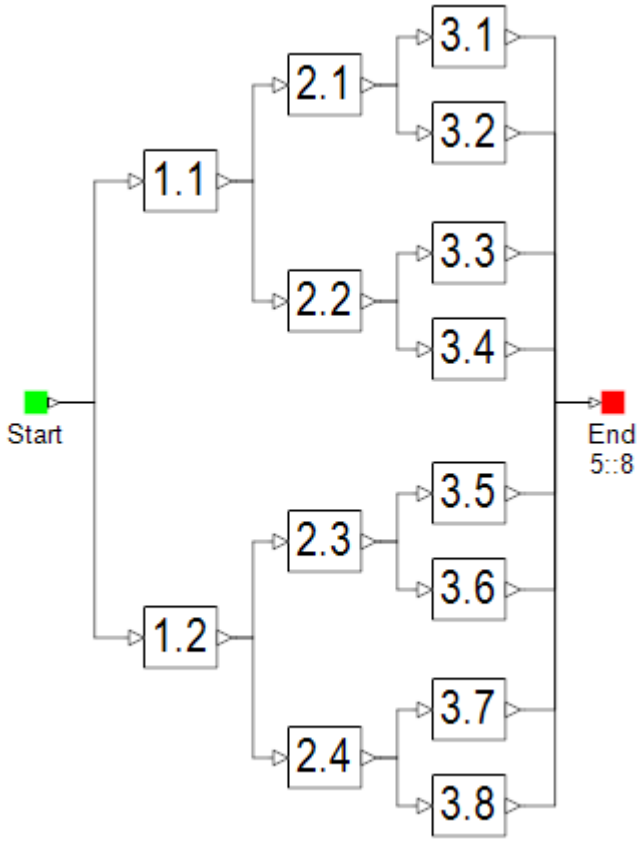


Рис.4.13. Трехъярусная структура с мажорированием выходов.

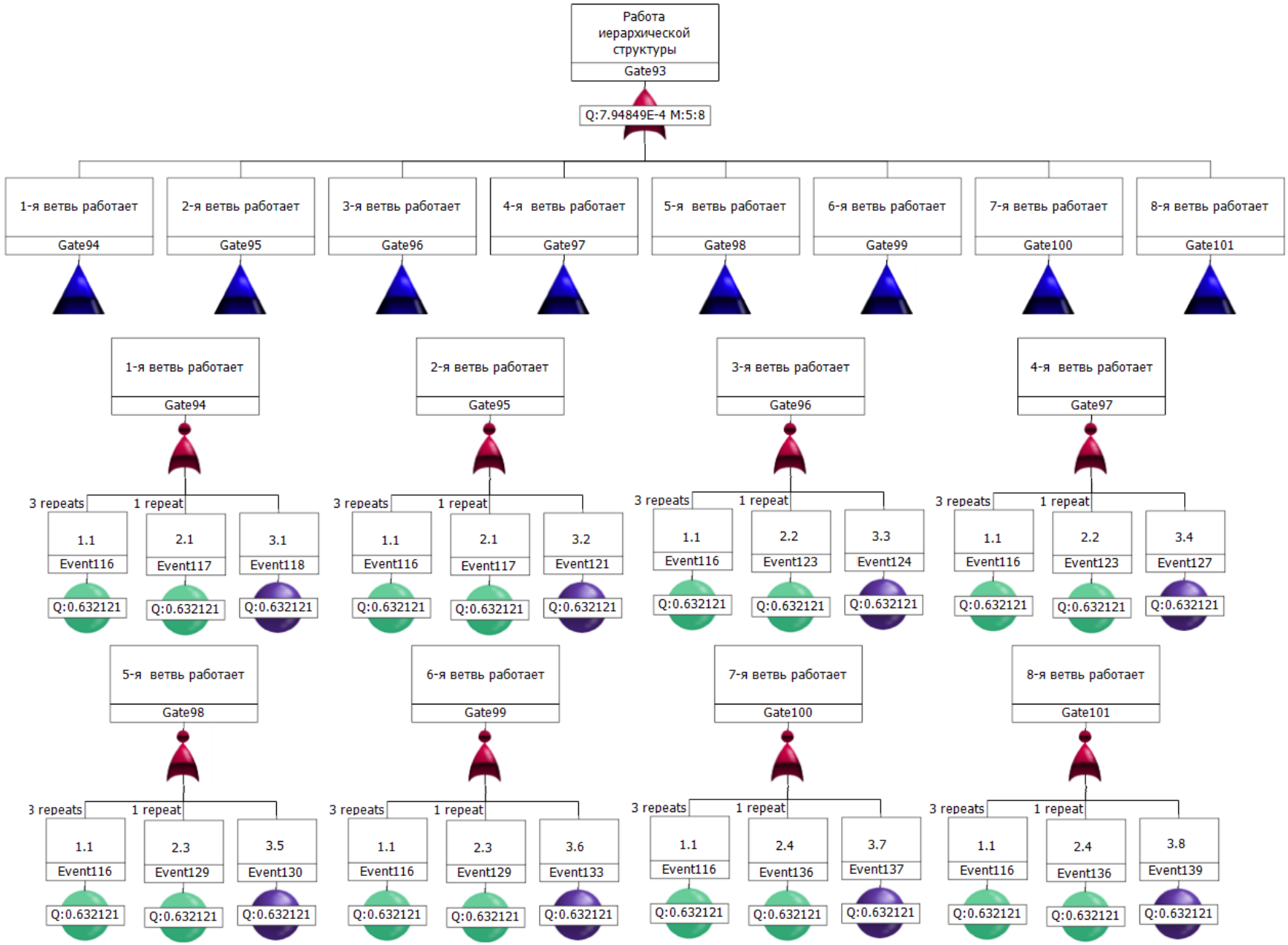


Рис.4.14. Дерево работоспособности трехъярусной структуры с мажорированием выходов

4.5. Качественный анализ деревьев отказов

Качественный анализ состоит в определении наборов минимальных сечений по дереву отказов или минимальных путей по дереву успехов (в дереве успехов базовые события соответствуют работоспособности элементов). Основными алгоритмами нахождения сечений и путей по дереву являются алгоритмы MOCUS [26,27,72] и MICSUP [73]. Алгоритм MOCUS основывается на общепринятом в анализе деревьев отказов подходе “сверху-вниз” (top-down) и учете тех фактов, что гейты OR порождают новые сечения дерева, а гейты AND увеличивают размер сечения (добавляют новые базовые события).

Например, для дерева отказов, показанного на рис.4.15, обозначив гейт i-G_i, базовое событие i –E_i, получаем набор минимальных сечений:

$$G_0 \to G_1 + G_2 \to G_3G_4 + (E_1 + G_5) \to (E_2 + G_6)(E_3E_4) + (E_1 + E_5 + E_6) \to$$
$$(E_2 + E_6 + E_7)(E_3E_4) + E_1 + E_5 + E_6 = E_2E_3E_4 + E_3E_4E_6 + E_3E_4E_7 + E_1 + E_5 + E_6 =$$
$$E_2E_3E_4 + E_3E_4E_7 + E_1 + E_5 + E_6$$

Алгоритм MICSUP основывается на тех же положениях, что и MOCUS, однако проход по дереву осуществляется “снизу-вверх”, (bottom-up), что позволяет строить сечения (пути) не только для вершинного события, но и для промежуточных гейтов. Так, для дерева на рис.4.15 имеем

сечение вершины G6: E_6+E_7

сечение вершины G5: E_5+E_6

сечение вершины G4: E_3E_4

сечение вершины G3: E_2 +G_6 = E_2+E_6+E_7

сечение вершины G2: E_1+G_5=E_1+E_5+E_6

сечение вершины G1: G_3G_4= (E_2+E_6+E_7)E_3E_4

сечение вершинного события G0: G_1+G_2=E_1+E_5+E_6+$E_2E_3E_4$+$E_3E_4E_7$

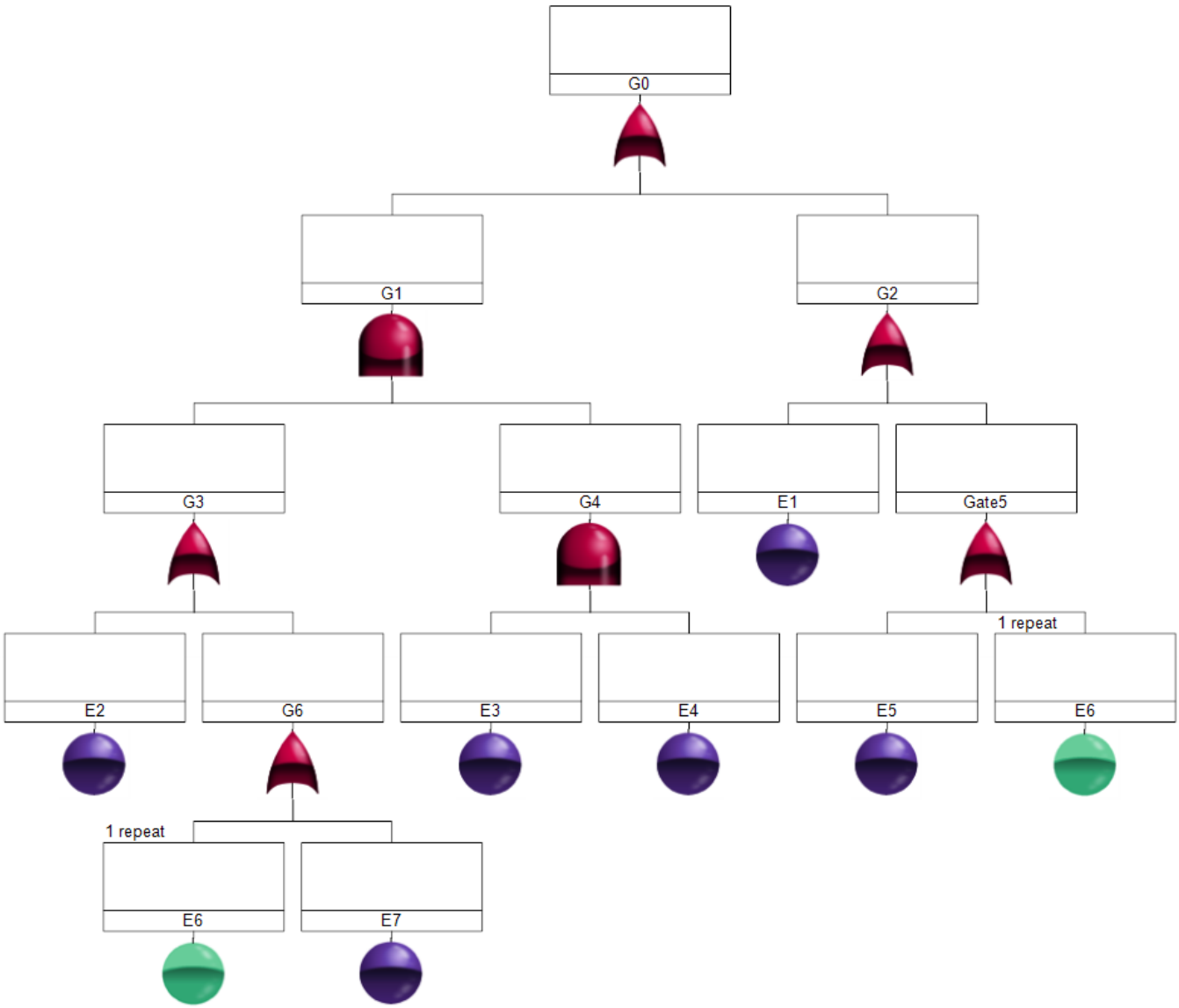


Рис.4.15. Дерево отказов с повторяющимся базовым событием (E6).

4.6. Использование диаграмм двоичных решений для количественного анализа деревьев отказов

Общепринятым, до недавнего времени, подходом к проведению количественного анализа деревьев отказов являлся подход, основанный на теореме сложения вероятностей совместных событий реализации минимальных путей (сечений) (см. формулу 3.10 раздела 3.2). В западной литературе [26,27] этот подход принято называть “принципом включения-исключения”, а выражение (3.10) – “формулой включения-исключения” (cross product). Так как проведение ручных расчетов надежности многоэлементных технических систем на основе принципа включения-исключения крайне затруднительно, то используют

соответствующее программное обеспечение. Программная реализация этого подхода является сложной программисткой задачей, так как требует разработки быстрых алгоритмов генерации наборов минимальных сечений и сложных процедур кодирования выражения 3.10. Новейшей тенденцией в автоматизации анализа деревьев отказов является привлечение современных эффективных методов дискретной математики для представления и манипуляции булевыми функциями, соответствующими деревьям отказов. В качестве искомого представления логики дерева предлагается применять диаграммы двоичных решений[3] (Binary Decision Diagram – BDD) [74]. В терминах BDD логические функции представляются в виде направленного ациклического графа (бинарного дерева), у которого внутренние вершины представляют аргументы функции. Кроме того, выделены два типа терминальных вершин, обозначенные как 0 и 1. Каждая нетерминальная вершина графа v имеет двух потомков left(v) и right(v). Ветви графа упорядочены – проход по левой означает, что аргументу присвоено значение 1, а по правой – значение 0. Присвоение 1 отображается сплошной линией ветви, присвоение 0 – пунктирной. Значение логической функции определяется спуском по дереву от корня к терминальным вершинам. Размерность BDD может быть снижена путем объединения всех единичных и нулевых терминальных вершин в две терминальные вершины 1 и 0. Дальнейшая редукция BDD связана с объединением нетерминальных вершин, соответствующих одинаковым аргументам и имеющих одинаковых потомков. Вершины, у которых left(v) = right(v), могут быть удалены. На рис.4.16 приведена мажоритарная схема с функцией работоспособности $S(x) = x_1x_2+x_1x_3+x_2x_3$, представленной в виде двух эквивалентных BDD. Первая диаграмм повторяет таблицу истинности. Вторая получена из первой путем удаления крайних нетерминальных вершин x_3 и объединения двух внутренних вершин x_3 в одну.

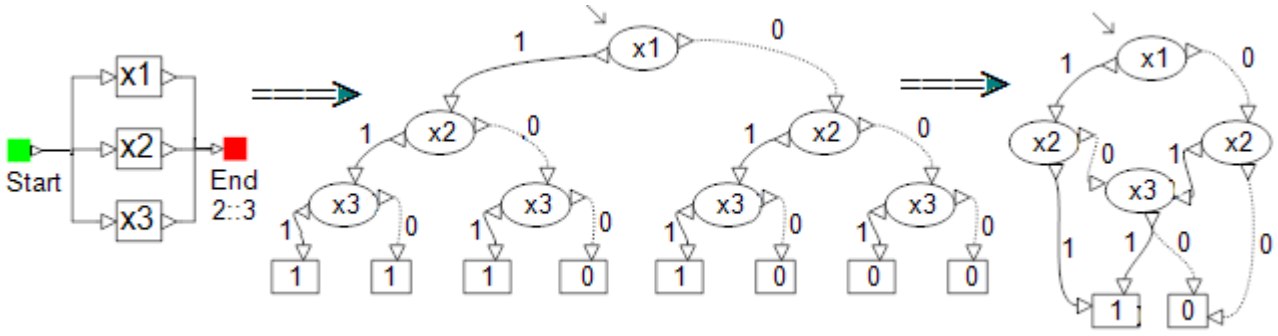


Рис.4.16. Диаграммы двоичных решений мажоритарной логики “2 из 3”.

[3] Также применяют термины двоичные разрешающие диаграммы, бинарные диаграммы решений.

При автоматизации анализа надежности важными преимуществом диаграмм двоичных решений являются

- представление логических функций в формах перехода к замещению, допускающих замещение логических переменных вероятностями, а логических операций арифметическими. Это достигается за счет того, что сам принцип построения BDD, подобно алгоритму разрезания (см. раздел 3.2) , обеспечивает разложение логической функции на ортогональные слагаемые.
- при машинной реализации BDD воплощается нелинейной динамической структурой данных – двоичным деревом, для которого разработаны эффективные алгоритмы обхода узлов, сложность которых зависит от количества уровней дерева, т.е. приблизительно от $\log_2 n$ (n – количество узлов).

Недостатком BDD является то, что размерность порождаемых диаграмм сильно зависит от предварительного этапа упорядочения аргументов, который в настоящее время недостаточно формализован.

Для того чтобы сохранить в качестве входного описания деревья отказов, а вычисления реализовывать на BDD, разработаны соответствующие алгоритмы преобразования деревьев в диаграммы двоичных решений [75-80]. Эти алгоритмы используют разложение логической функции f по аргументу x_i: $f = (x_i \wedge f_{xi=1}) \vee (x_0 \wedge f_{xi=0})$, иногда называемое разложением Шеннона. Разложение Шеннона описывают нотацией $ITE(x_i,f_1,f_0)$, где ITE есть сокращение от IF THEN ELSE.

Рассмотрим одну из возможных реализаций алгоритма преобразования.

- упорядочить базовые события дерева: $x_1<x_2<\ldots x_n$
- каждому базовому событию дерева соотнести нотацию $ITE(x_i,1,0)$
- для каждой вершины дерева сформировать нотацию ее логической функции $ITE(x_i,F_1,F_0)$, руководствуясь следующими правилами:

$$\text{ë}\begin{cases}\text{если } (x_i < x_j) \Rightarrow ITE(x_i, g_1 * H, g_0 * H)\\ \text{если } (x_i == x_j) \Rightarrow ITE(x_i, g_1 * h_1, g_0 * h_0)\end{cases}, \quad \text{где} \quad G = ITE(x, g_1, g_0); \quad H = ITE(y, h_1, h_0); \tag{4.1}$$

  * - логический оператор вершины дерева (OR или AND); G,H – логические функции ее входных вершин.
- последовательно применяя правила (4.1) для каждой вершины, получить ITE нотацию вершинного события дерева отказов

$$TOP = ITE(\underbrace{x_i}_{\text{корень}}, \underbrace{(x_j, g_1, g_0)}_{\text{ветвь при } x_i==1}, \underbrace{(x_k, h_1, h_0)}_{\text{ветвь при } x_i==0}) \quad (4.2)$$

- последовательно раскрывая “единичные” и “нулевые” составляющие выражения (4.2), сформировать двоичное дерево
- пройдя все пути двоичного дерева, ведущие от корня до терминальной вершины “1”, получить выражение для логической функции реализации вершинного события дерева отказов в дизъюнктивной ортогональной форме: $f = Y_1 \vee Y_2 \vee \ldots \vee Ym$, где $Y_i \wedge Y_j = 0$ для $i \neq j$; Y_i - бесповторная форма в базисе конъюнкция-отрицание.
- учитывая, что полученная форма логической функции является формой перехода к замещению, вычислить вероятность реализации вершинного события исходного дерева отказов непосредственной заменой логических переменных соответствующими вероятностями, а логических операций арифметическими

Рассмотрим пример преобразования дерева отказов с повторяющимися элементами (рис.4.17) в диаграмму двоичных решений:

1. Упорядочим элементы: $x_1<x_2<x_3<x_4$ и запишем $ITE(x_i,1,0)$ $(i=1\div4)$
2. Определим операторы G_i для каждой логической вершины, включая вершинное событие:

$$G_1 = x_2 + x_3 = ITE(x_2,1,0) + ITE(x_3,1,0) = ITE(x_2,1,ITE(x_3,1,0))$$
$$G_2 = x_2 + x_4 = ITE(x_2,1,0) + ITE(x_4,1,0) = ITE(x_2,1,ITE(x_4,1,0))$$

$$G_3 = G_1 \cdot G_2 = ITE(x_2,1,ITE(x_3,1,0)) \cdot ITE(x_2,1,ITE(x_4,1,0)) = ITE(x_2,1,ITE(x_3,ITE(x_4,1,0),0))$$
$$TOP = x_1 + G_3 = ITE(x_1,1,0) + ITE(x_2,1,ITE(x_3,ITE(x_4,1,0),0)) =$$
$$ITE(\underbrace{x_1}_{\text{корень}}, \underbrace{1}_{1}, \underbrace{ITE(x_2,\underbrace{1}_{1},\underbrace{ITE(x_3,ITE(x_4,1,0),0)}_{0})}_{0})$$

3. Диаграмма двоичных решений, построенная в соответствии с выражением для вершинного события (TOP), показана на рис.4.18
4. По полученной BDD запишем логическую функцию отказа для двухканальной схемы, как объединение путей, приводящих к единичным терминальным вершинам:

$x_1 + \bar{x}_1 x_2 + \bar{x}_1 \bar{x}_2 x_3 x_4$. Ортогональность полученной формы записи позволяет

подстановкой соответствующих вероятностей определить формулу для вероятности отказа системы: $q_1 + p_1q_2 + p_1p_2q_3q_4$.

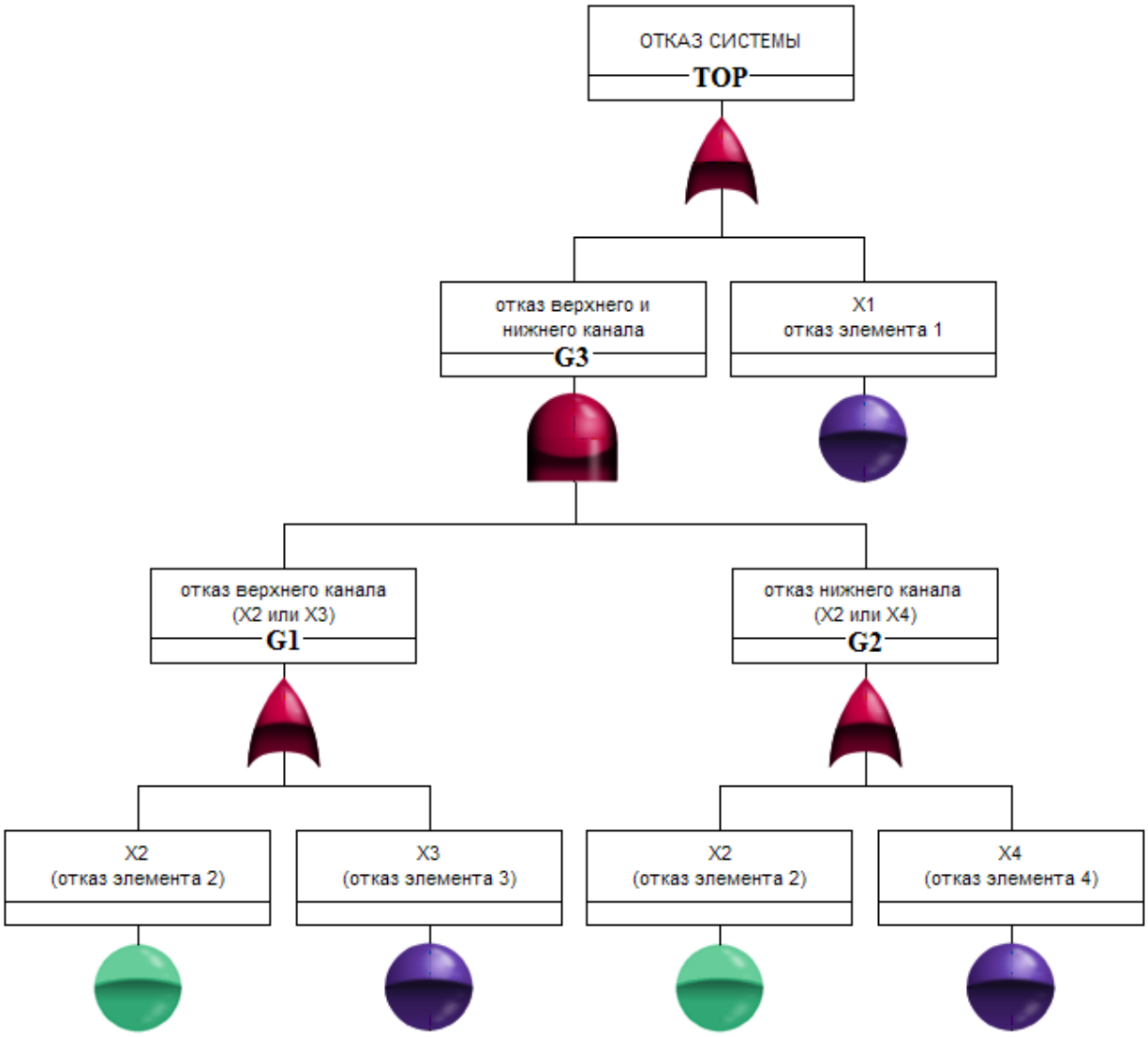


Рис.4.17. Дерево отказов двухканальной системы с повторяющимися элементами

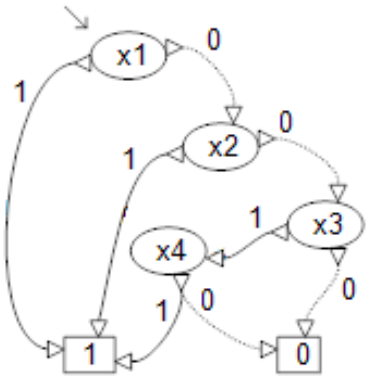


Рис.4.18. Диаграмма двоичных решений отказа двухканальной системы.

Применение диаграмм двоичных решений не ограничивается деревьями отказов/успехов. BDD могут использоваться при любом способе визуализации логико-вероятностных моделей, в частности, в блок-схемах надежности. Вернемся к рассмотрению блок-схемы надежности мостиковой структуры (рис.3.1) и преобразуем ее логическую функцию работоспособности $S(x)=x_1x_3+x_2x_4+x_1x_4x_5+x_2x_3x_5$ в формат BDD:

1. Упорядочим элементы: $x_1<x_2<x_3<x_4<x_5$ и запишем $ITE(x_i,1,0)$ $(i=1\div5)$
2. Запишем логические функции реализации минимальных путей мостика в ITE нотации:

$$x_1x_3 \Rightarrow G_1 = ITE(x_1, ITE(x_3,1,0),0);$$
$$x_2x_4 \Rightarrow G_2 = ITE(x_2, ITE(x_4,1,0),0);$$
$$x_1x_4x_5 \Rightarrow G_3 = ITE(x_1, ITE(x_4, ITE(x_5,1,0),0),0);$$
$$x_2x_3x_5 \Rightarrow G_4 = ITE(x_2, ITE(x_3, ITE(x_5,1,0),0),0);$$

3. Запишем логические функции объединения минимальных путей мостика в ITE нотации:

$$H_1 = G_1 + G_3 = ITE(x_1, S_1, 0),$$
$$\text{где } S_1 = ITE(x_3,1, ITE(x_4, ITE(x_5,1,0),0));$$
$$H_2 = G_2 + G_4 = ITE(x_2, S_2, 0),$$
$$\text{где } S_2 = ITE(x_4,1, ITE(x_3, ITE(x_5,1,0),0));$$
$$S = H_1 + H_2 = ITE(x_1, S_3, ITE(x_2, S_2, 0)),$$
$$\text{где } S_3 = S_1 + ITE(x_2, S_2, 0) = ITE(x_3,1, ITE(x_4, ITE(x_5,1, ITE(x_2,1,0)),0));$$

4. По полученному выражению для S построим диаграмму двоичных решений (рис.4.19)
5. По BDD (рис.4.19) выпишем выражение для показателя вероятности безотказной работы мостика:

$$P = p_1(p_3 + q_3p_4(p_5 + q_5p_2)) + q_1p_2(p_4 + q_4p_3p_5). \qquad (4.3)$$

Возможность автоматической генерации расчетных формул показателей надежности является еще одним преимуществом диаграмм двоичных решений. Так, например, Windchill Quality Solutions, использующий BDD в логико-вероятностных модулях (RBD, FT), может выводить аналитические выражения показателя вероятности безотказной работы невосстанавливаемых систем. На рис.4.20 приведена распечатка экрана выдачи результатов расчета модуля RBD. Полученная формула аналогична выражению (4.3).

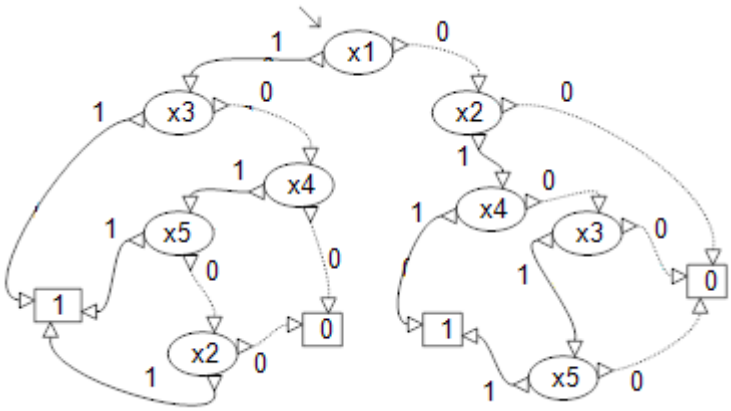


Рис.4.19. Диаграмма двоичных решений работоспособности мостика.

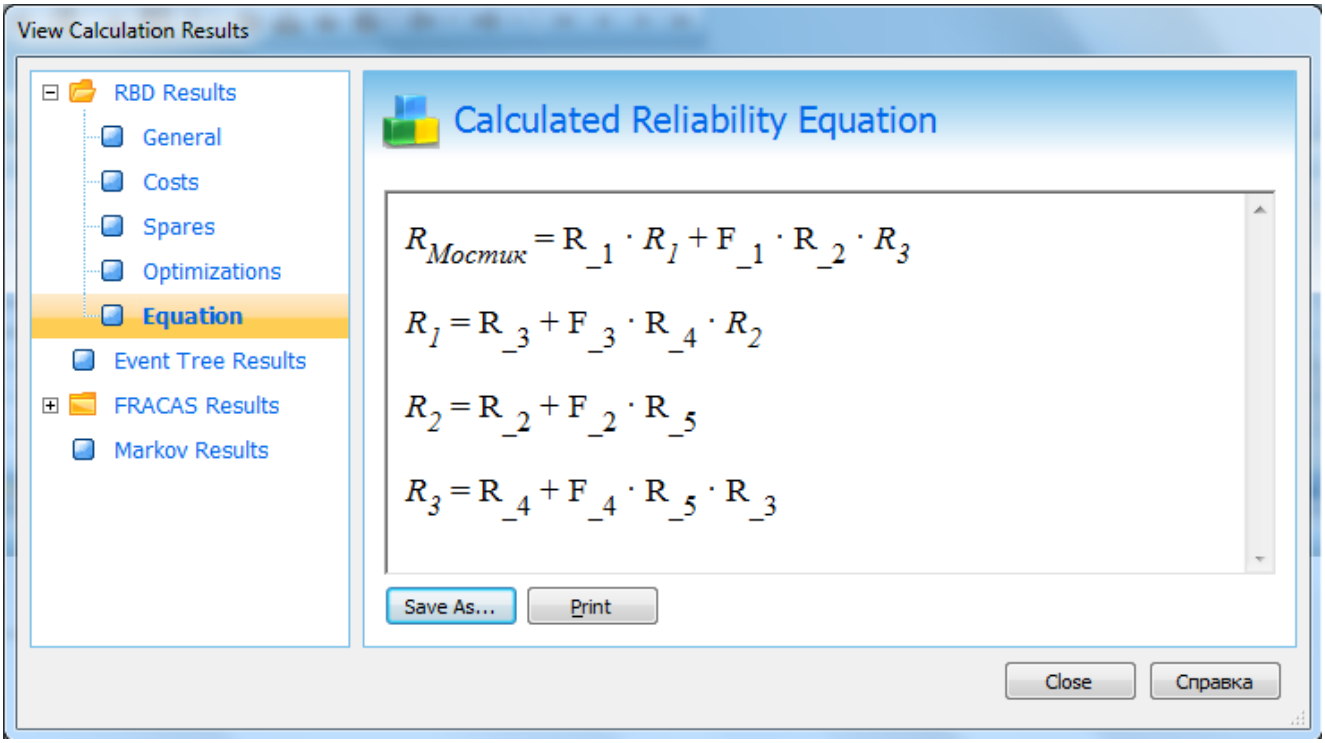


Рис.4.20. Распечатка экрана выдачи результатов расчета модуля блок-схем надежности Windchill Quality Solutions (R_i (F_i) – вероятности безотказной работы (отказа) i-го элемента).

4.7. Анализ отказов по общей причине

Для учета кратных отказов в группе идентичных элементов были разработаны специальные модели, получившие название модели отказов по общей причине (Common Cause Failures -CCF). Толчком к разработке этих моделей послужила статистика отказов, подтверждающая ненулевую вероятность одновременного отказа нескольких однотипных элементов системы [81]. Причинами появления кратных неисправностей являются

- ошибки проектирования и конструирования
- нарушение технологии изготовления и сборки
- ошибки при техническом обслуживании и регулировке
- неблагоприятные воздействия окружающей среды

Вычисления с учетом общих причин отказов состоят из двух составляющих:

1. вычисление вероятностных характеристик кратных отказов элементов
2. включение в общесистемную модель надежности вычисленных вероятностных характеристик кратных отказов.

1. *Модели расчета вероятностных характеристик кратных отказов*

Наиболее распространенными и реализованными почти во всех зарубежных программных продуктах анализа деревьев отказов являются модели вычисления вероятностных характеристик кратных отказов, известные под названиями модели β фактора (Beta-Factor Model), α фактора (Alpha-Factor Model), множественных греческих букв (Multiple Greek Letter Model), биномиальной (Binomial Failure Rate Model) [82,83].

Все расчетные соотношения CCF моделей достаточно просты и базируются на комбинаторных методах [84]. Простота моделей связана с введением в них ограничения на равную вероятность отказов всех m элементов CCF группы, что вполне корректно при рассмотрении схем постоянного резервирования. Суммарная вероятность отказа элемента Q_t учитывает как независимые одиночные отказы, так и k-кратные отказы (k=2÷m), происходящие одновременно с другими k-1 элементами CCF группы:

$$Q_t = \sum_{k=1}^{m} C_{m-1}^{k-1} Q_k \ . \qquad (4.4)$$

Предполагается, что кратность отказов элементов в группе обуславливается только общей причиной.

Бета-Факторная Модель (Beta-Factor Model - BFM)

Это простейшая однопараметрическая модель, в которой предполагается, что механизм воздействия общей причины таков, что одновременно отказывают все m элементов CCF группы. Единственный параметр модели β - доля кратных неисправностей, обусловленных появлением общей причины. Тогда вероятность возникновения одновременного отказа k элементов (Q_k) вычисляется как

$$Q_k = \begin{cases} (1-\beta)Q_t, & k = 1 \\ 0, & 1 < k < m \\ \beta Q_t, & k = m \end{cases} \qquad (4.5)$$

Модель Множественных Греческих Букв (Multiple Greek Letter -MGL)

Для учета отказов выделенного элемента, как одиночного, так и кратных совместно с другими элементами CCF группы была разработана MGL модель. Эта модель предполагает произвольную кратность k отказов по общей причине:

$$Q_k = C_{m-1}^{k-1}\left(\prod_{i=1}^{k}\rho_i\right)(1-\rho_{k+1})Q_t \quad (k = 1,\ldots,m), \qquad (4.6)$$

где $\rho_1=1$, $\rho_2=\beta$, $\rho_3=\gamma$, $\rho_4=\delta$, … , $\rho_{m+1}=0$;

ρ_i (i = 2÷k)- условная вероятность того, что произойдет отказ выделенного элемента либо одиночный, либо в группе с другими элементами (кратности ≥ i), при условии, что произошел отказ кратности ≥ i-1.

Поясним сказанное на примере группы из четырех идентичных элементов (m=4), на которые воздействует общая причина таким образом, что может вызвать двукратные (k=2), трехкратные (k=3) и четырехкратные (k=4) отказы. Общая вероятность отказа элемента группы, включая независимый одиночный отказ, будет $Q_t = Q_1 + 3Q_2 + 3Q_3 + Q_4$, а параметры модели вычисляются как

$$\beta = \frac{3Q_2 + 3Q_3 + Q_4}{Q_1 + 3Q_2 + 3Q_3 + Q_4}$$
$$\gamma = \frac{3Q_3 + Q_4}{3Q_2 + 3Q_3 + Q_4} \qquad (4.7)$$
$$\delta = \frac{Q_4}{3Q_3 + Q_4}$$

Тогда вероятность к-кратного отказа в группе из четырех элементов через параметры MGL модели, которые получены путем обработки статистического материала, определяется следующим образом:

$$
\begin{aligned}
Q_1 &= (1-\beta)Q_t \\
Q_2 &= \frac{\beta(1-\gamma)Q_t}{3} \\
Q_3 &= \frac{\beta\gamma(1-\delta)Q_t}{3} \\
Q_4 &= \beta\gamma\delta Q_t
\end{aligned}
\tag{4.8}
$$

Альфа-Факторная Модель (Alpha-Factor Model – AFM)

Параметры рассмотренных выше моделей должны быть получены из анализа статистики отказов элементов группы. Организация таких испытаний и наблюдений является чрезвычайно сложной задачей, что показано в [82]. Осуществление многопараметрического статистического анализа отказов по системе в целом (в отличие от наблюдений за одним элементом) облегчает задачу и позволяет более строго обосновать параметры CCF модели. В связи с этим была разработана модель отказов по общей причине, основанная на статистике отказов системного уровня, получившая название альфа-факторной модели. Параметрами этой модели являются коэффициенты α_k, определяемые как отношение вероятности отказа кратности k к суммарной вероятности отказа в группе из m элементов:

$$
\alpha_k = \frac{C_m^k Q_k}{\sum_{k=1}^{m} C_m^k Q_k} \quad . \tag{4.9}
$$

Значение параметров α_k для CCF группы из трех элементов определяются как

$$
\begin{aligned}
\alpha_1 &= \frac{3Q_1}{3Q_1 + 3Q_2 + Q_3}, \\
\alpha_2 &= \frac{3Q_2}{3Q_1 + 3Q_2 + Q_3}, \\
\alpha_3 &= \frac{Q_3}{3Q_1 + 3Q_2 + Q_3}.
\end{aligned}
\tag{4.10}
$$

Из (4.4) и (4.9) можно вывести формулу для вычисления вероятностей Q_k, как функции параметров α_k и суммарной вероятности отказа элемента Q_t

$$
Q_k = \frac{m\alpha_k}{C_m^k \alpha_t} Q_t , \tag{4.11}
$$

где $\alpha_t = \sum_{k=1}^{m} k\alpha_k$.

Очевидна взаимосвязь параметров MGL и альфа-факторной модели. Например, для m=3 имеем

$$\beta = \frac{2\alpha_2 + 3\alpha_3}{\alpha_1 + 2\alpha_2 + 3\alpha_3},$$
$$\gamma = \frac{3\alpha_3}{2\alpha_2 + 3\alpha_3}. \qquad (4.12)$$

Биномиальная Модель (Binomial Failure Rate Model - BFR)

BFR модель построена при предположении о том, что причиной кратных неисправностей являются внешние шоковые воздействия (ударные нагрузки, сотрясения…). Шок, воздействующий на систему, может быть летальный и нелетальный. При летальных воздействиях с вероятностью равной единице поражаются и отказывают все m элементов системы. При нелетальном шоковом воздействии могут возникать отказы элементов системы произвольной кратности. Кроме того, в BFR, как и в предыдущих моделях, учитывается возможность возникновения независимых одиночных отказов элементов. Таким образом, вероятность того, что в группе из m элементов возникнет одновременный отказ k элементов Q_k, определяется как

$$Q_k = \begin{cases} Q_1 + \mu\rho(1-\rho)^{m-1} & \text{при } k = 1 \\ \mu\rho^k(1-\rho)^{m-k} & \text{при } 1 < k < m \\ \omega + \mu\rho^m & \text{при } k = m \end{cases}. \qquad (4.13)$$

Параметры BFR модели в литературе часто называют по-разному – интенсивностью, частотой, долей, вероятностью. На самом деле все эти параметры получают из анализа статистического материала (наблюдений, испытаний) и определяют как отношение некоторого числа интересующих исходов к общему числу исходов, то есть, по существу, все они являются точечными оценками вероятностей соответствующих событий. Поэтому мы будем называть эти параметры вероятностями. Итак

Q_1 – вероятность возникновения одиночного независимого отказа отдельного элемента;

μ - вероятность возникновения нелетального шока;

ρ - условная вероятность отказа элемента при условии, что произошел нелетельный шок;

ω - вероятность возникновения летального шока.

