Министерство образования и науки РФ

Федеральное государственное бюджетное образовательное
учреждение высшего профессионального образования
«Тульский государственный университет»

Кафедра «Аэрология, охрана труда и окружающей среды»

Шейнкман Л.Э.,
докт. техн. наук, профессор

КОНСПЕКТ ЛЕКЦИЙ

по дисциплине

«НАДЁЖНОСТЬ ТЕХНИЧЕСКИХ СИСТЕМ И ТЕХНОГЕННЫЙ РИСК»

Направление подготовки: 280700 – Техносферная безопасность

Профиль подготовки: 280700.62 – Безопасность технологических процессов и производств

Квалификация (степень) выпускника: бакалавр

Тула 2011 г.

Рассмотрено на заседании кафедры
протокол № 1 от 31 августа 2011 г.
Зав. кафедрой_____Э.М. Соколов

Содержание

1 НАДЁЖНОСТЬ КАК КОМПЛЕКСНОЕ СВОЙСТВО ТЕХНИЧЕСКОГО ОБЪЕКТА (прибора, устройства, машины, системы)

1.1 Ретроспективный анализ развития теории надёжности технических систем

По очевидным причинам начальный импульс к созданию численных методов оценки надежности был дан авиационной промышленностью. После первой мировой войны в связи с увеличением интенсивности полетов и авиационных катастроф были выработаны критерии надежности для самолетов и требования к уровню безопасности. В частности, проведен сравнительный анализ одномоторных и многомоторных самолетов с точки зрения успешного завершения полета и выработаны требования по частоте аварий, отнесенных к 1 ч. полетного времени. К 1960 г., например, было установлено, что одна катастрофа приходится в среднем на 1 млн. посадок. Таким образом, для автоматических систем посадки самолетов можно было бы установить требования по уровню риска, не превышающего одной катастрофы на 10^7 посадок.

Р.Х. Дженнингс приводит хронологию развития теории и техники надежности в 40-70-х годах.

В США в **40-х годах** основные усилия для повышения надежности были сконцентрированы на всестороннем улучшении качества. Улучшенные конструкции, прочные материалы, повышение твердости и качества обработки изнашиваемых поверхностей, совершенные измерительные инструменты и т.д. – все было направлено на то, чтобы увеличить активную долговечность узлов и агрегатов. Электротехническое отделение фирмы «Дженерал моторс» (General Motors), например, увеличило активный ресурс приводных двигателей локомотивов с 400 тыс. до 1,6 млн. км за счет использования улучшенной изоляции и применения усовершенствованных конических и сферических роликовых подшипников, а также проведения испытаний при высокой температуре. Долговечность дизелей была намного увеличена благодаря разработке фирмой «Токко» технологии повышения твердости опорных поверхностей цанг и кулачков. Был достигнут прогресс в разработке ремонтопригодных конструкций в обеспечении предприятий оборудованием, инструментом и документаци-

ей для выполнения операций по техническому обслуживанию и профилактических работ. Другая форма прогресса была продемонстрирована в 40-е годы благодаря повышенному интересу руководителей промышленных предприятий к составлению и утверждению типовых графиков периодических проверок, карт контроля высокопроизводительного станочного оборудования, выработке уровней оценки и экономически обоснованного подхода к качеству продукции. Данные мероприятия ознаменовали вступление инженеров, работающих в промышленности в эту область, и, как результат, большинство инструкций и учебных курсов по надежности было посвящено обеспечению и контролю качества и относящимся к ним статистическим методам.

50-е годы. Большое значение придавалось безопасности, особенно в аэрокосмической и атомной областях. Эта декада отмечена началом использования основных понятий по надежности элементов, таких как интенсивность отказов, ожидаемая долговечность, соответствие конструкции заданным требованиям и прогнозирование качества.

Министерство обороны США обнаружило, что ненадежное оборудование требовало огромного объема работ по техническому обслуживанию и ремонту. Подсчитали, что годовая стоимость обслуживания вооружения составляет 2 долл. на каждый доллар стоимости самого оборудования электронного типа. Таким образом, при десятилетнем сроке эксплуатации необходимо 20 млн. долл. для содержания оборудования закупочной стоимостью в 1 млн. долл. Эти факты продемонстрировали правительству, что гораздо благоразумнее закладывать основы надежности конструкции при проектировании, чем ожидать, пока оборудование откажет, и после этого производить его ремонт.

Именно в начале 50-х годов были затрачены значительные усилия на то, чтобы понять и научиться исправлять ошибки человека, приводящие к отказам систем. Одна из первых количественных оценок возможностей человека была выполнена в 1952 г. в лаборатории «Сандиа». Было проведено исследование системы ядерного оружия на самолетах с использованием метода, базирующегося на экспериментальных оценках среднего количества ошибок оператора на выполняемую операцию. Задачи оператора были подразделены на две категории в зависимости от условий, в которых они выполнялись: частота возникновения ошибок принималась равной 0,01 для операций, выполняемых на земле, и

0,02 – в воздухе. Эти значения были введены в уравнения, описывающие надежность работы системы, наряду с другими событиями, относящимися к системе.

60-е годы. В 60-е годы стала очевидной острая необходимость в новых методах обеспечения надежности и более широкого их применения в различных приложениях. Центр внимания переместился от анализа поведения отдельных элементов различного типа (механических, электрических или гидравлических) на последствия, вызываемые отказом этих элементов в соответствующей системе. Вступление в эру межконтинентальных баллистических ракет и последующая разработка пилотируемых ракетно-космических кораблей, таких как «Меркурий» и «Джемини», ускорили реализацию девиза «успех любой ценой». Эти обстоятельства усугублялись требованием поражения цели «с одного выстрела», кульминация которого достигается при предстартовом отсчете перед запуском реактивных двигателей и других систем ракеты на пусковом столе.

Значительные усилия были затрачены на испытание систем и отдельных элементов в течение первых лет космической эры. Все данные по каждому отказу и результаты анализа тщательно регистрировались наряду с информацией по другим техническим недостаткам, вскрытым при анализе. Вид, механизм и причина каждого отказа любого элемента и вызываемые ими воздействия на систему оценивались с целью внесения изменений, исключающих их повторение. Анализ систем с использованием блок-схем в качестве основных моделей получил бурное развитие и широкое распространение для достижения высокой степени надежности и безопасности.

С увеличением сложности более изощренно составленных блок-схем появилась необходимость в другом подходе. В 1961 г. впервые Х.А.Уотсоном из лаборатории фирмы «Белл телефоун» (Bell Telephone) был предложен новый принцип анализа с помощью дерева отказов в качестве программы для оценки надежности системы управления запуском ракет «Минитмэн». Позднее фирма «Боинг» (Boeing) модифицировала этот принцип моделирования на ЭВМ. В 1965 г. Д.Ф. Хаасль развил методику построения дерева отказов применительно к широкому кругу различных технических проблем, относящихся к надежности и безопасности.

Изучение безопасности систем как отдельной независимой

деятельности было официально введено в практику в 1962 г. после катастрофических аварий на четырех подземных комплексах запуска межконтинентальных баллистических ракет (МБР). В 1966 г. министерство обороны США приняло стандарты ВВС и ввело требование по проведению анализа надежности на всех этапах разработки всех видов вооружения. Эти стандарты непрерывно дополнялись и перерабатывались, а в 1969 г. МО приняло стандарт MIL-STD-882 «Программа по обеспечению надежности систем, подсистем и оборудования: Требования» в качестве основного стандарта для всех промышленных подрядчиков по военным поставкам.

Параллельно МО разработало требования по надежности, работоспособности и ремонтопригодности промышленных изделий. Такие стандарты, как, например, MIL-STD-471, «Ремонтопригодность (проверка, подтверждение, оценка)» и MIL-STD-781 «Испытания на надежность (экспоненциальное распределение)» являются документами, которые, в частности, определяют высокую степень загруженности инженеров и консультантов по надежности среди военных и гражданских специалистов.

60-е годы также отмечены началом широкого издания книг и журналов в описываемой области. Монография И. Базовски «Надежность: теория и практика» была опубликована издательством «Прентис-холл» (Prentice-Hall) в 1961 г., а к концу десятилетия появились по меньшей мере еще 15 книг. В этот период увидел свет журанал IEEE «Transactions on Reliability», который под руководством д-ра Р. Эванса стал ведущим периодическим изданием в данной области. Видные математики, такие как З.У. Бирнбаум, Р. Барлоу, Ф. Прошаи, Д.Ж. Эзари и У. Вейбулл, проложили дорогу разработке статистических методов, относящихся к проблемам надежности и ремонтопригодности.

Кампания, начавшаяся в 50-х и ускорившаяся в 60-х годах, привела к накоплению и систематизации данных по параметрам элементов, системам и ошибкам человека-оператора.

Теория надежности в нашей стране начала интенсивно разрабатываться, начиная с 50-х годов. Первые отечественные книги Г.В. Дружинина, А.М. Половко, Н.А. Шишонка появились в начале 60-х годов. В 1965 году вышла в свет книга Б.В. Гнеденко, Ю.К.Беляева, А.Д.Соловьева «Математические основы теории надежности», сыгравшая особую роль в развитии математических основ надежности как в нашей стране, так и за рубежом.

Поскольку процессы изменения параметров систем, моменты их отказов, изменение условий эксплуатации и продолжительность работ по устранению отказов являются случайными, то основным математическим аппаратом теории надежности являются теория вероятности, математическая статистика, теория массового обслуживания. Для чтения настоящей книги предполагается знание студентами основных положений этих теорий (в объеме [1]).

70-е годы. Интенсивная работа по оценке риска, связанного с эксплуатацией атомных электростанций, была организована Комиссией по атомной энергии США и завершилась в 1977 г. выпуском отчета «WASH-1400. Анализ безопасности реактора». Проф. Н. Расмуссен и руководимая им группа исследователей с многомиллионным бюджетом проанализировали широкий спектр аварий, относящихся к атомной энергетике, численно классифицировали их в порядке вероятности появления, а затем оценили потенциальные последствия в отношении населения. Дерево событий, дерево отказов и техника оценки риска и последствий, использованные в этом отчете, были затем взяты на вооружение в химической и других отраслях промышленности. Исследования «по Расмуссену» получили распространение в странах Европы, Азии и в США.

Возрастающая озабоченность общественности в отношении индустриальных опасностей в сочетании с возрастающей степенью потребления и влиянием на окружающую среду произвели значительное воздействие в течение этого десятилетия. В Западной Европе вслед за серьезными промышленными авариями в Фликсборо (Великобритания) и Севезо (Италия) был принят ряд законов, предписывающих проведение исследований основных источников риска перед началом строительства любого предприятия. Закон по токсическим материалам, принятый в Великобритании, может повлиять на любое предприятие, имеющее хотя бы одну емкость со сжатым газом. В США введены законы об охране здоровья на производстве и об ответственности за качество продукции.

Многие приметы нашей нынешней жизни стали вполне привычными. Вот одна из них. Уже более 15 лет в России работает Министерство по чрезвычайным ситуациям, аналогичные структуры существуют во всех развитых странах. А ведь это означает, что аварии, катастрофы, стихийные бедствия стали не-

отъемлемой частью жизни человечества. При этом растут масштабы подобных бед, ширится их спектр, становится сильнее влияние разного рода внезапных происшествий на стратегию государств. Статистические данные показывают, что число пострадавших в результате техногенных катастроф и стихийных бедствий и величина ущербов приближаются к соответствующим показателям крупных вооруженных конфликтов. Число пострадавших в результате известной аварии на химическом комбинате в индийском городе Бхопал приблизительно равно числу жертв американской ядерной бомбардировки Хиросимы. Вопрос о создании в провинциях Рима добровольных пожарных дружин обсуждался еще в письмах Юлия Цезаря, а большие пожары вошли в историю почти всех крупных городов. Однако прогресс сделала мегаполисы гораздо более уязвимыми по отношению не только к традиционным угрозам, но и к совершенно новым опасностям, которые трудно предугадать. Еще полгода назад мало кто мог предвидеть, что «веерные» отключения в Приморье окажутся настолько пагубными для инфраструктуры и социальной сферы края или что разливы сибирских рек приведут к таким огромным потерям.

Заметим, что техногенные катастрофы – это не только гигантский материальный ущерб и унесенные человеческие жизни, это возможное изменение стратегии огромных отраслей экономики, «алгоритмов развития» цивилизации. Достаточно вспомнить знаковые катастрофы XX в. – Чернобыль и «Челленджер». На наш взгляд, и атомная энергетика, и космонавтика до сих пор не вполне оправились от шока, вызванного этими трагическими событиями. Закономерно поэтому, что и в России, и в других развитых странах на рубеже XXI в. Одной из основных технологий нашей цивилизации, от которой во многом зависят перспективы мировой динамики, считают технологию управления рисками.

Термин «управление рисками» пришел из страхового дела, как сейчас модно говорить, из актуарной математики. Промышленники и страховщики уже давно поняли, что полностью избежать риска не удастся, ибо неполадки, аварии, катастрофы, к сожалению, неизбежные спутники нашей технологической цивилизации. И сточки зрения экономики задача заключается в том, чтобы минимизировать экономический ущерб. Этому служат различные системы страхования, «размазывающие» риск, непосильный для одного экономического агента, на многих.

Однако развитие атомной промышленности, опасных химических производств, транспортных систем заставляет взглянуть на проблему более широко. В настоящее время обозначился большой круг задач, связанный с выбором наиболее безопасного и в тоже время экономически достаточно выгодного вектора развития техносферы, выработкой системы мер по прогнозированию и предупреждению бедствий и катастроф, по ликвидации возникших чрезвычайных ситуаций, по смягчению последствий уже происшедших бед.

Достаточно очевидно, что без глубоких серьезных исследований нельзя было обойтись. Надо сказать, что со времен Чернобыльской аварии они активно велись. В частности, под руководством академика К.В. Фролова и члена-корреспондента РАН Н.А. Махутова была сформирована Государственная научно-техническая программа «Безопасность», работы в рамках которой продолжаются и по сей день. Здесь на высоком инженерном и научном уровне решаются вопросы обеспечения безопасности различных технических объектов. Такой, в лучшем смысле слова, инженерный, отраслевой подход на определенном этапе дал весомые результаты.

Однако сегодня его уже недостаточно. Системный кризис заставляет думать о стратегии, обо всем наборе опасностей и угроз, с которыми может столкнуться наше общество, о привлечении в эту сферу методов фундаментальных наук. Иногда разницу между прикладной наукой и инженерной деятельностью, с одной стороны, и фундаментальными исследованиями – с другой, объясняют таким образом. В первой сфере рассматривают задачи, которые заведомо имеют решения, и вопрос лишь в том, сколько оно стоит и какого времени потребует. Во второй сфере, связанной с фундаментальными исследованиями, поставленные задачи могут как иметь, так и не иметь решения. В области управления риском, где, к сожалению, все чаще приходится выбирать между плохим и очень плохим вариантом, без фундаментальных исследований сейчас ничего не решить.

Кто-то из историков науки заметил, что, как правило, задачи и средства их решения с течением времени оказываются неплохо согласованными. Однако в определенные периоды задачи «забегали вперед», и после этого довольно быстро создавались средства (теории, аппарат, установки и пр.), нужные для их решения. Бывало, напротив, осуществлялся прорыв в «инструмен-

тальном сопровождении» науки и начинался поиск задач нового поколения, которые можно решать, используя эту технику. В случае управления риском мы, скорее всего, ближе ко второй ситуации.

Если преобладающими становятся сильные положительные обратные связи, то может возникнуть взрыв, эпидемия – по такому «катастрофическому» закону росло народонаселение Земли за последние 100 тыс. лет. Математическая теория таких процессов разрабатывается у нас в ИПМ РАН. Особенно любопытно, что в некоторых системах с такими свойствами существуют «предвестники» - легко вычисляемые параметры, показывающие, что рассматриваемый объект находится в опасном состоянии. Как важно было бы, имея это в виду, сделать шаг от теории к практике для многих конкретных систем.

Другой механизм связан с увеличением времени запаздывания реакции объекта на возмущающие воздействия. Он достаточно универсален и характерен для самых разных объектов – от тяжелых поражений иммунной системы организма до нашествий саранчи и предкатастрофических режимов работы ядерных реакторов.

Парадоксальным представляется поведение многих сложных систем, которые «сами идут к катастрофе», стремятся к критическому состоянию. Такие объекты подробно рассматриваются в теории самоорганизованной критичности, детально обсуждаемой в книге. Поразительно, как много явлений и процессов описывает данная теория, – это наводнения и биржевые крахи, землетрясения и инциденты с хранением ядерного оружия, ураганы и вспышки на Солнце, сели и утечка конфиденциальной информации. А. Пуанкаре писал, «…что единство нашего мира проявляется не в его материальности (что тривиально), а в единстве описывающих его математических (так и хочется добавить: компьютерных) моделей.». Развитие нелинейной динамики, междисциплинарных исследований подтверждает эту мысль классика.

Теория управления риском существенно отличается от обычных естественнонаучных теорий. Чтобы оказаться полезной, она должна быть понята и востребована не только исследователями, но и инженерами, управленцами, руководителями.

Концепция устойчивого развития в конкретных условиях России самым тесным образом связана с управлением риском природных и техногенных катастроф, социальных нестабильно-

стей. Повышение устойчивости общества относительно этих возмущений является необходимым условием для выхода из кризиса, для изменений к лучшему. Хочется надеяться, что это понимание найдет отражение не только в научных монографиях, но и в официальных документах разного уровня.

Среди множества рисков, которые затронуты в книге и с которыми мы сталкиваемся в реальности, наиболее существенны стратегические риски. Это те опасности, которые связаны с принятием решений (или отсутствием таковых), меняющих траекторию развития страны. В технике лет 30 назад была распространена концепция абсолютной надежности. В соответствии с ней строгое выполнение инструкций и соблюдение технологической дисциплины позволяют полностью избавиться от аварий. Затем на основе огромного накопленного опыта и научных разработок удалось перейти к концепции допустимого риска. Жизнь не дает нам возможности быть слишком большими оптимистами и в каждом случае надеяться на лучшее. Приходится, имея дело с любым опасным производством, оценивать вероятность катастрофы и возможный ущерб. По-видимому, назрела необходимость так же подходить и к широкому кругу принимаемых в стране решений, в частности, тех, от которых зависит национальная безопасность.

В 1997 году в нашей стране принят Федеральный закон «О промышленной безопасности опасных производственных объектов». Закон определяет правовые, экономические и социальные основы обеспечения безопасной эксплуатации опасных производственных объектов и направлен на предупреждение аварий на опасных производственных объектах и обеспечение готовности организаций к локализации и ликвидации последствий указанных аварий.

1.2. Система и элементы

Некоторые основные термины и определения в области надежности (например, отказ, восстановление, само понятие *надежность*) уже использовались ранее в предисловии. Однако для дальнейшего изучения теории надежности необходимо дать строгие определения этих терминов. При этом будем следовать нормативно-техническим документам в области надежности (в частности, ГОСТ 24.701-86 "Единая система стандартов автоматизи-

рованных систем управления. Основные положения").

Под *системой* понимают совокупность элементов, взаимодействующих между собой в процессе выполнения заданных функций. *Элементом* системы называют составную часть системы, которая рассматривается без дальнейшего разделения как единое целое; внутренняя структура элемента при данном рассмотрении не является предметом исследования.

Понятия "система" и "элементы" выражены одно через другое и условны: то, что является системой для одних задач, для других принимается элементом в зависимости от целей изучения, требуемой точности, уровня знаний о надежности и т.д. Даже такая сложная система как АСУ ТП, может рассматриваться как элемент более сложной системы – автоматизированного технологического комплекса, включающего, помимо АСУ ТП, технологический объект управления. Еще в большей степени это относится к составным частям АСУ ТП.

На рис.1.1 приведена схема АСУ ТП энергоблока АЭС, где каждый комплекс, субкомплекс, техническое средство или блок может рассматриваться и как система, состоящая из элементов, и как элемент системы более высокого уровня.

Приведенные далее термины пригодны как для разнообразных систем, так и для их элементов.

Работоспособным называется такое состояние системы (элемента), при котором значения параметров, характеризующих способность системы выполнять заданные функции, находятся в пределах, установленных нормативно-технической или конструкторской документацией. Соответственно *неработоспособным* называется состояние системы, при котором значение хотя бы одного параметра, характеризующего способность выполнять за данные функции, не находится в пределах, установленных указанной документацией. Например, система измерения температуры является неработоспособной, если основной параметр, характеризующий качество ее функционирования – погрешность измерения, превышает заданную величину.

Рис. 1.1. **Схема АСУ ТП энергоблока АЭС**

1.3 Состояния и события

Состояния системы могут быть также разделены на *исправное* (при котором система соответствует всем требованиям нормативно-технической и конструкторской документации) и *неис-*

правное (при котором имеется хотя бы одно несоответствие этим требованиям).

Отличие между исправным и работоспособным состояниями заключается в следующем. Работоспособная система удовлетворяет только тем требованиям, которые существенны для функционирования, и может не удовлетворять прочим требованиям (например, по сохранности внешнего вида элементов). Система, находящаяся в исправном состоянии, заведомо работоспособна.

Событие, заключающееся в нарушении работоспособности системы, т.е. в переходе ее из работоспособного в неработоспособное состояние, называется *отказом*. Событие, заключающееся в переходе системы из исправного в неисправное (но работоспособное) состояние, называется *повреждением*. Предметом дальнейшего изучения будут, как правило, отказы. Отличительный признак или совокупность признаков, по которым устанавливается факт возникновения отказа, называют *критериями отказа*. Выбор критериев отказов и классификация отказов различных систем и элементов рассмотрены в главе 6.