2. *Включение в общесистемную модель надежности вероятностных характеристик кратных отказов.*

Включение в общесистемную модель кратных отказов для всех методов вычисления характеристик кратных отказов (BFM, AFM, MGL, BFR) делается одинаково. В обычной модели системы (без учета кратных отказов) каждый элемент, базисное событие из группы с

общей причиной отсоединяется от логического оператора, к которому он подключен. Вместо него в это место вставляется логический оператор ИЛИ, на вход которого включается сам этот элемент (с вычисленной характеристикой однократного отказа) и все возможные комбинации (двукратные отказы, трехкратные отказы …) неработоспособности этого элемента. Например, если группа из трех элементов A, B, C (рис.4.21) может отказывать по общей причине, причем возможны и двукратные отказы, и трехкратные, то каждый один элемент будет подключаться к ИЛИ как показано на рис.4.22.

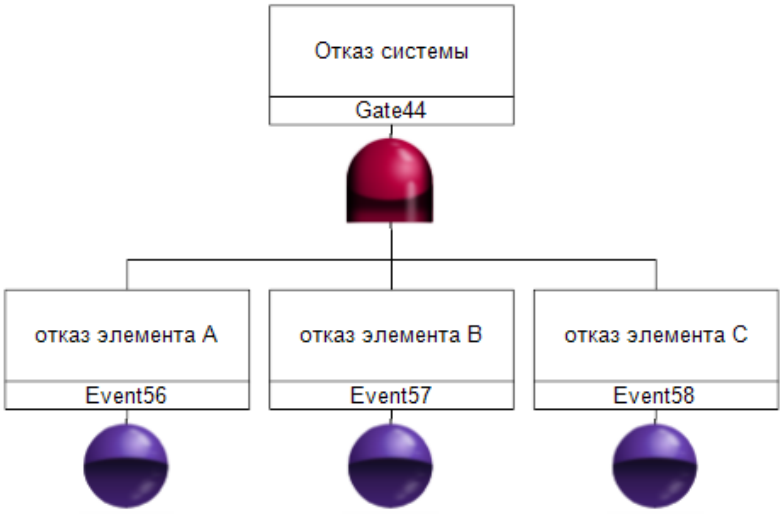


Рис.4.21. Дерево отказов резервированной схемы “1 из 3” без учета отказов по общей причине

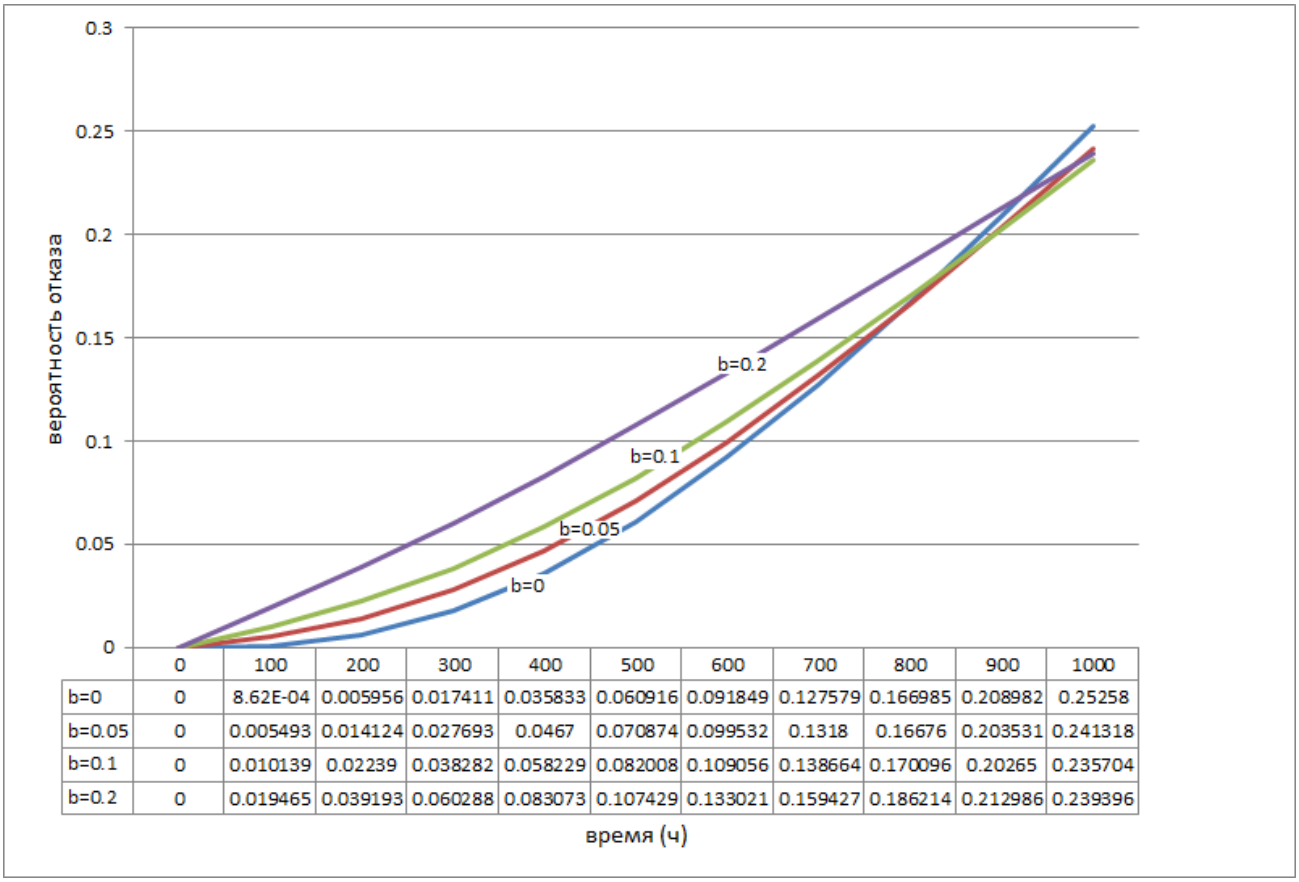
В заключении сделаем следующие критические замечания по поводу рассмотренной методологии учета отказов по общей причине:

– основным при вычислении *вероятностных характеристик кратных отказов* является не рассмотрение моделей внешних воздействий и реакций на это элементов структуры, а вычисления, «вырезающие» из статистической оценки вероятностной характеристики отказа элемента (вероятности отказа, интенсивности отказа) составляющих, которые определяют кратные отказы. В результате такого «вырезания» вероятность независимого однократного отказа элемента уменьшается, что может приводить к некоторым неожиданным результатам, когда учет общих причин приводит к уменьшению вероятности отказа системы. Статистическое обоснование такого подхода основывается на том, что в статистическую ненадёжность элемента при обработке могут также быть включены и кратные отказы (одновременный отказ

нескольких элементов). Различия в перечисленных выше моделях и состоит, именно, в методах вычисления кратного отказа.

- включение в общую модель происходит с серьезными недостатками, что также вносит дополнительные погрешности. Эти недостатки обуславливаются тем, что базовое событие, соответствующее одиночному отказу элемента, заменяется гейтом ИЛИ, входными базовыми событиями которого являются одиночный отказ и все комбинации кратных отказов, содержащих данный элемент. Вероятности возникновения этих входных базовых событий рассчитываются по соотношениям (4.5, 4.6, 4.11, 4.13), выведенным, исходя из предположения о несовместности отказов различной кратности. Несовместность событий предполагает их зависимость, в то время как все логико-вероятностные методы и, в частности, деревья отказов “работают” только при условии независимости событий отказов.

Все в совокупности, как вычисления, уменьшающие вероятность однократного отказа, так и некорректное включение в общее дерево, порождает трудно объяснимые явления, например, когда резервированная система “1 из 3”, в которой могут возникать только одиночные отказы, оказывается менее надежной, чем та же система, в которой могут возникать как одиночные отказы, так и отказы по общей причине различной кратности (см. график рис.4.23). Вычисления вероятности отказа системы с учетом кратных отказов по общей причине были проведены на бета-факторной модели. Семейство кривых вероятности отказа построено при значениях параметра β =0, 0.05, 0.1, 0.2. Интенсивность отказов отдельного элемента λ=0.001 1/ч..



	0	100	200	300	400	500	600	700	800	900	1000
b=0	0	8.62E-04	0.005956	0.017411	0.035833	0.060916	0.091849	0.127579	0.166985	0.208982	0.25258
b=0.05	0	0.005493	0.014124	0.027693	0.0467	0.070874	0.099532	0.1318	0.16676	0.203531	0.241318
b=0.1	0	0.010139	0.02239	0.038282	0.058229	0.082008	0.109056	0.138664	0.170096	0.20265	0.235704
b=0.2	0	0.019465	0.039193	0.060288	0.083073	0.107429	0.133021	0.159427	0.186214	0.212986	0.239396

Рис.4.23. Вероятность отказа системы “1 из 3” с учетом кратных отказов по общей причине.

Что касается практической организации расчетов отказов по общей причине, то в отечественной практике обычно делают следующим образом: рассчитывают интенсивности отказов элементов, используя стандарты типа MIL-HDBK-217, а затем вычисленную вероятность отказа элемента “развешивают” параметром β бета-факторной модели. Причем, значение β определяют на основе экспертных оценок. Такой подход недопустим, так как применение моделей отказов по общей причине правомерно в том и только том случае, если предварительно проводятся специально организованные статистические испытания групп элементов с требуемым анализом статистического материала на предмет выявления общих причин.

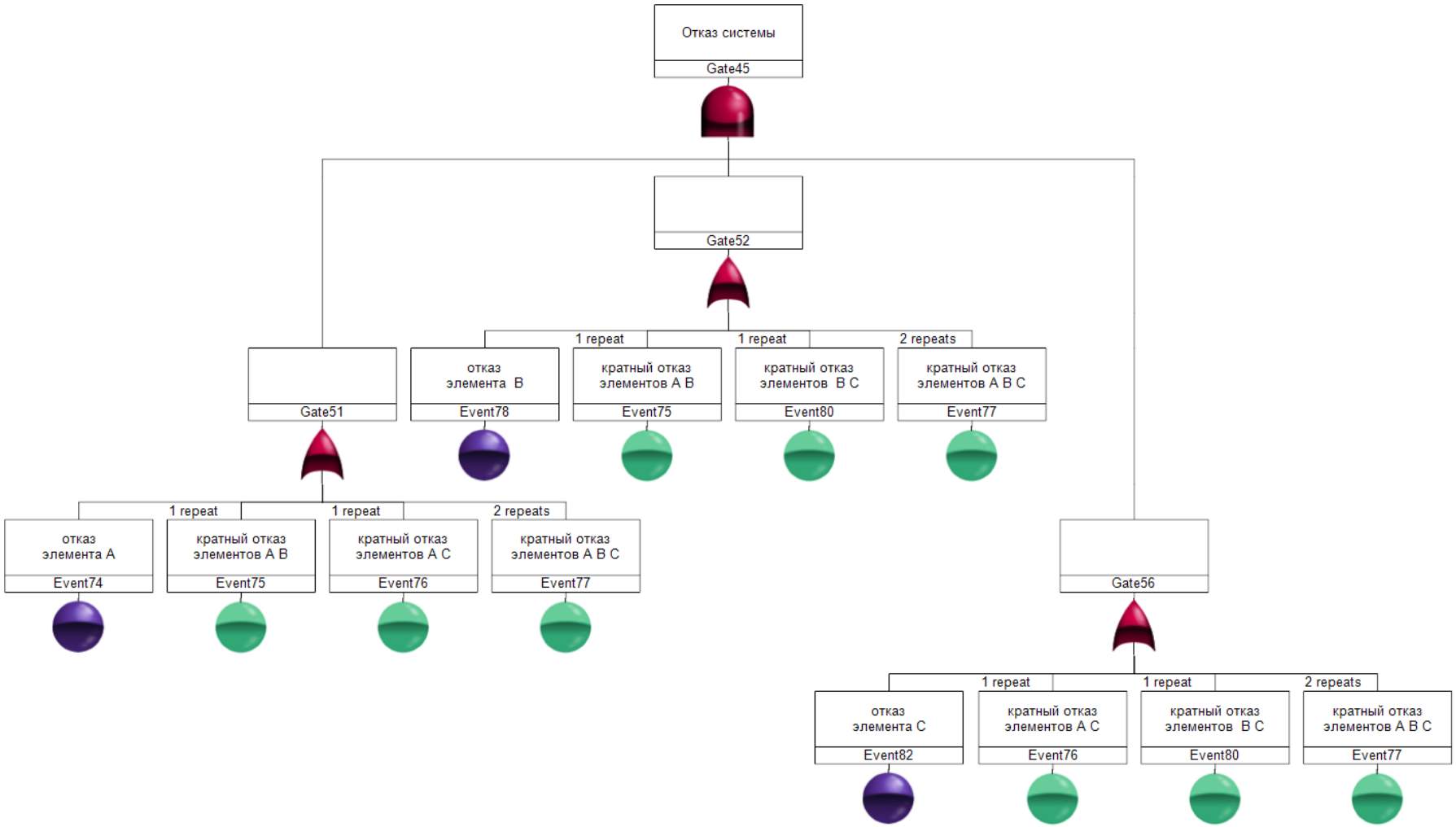


Рис.4.22. Дерево отказов резервированной схемы “1 из 3” с учетом отказов по общей причине

4.8. Оценка значимости базовых событий

К логико-вероятностным методам количественной оценки надежности относится группа методов оценки значимости элементов в системе [23,67, 85]. В программах, реализующих анализ деревьев отказов, обычно присутствуют следующие оценки значимости: Бирнбаума, Фассела-Весели, оценки критичности [86-89].

Оценка *Бирнбаума значимости* базового события А *(Birnbaum Importance Measure)* (чаще всего это событие соответствует отказу элемента) определяется как частная производная вероятности реализации вершинного гейта дерева (Q_{sys}) по вероятности базового события (q_A):

$$I_B(A) = \frac{\partial Q_{sys}}{\partial q_A} \tag{4.14}$$

Проведение оценок Бирнбаума требует знания вероятностных характеристик базовых событий дерева. Если оценка значимости проводится при отсутствии сведений об этих вероятностях, то даются рекомендации положить вероятность всех базовых событий равной 0.5. В этом случае оценка называется *структурной оценкой значимости (Structural Importance Measure – $I_S(A)$)*. Оценка $I_B(A)$ сконструирована таким образом, что она не учитывает вероятность возникновения события А. Для учета этой вероятности была введена *оценка критичности (Criticality Importance Measure):*

$$I_C(A) = \frac{\partial Q_{sys}}{\partial q_A} \cdot \frac{q_A}{Q_{sys}} = I_B(A) \cdot \frac{q_A}{Q_{sys}} \tag{4.15}$$

Оценка Фассела-Весели (*Fuessel-Vesely Importance Measure)* значимости элемента *(*базового события) А выражается через вероятность объединения минимальных сечений (C_i^A), содержащих этот элемент:

$$I_{FV}(A) = \frac{P(C_1^A \cup C_2^A \ldots \cup C_k^A)}{Q_{sys}} \tag{4.16}$$

Проведем оценки значимости элементов А и В в дублированной (D) и последовательной (S) схемах:

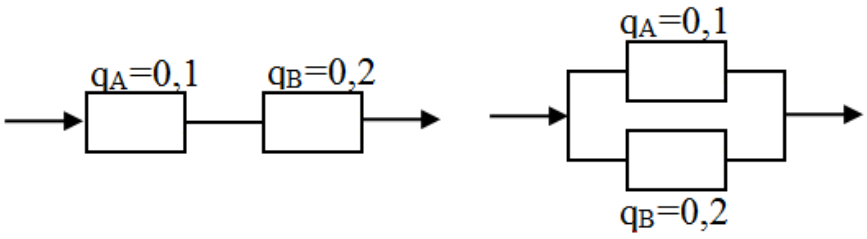


Рис.4.24. Простейшие последовательно-параллельные схемы.

*Оценка по Бирнбауму***.**

Последовательная схема:

$$I_B^S(A) = \frac{\partial Q_{sys}}{\partial q_A} = \frac{\partial(q_A + q_B - q_A q_B)}{\partial q_A} = 1 - q_B = 0{,}8; \quad I_B^S(B) = 1 - q_A = 0{,}9;$$

Дублированная схема:

$$I_B^D(A) = \frac{\partial Q_{sys}}{\partial q_A} = \frac{\partial(q_A q_B)}{\partial q_A} = q_B = 0{,}2; \quad I_B^D(B) = q_A = 0{,}1;$$

Структурная оценка

Последовательная схема:

$$I_S^S(A) == 1 - q_B = 0{,}5; \quad I_S^S(B) = 1 - q_A = 0{,}5;$$

Дублированная схема:

$$I_B^D(A) = q_B = 0{,}5; \quad I_B^D(B) = q_A = 0{,}5;$$

Оценка критичности

Последовательная схема:

$$I_C^S(A) = (1 - q_B)\frac{q_A}{q_A + q_B - q_A q_B} = 0{,}286; \quad I_C^S(B) = (1 - q_A)\frac{q_B}{q_A + q_B - q_A q_B} = 0{,}643;$$

Дублированная схема:

$$I_C^D(A) = q_B \frac{q_A}{q_B q_A} = 1; \quad I_C^D(B) = q_A \frac{q_B}{q_B q_A} = 1;$$

Оценка Фассела-Весели

Последовательная схема:

$$I_V^S(A) == \frac{q_A}{q_A + q_B - q_A q_B} = 0{,}357; \quad I_V^S(B) = \frac{q_B}{q_A + q_B - q_A q_B} = 0{,}714;$$

Дублированная схема:

$$I_V^D(A) = \frac{q_A q_B}{q_B q_A} = 1; \quad I_V^D(B) = \frac{q_A q_B}{q_B q_A} = 1;$$

Проанализируем полученные результаты. Сначала надо ответить на вопрос, что ожидается от оценки значимости элементов в системе. Основным назначением этих оценок должна быть возможность выявления «слабых мест» в системе, как в вероятностном, так и в структурном плане. С этой точки зрения все приведенные оценки не удовлетворяют этому назначению. Так, в оценке Бирнбаума в дублированной схеме более ненадежный элемент имеет меньшую значимость. А

должно быть наоборот, в однородных структурах (только последовательных, только параллельных, только m из n) более ненадежный элемент должен быть и более значим. Для последовательной схемы так и получилось, а для параллельной получили обратную картину. В других оценках значимости полученные значения, равные 1 для дублированной схемы, вообще не соответствуют никаким представлениям о влиянии отказа элемента на отказ системы (единица – это максимальная значимость элемента в структуре).

Трудно согласиться с якобы получаемой структурной значимостью, когда в оценки по Бирнбауму подставляются значения вероятности равными 0,5. Для оценок структурных характеристик должны использоваться структурные свойства, параметры элементов, путей, сечений, а не вероятности, тем более, что никаких вразумительных положений, почему подстановка для элементов значений 0,5 даст структурную значимость, нет. Например, структурными параметрами могут быть количество путей (сечений), в которые входит данный элемент, количество элементов в путях (сечениях), количество предотказовых состояний, в которые входит данный элемент и т.п. Подстановка вероятностей по 0,5 дала, естественно, вероятностную картину якобы структурной значимости, определив и в последовательной и в параллельной схемах структурную значимость каждого элемента, равную 0,5. То есть, в половине случаев и одна, и другая схемы отказывают по причине элемента 1, а в половине – элемента 2. В то время как очевидно, что структурная значимость каждого последовательно соединенного элемента должна быть 1 (независимо от количества элементов и надежностных структур с другими элементами), так как отказ любого последовательно соединенного в смысле надежности элемента приводит систему к отказу. Аналогично, структурная значимость каждого элемента в параллельных схемах (1 из n) должна быть 1/n. Кстати, оценка структурной значимости по отношению количества путей, в которые входит элемент i, к общему количеству путей даст, в частности, этот результат [90]. Однако и такая оценка имеет недостатки, но её можно модифицировать, оставаясь в рамках только структурных параметров.

Исходя из сделанного анализа, можно рекомендовать весьма осторожное и ограниченное применение предложенных оценок для анализа надежностной важности, значимости элементов системы.

4.9. Деревья событий

Метод деревьев событий (ДС) аналогично деревьям отказов опирается на графическое представление событий и их взаимосвязей. В качестве событий могут рассматриваться как внутренние события системы (отказы ее элементов), так и внешние (ураганы, падения метеоритов, самолетов, действия людей). Принципиальное отличие ДС от деревьев отказов состоит в том, что при составлении графических связей между событиями используется прямой ход анализа от причин к последствиям. При этом в качестве начальной вершины фигурирует исследуемое инициирующее событие, которое порождает (в зависимости от реализации других событий) множество последствий. Процедура построения дерева событий представляет собой индуктивный процесс, согласно которому исследователь начинает анализ с некоторого инициирующего события и определяет возможные наборы событий, связанных с данным, чтобы проследить пути возникновения опасных (или безопасных) исходов. Часто анализ на дереве событий называют анализом последовательности опасных событий. Но это не так! *События в дереве не рассматриваются, как возникающие последовательно во времени.* Каждая опасная цепочка (от инициирующего события до итогового) представляет собой совокупность событий, объединенных логическим оператором И. Учитывая это, можно сопрягать деревья отказов и деревья событий.

Приведем примеры использования деревьев событий для моделирования различных ситуаций.

На рис.4.25 показано дерево событий из Методических указаний по проведению анализа риска опасных производственных объектов РД 03-418-01 [91]. Дерево описывает аварию на установке первичной переработки нефти. Выходы дерева событий объединены в группы по уровню ущерба от аварии. Вероятность реализации каждого выхода определяется перемножением вероятностей ветвей (событий), приводящих к этому выходу. Например, вероятность минимального уровня ущерба вычисляется как 0.05*0.04*0.05 + 0.95*0.45*0.1 + 0.95*0.45*0.45.

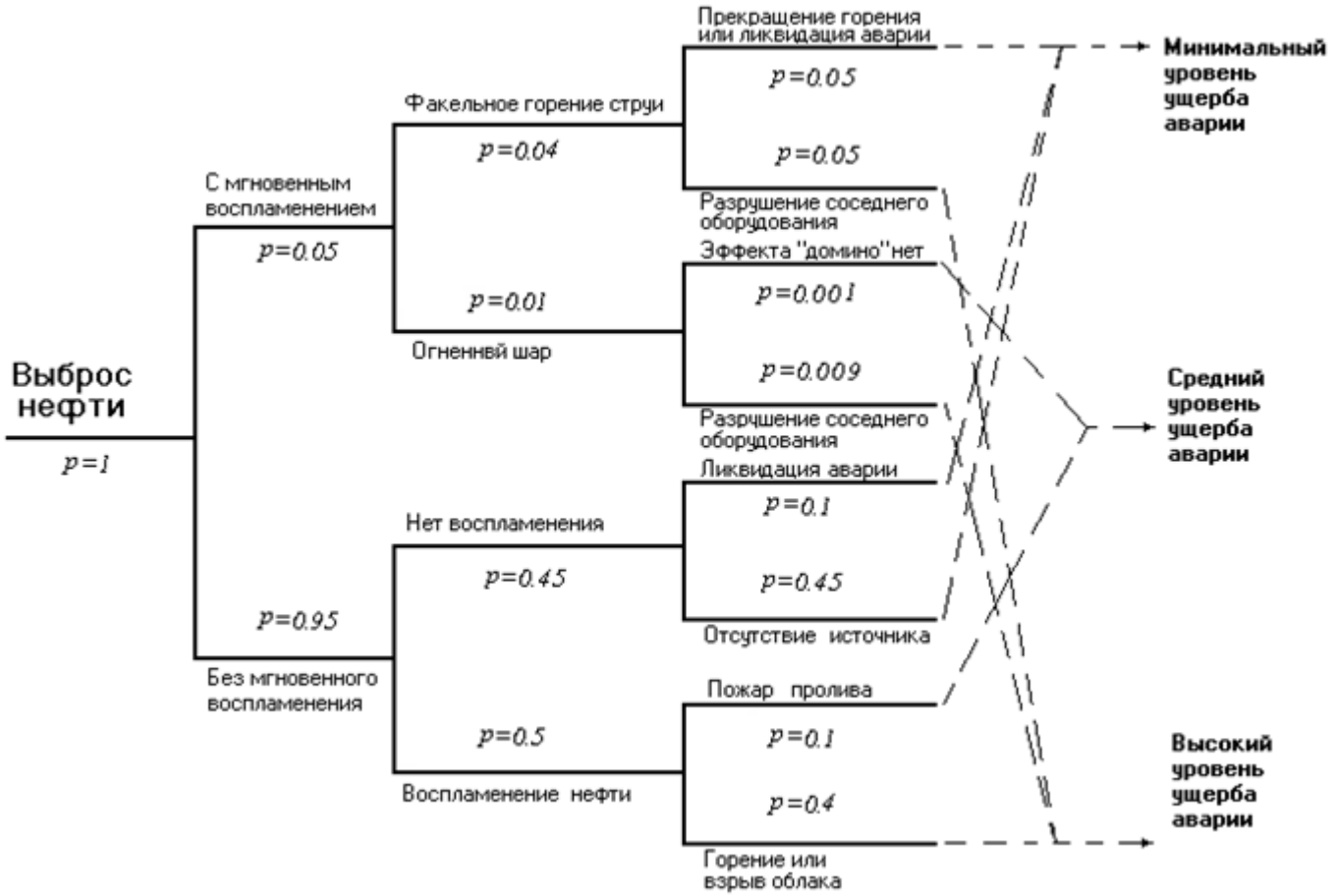


Рис. 4.25. Дерево событий аварии на установке первичной переработки нефти

В [92,93] модель деревьев событий используется для вычисления условных вероятностей, входящих как составляющие в комплексный показатель достоверности контроля. Деревья событий, в принципе, являясь переборным методом, удобны для вычисления условных вероятностей тем, что позволяют декомпозировать всю задачу, помещая условие в корень дерева и рассматривая его как исходное событие. Причем условие может состоять не из одного события, а из любой их логической комбинации. При оценке средств контроля исходными событиями (условиями) могут являться события $A(\overline{A})$ работоспособности (неработоспособности) объекта контроля. События $B(\overline{B})$ определены как признание объекта работоспособным (неработоспособным) средствами контроля. В качестве учитываемых факторов рассматривают полноту контроля и его состояния (работоспособность, отказ типа несрабатывание, отказ типа ложное срабатывание). Агрегирование показателей, вычисленных для выделенных при декомпозиции частей, в данном случае, проводится по формулам условной вероятности. Обозначим, η - полнота контроля, $C, \overline{C}_{fa}, \overline{C}_{no}$ - события работоспособности и отказов типа

ложного срабатывания и несрабатывания контроля. На рис 4.26, 4.27 представлены соответствующие деревья событий.

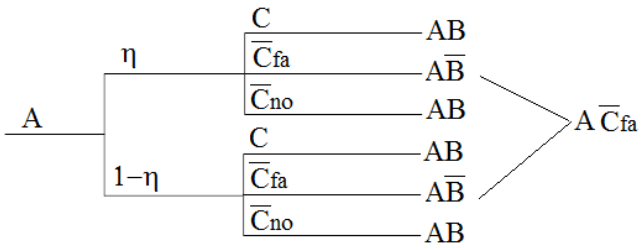


Рис.4.26. Дерево событий для вычисления условной вероятности признания контролем отказа объекта, при условии его работоспособности $P(\overline{B}/A)$

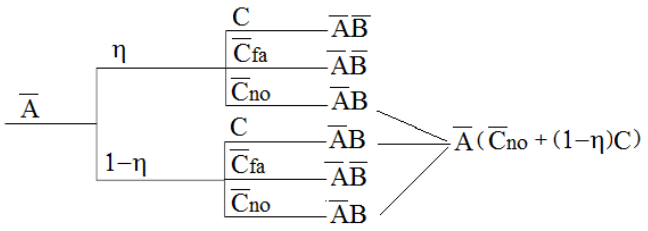


Рис.4.27. Дерево событий для вычисления условной вероятности признания контролем работоспособности объекта, при условии его отказа. $P(B/\overline{A})$

По построенным деревьям событий можно формально определить следующие результаты взаимодействия объекта и средств контроля:

- работоспособное состояние объекта признается контролем как работоспособное, что записывается $A \wedge B$;
- работоспособное состояние объекта признается контролем как неработоспособное, что записывается $A \wedge \overline{B}$;
- неработоспособное состояние объекта признается контролем как работоспособное, что записывается $\overline{A} \wedge B$;
- неработоспособное состояние объекта признается контролем как неработоспособное, что записывается $\overline{A} \wedge \overline{B}$.

Правильная оценка состояния объекта контроля происходит, когда результат взаимодействия объекта и средств контроля имеет вид $A \wedge B$ или $\overline{A} \wedge \overline{B}$. Поэтому достоверность контроля D определим как

$$D = P(A \wedge B) + P(\overline{A} \wedge \overline{B}) \ , \qquad (4.17)$$

а недостоверность как

$$\overline{D} = 1 - D = P(A \wedge \overline{B}) + P(\overline{A} \wedge B). \qquad (4.18)$$

Составляющие недостоверности контроля можно записать

$$P(A \wedge \overline{B}) = P(A) \cdot P(\overline{B}/A) \quad \text{и} \quad P(\overline{A} \wedge B) = P(\overline{A}) \cdot P(B/\overline{A}), \qquad (4.19)$$

где $P(A)$, $P(\overline{A})$ - вероятности работоспособного состояния и отказа объекта контроля, $P(\overline{B}/A)$, $P(B/\overline{A})$ - условные вероятности признания контролем отказа объекта, при условии его работоспособности, и работоспособности объекта, при условии его отказа, соответственно.

После вычисления по ним искомых условных вероятностей в соответствии с (4.18) получим

$$\overline{D} = P(A)\cdot P(\overline{C}_{fa}) + P(\overline{A})\cdot (P(C_{no}) + (1-\eta)\cdot P(C)). \qquad (4.20)$$

Деревья событий можно использовать для определения профиля производительности технологического комплекса (ТК), последовательно реализующего выполнение отдельных стадий технологического процесса автономными и независимыми (по технической реализации) технологическими системами. Примерами таких комплексов являются наземные и морские газодобычные комплексы. Основными причинами изменения производительности технологических систем являются: изменение объема и качественного состава потока входного продукта; снижение уровня работоспособности технологической системы, а соответственно и объема перерабатываемого продукта, обусловленное отказами оборудования.

Описание изменений производительности технологических систем может выполняться с помощью задания профиля производительности ПП – множества пар $\{П_k, P_k\}$ значений уровней производительности $П_k$ и вероятностей этих значений P_k.

Профиль производительности технологического комплекса определяется суперпозицией S профилей $ПП^1$, $ПП^2$,…,$ПП^N$ N последовательных технологических систем по следующему правилу $(ПП^i \; S \; ПП^j) = \{\min(П^i_k, П^j_k), (P^i_k \cdot P^j_k)\}$. Так, для двух последовательных систем с $ПП^1=\{П^1_1=100\%, P^1_1=0.8\}$ $\{П^1_2=80\%, P^1_2=0.1\}$ $\{П^1_3=0\%, P^1_3=0.1\}$ и $ПП^2=\{П^2_1=100\%, P^2_1=0.7\}$ $\{П^2_2=60\%, P^2_2=0.2\}$ $\{П^2_3=0\%, P^2_3=0.1\}$ выходной профиль производительности $ПП^3$ будет $\{П^3_1=100\%, P^3_1=0.56\}$ $\{П^3_2=80\%, P^3_2=0.07\}$ $\{П^3_3=60\%, P^3_3=0.18\}$ $\{П^3_4=0\%, P^3_4=0.19\}$.

Для совокупности из N систем профиль производительности определяется последовательной суперпозицией их профилей $ПП = (_1 \ldots (_N ПП^1 \; S \; ПП^2) \ldots) \; S \; ПП^{i-1}) \; S \; ПП^i) \ldots S \; ПП^{N-1}) \; S \; ПП^N)$.

Профиль производительности $ПП^i$ отдельной системы строится по результатам анализа технологического процесса, включая как экспертные заключения, так и на основе анализа надежности проектных решений этой системы.

На основе полученного профиля производительности может быть рассчитан основной показатель эффективности комплекса коэффициент сохранения эффективности:

$$К_{сохр.эф.} = \frac{\sum_{i=1}^{M} Р_i П_i}{П_{ном.}}, \qquad (4.21)$$

$П_{ном.}$ – есть номинальный уровень производительности, М – число уровней производительности комплекса.

Дерево событий для расчетов профиля производительности ТК строится таким образом, чтобы можно было осуществить полный перебор всех возможных сочетаний уровней производительности систем, входящих в комплекс. Корню дерева соотносится технологический комплекс, каждый последующий столбец дерева соответствует системе. Количество ветвей s-го столбца дерева определяется произведением $\prod_{i=1}^{s} n_i$, где n_i – количество уровней производительности i-й системы, каждая ветвь s-го столбца описываются парой $\{П^s_k, Р^s_k\}$. Выходные ветви дерева, имеющие одинаковые $П^N_к$, объединяются, а соответствующие им вероятности суммируются.

Дерево событий технологического комплекса, состоящего из трех систем, показано на рис.4.28. Результат расчета выходного профиля производительности ТК приведен на рис.4.29. Дерево набрано и рассчитано в модуле Event Tree Windchill Quality Solutions.

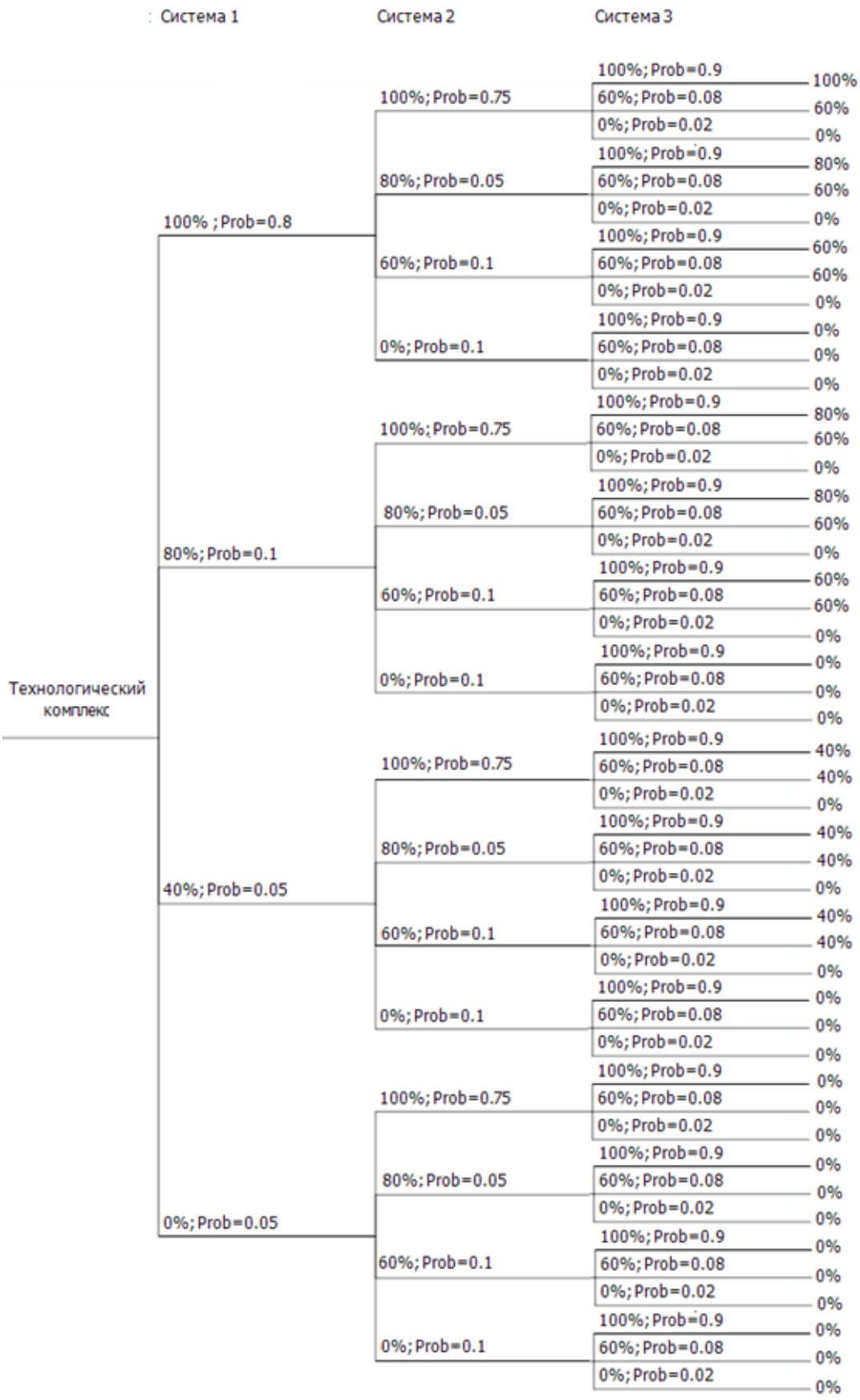
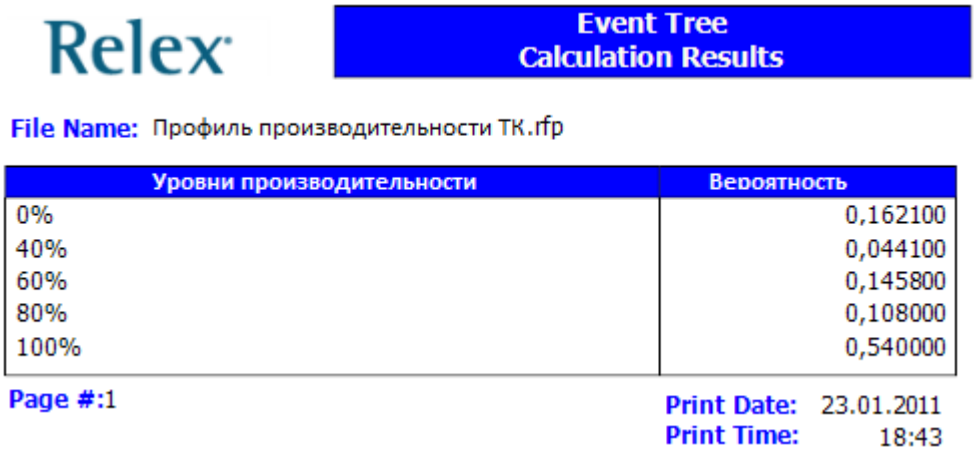


Рис. 4.28. Дерево событий для расчета профиля производительности ТК



Relex

Event Tree
Calculation Results

File Name: Профиль производительности ТК.rfp

Уровни производительности	Вероятность
0%	0,162100
40%	0,044100
60%	0,145800
80%	0,108000
100%	0,540000

Page #:1

Print Date: 23.01.2011
Print Time: 18:43

Рис.4.29. Результаты расчета профиля производительности ТК в модуле Event Tree Windchill Quality Solutions.

Глава 5. Динамические модели надежности.