Восстановлением называется событие, заключающееся в переходе системы из неработоспособного в работоспособное состояние. Соответственно к *невосстанавливаемым* относят системы, восстановление которых непосредственно после отказа считается нецелесообразным или невозможным, а к *восстанавливаемым* – в которых проводится восстановление непосредственно после отказа.

Одна и та же система в различных условиях применения может быть отнесена к невосстанавливаемым (например, если она расположена в необслуживаемом помещении, куда запрещен доступ персонала во время работы технологического агрегата) и к восстанавливаемым, если персонал сразу же после отказа может начать восстановление. Само понятие "восстановление" следует понимать не только как корректировку, настройку, пайку или иные ремонтные операции по отношению к тем или иным техническим средствам, но и как замену этих средств.

В принципе подавляющее большинство систем, применяемых для автоматизации технологических процессов, подлежит восстановлению после отказа, после чего они вновь продолжают работу. То же относится к большей части технических средств; к числу невосстанавливаемых можно отнести только такие элементы, как интегральные схемы, резисторы, конденсаторы и т.п.

Схема основных состояний и событий, характерных для

восстанавливаемых систем, приведена на рис.1.2. На этой схеме выделено также предельное состояние, при котором дальнейшее применение системы по назначению недопустимо или нецелесообразно. Предельное состояние может иметь место, если дальнейшее восстановление неработоспособного состояния невозможно или нецелесообразно. После попадания в предельное состояние может следовать ремонт (капитальный или средний), в результате чего восстанавливается исправное состояние, или же система окончательно прекращает использоваться по назначению.

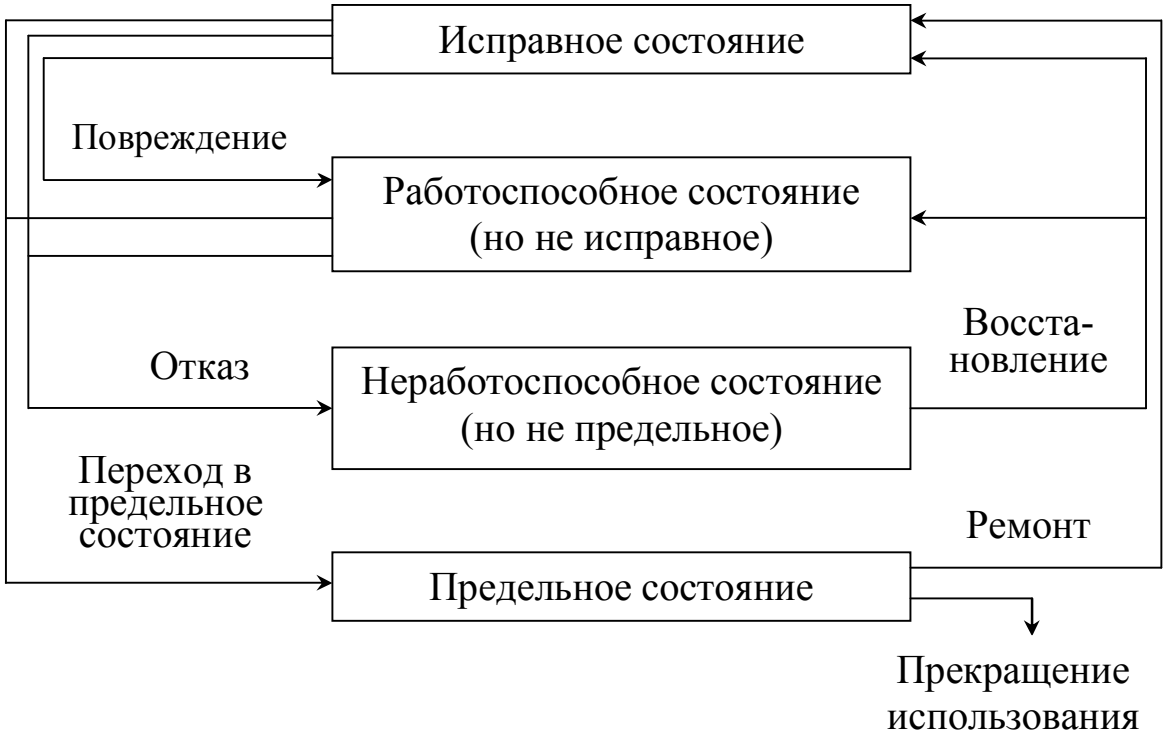


Рис.1.2. **Схема основных состояний и событий системы**

1.4. Понятие "наработка до отказа"

Рассмотрим систему, начинающую функционировать в момент времени t=0, причем в этот момент система находится в работоспособном состоянии. Предположим сначала, что такая система отключается только вследствие отказа. Обозначим через T время, прошедшее от момента начала функционирования до момента отказа. Величина T зависит от случайных отклонений технологических условий изготовления отдельных элементов от номинальных, различия условий транспортировки, монтажа, наладки и не будет одинаковой у различных систем даже при абсолютно одинаковых условиях эксплуатации. К тому же сами условия эксплуатации (температура, вибрация, качество технического об-

служивания, частота включения и т.д.) в определенной степени отличны друг от друга, поэтому величина T случайна.

Отключения системы могут происходить не только из-за ее отказов, но и для проведения технического обслуживания, вследствие отказов автоматизируемого технологического агрегата, из-за циклического графика работы системы, когда она включается на некоторые промежутки времени, определяемые технологическим режимом (например, в АСУ непрерывно-дискретными технологическими процессами).

Продолжительность работы системы в этой ситуации носит название *наработки*, а случайная величина – длительность работы до отказа называется *наработкой до отказа*, которую также будем обозначать T. Наработка до отказа в отличие от времени безотказной работы не всегда измеряется единицами времени; наработка до отказа может измеряться и числом включений (срабатываний, циклов). Однако для большей части систем наработка до отказа измеряется единицами времени. На рис.1.3. приведен график эксплуатации системы, где наработка до отказа

$$T = t_1 + (t_3 - t_2) + (t_4 - t_5),$$

где t_1 – момент отключения системы из-за останова технологического агрегата; t_2, t_4 – моменты включения системы в работу; t_3 – момент отключения системы на профилактику; t_5 – момент отказа системы.

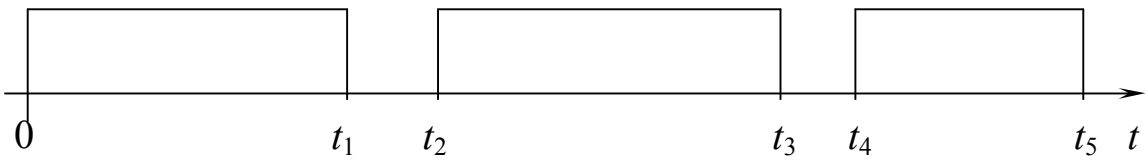


Рис.1.3. **К определению понятия "наработка до отказа"**

Очевидно, что для систем, работающих без отключений (кроме отказов), наработка до отказа совпадает с временем безотказной работы.

2 НАДЁЖНОСТЬ ТЕХНИЧЕСКИХ СИСТЕМ

2.1 Сущность надежности

Свойство системы сохранять во времени в установленных пределах значения всех параметров, характеризующих способность системы выполнять требуемые функции в заданных режимах и условиях эксплуатации называют *надежностью*.

Надежность является комплексным свойством, включающим в себя четыре составляющие: безотказность, ремонтопригодность, долговечность и сохраняемость.

Под *безотказностью* понимается свойство системы сохранять работоспособность (выполнять свои функции с эксплуатационными показателями не хуже заданных) в течение требуемого интервала времени непрерывно без вынужденных перерывов. Безотказность является наиболее важной компонентой надежности, так как она отражает способность системы длительное время функционировать без отказов. Безотказность систем в решающей степени влияет на эффективность их использования и определяется количеством и безотказностью элементов, режимом их работы, наличием резервирования, параметрами окружающей среды (температурой, запыленностью) и др.

Ремонтопригодность является свойством системы, заключающимся в ее приспособленности к предупреждению, обнаружению и устранению причин возникновения отказов, а также поддержанию и восстановлению работоспособного состояния путем проведения технического обслуживания и ремонтов. Ремонтопригодность зависит от того, выполнены ли элементы в виде отдельных, легко заменяемых блоков, а также от использования средств встроенного контроля работоспособности и диагностики. Следует отметить, что характеристики ремонтопригодности существенно зависят не только от свойств самой системы, но и от квалификации обслуживающего персонала и от организации эксплуатации.

Долговечность – свойство системы сохранять работоспособность до наступления предельного состояния с необходимыми перерывами для технического обслуживания и ремонтов. Долговечность системы зависит от долговечности технических средств и от подверженности системы моральному старению.

Сохраняемость характеризует свойство системы сохранять

значения показателей безотказности и ремонтопригодности в течение и после срока хранения и транспортировки. Поскольку системы в целом не хранятся, а могут сохраняться только отдельные технические средства и их элементы, то свойство сохраняемости для систем несущественно. Для технических средств и элементов это свойство имеет определенное значение, но менее важное, чем предыдущие свойства, так как эти средства обычно транспортируются только один раз – от завода-изготовителя к месту установки и длительность их хранения от момента поступления до монтажа и наладки (кроме технических средств и элементов, используемых в качестве запасных частей) относительно невелика. Вследствие этого вопросы сохраняемости ниже рассматриваться не будут.

2.2 Аналитические и статистические методы определения основных показателей надёжности технических систем

2.2.1 Функция и плотность распределения «наработки до отказа»

Показателями надежности называются количественные характеристики одного или нескольких свойств, составляющие надежность системы. При выборе показателей надежности следует иметь в виду, что эти показатели должны достаточно полно описывать надежностные свойства системы, быть удобными для аналитического расчета и экспериментальной проверки по результатам испытаний, должны иметь разумный физический смысл и, наконец, допускать возможность перехода к показателям эффективности.

Для невосстанавливаемых систем ограничимся здесь показателями безотказности. Отметим, что эти же показатели описывают системы, в принципе подлежащие восстановлению после отказов, но поведение которых целесообразно рассматривать до момента первого отказа. К их числу, например, можно отнести системы, чьи отказы чрезвычайно редки и вызывают особо тяжелые последствия.

Наработка до отказа T, как и любая иная случайная величина, описывается функцией распределения $F(t)$, определяемой как вероятность **P** случайного события, заключающегося в том, что наработка до отказа T меньше некоторой заданной наработки t:

$$F(t) = \mathbf{P}\ \{T < t\}. \qquad (2.1)$$

Эта вероятность рассматривается как функция t во всем диапазоне возможных значений величины T.

Функция распределения любой случайной величины является неубывающей функцией времени t. Примерный вид функции $F(t)$ дан на рис. 2.1. Так как значения T не могут быть отрицательны, то $F(0)=0$. При $t \to \infty$ величина $F(t)$ стремится к единице.

Кроме указанного выше вероятностного определения функции $F(t)$, для нее (как и для указанных ниже показателей надежности) можно привести и статистические определения, используемые при испытаниях на надежность. Статистические определения позволяют более полно объяснить смысл вероятностных определений. Чтобы их различать обозначения статистических определений далее будем отмечать волнистой чертой сверху.

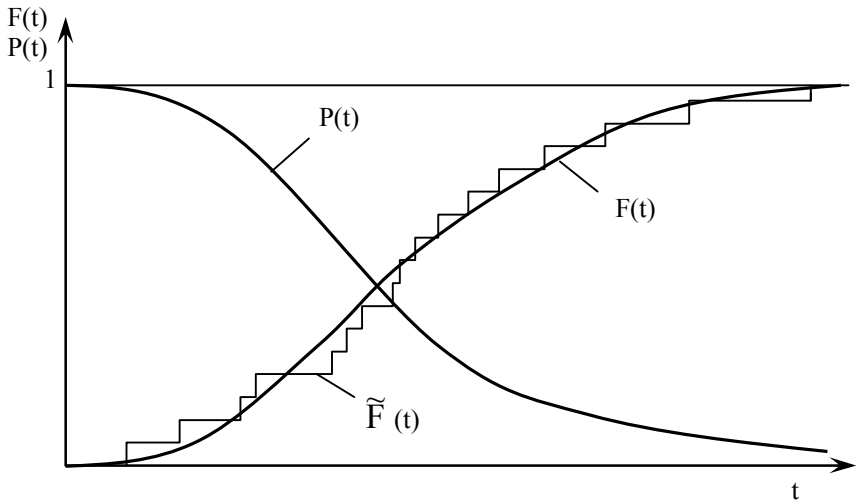


Рис.2.1 Примерный вид функции распределения $F(t)$ и функции надежности $P(t)$

Для рассмотрения статистических определений показателей надежности невосстанавливаемых систем предположим, что на испытания поставлено N одинаковых систем, условия испытаний одинаковы, а испытания каждой из систем проводятся до ее отказа. Обозначим $N(t)$ число систем, отказавших к моменту t, т. е. на интервале $(0, t)$. Очевидно, что $N(0)=0$, а при $t \to \infty$ величина $N(t) \to N$.

Статистическим определением функции распределения $F(t)$ (или, как говорят, эмпирической функцией распределения) является функция

$$\widetilde{F}(t) = N(t)/N \ , \qquad (2.2)$$

причем $\widetilde{F}(0) = 0$, а при величина $t \to \infty$ величина $\widetilde{F}(t) \to 1$.

График эмпирической функции распределения $\widetilde{F}(t)$ представляет собой ступенчатую линию со скачками, кратными $1/N$ в моменты отказов (рис. 3.1). В пределе с ростом числа N испытываемых систем функция распределения $\widetilde{F}(t)$ сходится по вероятности к распределению $F(t)$. Эту сходимость запишем следующим образом:

$$\mathrm{P}\left\{ \lim_{N\to\infty} \sup_{0<t<\infty} \left| \widetilde{F}(t) - F(t) \right| = 0 \right\} = 1 \ .$$

Укажем, что такая же сходимость имеет место для статистических определений показателей надежности как невосстанавливаемых (рассматриваемых ниже в настоящей главе), так и восстанавливаемых систем.

Так как события, заключающиеся в наступлении или ненаступлении отказа к моменту t, являются противоположными, то в соответствии с (2.1) введем еще одну функцию

$$P(t) = \mathrm{P}\{T \ge t\} = 1 - F(t) \ , \qquad (2.3)$$

которую часто называют функцией надежности. Так как при t=0 система работоспособна, то $P(0)$=1. С увеличением времени t $P(t)$ монотонно убывает, а при $t \to \infty$ величина $P(t) \to 0$. Примерный вид функции $P(t)$ дан на рис. 2.1.

Статистическое определение функции надежности следует из (2.2):

$$\widetilde{P}(t) = 1 - \widetilde{F}(t) = [N - N(t)]/N \ , \qquad (24)$$

где $[N–N(t)]$ – число систем, работоспособных к моменту t.

Функция $F(t)$, как правило, непрерывна, и существует непрерывная плотность распределения наработки до отказа

$$f(t) = \mathrm{d}F(t)/\mathrm{d}t \ . \qquad (2.5)$$

Для статистического определения плотности распределения

$f(t)$ рассмотрим интервал времени $(t-\Delta t/2, t+\Delta t/2)$, где Δt – длина этого интервала. Тогда

$$\tilde{f}(t)=\frac{N(t+\Delta t/2)-N(t-\Delta t/2)}{N\Delta t}=\frac{N(t-\Delta t/2, t+\Delta t/2)}{N\Delta t}\ , \qquad (2.6)$$

где $N(t-\Delta t/2, t+\Delta t/2)$ – число систем, отказавших в интервале времени $t-\Delta t/2, t+\Delta t/2$.

2.2.2 Вероятности отказа и безотказной работы

Зафиксируем в выражении (2.1) определенное значение $t=t_1$. Тогда

$$Q(t_1)=F(t_1)=\mathrm{P}\{T<t_1\} \qquad (2.7)$$

является *вероятностью отказа системы* до момента t_1.

В отличие от статистического определения функции $F(t)$ во всем диапазоне ее изменения при различных t статистическое определение вероятности отказа $\tilde{Q}(t_1)$ на интервале $(0, t_1)$ требует при той же точности оценивания меньших статистических данных. При фиксированном значении $t = t_1$ статистическое определение вероятности отказа

$$\tilde{Q}(t_1)=N(t_1)/N\ . \qquad (2.8)$$

Теперь зафиксируем значение $t = t_1$ в выражении (2.3). При этом

$$P(t_1)=\mathrm{P}\{T\geq t_1\} \qquad (2.9)$$

называется *вероятностью безотказной работы* до момента t_1 – вероятностью того, что система проработает безотказно на интервале $(0, t_1)$, начав работать в момент времени $t = 0$.

Статистическое определение вероятности безотказной работы

$$\tilde{P}(t_1)=1-\tilde{Q}(t_1)=[N-N(t_1)]/N\ . \qquad (2.10)$$

Для решения различных задач в качестве показателя надежности используется вероятность безотказной работы $P(t_1, t_2)$ системы на интервале (t_1, t_2) при условии, что эта система безотказно

проработала до момента t_1. Определим этот показатель по формуле умножения вероятностей, обозначив через A и B соответственно события, выражающие безотказную работу системы на интервалах $(0, t_1)$ и (t_1, t_2). Вероятность события AB – безотказной работы на интервале $(0, t_2)$ будет

$$\mathrm{P}\{AB\}=\mathrm{P}\{A\}\mathrm{P}\{B \mid A\}.$$

Отсюда

$$P(t_1,t_2)=\mathrm{P}\{B|A\}=\mathrm{P}\{AB\}/\mathrm{P}\{A\}=P(t_2)/P(t_1)\,. \qquad (2.11)$$

2.2.3 Интенсивность отказов

При описании надежности невосстанавливаемых систем широкое применение получила такая характеристика, как *интенсивность отказов* $\lambda(t)$. Она определяется как условная плотность вероятности отказа системы в момент t при условии, что до этого момента отказы не возникали.

Условная вероятность безотказной работы системы на интервале $(t, t+\Delta t)$ при условии, что система работоспособна в момент t, определяется выражением (2.11)

$$P(t,t+\Delta t)=P(t+\Delta t)/P(t)\,.$$

На интервале $(t, t+\Delta t)$ условная вероятность отказа системы

$$1-P(t,t+\Delta t)=1-P(t+\Delta t)/P(t)=-\left[P(t+\Delta t)-P(t)\right]/P(t)\,.$$

Разделим обе части равенства на Δt:

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

Устремив Δt к нулю, получим

$$\lambda(t)=\lim_{\Delta t\to 0}\left[\frac{1-P(t,t+\Delta t)}{\Delta t}\right]=-\frac{\mathrm{d}P(t)}{\mathrm{d}t}\frac{1}{P(t)}\,. \qquad (2.12)$$

Выражение (2.12) можно представить в виде

$$\lambda(t) = -\frac{\mathrm{d}[1-F(t)]}{\mathrm{d}t}\frac{1}{P(t)} = \frac{f(t)}{P(t)}\,, \qquad (2.13)$$

из чего следует, что $\lambda(t) \geq f(t)$.

Решим соотношение (2.12) относительно $P(t)$:

$$\int_0^t \lambda(t)\mathrm{d}t = -\int_0^t \mathrm{d}P(t)/P(t) = -\ln P(t)\,,$$

отсюда

$$P(t) = e^{-\int_0^t \lambda(t)\mathrm{d}t}\,. \qquad (2.14)$$

Для статистического определения интенсивности отказов в выражение (2.13) вместо $f(t)$ подставим $\tilde{f}(t)$ [см. (2.6)], а вместо $P(t)$ подставим $\tilde{P}(t)$[см. (2.4)], тогда

$$\tilde{\lambda}(t) = \tilde{f}(t)/\tilde{P}(t) = N(t-\Delta t/2, t+\Delta t/2)/\Delta t[N-N(t)]\,, \qquad (2.15)$$

где $N(t-\Delta t/2,\ t+\Delta t/2)$ – число систем, отказавших на интервале $(t-\Delta t/2,\ t+\Delta t/2)$; N-$N(t)$ – число систем, работоспособных к моменту t.

Так как функции $F(t)$ и $P(t)$ безразмерны, то размерность интенсивности отказов, как это следует из (2.13) , – величина, обратная наработке t (например, 1/ч).

Интенсивность отказов $\lambda(t)$ дает наглядную картину изменения безотказности. Типичная зависимость $\lambda(t)$ во времени дана на рис.2.2. Ниспадающий вид кривой $\lambda(t)$ относится к периоду приработки системы (1-й участок). При этом выявляются скрытые дефекты изготовления отдельных элементов системы, недостатки монтажа, наладки, нарушения, произошедшие в результате транспортировки. По окончании приработки наступает период нормальной эксплуатации (2-й участок). В течение этого времени интенсивность отказов относительно неизменна. Именно этот участок соответствует основному времени эксплуатации систем. Возрастание кривой $\lambda(t)$ относится к периоду старения системы из-за износа отдельных ее элементов и изменения их характеристик (3-й участок).

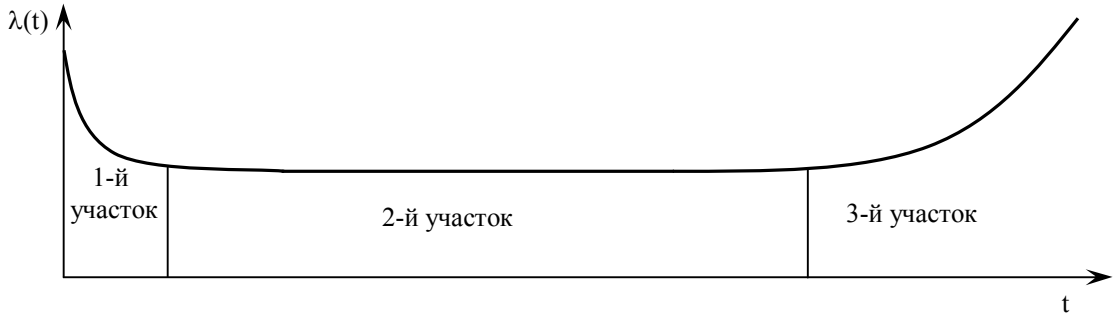


Рис. 2.2. **График изменения интенсивности отказов**

Пример 2.1. Пусть испытывалось N=100 невосстанавливаемых систем. К моменту t_1 = 7500 ч число отказавших систем $N(t_1)$=10; к моменту t_2 = 8000 ч $N(t_2)$=11, к моменту t_2=8500 ч $N(t_3)$=13.

Найти вероятность безотказной работы $P(t_2)$, вероятность отказа $Q(t_2)$, плотность распределения $f(t_2)$ и интенсивность отказов $\lambda(t_2)$ для t_2=8000 ч, причем при определении $f(t_2)$ и $\lambda(t_2)$ рассмотрим интервал времени ($t_1 = t_2 - \Delta t/2$; $t_3 = t_2 + \Delta t/2$), где $\Delta t = t_3 - t_1$ – длина этого интервала, а момент t_2 расположен посередине него.

Решение. Согласно соотношениям (3.8) и (3.10)

$$\tilde{Q}(8000) = N(8000)/N = 11/100 = 0{,}11 ;$$

$$\tilde{P}(8000) = \left[N - N(8000)\right]/N = (100-11)/100 = 0{,}89 .$$

Согласно (3.6)

$$\tilde{f}(8000) = \left[N(8500) - N(7500)\right]/N(N\Delta t) = (13-10)/(100\cdot 1000) = 3\cdot 10^{-5}\ \text{ч}^{-1} .$$

Согласно (3.15)

$$\tilde{\lambda}(8000) = \left[N(8500) - N(7500)\right]/\left[N - N(8000)\right]\Delta t = (13-10)/\left[(100-11)\cdot 1000\right] = 3{,}37\cdot 10^{-5}\ \text{ч}^{-1} .$$

2.2.4 Средняя наработка до отказа

Функции $F(t)$, $f(t)$, $P(t)$, $\lambda(t)$ полностью описывают случайную величину T. В то же время для решения значительного числа задач надежности достаточно знать только показатели, являющиеся числовыми характеристиками этой случайной величины. К ним в первую очередь относится *средняя наработка до отказа*

(среднее время безотказной работы) – математическое ожидание случайной величины T – наработки до отказа (или времени безотказной работы)

$$\tau = \mathrm{M}[T] = \int_0^\infty t f(t)\,\mathrm{d}t \ , \qquad (2.16)$$

где **M** – символ математического ожидания.

Преобразуем выражение (3.16) к виду

$$\tau = -\int_0^\infty t\mathrm{d}P(t) = -tP(t)\Big|_0^\infty + \int_0^\infty P(t)\,\mathrm{d}t = \int_0^\infty P(t)\,\mathrm{d}t \ . \qquad (2.17)$$

Отсюда следует, что средняя наработка до отказа геометрически равна площади под кривой $P(t)$ (см. рис. 2.1).

Статистическое определение средней наработки до отказа

$$\tilde{\tau} = \sum_{i=1}^{N} t_i / N \ , \qquad (2.18)$$

где t_i – наработка до отказа i-й системы; N – число систем.

Реже используются такие показатели, как дисперсия и среднеквадратическое отклонение наработки до отказа:

$$\mathrm{D}[T] = \mathrm{M}\left[(T-\tau)^2\right] = \int_0^\infty (t-\tau)^2 f(t)\,\mathrm{d}t = \int_0^\infty t^2 f(t)\,\mathrm{d}t - \tau^2 \ ;$$

$$\sigma[T] = \sqrt{\mathrm{D}[T]} \ , \qquad (2.19)$$

где τ и $\sigma[T]$ имеют размерность времени (обычно они выражаются в часах); **D**$[T]$ – квадрата времени.

Статистические определения дисперсии и среднеквадратического отклонения, соответственно

$$\tilde{\mathrm{D}}[T] = \sum_{i=1}^{N} (t_i - \tilde{\tau})^2 / (N-1); \qquad \tilde{\sigma}[T] = \sqrt{\tilde{\mathrm{D}}[T]} \ . \qquad (2.20)$$

Взаимосвязь показателей безотказности невосстанавливае-

мых систем показана в табл. 3.1. Знание любой функции $F(t)$, $f(t)$, $P(t)$, $\lambda(t)$ дает возможность найти три остальные.

Пример 2.2. Определить среднюю наработку до отказа $\tilde{\tau}$, дисперсию $\tilde{\mathrm{D}}[T]$ и среднеквадратическое отклонение $\tilde{\sigma}[T]$ наработки до отказа по результатам испытаний невосстанавливаемых систем. Число испытуемых систем $N = 8$. Наработка до отказа каждой i-й системы приведена ниже:

t_1	t_2	t_3	t_4	t_5	t_6	t_7	t_8
12300	7600	14100	2900	9300	8500	10600	13100

Решение. Согласно (3.18) средняя наработка до отказа

$$\tilde{\tau} = (12300 + 7600 + 14100 + 2900 + 9300 + 8500 + 10600 + 13100)/8 = 9780 \text{ ч}.$$

Согласно (2.20) имеем

$$\tilde{\mathrm{D}}[T] = 14 \cdot 10^6 \text{ ч}^2; \qquad \tilde{\sigma}[T] = 3740 \text{ ч}.$$

2.3 Основные законы распределения наработки до отказа

2.3.1 Экспоненциальное распределение

Непрерывная случайная величина – наработка системы до отказа может описываться различными законами распределения в зависимости от свойств системы и ее элементов, условий работы, характера отказов и др. Наибольшее распространение получило экспоненциальное (показательное) распределение, при котором функция распределения наработки до отказа

$$F(t) = 1 - e^{-\lambda t}, \qquad (2.21)$$

где λ – параметр этого распределения.

Согласно (2.5) соответствующая плотность распределения

$$f(t) = \lambda e^{-\lambda t}. \qquad (2.22)$$

Согласно (2.3) функция надежности

$$P(t) = e^{-\lambda t}. \qquad (2.23)$$

Согласно (2.7) и (2.9) вероятность отказа системы до момента t_1 и вероятность безотказной работы до момента t_1, соответственно, будут

$$Q(t_1) = 1 - e^{-\lambda t_1}; \quad P(t_1) = e^{-\lambda t_1} \quad .$$

Согласно (2.17) средняя наработка до отказа

$$\tau = \int_0^\infty P(t)\,\mathrm{d}t = \int_0^\infty e^{-\lambda t}\mathrm{d}t = 1/\lambda \quad , \qquad (2.24)$$

т. е. равна величине, обратной параметру λ экспоненциального распределения.

Подставив в (2.19) плотность распределения (2.22), после двукратного интегрирования по частям найдем дисперсию наработки до отказа

$$\mathrm{D}[T] = \int_0^\infty t^2 \lambda e^{-\lambda t}\mathrm{d}t - \tau^2 = -t^2 e^{-\lambda t}\Big|_0^\infty + 2\int_0^\infty te^{-\lambda t}\mathrm{d}t - 1/\lambda^2 =$$

$$= -\left(2te^{-\lambda t}/\lambda\right)\Big|_0^\infty + (2/\lambda)\int_0^\infty e^{-\lambda t}\mathrm{d}t - 1/\lambda^2 = 1/\lambda^2 \quad .$$

Из (2.13) следует, что интенсивность отказов

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

является постоянной величиной, не зависящей от времени и численно равной параметру распределения и, как видно из (2.24), обратной средней наработке до отказа.

Графики изменения показателей надежности при экспоненциальном распределении даны на рис. 4.1, *а*.

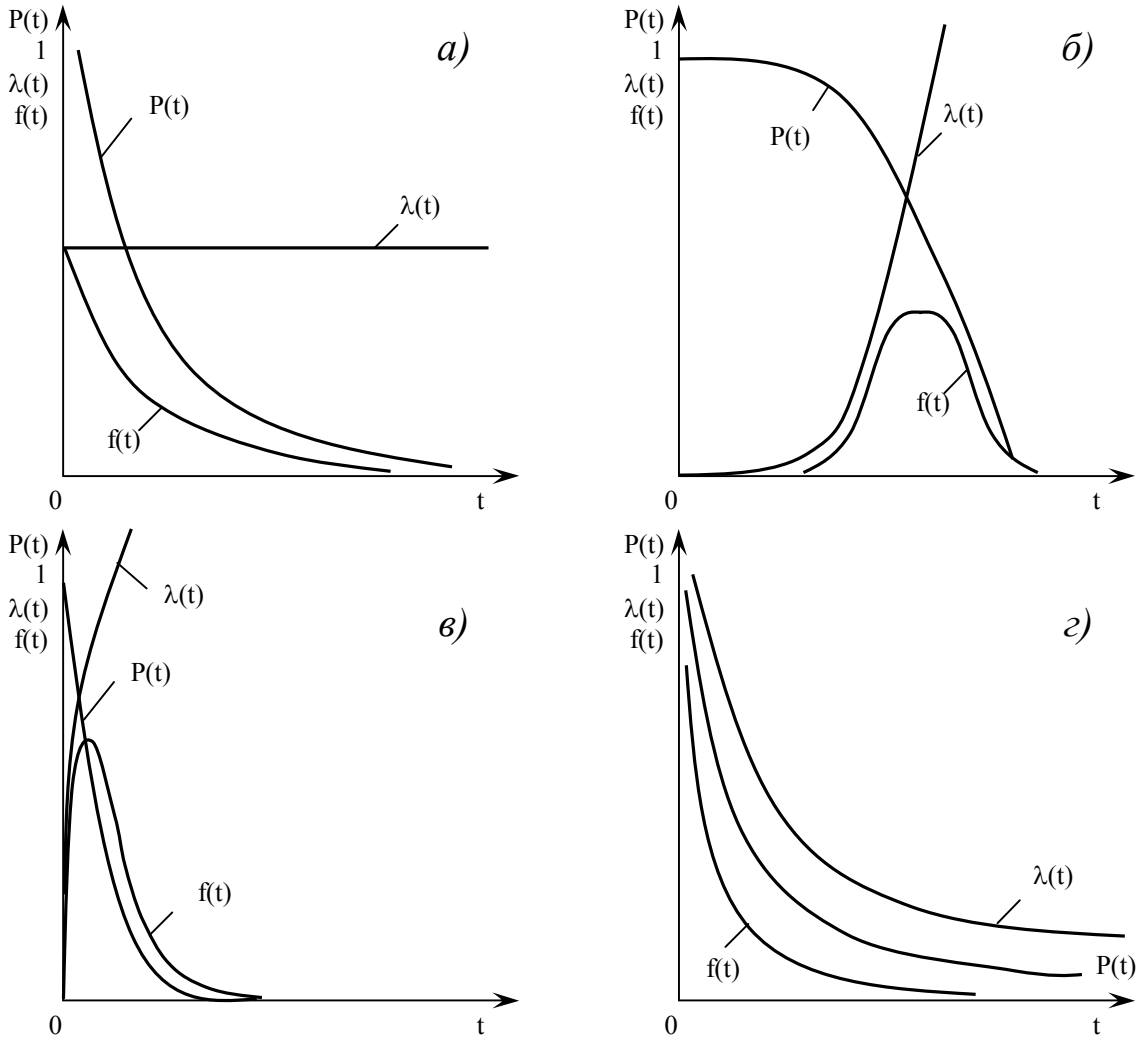


Рис.4.1. Графики изменения показателей надежности для различных законов распределения

При $\lambda t << 1$ т.е. времени t, намного меньшем средней наработки до отказа $\tau = 1/\lambda$ выражения (2.21) – (2.23) можно упростить, заменив $e^{-\lambda t}$ двумя первыми членами разложения $e^{-\lambda t}$ в степенной ряд. Тогда выражение (2.23) примет вид

$$P(t) \approx 1 - \lambda t = 1 - t/\tau.$$

Получающаяся при этом погрешность не превышает $0{,}5(\lambda t)^2$.

Отметим одно характерное свойство, присущее только экспоненциальному распределению: вероятность $P(t_1, t_2)$ безотказной работы системы на интервале (t_1, t_2) (при условии, что в момент t_1 система работоспособна) зависит только от длины интер-

вала $t_2 - t_1$ и не зависит от времени t_1 предшествующей работы системы, т.е. от ее «возраста». Чтобы это доказать, достаточно в (2.11) подставить значение (2.23):

$$P(t_1, t_2) = e^{-\lambda t_2} / e^{-\lambda t_1} = e^{-\lambda(t_2 - t_1)} . \qquad (2.25)$$

Так как для экспоненциального закона характерно постоянство интенсивности отказов λ=const, то область применения этого закона – системы и элементы, где можно не учитывать ни период приработки, ни участок старения и износа (например, многие средства вычислительной техники и регулирования). Можно показать, что экспоненциальное распределение хорошо описывает время безотказной работы сложных систем, состоящих из большого числа разнородных компонентов. Наконец, одна из основных причин широкого использования экспоненциального закона заключается в том, что вследствие неизменности величины λ расчеты надежности при применении этого распределения наиболее просты.

Пример 3.1. Наработка системы до отказа описывается экспоненциальным распределением с параметром $\lambda=1\cdot10^4$ ч$^{-1}$. Определить вероятность безотказной работы $P(t_1)$ и плотность распределения $f(t_1)$ при t_1 = 2000 ч, а также среднюю наработку до отказа τ.

Решение.

Согласно (2.23)

$$P(2000) = e^{-1\cdot10^{-4}\cdot2000} = 0{,}819.$$

Согласно (2.22)

$$f(2000) = 1\cdot10^{-4}\cdot e^{-1\cdot10^{-4}\cdot2000} = 0{,}819\cdot10^{-4} \text{ ч}^{-1} .$$

Согласно (2.24)

$$\tau = 1/\lambda = 10^4 \text{ ч}.$$

2.3.2 Нормальное распределение

В отличие от экспоненциального нормальное распределение используют для описания таких систем и особенно их элементов, которые подвержены действию износа. Функция и плотность распределения наработки до отказа T при этом соответственно будут

$$F(t)=\frac{1}{\sigma\sqrt{2\pi}}\int_{-\infty}^{t}e^{-(x-m)^2/(2\sigma^2)}\,\mathrm{d}x\ ; \qquad (2.26)$$

$$f(t)=\frac{1}{\sigma\sqrt{2\pi}}e^{-(t-m)^2/(2\sigma^2)}\ , \qquad (2.27)$$

где σ и m – параметры нормального распределения.

Пользуясь соотношениями (2.16) и (2.19), можно показать, что при нормальном распределении средняя наработка до отказа и дисперсия наработки до отказа будут

$$\tau=m;\ \ \mathrm{D}[T]=\sigma^2\ . \qquad (2.28)$$

Графики изменения показателей надежности при нормальном распределении даны на рис. 4.1, *б*.

Для практического использования соотношений (2.26) и (2.27) перейдем от случайной величины T к иной случайной величине

$$Z=(T-m)/\sigma\ , \qquad (2.29)$$

имеющей математическое ожидание **M**[Z]=0 и дисперсию **D**[Z]=1.

Согласно правилам определения закона распределения функции случайного аргумента (см. [1]) плотность распределения величины Z следует из (2.27) и (2.29):

$$\varphi(z)=f(z\sigma+m)\frac{\mathrm{d}(z\sigma+m)}{\mathrm{d}z}=\frac{1}{\sqrt{2\pi}}e^{-z^2/2}\ .$$

Соответственно функция распределения величины Z

$$\Phi(z) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} e^{-x^2/2} \mathrm{d}x \ .$$

Очевидно, что функция $\varphi(z)$ является симметричной, т.е. $\varphi(-z) = \varphi(z)$, а следовательно, $\Phi(-z) = 1 - \Phi(z)$.

В таблицах часто приводят значения не функции $\Phi(z)$, а несколько иной функции

$$\Phi_0(z) = \frac{1}{\sqrt{2\pi}} \int_{0}^{z} e^{-x^2/2} \mathrm{d}x \ . \qquad (2.30)$$

Функции $\Phi(z)$ и Φ_0 связаны между собой соотношением

$$\Phi(z) = \begin{cases} 0{,}5 + \Phi_0(z), & \text{при} \quad z \geq 0; \\ 0{,}5 - \Phi_0(|z|), & \text{при} \quad z \leq 0. \end{cases} \qquad (2.31)$$

Приведем значения функции (2.30) для нескольких положительных z:

$$\Phi_0(0{,}5) = 0{,}191; \quad \Phi_0(1) = 0{,}3413; \quad \underline{\Phi_0(2) = 0{,}477}.$$

Пример 4.2. Наработка до отказа системы описывается нормальным распределением с параметрами m = 4000 ч, σ= 1000 ч. Определить вероятность безотказной работы $P(t_1)$, плотность распределения $f(t_1)$, интенсивность отказов $\lambda(t_1)$ для t_1 = 2000 ч и среднюю наработку до отказа τ.

Решение. Согласно (2.3) и (2.26) определим сначала вероятность безотказной работы

$$P(2000) = 1 - \frac{1}{\sigma\sqrt{2\pi}} \int_{-\infty}^{t} \exp\left[-\frac{(x-m)^2}{2\sigma^2} \right] \mathrm{d}x \ .$$

Применив подстановку (2.29), получим

$$P(2000) = 1 - \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} e^{-x^2/2} \mathrm{d}x = 1 - \Phi(z) \ ,$$

где $z = (t-m)/\sigma = (2000-4000)/1000 = -2$.

Так как значение $z < 0$, то согласно (2.31)

$$\Phi(-2) = 0{,}5 - \Phi_0(2) = 0{,}023 \ ;$$
$$P(2000) = 1 - \Phi(-2) = 0{,}977 \ .$$

Подставив в (2.27) значения σ, m, t_1, определим плотность распределения

$$f(2000) = \frac{1}{1000\sqrt{2\pi}} e^{-(4000-2000)^2/\left(2\cdot 1000^2\right)} = 0{,}54\cdot 10^{-4} \text{ ч}^{-1} \ .$$

Согласно (2.13) при $t_1 = 2000$ ч интенсивность отказов

$$\lambda(2000) = f(2000)/P(2000) = 0{,}54\cdot 10^{-4} / 0{,}977 = 0{,}55\cdot 10^{-4} \text{ ч}^{-1} \ .$$

Согласно (2.28) средняя наработка до отказа

$$\tau = m = 4000 \text{ ч} \ .$$

Нормальное распределение, как это видно из соотношения (4.6), описывает поведение случайных величин в диапазоне (–∞, ∞). Однако наработка до отказа является неотрицательной величиной, чтобы это учесть, вместо нормального, в принципе, должно использоваться усеченное нормальное распределение. Область возможных значений случайной величины T может быть различной. Ниже примем, что эта область (0, ∞), и проведем усечение распределения в точке t=0. Тогда функция распределения случайной величины T имеет вид

$$F(t) = \begin{cases} 0, & t \le 0; \\ \dfrac{c}{\sigma\sqrt{2\pi}} \displaystyle\int_0^t e^{-(x-m)^2/\left(2\sigma^2\right)} \mathrm{d}x, & t > 0, \end{cases}$$

где c – нормирующий множитель; σ, m – параметры распределения.

При этом плотность распределения

$$f(t) = \frac{c}{\sigma\sqrt{2\pi}} e^{-(t-m)^2/\left(2\sigma^2\right)} \ .$$

Значение c выбирают из условия, что площадь под кривой плотности распределения равна единице. Использовав подстановку (4.9), можно показать, что

$$c = \sqrt{2\pi} \Big/ \int_{-m/\sigma}^{\infty} e^{-z^2/2}\,\mathrm{d}z \ .$$

В усеченном нормальном распределении средняя наработка до отказа и дисперсия наработки до отказа

$$\tau = m + \sigma c_1 \ ;$$

$$\mathrm{D}[T] = \sigma^2\left[1 - c_1^2 - c_1 m/\sigma\right] \ ,$$

где $c_1 = \dfrac{c}{\sqrt{2\pi}} e^{-m^2/(2\sigma^2)}$.

Усеченное нормальное распределение обычно применяют, если $m < 3\sigma$. В противном случае (как это было, например, в примере 2.22) использование более простого нормального (неусеченного) распределения дает достаточную точность.

2.3.3 Распределение Вейбулла - Гнеденко

В теории надежности получило применение распределение Вейбулла–Гнеденко, описываемое функцией и плотностью распределения, соответственно,

$$F(t) = 1 - e^{-\alpha t^k}; \quad f(t) = \alpha k t^{k-1} e^{-\alpha t^k} \ .$$

Это двухпараметрическое распределение, где параметр k определяет вид плотности распределения, параметр α – его масштаб. Так, при k=1 распределение Вейбулла–Гнеденко совпадает с экспоненциальным (рис. 4.1, *а*), когда интенсивность отказов постоянна; при $k > 1$ интенсивность отказов монотонно возрастает (рис. 4.1, *в*), при $k < 1$ монотонно убывает (рис 4.1, *г*). Распределение Вейбулла–Гнеденко может быть применено для описания наработки до отказа ряда электронных и механических технических средств, включая период приработки.

Соотношения для определения показателей надежности для трех рассмотренных выше распределений даны в табл. 4.1.

3. ДОЛГОВЕЧНОСТЬ, РЕМОНТОПРИГОДНОСТЬ И СОХРАНЯЕМОСТЬ КАК ОСНОВНЫЕ КОМПОНЕНТЫ НАДЁЖНОСТИ

Долговечность – свойство системы сохранять работоспособность до наступления предельного состояния с необходимыми перерывами для технического обслуживания и ремонтов. Долговечность системы зависит от долговечности технических средств и от подверженности системы моральному старению.