В разделе 1.2 все модели надежности были разделены на два класса статические и динамические. Статическая модель описывает “надежностное” состояние системы в момент времени t набором работоспособных и неработоспособных элементов. Главы 2-4 были посвящены методам анализа, используемым в статических моделях. В главе 2 рассматривалось применение основных формул теории вероятностей (вероятность суммы и произведения событий, формула полной вероятности) для расчета показателей безотказности резервированных систем с нагруженным резервом. В главах 3 и 4 изучались логико-вероятностные методы анализа надежности, основанные на записи логических условий работоспособности (неработоспособности) и их последующего преобразования в вероятностную форму. Эти методы оказываются недостаточными для исследования сложных систем. С точки зрения анализа надежности сложность систем обуславливается следующими факторами:

- наличие нескольких уровней эффективности функционирования (производительности) в работоспособных состояниях и постепенная деградация по эффективности при возникновении неисправностей; состояния неработоспособности могут также различаться по последствиям
- реализация разнообразных способов резервирования (структурного, временного, алгоритмического)
- использование различных стратегий восстановления. Ограничение на ЗИП и число ремонтных бригад.
- применение алгоритмических методов обработки неисправностей (в основном для вычислительных устройств) с классификацией на сбои и отказы
- возможность возникновения нескольких несовместных видов отказов элементов, приводящих при определенной кратности и последовательности возникновения к различным последствиям на системном уровне; наличие скрытых и явных отказов
- отказы по общей причине, индуцированные отказы.

Учет перечисленных факторов возможен в рамках динамических моделей надежности, описывающих происходящие в системе события, отказы как процессы, развивающиеся во времени.

Наиболее распространенными динамическими моделями “надежностного” поведения систем являются марковские случайные процессы, поэтому данная глава будет посвящена использованию марковских моделей надежности для анализа сложных систем.

5.1. Марковские случайные процессы

В теории вероятностей введено понятие случайной функции, т.е. такой функции, значение которой при каждом данном значении аргумента (или аргументов) является случайной величиной. Случайную функцию можно рассматривать как совокупность случайных величин, представляющих ее значения при различных значениях аргумента. В общем случае случайная функция равноценна бесконечному, несчетному множеству случайных величин. Каждая конкретная функция, которая может быть зарегистрирована при одном наблюдении случайной функции, называется реализацией этой функции. Элементарное изложение теории случайных функций, достаточное для понимания технических приложений теории вероятности и, в частности, теории надежности дано в [58, 94, 95].

Случайная функция времени характеризует процесс изменения случайной величины с течением времени. Случайные функции времени называют *случайными* или *стохастическими процессами.*

Говорят, что в некоторой системе S протекает случайный процесс, если ее состояния меняются с течением времени случайным образом. Процесс, протекающий в системе, называется *марковским* или *процессом без последействия*, если для каждого момента времени вероятность любого состояния системы в будущем зависит только от состояния системы в настоящий момент и не зависит от того, каким образом система пришла в это состояние.

Пространство возможных состояний системы может быть как непрерывным, так и дискретным, когда состояния системы можно перечислить или пронумеровать. При исследовании надежности систем, состоящих из элементов с заданными надежностными характеристиками, пространство состояний всегда дискретно.

Математическое описание марковского случайного процесса, протекающего в системе с дискретными состояниями, зависит от того, в какие моменты времени могут происходить переходы системы из состояния в состояние. Если переходы между состояниями могут происходить только в заранее определенные моменты времени, то такой процесс называют марковским процессом с дискретным временем. Если переходы могут происходить в любые случайные моменты времени, то такой процесс называют марковским процессом с непрерывным временем. При экспоненциальном распределении случайного времени пребывания системы в каждом из своих состояний марковский процесс является однородным (интенсивности переходов между состояниями не зависят от времени). Однородные марковские процессы с дискретным множеством состояний и непрерывным временем являются основным аппаратом исследования

надежности сложных систем с восстановлением. Это объясняется тем, что именно они позволяют получать аналитические выражения или вычислительные схемы для расчета различных показателей надежности. Кроме того, в подавляющем большинстве случаев исходными данными для элементов являются либо константные интенсивности отказов, либо средние наработки до отказа.

Построение марковских моделей надежности происходит следующим образом. На основе информации о структуре и принципах функционирования исследуемой системы определяется множество ее возможных состояний. Это множество разделяется на два подмножества – работоспособных состояний и состояний отказа. Далее строится марковский граф переходов, вершинами которого являются состояния системы, а ребрами – возможные переходы между состояниями. Интенсивности переходов определяются характеристиками безотказности и ремонтопригодности элементов системы. По графу переходов составляется необходимая система уравнений, аналитическое решение которой позволяет получить формульные выражения для требуемых показателей надежности. Если решение системы возможно только численными методами, то получают численные значения показателей надежности в заданные моменты времени.

5.2. Уравнение Колмогорова-Чепмена. Марковская модель надежности восстанавливаемого элемента.

Рассмотрим функционирование восстанавливаемого элемента, при следующих предположениях: (1) поток отказов элемента – пуассоновский с параметром λ (интенсивность отказов); (2) поток восстановлений элемента - пуассоновский с параметром μ (интенсивность восстановления). Предположения (1) и (2) равносильны предположению об экспоненциальном распределении случайных времен отказа и восстановления. Элемент может находиться в двух состояниях: **1** - исправное состояние; **2** – состояние отказа. Марковский граф переходов элемента между исправным состоянием и состоянием отказа показан на рис.5.1.

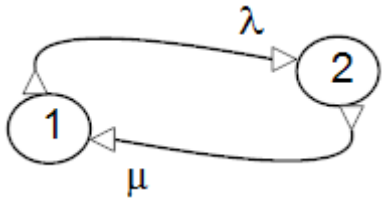


Рис.5.1. Марковский граф переходов для восстанавливаемого элемента.

Обозначим: $P_1(t)$ – вероятность нахождения элемента в момент времени t в состоянии 1. $P_2(t)$ – вероятность нахождения элемента в момент времени t в состоянии 2. Событие А работоспособности элемента (нахождения в состоянии 1) в момент времени $t+\Delta t$ может произойти двумя способами. Либо произойдет событие В, состоящее в том, что в момент t элемент уже находился в работоспособном состоянии 1 и за время Δt не вышел из этого состояния (отказ за Δt не произошел). Либо произойдет событие С, состоящее в том, что в момент t элемент была в состоянии отказа 2 и за время Δt перешел из состояния 2 в состояние 1 (работоспособность элемента была восстановлена за Δt).

Вероятность события В равна

$$P(B) = P_1(t)e^{-\lambda\Delta t} \tag{5.1}$$

Разлагая экспоненту в ряд, получаем $e^{-\lambda\Delta t} = 1 - \lambda\Delta t + \frac{(\lambda\Delta t)^2}{2!} - \frac{(\lambda\Delta t)^3}{3!} + ... = 1 - \lambda\Delta t + 0(\Delta t)$.

Или с точностью до величин высшего порядка малости

$$P(B) \approx P_1(t)(1 - \lambda\Delta t) \tag{5.2}$$

Вероятность события С равна

$$P(C) = P_2(t)(1 - e^{-\mu\Delta t}) \approx P_2(t)\mu\Delta t \tag{5.3}$$

Тогда вероятность события А (работоспособности элемента в момент времени $t+\Delta t$), с учетом того, что события В и С несовместны, определяется как:

$$P(A) = P_1(t + \Delta t) = P_1(t)(1 - \lambda\Delta t) + P_2(t)\mu\Delta t \tag{5.4}$$

Если мы перенесем $P_1(t)$ в левую часть уравнения, разделим полученное приращение функции на приращение аргумента, устремив Δt к нулю, то получим дифференциальное уравнение относительно неизвестной вероятности $P_1(t)$:

$$P_1'(t) = P_1(t)(-\lambda) + P_2(t)\mu \tag{5.5}$$

Аналогично рассуждая, можно получить дифференциальное уравнение относительно вероятности $P_2(t)$. Таким образом, мы получили для вероятностей $P_1(t)$ и $P_2(t)$ систему обыкновенных дифференциальных уравнений:

$$\begin{cases} P_1'(t) = -\lambda P_1(t) + P_2(t)\mu \\ P_2'(t) = \lambda P_1(t) - P_2(t)\mu \end{cases} \tag{5.6}$$

Полученную систему дифференциальных уравнений решают при начальных условиях $P_1(0)$, $P_2(0)$, задающих распределение вероятностей состояний в начальный момент времени t=0. Так как

для любого момента времени события нахождения элемента в одном из своих возможных состояний составляют полную группу, то выполняется нормировочное условие $P_1(t) + P_2(t) = 1$.

Интенсивности уравнения (5.6) можно представить в виде квадратной матрицы $T = \begin{vmatrix} 0 & \lambda \\ \mu & 0 \end{vmatrix}$, имеющей однозначное соответствие с марковским графом.

В матричном виде (5.6) можно записать как

$$\left[P_1'(t), P_2'(t)\right] = \left[P_1(t), P_2(t)\right] \begin{bmatrix} -\lambda & \lambda \\ \mu & -\mu \end{bmatrix} \text{ или } P'(t) = P(t) \cdot \Lambda . \qquad (5.7)$$

Здесь $P'(t)$, $P(t)$ – вектор строки, Λ – инфинитезимальная матрица. Между элементами матриц T и Λ имеется очевидная связь: $\lambda_{ij} = t_{ij}$ при $i \neq j$; $\lambda_{ij} = -\sum_{j=1}^{n} t_{ij}$ при $i = j$.

Если мы будем строить марковские модели надежности систем, состоящих из нескольких элементов, учитывать дополнительные факторы, то очевидно, что пространство состояний модели будет увеличиваться. Система дифференциальных уравнений относительно $P_i(t)$ (i = 1, 2, … , n) в общем виде записывается как

$$\begin{aligned} P_1'(t) &= -P_1(t)\sum_{i \in g_1} \lambda_{1i} + \sum_{i \in G_1} P_i(t)\lambda_{i1} \\ &\ldots \\ P_k'(t) &= -P_k(t)\sum_{i \in g_k} \lambda_{ki} + \sum_{i \in G_k} P_i(t)\lambda_{ik} \quad , \\ &\ldots \\ P_n'(t) &= -P_n(t)\sum_{i \in g_n} \lambda_{ni} + \sum_{i \in G_n} P_i(t)\lambda_{in} \end{aligned} \qquad (5.8)$$

где g_k – множество состояний, в которые возможен непосредственный переход из данного состояния k; G_k – множество состояний, из которых возможен непосредственный переход в состояние k.

Уравнения вида (5.8) для вероятностей состояний марковского процесса с непрерывным временем и дискретным множеством состояний называются уравнениями Колмогорова-Чепмена.

Произведение $P_i(t)\lambda_{ij}$ имеет название потока вероятности. При составлении уравнений Коломогорова-Чепмена по графу переходов удобно пользоваться следующим правилом: производная вероятности любого состояния равна сумме потоков вероятности, переводящих систему в это состояние, минус сумме всех потоков вероятности, выводящих систему из этого состояния.

5.3. Аналитические методы решения уравнений Колмогорова-Чепмена на примере восстанавливаемого элемента

1. Метод решения, основанный на преобразовании Лапласа.

Применим к системе дифференциальных уравнений (5.6), описывающих процесс отказов и восстановлений элемента, преобразование Лапласа. В результате получаем систему алгебраических уравнений

$$\begin{cases} sP_1(s) - 1 = -\lambda P_1(s) + P_2(s)\mu \\ sP_2(s) = \lambda P_1(s) - P_2(s)\mu \end{cases}, \tag{5.9}$$

где $P_i(s) = \int_0^\infty P_i(t)e^{-st}dt$ - есть преобразование Лапласа для $P_i(t)$.

Таблица преобразований Лапласа основных функций, используемых при расчетах надежности, приведена ниже.

Таблица 5.1. Формулы преобразований Лапласа.

Изображение	Оригинал	Изображение	Оригинал
$\alpha p_1(s)+\beta p_2(s)$	$\alpha p_1(t)+\beta p_2(t)$	$1/s$	$1(t)$
$sp(s)-p(0)$	$p'(t)$	$1/s^n$, n=1,2…	$t^{n-1}/(n-1)!$
$e^{-bs}p(s)$	$p(t-b)$	$1/(s-b)$	e^{bt}
$(1/b)p(s/b)$, b>0	$p(bt)$	$1/(s-b)^n$, n=1,2…	$(t^{n-1}/(n-1)!)e^{bt}$

Систему (5.9) удобно записать в виде

$$\begin{cases} (s+\lambda)P_1(s) - \mu P_2(s) = 1 \\ \lambda P_1(s) - (\mu + s)P_2(s) = 0 \end{cases} \tag{5.10}$$

Находим решение системы алгебраических уравнений (5.10), например, используя правило Крамера, и далее представляем его в виде суммы простых дробей для получения обратного преобразования Лапласа:

$$\begin{aligned} P_1(s) &= \frac{\mu + s}{s(s + (\lambda + \mu))} = \frac{A_1}{s} + \frac{B_1}{s + (\lambda + \mu)} \\ P_2(s) &= \frac{\lambda}{s(s + (\lambda + \mu))} = \frac{A_2}{s} + \frac{B_2}{s + (\lambda + \mu)} \end{aligned} \tag{5.11}$$

Соотношения $(A_1 + B_1)s + A_1(\lambda + \mu) = \mu + s; (A_2 + B_2)s + A_2(\lambda + \mu) = \lambda$ позволяют найти искомые коэффициенты:

$$A_1 = \frac{\mu}{\lambda + \mu}; B_1 = \frac{\lambda}{\lambda + \mu}; A_2 = \frac{\lambda}{\lambda + \mu}; B_2 = -\frac{\lambda}{\lambda + \mu}. \quad (5.12)$$

Воспользовавшись формулами таблицы 5.1, находим $P_1(t)$ и $P_2(t)$ как обратное преобразование Лапласа от $P_1(s)$ и $P_2(s)$:

$$P_1(t) = \frac{\mu}{\lambda + \mu} + \frac{\lambda}{\lambda + \mu} e^{-(\lambda+\mu)t};$$
$$P_2(t) = \frac{\lambda}{\lambda + \mu}(1 - e^{-(\lambda+\mu)t}). \quad (5.13)$$

Вероятность $P_1(t)$ есть вероятность застать восстанавливаемый элемент в работоспособном состоянии *в произвольный момент времени t*. Эта вероятность является одним из важнейших показателей надежности восстанавливаемых систем и называется коэффициентом готовности $К_Г(t)$.

Вероятность $P_2(t)$ есть вероятность застать восстанавливаемый элемент в неработоспособном состоянии *в произвольный момент времени t*. Этот показатель называется коэффициентом простоя $К_П(t)$.

2. *Метод решения, основанный на сведении системы n уравнений к уравнению n-го порядка*

Выразим из второго уравнения системы (5.6) неизвестную вероятность $P_1(t)$

$$P_1(t) = \frac{P_2'(t) + \mu P_2(t)}{\lambda}. \quad (5.14)$$

Подставив полученное выражение в первое уравнение системы (5.6), получим линейное однородное дифференциальное уравнение второго порядка:

$$P_2''(t) + (\lambda + \mu)P_2'(t) = 0. \quad (5.15)$$

Характеристическое уравнение для (5.15) имеет вид

$$x^2 + (\lambda + \mu)x = 0 \ . \quad (5.16)$$

Корни характеристического уравнения равны: $x_1 = 0, x_2 = -(\lambda + \mu)$.

Корню x_1=0 соответствует решение $C_1 e^{x_1 t} = C_1$. Корню $x_2 = -(\lambda+\mu)$ соответствует решение $C_2 e^{x_2 t} = C_2 . e^{-(\lambda+\mu)t}$.

Общее решение однородного уравнения (5.16) имеет вид:

$$P_2(t) = C_1 e^{x_1 t} + C_2 e^{x_2 t} = C_1 + C_2 e^{-(\lambda+\mu)t} \quad (5.17)$$

Найдем значение произвольных постоянных C_1 и C_2. Для этого подставим в общее решение начальное условие $P_2(0)=0$. Тогда $C_1 = - C_2$. Выразим (5.14) через общее решение и, учитывая начальное условие $P_1(0)=1$, получим

$$C_1 = \frac{\lambda}{\lambda+\mu}; C_2 = -\frac{\lambda}{\lambda+\mu}. \quad (5.18)$$

Рассмотренные два метода не являются единственными методами аналитического решения систем дифференциальных уравнений, описывающих динамику вероятностей пребывания системы в множестве ее возможных "надежностных" состояний. Например, известны и успешно применяются при решении задач анализа надежности методы, основанные на вычислении собственных значений и собственных векторов [96]. В заключении отметим, что все аналитические методы явным или неявным образом связаны с решением характеристического уравнения, которое для систем большой размерности не решается аналитически. Поэтому в современном программном обеспечении анализа надежности на марковских моделях решение уравнений Колмогорова-Чепмена реализуется численными методами. Так как марковские модели надежности в виду большой разницы в значениях интенсивностей отказов ($\lambda \approx 10^{-6} \div 10^{-9}$) и интенсивностей восстановлений ($\mu \approx 1 \div 100$) порождают жесткие дифференциальные уравнения, то пользуются специальными численными методами. Создание эффективных методов для решения жестких уравнений является областью активных математических исследований. Обсуждение этих методов выходит за рамки тематики данной книги, а интересующимся читателям можно предложить публикации [97,98]

5.4 Расчет показателей безотказности восстанавливаемых систем на марковских моделях.

1. Расчет вероятности безотказной работы.

Для восстанавливаемых систем при нахождении показателя вероятности безотказной работы необходимо все состояния отказа сделать поглощающими. Формально это означает удаление всех ветвей марковского графа (или обнуление интенсивностей перехода), соответствующих возврату из отказовых состояний в работоспособные. После этого для каждого k-го состояния работоспособности системы можно записать следующее дифференциальное уравнение:

$$P'_k(t) = -P_k(t)\sum_{i \in g_k} \lambda_{ki} + \sum_{i \in G_+ \cap G_k} P_i(t)\lambda_{ik}, \quad (5.19)$$

где G_+ - множество состояний работоспособности системы.

Для случая восстанавливаемого элемента марковский граф с поглощающим состоянием отказа имеет вид, показанный на рис.5.2.

Рис.5.2. Марковский граф с поглощающим состоянием отказа элемента.

огда вероятностью безотказной работы будет $P_1(t)$, которая определяется из решения уравнения:

$$P_1'(t) = -\lambda P_1(t). \tag{5.20}$$

Начальное условие: $P_1(0)=1$.

Разделяя переменные и интегрируя левую и правую части, получаем известное выражение для вероятности безотказной работы экспоненциально распределенного элемента (P(t)):

$$\int \frac{P_1'(t)}{P_1(t)} dt = -\int \lambda dt; P_1(t) = C_1 e^{-\lambda t}; P_1(0) = 1 \Rightarrow C_1 = 1.$$

$$P(t) = P_1(t) = e^{-\lambda t} \tag{5.21}$$

2. Расчет средней наработки до отказа

Известно, что средняя наработка до отказа (T) и вероятность безотказной работы связаны соотношением $T = \int_0^\infty P(t)dt$. Следовательно, показатель средней наработки до отказа можно получить, интегрируя систему дифференциальных уравнений для модели с “поглощением”. Рассмотрим общий случай системы с n состояниями, в которой состояние n является поглощающим (отказ системы):

$$\begin{aligned}
&P_1'(t) = -P_1(t)\sum_{i\in g_1}\lambda_{1i} + \sum_{i\in G_+\cap G_1} P_i(t)\lambda_{i1}\\
&\ldots\\
&P_k'(t) = -P_k(t)\sum_{i\in g_k}\lambda_{ki} + \sum_{i\in G_+\cap G_k} P_i(t)\lambda_{ik}\\
&\ldots\\
&P_{n-1}'(t) = -P_{n-1}(t)\sum_{i\in g_{n-1}}\lambda_{(n-1)i} + \sum_{i\in G_+\cap G_{n-1}} P_i(t)\lambda_{i(n-1)}
\end{aligned} \tag{5.22}$$

Начальные условия: $P_1(0)=1$, …$P_k(0)=0$,…$P_n(0)=0$.

Проинтегрируем левые и правые части уравнений (5.22). Учитывая, что при наличии поглощающего состояния $P_i(\infty)=0$, имеем

$$\begin{aligned}
&-T_1\sum_{i\in g_1}\lambda_{1i}+\sum_{i\in G_+\cap G_1}T_i\lambda_{i1}=-1\\
&\ldots\\
&-T_k\sum_{i\in g_k}\lambda_{ki}+\sum_{i\in G_+\cap G_k}T_i\lambda_{ik}=0 \qquad ,\\
&\ldots\\
&-T_{n-1}\sum_{i\in g_{n-1}}\lambda_{(n-1)i}+\sum_{i\in G_+\cap G_{n-1}}T_i\lambda_{in-1}=0
\end{aligned} \tag{5.23}$$

где T_i – среднее время пребывания в работоспособном состоянии i при начале работы из исправного состояния.

Средняя наработка до отказа T определяется суммированием T_i по всем работоспособным состояниям:

$$T=\sum_{i\in G_+}T_i \tag{5.24}$$

Для одного элемента, с учетом $P_1(0)=1$, имеем: $-1=-\lambda T$, откуда

$$T=\frac{1}{\lambda}. \tag{5.25}$$

5.5. Расчет стационарных показателей на марковских моделях надежности

В теории случайных процессов доказано, что однородный марковский процесс без поглощающих состояний (состояний, из которых нет выхода) имеет стационарный режим, который обязательно наступит при достаточно больших временах ($t\to\infty$). Стационарный режим характеризуется тем, что вероятности P_i уже не зависят от времени, а, следовательно, их производные становятся равными нулю. Поэтому для вычисления стационарных вероятностей состояний системы необходимо приравнять к нулю производные, стоящие в левых частях уравнений (5.8). Чтобы полученная система не была вырожденной, одно из уравнений заменяют на условие нормировки ($\sum_{i=1}^{n}P_i=1$). В результате получаем следующую систему n алгебраических уравнений для определения стационарных показателей надежности:

$$
\begin{aligned}
&-P_1\sum_{i\in g_1}\lambda_{1i}+\sum_{i\in G_1}P_i\lambda_{i1}=0\\
&\ldots\\
&-P_k\sum_{i\in g_k}\lambda_{ki}+\sum_{i\in G_k}P_i\lambda_{ik}=0\\
&\ldots\\
&-P_{n-1}\sum_{i\in g_{n-1}}\lambda_{(n-1)i}+\sum_{i\in G_{n-1}}P_i\lambda_{i(n-1)}=0\\
&P_1+\ldots+P_k+..+P_{n-1}+P_n=1
\end{aligned}
\qquad (5.26)
$$

Решение системы (5.26) позволяет получить такие показатели надежности как стационарный коэффициент готовности $К_Г$ (вероятность застать объект в работоспособном состоянии в произвольный, достаточно удаленный момент времени) и стационарный коэффициент простоя $К_П$ (вероятность застать объект в неработоспособном состоянии в произвольный, достаточно удаленный момент времени).

$$К_Г=\sum_{i\in G_+}P_i\ , \qquad (5.27)$$

$$К_П=\sum_{i\in G_-}P_i\ , \qquad (5.28)$$

где G_- - множество всех неработоспособных состояний системы.

Проведем исследование надежности системы из одного восстанавливаемого элемента (рис.5.1) на стационарном участке. Система алгебраических уравнений, полученных из (5.6) при $t\to\infty$, имеет вид

$$\begin{cases}-\lambda P_1+\mu P_2=0\\ P_1+P_2=1\end{cases}. \qquad (5.29)$$

Решение системы: $P_1=\dfrac{\mu}{\lambda+\mu};\ P_2=\dfrac{\lambda}{\lambda+\mu}$.

Полученные на марковской модели показатели надежности восстанавливаемого элемента сведены в таблицу 5.2.

Таблица 5.2. Формулы показателей надежности восстанавливаемого элемента.

Коэффициент готовности:	$K_г(t) = \frac{\mu}{\lambda+\mu} + \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t}$
Коэффициент простоя:	$K_П(t) = \frac{\lambda}{\lambda+\mu}(1 - e^{-(\lambda+\mu)t})$
Стационарный коэффициент готовности:	$K_г = \frac{\mu}{\lambda+\mu}$
Стационарный коэффициент простоя:	$K_П = \frac{\lambda}{\lambda+\mu}$
Вероятность безотказной работы	$P(t) = e^{-\lambda t}$
Средняя наработка до отказа:	$T = \frac{1}{\lambda}$

5.6. Укрупнение состояний марковской модели

Аналитические марковские модели являются мощным и достаточно универсальным математическим аппаратом анализа надежности сложных систем. Однако при их применении возникают известные проблемы размерности – рост пространства состояний модели и связей между состояниями при увеличении количества элементов анализируемой системы. В общем случае размерность пространства состояний марковской модели $\geq \prod_{i=1}^{n} K_i$, где n – количество элементов системы, K_i – количество состояний, в которых может находиться i-й элемент системы, например, устройство контроля может находиться в трех состояниях (работоспособном и состояниях, соответствующих двум вида неработоспособности: отказа типа несрабатывания, отказа типа ложное срабатывание). Если элемент может находиться в двух состояниях, работоспособном и неработоспособном, то размерность марковской модели будет $\geq 2^n$.

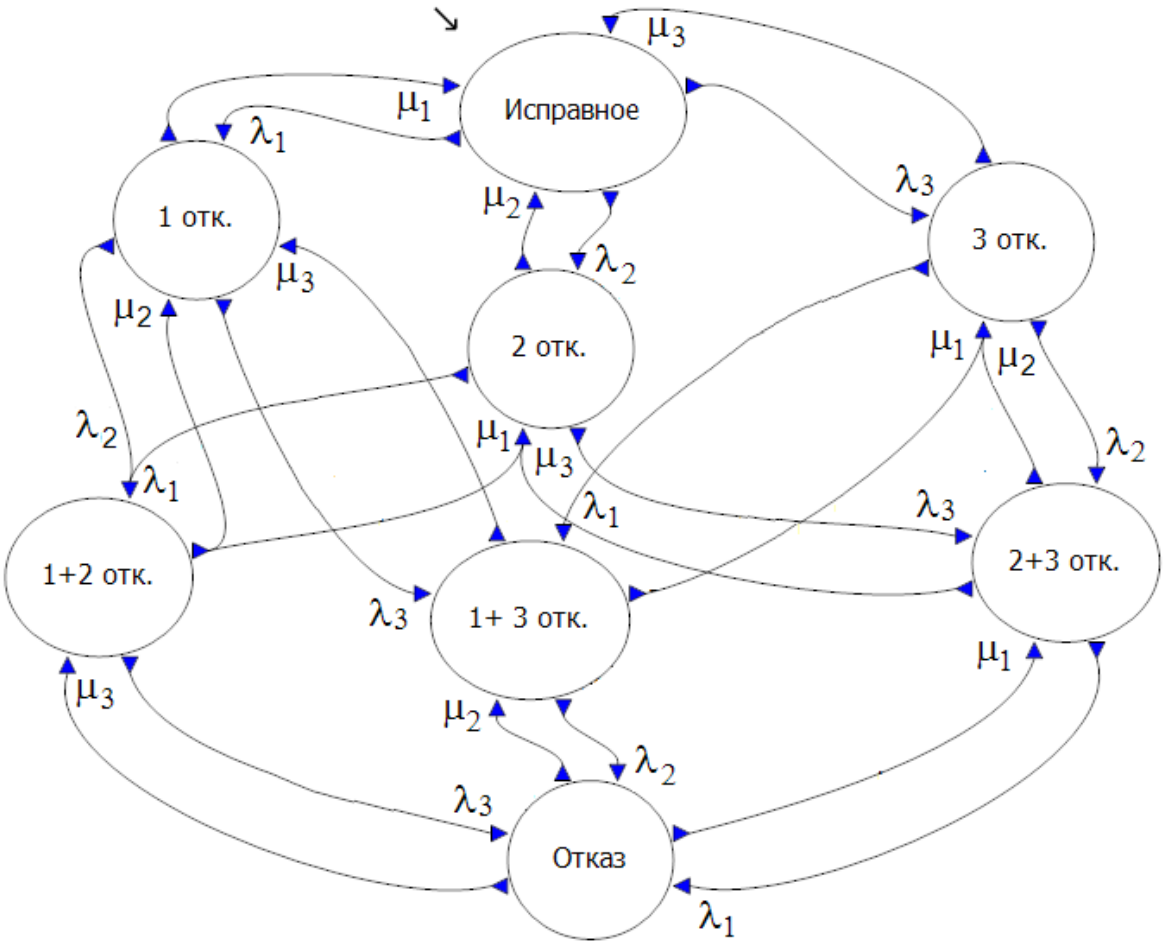
Сравним с точки зрения размерности три модели надежности: блок-схему, дерево отказов, марковский граф для системы из трех разнонадежных параллельно работающих элементов, отказом которой является отказ всех трех ее элементов (критерий работоспособности “1 из 3”). На рис. 5.3 а,б,в показаны три разные модели надежности этой системы – марковский граф, блок-схема, дерево отказов, набранные в ПО Windchill Quality Solutions. Очевидно, что в данном случае логико-вероятностные модели оказываются гораздо более компактными, чем марковские. Если к тому же учесть, что для расчета показателей надежности на марковской модели необходимо

составить и решить систему дифференциальных уравнений, а расчет на блок-схемах и деревьях сведется в данном случае к достаточно простому преобразованию логических функций и замене логических переменных вероятностными, то сравнение будет не в пользу марковского моделирования. Однако это не так:

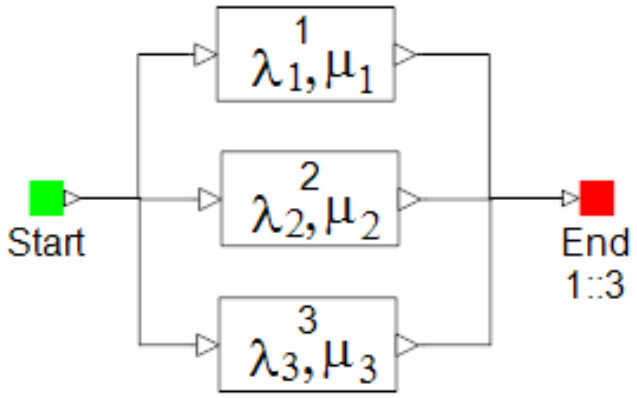
1. Как только мы захотим снять предположение о полной независимости процесса восстановления элементов (модели рис.5.3 построены именно при этом предположении), то логико-вероятностные методы перестают “работать”. На марковской модели мы можем учесть ряд особенностей процесса восстановления (ограничение на число ремонтных бригад, приоритеты, останов системы при ремонте и пр.). Логико-вероятностные модели описывают только случай неограниченного, независимого восстановления элементов, причем восстановление производится при работающей системе, что очень редко выполняется на практике.
2. Для систем с восстановлением на логико-вероятностных моделях рассчитываются лишь точечные показатели надежности, определяемые в момент времени t, например, коэффициент готовности, коэффициент простоя. Марковские модели позволяют вычислять все основные показатели надежности, как точечные, так и интервальные, например, вероятность безотказной работы (отказа) на интервале времени (0,t), средняя наработка до отказа.
3. Вычислительные мощности современных компьютеров позволяют находить численное решение систем дифференциальных и алгебраических уравнений большой размерности, порождаемых марковскими графами. В самом деле, быстродействие, объемы оперативной памяти, средства динамического распределения памяти времени исполнения, присутствующие в современных языках программирования, позволяют легко решать системы уравнений с тысячами и более неизвестных даже на современных персональных компьютерах и ноутбуках, не говоря уже о крупномасштабных специализированных вычислительных машинах типа мейнфреймов (http://www.serverwatch.com).

Все же проблема размерности марковских моделей решена быть полностью не может. Актуальной является эргономическая часть проблемы, связанная с трудностью входного описания модели и определения ее параметров человеком. Построение марковского графа с тысячью вершин является чрезвычайно трудной задачей именно для человека. Здесь не помогают даже самые совершенные графические редакторы, внедренные в современное ПО анализа надежности. Поэтому при построении марковских моделей обычно не рассматривают все множество возможных состояний системы, а стараются или удалить некоторые состояния, исходя из условий

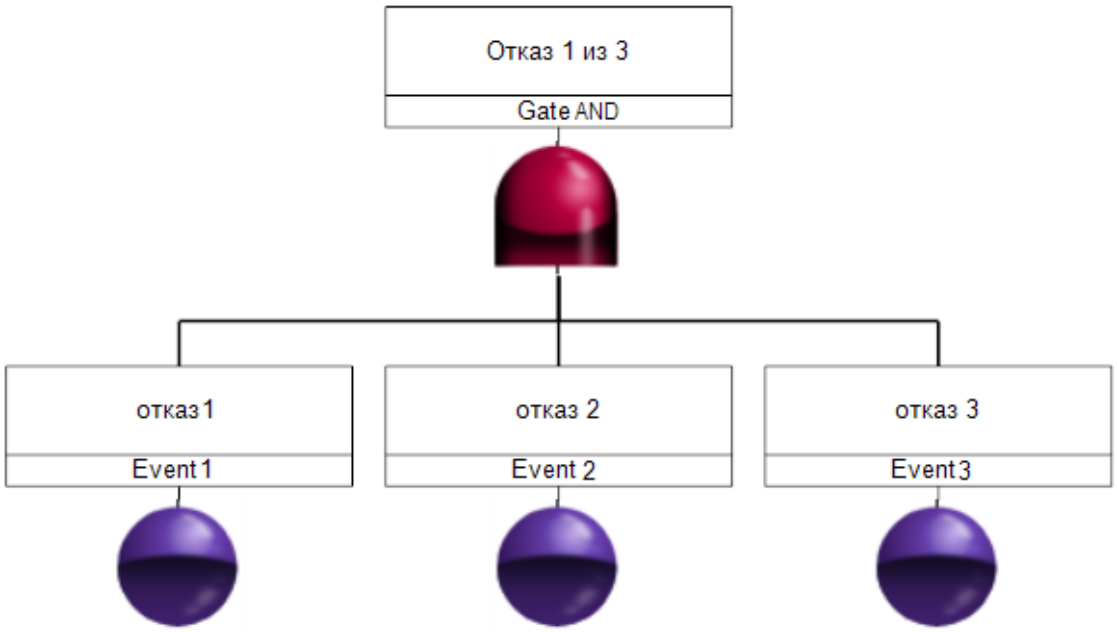
функционирования системы, и/или укрупнить (объединить) некоторые группы состояний в одно. Поэтому данный раздел будет посвящен изучению формальных правил укрупнения состояний марковской модели.



а). марковская модель.



б). блок-схема надежности



в). дерево отказов.

Рис.5.3. Модели надежности системы “1 из 3” из разнонадежных элементов.

Укрупнение состояний марковского процесса может быть точным или приближенным. Исследуем условия реализации точного укрупнения и продемонстрируем технику объединения состояний на конкретном примере. Построим марковскую модель надежности *дублированной системы из разнонадежных элементов* с интенсивностью отказов λ_1, λ_2 и интенсивностью

восстановления μ_1, μ_2 соответственно (рис.5.4). Здесь 0 –исправное состояние, 1 и 2 – работоспособные состояния одиночного отказа, 3 – отказ системы.

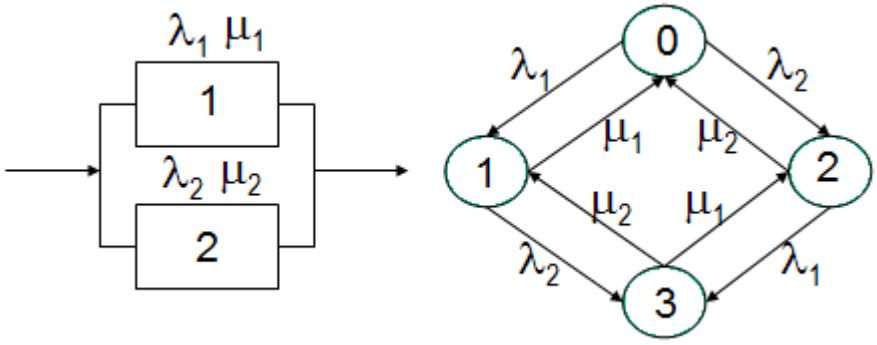


Рис.5.4. Марковский граф дублированной системы из разнонадежных элементов.

Система дифференциальных уравнений относительно состояний марковского процесса имеет вид

$$\begin{aligned} P_0'(t) &= -(\lambda_1+\lambda_2)P_0(t)+\mu_1 P_1(t)+\mu_2 P_2(t) \\ P_1'(t) &= \lambda_1 P_0(t)-(\lambda_2+\mu_1)P_1(t)+\mu_2 P_3(t) \\ P_2'(t) &= \lambda_2 P_0(t)-(\lambda_1+\mu_2)P_2(t)+\mu_1 P_3(t) \\ P_3'(t) &= \lambda_2 P_1(t)+\lambda_1 P_2(t)-(\mu_1+\mu_2)P_3(t) \end{aligned} \quad . \tag{5.30}$$

Начальные условия: $P_0(0)=1$; $P_1(0)=P_2(0)=P_3(0)=0$.

Прямое преобразование Лапласа от системы дифференциальных уравнений (5.30):

$$\begin{aligned} sP_0(s)-1 &= -(\lambda_1+\lambda_2)P_0(s)+\mu_1 P_1(s)+\mu_2 P_2(s) \\ sP_1(s) &= \lambda_1 P_0(s)-(\lambda_2+\mu_1)P_1(s)+\mu_2 P_3(s) \\ sP_2(s) &= \lambda_2 P_0(s)-(\lambda_1+\mu_2)P_2(s)+\mu_1 P_3(s) \\ sP_3(s) &= \lambda_2 P_1(s)+\lambda_1 P_2(s)-(\mu_1+\mu_2)P_3(s) \end{aligned} \tag{5.31}$$

Корни характеристического уравнения $|Q-sE|=0$, где Q – инфинитезимальная матрица, E-единичная матрица, равны: $S_1=0$; $S_2=-(\lambda_1+\mu_1)$; $S_3=-(\lambda_2+\mu_2)$; $S_4=-(\lambda_1+\mu_1+\lambda_2+\mu_2)$. Обозначим $\beta=\lambda_1+\mu_1$, $\gamma=\lambda_2+\mu_2$, тогда $S_1=0$; $S_2=-\beta$; $S_3=-\gamma$; $S_4=-(\beta+\gamma)$.