Ремонтопригодность является свойством системы, заключающимся в ее приспособленности к предупреждению, обнаружению и устранению причин возникновения отказов, а также поддержанию и восстановлению работоспособного состояния путем проведения технического обслуживания и ремонтов. Ремонтопригодность зависит от того, выполнены ли элементы в виде отдельных, легко заменяемых блоков, а также от использования средств встроенного контроля работоспособности и диагностики. Следует отметить, что характеристики ремонтопригодности существенно зависят не только от свойств самой системы, но и от квалификации обслуживающего персонала и от организации эксплуатации.

Сохраняемость характеризует свойство системы сохранять значения показателей безотказности и ремонтопригодности в течение и после срока хранения и транспортировки. Поскольку системы в целом не хранятся, а могут сохраняться только отдельные технические средства и их элементы, то свойство сохраняемости для систем несущественно. Для технических средств и элементов это свойство имеет определенное значение, но менее важное, чем предыдущие свойства, так как эти средства обычно транспортируются только один раз – от завода-изготовителя к месту установки и длительность их хранения от момента поступления до монтажа и наладки (кроме технических средств и элементов, используемых в качестве запасных частей) относительно невелика. Вследствие этого вопросы сохраняемости ниже рассматриваться не будут.

3.1. Показатели надёжности восстанавливаемых систем

3.1.1 Потоки отказов восстанавливаемых систем

После каждого отказа восстанавливаемой системы следует ее восстановление. Продолжительностью восстановления будем пренебрегать в настоящем параграфе. График функционирования системы при этом допущении представлен на рис. 3.1, *а*.

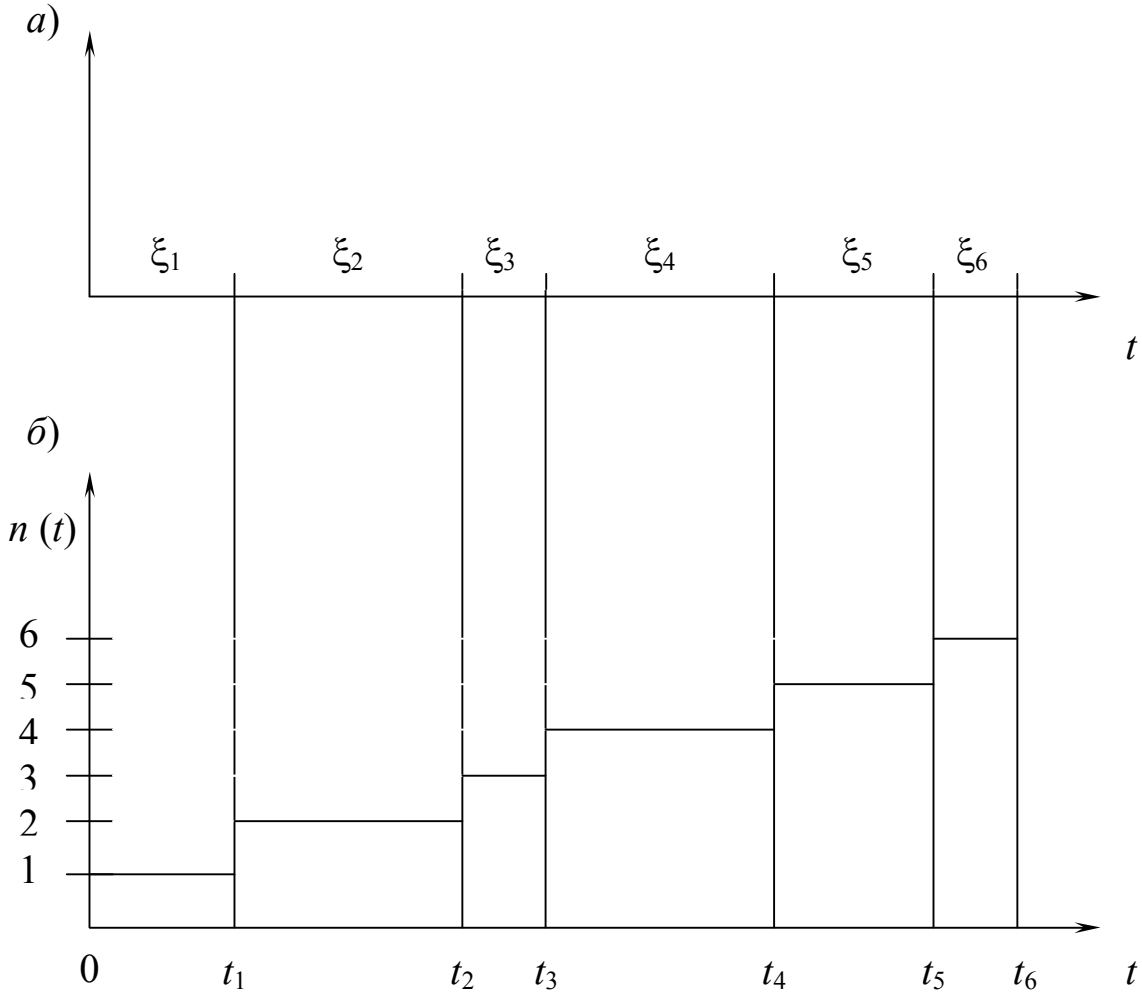


Рис. 3.1. **График функционирования восстанавливаемой системы**

Последовательность отказов, происходящих один за другим в случайные моменты времени, носит название *потока отказов*.

Возможны два основных способа задания потока отказов.

Первый заключается в изучении некоторого случайного процесса $\eta(t)$ – числа отказов на промежутке времени $(0, t)$. Одна из возможных реализаций $n(t)$ этого процесса дана на рис. 5.1, *б*.

Второй способ заключается в изучении последовательности

непрерывных случайных наработок $\xi_1=t_1$; $\xi_2=t_2-t_1$; $\xi_3=t_3-t_2$,… между отказами.

Также как случайную величину можно задать функцией распределения вероятности принимаемых ею значений, процесс $\eta(t)$ можно было бы задать распределением вероятности всех его реализаций $n(t)$. Однако попытка явного задания такого распределения сопряжена с определенными трудностями.

3.1.2 Показатели безотказности

В соответствии с двумя способами задания потока отказов для восстанавливаемых систем можно применять различные показатели безотказности.

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

$$\omega(t) = \mathrm{d}W(t)/\mathrm{d}t, \quad \text{где} \quad W(t) = \mathrm{M}[\eta(t)] .$$

Для статистического определения параметра потока отказов поставим на испытания N одинаковых восстанавливаемых систем в одинаковых условиях эксплуатации и при одинаковом техническом обслуживании. В момент $t = 0$ все системы работоспособны и начинают работу. Не нарушая общности, будем пренебрегать продолжительностью восстановления.

Обозначим $n_i(t)$ число отказов i-ой системы ($i = 1,..., N$) на интервале $(0, t)$. Тогда

$$\omega(t) = \sum_{i=1}^{N} [n_i(t+\Delta t) - n_i(t)]/(N\Delta t) .$$

Таким образом, параметр потока отказов – отношение числа отказов системы на некотором малом отрезке времени к значению этого отрезка.

При задании потока отказов как последовательности случайных величин ξ_1, ξ_2, … наработок между отказами [в предположении, что эти наработки имеют одинаковое распределение с плотностью $f(t)$] показателем безотказности является средняя на-

работка на отказ

$$\theta = \mathrm{M}[\xi_i] = \int_0^\infty t f(t)\,\mathrm{d}t, \quad (i = 1, 2, \ldots) .$$

Отметим, что в простейшем потоке средняя наработка на отказ θ и параметр потока ω(*t*) связаны соотношением θ = 1/ω. Для статистического определения средней наработки на отказ $\tilde{\theta}$ будем, как и выше, испытывать *N* одинаковых восстанавливаемых систем. Предположим, что каждая из них проработала в течение времени *t*. Тогда

$$\tilde{\theta} = Nt \Big/ \sum_{i=1}^{N} n_i(t) . \qquad (3.1)$$

3.1.3 Показатели ремонтопригодности

Ранее предполагалось, что продолжительностью восстановления можно пренебречь по сравнению с временем между отказами. На практике продолжительность восстановления почти всегда существенно меньше времени между отказами, однако нельзя не учитывать продолжительность восстановления для решения многих задач надежности (например, расчета потерь из-за отказов, количества необходимого ремонтного персонала и др.).

Обозначим $T_в$ случайную величину – продолжительность восстановления работоспособного состояния системы после отказа (далее сокращенно – время восстановления).

Будем полагать, что распределение величины $T_в$ не зависит ни от времени, ни от порядкового номера восстановления, ни от длительности предыдущего восстановления, ни от предшествующей наработки между отказами. Функцию распределения величины $T_в$ обозначим *G*(*t*), плотность распределения *g*(*t*). Если к тому же наработки между отказами ξ_1, ξ_2, ξ_3, … одинаково распределены и не зависят друг от друга и от величины $T_в$, то такой поток отказов с учетом времени восстановления носит название альтернирующего процесса восстановления. Отметим, что в этом процессе, как и в процессе восстановления, средняя наработка на отказ θ равна средней наработке до отказа τ.

График функционирования системы с учетом времени восстановления дан на рис. 3.2. Для упрощения принято, что единственной причиной отключения системы являются ее отказы – отключения по всем иным причинам не рассматриваются.

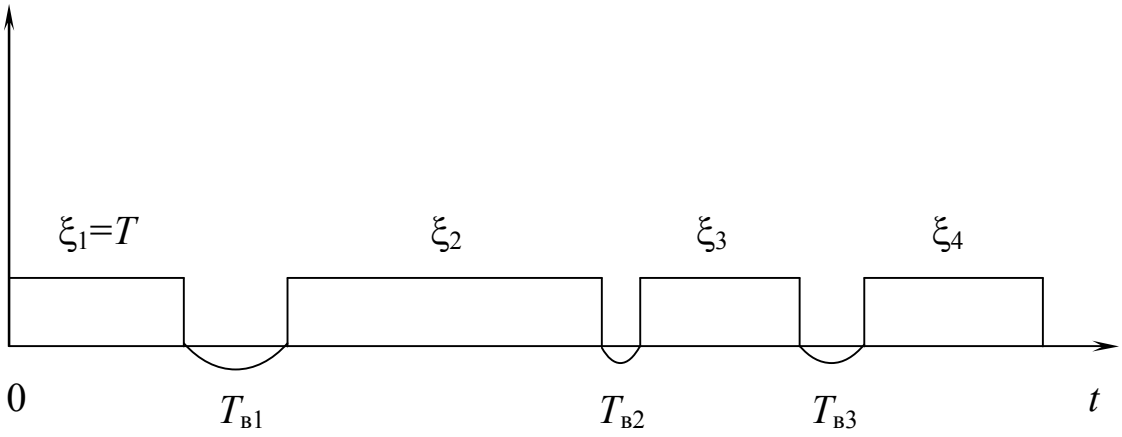


Рис. 3.2. График функционирования системы с учетом времени восстановления

Показателями ремонтопригодности являются вероятность восстановления работоспособного состояния за заданное время t_1 и среднее время восстановления соответственно

$$G(t_1) = \mathrm{P}\{T_\text{в} < t_1\}; \quad \tau_\text{в} = \mathrm{M}[T_\text{в}]\,. \tag{3.2}$$

Статистические определения этих показателей:

$$\widetilde{G}(t_1) = l(t_1)/m; \quad \widetilde{\tau}_\text{в} = \sum_{i=1}^{m} t_{\text{в}i}/m\ , \tag{3.3}$$

где $l(t_1)$ – число восстановлений, длительность которых меньше t_1; m – общее число восстановлений; $t_{\text{в}i}$ – время восстановления после i-го отказа.

3.1.4 Показатели долговечности

Календарную продолжительность от начала эксплуатации системы до перехода в предельное состояние называют *сроком службы системы*. Срок службы системы может быть случайной величиной, которую обозначим $T_\text{с}$. Тогда в качестве показателя долговечности можно принять средний срок службы

$$\bar{t}_\text{с} = \mathrm{M}[\mathrm{T_с}]$$

или гамма-процентный срок службы t_γ, который определяется соотношением

$$\mathrm{P}\{T_\mathrm{c} > t_\gamma\} = \gamma / 100 \ .$$

Таким образом t_γ – календарная продолжительность от начала эксплуатации объекта, в течение которой он не достигнет предельного состояния с заданной вероятностью γ (выраженной в процентах).

Для некоторых систем показателем долговечности является установленный срок службы, который должна достигнуть каждая система. Этот показатель можно интерпретировать как t_γ при γ=100%.

В качестве случайной величины при рассмотрении долговечности может быть принят не только календарный срок службы системы, но и ее ресурс – наработка от начала эксплуатации до перехода в предельное состояние.

3.1.5 Комплексные показатели надежности

Кроме приведенных выше показателей, каждый из которых характеризует одну из составляющих надежности, используются также комплексные показатели, отражающие совместно безотказность и ремонтопригодность. К ним относятся: коэффициент готовности $k_\mathrm{г}$, коэффициент оперативной готовности $k_{\mathrm{о.г}}(t)$ и коэффициент технического использования $k_{\mathrm{т.и}}$.

Коэффициентом готовности $k_\mathrm{г}$ называют вероятность того, что система окажется работоспособной в произвольно выбранный момент времени в установившемся процессе эксплуатации. Можно показать (см., например, [2]), что в альтернирующем процессе восстановления коэффициент готовности

$$k_\mathrm{г} = \theta / (\theta + \tau_\mathrm{в}) \ , \qquad (3.4)$$

т. е. этот коэффициент численно равен средней доле времени, в течение которого система пребывает в работоспособном состоянии.

Для статистического определения коэффициента готовности поставим на испытания N одинаковых восстанавливаемых систем и обозначим $N_\mathrm{р}(t_\mathrm{х})$ число систем, находящихся в состоя-

нии работоспособности в произвольный, достаточно удаленный от начала испытаний момент времени $t_х$. Тогда статистическое определение коэффициента готовности

$$\widetilde{k}_г = N_р(t_х)/N \ .$$

Коэффициентом оперативной готовности $k_{о.г}(t)$ называют вероятность того, что система окажется работоспособной в произвольно выбранный момент времени в установившемся режиме эксплуатации и что, начиная с этого момента, система будет работать безотказно в течение заданного интервала времени t. Из этого определения и из (5.4) следует, что в альтернирующем процессе восстановления

$$k_{о.г}(t) = \frac{\theta}{\theta + \tau_в} P(t_х, t_х + t) \ , \qquad (3.5)$$

где $P(t_х, t_х+t)$ – условная вероятность безотказной работы системы на интервале $(t_х, t_х+t)$ при условии, что в момент $t_х$ система была работоспособна.

Если распределение времени безотказной работы системы является экспоненциальным, то (5.5) можно упростить, учитывая свойство (4.5) экспоненциального распределения: независимость вероятности безотказной работы на интервале $(t, t+\Delta t)$ от момента t. Тогда

$$k_{о.г}(t) = \frac{\theta}{\theta + \tau_в} e^{-\lambda t} \ . \qquad (3.6)$$

Отметим, что при определении коэффициента готовности и коэффициента оперативной готовности из рассмотрения исключены планируемые периоды времени, в течение которых применение систем по назначению не предусматривается (например, интервалы планового технического обслуживания). Эти периоды времени учитываются коэффициентом технического использования

$$k_{т.и} = \tau_{рΣ}/(\tau_{рΣ} + \tau_{т.оΣ} + \tau_{вΣ}),$$

где $\tau_{рΣ}$, $\tau_{т.оΣ}$, $\tau_{вΣ}$ – соответственно математические ожидания суммарных времен пребывания системы в работоспособном состоянии, технического обслуживания и восстановления за некоторый

период эксплуатации τ_{Σ}.

Пример.31. Средняя наработка на отказ регулятора θ=5000 ч, среднее время восстановления $\tau_{в}$=2 ч. Время между отказами распределено по экспоненциальному закону. Определить коэффициент готовности $k_{г}$ и коэффициент оперативной готовности $k_{о.г}(t)$ при t=200 ч.

Решение. Согласно (3.4) коэффициент готовности

$$k_{г} = 5000/(5000+2) = 0{,}9996 .$$

Согласно (5.6) коэффициент оперативной готовности

$$k_{о.г}(200) = \frac{5000}{5000+2} e^{-\frac{200}{5000}} = 0{,}9604 .$$

3.2 Расчеты надёжности различных резервированных систем

Основные этапы расчета надежности

Задачей расчета надежности технологических систем регулирования, контроля, защиты и дистанционного управления является определение показателей, характеризующих их безотказность и ремонтопригодность. Расчет складывается из следующих этапов: а) определение критериев и видов отказа системы и состава рассчитываемых показателей надежности; б) составление структурной (логической) схемы, основанной на анализе функционирования системы, учете резервирования, восстановления, контроля исправности элементов и др.; в) выбор метода расчета надежности с учетом принятых моделей описания процессов функционирования и восстановления; г) получение в общем виде математической модели, связывающей определяемые показатели надежности с характеристиками элементов; д) подбор данных по показателям надежности элементов; е) выполнение расчета и анализ полученных результатов.

Содержание перечисленных этапов в значительной мере зависит от выбранных критериев отказа и рассчитываемых показа-

телей надежности. К наиболее характерным показателям надежности технологических систем относятся средняя наработка до отказа системы, вероятность ее безотказной работы за заданное время, коэффициент готовности, коэффициент оперативной готовности, параметр потока отказов.

Близкие по характеру показатели распространяются и на элементы системы – технические средства, с помощью которых реализуются технологические системы. Количество рассматриваемых показателей расширяется, если анализируется вероятность работы систем с ухудшенными показателями качества функционирования, т. е. при учете постепенных (метрологических) отказов элементов.

Рассмотренные показатели применяются как при создании систем, так и при их эксплуатации.

Составление структурной схемы, являющейся логической схемой для расчета надежности как системы, так и отдельного технического средства, включает некоторые моменты, на которых необходимо остановиться более подробно. *Структурная схема* для расчета надежности в общем случае существенно отличается от функциональной схемы. Структурной схемой для расчета надежности называется графическое отображение элементов системы, позволяющее однозначно определить состояние системы (работоспособное или неработоспособное) по состоянию (работоспособное или неработоспособное) ее элементов.

Для многофункциональных систем, например АСУ ТП, такие структурные схемы составляют по каждой функции; их обычно называют надежностными схемами функции или надежностно-функциональными схемами [3].

При составлении схемы элементы системы могут соединяться последовательно (рис. 3.3, *а*) или параллельно (рис. 3.3, *б*) в зависимости от их влияния на работоспособное состояние системы. Если отказ элемента независимо от его назначения вызывает отказ системы, то элемент соединяют последовательно. Если отказ системы возникает при отказе всех или части однотипных элементов, то такие элементы соединяют параллельно. Последовательное соединение элементов называют также основным, а параллельное – резервным.

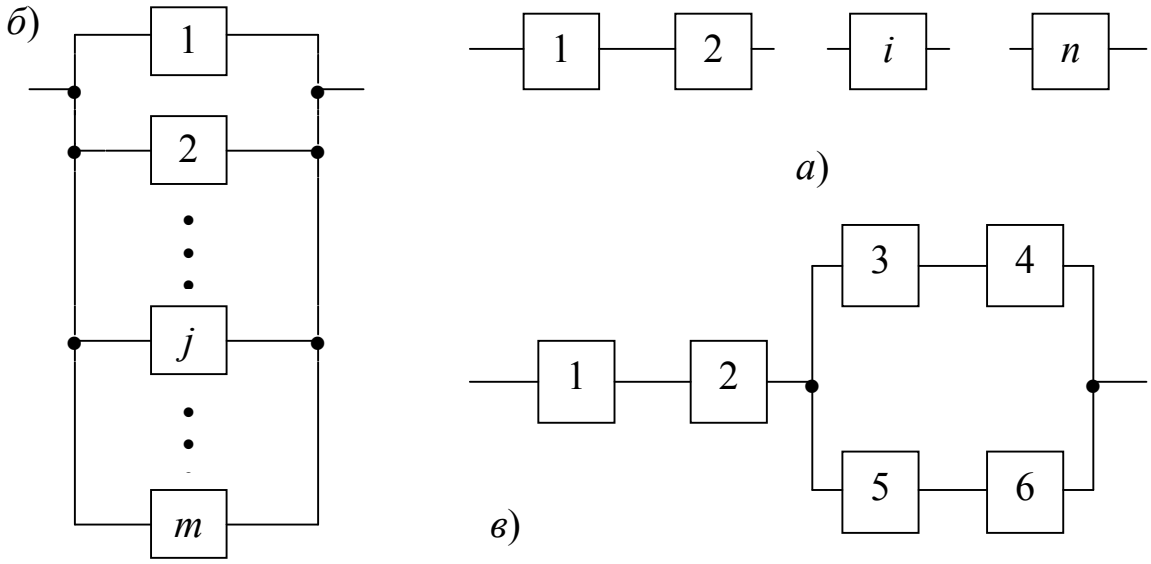


Рис. 3.3. **Соединение элементов системы: *а* – последовательное (основное); *б* – параллельное (резервное); *в* – смешанное**

Для иллюстрации принципов составления структурной схемы на рис. 3.4 представлены упрощенная функциональная и структурные схемы трехимпульсного регулятора уровня в барабане котла. Расходомеры питательной воды $F_в$, пара $F_п$, уровнемер уровня в барабане котла L и задатчик уровня Зд на структурной схеме включены последовательно, поскольку отказ любого из устройств, как и отказ регулирующего прибора Р, приводит к отказу регулятора уровня. Регулирующие органы РО с исполнительными механизмами ИМ могут находиться в основном (рис. 3.4 *б*) или резервном (рис.3.4, *в*) соединении в зависимости от того, способна ли функционировать система с одним регулирующим органом или нет. Если для поддержания постоянства уровня в барабане котла достаточно регулирования подачи питательной воды только по одной нитке, что обычно имеет место, то исполнительные механизмы с регулирующими органами соединяются на структурной схеме параллельно, как показано на рис. 3.4, *в*, в противном случае их включают последовательно (рис. 3.4, *б*).

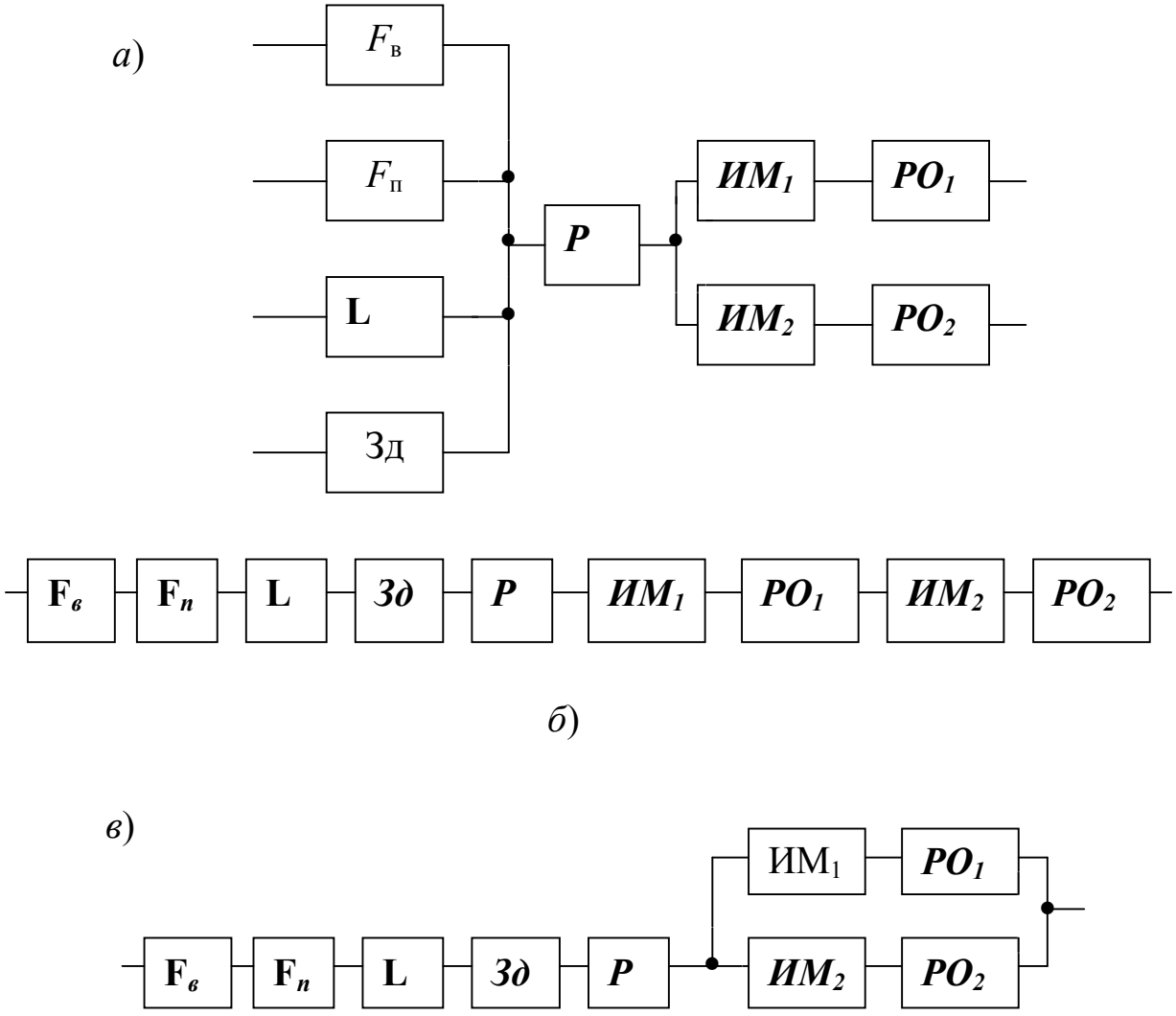


Рис. 3.4. Функциональная (*а*) и структурные схемы (*б*, *в*) трехимпульсного регулятора уровня в барабане котла

Для одних и тех же технологических систем могут быть составлены различные структурные схемы в зависимости от анализируемой функции системы, если она является многофункциональной, и вида отказа. Так, для улучшения качества регулирования во многих технологических системах вводятся сигналы по производной от регулируемой величины или динамические связи между параметрами. Естественно, что отказ элементов, участвующих в формировании этих сигналов, приведет к ухудшению качества регулирования, но, как правило, не вызовет отключения системы регулирования. В связи с этим структурные схемы систем, составленные по внезапным и параметрическим отказам, могут существенно отличаться. Аналогичные структурные схемы составляют при расчете надежности техни-

ческих средств, входящих в состав системы. В качестве их элементов выступают блоки: измерительные, усиления, питания, регистрации, индикации и др. с входящими в их состав механическими (редукторы, рычажные передачи), электромеханическими (реле, двигатели, трансформаторы), радиоэлектронными (резисторы, интегральные схемы, конденсаторы) и другими элементами, имеющими индивидуальные показатели надежности. На рис. 3.5, *а* и *б* представлены функциональная и структурная схемы нормирующего преобразователя температуры, включающего блоки: измерительный ИБ, усилительный УБ, отрицательной обратной связи БОС и питания БП.

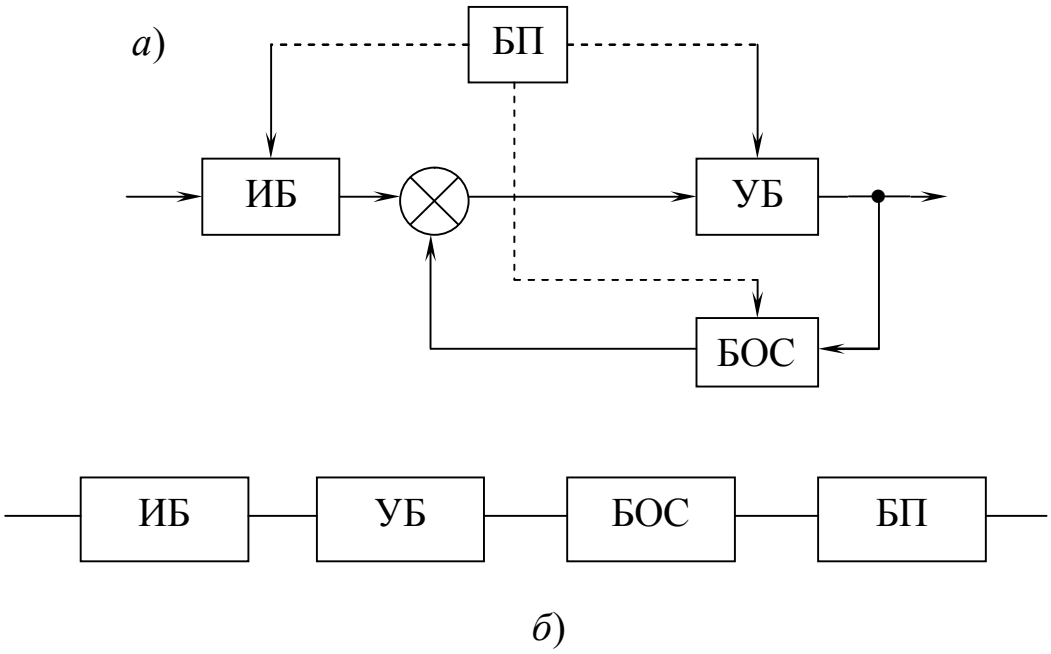


Рис.3.5. Функциональная (*а*) и структурная (*б*) схемы нормирующего показателя.

В настоящее время существует ряд руководящих технических материалов, регламентирующих аналитические методы расчета надежности комплекса технических средств АСУ ТП на этапе проектирования. Но при всем многообразии существующих методов расчета надежности систем последние можно разбить на три группы, относящиеся к системам:

- с простой структурой, сводящейся к последовательно–параллельному соединению элементов без учета их восстановления (оценка показателей безотказности);

- со сложной структурой, не сводящейся к последовательно–параллельному соединению элементов без учета их восстановления (оценка показателей безотказности);
- с восстанавливаемыми элементами как при нулевом, так и при конечном времени замены (восстановления) отказавшего элемента исправным (оценка показателей безотказности, ремонтопригодности и комплексных показателей).

Разновидности методов первых двух групп оперируют с количественными показателями безотказности при любых законах распределения наработки до отказа элементов. К числу этих методов относятся классический метод, базирующийся на основных понятиях и теоремах теории вероятности, и логико – вероятностный. Разновидности методов третьей группы определяются видом законов распределения наработки до отказа и восстановления, сложностью системы. К основным из них относятся методы переходных вероятностей и интенсивностей, использующие аппарат марковских процессов с дискретным и непрерывным временем, и метод, использующий аппарат полумарковских процессов.

С помощью выбранного метода, исходя из структурной схемы системы, определяют аналитические модели, связывающие ее показатели надежности с характеристиками элементов и процессов их обслуживания. Аналитические модели в виде формульных зависимостей, связывающих перечисленные величины и являющихся удобными для выполнения анализа надежности, удается получить для сравнительно простых систем при введении целого ряда упрощающих допущений в математическом описании характеристик систем и процессов. Для сложных восстанавливаемых систем, к числу которых относятся подсистемы АСУ ТП, показатели надежности часто определяются с использованием статистического (имитационного) моделирования.

Подбор характеристик надежности элементов структурной схемы систем сопряжен с трудностями, определяемыми рядом факторов. К их числу относится зависимость показателей надежности от условий эксплуатации, которые могут существенно различаться на разнородных видах производств, поэтому паспортные данные по надежности могут не соответствовать их фактическим значениям. По некоторым элементам, входящим в состав системы, эти показатели могут отсутствовать, например, по запорной арматуре, проводным и трубным линиям связи и др. По показателям ремонтопригодности устройств данные зачастую отсутствуют. В связи с этим, при подборе показателей надежности элементов систем приходится пользоваться данными по надежности других устройств, близких к ним по конст-

рукции.

Используя показатели надежности элементов, по полученным математическим моделям производят расчет показателей надежности систем, который может быть выполнен вручную или на ЭВМ с использованием соответствующих пакетов прикладных программ.

3.2.1 Методы расчета надежности невосстанавливаемых систем

При расчете вероятности безотказной работы, средней наработки до возникновения первого отказа элементы системы рассматриваются как невосстанавливаемые. В этом случае, если структура системы сводится к основному или резервному соединению элементов, при условии, что работа одного из параллельно соединенных элементов обеспечивает работоспособное состояние системы, показатели безотказности последней определяются по показателям безотказности элементов с использованием классического метода расчета надежности.

Поскольку при основном соединении элементов (см. рис. 3.3, *а)* работоспособное состояние системы имеет место при совпадении работоспособных состояний всех элементов, то вероятность этого состояния системы определяется произведением вероятностей работоспособных состояний всех элементов [1]. Если система состоит из n последовательно включенных элементов, то при вероятности безотказной работы каждого из элементов $p_i(t)$ вероятность безотказной работы системы

$$P_{\text{с}}(t) = p_1(t)p_2(t)...p_n(t) = \prod_{j=1}^{n} p_j(t) \; . \qquad (7.1)$$

При параллельном соединении элементов и при условии, что для работы системы достаточно работы одного из включенных параллельно элементов, отказ системы является совместным событием, имеющим место при отказе всех параллельно включенных элементов. Если параллельно включены m элементов (см. рис. 3.3, *б*) и вероятность отказа каждого $q_j(t)=1-p_j(t)$, то вероятность отказа этой системы

$$Q_{\text{р}}(t) = q_1(t)q_2(t)...q_m(t) = \prod_{j=1}^{m} q_j(t) \; . \qquad (7.2)$$

Если структурная схема надежности системы состоит из последовательно и параллельно соединенных элементов, то расчет ее надежности может быть произведен с использованием (7.1), (7.2). Так,

для системы, структурная схема надежности которой представлена на рис. 3.3, *в*, вероятность безотказной работы

$$P_{\text{с}}(t) = p_1(t)p_2(t)p_{3456}(t) = p_1(t)p_2(t)\{1-[1-p_3(t)p_4(t)]\times[1-p_5(t)p_6(t)]\}$$

Пример 7.1. Рассчитать с помощью (7.1) и (7.2) вероятности безотказной работы за 2000ч $P(2000)$ систем регулирования уровня, структурные схемы которых представлены на рис. 7.2, *б* и *в*, при последующих вероятностях безотказной работы элементов: $p_{F_{\text{п}}} = p_{F_{\text{в}}} = p_L =$ 0,94; $p_{\text{Зд}} = 0{,}99$; $p_{\text{Р}}=0{,}93$; $p_{\text{ИМ}} = 0{,}92$; $p_{\text{РО}} = 0{,}74$.

Решение. Вероятность безотказной работы системы в случае обязательной работы двух регулирующих органов (см. рис. 3.4, *б*) составит

$$P_{\text{с}}(2000) = 0{,}94^3 \cdot 0{,}99 \cdot 0{,}93 \cdot 0{,}92^2 \cdot 0{,}74^2 = 0{,}35 \ .$$

Если для работы системы достаточно работы одного регулирующего органа (см. рис. 3.4, *в*), то вероятность безотказной работы системы регулирования уровня

$$P_{\text{с}}(2000) = 0{,}94^3 \cdot 0{,}99 \cdot 0{,}93\left[1-(1-0{,}92\cdot 0{,}74)^2\right] = 0{,}69.$$

Таким образом, использование резерва по регулирующему органу с исполнительным механизмом, являющихся наименее надежными элементами системы, обеспечивает повышение вероятности ее безотказной работы за 2000 ч с 0,35 до 0,69.

Чтобы определить значение средней наработки системы до отказа и другие показатели надежности, требуется знать законы распределения времени безотказной работы элементов (наработки до отказа) системы. Поскольку на участке нормальной эксплуатации с удовлетворительной точностью в качестве закона распределения времени безотказной работы элементов может быть принят экспоненциальный, то при основном соединении элементов выражение (7.1) примет следующий вид:

$$P_{\text{с}}(t) = e^{-\lambda_1 t}e^{-\lambda_2 t}\ldots e^{-\lambda_n t} = e^{-\lambda_c t}, \qquad (7.3)$$

где $\lambda_{\text{с}} = \lambda_1 + \lambda_2 + \ldots + \lambda_n = \sum_{i=1}^{n}\lambda_i$.

Таким образом, при основном соединении элементов, имеющих экспоненциальный закон распределения времени безотказной работы, закон распределения времени безотказной работы системы также будет экспоненциальным. В соответствии с этим, согласно (2.21) – (2.24), имеем

$$F_{\text{c}}(t)=1-e^{-\lambda_{\text{c}}t};\;\; f_{\text{c}}(t)=\lambda_{\text{c}}e^{-\lambda_{\text{c}}t};\;\; \tau_{\text{c}}=1/\lambda_{\text{c}};\;\; \sigma_{\text{c}}=1/\lambda_{\text{c}}. \qquad (7.4)$$

При резервном соединении m элементов, имеющих экспоненциальный закон распределения времени безотказной работы, вероятность отказа группы параллельно включенных элементов имеет вид:

$$Q_{\text{p}}(t)=\left(1-e^{-\lambda_1 t}\right)\left(1-e^{-\lambda_2 t}\right)\ldots\left(1-e^{-\lambda_m t}\right)=\prod_{j=1}^{m}\left(1-e^{-\lambda_j t}\right). \qquad (7.5)$$

Если все элементы равнонадежны и $\lambda_1=\lambda_2=\lambda_m=\lambda_j=\lambda$, то

$$Q_{\text{p}}(t)=\left(1-e^{-\lambda t}\right)^m;\;\; P_{\text{p}}(t)=1-\left(1-e^{-\lambda t}\right)^m \;.$$

Таким образом, при резервном соединении элементов экспоненциальный закон распределения времени безотказной работы не сохраняется.

Рассмотренный метод расчета широко применяют для оценки надежности локальных систем и элементов, входящих в их состав. На стадии проектирования при известных интенсивностях отказов элементов оценивают вероятность безотказной работы системы и предусматривают мероприятия, направленные на ее повышение и заключающиеся в резервировании наименее надежных и наиболее ответственных элементов, облегчении условий эксплуатации, снижении уровня нагрузки и др.

Анализируют надежность на стадии проектирования обычно в несколько этапов. На первом этапе, проводимом на стадии составления технического задания на локальную систему или отдельное техническое средство, когда их структуры еще не определены, производится прикидочная оценка надежности. Она исходит из априорной информации о надежности близких по характеру систем и элементов, с помощью которых они могут быть реализованы. На втором этапе проводится ориентировочная оценка надежности. При этом известны структура системы и входящие в ее состав элементы, их показатели надежности, заданные при нормальных (номинальных) условиях эксплуатации. Окончательный расчет надежности технических средств, иногда называемый коэффициентным, проводит-

ся на стадии завершения технического проекта, когда проведена эксплуатация опытных образцов устройства и известны условия эксплуатации всех элементов. Последние определяются уровнем нагрузок, характером изменения таких влияющих величин, как температура окружающей и регулируемой среды, уровень вибрации, колебания напряжения питания и частоты, колебания влажности и др. Учет этих величин позволяет произвести коррекцию значений интенсивностей отказов элементов. Так, их работа при пониженных нагрузках приводит к снижению интенсивностей отказов.

Влияние отклонения этих величин на интенсивность отказов учитывают путем использования поправочных коэффициентов k_i

$$\lambda = \lambda_{\text{ном}} k_1 k_2 \ldots k_n ,$$

где $\lambda_{\text{ном}}$ – номинальное значение интенсивности отказов, соответствующее нормальным условиям эксплуатации; k_1, k_2, ..., k_{n} – поправочные коэффициенты, учитывающие отклонения влияющих величин от нормальных значений.

Следует отметить, что достоверные данные по поправочным коэффициентам известны только для радиоэлектронных элементов, что позволяет производить окончательный расчет структурной надежности устройств, включающих эти элементы. По общепромышленным средствам АСУ ТП эти данные в подавляющем большинстве случаев отсутствуют. Последнее в значительной мере определяется разнообразием условий эксплуатации устройств в различных отраслях промышленности и сложностью получения этих данных. Во многих случаях рассмотренный выше способ расчета надежности не может быть использован, так как не всегда схема надежности содержит последовательно-параллельное соединение элементов.

Существуют несколько разновидностей классического метода расчета надежности систем со сложной структурой, часть из которых будет рассмотрена ниже применительно к анализу надежности мостиковой схемы, изображенной на рис. 3.6 (эта схема не сводится к последовательно-параллельному соединению элементов). Для всех элементов схемы известны вероятности безотказной работы p_1, p_2, p_3, p_4, p_5 и соответствующие им вероятности отказа типа “обрыв” q_1, q_2, q_3, q_4, q_5. Необходимо определить вероятность наличия цепи между точками a и b схемы.

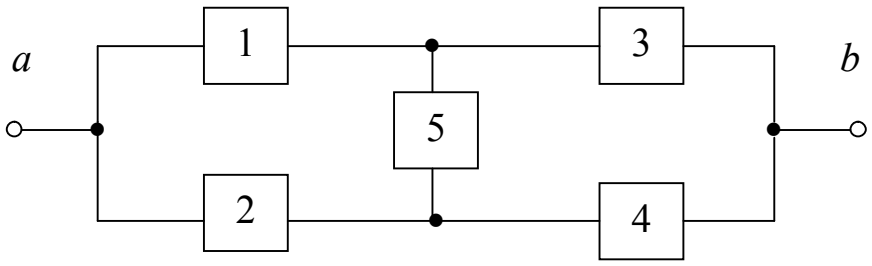


Рис. 3.6. Мостиковая схема соединения элементов

Следует отметить, что рассматриваемая схема является довольно распространенной не только в электротехнических устройствах, – например, к этой структуре сводится система регулирования мощности реактора, предусматривающая возможность перехода от одной неисправной цепи регулирования к другой, находящейся в резервном состоянии.

3.2.1.1 Метод перебора состояний

Расчету надежности любой системы независимо от используемого метода предшествует определение двух непересекающихся множеств состояний элементов, соответствующих работоспособному и неработоспособному состояниям системы. Каждое из этих состояний характеризуется набором элементов, находящихся в работоспособном и неработоспособном состояниях. Поскольку при независимых отказах вероятность каждого из состояний определяется произведением вероятностей нахождения элементов в соответствующих состояниях, то при числе состояний, равном m, вероятность работоспособного состояния системы

$$P = \sum_{j=1}^{m} \prod_{l_j} p_l \prod_{k_j} q_k , \qquad (7.6)$$

вероятность отказа

$$Q = 1 - \sum_{j=1}^{m} \prod_{l_j} p_l \prod_{k_j} q_k , \qquad (7.7)$$

где m – общее число работоспособных состояний, в каждом j-ом из которых число исправных элементов равно l_j, а вышедших из строя – k_j.

Расчет с использованием метода перебора состояний удобно представить в виде табл. 7.1, где знаком плюс отмечены работоспособные состояния, а знаком минус – неработоспособные.