Далее, разлагая выражения для $P_i(s)$ на простые дроби и обращая их по стандартным формулам обратного преобразования Лапласа, получаем ответ:

$$P_0(t)=\frac{1}{\beta\cdot\gamma}(\mu_1\mu_2+\lambda_1\mu_2 e^{-\beta t}+\lambda_2\mu_1 e^{-\gamma t}+\lambda_1\lambda_2 e^{-(\beta+\gamma)t})$$

$$P_1(t)=\frac{1}{\beta\cdot\gamma}(\lambda_1\mu_2-\lambda_1\mu_2 e^{-\beta t}+\lambda_1\lambda_2 e^{-\gamma t}-\lambda_1\lambda_2 e^{-(\beta+\gamma)t}) \tag{5.32}$$

$$P_2(t) = \frac{1}{\beta \cdot \gamma}(\lambda_2\mu_1 + \lambda_1\lambda_2 e^{-\beta t} - \mu_1\lambda_2 e^{-\gamma t} - \lambda_1\lambda_2 e^{-(\beta+\gamma)t})$$

$$P_3(t) = 1 - \sum_{i=0}^{2} P_i(t) = \frac{\lambda_1\lambda_1}{\beta \cdot \gamma}(1 - e^{-\beta t} - e^{-\gamma t} + e^{-(\beta+\gamma)t})$$

Из (5.32) получаем выражение для нестационарного коэффициента готовности дублированной системы с двумя разными элементами:

$$K_г(t) = \sum_{i=1}^{2} P_i(t) \tag{5.33}$$

Стационарные вероятности состояний равны:

$$P_0 = \frac{\mu_1\mu_2}{\beta \cdot \gamma}; \quad P_1 = \frac{\lambda_1\mu_2}{\beta \cdot \gamma}; \quad P_2 = \frac{\lambda_2\mu_1}{\beta \cdot \gamma}; \quad P_3 = 1 - \sum_{i=0}^{2} P_i = \frac{\lambda_1\lambda_1}{\beta \cdot \gamma}. \tag{5.34}$$

Стационарный коэффициент готовности системы:

$$K_г = \frac{\mu_1\mu_2 + \lambda_1\mu_2 + \lambda_2\mu_1}{(\lambda_1 + \mu_1)(\lambda_2 + \mu_2)} \tag{5.35}$$

Попробуем сократить пространство состояний модели, объединив два состояния 1 и 2 в одно. Это будет соответствовать ситуации, когда один элемент работает, а другой отказал и восстанавливается, то есть мы не будем различать какой из элементов работает, а какой отказал (рис.5.5). Но если интенсивности отказов и восстановлений каждого элемента разные, то свойство марковости будет при таком укрупнении нарушено! Если в обобщенное (укрупненное) состояние переход происходит при отказе элемента 1, то выход будет связан с отказом элемента 2 или с восстановлением элемента 1. В случае попадания в него при отказе элемента 2 – все наоборот. Для марковского же процесса неважно как система попадает в состояние, из которого в данный момент стартует. Налицо нарушение свойства отсутствия последействия – имеет значение прошлое и точно написать интенсивности выхода из укрупненного состояния нельзя. В этом случае можно построить приближенную укрупненную модель, показанную на рис.5.6. Эквивалентные интенсивности переходов $\lambda_э$ и $\mu_э$ приближенной модели рассчитываются по формулам

$$\lambda_э = \lambda_2 \frac{P_1}{P_1 + P_2} + \lambda_1 \frac{P_2}{P_1 + P_2} \tag{5.36}$$

$$\mu_э = \mu_1 \frac{P_1}{P_1 + P_2} + \mu_2 \frac{P_2}{P_1 + P_2} \tag{5.37}$$

Здесь P_1 и P_2 рассчитываются по формулам (5.34), $\frac{P_1}{P_1 + P_2}$ - есть стационарная условная вероятность отказа первого элемента при условии, что откажет либо первый, либо второй, $\frac{P_2}{P_1 + P_2}$ - стационарная условная вероятность отказа второго элемента при условии, что откажет либо первый, либо второй. Точность приближения исходного (неукрупненного) процесса укрупненному зависит от соотношения интенсивностей отказов и восстановления. Чем большая разница между λ_i и μ_i, тем точнее приближение.

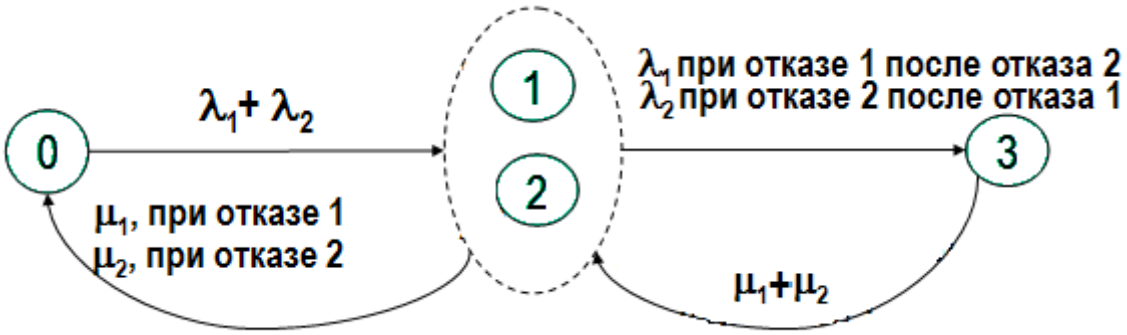


Рис.5.5. Попытка укрупнения состояний однократного отказа марковской модели дублированной системы из разных элементов.

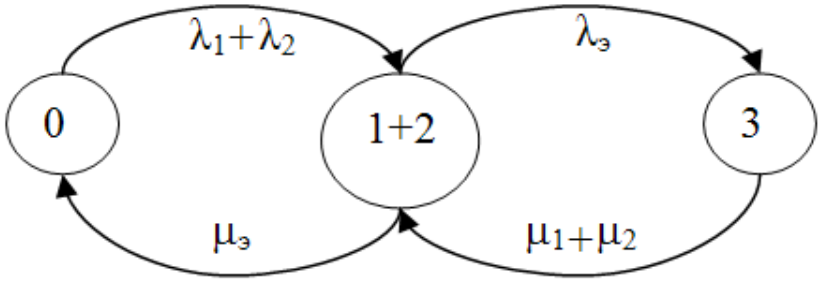


Рис.5.6. Приближенное укрупнение состояний однократного отказа марковской модели дублированной системы из разных элементов.

В подавляющем большинстве случаев резервированные системы формируются из одинаковых элементов. Рассмотрим дублированную систему с равнонадежными элементами ($\lambda_1 = \lambda_2$ и $\mu_1 = \mu_2$). Для модели этой системы (рис.5.7) интенсивности выхода из укрупненного состояния одинаковы и не зависят от того, каким образом мы в него попали. В этом случае укрупнение корректно и не нарушает свойство марковости.

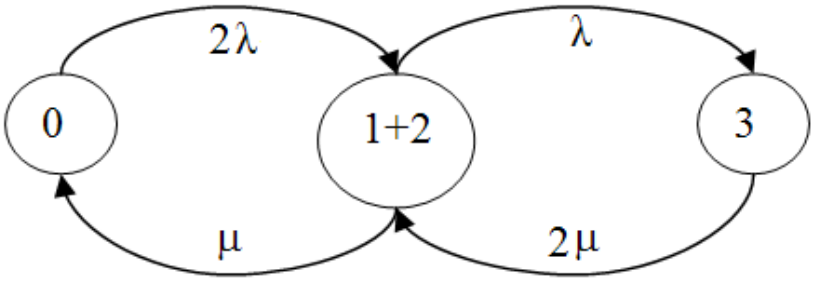


Рис.5.7. Точное укрупнение состояний однократного отказа марковской модели дублированной системы из одинаковых элементов.

Итак, точное укрупнение состояний марковской модели можно проводить при выполнении следующих условий:

1. Переходы из каждого из укрупняемых состояний возможны лишь в одни и те же состояния, т.е., если из одного из состояний, укрупняемых в одно, есть переходы в некоторое подмножество других состояний, то из других состояний, укрупняемых в одно, должны быть переходы в это же подмножество состояний.
2. Интенсивности выхода из состояний, укрупняемых в одно, должны быть одинаковыми

При соблюдении условий 1 и 2 необходимо руководствоваться следующими правилами:

1. Интенсивность перехода в укрупненное состояние равна сумме интенсивностей переходов в каждое из укрупняемых состояний.
2. Интенсивности выхода из укрупненного состояния равны интенсивностям выхода из одного из укрупняемых состояний.

В соответствии с перечисленными правилами проведем укрупнение состояний марковской модели дублированной восстанавливаемой системы с резервным элементом, работающим в облегченном режиме (рис.6). Интенсивность отказов облегченного резерва = $\alpha\lambda$ ($0 \le \alpha \le 1$).

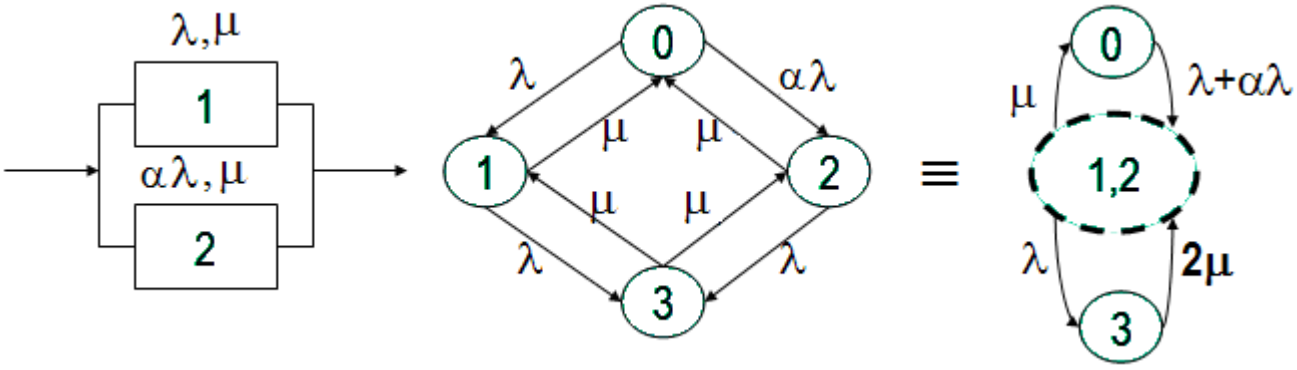


Рис.5.8. Марковская модель дублированной системы с облегченным резервом.

Система дифференциальных уравнений:

$$\begin{aligned} P_0'(t) &= -(\lambda + \alpha\lambda)P_0(t) + \mu P_1(t) + \mu P_2(t) \\ P_1'(t) &= \lambda P_0(t) - (\lambda + \mu)P_1(t) + \mu P_3(t) \\ P_2'(t) &= \alpha\lambda P_0(t) - (\lambda + \mu)P_2(t) + \mu P_3(t) \\ P_3'(t) &= \lambda P_1(t) + \lambda P_2(t) - 2\mu P_3(t) \end{aligned} \qquad (5.38)$$

В этой модели можно укрупнить состояния 1 и 2. Система дифференциальных уравнений после укрупнения имеет вид

$$\begin{aligned} P_0'(t) &= -(\lambda + \alpha\lambda)P_0(t) + \mu P_{1,2}(t) \\ P_{1,2}'(t) &= (\lambda + \alpha\lambda)P_0(t) - (\lambda + \mu)P_{1,2}(t) + P_3(t)2\mu \\ P_3'(t) &= \lambda P_{1,2}(t) - 2\mu P_3(t) \end{aligned} \qquad (5.39)$$

Отметим, что система (5.39) могла быть получена формально в результате сложения уравнений относительно состояний 1 и 2 ($P_{1,2}'(t) = P_1'(t) + P_2'(t)$). Система (5.39) полностью идентична (5.38) (в смысле одинаковости решений и определения всех показателей надежности), что подтверждает полную идентичность исходного и укрупненного графов переходов (рис.5.8).

Достаточно часто повышение надежности обеспечивается комбинацией нагруженного и ненагруженного резерва. В этом случае говорят, что в системе реализовано гибридное резервирование. Построим марковскую модель надежности системы с гибридным резервом, в которой имеется рабочий блок, состоящий из трех одинаковых параллельно работающих элементов. Кроме того, имеется два ненагруженных резервных элемента, подключаемых на место отказавших элементов рабочего блока (рис.5.9). Восстановление работоспособности отказавших элементов осуществляется двумя ремонтными бригадами. После попадания в отказовое состояние запуск системы в работу осуществляется только после того, как будет полностью восстановлен рабочий блок (отремонтированы все три элемента).

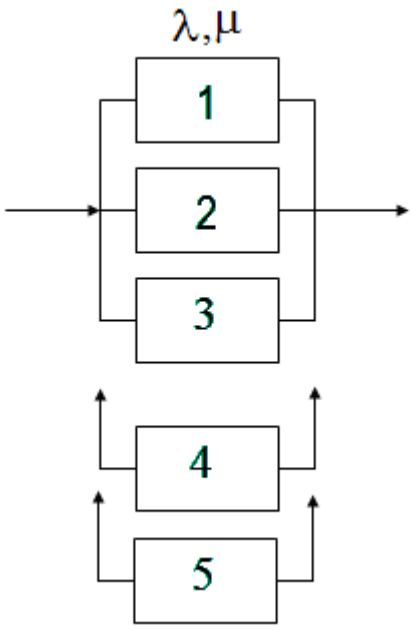


Рис. 5.9. Система с гибридным резервированием

Марковский граф системы показан на рис.5.10. Каждому состоянию (вершине графа) приписан код – N,K,W, где N – количество работоспособных элементов рабочего блока, K – количество работоспособных ненагруженных резервных элементов, W – количество элементов, ожидающих ремонта. Буква G означает исправное состояние, буква F – отказ.

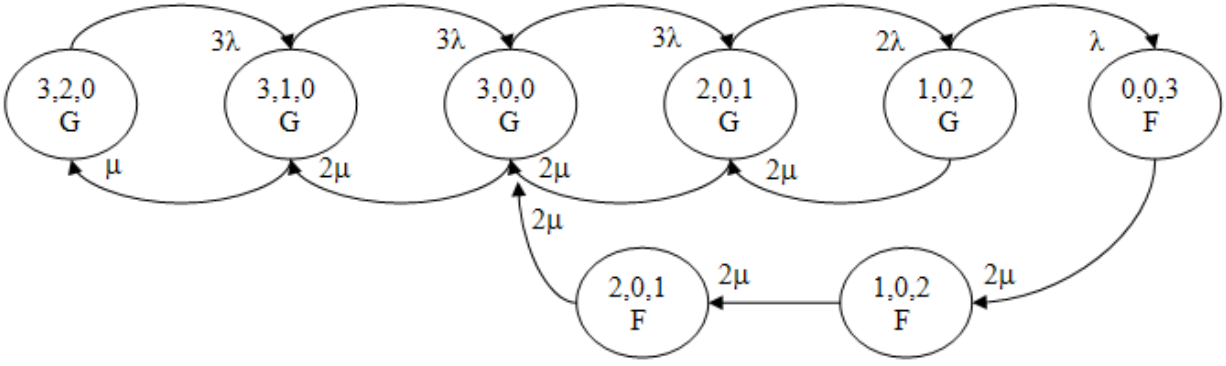


Рис.5.10. Марковский граф системы с гибридным резервированием.

В построенной марковской модели учтены следующие особенности:

– ненагруженное резервирование
– ограничение на число ремонтных бригад
– специальная стратегия восстановления системы

Ни одна из перечисленных особенностей не могла бы быть учтена в логико-вероятностных моделях. За счет укрупнения состояний одинаковой кратности отказов рабочего блока размерность модели снижена.

5.7. Исследование надежности сложных, восстанавливаемых систем на марковских моделях.

Продолжим исследовать надежность систем, для корректного моделирования которых необходимо применять марковские процессы. Рассмотрим три примера

I. Расчет коэффициента готовности системы с зависимым функционированием элементов.

II. Построение модели надежности системы с встроенным контролем и восстановлением, отложенным до окончания выполнения задания.

III. Расчет стационарных показателей параметра потока отказов и среднего времени работы между отказами для резервированных структур с восстановлением элементов.

I. Последовательная, восстанавливаемая система с зависимым функционированием элементов.

Рассмотрим систему, состоящую из n последовательно в смысле надежности соединенных элементов. Пусть при отказе любого одного элемента система отключается, т.е. функционирование прекращается для восстановления этого элемента. Это самое обычное условие эксплуатации. Например, телевизор состоит из модулей питания, строчной развертки, кадровой развертки, блока цвета, усилителя звука, высокочастотного усилителя сигнала….Отказ любого из модулей приводит к отказу телевизора, а для восстановления (ремонта) надо обязательно телевизор выключить. Это означает, что во время ремонта отказавшего модуля отказы других модулей или невозможны или их вероятностью можно пренебречь! Тогда число состояний марковской модели системы будет равно n+1, а не 2^n (рис.5.11).

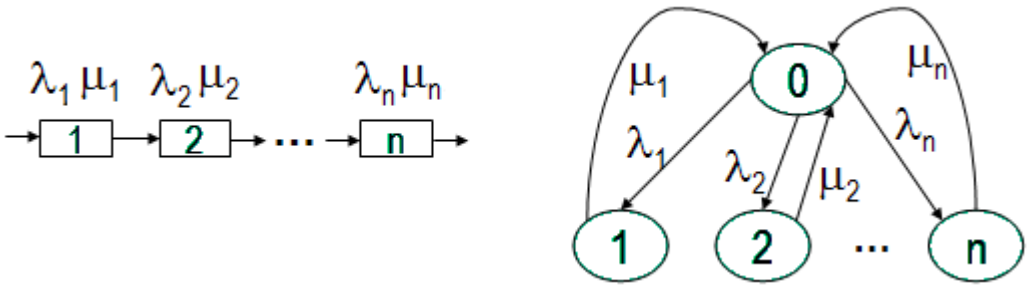


Рис.5.11. Марковская модель системы с зависимым функционированием элементов.

Выражение для стационарного коэффициента готовности находится из системы уравнений:

$$\begin{aligned}
&\lambda_1 P_0 - \mu_1 P_1 = 0\\
&\lambda_2 P_0 - \mu_2 P_2 = 0\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
&\lambda_{n-1} P_0 - \mu_{n-1} P_{n-1} = 0\\
&P_0 + P_1 + \ldots + P_{n-1} + P_n = 1
\end{aligned} \qquad (5.40)$$

Решая (5.40), получаем

$$P_j = \frac{\lambda_j}{\mu_j} P_0, \qquad (5.41)$$

То есть выражаем стационарную вероятность отказа i-го элемента (i=1, 2,…n) через вероятность исправного состояния P_0.

Подставив (5.41) в последнее уравнение системы (5.40), получаем выражение для стационарного коэффициента готовности системы

$$K_{г.стац.} = P_0 = \frac{1}{1+\sum_{j=1}^{n} \frac{\lambda_j}{\mu_j}} \qquad (5.42)$$

Выразим стационарный коэффициент готовности системы $K_{г.стац.}$ через коэффициенты готовности ее элементов K_j, где $K_j = \frac{\mu_j}{\lambda_j + \mu_j}$. Тогда $\mu_j = \frac{\lambda_j K_j}{1-K_j}$, откуда получаем

$$K_{г.стац.} = P_0 = \frac{1}{1+\sum_{j=1}^{n} \left(\frac{1}{K_j} - 1\right)} \qquad (5.43)$$

Пусть n=3 K_1=0,61, K_2=0,72, K_3=0,63. Тогда из (5.43) $K_{г.стац.}$=0,38

Обычная ошибка состоит в вычислении коэффициента готовности такой системы умножением коэффициентов готовности элементов: $K_{г.стац.} = K_1 K_2 K_3 = 0{,}28$, что дает неверный результат. Это объясняется тем, что перемножать коэффициенты готовности элементов для получения оценки показателя готовности системы можно лишь при независимости элементов! В данном случае имеется зависимость - при отказе одного из элементов другие не отказывают. Рассчитывать надо по выражению (5.43), полученному с помощью марковского моделирования.

II. Система с встроенным контролем и восстановлением, отложенным до окончания выполнения задания.

Оперативный встроенный контроль (BIT – built-in-test) технического состояния элементов и систем, контроль правильности выполнения функций позволяет в полной мере реализовать возможности резервирования, своевременно принимать меры по реконфигурации систем и изменению режимов функционирования, обеспечивая, тем самым, свойство отказобезопасности системы в целом. Однако контроль не является идеальным – во-первых, он сам отказывает, а, во-вторых, не абсолютно все отказы им распознаются. Поэтому для обеспечения высоких показателей надежности и безопасности требуется проведение тщательного «надежностного» анализа систем с учетом характеристик контроля. Одной из важнейших таких характеристик является *полнота контроля,* характеризующая долю отказов объекта контроля, обнаруживаемых при контроле работоспособности. В общем случае качество контроля определяется перечнем элементов (модулей), отказы которых выявляются контролем. Поэтому одной из характеристик полноты контроля может быть отношение числа контролируемых элементов к общему числу элементов рассматриваемого объекта контроля (например, в процентах). Однако для совместного моделирования «надежностного поведения» объекта и средств контроля желательно задавать полноту контроля как некоторый вероятностный показатель или как отношение характеристик надежности (отказа) контролируемых элементов ко всем элементам. Целесообразность такого задания объясняется тем, что при моделировании «надежностного поведения» анализируемого объекта можно будет «разбить» общий поток отказов на две составляющие – выявляемые контролем отказы и скрытые отказы. Полноту контроля в этом случае можно определить как условную вероятностью контролируемого отказа, при условии, что отказ произошел:

$$\eta = \mathrm{Prob}\{\text{контролируемый отказ} / \text{отказ произошел на } (0,t)\} = \frac{1 - e^{-\int_0^t \Lambda_к(t)dt}}{1 - e^{-\int_0^t \Lambda(t)dt}}, \qquad (5.44)$$

где Λ – суммарная интенсивность отказов объекта контроля (контролируемые + неконтролируемые); $\Lambda_к$ - суммарная интенсивность контролируемых отказов.

Проведя усреднение интенсивностей отказов на интервале (0,t), получаем:

$$\eta = \frac{1 - e^{-\lambda_{к.усp.}t}}{1 - e^{-\lambda_{усp.}t}} = \frac{\lambda_{к.усp.}}{\lambda_{усp.}}, \qquad (5.45)$$

где $\lambda_{\text{ср.}} = \frac{1}{t}\int_0^t \lambda(t)dt$ и для реальных высоконадежных систем $\lambda_{\text{ср}} t << 1$.

Общие выражения (5.44, 5.45) для полноты контроля при экспоненциальных распределениях наработки до отказа элементов наиболее удобно задавать как отношение суммарной интенсивности отказов контролируемых элементов к суммарной интенсивности отказов всех элементов, т.е.

$$\eta = \frac{\sum_{j \in K} \lambda_j}{\sum_{i=1}^{n} \lambda_i}, \qquad (5.46)$$

где η - полнота контроля; n –количество элементов объекта контроля; К - подмножество контролируемых элементов; λ_i – интенсивность отказа элемента. В этом случае определяемая полнота является условной стационарной вероятностью контролируемого отказа, при условии, что отказ произошел.

Построим модель надежности дублированной системы с встроенным контролем и восстановлением. Средства контроля будем считать абсолютно надежными, а его качество будем оценивать показателем полноты согласно (5.46). Восстановление работоспособности элементов происходит лишь при возникновении отказов, выявляемых BIT. Тогда дублированная система может быть представлена как параллельное соединение двух каналов, каждый из которых состоит из контролируемой и восстанавливаемой и неконтролируемой и невосстанавливаемой частей (рис.5.12). Интенсивности отказов контролируемой и неконтролируемой частей равны $\eta\lambda$ и $(1-\eta)\lambda$ соответственно.

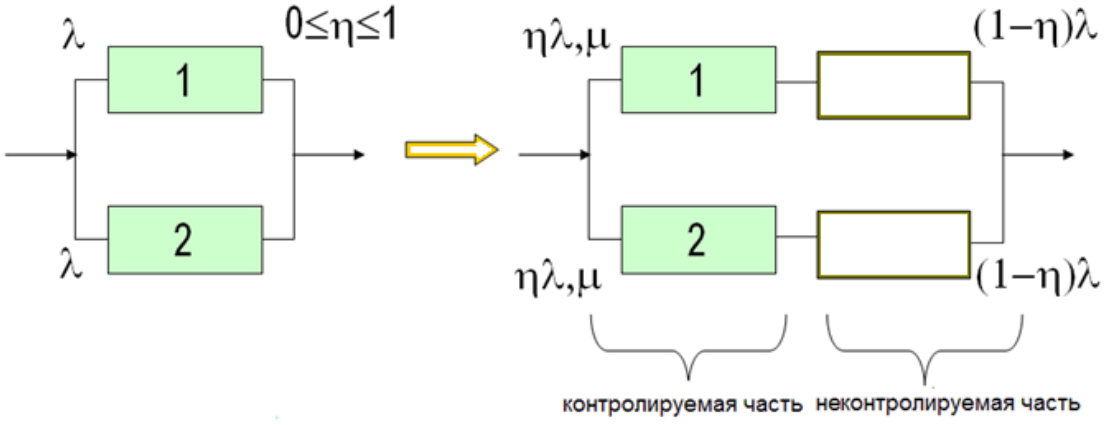


Рис.5.12. Дублированная система с восстановлением и неполным контролем

Отразим в модели циклический режим работы системы. Цикл состоит из выполнения задания и восстановительных работ, которые проводятся лишь после выполнения задания. Режим типичен для транспортных систем. Марковская модель надежности системы показана на рис.5.13.

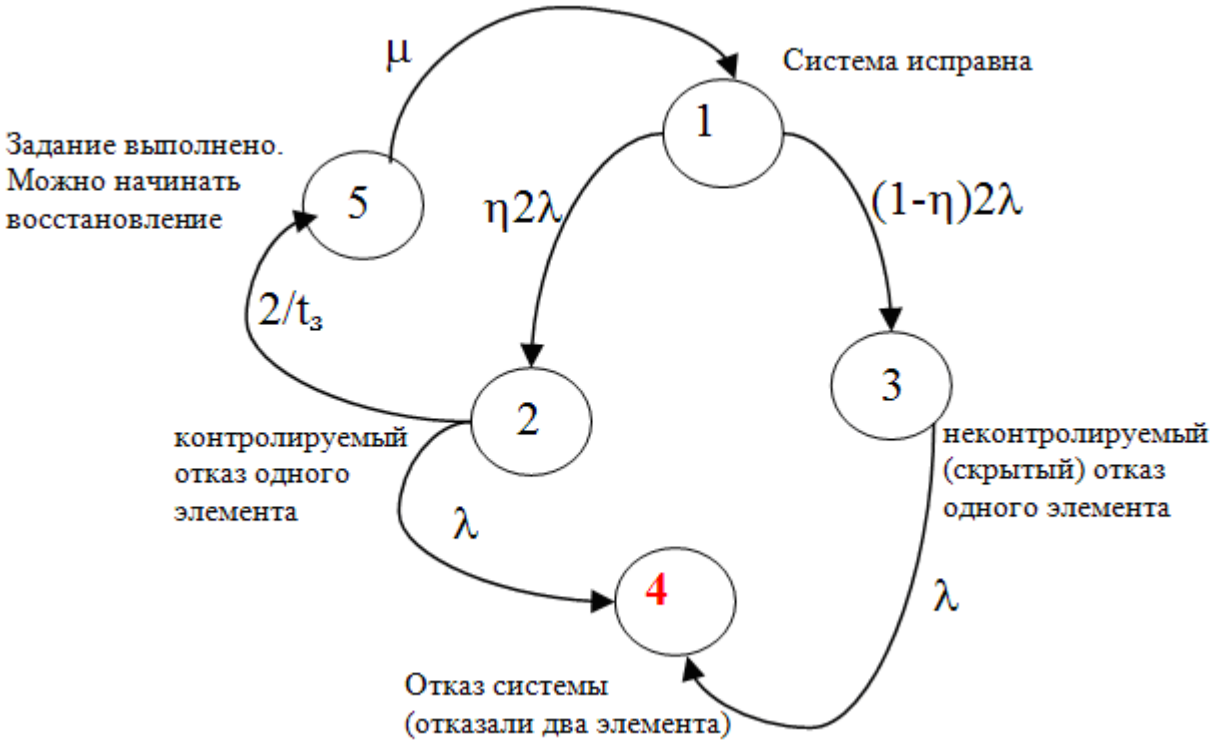


Рис.5.13. Марковская модель дублированной системы с восстановлением и неполным контролем. Циклический режим работы.

Для определения интенсивности перехода из состояния 2 в состояние 5 вычислим среднее время наступления отказа при условии, что отказ наступил на интервале времени выполнения задания (0,tз) $T_{ср/tз}$:

$$T_{ср/tз} = M\{t/t<t_з\} = \int_0^{t_з} t f(t/t<t_з)dt = \int_0^{t_з} t dF(t/t<t_з) = \int_0^{t_з} t dP(\xi<t/\xi<t_з) = \int_0^{t_з} t d\frac{F(t)}{F(t_з)} =$$

$$\frac{\int_0^{t_з} P(t)dt - P(t_з)t_з}{1-P(t_з)} = \frac{\frac{1}{\lambda} - e^{-\lambda t_з}(t_з + \frac{1}{\lambda})}{1-e^{-\lambda t_з}}, \qquad (5.47)$$

где M{t}, F(t), f(t) – есть соответственно математическое ожидание, функция распределения и плотность распределения случайного времени возникновения отказа.

Для значений интенсивности отказа λ = 1e-3 на рис. 5.14 построен график, демонстрирующий тот факт, что если $t_з << 1/\lambda = T_{ср}$, то $T_{ср/tз} \approx t_з/2$. При $t_з > T_{ср}$ $T_{ср/tз} \rightarrow T_{ср}$. Поэтому для систем, время выполнения задания которых не превышает нескольких десятков часов, вполне корректным является допущение о том, что отказ происходит на середине интервала $(0,t_з)$, а следовательно интенсивность перехода из 2 в 5 равна $2/t_з$.

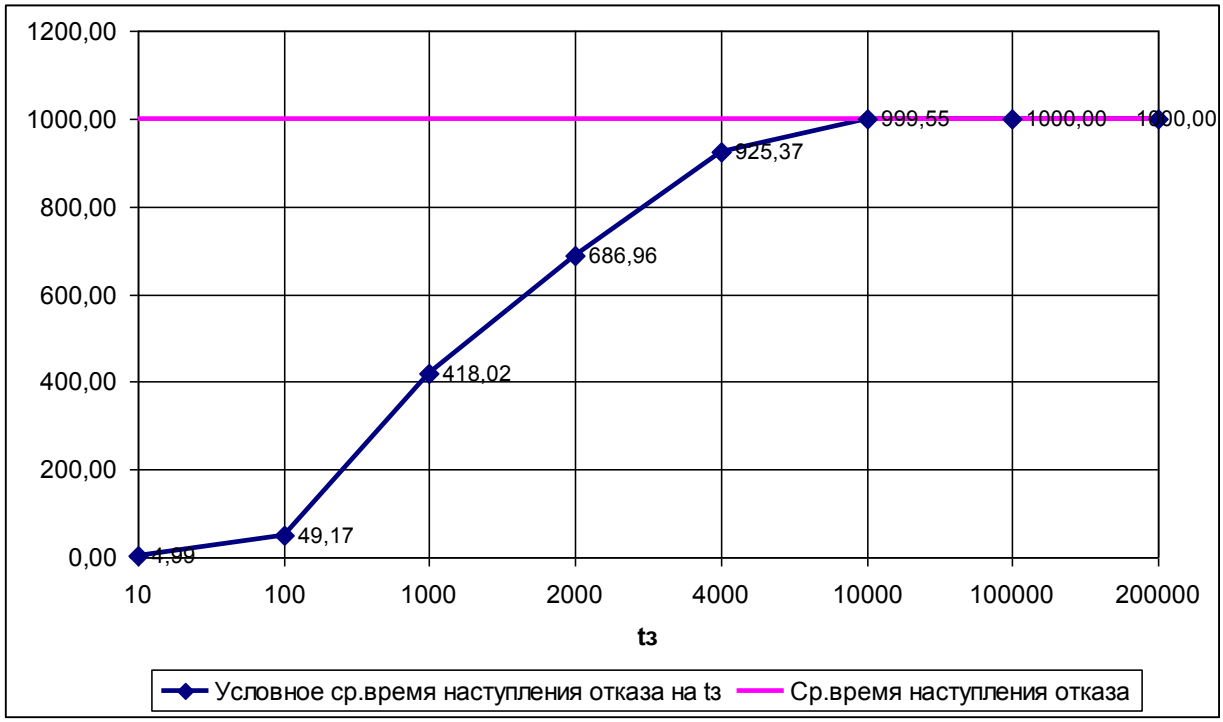


Рис.5.14. Условное среднее время возникновения отказа на интервале времени выполнения задания

III. Расчет стационарных показателей параметра потока отказов и среднего времени работы между отказами для резервированных схем с восстановлением элементов

Стационарный режим работы восстанавливаемой системы, моделируемой однородным марковским процессом без поглощающих состояний, может быть охарактеризован рядом специальных показателей. Два важнейших показателя - стационарный коэффициент готовности (5.27)] и стационарный коэффициент простоя (5.28) были рассмотрены в разделе 5.5. Здесь мы рассмотрим два других стационарных показателя – параметр потока отказов и средняя наработка между отказами и обсудим связь между этими показателями.

В марковских моделях надежности параметр потока отказов определяется из следующего выражения:

$$\omega(t) = \sum_{i \in G_+} P_i(t) \cdot \sum_{j \in G_-} \lambda_{ij} \ . \qquad (5.48)$$

Для стационарного участка

$$\omega_{стац} = \sum_{i \in G_+} P_i \cdot \sum_{j \in G_-} \lambda_{ij} \ , \qquad (5.49)$$

где G_+ - множество состояний работоспособности системы, G_- - множество состояний неработоспособности системы.

Параметр потока отказов является производной по времени от среднего числа отказов. Поэтому, зная параметр потока отказов, можно вычислить среднее число отказов на интервале времени (t_1,t_2):

$$N_{ср}(t_1, t_2) = \int_{t_1}^{t_2} \omega(t)dt \qquad (5.50)$$

Для стационарного участка

$$N_{ср}(t_1, t_2) = \omega_{стац} \cdot (t_2 - t_1) \qquad (5.51)$$

Параметр потока отказов часто используется в моделях анализа безопасности, где необходимо оценить потери, связанные с переходами в состояния отказов.

Если рассматривать стационарный участок, то параметр потока отказов, характеризующий частоту возникновения событий отказа в восстанавливаемых системах, обратно пропорционален среднему времени между отказами (строгое доказательство этого положения приведено в теории восстановления [14]). Поэтому

$$T_{ср.между} = \frac{1}{\omega_{стац.}}. \qquad (5.52)$$

Для обозначения показателя среднего времени между отказами в западной литературе используется аббревиатура MTBF (Mean Time Between Failures), которая в настоящее время стала применяться и отечественными специалистами. Здесь необходимо отметить, что в отечественной литературе присутствует показатель *средней наработки* между отказами ($T_{ср.}$) (рис.5.15). Связь между этими показателями следующая:

$$T_{ср.между} \equiv MTBF = T_{ср.} + T_в \ , \qquad (5.53)$$

где $T_в$ – среднее время восстановления.

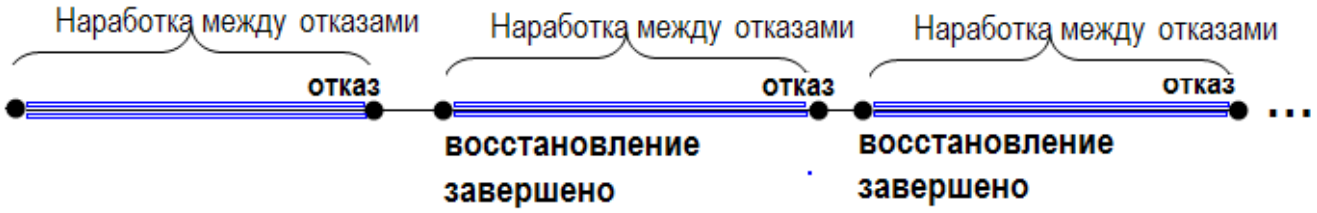


Рис.5.15. Стационарный участок работы восстанавливаемой системы.

С учетом того, что $K_{г.стац.} = \dfrac{T_{ср.}}{T_{ср.} + T_{в}}$ и выражения (5.49) получим

$$T_{ср} = K_{г.стац.} \cdot T_{ср.между} = \frac{K_{г.стац.}}{\omega} = \frac{\sum\limits_{i \in G_+} P_i}{\sum\limits_{i \in G_+} P_i \cdot \sum\limits_{j \in G_-} \lambda_{ij}}. \qquad (5.54)$$

Для восстанавливаемого элемента параметр потока отказов равен

$$\omega_{стац.} = \frac{\mu}{\lambda + \mu} \cdot \lambda = \frac{1}{\frac{1}{\lambda} + \frac{1}{\mu}} \qquad (5.55)$$

В главе 2 были выведены формулы для вычисления коэффициента готовности основных схем нагруженного резервирования.

Рассмотрим общую модель резервированных схем из идентичных элементов, показанную на рис.5.16. Модель пригодна для анализа надежности следующих схем:

1. дублированной схемы с нагруженным резервом
2. дублированной схемы с ненагруженным резервом
3. мажоритарной схемы

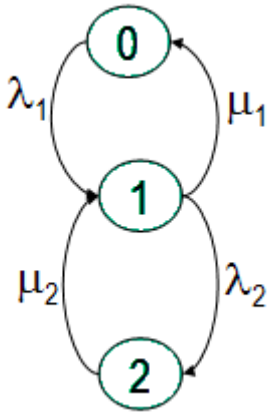


Рис.5.16. Общая марковская модель резервированных схем.

Стационарные вероятности состояний определяются по формулам:

$$P_0 = \frac{\mu_1\mu_2}{\lambda_1\lambda_2 + \lambda_1\mu_2 + \mu_1\mu_2}$$
$$P_1 = \frac{\lambda_1\mu_2}{\lambda_1\lambda_2 + \lambda_1\mu_2 + \mu_1\mu_2} \qquad (5.56)$$
$$P_2 = \frac{\lambda_1\lambda_2}{\lambda_1\lambda_2 + \lambda_1\mu_2 + \mu_1\mu_2}$$

Исходя из выражений (5.52)-(5.54) и учитывая, что $K_{стац} = P_0 + P_1$, получены расчетные формулы для основных показателей надежности резервированных схем (см. таблицу 5.3). Вывод формул для показателя средней наработки до отказа осуществлялся согласно (5.23,5.24).

Таблица 5.3. Основные показатели надежности резервированных схем.

Схема	Стратегия восстановления	Параметры Модели	Стационарный коэффициент готовности	Параметр потока отказов	Средняя наработка между отказами	Среднее время работы до отказа
Дублированная схема с нагруженным резервом	Неограниченное восстановление (две бригады)	$\lambda_1 = 2\lambda$, $\lambda_2 = \lambda$, $\mu_1 = \mu$, $\mu_2 = 2\mu$.	$\frac{2\lambda\mu + \mu^2}{(\lambda + \mu)^2}$	$\frac{2\lambda^2\mu}{(\lambda + \mu)^2}$	$\frac{\mu + 2\lambda}{2\lambda^2}$	$\frac{\mu + 3\lambda}{2\lambda^2}$
Дублированная схема с нагруженным резервом	Ограниченное восстановление (одна бригады)	$\lambda_1 = 2\lambda$, $\lambda_2 = \lambda$, $\mu_1 = \mu$, $\mu_2 = \mu$.	$\frac{2\lambda\mu + \mu^2}{2\lambda^2 + 2\lambda\mu + \mu^2}$	$\frac{2\lambda^2\mu}{2\lambda^2 + 2\lambda\mu + \mu^2}$	$\frac{\mu + 2\lambda}{2\lambda^2}$	$\frac{\mu + 3\lambda}{2\lambda^2}$
Дублированная схема с ненагруженным резервом	Неограниченное восстановление (две бригады)	$\lambda_1 = \lambda$, $\lambda_2 = \lambda$, $\mu_1 = \mu$, $\mu_2 = 2\mu$.	$\frac{2\mu(\mu + \lambda)}{\lambda^2 + 2\lambda\mu + 2\mu^2}$	$\frac{2\lambda^2\mu}{\lambda^2 + 2\lambda^2 + 2\mu^2}$	$\frac{\mu + \lambda}{\lambda^2}$	$\frac{\mu + 2\lambda}{\lambda^2}$
Мажоритарная структура “2 из 3”	Неограниченное восстановление (две бригады)	$\lambda_1 = 3\lambda$, $\lambda_2 = 2\lambda$, $\mu_1 = \mu$, $\mu_2 = 2\mu$.	$\frac{\mu^2 + 3\lambda\mu}{\mu^2 + 3\lambda\mu + 6\lambda^2}$	$\frac{6\lambda^2\mu}{\mu^2 + 3\lambda\mu + 6\lambda^2}$	$\frac{\mu + 3\lambda}{6\lambda^2}$	$\frac{\mu + 5\lambda}{6\lambda^2}$

5.8. Марковские процессы с доходами

Марковские надежностные модели функционирования и отказов сложных систем позволяют учитывать практически любые зависимости и условия возникновения отказов, условия изменения характеристик. Единственным требованием является необходимость экспоненциальных распределений всех учитываемых факторов, переменных модели. Отсутствие последействия экспоненциальных распределений приводит к относительной простоте формирования пространства состояний и графа переходов, системы уравнений для состояний. Сложность заключается лишь в быстром росте размерности модели при увеличении учитываемых факторов, переменных. Частично эту проблему можно решить укрупнением состояний с расчетом эквивалентных асимптотических интенсивностей выходов из укрупненного состояния.