Таблица 7.1 Расчет надёжности методом полного перебора

Номер состояния	Состояние элементов					Вероятность состояний
	1	2	3	4	5	
1	+	+	+	+	+	$p_1p_2p_3p_4p_5 = 0{,}9^5$
2	–	+	+	+	+	$p_2p_3p_4p_5q_1$
3	+	–	+	+	+	$p_1p_3p_4p_5q_2$
4	+	+	–	+	+	$p_1p_2p_4p_5q_3$ $= 0{,}1\cdot0{,}9^4$
5	+	+	+	–	+	$p_1p_2p_3p_5q_4$
6	+	+	+	+	–	$p_1p_2p_3p_4q_5$
7	–	+	–	+	+	$p_2p_4p_5q_1q_3$
8	–	+	+	–	+	$p_2p_3p_5q_1q_4$
9	–	+	+	+	–	$p_2p_3p_4q_1q_5$
10	+	–	–	+	+	$p_1p_4p_5q_2q_3$
11	+	–	+	–	+	$p_1p_3p_5q_2q_4$ $= 0{,}1^2\cdot0{,}9^3$
12	+	–	+	+	–	$p_1p_3p_4q_2q_5$
13	+	+	–	+	–	$p_1p_2p_4q_3q_5$
14	+	+	+	–	–	$p_1p_2p_3q_4q_5$
15	–	+	–	+	–	$p_2p_4q_1q_3q_5$ $= 0{,}1^3\cdot0{,}9^2$
16	+	–	+	–	–	$p_1p_3q_2q_4q_5$

В числовом примере все элементы приняты равнонадежными с вероятностью безотказной работы, равной 0,9, за заданное время:

$$P = \sum_{j=1}^{16} \prod_{l_j} p_l \prod_{k_j} q_k = p_5 + 5p^4q + 8p^3q^2 + 2p^2q^3 = 0{,}978.$$

Из рассмотренного примера видно, что даже при сравнительно простой структуре применение метода перебора состояний сопряжено с громоздкими выкладками.

3.2.1.2 Метод разложения относительно особого элемента

Этот метод основан на использовании формулы полной вероятности [1]. В сложной системе выделяется особый элемент, все возможные состояния H_i которого образуют полную группу $\sum_{i=1}^{n} P\{H_i\} = 1$. Если анализируемое состояние системы - *A,* то его вероятность

$$P\{A\} = \sum_{i=1}^{n} P\{H_i\} P\{A \mid H_i\} = \sum_{i=1}^{n} P_i\{A\} \ . \qquad (7.8)$$

Второй сомножитель в (7.8) определяет вероятность состояния *A* при условии, что особый элемент находится в состоянии H_i. Рассмотрение H_i-го состояния особого элемента как безусловного позволяет упростить структурную схему надежности и свести ее к последовательно-параллельному соединению элементов.

Так, в рассматриваемой мостиковой схеме выделение элемента *5* в качестве особого с двумя возможными состояниями (*1* – наличие и *2* – отсутствие цепи) $P\{H_1\}=p_5$; $P\{H_2\}=q_5$ позволяет от структурной схемы, представленной на рис. 3.6, перейти при безусловно исправном состоянии элемента *5* к схеме, представленной на рис.3.7, *а*. При отказе элемента *5* структурная схема имеет вид, представленный на рис. 3.7 *б*.

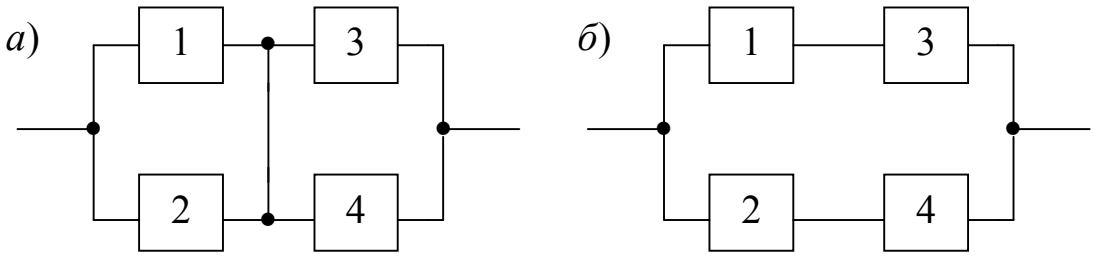


Рис. 3.7. **Структурные схемы мостикового соединения элементов, соответствующих наличию (*а*) цепи в элементе *5* и ее отсутствию (*б*)**

Если состояние *A* – наличие цепи между *a* и *b*, то в соответствии с (7.1) и (7.2) имеем

$$P_1\{A\} = p_5(1 - q_1 q_2)(1 - q_3 q_4) = 0{,}882 \,,$$

$$P_2\{A\} = q_5\left[1 - (1 - p_1 p_3)(1 - p_2 p_4)\right] = 0{,}0964 \,,$$

$$P\{A\} = P_1\{A\} + P_2\{A\} = p_5(1 - q_1 q_2)(1 - q_3 q_4) + \\ + q_5(p_1 p_3 + p_2 p_4 - p_1 p_2 p_3 p_4) = 0{,}978 \,.$$

Сопоставление обоих методов расчета надежности показывает, что выделение особого элемента с последующим анализом упрощенных структурных схем существенно сокращает выкладки.

Используя формулу полной вероятности и производя последовательное выделение особых элементов, можно проанализировать

сложные системы, имеющие перекрестные связи. Так, вероятность безотказной работы двойной мостиковой схемы (рис. 3.7)

$$
\begin{aligned}
P\{A\} = p_5\{&p_6(1-q_1q_2)(1-q_3q_4)(1-q_7q_8)+\\
&+q_6(1-q_1q_2)(p_3p_7+p_4p_8-p_3p_7p_4p_8)\}+\\
&+q_5\{p_6(p_1p_3+p_2p_4-p_1p_3p_2p_4)(1-q_7q_8)+\\
&+q_6(p_1p_3p_7+p_2p_4p_8-p_1p_3p_7p_2p_4p_8)\}.
\end{aligned}
$$

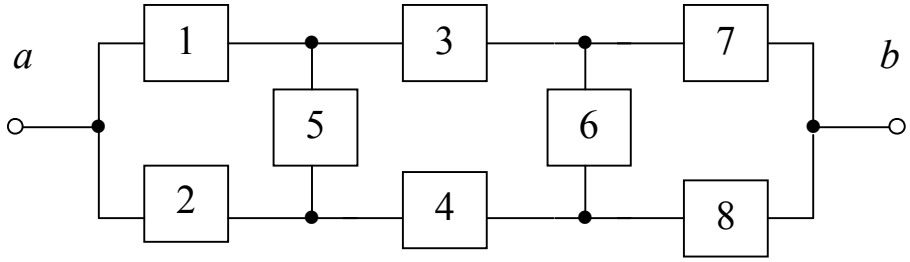


Рис. 3.7. **Двойная мостиковая схема соединения элементов**

3.2.1.3 Метод минимальных путей и сечений

В ряде случаев для анализа надежности сложной системы бывает достаточным определить граничные оценки надежности сверху и снизу.

При оценке вероятности безотказной работы сверху определяют минимальные наборы работоспособных элементов (путей), обеспечивающих работоспособное состояние системы. При формировании пути, считая, что все элементы находятся в неработоспособном состоянии, последовательным переводом элементов в работоспособное состояние производят подбор вариантов соединений элементов, обеспечивающих наличие цепи. Набор элементов образует минимальный путь, если исключение любого элемента из набора приводит к отказу пути. Из этого вытекает, что в пределах одного пути элементы находятся в основном соединении, а сами пути включаются параллельно. Так, для рассмотренной мостиковой схемы (см. рис. 3.6) набор минимальных путей представлен на рис. 3.8. Поскольку один и тот же элемент включается в два параллельных пути, то в результате расчета получается оценка безотказности сверху:

$$
\begin{aligned}
&P_{\text{в}} = 1 - Q_{13}Q_{24}Q_{154}Q_{253} = \\
&= 1 - (1-p_1p_3)(1-p_2p_4)(1-p_1p_5p_4)(1-p_2p_5p_3) = 0{,}997 .
\end{aligned}
$$

При определении минимальных сечений осуществляется подбор минимального числа элементов, перевод которых из работоспо-

собного состояния в неработоспособное вызывает отказ системы. При правильном подборе элементов сечения возвращение любого из элементов в работоспособное состояние восстанавливает работоспособное состояние системы. Поскольку отказ каждого из сечений вызывает отказ системы, то первые соединяются последовательно. В пределах каждого сечения элементы соединяются параллельно, так как для работы системы достаточно наличия работоспособного состояния любого из элементов сечения.

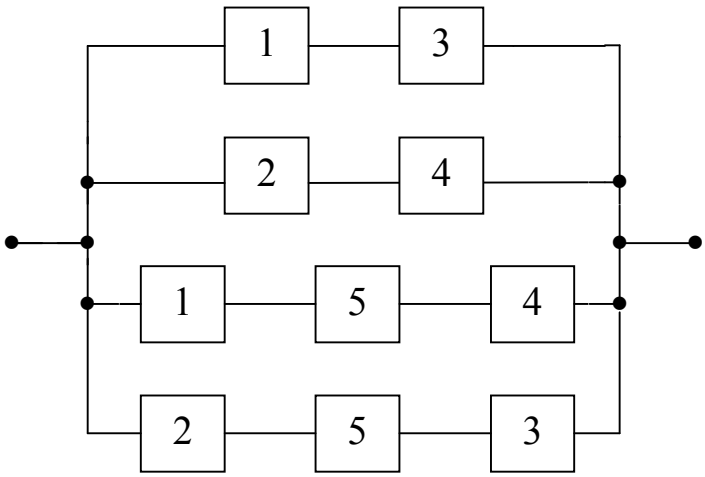


Рис. 3.8. Набор минимальных путей

Схема минимальных сечений для мостиковой схемы приведена на рис. 3.9.

Поскольку один и тот же элемент включается в два сечения, то полученная оценка является оценкой снизу

$$P_{\text{н}} = p_{12}p_{34}p_{154}p_{253} =$$
$$= (1-q_1q_2)(1-q_3q_4)(1-q_1q_5q_4)(1-q_2q_5q_3) = 0{,}978\,.$$

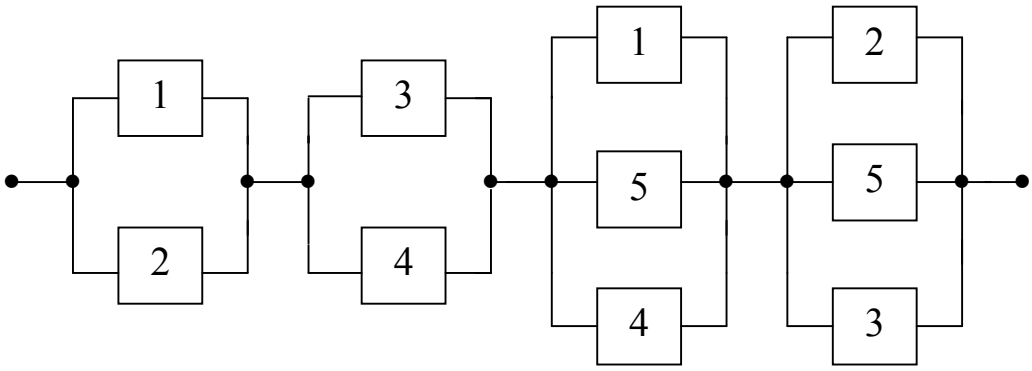


Рис. 3.9. Набор минимальных сечений

В рассматриваемом примере оценка безотказности снизу совпадает с фактической безотказностью, рассчитанной по первым двум методам.

Таким образом, при составлении минимальных путей и сечений любая система преобразуется в структуру с параллельно-последовательным или последовательно-параллельным соединением элементов.

3.2.3 Методы расчета надежности систем с резервированием

3.2.3.1 Виды резервирования

Для повышения надежности систем и элементов применяют резервирование, основанное на использовании того или иного вида избыточности. Последняя определяет следующие разновидности резервирования: функциональное, временное, информационное, структурное.

В том случае, если различные системы или устройства выполняют близкие функции, осуществляется функциональное резервирование. Такое резервирование часто применяют для многофункциональных систем. Так, значение температуры пара на выходе котлоагрегата может быть определено по показаниям потенциометра, осуществляющего в комплекте с термоэлектрическим преобразователем индивидуальный контроль ответственного параметра, и с помощью вызова этого параметра на электронно-лучевой индикатор информационно-измерительной системы, осуществляющей расчет технико-экономических и других показателей.

Временное резервирование заключается в том, что допускается перерыв функционирования системы или устройства из-за отказа элемента. Во многих случаях временное резервирование, обеспечивающее непрерывность технологического процесса, осуществляется за счет введения аккумулирующих емкостей, складов сырья и полуфабрикатов. Временное резервирование также может иметь место из-за аккумулирующей способности технологического объекта. Так, кратковременный перерыв в подаче топлива не приведет к прекращению генерации пара из-за аккумуляции теплоты поверхностями нагрева котлоагрегата.

Информационное резервирование связано с возможностью компенсации потери информации по одному каналу информацией по другому. На большинстве технологических объектов, бла-

годаря внутренним связям, имеет место информационная избыточность, которая часто используется для оценки достоверности информации. Так, усредненный расход пара на выходе котла соответствует усредненному расходу воды на его выходе, расход газа на котле определяет расход воздуха при фиксированном составе дымовых газов.

Для технологических систем наиболее характерно структурное резервирование. При использовании последнего повышение надежности достигается путем введения дополнительных элементов в структуру системы. Структурное резервирование разделяют на общее и поэлементное (раздельное). В первом случае система или устройство резервируются в целом, во втором резервируются отдельные элементы или их группы. Если резервные элементы функционируют наравне с основными, то имеет место постоянное резервирование, являющееся пассивным. Схемы общего (*а*) и поэлементного (*б*) постоянного резервирования приведены на рис. 3.9.

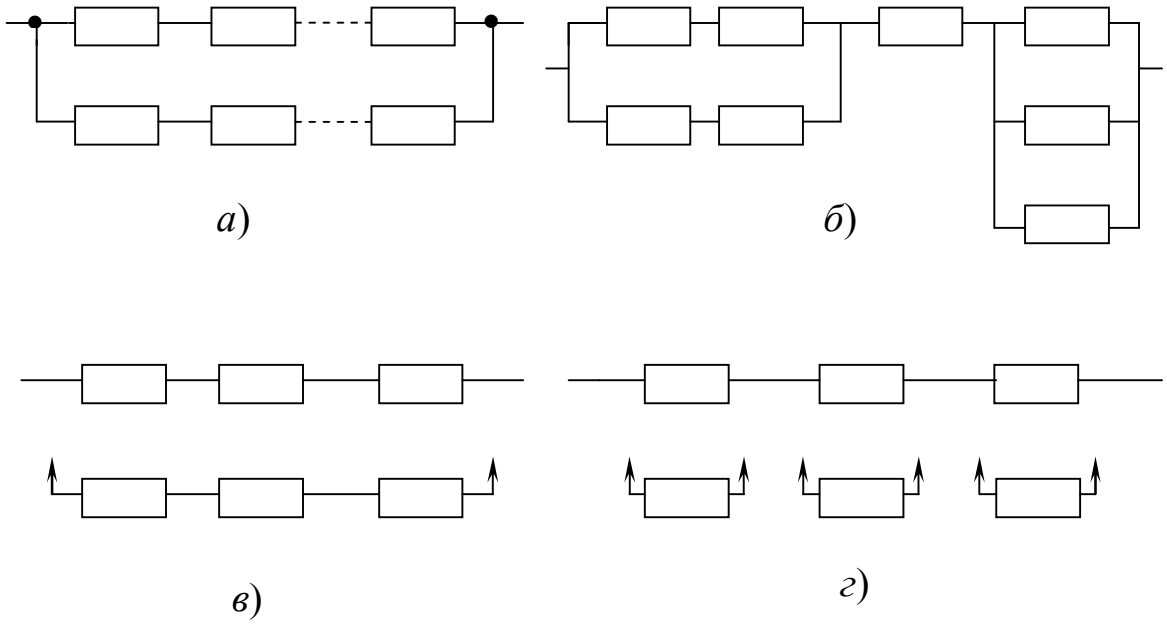


Рис. 3.9. Схемы постоянного резервирования и резервирования замещением

Если резерв вводится в состав системы после отказа основного элемента и сопровождается переключающими операциями, то имеет место резервирование замещением – активное резервирование.

При этом способе резервирования (рис. 3.9, *в* и *г*) резервные элементы могут находиться в нагруженном, облегченном и нена-

груженном состоянии. При нагруженном (горячем) резерве интенсивность отказов основного $\lambda_о$ и резервного $\lambda_н$ элементов одинакова, $\lambda_о = \lambda_н$. У облегченного (теплового) резерва интенсивность отказов резервных элементов $\lambda_{об}$ ниже, чем у основных работающих, $\lambda_о > \lambda_{об}$. При ненагруженном (холодном) резерве вероятностью отказов элементов в состоянии резерва пренебрегают, $\lambda_х = 0$.

При резервировании замещением один и тот же резерв может быть использован для замены любого из ряда однотипных элементов. Такой способ резервирования называют *скользящим* или с *неоднозначным соответствием*. В подсистемах АСУ ТП широко используются все рассмотренные способы резервирования. В технологических системах в основном применяют поэлементное (рис. 3.9, *г*) резервирование замещением с ненагруженным резервом. Отказавшие первичные и вторичные приборы, регулирующие блоки управления, датчики, исполнительные механизмы, заменяют исправными, хранящимися на складе. Поскольку замена регулирующего органа сопровождается, как правило, снижением производительности объекта или его остановом, то для регулирующих органов используют постоянное резервирование в сочетании с резервированием замещением. Так, регулирование подачи топлива и питательной воды в котлоагрегат осуществляется по нескольким ниткам. Нагруженный и облегченный резерв используют при резервировании элементов вычислительного комплекса (блоков питания, процессора и др.).

Для характеристики соотношения между общим числом однотипных элементов n и числом r необходимых для функционирования системы работающих элементов вводится понятие кратности резервирования

$$k = (n - r)/r, \qquad (8.1)$$

Значение k может быть целым, если $r = 1$, и дробным, если $r > 1$. В последнем случае дробь (8.1) нельзя сокращать. Скользящее резервирование является разновидностью резервирования с дробной кратностью.

Поскольку структурное резервирование сопряжено с дополнительными затратами на резервные элементы, то последние должны окупаться за счет повышения надежности системы и снижения потерь от ее отказов. Наиболее простыми для определения показателями эффективности резервирования являются следующие:

$$B_\tau = \tau_р / \tau; \quad B_р = P_р / P; \quad B_Q = Q / Q_р, \tag{8.2}$$

где B_τ – выигрыш за счет повышения средней наработки до отказа резервированной системы $\tau_р$ по сравнению с наработкой нерезервированной системы τ; $B_р$, B_Q – аналогичные показатели по повышению вероятности безотказной работы и снижению вероятности отказа. Резервирование эффективно, если значение показателей B_τ, $B_р$, B_Q больше единицы.

Поскольку технологические системы включают в свой состав элементы, имеющие различный вид резерва, то для расчета надежности систем необходимо рассмотреть методы расчета надежности систем при различных способах резервирования. Простейший вариант этой задачи – определение показателей безотказности систем, содержащих резервированные невосстанавливаемые элементы.

Методы расчета надежности невосстанавливаемых систем с постоянным резервом

Общее постоянное резервирование с целой кратностью

Вероятность отказа $Q_р$ параллельно работающих m элементов при r =1 определяется выражением (7.2), откуда для равнонадежных элементов

$$Q_р = q^m = q^{k+1}; \quad B_Q = q / q^m = 1 / q^k. \tag{8.3}$$

Чем меньше вероятность отказа каждого из элементов, тем выше эффективность постоянного резервирования. Так, если q = 0,1 и 0,01, а k = 1, то выигрыш в снижении вероятности отказа при резервировании составит соответственно 10 и 100. Рассмотрим связь показателей надежности группы резервированных элементов, кратности резервирования k и длительности работы элементов t при экспоненциальном законе распределения времени их безотказной работы. Если интенсивность отказов каждого из элементов λ, то согласно (3.12), (4.1), (4.2) имеем

$$Q_{\text{р}}(t) = F_{\text{р}}(t) = \left(1 - e^{-\lambda t}\right)^{k+1}; \quad P_{\text{р}}(t) = 1 - \left(1 - e^{-\lambda t}\right)^{k+1}; \qquad (8.4)$$

$$f_{\text{р}}(t) = (k+1)\lambda\left(1 - e^{-\lambda t}\right)^{k} e^{-\lambda t};$$

$$\lambda_{\text{р}}(t) = f_{\text{р}}(t) / P_{\text{р}}(t) = (k+1)\lambda\left(1 - e^{-\lambda t}\right)^{k} e^{-\lambda t} / \left[1 - \left(1 - e^{\lambda t}\right)^{k+1}\right];$$

$$\lim_{t \to 0} \lambda_{\text{р}}(t) = 0; \quad \lim_{t \to \infty} \lambda_{\text{р}}(t) = \lambda = 1/\tau.$$

Графики изменения $P_{\text{р}}$ (t/τ) и $\lambda_{\text{р}}(t/\tau)/\lambda$ в зависимости от кратности резервирования и длительности работы системы представлены на рис. 3.10. Они показывают, что постоянное резервирование эффективно на начальном участке работы системы, когда $t \le \tau$.