Марковские процессы также могут быть использованы при моделировании многоуровневых систем и вычислении различных показателей эффективности их функционирования, в частности, интегральной выработки, интегрального дохода, коэффициента сохранения эффективности. В Институте Проблем Управления РАН в лаборатории №5 в середине 80-х годов были разработаны для моделирования многоуровневых систем метод и алгоритмы вычисления показателей на основе марковских процессов с доходами [12,99]. Метод марковских процессов с доходами (МПД – метод) в некотором смысле обобщает методы марковских процессов с непрерывным временем и дискретным пространством состояний. Его применение позволяет вычислять ряд показателей, вычисление которых в обычных марковских процессах не может быть осуществлено впрямую. Формально, марковские процессы с доходами являются способом вычисления показателей по выражению (3.16), но не только интегральных, но и дифференциальных.

Рассмотрим применение марковских процессов с доходами (МПД) к вычислению показателей надежности и эффективности систем сложной структуры.

Математическое ожидание дохода H(t) удовлетворяет системе дифференциальных уравнений:

$$\frac{dH(t)}{dt}=\Lambda H(t)+R\,, \qquad (5.57)$$

где **H(t)** - вектор столбец математических ожиданий дохода;

$H^T(t) = (H_1(t), H_2(t), \ldots, H_n(t))$ – транспонированный вектор столбец; **n** - число состояний системы;

$H_i(t)$ - математическое ожидание дохода системы за время функционирования t, если в момент **t=0** система находилась в состоянии i;

Λ - матрица интенсивности переходов из i-го состояния в j-ое;

R - вектор столбец свободных членов

$$R_i = w_i + \sum_{j, j \neq i} \lambda_{ij} w_{ij} \ ;$$

w_{ij} $(i \neq j)$ -доход, получаемый в системе при переходе из i-го состояния в j-е;

w_i - доход в единицу времени, если система находится в состоянии i**.**

Здесь понятие доход - обобщающий термин. Это может быть какой-нибудь эффект, производительность, потери, затраты и т.п. Специальным выбором матрицы доходов $W=(w_{ij})$ достигается возможность вычисления большого спектра показателей надежности и эффективности (практически любых встречающихся в нормативно-технических документах). Перечислять здесь все виды матрицы доходов для всех показателей мы не будем, это можно посмотреть в [99].

Для примера укажем лишь некоторые:

1. Вероятность отказа Q системы за время t.

При вычислении Q(t) необходимо взять матрицу доходов W, у которой элементы столбца (столбцов), соответствующие состоянию (состояниям) отказа системы, равны единице, а все остальные элементы равны нулю. При этом состояния отказа надо сделать поглощающими, поскольку данный показатель характеризует поведение системы до первого попадания ее в состояние отказа. Вычисления проводятся по (5.57).

2. Средняя наработка до отказа Tср.

Матрица W должна иметь диагональные элементы w_i ,соответствующие работоспособным состояниям, равными единице, остальные - нулю. Состояния отказа необходимо сделать поглощающими. Так как этот показатель определяется на **(0, ∞)**, то уравнения (5.57) предельным переходом преобразуются в (5.58), и расчет выполняется по (5.58).

$$\Lambda \cdot H + R = 0 \, . \qquad (5.58)$$

3. Параметр потока отказов ω(t) *и среднее число отказов N(t)*

Параметр потока отказов ω(t) является дифференциальным показателем по отношению к интегральному показателю N(t) (среднему числу отказов на **(0,t))**. То есть ω(t) = dN(t)/dt и определяется в момент t. Вычисление ω(t) производится в два этапа. Сначала по (5.57) определяется N(t). В матрице W для этого необходимо положить элементы w_{ij} равные единице ($i \neq j$), если i - состояние работоспособности, а j - состояние отказа. Остальные элементы равны нулю. Затем полученный вектор N(t) подставляется в (5.57) и находят производную, равную в этом случае параметру потока отказов.

$$\frac{dH(t)}{dt} = \frac{dN(t)}{dt} = \omega(t) \ . \qquad (5.59)$$

В модели МПД разработано также вычисление следующих показателей надежности и эффективности (в том числе в многоуровневых моделях системы):

- среднее время восстановления
- интенсивность отказов системы в момент **t**
- дисперсия времени безотказной работы
- вероятность пребывания в момент времени t на i-ом уровне функционирования (в двухуровневой модели (работоспособность/отказ) этот показатель называется коэффициентом готовности/простоя)
- вероятность застать систему в момент времени t на i-ом уровне функционирования и не опустится ниже этого уровня за время τ от момента t (в двухуровневой модели этот показатель называется коэффициентом оперативной готовности)
- среднее число переходов с i-го на j-ый уровень работоспособности (в двухуровневой модели среднее число отказов/восстановлений)
- среднее суммарное время пребывания системы на i-ом уровне функционирования на интервале (0,t)
- математическое ожидание эффективности (уровня функционирования) в момент времени t
- математическое ожидание интегральной эффективности функционирования на интервале (0,t)
- усредненное на интервале (0,t) значение эффективности функционирования
- коэффициент сохранения эффективности на интервале функционирования (0,t**)**

Моделирование систем с применением марковских процессов с доходами позволило расширить перечень определяемых показателей надежности и дополнить его показателями эффективности.

Рассмотрим пример применения МПД-метода для анализа и обоснования требований объекта с защитой. Пример был разработан авторами в процессе выполнения работы по сравнению программных комплексов анализа надежности [30]. Рассматривается конфигурация технологический объект (ТО) + система защиты (СЗ) (рис. 5.17.). Система защиты состоит в свою очередь из устройства контроля (УК) и исполнительного механизма (ИМ).

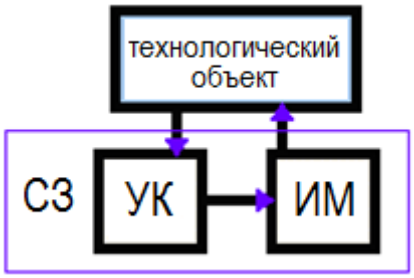


Рис. 5.17. Конфигурация технологический объект + система защиты

Рассмотрим более подробно работу и отказы в системе.

Подсистемы защиты предназначены для выработки управляющих воздействий на защищаемый объект (технологическое оборудование) с целью предотвращения развития нештатных отклонений в работе объекта и, в частности, перерастания отказов в аварию (здесь будем рассматривать только отклонения в работе объекта, связанные с отказами). Управляющие воздействия могут быть различными (например, изменение режима работы, снижение производительности). В некоторых случаях они реализуют отключение аварийно отказавших элементов и других элементов, связанных с первыми по технологической цепи. Тем самым предотвращается развитие событий, приводящих к аварии. Как правило, это бывает эквивалентно останову объекта, технологического процесса. Здесь будем рассматривать именно такой случай, но предлагаемый подход годится и для управляющих воздействий, приводящих к снижению производительности, изменению режима.

Функция противоаварийной защиты выполняется эпизодически, в момент возникновения аварийной ситуации, поэтому СЗ работает в ждущем временном режиме. Характер доходов в работоспособных состояниях и потерь в неработоспособных состояниях технологического объекта (ТО) предполагается следующим. Во-первых, в системе (в данном примере это ТО + СЗ) возможны четыре группы технических состояний (техническое состояние характеризуется наборами отказавших и работоспособных элементов модели (СЗ, ТО), видами и последовательностью возникновения отказов). Первая группа содержит такие технические состояния, в которых объект нормально функционирует и приносит удельный доход в единицу времени пребывания в этих состояниях (например, этим состояниям соответствует номинальная производительность ТО). Отметим, что в эту группу входят состояния со скрытым отказом (типа несрабатывания на требование) системы защиты. Вторая группа состояний характеризуется безаварийным остановом объекта. Потери здесь связаны только с простоем объекта; доход в этих состояниях либо равен нулю, либо отрицательный, если простой приводит к дополнительным потерям в единицу времени. Третья и четвертая группы состояний – аварийные отказы объекта двух видов. Переход в эту

группу состояний из состояний первой группы приносит единовременный ущерб (отрицательный доход) связанный с возникновением аварии (гибель людей, поломки оборудования, выбросы в атмосферу и т.п.). Таким образом, нормальное функционирование объекта сопровождается линейным ростом интегрального дохода пропорционально времени пребывания в первой группе состояний. Простои объекта в состояниях второй, третьей и четвертой групп ведут к сохранению достигнутого уровня интегрального дохода (при нулевых значениях удельных доходов в каждом из состояний этих групп) либо к его убыванию (при отрицательных значениях соответствующих удельных доходов) пропорционально времени пребывания в этих состояниях. При переходах между состояниями имеет место скачкообразное изменение (чаще уменьшение) интегрального дохода в тех случаях, когда с соответствующими переходами связаны единовременные доходы за каждый переход, Обычно эти доходы отрицательны, обусловлены затратами на восстановление последствий отказов, аварий, приобретение оборудования, ЗИП′а, штрафы, страховку и т.п.

Предположим, что все аварийные ситуации возникают только при отказах технологического оборудования. Пусть СЗ при возникновении распознаваемой ей аварийной ситуации мгновенно останавливает технологический процесс, производя необходимое управление оборудованием (например, отключение). Причем работоспособная СЗ с ″покрытием″ β ($0 \le \beta \le 1$) распознает аварийные ситуации. Отказы в СЗ, которые возникают на интервале нормального функционирования ТО, могут приводить к различным последствиям. Выделим отказы двух видов: скрытые отказы и ложные срабатывания. Скрытые отказы не приводят к срабатыванию защиты и не изменяют режим работы объекта. Они проявляются в виде несрабатывания защиты при возникновении аварийной ситуации, что влечет за собой аварию.

Параметры модели:

W_{ij} – потери от переходов в состояния аварии;

β - “покрытие”- доля распознаваемых аварийных ситуаций работоспособной СЗ;

α - доля скрытых отказов устройств СЗ типа «несрабатывание»;

$1-\alpha$ - доля явных отказов устройств СЗ типа «ложное срабатывание»;

η_1, η_2 – доля аварийных отказов ТО I и II рода;

λ, μ - интенсивности отказов и восстановления СЗ, ТО.

Рассматриваемая система (ТО + СЗ) имеет 4 подмножества состояний:

- нормальное функционирование;
- останов (безаварийный);
- авария I;

– авария II.

Необходимо сделать расчет средних рисков на интервале (t =0 ÷ 1000ч) для трех значений параметра β. Рассматриваются случаи наличия и отсутствия восстановления из состояний аварий. Среднее время восстановления из аварии I – 5 суток. Среднее время восстановления из аварии II – 10 суток. Ущербы от перехода в состояние аварии II равны 8 баллов, в состояние аварии I - 4 балла.

Граф переходов марковской модели представлен на рис. 5.18.

Интенсивности переходов между состояниями равны

$\lambda_{12} = [1-(1-\beta)(\eta_1+\eta_2)]\lambda_{то}+(1-\alpha_{ук})\lambda_{ук}+(1-\alpha_{им})\lambda_{им}$;

$\lambda_{13} = \alpha_{ук}\lambda_{ук}$;

$\lambda_{14} = \alpha_{им}\lambda_{им}$;

$\lambda_{15} = (1-\beta)\eta_1\lambda_{то}$;

$\lambda_{17} = (1-\beta)\eta_2\lambda_{то}$;

$\lambda_{21} = \lambda_{61} = \mu$;

$\lambda_{32} = (1-\eta_1-\eta_2)\lambda_{то}+(1-\alpha_{им})\lambda_{им}$;

$\lambda_{37} = \lambda_{47} = \eta_2\lambda_{то}$;

$\lambda_{35} = \lambda_{45} = \eta_1\lambda_{то}$;

$\lambda_{46} = (1-\eta_1-\eta_2)\lambda_{то}$.

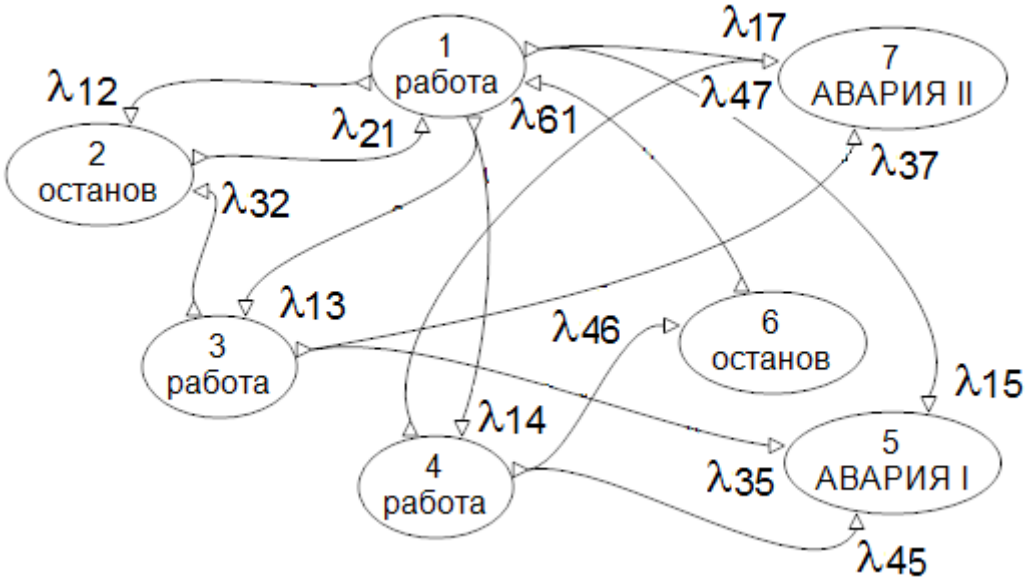


Рис. 5.18. Марковская модель надежности конфигурации ТО+СЗ.

Численные значения параметров модели:

$\lambda_{то} = 0.005$; $\lambda_{ук} = 0.001$; $\lambda_{им} = 0.002$; $\alpha_{ук} = 0.3$; $\alpha_{им} = 0.5$; $\eta_1 = 0.4$; $\eta_2 = 0.3$; $\mu = 0.05$.

Балльная оценка ущербов произведена по результатам проведения экспертами качественного анализа видов и последствий отказов:

Таблица 5.4. Виды и бальная оценка последствий отказов.

Характеристика последствий отказа	Баллы
Отказ вызывает разгерметизацию аппаратов объекта, выброс опасной среды, пожар, взрыв, образование токсического облака, цепное развитие аварии на промплощадке предприятия и за его пределами. Среди персонала и населения могут быть жертвы; есть необходимость эвакуации населения; окружающая среда получит значительный ущерб; объект – полное разрушение; остановка производства может быть 1 месяц и более.	9 - 10
Отказ вызывает разгерметизацию аппаратов объекта, выброс опасной среды, пожар, взрыв, повреждение близлежащего оборудования, развитие аварии не выходит за пределы предприятия. Среди персонала могут быть травмированные; возможна эвакуация населения и нанесение восполнимого ущерба окружающей среде, остановка производства более 10 суток.	7 - 8
Отказ вызывает разгерметизацию аппаратов объекта, выброс опасной среды, пожар, развитие аварии не выходит за пределы технологической установки объекта. Персонал может получить незначительные травмы; население – опасности нет; окружающая среда – ущерба нет; остановка производства более 5 суток.	5 - 6
Отказ вызывает разгерметизацию аппаратов объекта, выброс опасной среды из аппаратуры, пожар, развитие аварии не выходит за пределы технологического блока. Персонал может получить незначительные травмы; население – опасности нет; окружающая среда – ущерба нет; остановка производства более суток	3 – 4
Отказ вызывает незначительную разгерметизацию, загорание непосредственно в пределах технологического блока. Персоналу, населению, окружающей среде угрозы нет; остановка производства менее суток.	1 - 2

Результаты расчетов приведены в таблице 5.5.

Таблица 5.5. Средние риски эксплуатации технологического объекта на интервале (t =0 ÷ 1000ч).

β		с СЗ	Без СЗ
0.8	с восстановлением	-5.3	-12
	без восстановления	-3.9	-5.5
0.99	с восстановлением	-2.9	-12
	без восстановления	-2.6	-5.5
1	с восстановлением	-2.8	-12
	без восстановления	-2.5	-5.5

5.9. Анализ надежности отказоустойчивых вычислительных систем методом агрегирования марковских моделей

Кратковременная утрата работоспособности, вызванная внешними помехами, или сбой есть характерное явление, свойственное полупроводниковым схемам, комплектующим функциональные блоки вычислительных систем. Частота возникновения сбоев на несколько порядков превышает частоту возникновения постоянных отказов, причем наблюдается усугубление этой тенденции в связи с созданием новых технологий и совершенствованием методов повышения выхода годных СБИС. При проектировании современных отказоустойчивых вычислительных систем (ОВС) большие аппаратные и программные ресурсы тратятся на парирование сбоев, поэтому в моделях надежности должны обязательно учитываться как отказы, так и сбои с программно-реализованными алгоритмами их обработки.

Известные модели надежности ОВС [100-107], разработанные для оценки эффективности проектных решений, основываются на декомпозиция надежностного поведения системы на медленные (возникновение неисправностей) и быстрые (обработка неисправностей) процессы. Процесс возникновения неисправностей и последующей деградации технической структуры системы обычно исследуется с привлечением логико-вероятностных моделей или марковских процессов с непрерывным временем. Для анализа сложной многоэтапной процедуры обработки неисправностей и оценки эффективности процедур парирования сбоев привлекаются дискретные марковские цепи или статистическое моделирование на основе формального описания в виде сетей Петри.

При агрегировании моделей быстрых процессов обработки неисправностей в марковские модели надежности ОВС обычно проводят укрупнение состояний сбой и отказ в одно состояние и корректировку интенсивностей выхода из укрупненного состояния с учетом успешности завершения процедур парирования сбоев. Анализ результатов расчетов показателей надежности на моделях с укрупнением показал, что укрупнение существенно различных состояний (сбой, из которого есть возврат в исходное состояние; отказ, из которого принципиально отсутствует возврат в исходное состояние) порождает недопустимую погрешность, что позволило сделать вывод о недопустимости подобного укрупнения [108].

В данном разделе на примере анализа надежности трехмашинной ОВС будет продемонстрирована свободная от указанных недостатков модель обработки неисправностей и техника ее интеграции в общую модель надежности системы [109].

Анализируемая отказоустойчивая вычислительная система состоит из трех машин, связанных между собой (полносвязный граф, т.е. каждая вычислительная машина связана с двумя другими). Отдельная машина состоит из базовой части (БЧ), адаптера связи с абонентом (А), приемо-передатчика межмашинного обмена (П/П). Критерием отказа ОВС является невозможность правильной работы не менее, чем по двум (из трех) каналам связи с абонентом внешней среды. На рис.5.19 приведена укрупненная функциональная структура трехмашинной ОВС.

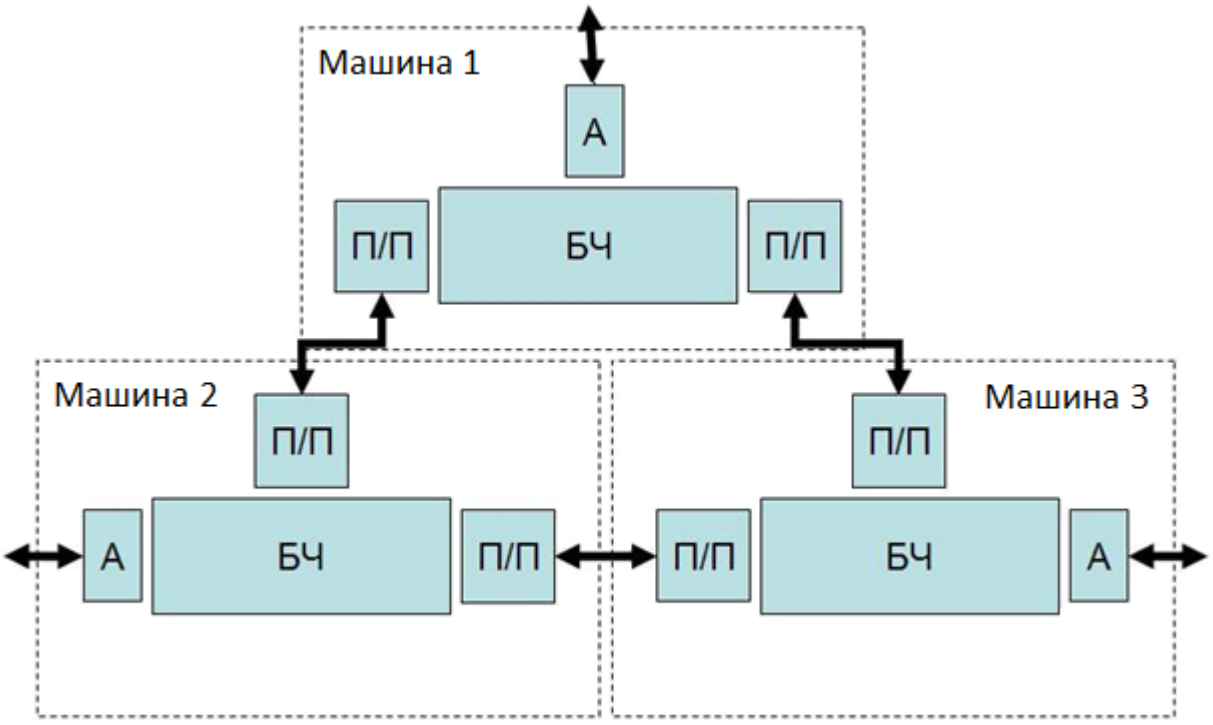


Рис.5.19 Функциональная структура трехмашинной ОВС

Факторами, учитываемыми при построении модели надежности, являются

- возможность возникновения двух типов неисправностей – отказов и сбоев
- отсутствие восстановления работоспособности ОВС, нарушенной возникновением отказов
- наличие резервирования (троирование) базовых и периферийных частей
- введение специальных процедур обработки сбоев базовых частей машин
- наличие видов отказов (например, пробой по питанию) элементов не базовой части ОВС (адаптер, приемник-передатчик), которые могут привести к неисправности базовой части

Процедура обработки неисправностей рассматривается как последовательность k программных попыток восстановления нормального хода вычислительного процесса ((перезапись памяти, повторы сегментов программ, откаты на контрольные точки…)). Предполагается, что неуспех i-ой попытки восстановления может быть вызван тремя факторам

- длительность сбоя (как физического явления) превышает длительность i-ой попытки восстановления
- за время выполнения i-ой попытки восстановления произошел повторный сбой восстанавливаемой базовой части ОВС
- за время выполнения i-ой попытки восстановления произошел сбой или отказ других частей ОВС

Кроме того, предполагается, что часть отказов и сбоев может носить катастрофический характер (система переходит в отказ, минуя деградацию).

бщий подход к моделированию заключается в раздельном построении моделей обработки неисправностей и моделей деградации технической структуры ОВС. На модели обработки неисправностей рассчитываются вероятности успеха и неуспеха восстановления по сбоям, с помощью которых корректируются интенсивности переходов модели деградации.

Модель обработки неисправностей, возникающих в ОВС, представляет собой дискретный марковский процесс, показанный на графе, приведенном на рис.5.20. Дискретность времени процесса определяется тем, что переход в состояния выполнения i-ой процедуры восстановления, успешного или неуспешного завершения восстановления возможен лишь в строго определенные моменты времени, определяемые протоколом отказо-сбоеустойчивого обмена данными базовых частей ОВС [110].

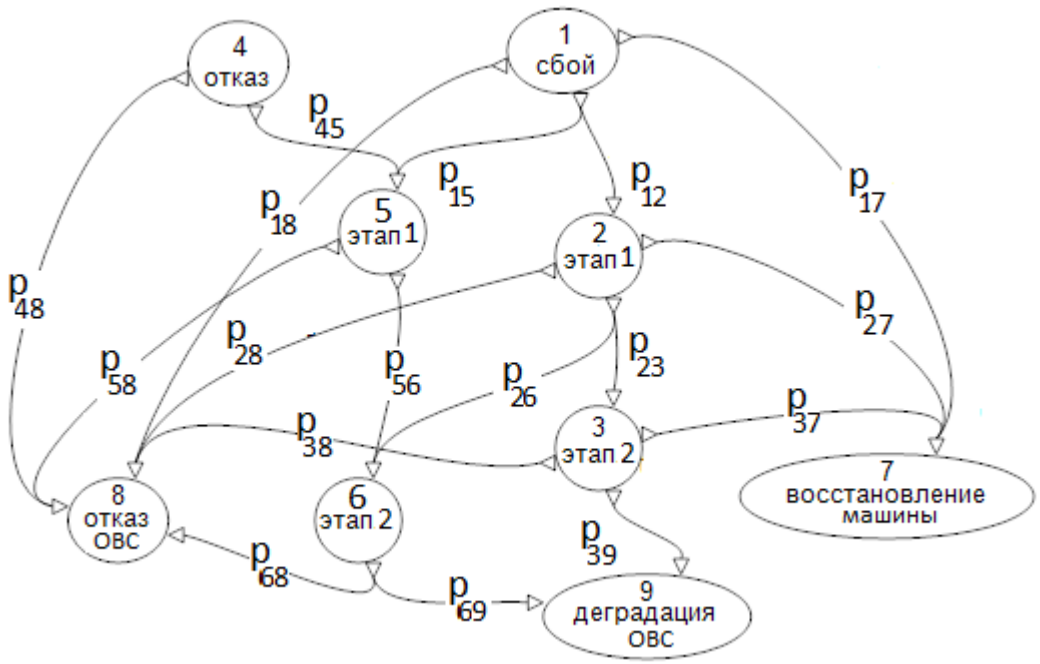


Рис. 5.20. Марковский граф процесса обработки неисправностей отдельной машины ОВС (k=3)

Состояние 1 – сбой машины ОВС. Состояние 4 – отказ машины ОВС. Состояния 2 и 5 графа соответствуют неуспешному завершению первой попытки программного восстановления “сбоящей” машины ОВС. Состояния 3 и 6 – неуспеху второй попытки. Всего в системе реализовано три попытки восстановления. Состояние 7 – работоспособность машины, нарушенная сбоем, восстановлена. Состояние 8 – произошел отказ ОВС. Состояние 9 – деградация структуры ОВС (машина отключается из рабочей конфигурации).

Элементы матрицы переходов P находятся из следующих соотношений:

$$
\begin{aligned}
&p_{12} = q_{в}, p_{15} = q_{отк}, p_{17} = p_{в}, p_{18} = q_{ко} \\
&p_{23} = q_{в}, p_{26} = q_{отк}, p_{27} = p_{в}, p_{28} = q_{ко} \\
&p_{37} = p_{в}, p_{38} = q_{ко}, p_{39} = q_{в} + q_{отк} \\
&p_{45} = 1 - q^{o}_{ко}, p_{48} = q^{o}_{ко} \\
&p_{56} = 1 - q^{o}_{ко}, p_{58} = q^{o}_{ко} \\
&p_{69} = 1 - q^{o}_{ко}, p_{68} = q^{o}_{ко}
\end{aligned}
\qquad (5.60)
$$

Вероятность успешного восстановления по сбоям:

$$p_{в} = p_{нс} p_{2} (1 - q_{отк})(1 - p_{t})(1 - q_{сб}) \ , \qquad (5.61)$$

где

$p_2 = e^{-2(\lambda сб+\lambda б+\lambda нб)\tau}$ - вероятность отсутствия сбоя или отказа с двумя другими машинами, $\lambda_б$ – интенсивность отказов базовой части машины, $\lambda_{нб}$ интенсивность отказов не базовой части;

$p_{нс}$ -условная вероятность возникновения некатастрофического сбоя;

$p_{но}$ -условная вероятность возникновения некатастрофического отказа;

$p_t = e^{-\tau/\sigma}$ - вероятность того, что длительность сбоя (σ) превышает время одной попытки восстановления (τ);

$q_{сб} = 1 - e^{-\lambda сб\tau}$ - вероятность повторного сбоя машины во время ее восстановления;

$q_{отк} = 1 - e^{-(\lambda б+\lambda нб)\tau}$ - вероятность отказа машины во время ее восстановления.

Вероятность неуспеха восстановления по сбоям:

$$q_в = p_{нс}p_2(1-q_{отк})((1-p_t)q_{сб} + p_t) \quad (5.62)$$

Вероятность перехода в отказ во время восстановления:

$$q_{ко} = 1 - p_{нс} + p_{нс}(1-p_2) \quad (5.63)$$

Вероятность перехода в отказ системы во время бессмысленного восстановления по сбоям машины, в которой на самом деле произошел постоянный отказ

$$q^o_{ко} = 1 - p_{но}p_2 \quad (5.64)$$

Переходная матрица P и вектор начальных условий p(0) позволяют вычислить распределение финальных вероятностей за n шагов, как $[0, 0, 0, 0, 0, 0, p_7(n), p_8(n), p_9(n)] = p(0)P^n$. Причем, если p(0) = [1, 0, 0, 0, 0, 0, 0, 0, 0], т.е. моделируется событие возникновения постоянного отказа, то при $n \geq 3$ $p_7(n) = 0$, $p_8(n) = P_F$, $p_9(n) = P_D$. Если рассматривается возникновение сбоя, то p(0) = [0, 0, 0, 1, 0, 0, 0, 0, 0] и при $n \geq 3$ $p_7(n) = P_r$, $p_8(n) = P_f$, $p_9(n) = P_d$. Таким образом, минуя укрупнения состояний сбой и отказ, получены коэффициенты, корректирующие интенсивности переходов непрерывной марковской модели надежности ОВС.

Модель деградации технической структуры ОВС в целом представляет собой непрерывный марковский процесс с дискретным множеством состояний, показанный на графе, приведенном на рис.5.21

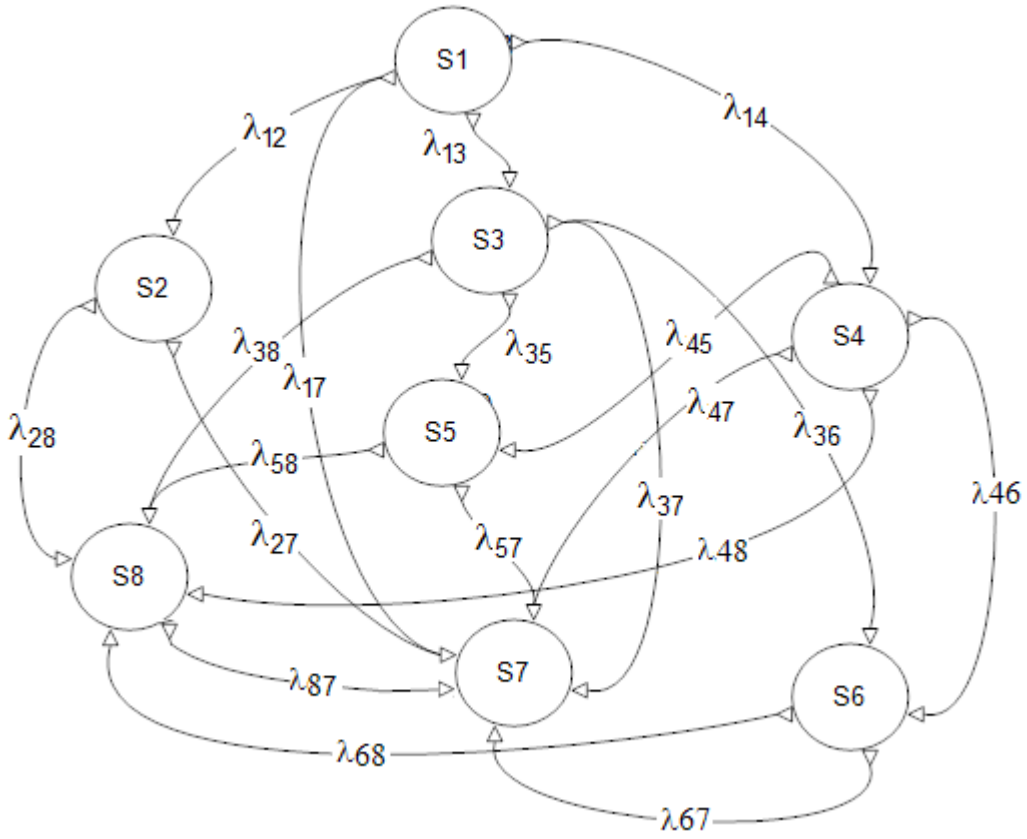


Рис.5.21 Марковский граф деградации технической структуры ОВС.

Состояния марковской модели:

S1 – система исправна

S2 – работают две машины, одна заблокирована

S3 – работают три машины, но у одной из машин отказала 1 межмашинная связь

S4 – работают три машины, но у одной отказала связь с абонентом

S5 – работают две машины на 2 канала связи с абонентом

S6 – работают две машины на 2 канала связи с абонентом

S7 – отказ ОВС

S8 – одна машина работает, вторая – “подслушивает” и транслирует связь с абонентом

Интенсивности переходов марковской модели:

$$\lambda_{12} = 3\lambda_{\Sigma}P_D + 3\lambda_{сб}, \quad \lambda_{13} = 6\lambda_{пп}, \quad \lambda_{14} = 3\lambda_a, \quad \lambda_{17} = 3\lambda_{\Sigma}P_F + 3\lambda_{сб}P_f$$
$$\lambda_{27} = 2(\lambda_{\Sigma} + \lambda_a + \lambda_{пп} + \gamma\lambda_{сб}), \quad \lambda_{28} = 2\cdot(1-\gamma)\lambda_{сб}$$
$$\lambda_{35} = \lambda_{\Sigma}P_D + 2\lambda_{пп} + \lambda_a + \lambda_{сб}P_D, \quad \lambda_{36} = \lambda_a, \quad \lambda_{37} = \lambda_{\Sigma} + \gamma\lambda_{сб} + \lambda_{\Sigma}P_f + \lambda_{сб}P_f, \quad \lambda_{38} = (1-\gamma)\lambda_{сб}$$
$$\lambda_{45} = 4\lambda_{пп} + \lambda_{\Sigma}P_D, \quad \lambda_{46} = 2\lambda_{пп}, \quad \lambda_{47} = 2(\lambda_{\Sigma} + \lambda_a + \gamma\lambda_{сб}) + \lambda_{\Sigma}P_f, \quad \lambda_{48} = 2\cdot(1-\gamma)\lambda_{сб} \qquad (5.65)$$
$$\lambda_{57} = 2(\lambda_{\Sigma} + \lambda_a + \lambda_{пп} + \gamma\lambda_{сб}), \quad \lambda_{58} = 2\cdot(1-\gamma)\lambda_{сб}$$
$$\lambda_{67} = 3(\lambda_{\Sigma} + \gamma\lambda_{сб}) + 4\lambda_{пп} + 2\lambda_a, \quad \lambda_{68} = 3\cdot(1-\gamma)\lambda_{сб}$$
$$\lambda_{87} = 2(\lambda_{\Sigma} + \lambda_a + \lambda_{пп} + \lambda_{сб})$$

$\lambda_{\Sigma} = \lambda_б + \lambda_{нб}$; $\lambda_{пп}$ – интенсивность отказов приемо-передатчика; λ_a – интенсивность отказов адаптера, $(1-\gamma)$ - доля отказов не базовой части, приводящей к отказу базовой.

Осуществляя расчеты при варьировании параметров модели, можно исследовать многие аспекты надежности ОВС. В частности ответить на вопросы о том, какой вклад в общую ненадежность системы вносят сбои, насколько удается повысить надежность ОВС за счет введения специальных процедур обработки сбоев. Для ответа на эти вопросы были проведены расчеты, сведенные в таблицу 5.6. Расчеты выполнены для следующих значений параметров модели и интенсивностей отказов подсистем ОВС: интенсивность отказов базовой части $\lambda_б = 4*10^{-6}$, интенсивность отказов небазовой части $\lambda_{нб} = 0{,}6*10^{-6}$, интенсивность отказов приемо-передатчика $\lambda_{пп} = 0{,}9*10^{-6}$, интенсивность отказов адаптера $\lambda_a = 0{,}6*10^{-6}$, доля отказов не базовой части, не влияющей на отказы базовой $\gamma = 0{,}3$. Параметры процедуры восстановления по сбоям: число попыток восстановления k=3, средняя длительность сбоя σ=10мс, длительность одной попытки восстановления τ=20мс, интенсивность потока сбоев в 100 раз превышает интенсивность постоянных отказов ОВС. Время функционирования системы 8760ч (1 год).

Таблица 5.6. Расчет показателей надежности ОВС

	Вид расчета		
Показатели	Расчет по постоянным отказам без учета сбоев	Расчет по сбоям и постоянным отказам без учета специальных процедур обработки неисправностей	Расчет по сбоям и постоянным отказам с учетом специальных процедур обработки неисправностей
Вероятность безотказной работы	0,992122	4,137050E-03	0,848385
Вероятность отказа	7,878300E-03	0,995863	0,151615

Анализ отказоустойчивого трехмашинного вычислительного комплекса на предложенной модели подтверждает факт существенной зависимости надежности ОВС от сбоев. Неучет в

моделях надежности ОВС сбоев приводит к получению необоснованно завышенных оценок показателей надежности. В тоже время, если в моделях надежности будут учитываться сбои, но не будет отражен факт просеивания потока сбоев введением специальных процедур восстановления, то будет получена недопустимо заниженная оценка надежности системы. Показатели вероятности безотказной работы, рассчитанные без и с учетом парирования сбоев, отличаются друг от друга более, чем в 200 раз.

Глава 6. Динамические деревья отказов

В процессе создания моделей надежности сложных систем возникает противоречие, связанное со стремлением учета существенных факторов, определяющих надежность системы, с одной стороны, и необходимостью преодоления большой размерности, с другой стороны. Решением проблемы является проведение декомпозиции системы, построение статических и/или динамических моделей выделенных частей и агрегирование полученных моделей, либо уже вычисленных показателей для частей системы в общесистемную модель или показатели. Для оценки характеристик надежности частей системы, выделяемых при декомпозиции, возможно использование различных методов, адекватных учитываемым особенностям “надежностного поведения”. Наиболее рациональным сочетанием здесь является комбинация логико-вероятностных моделей деревьев отказов и марковского моделирования при сохранении мнемоники деревьев отказов. В деревья отказов внедряются динамические операторы (динамические вершины), учитывающие развитие процесса возникновения базовых событий во времени с помощью марковских моделей. Эти агрегированные модели называют динамическими деревьями отказов [122,123]. Крупнейшие разработчики специализированных программ анализа надежности и безопасности начали активно реализовывать динамические деревья отказов. Возможность построения динамических моделей надежности с помощью аппарата деревьев отказов обеспечивается введением в них четырех специальных вершин PAND, SEQ, SPARE, FDEP. Реализация этих вершин с помощью марковских моделей и интегральных соотношений будет детально рассмотрена в данной главе. Все представленные примеры динамических деревьев отказов набраны и рассчитаны в модуле Fault Tree Windchill Quality Solutions.

6.1. Динамическая вершина PAND.

PAND (Priority AND Gate) - *динамическая вершина (оператор) приоритетное* И, обозначаемая как  . PAND моделирует ситуацию последовательного возникновения входных событий. Входными событиями могут быть как базовые события, так и выходы других логических вершин. Последовательность “срабатывания” входов формируется слева на право (первый элемент последовательности - самое левое входное событие). Так как динамические вершины реализуются марковскими моделями, то случайные времена возникновения входных событий описываются экспоненциальным распределением.

Рассмотрим механизм “срабатывания” приоритетного И на примерах. Пусть система состоит из двух разнонадежных, восстанавливаемых элементов с интенсивностями отказов и восстановления соответственно λ_1, λ_2 и μ_1, μ_2. Отказом системы является отказ двух ее элементов в последовательности - первый элемента, а затем второй элемент. Динамическое дерево отказов с вершинным PAND гейтом, моделирующее эту ситуацию, представлено на рис.6.1. Представленное дерево реализуется марковским графом, показанным на рис.6.2. Для кодировки состояний графа здесь и далее используется позиционный код (i j), означающий отказ элемента i, а затем элемента j; 0 – указывает на работоспособность элемента. Состояние (1 2) является состоянием отказа системы.