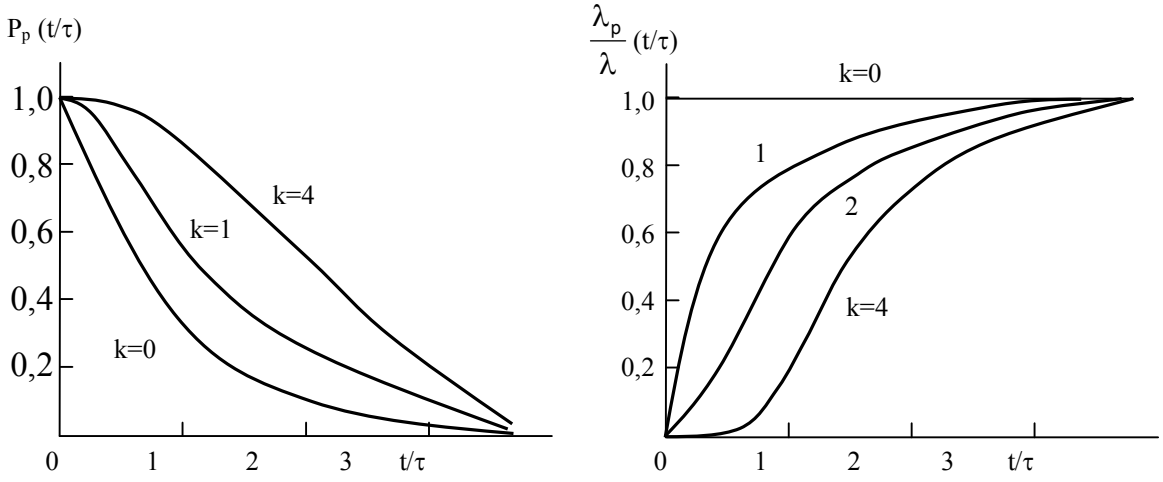


Рис. 3.10. Графики зависимости вероятности безотказной работы (*а*) и интенсивности отказов (*б*) от кратности резервирования

Для группы резервированных элементов средняя наработка до отказа

$$\tau_{\text{р}} = \int_0^{\infty} P_p(t)\,\mathrm{d}t = \int_0^{\infty} \left[1 - \left(1 - e^{-\lambda t}\right)^{k+1}\right] \mathrm{d}t.$$

Подставив $1 - e^{-\lambda t} = z$; $\mathrm{d}t = \mathrm{d}z / [\lambda(1 - z)]$, получим под знаком интеграла сумму первых k+1 членов убывающей геометрической прогрессии:

$$\tau_{\text{р}} = \frac{1}{\lambda}\int_0^1 \frac{1 - z^{k+1}}{1 - z}\,\mathrm{d}z = \frac{1}{\lambda}\int_0^1 \left(1 + z + z^2 + \ldots + z^k\right)\mathrm{d}z =$$

$$= \frac{1}{\lambda}\left(1+\frac{1}{2}+\frac{1}{3}+...+\frac{1}{k+1}\right) = \tau\sum_{i=1}^{k+1}\frac{1}{i}. \qquad (8.5)$$

Из последнего выражения видим, что выигрыш в средней наработке до отказа, полученный путем введения резервных элементов, снижается по мере увеличения кратности резервирования. Так, введение первого элемента приводит к увеличению средней наработки на 50%, второго – на 22%, третьего – на 13%.

Работа рассматриваемой группы резервированных элементов характеризуется последовательным переходом по мере возникновения отказов от m работающих элементов к $m-1$, $m-2$ и далее до одного, отказ последнего приводит к отказу всей группы. Эту последовательность переходов иллюстрирует график, представленный на рис. 3.11.

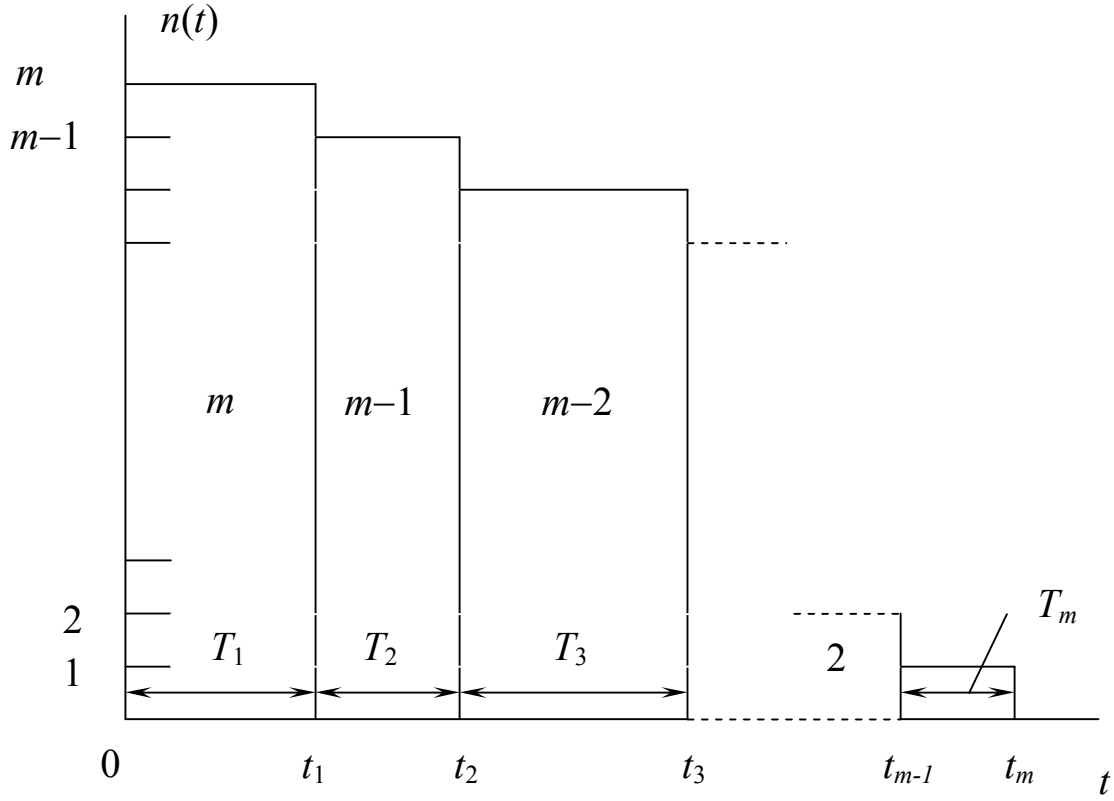


Рис. 3.11. Временная диаграмма изменения числа параллельно функционирующих устройств

В случайные моменты времени t_1, t_2 и т.д. происходят отказы элементов, число работающих элементов $n(t)$ постепенно снижается. Поскольку на каждом из участков $T_1=t_1$, $T_2= t_2-t_1$ и т.д. имеет место совместное функционирование m, $m-1$ и т.д. элементов, то случайные интервалы времени T_1, T_2, ..., T_m имеют

экспоненциальное распределение с интенсивностями отказов соответственно $m\lambda$, $(m-1)\lambda,\ldots,\lambda$ и средней продолжительностью $\tau_1=1/(m\lambda)$, $\tau_2=1/[(m-1)\lambda]$, …, $\tau_m=1/\lambda$. Поскольку $\tau_p=\tau_1+\tau_2+\ldots+\tau_m$, то значит средняя наработка до отказа группы резервированных элементов определяется как $\tau_p=1/(m\lambda)+1/[(m-1)\lambda]+\ldots+1/\lambda$, что совпадает с (8.5).

Резервирование двухполюсных элементов

В большинстве случаев резервные элементы подключают параллельно основному. Однако при дифференциации видов отказов резервирование по каждому из них может осуществляться при различных способах включения резервных элементов. Наиболее характерным в этом отношении является резервирование элементов при отказах типа «обрыв» и «короткое замыкание» (КЗ). Для двухполюсных элементов релейного типа, имеющих два возможных состояния 1 и 0, этим отказам соответствует несрабатывание при наличии управляющего сигнала или ложное срабатывание при отсутствии последнего.

При последовательном соединении релейных элементов (рис. 3.12, *а*) несрабатывание любого из элементов приводит к отсутствию цепи между точками *a* и *b*. Таким образом, для этого типа отказов последовательное соединение релейных элементов является основным. Для отказов типа ложное срабатывание последовательное соединение является резервным, поскольку этот вид отказа цепи будет иметь место только при отказе двух элементов.

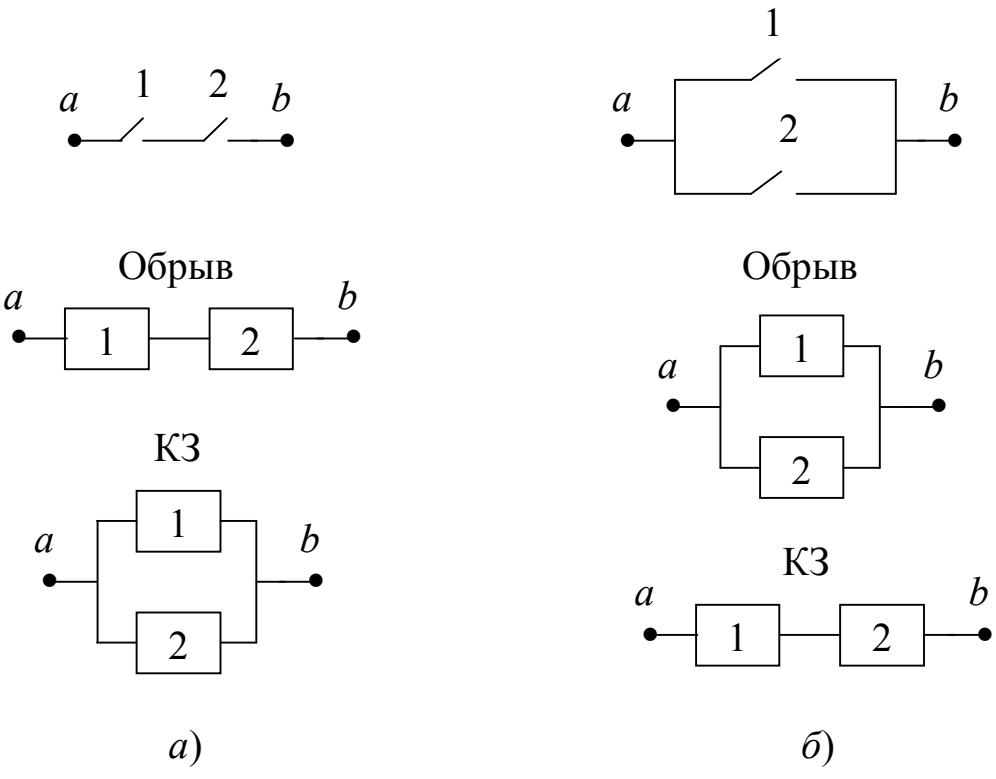


Рис. 3.12. Схемы последовательного (*а*) и параллельного (*б*) соединения релейных элементов и соответствующие им структурные схемы

Из рассмотренного вытекает, что одному и тому же соединению элементов для этих видов отказов соответствуют две структурные схемы. При последовательном соединении релейных элементов осуществляется резервирование по отказам типа КЗ. Если вероятность отказов этого типа для каждого элемента q, то $B_Q=q/q^2=q^{-1}$. Для отказов типа обрыв $B_Q=q/[1-(1-q)^2]=1/(2-q)<1$ т.е. последовательное включение релейных элементов приводит к повышению вероятности возникновения отказов типа *обрыв* цепи. При параллельном соединении релейных элементов (рис.3.12, *б*) осуществляется резервирование по отказам типа *обрыв* с эффективностью $B_Q=1/q$, а по отказам типа *КЗ* надежность снижается.

Резервирование с дробной кратностью

При резервировании с дробной кратностью система может функционировать если из n однотипных работающих параллельно элементов в работоспособном состоянии находятся r. Система отказывает, если число отказавших элементов z составляет $z \geq m=n-r+1$. Используя метод перебора состояний, определим вероятность отказа такой системы

$$Q = P\{z = m\} + P\{z = m+1\} + \ldots + P\{z = n\}.$$

В каждом из состояний число работоспособных элементов составляет $n–z$, а вероятность этого состояния $Q_z = C_n^z q^z (1-q)^{n-z}$, тогда

$$Q = \sum_{z=m}^{n} C_n^z q^z (1-q)^{n-z}, \qquad (8.6)$$

где $C_n^z = n!/[z!(n-z)!]$ – число сочетаний из n элементов по z, причем 0! =1; $C_n^0 = C_n^n = 1$. При $q<<1$ $Q \approx C_n^m q^m (1-q)^{n-m}$.

При экспоненциальном законе распределения времени безотказной работы и интенсивностях отказов λ каждого из элементов

$$Q(t) = \sum_{z=m}^{n} C_n^z \left(1 - e^{-\lambda t}\right)^z e^{-\lambda t (n-z)}. \qquad (8.7)$$

Поскольку без резерва система включает r работающих элементов, то вероятность отказа исходной системы при оценке эффективности резервирования составляет $1–(1–q)^r$. Так, если система включает три параллельно работающих элемента и r=2, то при q=0,1, k =1/2, m =2 согласно (8.6)

$$Q = C_3^2 q^2 (1-q) + C_3^3 q^3 = 3q^2 - 2q^3;$$

$$B_Q = \left[1 - (1-q)^2\right] / \left(3q^2 - 2q^3\right) = 6{,}8.$$

Резервирование с голосованием по большинству

Разновидностью постоянного резервирования с дробной кратностью является резервирование с голосованием по большинству (мажоритарное). Структурная схема системы, использующей этот способ резервирования, представлена на рис. 8.5. Параллельно работает нечетное число элементов, их выходные сигналы x_1, x_2, ..., x_n поступают на вход элемента голосования Г

(кворум-элемент), входной сигнал которого совпадает с сигналом большинства элементов. В системах с таким способом резервирования обычно используются три элемента, реже пять. Для работоспособного состояния системы необходима правильная работа большинства элементов. Отказ системы наступает при числе отказов $z \geq m = (n+1)/2$.

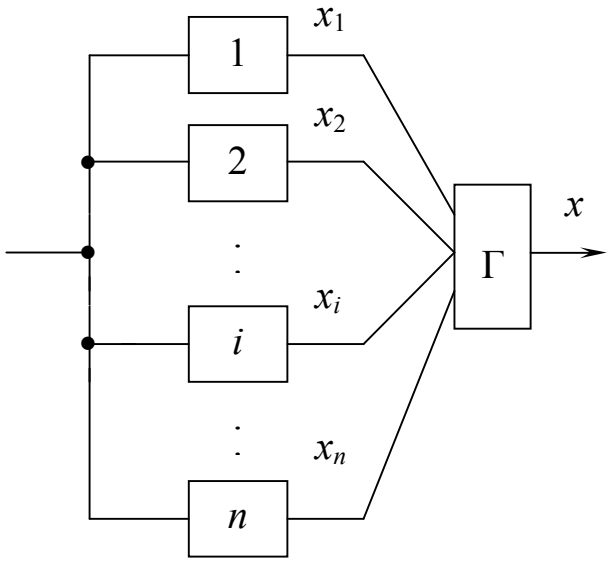


Рис. 3.13. Схема соединения элементов с голосованием по большинству

Вероятность отказа системы с мажоритарным резервированием при n=3 и n=5 равнонадежных элементах согласно (8.6) составляет соответственно:

$$Q_3 = 3q^2 - 2q^3; \quad Q_5 = 10q^3 - 15q^4 + 6q^5. \qquad (8.8)$$

Эффективность этого способа резервирования при n=3 составляет $B_Q = q/(3q^2-2q^3)=1/(3q-2q^2)$. Если $q < 0{,}5$, резервирование эффективно, при $q = 0{,}5$ надежность системы при резервировании не изменяется, а при $q > 0{,}5$ резервирование приводит к снижению надежности.

Мажоритарное резервирование широко применяют в системах защиты реакторов и теплотехнического оборудования. Так, система защиты от превышения давления в барабане котла, изображенная на рис. 8.6, *а*, включает электроконтактные манометры М1, М2, М3, силовое реле СР и электрический клапан сброса давления К. Система защиты срабатывает при замыкании контак-

тов любых двух манометров из трех. Схема соединения контактов манометров представлена на рис. 3.14, *б*. Ток через обмотку силового реле СР протекает при замыкании любых двух пар контактов, специального кворум-элемента в таких системах не требуется. Отказы вида "ложное срабатывание" или "несрабатывание" в системе возникают при соответствующих отказах двух манометров из трех, т.е. этот способ резервирования равнонадежен для обоих видов отказов. Легко заметить, что в рассматриваемой системе осуществляется логическое преобразование сигналов, изображенное на рис. 7.10. Выражение для вероятности безотказной работы системы (7.18), полученное с применением логико-вероятностных методов расчета надежности, соответствует выражению (8.8). Их совпадение определяется тем, что исправная и ложная работа системы симметрична по отношению к исправным и неработоспособным состояниям ее элементов.

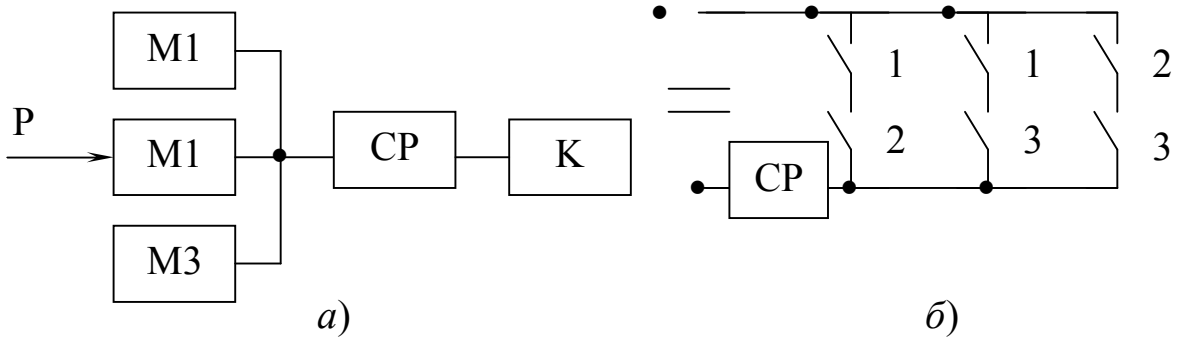


Рис. 3.14. **Схема защиты от превышения давления в барабане котла**

Поэлементное резервирование

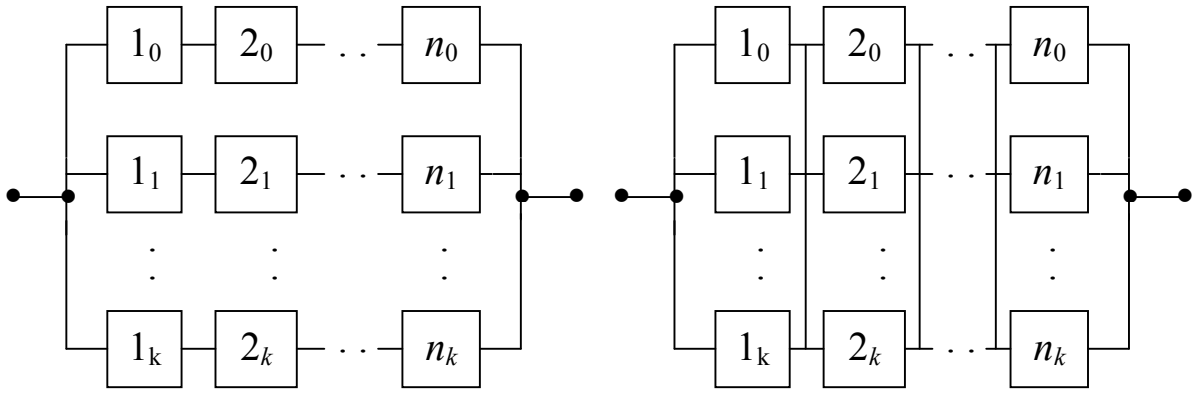
Надежность системы, содержащей группы элементов или отдельные элементы с поэлементным резервированием (см. рис. 8.1,*б*), рассчитывают с использованием формул общего постоянного резервирования (7.1), (7.2), (8.6). Так, если система состоит из n участков с поэлементным резервированием, целой кратностью k_i, то вероятность безотказной работы системы

$$P = \prod_{i=1}^{n} P_i = \prod_{i=1}^{n} \left(1 - \prod_{j=0}^{k_i} q_{ij} \right), \qquad (8.9)$$

где q_{ij} – вероятность отказа j-го элемента, входящего в i-й участок

резервирования.

Для сопоставления эффективности общего и поэлементного резервирования сравним вероятности отказа двух систем, включающих одинаковое $n(k+1)$ число равнонадежных элементов (рис. 3.15). В первом случае (рис. 3.15, *а*) осуществляется общее резерви- рование системы из n элементов кратностью k, во втором случае (рис. 3.15, *б*) при поэлементном резервировании каждый из n элементов системы имеет k резервных.



а) *б*)

Рис. 3.15. **Схема соединения элементов**

Вероятность отказа системы с общим резервированием

$$Q_{\text{о.р.}} = \left[1-(1-q)^n\right]^{k+1} .$$

Считая, что вероятность отказа каждого из элементов $q<<1$ и $(1-q)^n \approx 1-nq$, получаем $Q_{\text{о.р.}}=n^{k+1}q^{k+1}$. Для раздельного резервирования, используя (8.9) и считая $q<<1$, получаем

$$Q_{\text{пр}} = 1-\left(1-q^{k+1}\right)^n \approx nq^{k+1} .$$

Эффективность поэлементного резервирования по сравнению с общим $Q_{\text{о.р.}}/Q_{\text{пр}}$ составит n^k. С увеличением глубины n и кратности k резервирования его эффективность растет. Использование поэлементного резервирования сопряжено с введением дополнительных подключающих элементов, имеющих ограниченную надежность. В связи с этим имеется оптимальная глубина резервирования $n_{\text{опт}}$, при $n>n_{\text{опт}}$ эффективность резервирования

снижается.