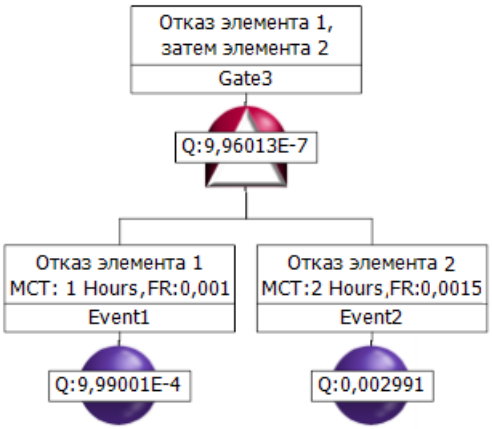


Рис.6.1. Динамическое дерево отказов с двухвходовым PAND.

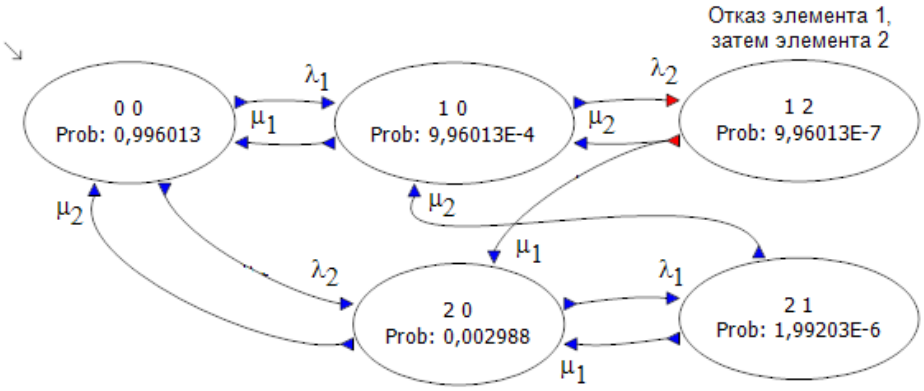


Рис 6.2. Марковский граф для двухвходового PAND.

Трехвходовой PAND и соответствующий марковский граф для случая невосстанавливаемых равнонадежных элементов показаны на рис.6.3 и 6.4 соответственно. Состояние S_1 графа соответствует одиночному отказу элементов 2 или 3; состояние S_2 – любому двойному отказу,

кроме отказа в последовательности 1,2; S_3 – любому тройному отказу, кроме отказа в последовательности 1,2,3.

Рис.6.3. Динамическое дерево отказов с трехвходовым PAND.

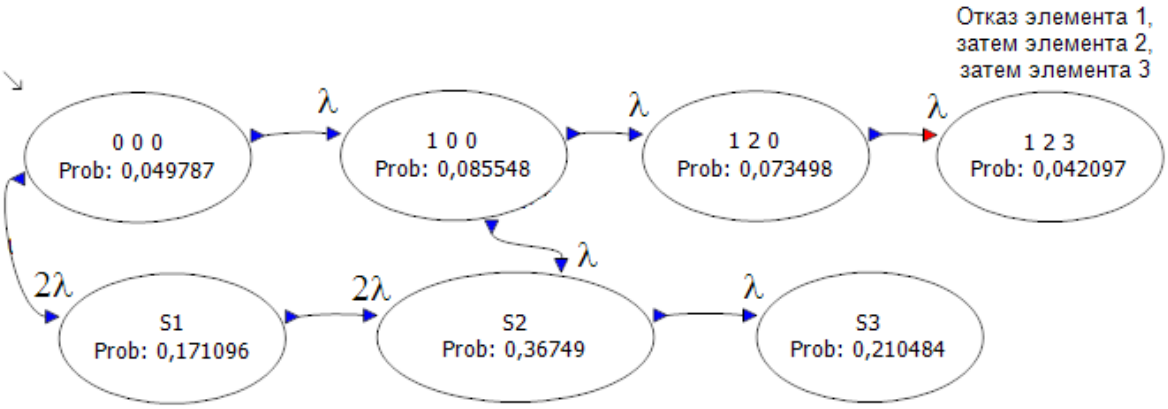


Рис.6.4. Марковский граф для трехвходового PAND.

При отсутствии восстановления динамическая вершина PAND может быть смоделирована интегральным соотношением как свертка распределений базовых событий. Например, для дерева, показанного на рис.6.1, вероятность вершинного гейта PAND (Q(t)) можно записать любым из двух способов

$$Q_{PAND}(t) = \int_0^t f_1(\tau)(1 - F_2(\tau))F_2(t - \tau)d\tau \qquad (6.1)$$

или

$$Q_{PAND}(t) = \int_0^t f_2(\tau)(\int_0^\tau f_1(\xi)d\xi)d\tau\,. \qquad (6.2)$$

Здесь $f_i(t)$, $F_i(t)$ – соответственно плотность и функция распределения случайных наработок до отказа, соответствующих i-му базовому событию.

Для общего случая PAND с n входами интегральное рекуррентное соотношение будет иметь вид

$$Q^n_{PAND}(t) = \int_0^t f_n(\tau)\cdot Q^{n-1}_{PAND}(\tau)d\tau \qquad (6.3)$$

Преимуществом использования рекуррентного интегрального соотношения вместо марковской модели последовательности отказов является снятие ограничения на экспоненциальность распределения случайных наработок элементов.

Для экспоненциального случая интегрирование выражений (6.1) или (6.2) позволяет получить формулу

$$Q_{PAND}(t) = \frac{\lambda_1}{\lambda_1+\lambda_2} + \frac{\lambda_2}{\lambda_1+\lambda_2}e^{-(\lambda_1+\lambda_2)t} - e^{-\lambda_2 t}\,.\,, \qquad (6.4)$$

которая так же могла быть получена на марковской модели без восстановления.

Дифференциальные уравнения, соответствующие марковскому графу (рис.6.2), в котором отсутствуют переходы, связанные с восстановлением, имеют вид:

$$\begin{cases} P_{00}'(t) = -(\lambda_1+\lambda_2)P_{00}(t) \\ P_{10}'(t) = \lambda_1 P_{00}(t) - \lambda_2 P_{10}(t) \\ P_{12}'(t) = \lambda_2 P_{10}(t) \end{cases} \qquad (6.5)$$
$$P_{00}(0) = 1$$

Решая (6.5), получим

$$\begin{aligned} P_{00}(t) &= e^{-(\lambda_1+\lambda_2)t} \\ P_{10}(t) &= e^{-\lambda_2 t} - e^{-(\lambda_1+\lambda_2)t} \\ P_{12}(t) &= \frac{\lambda_1}{\lambda_1+\lambda_2} + \frac{\lambda_2}{\lambda_1+\lambda_2}e^{-(\lambda_1+\lambda_2)t} - e^{-\lambda_2 t} \end{aligned} \qquad (6.6)$$

Используя PAND, можно моделировать “надежностное поведение” систем, с несколькими видами отказов, различающихся по тяжести последствий. Рассмотрим работу объекта с системой аварийной защиты (СЗ), останавливающей отказавший объект с помощью исполнительного механизма (ИМ) при получении сигнала об отказе объекта с устройства контроля (УК) (рис.6.5).

При построении дерева отказов необходимо учитывать очередность возникновения отказов АЗ и объекта, так как авария может возникнуть лишь при отказе объекта после отказа АЗ. Если объект откажет при работоспособности защиты или до ее отказа, то он будет переведен в режим штатного останова, препятствующий возникновению аварии. Таким образом, вершинное событие отказа системы (оператор OR) складывается из трех составляющих:

- авария (отказала АЗ, а затем объект)
- неаварийный (штатный) останов I (отказал объект, а затем АЗ)
- неаварийный (штатный) останов II (отказал объект, АЗ исправна).

Динамическое дерево отказов системы “объект + АЗ” показано на рис.6.5. Попадание в состояния аварии и неаварийного отказа I моделируются вершинами приоритетного И. Другими вершинами дерева являются:  - AND (И),  - OR (ИЛИ),  - NOR (ИЛИ-НЕ).

Марковская модель, соответствующая дереву, приведена на рис.6.6.

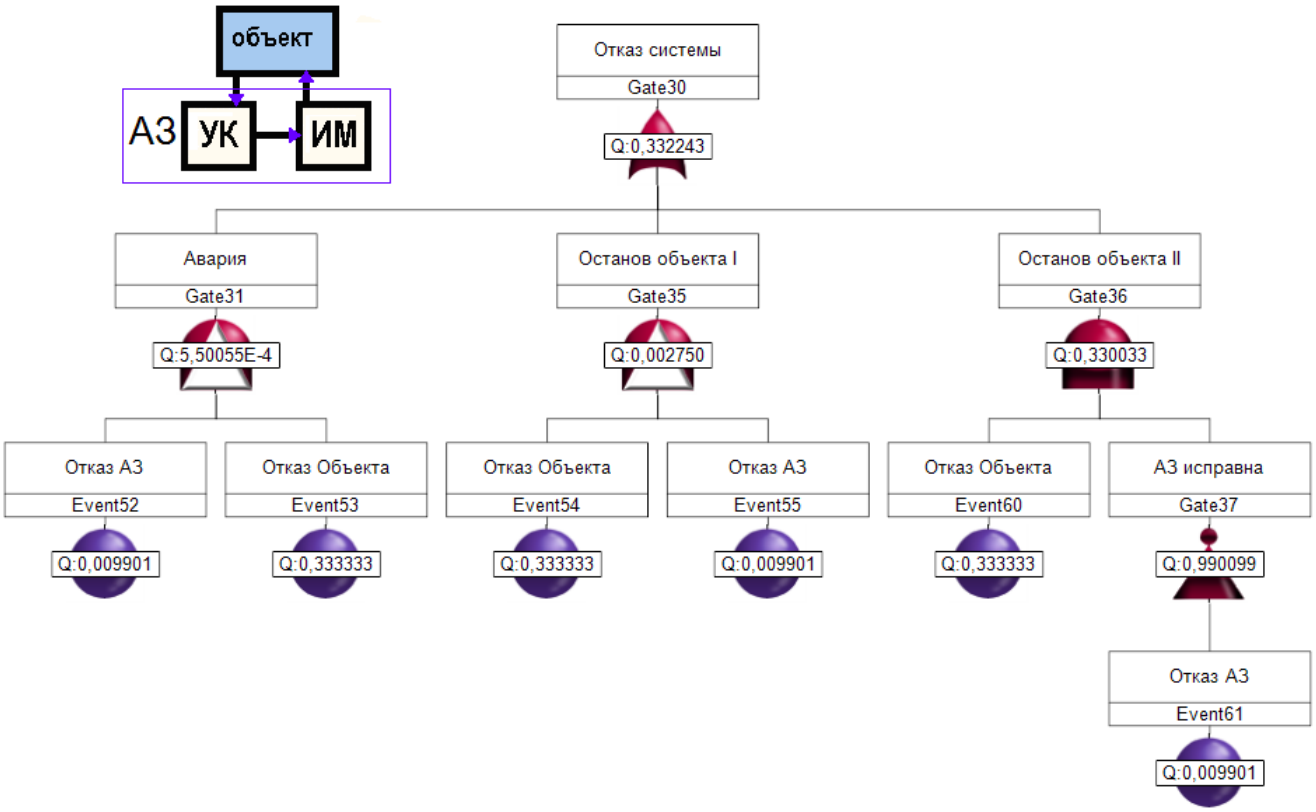


Рис.6.5. Динамическое дерево отказов системы “объект+аварийная защита”.

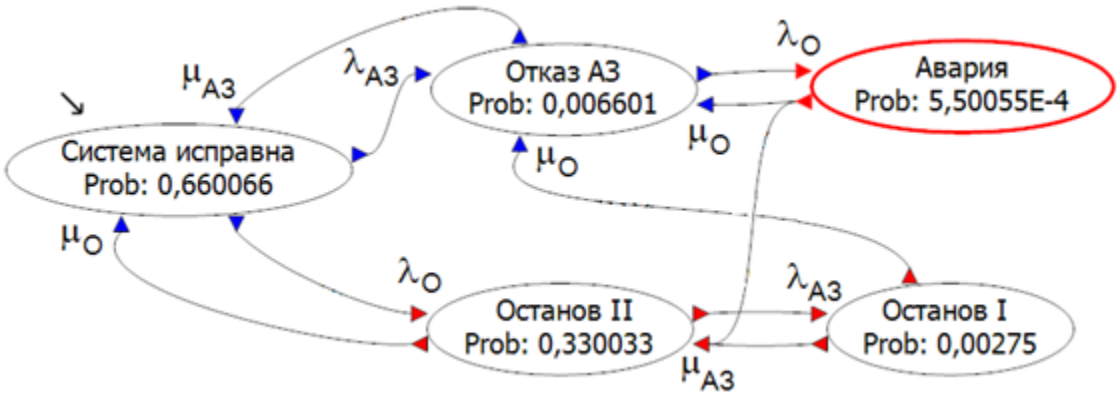


Рис.6. 6. Марковская модель динамического дерева отказов системы “объект+АЗ”.

6.2. Динамическая вершина SEQ.

SEQ (Sequence Enforcing Gate) – динамическая вершина (оператор) последовательного возникновения событий, обозначаемая как  . SEQ моделирует процесс возникновения событий, которые могут происходить в одной и только одной определенной последовательности. Такие процессы происходят в системе ненагруженного резервирования из идентичных элементов; в системе ненагруженного функционального резервирования с различными элементами; в системах с накоплением нарушений. Sequence enforcing gate так же может быть использована при моделировании процессов развития аварии. Вершина SEQ с тремя входами показана на рис.6.7. Возможная интерпретация входных базовых событий и вершины SEQ представлена в таблице 6.1.

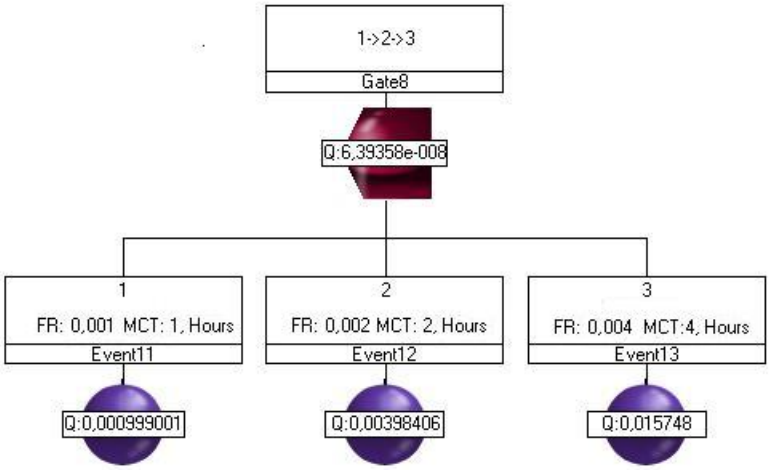


Рис.6.7. Динамическое дерево отказов с трехвходовым SEQ.

Таблица 6.1. Примеры SEQ модели.

Моделируемая система или ситуация	Вход 1	Вход 2	Вход 3	Вершинное событие SEQ
Ненагруженное резервирование (идентичные элементы). Один элемент рабочий, два в холодном резерве.	Отказ рабочего элемента	Отказ первого резервного элемента, после подключения на место рабочего.	Отказ второго резервного элемента, после подключения на место рабочего.	Отказ резервированной схемы.
Ненагруженное функциональное резервирование в управляющей системе. Первая функция – полностью автоматическое управление, вторая – смешанное управление (автомат+человек), третья – полностью ручное управление (человек)	Отказ устройства автоматического управления. Переход на “полуавтомат”	Отказ “полуавтомата”, переход на полностью ручное управление	Ошибка человека-оператора, осуществляющего ручное управление	Отказ от выполнения функции управления
Устройство циркулярной пилы	Минимальная степень затупления пилящего диска	Средняя степень затупления пилящего диска	Максимальная степень затупления пилящего диска	Полное затупление циркулярной пилы
Установка первичной переработки нефти	Выброс нефти	Появление источника воспламенения	Воспламенение пролива	Авария (пожар и (или) взрыв облака)

В отличие от PAND в марковской модели SEQ не рассматриваются альтернативные последовательности событий, поэтому граф состояний модели представляет собой схему гибели и размножения (рис.6.8).

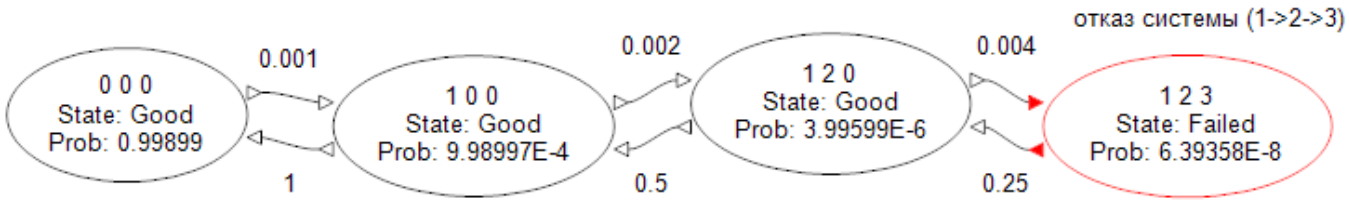


Рис.6.8. Марковский граф для трехвходового SEQ.

6.3. Динамическая вершина SPARE

SPARE (Spare Gate) – динамическая вершина (оператор), моделирующий надежностное поведение схем гибридного резервирования и обозначаемый как  . SPARE описывает процесс отказа сложных резервированных схем, работающих вплоть до отказа последнего компонента схемы (критерий работоспособности “1 из n”). В качестве входов вершина SPARE может принимать только базовые события специального вида, называемые SPARE Event  . Это событие имеет два параметра, определяющих структуру резервированной схемы: Sp - *spare pool* (количество идентичных резервных элементов), Df - *dormancy factor* (коэффициент нагруженности резерва). Варьирование коэффициента нагруженности в диапазоне от 0 до 1 позволяет моделировать работу схем: резервирования замещением (ненагруженный резерв), схем постоянного резервирования с параллельно работающими нагруженными элементами, схем с облегченным резервом. Аналогично гейту PAND логика “срабатывания” вершины SPARE зависит от расположения входных SPARE событий. Все входные события делятся на два подмножества основных (рабочих) и резервных элементов схемы. К рабочим элементам относятся все элементы, входящие в крайнее левое SPARE событие. Рабочее подмножество может состоять как из одного элемента, так и из произвольного количества идентичных элементов, задаваемого параметром *Sp* левой вершины. Остальные SPARE события являются резервом, последовательно подключаемым после отказа всех рабочих элементов. Этот режим подключения несколько отличен от классической схемы гибридного резервирования, где ненагруженные резервные элементы замещают параллельно работающие рабочие элементы по мере их отказа.

На рис. 6.9. представлена модель надежности схемы резервирования замещением с одним облегченным резервом в виде динамического дерева отказов с вершиной SPARE и граф переходов марковской реализации этой вершины. Запишем вероятность $Q_{SPARE}(t)$ возникновения события отказа схемы, моделируемой SPARE вершиной рис.6.9, в общем виде для произвольно распределенных элементов схемы. Отказ этой схемы может произойти на интервале времени (0,t), если произойдет одно из двух несовместных событий:

- на интервале (0,t) сначала откажет рабочий элемент, а затем подключенный на его место резерв
- на интервале (0,t) сначала откажет резервный элемент, а затем рабочий

Исходя из этого

$$Q_{SPARE}(t) = \int_0^t (1 - F_{2D}(\tau)) f_1(\tau) F_{2A}(t - \tau) d\tau + \int_0^t F_{2D}(\tau)) f_1(\tau) d\tau, \quad (6.7)$$

где $f_1(t)$ – плотность распределения случайной наработки рабочего элемента, $F_{2D}(t)$ – функция распределения случайной наработки резерва до включения его в работу, $F_{2A}(t)$ – функция распределения случайной наработки резерва после включения его в работу.

Ряд аналогичных моделей для моделирования динамических операторов можно посмотреть в [113,114]. Приведем критические соображения относительно подхода с интегральными выражениями к моделированию динамических операторов в деревьях отказов. Во-первых, этот подход справедлив лишь при отсутствии восстановления возникающих отказов (т.е. применим для невосстанавливаемых систем, модулей). Наверное, все промышленные системы являются восстанавливаемыми объектами. Во-вторых, нахождение аналитического решения этих интегральных выражений при произвольных функциях распределений практически невозможно. По-видимому, из широко распространённых (неэкспоненциальных) распределений можно говорить лишь о возможности решения для распределений Вейбулла, Эрланга. Да и то, получаемые решения будут достаточно громоздки. Если же решение искать численными методами, то, пожалуй, наиболее общим вариантом нахождения решения для произвольных распределений будет применение статистического моделирования. Причем рассмотрение не всей системы, а отдельных операторов, выделенных при структурной декомпозиции, позволит применять различные эффективные методы ускорения моделирования, что повысит точность оценок. Наилучшим способом для экспоненциальных распределений является применение марковского моделирования. И марковское, и статистическое моделирование позволят учесть и разнообразные стратегии восстановления.

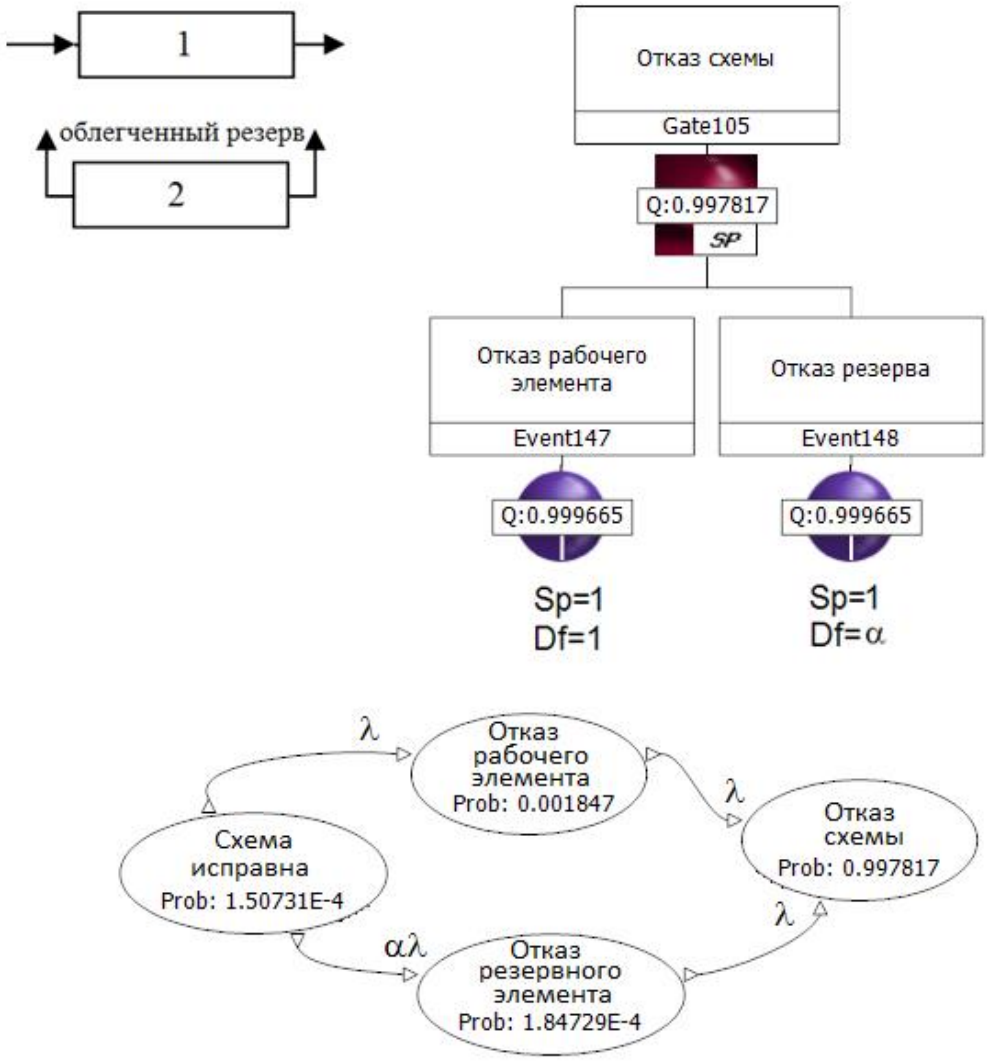


Рис. 6.9. Динамическое дерево отказов схемы резервирования замещением с облегченным резервом.

Динамическое дерево отказов схемы гибридного резервирования, состоящей из двух параллельно работающих рабочих элементов (1,2), двух “холодных” резервов (3,4) и одного резервного элемента, работающего в облегченном режиме (5), показано на рис.6.10.

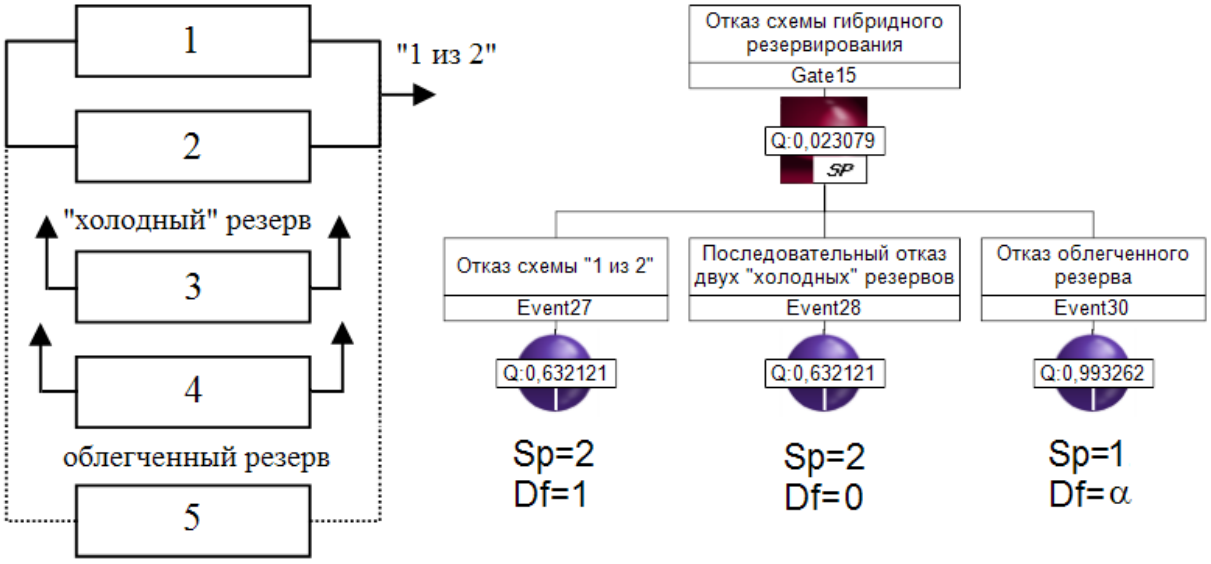


Рис.6.10. Динамическое дерево отказов схемы гибридного резервирования с вершиной SPARE.

Марковская модель дерева отказов схемы гибридного резервирования показана на рис.6.11. Для кодировки состояний графа используется код M,N,K, где M – количество параллельно работающих рабочих элементов M∈{0,1,2}, N – количество элементов холодного резерва N∈{0,1,2}, K – количество элементов облегченного резерва K∈{0,1,}. λ – интенсивность отказов элементов 1 и 2 и элементов 3,4,5 (после включения), λo – интенсивность отказов облегченного резерва до включения.

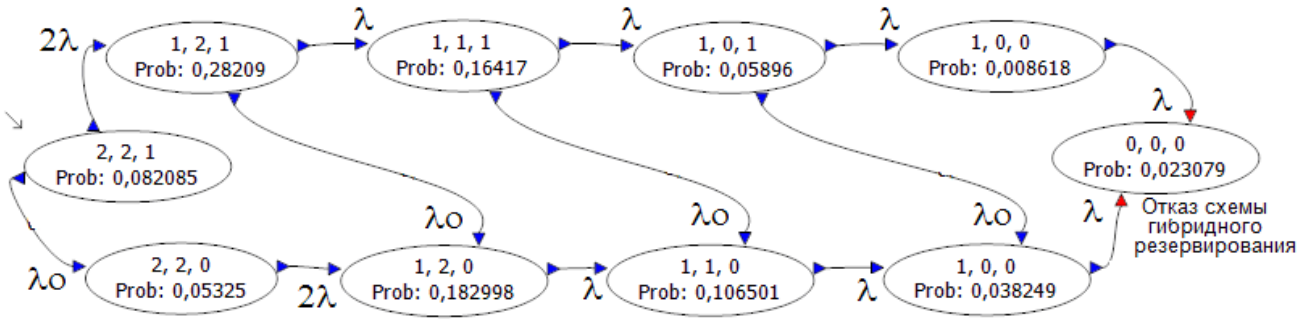


Рис.6.11. Марковская модель динамического дерева отказов схемы гибридного резервирования.

6.4 Динамическая вершина FDEP

FDEP (Functional Dependency Gate) – динамическая вершина (оператор), моделирующая функциональную зависимость отказов и обозначаемая как 

Динамическая вершина FDEP моделирует процесс возникновения зависимых каскадных отказов и кратных отказов по общей причине. Марковские модели, положенные в основу реализации FDEP, предоставляют большие возможности, чем известные комбинаторные модели анализа отказов по общей причине, описанные в разделе 4.7 (Alpha, Beta, MGL CCF model). Вершина FDEP имеет два вида входных событий – триггерное событие или просто триггер и зависимые события. Зависимые события представляют собой повторяющиеся базовые события (repeated event), присутствующие в других ветвях дерева. Срабатывание триггера моделирует событие возникновения общей причины, воздействующей на зависимые входные события FDEP. Рассмотрим простую последовательно-параллельную схему, показанную на рис.6.12. На дублированную часть схемы может воздействовать общая причина, вызывающая одновременный отказ элементов 1 и 2. Для учета общей причины в дерево отказов схемы (рис.6.12) включена вершина FDEP. Марковский граф, соответствующий данной FDEP вершине, показан на рис.6.13. λ – интенсивность отказов элемента схемы, λ_{ccf} – интенсивность возникновения общей причины. Состояние графа S1 соответствует исправному состоянию системы, S2 – одиночный отказ элемента 1 или элемента 2, S3 – отказ дублированной схемы, вызванный появлением общей причины или отказом двух ее элементов.

Последовательно-параллельный характер схемы позволяет записать простую формулу для вычисления вероятности ее отказа с учетом общей причины:

$$Q_{\text{схемы}}(t) = Q_{ccf}(t) \cdot Q^{I}_{\text{схемы}}(t) + (1 - Q_{ccf}(t)) \cdot Q^{II}_{\text{схемы}}(t), \qquad (6.8)$$

где $Q_{ccf}(t)$ - вероятность возникновения общей причины на интервале (0,t);

$Q^{I}_{\text{схемы}}(t)$ - вероятность отказа схемы на (0,t) при возникновении общей причины: $Q^{I}_{\text{схемы}}(t) = 1$;

$Q^{II}_{\text{схемы}}(t)$ - вероятность отказа схемы на (0,t) при отсутствии общей причины: $Q^{II}_{\text{схемы}}(t) = q_1(t)q_2(t) + q_3(t) - q_1(t)q_2(t)q_3(t)$, где $q_i(t)$ – вероятность отказа i-го элемента схемы.

Численные значения вероятности реализации вершинного события дерева (рис.6.12) и вероятности отказа по (6.8) полностью совпадают.

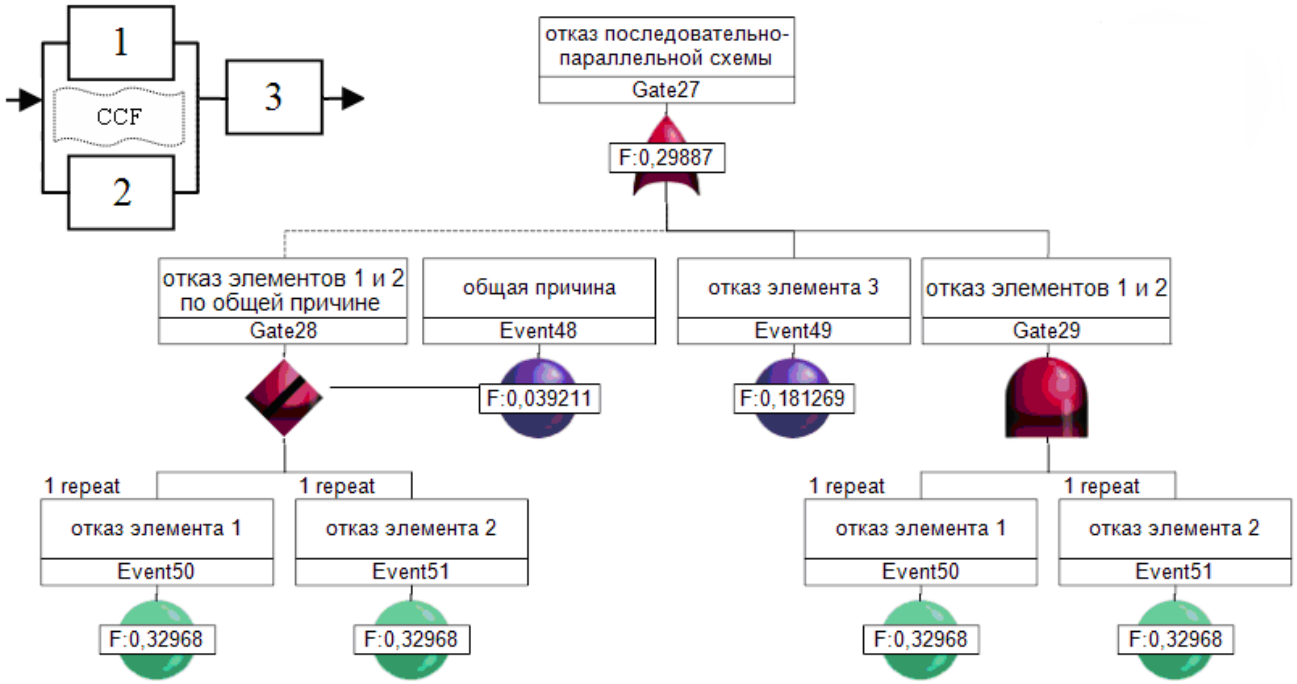


Рис.6.12. Динамическое дерево отказов последовательно-параллельной схемы с вершиной FDEP.

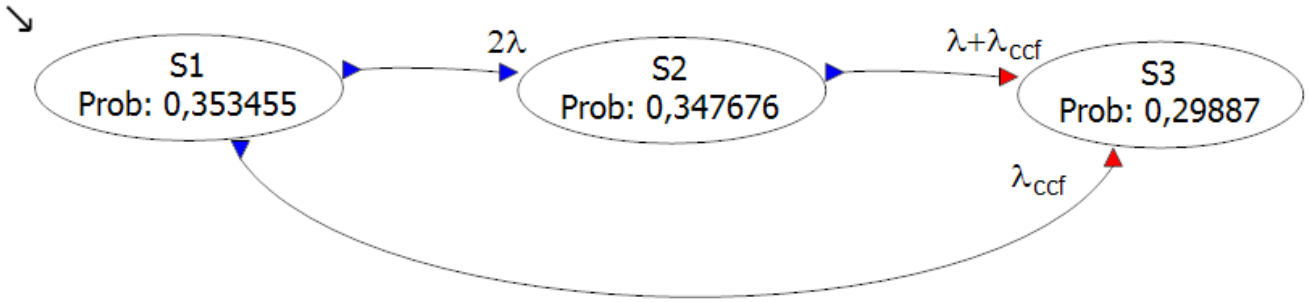


Рис.6.13. Марковский граф процесса попадания в состояние отказа с учетом общей причины для дублированной схемы.

6.5. Сложные динамические деревья отказов

Сложным динамическим деревом будем называть дерево, содержащее несколько разных видов динамических вершин. Наиболее распространенной комбинацией динамических вершин является SPARE+FDEP. Эта комбинация позволяет моделировать достаточно сложное поведение резервированных систем, подверженных влиянию общих причин. Так например, схема скользящего резервирования с неабсолютно надежным переключающим устройством описывается динамическим деревом, представленным на рис.6.14. Скользящее резервирование, когда один и тот же резервный элемент может заменить любой из отказавших рабочих элеметов, учитывается вводом в две отдельные SPARE вершины повторяющегося SPARE события (Event44). Учет ненадежности переключателя осуществляется с помощью FDEP вершины, входом которой также является повторяющееся SPARE событие, соответствующее отказу скользящего резерва. Такая конфигурация дерева описывает следующее “надежностное поведение”. При исправном переключателе схема деградирует по траектории (2,1)->(2,0)->(1,0)->(0,0). При отказавшем переключателе – (2,0)->(1,0)->(0,0). Марковская модель данного динамического дерева показана на рис.6.15. Отказ переключателя приводит к тому, что резерв становится недоступен вне зависимости от того подключен или не подключен он в рабочую конфигурацию. Поэтому из состояния (2, 0, 1п) (переключатель исправен и параллельно работают два элемента, один из которых рабочий, а другой – резерв, подключенный на место отказавшего рабочего) возможен переход в три состояния:

(1, 0 , 1п) (1) – при отказе рабочего элемента

(1, 0, 1п) (2) – при отказе резерва, заменившего отказавший рабочий элемент

(1, 0, 0п) – при отказе переключателя, который делает недоступным резерв, заменивший отказавший рабочий элемент.

Схема гибридного резервирования с ненадежным переключателем моделируется деревом (рис.6.16). Здесь каждая SPARE вершина имеет уникальные SPARE события, соответствующие жестко закрепленным за рабочими элементами “холодным” резервам (Event36, Event38). Отказ переключателя, моделируемый FDEP вершиной, приводит к одновременному отказу обоих резервов. Соответствующая марковская модель приведена на рис.6.17.

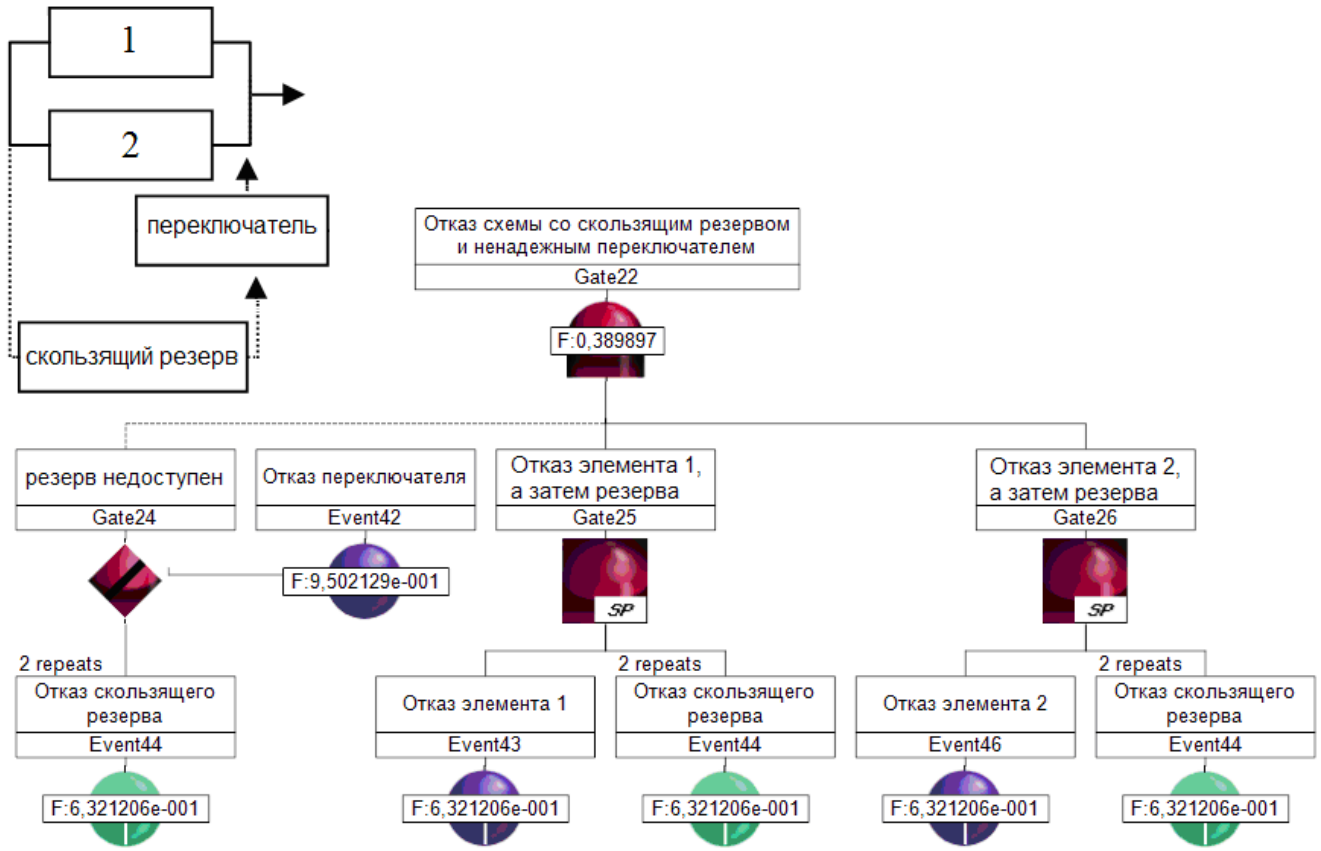


Рис. 6.14. Сложное динамическое дерево отказов схемы скользящего резервирования с ненадежным переключателем.

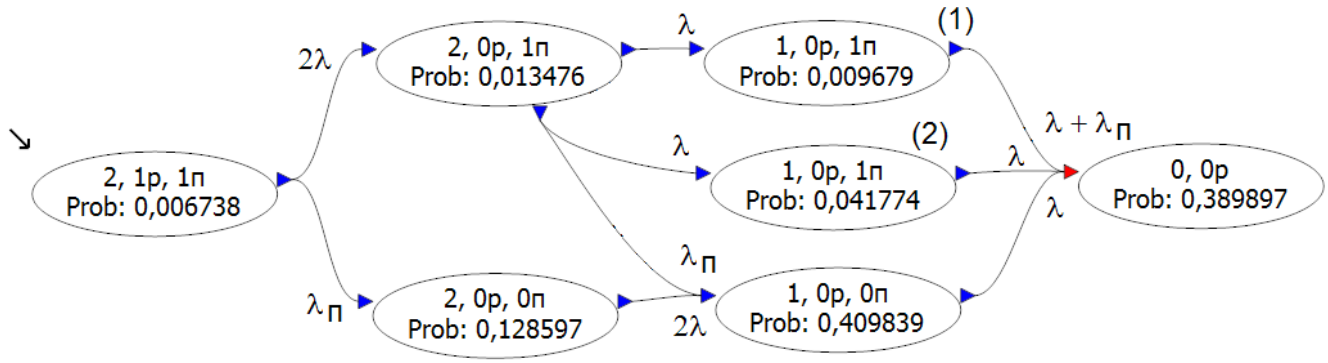


Рис.6.15. Марковская модель динамического дерева отказов схемы со скользящим резервированием и ненадежным переключателем.

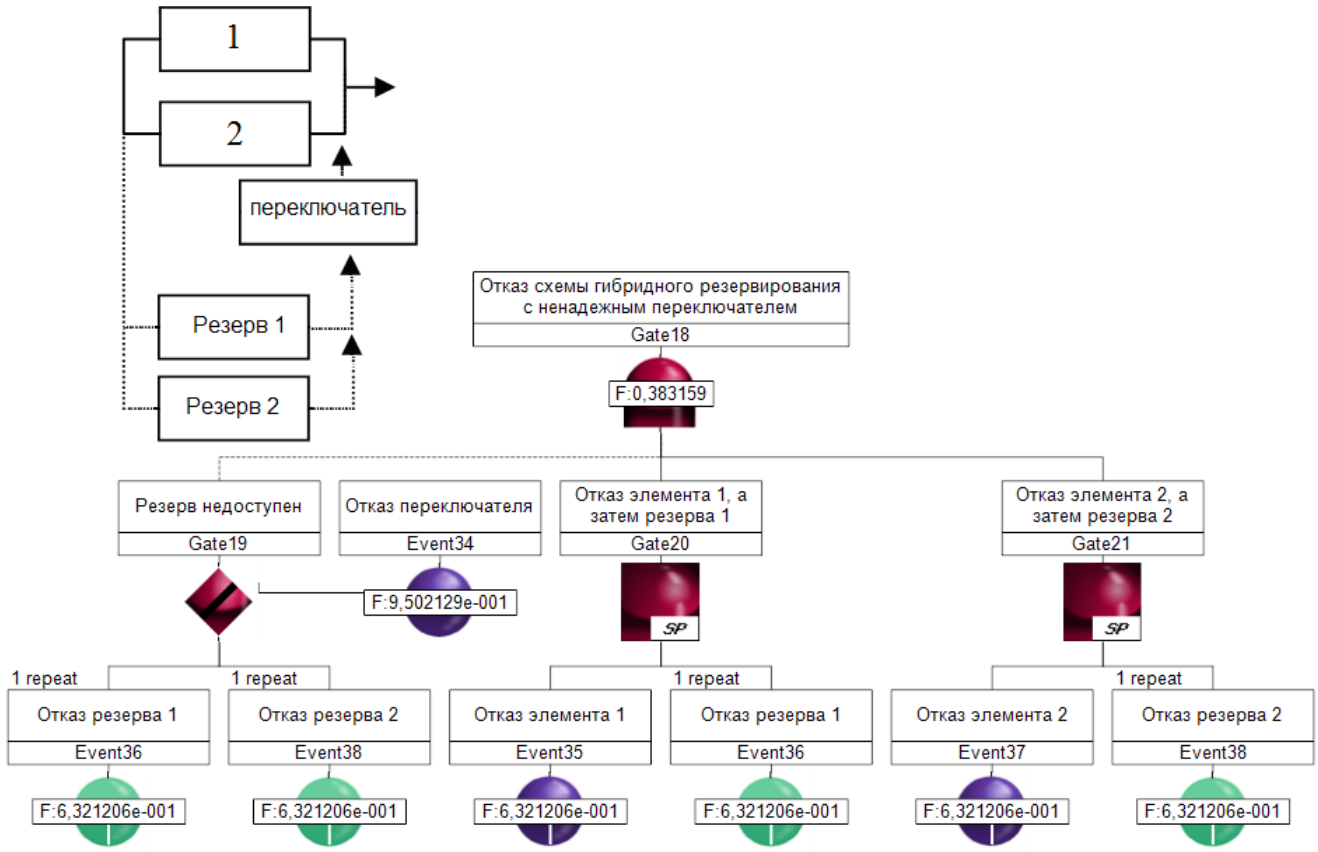


Рис. 6.16. Сложное динамическое дерево отказов схемы гибридного резервирования с ненадежным переключателем.

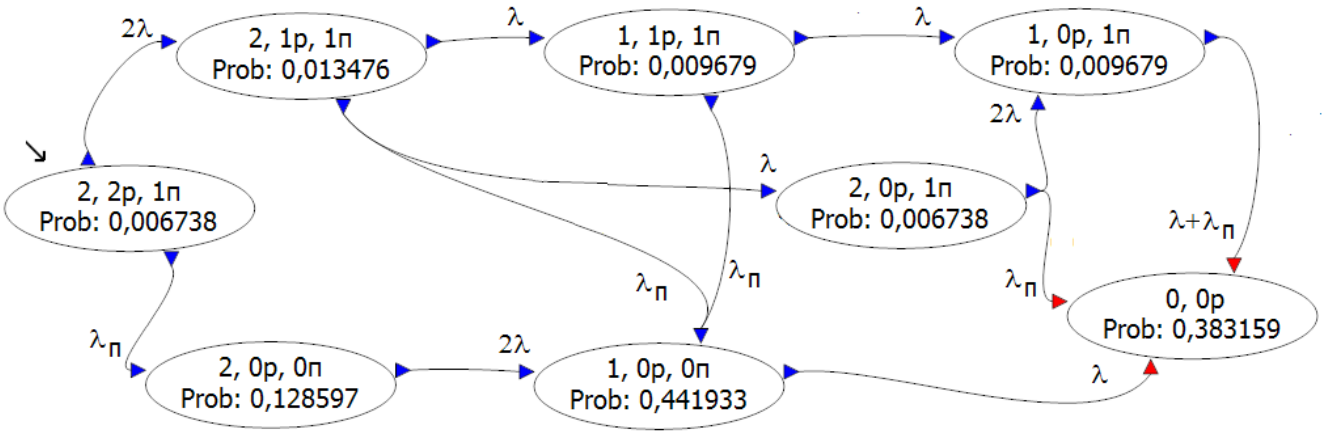


Рис.6.17. Марковская модель динамического дерева отказов схемы гибридного резервированием с ненадежным переключателем.

В заключение отметим, что, хотя деревья отказов являются широко распространенным на практике аппаратом анализа надежности, имеются ограничения на их использование для анализа надежности сложных систем, связанные с невозможностью учета последовательности и зависимости отказов логико-вероятностными методами. Снятие этих ограничений достигается

введением динамических вершин деревьев отказов, реализуемых с помощью марковских моделей. Использование динамических деревьев отказов позволяет строить более адекватные модели и, как следствие, повысить точность расчетов показателей надежности сложных систем. Кроме того, динамические вершины являются эффективным средством борьбы с размерностью марковских моделей надежности за счет автоматизации их построения. Применяемые в настоящее время и внедренные в ведущие программные комплексы анализа надежности динамические вершины реализуются только на марковских моделях. Дальнейшее направление исследований в данной области может быть связано с привлечением статистического моделирования и полумарковских случайных процессов для реализации динамических вершин деревьев отказов.

Глава 7. Анализ видов, последствий и критичности отказов

В отечественной нормативной документации [115, 116] анализ видов и последствий отказов (сокр. АВПО или АВОП) определяется как “формализованная, контролируемая процедура качественного анализа проекта, технологии изготовления, правил эксплуатации и хранения, системы технического обслуживания и ремонта изделия, заключающаяся в выделении на некотором уровне разукрупнения его структуры возможных (наблюдаемых) отказов разного вида, в прослеживании причинно-следственных связей, обуславливающих их возникновение, и возможных (наблюдаемых) последствий этих отказов на данном и вышестоящих уровнях, а также - в качественной оценке и ранжировании отказов по тяжести их последствий”.

Наиболее развитой и распространенной формой АВОП является проектный анализ видов и последствий отказов компонентов технической и функциональной структур проектируемой системы. Как правило, АВОП является первым и одним из важнейших этапов проектного исследования надежности и безопасности систем. Результаты выполнения АВОП на стадии проектирования имеют как самостоятельное значение для характеристики надежности и безопасности проектируемой системы, так и могут использоваться как исходные данные для проведения дальнейшего более детального анализа надежности на логико-вероятностных и марковских моделях, рассмотренных в предыдущих главах.

Общепринятой международной аббревиатурой для обозначения качественного и упрощенного количественного анализа видов и последствий отказов является FMEA (failure mode and effect analysis). Если проводятся количественные оценки, то употребляется термин FMECA (failure mode effect and criticality analysis – анализ видов, последствий и критичности отказов). Первые опыты проведения FMEA относятся к аэрокосмическим проектам 60-х годов СССР и США. В 80-х годах процедуры FMEA стали внедряться в автомобильной промышленности США в Ford Motor Company. В настоящее время анализ видов и последствий отказов является обязательным этапом проектной оценки надежности и безопасности объектов космической, авиастроительной, атомной, химико-технологической, газо-нефтеперерабатывающих и др. отраслей. В областях, где этот этап не является обязательным, возникают опасные инциденты, приводящие к большим экономическим и экологическим потерям и угрожающие жизни и здоровью людей. Достаточно вспомнить драматические события обрушения публичных московских зданий, построенных по проектам, где дефект лишь одного элемента несущей конструкции (штифта, колонны) привел к катастрофическим последствиям.

FMEA выполняется во всех международных технических проектах, осуществляемых в нашей стране, поэтому при введении наиболее употребляемых терминов мы будем приводить их английский перевод.

Можно выделить следующие этапы выполнения FMEA/FMECA на стадии проектирования:

- построение иерархической, функциональной или технической, структуры системы
- выявление потенциально-возможных видов отказов/неисправностей (failure modes) компонентов структуры и определение их влияния на работоспособность самого анализируемого компонента (local effect); блока, подсистемы, функции, к которой он относится (next higher level effect); системы в целом (end effect)
- определение возможных причин возникновения видов отказов (cause of failure) и способов (средств) их обнаружения (failure detection method)
- классификация и балльная оценка видов отказов по частоте возникновения (occurrence), уровням критичности/серьезности/тяжести последствий (severity), возможности обнаружения средствами контроля (detection) и вычисление агрегированной балльной оценки каждого вида отказа
- проведение расчетов показателей критичности для каждого уровня иерархии технической или функциональной структуры системы
- графическая интерпретация результатов анализа в виде матриц критичности и диаграмм уровней риска
- выдача рекомендаций по пересмотру проектных решений с целью компенсации или устранения опасных видов отказов; возможная последующая оценка эффективности этих рекомендаций

FMEA является наиболее стандартизованной областью “надежностных” исследований. Процедура проведения и вид входной/выходной документации регламентируется соответствующими стандартами. Международно признанными являются документы:

- MIL-STD-1629 - руководство по проведению анализа видов и последствий отказов, оценки критичности, выявлению узких мест конструкций с точки зрения ремонтопригодности и живучести. Первоначально был ориентирован на военные применения.
- SAE J1739, AIG-FMEA3, FORD FMEA – пакет документов, регламентирующих проведение анализа видов и последствий отказов для объектов автомобильной промышленности, включая стадии проектирования и изготовления

– SAE ARP5580 – руководство по проведению FMEA как коммерческих, так и военных проектов, объединяющее положения MIL-STD-1629 и автомобильных стандартов. Введено понятие групп эквивалентных отказов, т.е. отказов, порождающих одинаковые последствиями и требующих проведения одинаковых корректирующих действий.

Общим для всех стандартов является то, что они регламентируют лишь последовательность и взаимосвязь этапов анализа, оставляя проектировщику свободу действий при конкретной реализации каждого этапа. Так, допускается произвольная настройка структуры таблиц FMEA, определение шкал частот возникновения отказов и тяжести последствий, введение дополнительных признаков классификации отказов и пр.

7.1. Описание структуры

АВОП может проводиться относительно

– функциональной структуры системы (functional FMEA)
– технической структуры системы (component FMEA)
– процессов изготовления и обслуживания системы (process FMEA)

Рассмотрим возможные виды и этапы АВОП на примере планшетного компьютера промышленного типа, данные для которого взяты из демонстрационного проекта Windchill Quality Solutions “Tablet PC”.

Техническая структура планшетного ПК имеет три уровня иерархии, как показано в таблице 7.1. Уровень 0 – это сам планшетный ПК. Уровень 1 или уровень агрегатов (assembly) содержит 3 компонента (системная плата, плата памяти, сборка жесткого диска). Уровень 2 это уровень элементов (part), к которому относятся аккумулятор, сенсорная панель, микропроцессор, SRAM, тактовый генератор, видеопроцессор, DRAM, контроллер DRAM, жесткий диск, контроллер RAID. На каждый компонент (помимо описательной информации) задаются или вычисляются интенсивности отказов, необходимые для дальнейших расчетов показателей критичности. Интенсивности отказов элементов вычисляются согласно методикам соответствующих нормативных документов [31-35,38,39] или задаются на основе статистических данных [36,37].

Упрощенная функциональная структура приведена в таблице 7.2, где выделены две основные функциональные подсистемы ПК – обрабатывающая секция и устройство ввода.

FMEA процесса изготовления рассмотрим на примере пайки и сборки аккумуляторной батареи (таблица 7.3).

Таблица 7.1. Промышленный планшетный ПК (техническая структура).

Наименование системы/агрегата/элемента	Идентификатор (part number)	Количество	Инт.отк *10-6 (1/ч)	Уровень
Промышленный планшетный ПК	PC070101	1	23.175339	0
Аккумуляторная батарея (АБ)	BAT56A04	1	2.242700	2
Сенсорная панель	TP55401A	1	6.550000	2
Системная плата	MB060415	1	5.298192	1
Микропроцессор (МП)	MIC870A	1	4.670594	2
Статическое ОЗУ (SRAM)	SRAM031	4	0.512888	2
Тактовый генератор (ТГ)	CLKS04	1	0.056319	2
Видеопроцессор (ВП)	VP899011	1	0.058390	2
Плата памяти	MEM061789	1	1.355120	1
Контроллер DRAM	DRAMC7001	1	0.958604	2
Динамическое ОЗУ (DRAM)	DRAM512-31	2	0.396516	2
Сборка жесткого диска	HD061455	1	7.729327	1
Контроллер RAID	RAID-023C	1	0.229327	2
Жесткий диск	HD70AS-500	2	7.500000	2

Таблица 7.2. Промышленный планшетный ПК (функциональная структура).

Наименование системы/функциональной подсистемы	Описание функции
Промышленный планшетный ПК	
Обрабатывающая секция	Передача и обработка данных
Устройство ввода данных	Запуск приложений, ввод данных, взаимодействие с операционной системой

Таблица 7.3 Аккумулятор (этапы процесса изготовления).

Наименование Процесса	Описание процесса
Аккумуляторная батарея	
Сборка	Сборка и проклейка аккумуляторных пластин, соединение с печатной платой
Пайка	Пропайка печатной платы и выводов на клеммы

7.2. Формирование списков потенциальных отказов

Вне зависимости от вида АВОП при формировании списка потенциальных отказов рекомендуется применение подхода “снизу-вверх”, при котором возможные виды отказов перечисляются для компонентов нижнего уровня (элементов), а их последствия оцениваются с точки зрения влияния на подсистемы следующего уровня и систему в целом. Для обеспечения целостности данных рекомендуется не задавать виды отказов компонентов высших уровней иерархии, а формировать их на основе локальных последствий (local effect) компонентов низших уровней. Эти рекомендации используются при автоматизации АВОП. Процедура автоматического порождения списков потенциальных отказов компонентов всех уровней иерархии, кроме низшей (элементы), называется “Roll Up FMEA”. Список видов отказов для элементов формируется в результате совместной работы проектировщиков системы и специалистов по надежности. Для облегчения этого трудоемкого и плохо формализуемого процесса можно использовать специальные базы данных и издаваемые на их основе справочники по видам отказов электронного, механического, электромеханического, теплотехнического и химико-технологического оборудования (FMD91, FMD97, MIL-HDBK-338, NPRD3, RADC-TR-84-244, OREDA).

Виды отказов элементов планшетного ПК сведены в таблице 7.4[4]. На основании последствий отказов компонентов нижнего уровня (уровень 2) сформированы списки видов отказов агрегатов (уровень 1, таблица 7.5). Исходя из последствий отказов агрегатов, сформирован список видов и причин отказов планшетного ПК (уровень 0, таблица 7.6).

Таблица 7.4. Виды отказов элементов планшетного ПК (уровень 2).

Компонент/Функция	Вид отказа	Последствие	Критич-ность	Частота	Обнару-жение	R.P.N.
Микропроцессор (МП)/ Управление ПК, выполнение арифметических и логических операций	Ухудшение характеристик	Ухудшение функциональности процессора	7	2	2	28
	Обрыв или короткое замыкание микросхем	Отказ процессора	9	1	1	9
Статическое ОЗУ (SRAM)/ Хранение и произвольная выборка данных	Потеря битов данных	Потеря информации	9	1	1	9
	Обрыв или короткое замыкание микросхем	Отказ SRAM	9	1	1	9

[4] Пример FMEA планшетного ПК носит учебный, демонстрационный характер, поэтому рассматривается усеченный список видов отказов элементов с упрощенными формулировками.

Тактовый генератор (ТГ)/ Генерация синхроимпульсов	Залипание выхода на низком или высоком уровне	Залипание выхода ТГ на одном из уровней	9	1	1	9
	Обрыв входа или выхода	Нет сигнала ТГ	9	1	1	9
Контроллер/ Управляет вводом/выводом информации в/из DRAM	Ухудшение рабочих характеристик	Полная или частичная потеря функциональности контроллера	9	1	2	18
	Обрыв или короткое замыкание микросхем	Отказ контроллера	9	1	1	9
Динамическое ОЗУ/ Хранение информации	Потеря битов данных	Потеря информации	9	1	1	9
	Обрыв или короткое замыкание микросхем	Отказ динамического ОЗУ	9	1	1	9
Контроллер RAID/ Управление диском	Функциональный отказ	Отказ RAID контроллера	9	2	1	18
	Обрыв или короткое замыкание микросхем	Отказ RAID контроллера	9	2	1	18
Жесткий диск/ Хранение данных	Неисправность накопителя	Отказ жесткого диска	9	2	1	18
	Отказ микросхем	Отказ жесткого диска	9	2	1	18
Видеопроцессор (ВП)/ Управление видеовыходом ПК	Обрыв или короткое замыкание микросхем	Отказ ВП	7	3	1	21
	Прочие виды неисправностей	Отказ ВП	9	1	1	9
Аккумуляторная батарея (АБ)/ Источник электрической энергии	Ухудшение рабочих характеристик	Снижение выходной мощности АБ	7	2	3	42
	Прочие виды неисправностей (отказы входных/выходных цепей, предохранителя, трансформатора)	Отказ АБ	7	2	1	14
	Утечки	Нанесение ущерба оборудованию или человеку из-за утечек АБ	10	1	1	10

Таблица 7.5. Виды отказов агрегатов планшетного ПК (уровень 1).

Компонент/Функция	Вид отказа	Последствие	Критич-ность	Частота	Обнару-жение	R.P.N.
Системная плата/ Объединяет и координирует работу МП, SRAM. ТГ, ВП	Ухудшение функциональности процессора	Ухудшение функциональности системной платы	7	2	2	28
	Отказ процессора	Отказ системной платы	9	1	1	9
	Потеря данных SRAM	Отказ системной платы	9	1	1	9
	Отказ SRAM	Отказ системной платы	9	1	1	9
	Залипание выхода ТГ на одном из уровней	Отказ системной платы	9	1	1	9
	Нет сигнала ТГ	Отказ системной платы	9	1	1	9
	Отказ ВП	Отказ системной платы	9	2	1	18
Плата памяти (DRAM)/ Хранение результатов вычислений процессора	Потеря информации	Отказ DRAM	9	1	1	9
	Полная или частичная потеря функциональности контроллера	Отказ DRAM	9	1	2	18
	Отказ контроллера	Отказ DRAM	9	1	1	9
	Отказ динамического ОЗУ	Отказ DRAM	9	1	1	9
Накопитель на жестком диске (HDD)/ Энергонезависимое хранение данных	Отказ RAID контроллера	Отказ HDD	9	2	1	18
	Отказ жесткого диска	Отказ HDD	9	2	1	18
Сенсорная панель/ Ввод информации и управляющих воздействий	Отсутствие реакции на прикосновение	Отказ сенсорной панели	9	3	1	27
	Неточное позиционирование	Потеря управления сенсорной панелью	7	3	1	21

Таблица 7.6. Виды отказов планшетного ПК (уровень 0).

Компонент/ Функция	Вид отказа	Последствие	Причины	Кр.	Ч-а	Обн.	R.P.N.	Коррект. действия	Кр.	Ч-а	Обн.	R.P.N.
Промышленный планшетный ПК/ Обработка и хранение информации	Отказ сенсорной панели	Отказ ПК	Отказ компонентов сенсорной панели	9	3	1	27	Закупка оборудо-вания у официаль-ных дистри-бьюторов компаний с хорошей репутацией	9	1	1	9
	Потеря управления сенсорной панелью	Неустойчивое взаимодействие с ПК	Отказ компонентов сенсорной панели	7	3	1	21		7	1	1	7
	Ухудшение функциональности системной платы	Ухудшение характеристик функционирования ПК	Ухудшение функциональности компонентов системной платы (МП, SRAM, ТГ, ВП)	7	3	2	42		7	1	1	7
	Отказ системной платы	Отказ ПК	Отказ компонентов системной платы (МП, SRAM, ТГ, ВП)	9	1	1	9		9	1	1	9
	Отказ DRAM	Отказ ПК	Отказ компонентов DRAM (контроллера, микросхем памяти)	9	1	2	18		9	1	1	9
	Отказ HDD	Потеря информации	Отказ компонентов HDD (диска, RAID контроллера)	9	2	1	18		9	1	1	9
	Отказ АБ	Отказ ПК	Отказ компонентов АБ (входные/выходные цепи, трансформатор, предохранители)	7	2	1	14	Увеличение частоты техничес-ких осмотров и повышение качества техничес-кого обслужи-вания	7	1	1	7
	Нанесение ущерба оборудованию или человеку из-за утечек АБ	Гарантийные или правовые разбирательства	Утечки тока в АБ	10	1	1	10		10	1	1	10
	Снижение выходной мощности АБ	Ухудшение характеристик функционирования ПК	Ухудшение рабочих характеристик компонентов АБ	7	2	3	42		7	1	1	7

7.3. Балльная оценка видов отказов и ее графическая интерпретация.

При выполнении количественных оценок проектных решений по FMEA виды отказов компонентов принято характеризовать с точки зрения частоты возникновения, возможности обнаружения различными средствами контроля, тяжести последствий. Если расчеты носят предварительный характер и проводятся на самых ранних этапах проектирования, то обычно используют балльные экспертные оценки этих параметров.

Индикатором тяжести последствий может являться как число, так и словесное описание. Примерами шкал (списков) для характеристики тяжести последствий видов отказов являются: {1,2,3,4}, {*Catastrophic*,*Hazardous*,*Major*,*Minor*}-применяется в зарубежном самолетостроении, {Катастрофический, Аварийный, Сложная ситуация, Усложнение условий полета} - применяется в отечественном самолетостроении; {1,2,3,4,5,6,7,8,9,10} – применяется в зарубежном автомобилестроении. Тяжесть последствий ухудшается справа-налево. Каждому значению списка присваиваются определенные баллы. Пример классификации видов отказов по тяжести последствий приведен в таблице 7.7.

Таблица. 7.7. Классификация видов отказов по тяжести последствий.

Вид отказа	Тяжесть последствий	Кате-гория	B_1, баллы
Катастрофический	Отказ приводит к смерти людей, потере объекта, наносит невосполнимый (в обозримое время) ущерб окружающей среде	I	9 – 10
Критический	Отказ приводит к невыполнению объектом своих функций, что может угрожать жизни людей, приводить к потере объекта, наносить вред окружающей среде	II	7 – 8
Некритический	Отказ приводит к экономическим потерям.	III	4 – 6
Несущественный	Несущественный отказ с пренебрежимо малыми последствиями, которые не относятся ни к одной из перечисленных категорий.	IV	1 – 3

Шкалы частот видов отказов для военных объектов имеют обычно 5 позиций - {Frequent, Reasonable Probable, Occasional, Remote, Extremely Unlikely}, {Частый, Вероятный, Редкий, Очень редкий, Невероятный}; в автомобильной промышленности -10 позиций {1,2,3,4,5,6,7,8,9,10}.

Экспертная интерпретация частоты отказа достаточно относительная и зависит от области применения анализируемого объекта. Для объектов общепромышленного применения и авиастроения категории видов отказов, например, “редкий”, по значению показателя

интенсивности отказов могут отличать в несколько порядков. Пример классификации видов отказов по частоте для опасных производственных объектов приведен в таблице 7.8.

Таблица 7.8. Классификация видов отказов по частоте.

Характеристика частоты отказов	Интенсивность отказов [1/ч]	B_2, баллы
Невероятный	$10^{-9} – 10^{-8}$	1 – 2
Очень редкий	$10^{-8} – 10^{-7}$	3 – 4
Редкий	$10^{-7} – 10^{-6}$	5 – 6
Вероятный	$10^{-6} – 10^{-4}$	7 – 8
Частый	$> 10^{-4}$	9 – 10

Возможность обнаружения видов отказов обычно также оценивается по десятибалльной шкале. Так, например, в [115] приведен следующий пример классификации видов отказов по вероятности их обнаружения до поставки изделия потребителю:

Таблица 7.9. Оценка вероятности обнаружения отказа до поставки изделия потребителю

Виды отказов по вероятности обнаружения до поставки	Вероятность обнаружения отказа, оцененная расчетным или экспертным путем	Оценка вероятности в баллах B_3
Очень высокая вероятность выявления отказа при контроле, сборке, испытаниях	Более 0,95	1
Высокая вероятность выявления отказа при контроле, сборке, испытаниях	От 0,95 до 0,85	2-3
Умеренная вероятность выявления отказа при контроле, сборке, испытаниях	От 0,85 до 0,45	4-6
Высокая вероятность поставки потребителю дефектного изделия	От 0,45 до 0,25	7-8
Очень высокая вероятность поставки потребителю дефектного изделия	Менее 0,25	9-10

Агрегированная балльная оценка риска вида отказа, характеризующая тяжесть последствий, частоту и степень выявления, рассчитывают как произведение баллов $B_1 \cdot B_2 \cdot B_3$. В западной литературе этот агрегированный балльный показатель называют R.P.N. – Risk Priority Number.

Обычно R.P.N рассчитывают для видов отказов всех компонент иерархической структуры – элементов (таблица 7.4), агрегатов (таблица 7.5), системы в целом (таблица 7.6). Полезным для демонстрации эффективности корректирующих действий является проведения повторных вычислений этого показателя, как это показано в таблице 7.6.

Удобной графической интерпретацией расчетов критичности видов отказов является матрица критичности. Строки этой матрицы обычно соответствуют шкале частоты, а столбцы – шкале тяжести последствий. Возможно любая другая попарная комбинация шкал частоты, тяжести последствий, обнаружения. Фиксированному значению частоты-тяжести последствий соответствует количество отказов, выявленных в ходе проведения FMEA. Так на рис.7.1. показана матрица критичности, соответствующая таблицам FMEA промышленного планшетного ПК (табл.7.4-7.6). На матрице критичности посредством выбора граничных значений шкал можно задать уровни риска (risk level). Обычно задают три уровня риска – высокий (high), средний (medium), низкий (low). На рис. 7.1. высокому уровню риска соответствуют виды отказов с $7 \leq B_1 \leq 10$ и $7 \leq B_2 \leq 10$; среднему с $3 \leq B_1 < 7$ и $3 \leq B_2 < 7$; низкому $0 < B_1 \leq 2$ и $0 < B_2 \leq 2$. Относительно видов отказов, распределенных по разным областям риска, могут быть рекомендованы различные корректирующие мероприятия от минимальных до полного пересмотра проектных решений.

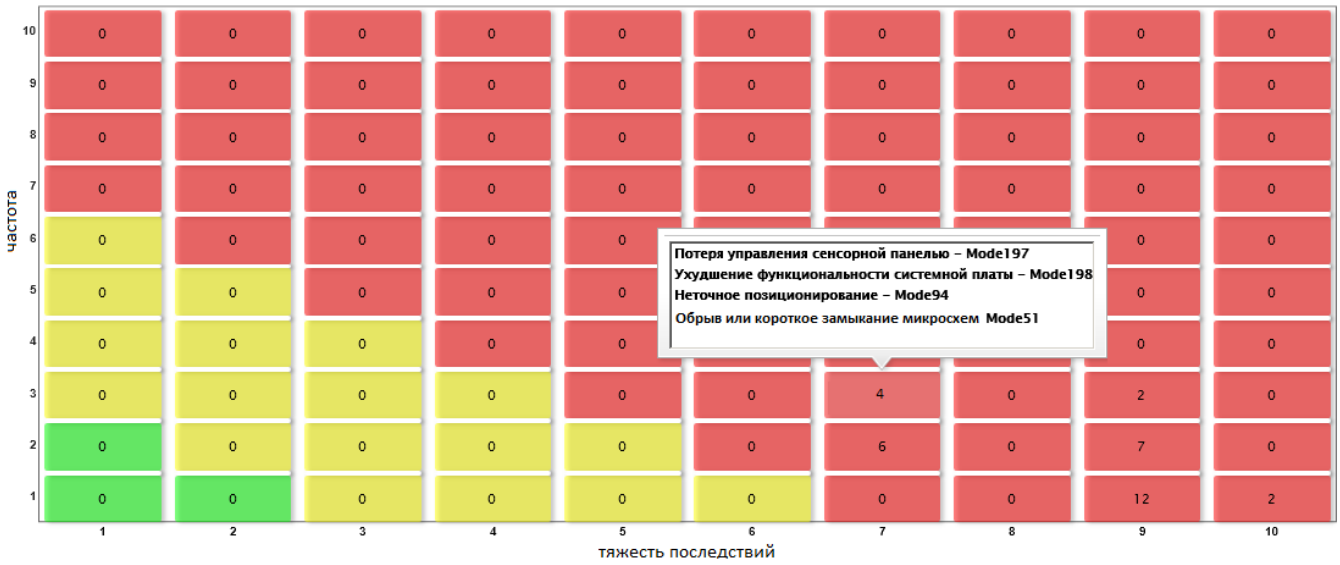


Рис.7.1. Матрица критичности промышленного планшетного компьютера.

7.4. Количественный расчет показателей критичности.

Количественный расчет показателей критичности, регламентируемый стандартом MIL-STD-1629, проводится на более поздних этапах проектирования, когда аналитикам уже могут быть известны надежностные характеристики элементной базы проектируемой системы, этапы

выполнения задания и условия эксплуатации. В этом случае по отношению к видам отказов и компонентам системы могут быть вычислены простые вероятностные показатели. Эти расчеты также как и балльные оценки носят предварительный характер, так как не учитывают резервирования, восстановления и других особенностей надежностного поведения сложных систем. Для проведения расчетов показателей критичности таблицу FMEA дополняют следующими столбцами:

- суммарная интенсивность отказов i-го компонента (λ_i)
- доля каждого вида отказов от суммарной интенсивности (α_{ij})
- условная вероятность того, что данный вид отказа приведет к последствиям данной тяжести, при условии, что данный вид отказа произошел (β_{ij})

На основе значений этих столбцов вычисляют следующие показатели:

Критичность j-го вида отказа i-го компонента системы на интервале времени (0÷t)

$$C_{ij} = \alpha_{ij} \cdot \beta_{ij} \cdot \lambda_i t \tag{7.1}$$

Критичность i-го компонента системы на интервале времени (0÷t)

$$C_i = \sum_{j=1}^{m} \alpha_{ij} \cdot \beta_{ij} \cdot \lambda_i t \tag{7.2}$$

Распределение критичности видов отказа i-го компонента по уровням r=[1÷l] тяжести последствий sev:

$$C_{ir} = \sum_{j:sev_j = r} C_{ij} \tag{7.3}$$

где l – количество категорий (уровней) тяжести последствий. В MIL-STD-1629 используются четыре категории {*Catastrophic (I), Critical (II), Marginal (III), Minor (IV)*} и четыре градации условной вероятности β_{ij} {*Actual loss(β_{ij}=1), Probable loss(0.1<β_{ij}<1), Possible loss (0<β_{ij}≤0.1, No effect (β_{ij}=0)*}.

Результаты анализа видов, последствий и критичности отказов планшетного ПК сведены в таблицу 7.10.

Таблица 7.10. Расчет показателей критичности видов отказов планшетного ПК.

Компонент/ Интенсивность отказов [1/ч]/ Время функционирования [ч]	Вид отказа	α(%)	β	Sev	C_j	C	Распределение критичности
Промышленный планшетный ПК/ $\lambda = 0.001$ / $t = 8760$	Отказ сенсорной панели	3	1	II	0.2628	8.6724	I -0.0876; II – 5.5188; III – 0; IV – 3.066
	Потеря управления сенсорной панелью	5	1	IV	0.4387		
	Ухудшение функциональности системной платы	10	1	IV	0.8767		
	Отказ системной платы	20	1	II	1.752		
	Отказ DRAM	20	1	II	1.752		
	Отказ HDD	20	1	II	1.752		
	Отказ АБ	10	1	IV	0.876		
	Нанесение ущерба оборудованию или человеку из-за утечек АБ	2	0.5	I	0.0876		
	Снижение выходной мощности АБ	10	1	IV	0.876		

При проектировании уникальных технических объектов, в условиях отсутствия информации по объектам-аналогам результаты проведения FMEA являются одним из основных источников исходных данных для различных направлений исследований свойств сложных систем, в частности, анализа безопасности, контролепригодности, логистики. В соответствии с документом MSG-3 FMEA является основой проектной разработки рекомендаций по проведению планового технического обслуживания объектов (самолетов, электростанций…) на начальной стадии их эксплуатации.

Приложение 1. Случайные события. Основные формулы теории вероятностей.

Одним из основных понятий теории вероятностей является понятие случайного события. Любая качественная характеристика результата опыта есть событие. События можно разделить на три вида – достоверные, невозможные, случайные.

- достоверное событие - событие, обязательно происходящее в результате опыта
- невозможное событие - событие, заведомо не происходящее в результате опыта
- случайное событие - событие, которое либо происходит, либо не происходит в результате опыта.

Случайные события могут быть совместными и несовместными.

События называются совместными, если появление одного из них не исключает появление других событий

События называются несовместными, если появление одного из них исключает появление других событий

Случайные события бывают зависимые и независимые.

Независимые события - появление одного из них не влияет на появление других

Зависимые события - появление одного из них влияет на появление других

Противоположное (дополнительное) событие относительно случайного события A есть событие $\bar{A}$, состоящее в непоявлении A.

Полная группа событий – такая совокупность событий, что в результате опыта обязательно должно произойти хотя бы одно из событий этой совокупности.

Основной теоретической характеристикой случайного события A является его вероятность P(A). В современной теории вероятностей вероятность случайного события A вводится аксиоматически [58]. Но с прикладной точки зрения вероятностью события называется число, характеризующее частоту события при большом числе опытов ($(W(A) = \frac{m}{n} \underset{n\to\infty}{\to} P(A))$, где m – число появлений событий A, n – общее число опытов.

Наиболее часто изучаемые в теории надежности случайные события – есть события отказов технических объектов.

1.Теорема сложения вероятностей.

Сумма событий A и B – это событие (A+B), состоящее в появлении событий A, B, или их обоих (AB). Для трех событий: (A+B+C) – A, B, C, AB, AC, BC, ABC.

Если A и B – несовместны, то

$$P(A+B) = P(A) + P(B) \qquad (П1.1)$$

Если A и B – совместны, то

$$P(A+B) = P(A) + P(B) - P(AB) \qquad (П1.2)$$

Для иллюстрации на рис.1. показана сумма двух событий A и B как область, объединенная жирной чертой. a) соответствует случаю, когда A и B совместны, b) – несовместны.

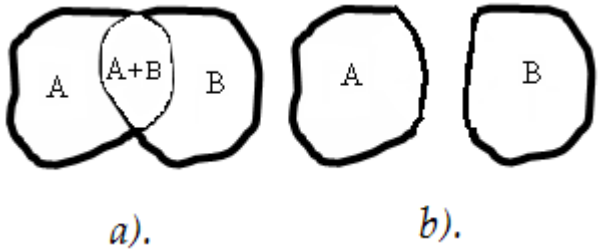


Рис. П1.1. Объединение событий A и B.

Теорема обобщается на произвольное число событий.

Если A, B, C, … - полная группа несовместных событий, то

$$P(A) + P(B) + P(C) + \ldots = 1 \qquad (П1.3)$$

Для противоположных событий:

$$P(A) + P(\bar{A}) = 1 \qquad (П1.4)$$

2. Теорема умножения вероятностей

Произведение событий A, B – это событие, состоящее в совместном появлении событий (AB)

Если A и B – независимы, то

$$P(AB) = P(A)*P(B) \qquad (П1.5)$$

Если A и B – зависимы, то

$$P(AB) = P(A)*P(B/A) = P(B)*P(A/B), \qquad (П1.6)$$

где P(B/A) – условная вероятность появления события B при условии, что событие A произошло

Теорема обобщается на произвольное число событий.

3. Формула полной вероятности.

Пусть $B_1, B_2, \ldots B_n$ – полная группа несовместных событий. Случайное событие A наступает при наступление одного из B. Тогда вероятность появления события A равна

$$P(A)=P(B_1)P(A/B_1)+ P(B_2)P(A/B_2) +\ldots+ P(B_n)P(A/B_n) \qquad (П1.7)$$

Приложение 2. Основные положения и соотношения алгебры логики.

Функции, принимающие лишь два значения (1 или 0) и определяемые различными наборами двоичных аргументов, называются функциями алгебры логики (ФАЛ). ФАЛ могут быть заданы в табличном или формульном виде. Табличное представление ФАЛ, при котором перечисляются все возможные значения аргументов (переменных) и указываются соответствующие им значения функции, называют таблицей истинности.

В алгебре логики рассматриваются три основные операции над логическими переменными:

Отрицание (инверсия). Если A – высказывание (принимает значение 1 –истина, 0 – ложь), то отрицание A обозначается как $\overline{A}$ и читается, как "не A". $\bar{1}=0, \bar{0}=1$

Конъюнкция (умножение, пересечение): A&B или A*B или A∧B. Читается как "A и B". 0&0=0, 0&1=0, 1&0=0, 1&1=1.

Дизъюнкция (сложение, объединение): A+B или A∨B. Читается как "A или B". 0 ∨ 0=0, 0 ∨ 1=1, 1 ∨ 0=1, 1 ∨ 1=1

Преобразование логических выражений осуществляется по определенным правилам, которые легко доказываются, либо очевидны.

Правила для одной переменной.

1. $A \wedge 1 = A$ 2. $A \wedge 0 = 0$ 3. $A \wedge A = A$ 4. $A \wedge \overline{A} = 0$

5. $A \vee 1 = 1$ 6. $A \vee 0 = A$ 7. $A \vee A = A$ 8. $A \vee \overline{A} = 1$

9. $\overline{\overline{A}} = A$ 10. $\overline{\overline{\overline{A}}} = \overline{A}$

Правила для двух, трех переменных.

Сочетательный (ассоциативный) закон.

11. $A \wedge (B \wedge C) = (A \wedge B) \wedge C = A \wedge B \wedge C$ 12. $A \vee (B \vee C) = (A \vee B) \vee C = A \vee B \vee C$

В силу 11,12 логические выражения можно писать без скобок, как в обычной алгебре, и умножение также считается старшей операцией.

Переместительный (коммутативный) закон.

13. $A \wedge B = B \wedge A$ 14. $A \vee B = B \vee A$

Распределительный (дистрибутивный) закон.

15. $A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$ 16. $A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$

Выражения 11-16 – "симметричны", т.е. получаются одно из другого заменой $\wedge$ на $\vee$ и наоборот.

Закон двойственности (инверсий).

17. $\overline{(A \wedge B)} = \overline{A} \vee \overline{B}$ 18. $\overline{(A \vee B)} = \overline{A} \wedge \overline{B}$

Если к 17,18 применить 9, то получим *формулы де Моргана:*

19. $A \wedge B = \overline{(\overline{A} \vee \overline{B})}$ 20. $A \vee B = \overline{(\overline{A} \wedge \overline{B})}$

Операция поглощения.

21. $(A \wedge B) \vee A = A$ 22. $A \wedge (B \vee A) = A$

Операция склеивания.

23. $(A \wedge B) \vee (A \wedge \overline{B}) = A \wedge (B \vee \overline{B}) = A$

Из 4 и 15 можно получить:

24. $A \wedge (\overline{A} \vee B) = AB$ 25. $A \vee (\overline{A} \wedge B) = A \vee B$

Элементарной конъюнкцией называется конъюнкция нескольких логических переменных, взятых с отрицанием или без отрицания, причём среди переменных могут быть одинаковые.

Элементарной дизъюнкцией называется дизъюнкция нескольких переменных, взятых с отрицанием или без отрицания, причём среди переменных могут быть одинаковые.

Всякую дизъюнкцию элементарных конъюнкций называют *дизъюнктивной нормальной формой* (ДНФ). Всякую конъюнкцию элементарных дизъюнкций называют *конъюнктивной нормальной формой* (КНФ).

Совершенной ДНФ логической функции (СДНФ) называется ДНФ, в которой нет равных элементарных конъюнкций и все они содержат одни и те же переменные, причём каждую переменную только один раз (возможно с отрицанием). *Совершенной КНФ* (СКНФ) называется КНФ, в которой нет равных элементарных дизъюнкций и все они содержат одни и те же переменные, причём каждую переменную только один раз (возможно с отрицанием).

Бесповторной называют формулу логической функции, в которую каждая переменная входит только один раз. Для получения бесповторной формы используют операции поглощения, склеивания, распределительный закон.

Формой перехода к замещению логической функции работоспособности (отказа) системы называется форма представления логической функции, при которой замена логических переменных вероятностями, а логических операций арифметическими позволяет получить точное значение показателя надежности. Одними из форм перехода к замещению являются СДНФ и бесповторная форма логической функции в базисе конъюнкция-отрицание. Для перехода к базису конъюнкция-отрицание выполняют исключение операции дизъюнкции по правилу де-Моргана.

Ниже приведены некоторые возможные формы представления логической функции работоспособности схемы “1 из 3” (таблица истинности, ДНФ, СДНФ, ФПЗ):

x_1	x_2	x_3	$S(x_1,x_2,x_3)$
1	1	1	1
1	1	0	1
1	0	1	1
0	1	1	1
1	0	0	1
0	1	0	1
0	0	1	1
0	0	0	0

1. ДНФ:

$$S(x_1, x_2, x_3) = x_1 \vee x_2 \vee x_3$$

2. СДНФ:

$$S(x_1, x_2, x_3) = x_1x_2x_3 \vee x_1x_2\bar{x}_3 \vee x_1\bar{x}_2x_3 \vee \bar{x}_1x_2x_3 \vee x_1\bar{x}_2\bar{x}_3 \vee \bar{x}_1x_2\bar{x}_3 \vee \bar{x}_1\bar{x}_2x_3$$

3. ФПЗ:

$$S(x_1, x_2, x_3) = x_1 \vee x_2 \vee x_3 = \overline{\bar{x}_1\bar{x}_2\bar{x}_3}$$

Приложение 3. Примеры вычисления показателя средней наработки на отказ.

Пример 1.

Рассмотрим дублированный блок с восстановлением, марковская модель надежности которого приведена ниже

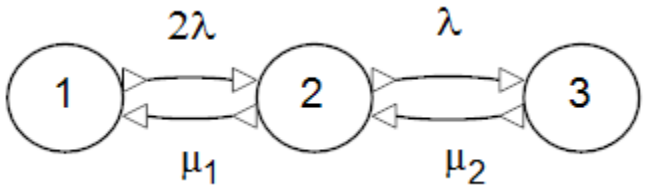


Рис. П3.1. Марковская модель надежности дублированного блока с восстановлением.

Состояние 1 – оба блока работоспособны; состояние 2 – один из блоков отказал, другой работоспособен; состояние 3 – оба блока отказали. Состояния 1 и 2 соответствуют работоспособности резервированной структуры, состояние 3 – отказ резервированной структуры. Интенсивность отказа каждого из блоков равна λ, интенсивность восстановления одного любого блока из состояния 2 равна μ_1, а из состояния 3 - μ_2.

Способ вычисления $T_{на}(t_н)$ состоит в следующем. Получим аналитическое выражение для среднего числа отказов $N_1(t)$ с использованием марковских процессов с доходами (t календарное время функционирования структуры, которое состоит из безотказной наработки $t_н$ и времени пребывания в неработоспособном для структуры состоянии 3). Устремим μ_2 в бесконечность, тогда восстановление из состояния отказа структуры будет мгновенным и время, проведенное в состоянии 3, будет равно нулю. Поэтому всё время моделирования t окажется равным безотказной наработке $t_н$. Далее проведем вычисления по (1.31), разделив t на $N_1(t)$.

Система дифференциальных уравнений для среднего числа отказов имеет вид (см. раздел 5.8, п.3)

$$\begin{aligned}
\dot{N}_1(t) &= -2\lambda N_1(t) + 2\lambda N_2(t) \\
\dot{N}_2(t) &= \mu_1 N_1(t) - (\lambda + \mu_1) N_2(t) + \lambda N_3(t) + \lambda \\
\dot{N}_3(t) &= \mu_2 N_2(t) - \mu_2 N_3(t)
\end{aligned} \qquad (П3.1)$$

Напомним, что $N_i(t)$ – среднее число отказов (определяемое выбором матрицы доходов с единицей на месте перехода из состояния 2 в состояние 3 (в матрице W w_{23}=1)) при условии начального состояния i.

Решая систему уравнений (П3.1), получим неоднородное дифференциальное уравнение третьего порядка

$$\dddot{N}_1(t)+(3\lambda+\mu_1+\mu_2)\ddot{N}_1(t)+(2\lambda^2+2\lambda\mu_2+\mu_1\mu_2)\dot{N}_1(t)=2\lambda^2\mu_2, \qquad (П3.2)$$

общее решение которого имеет вид

$$N_1(t)=C_1+C_2e^{x_1t}+C_3e^{x_2t}+\frac{2\lambda^2\mu_2 t}{2\lambda^2+2\lambda\mu_2+\mu_1\mu_2}, \qquad (П3.3)$$

где первые три слагаемых с константами C_i и корнями характеристического уравнения $x_0 = 0$, x_1, x_2 представляют собой общее решение однородного дифференциального уравнения, соответствующего уравнению (П3.1), а четвертое слагаемое – частное решение неоднородного уравнения (П3.1).

Исследуя решение (П3.3), константы C_i и корни x_j при $\mu_2 \to \infty$ получим предельное решение

$$N_1(t) \underset{\mu_2\to\infty}{\longrightarrow} \frac{2\lambda^2 t}{(2\lambda+\mu_1)}+\frac{2\lambda^2}{(2\lambda+\mu_1)^2}e^{-(2\lambda+\mu_1)t}-\frac{2\lambda^2}{(2\lambda+\mu_1)^2}\ . \qquad (П3.4)$$

Проведем некоторые численные расчеты для $T_{на}(t_н)$. Пусть $\lambda = 1\cdot E\text{-}3$ час$^{-1}$, $\mu_1 = 0{,}1$ час$^{-1}$ (соответствует среднему времени восстановления $\tau_в$=10 час.). В таблице П3.1 приведены значения (в часах) $T_{на}(t_н)$ для разных $t_н$, средняя наработка между отказами Т и средняя наработка до отказа T_1.

Таблица П3.1. Результаты расчетов показателей $T_{на}(t_н)$, Т, T_1.

	$t_н = 0{,}1$	$t_н = 1$	$t_н = 10$	$t_н = 100$	$t_н = 2000$
$T_{на}(t_н)$	14285714,3	1030927,8	136680,8	56543,2	51252,2
Т	51000				
T_1	51500				

Пример 2.

Рассмотрим один восстанавливаемый элемент с экспоненциально распределенными наработкой до отказа (с интенсивностью λ) и временем восстановления (с интенсивностью μ). Приведем формулы для вычисления основных показателей надежности.

Вероятность безотказной работы: $P(t) = e^{-\lambda t}$;

средняя наработка до отказа: T_1: = $T_{до} = 1/\lambda$;

коэффициент готовности: $К_г = \mu/(\lambda+\mu)$;

параметр потока отказов: $\omega = \mu\cdot\lambda/(\lambda+\mu)$;

средняя наработка между отказами: $T = T_{между} = 1/\lambda$;

среднее число отказов: $N_1(t) = [\mu\cdot\lambda\cdot t/(\lambda+\mu)] + [\lambda^2/(\lambda+\mu)^2]\cdot[1 - e^{-(\lambda+\mu)\cdot t}]$ и при $\mu\to\infty$

$N_1(t) \to \lambda t$, поэтому средняя наработка на отказ $T_{на}(t_н) = 1/\lambda$.

Для данного примера (одного элемента) $T_1 = T_{на}(t_н) = T$.

Пример 3.

Рассмотрим дублированный блок, аналогичный описанному в примере 1, но в данном случае предположим невозможность восстановления в процессе функционирования. А именно, система работает до отказа, после чего восстанавливается в полностью исправное состояние. Модель изображена на рис.П3.2.

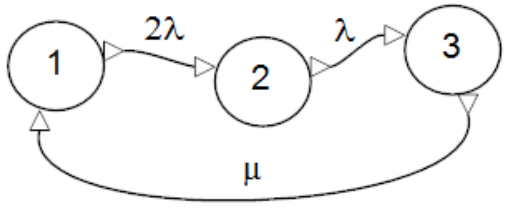


Рис.П3.2. Марковская модель надежности дублированного блока с восстановлением из состояния отказа

Система уравнений для определения $T_{до}$ имеет вид:

$$\begin{aligned} -1 &= -2\lambda\cdot T_1 \\ 0 &= 2\lambda\cdot T_1 - \lambda\cdot T_2 \end{aligned} . \qquad (П3.5)$$

Решив систему, получим известный результат

$$T_{до} = T_1 + T_2 = \frac{3}{2\lambda}. \qquad (П3.6)$$

Для определения $T_{между}$ найдем $K_г$ и ω. Система уравнений для $K_г$ имеет вид:

$$\begin{aligned} 0 &= -P_1\cdot 2\lambda + P_3\cdot\mu \\ 0 &= P_1\cdot 2\lambda - P_2\cdot\lambda \\ 1 &= P_1 + P_2 + P_3 \end{aligned} . \qquad (П3.7)$$

Решив систему П3.7, получим

$$K_г = P_1 + P_2 = \frac{3\mu}{2\lambda + 3\mu} . \qquad (П3.8)$$

Параметр потока отказов

$$\omega = P_2\cdot\lambda = \frac{2\lambda\mu}{2\lambda + 3\mu} . \qquad (П3.9)$$

Тогда

$$T_{\text{между}} = \frac{K_г}{\omega} = \frac{3}{2\lambda}\ , \qquad (П3.10)$$

т.е. совпадает с $T_{до}$.

Для определения $T_{на}$ сделаем то же, что и в примере 1. Система уравнений марковского процесса с доходами для определения среднего числа отказов имеет вид:

$$\begin{aligned} \dot{N}_1 &= -2\lambda \cdot N_1 + 2\lambda \cdot N_2 \\ \dot{N}_2 &= -\lambda \cdot N_2 + \lambda \cdot N_3 + \lambda\ . \\ \dot{N}_3 &= \mu \cdot N_1 - \mu \cdot N_3 \end{aligned} \qquad (П3.11)$$

Приведем конечный результат без промежуточных выкладок, тем более, что мы его получим и другим способом. Решая уравнения и устремляя μ к бесконечности, получим

$$N_1(t) \xrightarrow[\mu\to\infty]{} \frac{2}{9}e^{-3\lambda\cdot t} + \frac{2}{3}\lambda t - \frac{2}{9}. \qquad (П3.12)$$

Продемонстрируем ещё один способ вычисления. Выражение (П3.12) может быть получено и другим способом, если применить результаты теории восстановления. Известна такая модель как *простой процесс восстановления.* Суть этого процесса заключается в том, что новый элемент, начав функционировать в момент t=0, при отказе в момент t_1 мгновенно заменяется новым, который, проработав время t_2 и отказав, также мгновенно заменяется следующим и т.д. Плотности распределения времени безотказной работы элементов одинаковы и равны f(t). Для функции восстановления – среднего числа восстановлений за время t – известно выражение (для простого процесса восстановления) в форме преобразования Лапласа [14]. Это выражение имеет вид:

$$N(s) = \frac{f(s)}{s \cdot (1 - f(s))}, \qquad (П3.13)$$

где N(s) – преобразование Лапласа от функции восстановления;

f(s), s – преобразование Лапласа от плотности распределения и переменная преобразования, соответственно.

Отметим, что, во-первых, все время t является суммарной наработкой, т.к. время восстановления равно нулю, и, во-вторых, число восстановлений равно числу отказов, т.к. момент t=0 не считается восстановлением, а момент последнего отказа (в момент t) является и моментом восстановления из-за мгновенного восстановления.

Найдем плотность распределения для примера 3. Так как это обычное дублирование без восстановления из работоспособного состояния с одним отказом, то можно не решать систему

дифференциальных уравнений для модели рис.П3.2 с «поглощающим экраном», а непосредственно написать формулу для функции и плотности распределения F(t), f(t):

$$\begin{aligned} F(t) &= (1-\exp\{-\lambda\cdot t\})^2 \\ f(t) &= F'(t) = 2\lambda\cdot(1-\exp\{-\lambda\cdot t\})\cdot\exp\{-\lambda\cdot t\} \end{aligned}. \qquad (П3.14)$$

Преобразование Лапласа от f(t) имеет вид:

$$f(s) = \frac{2\lambda}{s+\lambda} - \frac{2\lambda}{s+2\lambda}. \qquad (П3.15)$$

Подставляя в (П3.13) и делая обратное преобразование Лапласа, получаем

$$N(s) = \frac{2\lambda^2}{s^2\cdot(s+3\lambda)} \Rightarrow \frac{2}{9}\cdot e^{-3\lambda\cdot t} + \frac{2}{3}\cdot\lambda t - \frac{2}{9} = N(t)\ , \qquad (П3.16)$$

что совпадает с (П3.12) и говорит о правильности подхода с использованием моделей марковских процессов с доходами.

Применение марковских моделей при наличии программного продукта, реализующего численные процедуры решения алгебраических и дифференциальных уравнений, лучше, чем применение операционных преобразований, например, Лапласа. Дело в том, что «ручное» применение преобразования Лапласа все равно требует решения характеристического уравнения для нахождения корней. А это возможно (для размерностей больше 2) лишь на машине численными методами. Далее, в общем виде (не с числами, а с выражениями!) необходимо осуществить ряд преобразований и найти как прямое преобразование, так и обратное, опять предварительно осуществив ряд преобразований с выражениями. При больших размерностях выполнить такие преобразования практически невозможно. Численные же алгоритмы преобразований Лапласа весьма сложны, да и мало известны. Напротив, алгоритмы численного решения дифференциальных и алгебраических уравнений хорошо известны и достаточно просты (даже если иметь в виду жесткие, плохо обусловленные системы уравнений [98]).

Окончательно для примера 3 имеем:

$$T_{на} = \frac{t}{\frac{2}{9}\cdot e^{-3\lambda\cdot t} + \frac{2}{3}\cdot\lambda t - \frac{2}{9}}. \qquad (П3.17)$$

Очевидно, что при $t \to \infty$ $T_{на} \to (3/2\lambda) = T_{между} = T_{до}$. А при $t \to 0$, $T_{на} \to \infty$.

Литература

1. Надежность технических систем: Справочник / Ю.К. Беляев, В.А. Богатырев, В.В. Болотин и др.; под ред. И.А. Ушакова. М.: Радио и связь, 1985. – 606 с.
2. Волик Б.Г. Проблемы анализа техногенной безопасности. Автоматика и телемеханика, 2002, № 12, с.174–180.
3. Волик Б.Г. Экономическая эффективность управляющих систем. Проблемы управления, 2007, №2, с. 60-63.
4. Волик Б.Г. Работоспособность управляющих систем. Датчики и системы, - 2010. №5 с. 75-78.
5. Волик Б.Г. Анализ и выбор средств обеспечения техногенной безопасности технических объектов. Датчики и системы, 2012, № 6, с.57-63.
6. Барлоу Р., Прошан Ф. Математическая теория надежности. М.: Радио и Связь, 1969. - 488с.
7. Половко А.М., Гуров С.М. Основы теории надежности. BHV- Санкт-Петербург, 2006. – 560 с.
8. Шубинский И.Б. Основы анализа сложных систем. – Пушкин: ПВУРЭ, 1988.–206 с.
9. Черкесов Г.Н. Основы теории надежности автоматизированных систем управления. – Л.: ЛПИ, 1975. – 219 с.
10. Ушаков И.А. Вероятностные модели надежности информационно-вычислительных систем. М.: Радио и Связь, 1991. – 132 с.
11. Дружинин Г.В. Надежность автоматизированных производственных систем. М.: Энергоатомиздат, 1986. – 480 с.
12. Волик Б.Г., Буянов Б.Б., Лубков Н.В. и др. Методы анализа и синтеза структур управляющих систем. – М.: Энергоатомиздат, 1988. – 296 с.
13. Розенберг Е.Н., Шубинский И.Б. Графовый полумарковский метод моментов расчета функциональной безопасности систем железнодорожной автоматики и связи/ Труды Российского научно-исследовательского института управления на железнодорожном транспорте. – М.: ВНИИУП МПС Россия, 2002. с.79-86.
14. Кокс Д.Р., Смит В.Л. Теория восстановления. – М.: Советское Радио, 1967. – 300 с.
15. Гнеденко Б.В., Беляев Ю.К., Соловьев А.Д. Математические методы в теории надежности. – М.: Наука, 1965. – 524 с.

16. Коваленко И.Н., Кузнецов Н.Ю. Методы расчета высоконадежных систем. - М.: Радио и связь, 1988. - 176 с.

17. Kalashnikov V.V. Topics on Regenerative Processes. Boca Raton: CRC Press, 1994. – p.240.

18. Калашников В.В. Организация моделирования сложных систем.- М.:Знание, 1982.- 64 с.

19. Бусленко Н.П., Калашников В.В., Коваленко И.Н. Лекции по теории сложных систем. – М.: Советское радио, 1973. – 440 с.

20. Заренин Ю.Г., Збырко М.Д., Креденцер Б.П. и др. Надежность и эффективность АСУ. – К.: Техніка, 1975. – 368 с.

21. Бусленко Н. П. Моделирование сложных систем. М. Наука, 1978. – 399 с.

22. Диллон Б., Сингх Ч. Инженерные методы обеспечения надежности систем. М: Мир, 1984. -318 с.

23. Рябинин И.А. Основы теории и расчета судовых электроэнергетических систем. Л.: Судостроение, 1971. – 456 с.

24. Рябинин И.А. Надежность и безопасность сложных систем. // СПб.: Политехника, 2000. – 248 с.

25. Vesely W.E., Goldberg F.F., Roberts N.H., Haas D.F. NUREG-0492. Fault Tree Handbook/ U.S. Nuclear Regulatory Commission, D.C. 20555, January, 1981, p.209. (http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0492/)

26. Хенли Э.Дж., Кумамото Х. Надежность технических систем и оценка риска. – М.: Машиностроение, 1984. – 528 с.

27. Kumamoto H., Henley E. J. Probabilistic Risk Assessment and Management for Engineers and Scientists, Second Edition, N.Y.: IEEE Press, 1996, p.522.

28. Можаев А.С. Общий логико-вероятностный метод анализа надежности сложных систем. Уч. пособие. Л.: ВМА, 1988. – 68 с.

29. Можаев А.С., Громов В.Н. Теоретические основы общего логико-вероятностного метода автоматизированного моделирования систем. СПб. ВИТУ, 2000. – 144 с.

30. Отчет о НИР. Сравнительный анализ технологий деревьев отказов и автоматизированного структурно-логического моделирования, используемых для выполнения работ по вероятностному анализу безопасности АЭС и АСУТП на стадии проектирования. («Технология-2004»). ФГУП "СПбАЭП", СПИК СЗМА, ИПУ РАН. СПб: 2005 г. – 282 с. (www.szma.com/obzor4.shtml).

31. MIL-HDBK-217F(2) Reliability Prediction of Electronic Equipment, Department of Defense. Washington, 1993. http://assist.daps.dla.mil/quicksearch/basic_profile.cfm?ident_number=53939

32. Handbook of Reliability Prediction Procedures for Mechanical Equipment. CARDEROCKDIV, NSWC-94/L07, 1994.

33. TR-332. Reliability Prediction Procedures for Electronic Equipment. Bellcore, Issue 6, 1997.

34. RDF 2000: Reliability Data Handbook. A universal model for reliability prediction of Electronocs components, PCBs and equipment. UTE C 80-810, July 2000.

35. RiAC-HDBK-217Plus. Handbook of 217Plus Reliability Prediction Models/RiAC, 2006.

36. Offshore Relability Data Handbook 4th Edition (OREDA 2002)/SINTEF, DNV (Norway), p.837. (http://www.dnv.com, http://www.sintef.no)

37. Electronic Parts Reliability Data (EPRD-97), Nonelectronic Parts Reliability Data (NPRD-95). - Reliability Analysis Center (RAC). http://www.lricks.com/rac.htm

38. Шавыкин Н. А., Петрухин Б.П., Жидомирова Е.М. Методика оценки безотказности технических средств. М.: Институт проблем управления, 1997. – 79 с.

39. Надежность ЭРИ: Справочник. // С.Ф. Прытков, В.М. Горбачева, А.А. Борисов и др. М.: 22 ЦНИИИ МО РФ, 2006. - 674 с.

40. Стрельников В.П., Федухин А.В. Оценка и прогнозирование надежности электронных элементов и систем. – К.: Логос, 2002, с.486.

41. MIL-HDBK-472 (NOTICE 1), Military Standardization Handbook: Maintainability Prediction, 1984.

42. ГОСТ 27.310-95 Анализ видов, последствий и критичности отказов.

43. MIL-STD-1629A. Procedures for Performing a Failure Mode, Effects and Criticality Analysis, 1980.

44. Гнеденко Б.В., Беляев Ю.К., Соловьев А.Д. Математические методы в теории надежности: Основные характеристики надежности и их статистический анализ. Изд.2. М.: URSS, 2013. - 584 с.

45. Заренин Ю.Г. Контрольные испытания на надежность. М.: Изд-во стандартов, 1970. – с.123.

46. Заренин, Ю. Г., Стоянова И.И. Определительные испытания на надежность. М. : Изд-во стандартов, 1978. - 168 с.

47. Острейковский В.А. Теория Надежности. М.: “Высшая Школа”, 2003. - с.463.

48. MIL-STD-2155 (AS) Failure Reporting, Analysis and Corrective Action System (FRACAS). – Department of Defense. Washington, 1985, D.C. 20301. http://www.weibull.com/mil_std/mil_std_2155.pdf

49. Викторова В.С. , Кунтшер Х.П., Петрухин Б.П., Степанянц А.С. Relex – программа анализа надежности, безопасности, рисков. - Надежность, 2003, №4 (7), сс.42-64.

50. Викторова В.С. , Степанянц А.С. Использование модулей Relex при анализе надежности и безопасности систем. - Надежность, 2004, №2 (9), с. 64-71.

51. Викторова В.С. , Степанянц А.С. Анализ программного обеспечения моделирования надежности и безопасности систем. - Надежность, 2006, №4 (19), с. 46-57.

52. Викторова В.С. , Кунтшер Х.П., Степанянц А.С. Обзор программных разработок по анализу надежности и безопасности систем. Труды международной конференции “Программные продукты информационного обеспечения безопасности полетов, надежности и технической эксплуатации авиационной техники”, Москва, 14-16 марта 2006, с. 17-26.

53. Шубинский И.Б., Шулика В. Ф. Программный комплекс «Универсал» для расчетов надежности и функциональной безопасности технических устройств и систем (общее описание). – Надежность, 2003, №4,- с.65-71.

54. Можаев А.С., Киселев А.В., Струков А.В., Скворцов М.С. Отчет о верификации программного средства “Программный комплекс автоматизированного структурно-логического моделирования и расчета надежности и безопасности систем” (ПК АСМ СЗМА, базовая версия 1.0 “АРБИТР”). Заключительная редакция СПб.: ОАО “СПИК СЗМА”, 2007, с.498.

55. Можаев А.С., Нозик А.А. Программный комплекс "АРБИТР" для моделирования, расчета надежности и безопасности систем. Информационный сборник ОАО Ассоциация "Монтажавтоматика": "Монтаж и наладка средств автоматизации и связи", вып. № 2. М.: ЛИКА, 2007, с. 32-40.

56. Можаев А.С., Нозик А.А., Потапычев С.Н.,Скворцов М.С. Программный комплекс автоматизированного моделирования и расчета надежности и безопасности АСУТП на стадии

проектирования. Материалы III Международной научно-практической конференции: Моделирование. Теория, методы и средства. Часть 1. Новочеркасск: НПИ, 2003, с. 28-35.

57. Филин, Б. П. Методы анализа структурной надежности сетей связи. М.: Радио и связь, 1988. - 203 с.

58. Пугачев В.С. Введение в теорию вероятностей. Издательство “Наука”. Главная редакция физико-математической литературы, 1968, с.368.

59. Рябинин И.А., Черкесов Г.Н. Логико-вероятностные методы исследования надежности структурно-сложных систем. М.: Радио и связь, 1981, - с.264.

60. Рябинин И.А., Парфенов Ю.М. Надежность, живучесть, безопасность корабельных электроэнергетических систем. СПб.: Военно-морская академия им. Адмирала Флота Советского Союза Н.Г. Кузнецова, 1997, - с.430.

61. Филин Б.П. О принципе дуальности в задачах анализа структурной надежности сложных систем // А и Т, 1989, №6, с.158-172.

62. Можаев А.С., Алексеев А.О. Автоматизированное структурно-логическое моделирование и вероятностный анализ сложных систем. В сб. «Теория и информационная технология моделирования безопасности сложных систем», вып. 2, под ред. И.А. Рябинина, СПб, 1994, с.17-42.

63. Акулова Л.Г. О стохастической сложности вычисления надежности булевских систем. Ярославль, ЯГУ, 1983.

64. Черняк А.А. Комбинаторно-графовый метод анализа надежности сложных систем с монотонными булевыми функциями //А и Т, 1991, №4, с.165-174.

65. Черняк А.А., Черняк Ж.А. Логико-вероятностный метод анализа надежности многозначных систем большой размерности //А и Т, 1998, №1, с.171-180.

66. Степанянц А.С. Вычисление параметра потока отказов в логико-вероятностных моделях методом рекурсивного наращивания переменных.- Автоматика и Телемеханика, № 9, 2007, с. 161-175

67. Рябинин И.А., Парфенов Ю.М. Определение “веса” и “значимости” отдельных элементов при оценке надежности сложной системы // Изв. АН СССР. Энергетика и транспорт. 1978. №6, с. 22 – 32.

68. Филин Б.П. Об аналитическом методе приближенного вычисления надежности сложных систем //А и Т, 1982, №11, с.159-170.

69. Викторова В.С., Свердлик Ю.М., Степанянц А.С. Анализ надежности систем сложной структуры на многоуровневых моделях. – Автоматика и Телемеханика, 2010, №7, с.143-148.

70. Викторова В.С., Свердлик Ю.М., Степанянц А.С. Анализ надежности газоснабжения потребителей природного газа на объектах ОАО «ГИПРОГАЗЦЕНТР». Сб. трудов VI Международной конференции MMR 2009 – Математические методы в теории надежности. М., 2009, с. 538 – 542.

71. Рябинин И.А. Задача № 35 и история ее исследований // Морской Вестник, №4(8), 2003, с. 48-51.

72. Rauzy A. Toward an efficient implementation of the MOCUS algorithm. - IEEE Transactions on Reliability, Volume 52, Issue 2, June 2003 Page(s): 175 – 180.

73. Pandle P.K. et al. Computerized Fault Tree Analysis: TREEL and MICSUP. – Operational Research Center. University of California. Berkeley. ORC 75-3. April 1975.

74. Drechsler R., Becker B. Binary Decision Diagrams – Theory and Implementations / Springer, 2010, pp.210.

75. Rauzy A. New Algorithms for Fault Tree Analysis. - Reliability Engineering and System Safety. Vol. 40, 1993, pp. 203-211.

76. Sinnamon R., Andreas J. Fault Tree Analysis and Binary Decision Diagrams. - Proceedings of the Reliability and Maintainability Symposium, January 1996, pp. 215-222.

77. Zhou Jinglun, Sun Quan. Reliability analysis based on binary decision diagrams. Journal of Quality in Maintenance Engineering. 1998, vol.4, issue 2, pp. 150-161.

78. Fault Tree Handbook with Aerospace Applications. NASA, 2002, p. 205.

79. Woo Sik Jung, Sang Hoon Han and Jaejoo Ha. A fast BDD algorithm for large coherent fault trees analysis. - Reliability Engineering & System Safety, 2004, Vol. 83, Issue 3, pp. 369-374.

80. Remenyte R.; Andrews, J.D. A simple component connection approach for fault tree conversion to binary decision diagram. - Availability, Reliability and Security, 2006. ARES 2006. /The First International Conference, 20-22 April 2006 , 8 pp.

81. Wierman T.E., Rasmuson D.M., Stockton N.B. Common-Cause Failure Event Insights. Circuit Breakers. – NUREG/CR-6819, Vol. 4, INEEL/EXT-99-00613, May 2003, 150 pp.

82. Mosleh A., Fleming K., Parry G., Paula H., Worledge D., Rasmuson D. Procedures for treating common cause failure. Safety and Reliability Studies. - NUREG/CR4780 EPRI NP-5613, vol. 1, Jan. 1988, 148 pp.

83. Reliability: A Practitioner’s Guide. – London: Intellect, The Information Technology Telecommunications and Electronics Associations, 2003, pp.294.

84. Рыбников К.А. Введение в комбинаторный анализ. – М.: Наука, 1985, с.308.

85. Рябинин И.А. Надежность и безопасность структурно-сложных систем. – СПб.: Изд. С.-Петерб. ун-та, 2007, с. 276.

86. Meng F.C. Relationships of Fussell-Vesely and Birnbaum importance to structural importance in coherent systems. – Reliability Engineering and System Safety, Vol.67, Num.1, January 2000, pp. 55-60.

87. Meng F.C. Comparing Birnbaum importance measure of system components. – Probability in Engineering and Informational Sciences, 2004, 18, pp. 237-245.

88. Wendai Wang; Loman J.; Vassiliou P. Reliability importance of components in a complex system. - Reliability and Maintainability, 2004 Annual Symposium – RAMS, pp. 6 – 11.

89. Borgonovo E. Differential, criticality and Birnbaum importance measures: An application to basic event, groups and SSCs in event trees and binary decision diagrams. -Reliability Engineering & System Safety.Vol. 92, Issue 10, October 2007, pp. 1458-1467

90. Нечипоренко В. И. Структурный анализ и методы построения надежных систем. М.: «Советское радио», 1968, с.256.

91. Методические указания по проведению анализа риска опасных производственных объектов (РД 03-418-01). Серия 03. Выпуск 10/ Колл. авт. – М.: - Государственное унитарное предприятие “Научно-технический центр по безопасности в промышлденности Госгортехнадзора России”, 2001, с.60.

92. Викторова В.С., Ведерников Б.И., Спиридонов И.Б., Степанянц А.С. Моделирование и анализ контролепригодности бортовых систем самолетов.- Надежность. №3 (22), 2007, с.62-71.

93. .Spiridonov I., Stepanyants A., Victorova V. Design testability analysis of avionic systems. Reliability: Theory and Applications (RT&A) # 03 (26) (Vol.7) 2012, September, pp. 66-73.

94. Вентцель Е.С. Теория вероятностей. М.: Наука, 1969, с.576.

95. Вентцель Е.С., Овчаров Л.А. Теория вероятностей и ее инженерные приложения. Изд. Академия, 2003, с.464.

96. Ng Y.W., Avizienis A.A. A unified reliability model for fault tolerant computers. IEEE Transactions on Computers, vol. C-29, no.11, Nov. 1980, pp.1002-1011.

97. Хайрер Э., Ваннер Г. Решение обыкновенных дифференциальных уравнений. Жесткие и дифференциально-алгебраические задачи. М: Мир, 1999, с.685.

98. Форсайт Дж., Малькольм М., Моулер К. Машинные методы математических вычислений. – М.: МИР, 1980, с. 279.

99. Буянов Б.Б., Злобинский В.И., Лубков Н.В., Степанянц А.С. АСУ ТП. Оценка надежности и эффективности на основе моделей марковских процессов с доходами (МПД-метод). РМ 25431-87, М.: Минприбор, 1987, с.36.

100. Ng Y.W., Avizienis A.A. A unified reliability model for fault tolerant computers. IEEE Transactions on Computers, vol. C-29, no.11, Nov. 1980, pp.1002-1011.

101. Castes A., Doucet J.E., Landrault C., Laprie J.S. SURF: A program for dependability evaluation of complex fault-tolerant computing systems. – Proc.1981, Int.Symp. Fault Tolerant Computing Systems, FTCS-11, 1981, pp. 72-78.

102. Makam S.V., Avizienis A.A. ARIES 81: A reliability and life-cycle evaluation tool for fault-tolerant systems. – Proc. IEEE 12-th Fault Tolerant Computing Smposium, 1982 Jun, pp.267-274.

103. Muazzani M., Trivedi K. Dependability prediction: comparison of tools and techniques. – SAFECOMP ’86: Trends in safe real time computer systems: proceedings of the Fifth IFAC Workshop, Sarlet, France, 14-17 October 1986, pp. 171-178.

104. Bavuso S.J., Dugan J.B., Trivedi K.S., Rothmann E.M., Smith W.E. Analysis of typical fault-tolerant architectures using HARP. – IEEE Transactions on Reliability, vol. R-36, no.2, 1987, Jun, pp.176-185.

105. Geist R.; Trivedi K.S. Reliability estimation of fault-tolerant systems: tools and techniques.- Computer, vol. 23, Issue 7, Jul 1990, pp. 52 – 61.

106. Balakrishnan M., Raghavendra C.S. An Analysis of a Reliability Model for Repairable Fault-Tolerant Systems. - IEEE Transactions on Computers, vol.42, no.3, Mar.,1993, pp. 327-339.

107. Shooman M.L. Reliability of Computer Systems and Networks \John Wiley & Sons Inc., 2002, p.521.

108. Викороваа В.С. Агрегирование моделей анализа надежности и безопасности технических систем сложной структуры: Дис. докт. техн. наук. Москва. 2009. - 223 с.

109. Викторова В.С., Волик Б.Г., Степанянц А.С. Анализ надежности вычислительного управляющего комплекса методом комбинации расчетных моделей. – Надежность. №2 (17), 2006, с. 53-59.

110. Викторова В.С. Выбор параметров процедуры обработки неисправностей в вычислительной системе с программно-управляемой сбое- и отказоустойчивостью. – Приборы и системы управления, 1993, №7, с.18-21.

111. Викторова В.С., Степанянц А.С. Динамические деревья отказов. – Надежность, 2011, №3, с. 20-32.

112. Boudali H., Dugan J.B. A continuous-time Bayesian network reliability modeling, and analysis framework. - IEEE Transactions on Reliability, vol. 55, No. 1, March 2006, pp. 86-97.

113. Кондратенков В.А., Котельников Г.Н., Мамченков В.Л., Отрохов В.П. Вопросы теории надежности технических систем. – Смоленск: Русич, 1998 – 224 с.

114. Merle G., Roussel .-M., Lesage J.-J., Vayatis N. Analytical Calculation of Failure Probabilities in Dynamic Fault Trees including Spare Gates. – Proceedings of ESREL 2010 - European Safety a& Reliability Conference. September 2010.

115. ГОСТ 27.310-95 Анализ видов, последствий и критичности отказов. – 13с.

116. ГОСТ Р 51814.2-2001 “Системы качества в автомобилестроении. Метод анализа видов и последствий потенциальных дефектов”. – 18 с.

117. ГОСТ Р 51901-2002. Управление надежностью. Анализ риска технологических систем. - 21 с.