3.3 Определение безопасности и ее значение в комплексной оценке надёжности технических систем и опасных производственных объектов

Свойство систем не допускать ситуаций, опасных для людей и окружающей среды называют безопасностью. Это свойство особо существенно для атомных станций. Согласно ГОСТ 26291-84 под *безопасностью атомной станции* понимают ее свойство с помощью технических средств и специальных организационных мероприятий исключать превышение установленных доз по внутреннему и внешнему облучению персонала и населения, а также превышение установленных норм содержания радиоактивных продуктов в окружающей среде. Вероятность отсутствия такого превышения является одним из показателей безопасности.

Отказы некоторых элементов АСУ ТП атомной станции (в первую очередь, так называемых управляющих систем безопасности, выполняющих функции автоматического включения и контроля устройств защитных, локализующих и обеспечивающих систем безопасности) могут приводить к нарушению безопасности. Поэтому к надежности АСУ ТП атомных станций предъявляют особо высокие как количественные, так и качественные требования, а пути обеспечения надежности и безопасности этих систем во многом совпадают. Примерами качественных требований являются наличие не менее двух независимых каналов, проверка и испытания элементов в процессе эксплуатации, наличие бесперебойного энергопитания и др.

Проблема надежности в АСУ ТП АЭС имеет особое значение, поэтому в заключение рассмотрим некоторые особенности обеспечения надежности АСУ ТП энергоблоков АЭС.

Пути обеспечения безопасности и надежности во многом совпадают, поэтому для подсистем и технических средств, которые относятся к группе "важных для безопасности", будем пользоваться нормативными документами по безопасности АЭС: "Общими положениями обеспечения безопасности атомных станций при проектировании, сооружении и эксплуатации (ОПБ-82)" и "Правилами ядерной безопасности атомных станций (ПБЯ 04-74)". Согласно ОПБ-82 важными для безопасности называют системы нормальной эксплуатации (предназначенные для осуществления нормальной эксплуатации, включая работу на заданных

уровнях мощности, процессы пуска и останова, техническое обслуживание, ремонты и перегрузку ядерного топлива), повреждения которых являются исходными событиями аварий, и системы безопасности (предназначенные для предупреждения аварий и ограничения их последствий). *Исходным событием* называют единичный отказ в системах, внешнее событие или ошибочное действие персонала, которое приводит к нарушению нормальной эксплуатации и может привести к нарушению пределов и (или) условий безопасности эксплуатации. Примером систем нормальной эксплуатации, важных для безопасности, являются системы автоматического регулирования мощности ядерного реактора; примером системы безопасности является управляющая система безопасности, которая выполняет функцию включения устройств защиты от аварий, локализации аварии и др.

К системам, важным для безопасности, предъявляется требование удовлетворения принципу единичного отказа. В соответствии с этим принципом система должна выполнять заданные функции при любом, требующем ее работы исходным событии и независимом от этого события отказе одного из элементов системы. Принцип единичного отказа является одним из проявлений отказоустойчивости системы – свойства системы функционировать при отказах элементов.

В последнее время свойство отказоустойчивости широко используют при разработке разнообразных элементов и средств вычислительной техники.

В отличие от безотказности отказоустойчивость (как и выполнение принципа единичного отказа) зависит только от структуры системы и не зависит от показателей надежности элементов, входящих в систему. Тем самым, при рассмотрении отказоустойчивости не существенны любые ошибки в определении показателей надежности элементов. Очевидно, что принципу единичного отказа не удовлетворяют системы без резервирования.

Определенные требования к надежности и безопасности согласно ПБЯ 04-74 предъявляют к системам управления и защиты реактора. Должна быть предусмотрена возможность останова реактора из другого помещения в случае нарушения доступа в помещение блочного щита управления (например, из-за пожара). Для измерения уровня мощности и скорости ее изменения должно быть как минимум по три независимых между собой канала. Для

аварийной защиты по этим параметрам, обеспечивающей гашение цепной реакции, также должно быть по три независимых канала (например, включенных по схеме "два из трех"), Автоматическое регулирование мощности должно быть реализовано не менее чем двумя независимыми автоматическими регуляторами с автоматическим переключением резерва.

Определенные требования к надежности и безопасности согласно ОПБ-82 предъявляют к управляющим системам безопасности. Для этих систем требуется наличие не менее двух независимых каналов. Кроме того, должна быть предусмотрена возможность ручного приведения в действие систем безопасности как с блочного щита управления, так и из другого помещения. Должны быть предусмотрены средства проверки работоспособности каналов и систем в целом в процессе эксплуатации: при неработоспособности на пульт управления должна быть передана информация об этом.

В качестве примера использования резервирования в АСУ ТП АЭС приведем надежностную схему простой функции индикации технологических параметров первой группы важности управляющей вычислительной системы "Комплекс – Титан 2" энергоблоков с реактором ВВЭР-1000 (рис. 3.16).

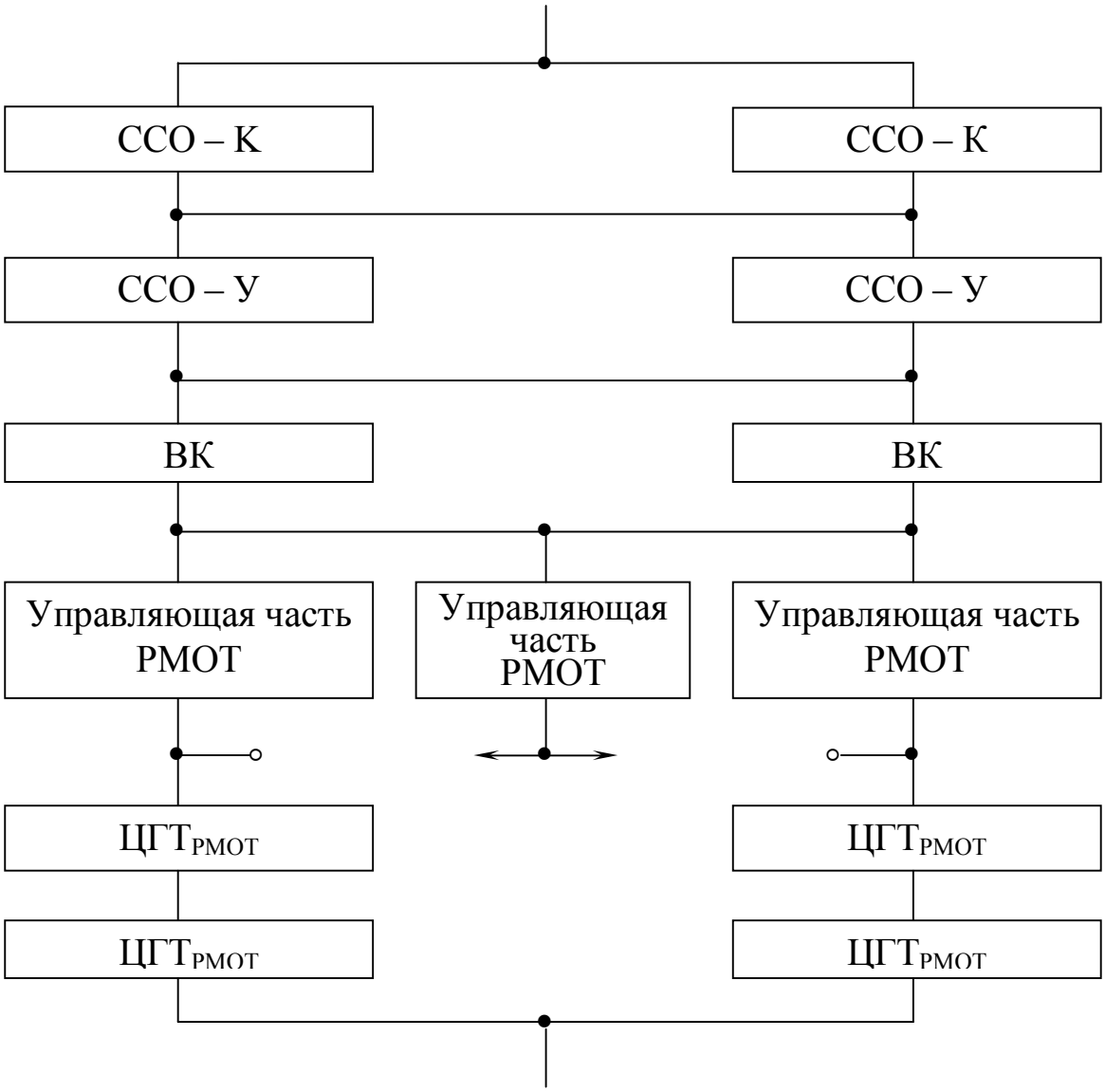


Рис. 3.16. **Надежностная схема простой функции индикации технологических параметров первой группы важности в управляющей вычислительной системе "Комплекс – Титан2" энергоблоков АЭС с реактором ВВЭР-1000**

Здесь предусмотрено: дублирование ввода и первичной обработки информации о параметрах и субкомплексах связи с объектом (ССО-К), децентрализация этих субкомплексов; дублирование концентратов информации – субкомплексов ССО-У; дублирование специализированных вычислительных комплексов (ВК) (причем каждый из них является двухпроцессорным); отображение информации с помощью двух рабочих мест оператора-технолога (РМОТ), каждый из которых включает по два цифровых графических терминала (ЦГТ); наличие еще одного РМОТ (без ЦГТ), осуществляющего скользящий резерв управляющих

частей двух первых РМОТ; децентрализация обработки информации (например, масштабирование и обнаружение отклонений аналоговых параметров выполняется в ССО-К, хранение и обработка изображений фрагментов мнемосхем – в РМОТ).

Необходимо отметить, что на АЭС надежность оперативного персонала играет особо существенную роль. Число вынужденных остановов ядерных реакторов по вине оперативного персонала составляет 25-30% их общего числа. Ошибки операторов стали причинами тяжелых аварий на втором энергоблоке АЭС "Три – Майл – Айленд" (США) в 1979 г. и на четвертом блоке Чернобыльской АЭС в 1986 году. Так, на Чернобыльской АЭС в процессе подготовки и проведения испытаний персонал отключил ряд технических средств защиты и нарушил важнейшие положения регламента эксплуатации по безопасности ведения технологического процесса. В частности, был нарушен режим эксплуатации: проведена блокировка защиты реактора по сигналу останова двух турбогенераторов и защит по уровню воды и давлению пара в барабане-сепараторе и отключена система аварийного охлаждения реактора. Авария привела к частичному разрушению активной зоны реактора, полному разрушению системы охлаждения и выбросу части накопившихся в активной зоне радиоактивных продуктов в атмосферу.

4. НОМЕНКЛАТУРА ОСНОВНЫХ ИСТОЧНИКОВ АВАРИЙ И КАТАСТРОФ. КЛАССИФИКАЦИЯ АВАРИЙ И КАТАСТРОФ. СТАТИСТИКА АВАРИЙ И КАТАСТРОФ

4.1 Определение аварий, инцидентов и чрезвычайных ситуаций

Чрезвычайное событие – происшествие, заключающееся в резком отклонении от норм протекающих процессов или явлений и оказывающее значительное отрицательное воздействие на жизнедеятельность человека, функционирование экономики, социальную сферу и природную среду.

Чрезвычайные условия – характерные черты общей обстановки, сложившейся в соответствующей зоне в результате чрезвычайного события и других факторов, в том числе местных особенностей.

Чрезвычайная ситуация – совокупность исключительных обстоятельств, сложившихся в соответствующей зоне в результате чрезвычайного события и других факторов, в том числе местных особенностей.

Обстановка в районе чрезвычайной ситуации – конкретная характеристика зоны, в которой сложилась чрезвычайная ситуация, выявленная на определенный момент времени и содержащая сведения о состоянии, последствиях, ресурсах и проведенных работах, а также данные о внешних условиях.

Авария – чрезвычайное событие, происходящее по техногенным причинам, а также из-за случайных внешних воздействий и заключающееся в повреждении, выходе из строя, разрушении технических устройств или сооружений.

Академик Легасов (1988) дал следующее определение аварии промышленного предприятия.

«*Авария промышленного предприятия* – процесс разрушительного высвобождения его собственного энергозапаса, при котором сырье, промежуточные продукты, продукция предприятия и отходы производства, установленное на промышленной площадке технологическое оборудование, вовлекаясь в аварийный процесс, создают поражающие факторы для населения, окружающей среды, самого предприятия и соседних промышленных объектов».

Крупная авария (катастрофа) – авария, повлекшая за собой многочисленные человеческие жертвы, значительный материальный ущерб и другие тяжелые последствия.

В. Маршалл приводит такое определение крупной аварии. *Крупная авария* – такая авария промышленного предприятия, при которой или погибло не менее определенного количества людей, или пострадало не менее определенного количества людей, или материальный ущерб превысил определенную сумму, или имело место некоторое сочетание этих обстоятельств. (В. Маршалл относит к крупным авариям те аварии, в которых погибло не менее 10 человек).

Авария и катастрофа, помимо причин и обычно длительности процесса, различаются главным образом количественно – по размеру ущерба.

Шкала теоретических ущербов приблизительно такова:

- глобальная катастрофа с разрушением условий жизни на Земле – сумма ущербов стремится к бесконечности, т.е. экономически бессмысленна, т.к. экономика имеет дело только с конечными величинами;
- крупнейшая социально-политическая катастрофа с глобальными последствиями (типа мировой войны) – порядка 10^{17} долл.;
- крупнейшая техногенная катастрофа типа чернобыльской –до $5 \cdot 10^{12}$ долл. (авария на АЭС «Три Майл Айленд» в США – до $2 \cdot 10^{10}$ долл. Аварии на АЭС имеют градации от 1-й до 7-й степени тяжести, чернобыльская – 7 баллов, на «Три Майл Айленд» – 5 баллов);
- крупномасштабная природно – антропогенная катастрофа типа аральской – до $5 \cdot 10^{12}$ долл.;
- крупнейшая природная катастрофа типа мощного землетрясения – до 10^{12} долл.;
- локальная социально-политическая катастрофа с экологическими последствиями – до 10^{12} долл.;
- крупная техногенная или природная катастрофа (авария) – до 10^{9} долл.;
- крупная техническая авария – до 10^{7} долл.;
- «рядовая» техническая авария – до 10^{6} долл.;
- мелкая техническая авария – до 10^{5} долл.

В расчетах экономическая оценка человеческой жизни рав-

на $2 \cdot 10^6$ долл., что примерно в 1,5 раза ниже максимально принимаемой в практике высокоразвитых стран.

Опасное природное явление – стихийное событие природного происхождения, которое по своей интенсивности, масштабу распространения и продолжительности может вызвать отрицательные последствия для жизнедеятельности людей и экономики.

Стихийное бедствие – катастрофическое природное явление, которое может вызвать многочисленные человеческие жертвы, значительный материальный ущерб и другие тяжелые последствия.

Экологическое бедствие – чрезвычайное событие, вызванное изменением под действием антропогенных факторов состояния суши, атмосферы, гидросферы и биосферы и заключающееся в проявлении резкого отрицательного влияния этих изменений на здоровье людей, их духовную сферу, экономику и генофонд.

Экологическая катастрофа – экологическое бедствие особо крупных масштабов, сопровождающееся необратимыми изменениями природной среды.

Чрезвычайная ситуация, как правило, именуется по лежащему в ее основе чрезвычайному событию. Чрезвычайные ситуации в своем развитии проходят пять условных фаз.

Фазы развития чрезвычайных ситуаций:

- первая – накопление отклонений от нормального состояния или процесса;
- вторая – инициирование чрезвычайного события (аварии или стихийного бедствия);
- третья – процесс чрезвычайного события (аварии или стихийного бедствия), во время которого оказывается воздействие на людей, объекты и природную среду. Третья фаза является следствием и развитием второй;
- четвертая – действие остаточных факторов поражения и сложившихся чрезвычайных условий;
- пятая – ликвидация последствий чрезвычайной ситуации.

Пятая фаза может по времени начинаться еще до завершения третьей фазы и совмещаться с четвертой. На основе фаз развития чрезвычайных ситуаций можно построить типовые модели их возникновения и развития.

Для практических целей общую классификацию чрезвычайных ситуаций целесообразно строить *по масштабу распространения* (рис.4.1) и *причине возникновения* (рис.4.2) лежащих в их основе чрезвычайных событий. Такая классификация является

наиболее общей, так как раскрывает сущность явлений, происходящих при чрезвычайных событиях.

Рис.4.1. **Классификация чрезвычайных ситуаций по масштабу их распространения**

Локальные чрезвычайные ситуации имеют последствия, не выходящие за пределы рабочего места, рабочего участка, усадьбы, квартиры.

При объектовых чрезвычайных ситуациях последствия ограничиваются пределами объекта народного хозяйства и могут быть устранены за счет его сил и ресурсов.

Местные чрезвычайные ситуации имеют масштаб распространения в пределах населенного пункта, крупного города, несколько районов или областей и могут быть устранены за счет сил и ресурсов области.

В региональных чрезвычайных ситуациях последствия ограничиваются пределами нескольких областей, автономной республики и могут быть ликвидированы за счет сил и ресурсов государства.

Национальные чрезвычайные ситуации имеют последствия, охватывающие несколько экономических районов или государств СНГ; ликвидируется чрезвычайная ситуация национального масштаба силами и ресурсами государства, зачастую с привлечением иностранной помощи.

При глобальной чрезвычайной ситуации ее последствия выходят за пределы страны и распространяются на другие государства. Эти последствия устраняются как силами каждого государства на своей территории, так и силами международного сообще-

ства.

Классификация чрезвычайных ситуаций по скорости распространения опасности

По скорости распространения опасности чрезвычайные ситуации могут быть:

- внезапные (взрывы, транспортные аварии, землетрясения и т.д.);
- с быстро распространяющейся опасностью (аварии с выбросом газообразных сильно действующих ядовитых веществ (СДЯВ), гидродинамические аварии с образованием волны прорыва, пожары и т.д.);
- с опасностью распространяющейся с умеренной скоростью (аварии с выбросом радиоактивных веществ, аварии на коммунальных системах, извержения вулканов, паводковые наводнения и т.д.);
- с медленно распространяющейся опасностью (аварии на промышленных очистных сооружениях, засухи, эпидемии, экологические опасные явления и т.д.).

4.2 Источники аварий на примере добычи твердых полезных ископаемых

До настоящего времени проблема безопасности труда в промышленности рассматривалась с точки зрения соответствия фактических данных нормативным. При этом в лучшем случае использовалась статистическая обработка ретроспективных данных об отказах оборудования, авариях и травмах на производстве. В такой методологической постановке безопасность труда являлась категорией слабоуправляемой.

В данной дисциплине на основе системно-динамических методов моделирования откликов производственной системы на управляющие воздействия предлагается прогнозировать целевую функцию безопасности в зависимости от различных видов рисков (травм, смертельных случаев профессиональных заболеваний и др.). В качестве целевой функции безопасности выбрана средняя ожидаемая продолжительность предстоящей трудовой деятельности (СОППТД) работников. В качестве управляющих воздействий используются организационно-методические, технические и другие решения, направленные на снижение различных видов риска.

Система управления безопасностью труда включает:

1. Базу данных, содержащую сведения об авариях, несчастных случаях, инцидентах технических систем, состоянии и износе оборудования, нарушениях требований нормативно-правовых документов, аттестации рабочих мест, обеспеченности средствами индивидуальной защиты персонала, укомплектованности штатов надзорных органов, уровне знаний по охране труда и др.

2. Комплекс методов моделирования откликов производственной системы на управляющие воздействия.

3. Методику и организацию обнаружения нарушений и отклонений от нормативных и установленных значений показателей, влияющих на безопасность труда (далее по тексту индикаторов опасности), включающих: классификацию несчастных травм, профзаболеваний; анализ причин их возникновения; анализ последствий аварийной ситуации и оценку безопасности труда по фактическим значениям индикаторов опасности.

4. Комплекс организационно-технических, методических и информационных решений для реализации эффективной стратегии управления безопасностью труда.

Как и во многих динамических задачах полезным и упрощающим дальнейший анализ является поиск квазистационарных параметров, определяющих математическую модель процесса. Так, в данном случае анализ массива несчастных случаев за последние годы в динамике с учетом классификации несчастных случаев со смертельным исходом на опасных производственных объектах РФ по техническим и организационным причинам позволил выявить некоторые закономерности, приведенные в таблице.

Причины и распределение несчастных случаев

Основные причины	Количество несчастных случаев, %
Травмирование в результате аварии	6,4
Нарушение технологии производства работ, неисправность или умышленное исключение технических устройств, в т.ч. приборов безопасности	28,2
Низкий уровень защиты исполнителей работ	10,2
Недисциплинированность, неосторожность, неправомочные действия исполнителей работ	22,9
Низкий уровень управления производством	28,3
Другие причины, не связанные с промышленной безопасностью (умышленные действия пострадавших, заболевания, не связанные с производством, алкогольное опьянение и др.)	3,9

Эти закономерности сводятся в частности к тому, что частая повторяемость однородных несчастных случаев связана не только с несовершенством технических устройств и приемами работ, которые, как правило, бывают малоизвестными и не отражаются в актах о несчастных случаях, и, следовательно, могут быть мало полезными уроками на будущее. Анализ причин несчастных случаев путем предлагаемой классификации, позволил выявить набор индикаторов опасности, указывающих на возможность возникновения внештатной ситуации и как, следствие, приводящих к несчастному случаю. На основе метода факторного анализа получен следующий набор факторов (индикаторов опасности): 1) уровень знаний по охране труда; 2) обеспеченность средствами индивидуальной защиты персонала; 3) доля неисправного оборудования в подразделении; 4) доля аттестованных рабочих мест в подразделении; 5) доля работающего не по специальности персонала; 6) укомплектованность штатов надзорных органов; 7) степень износа оборудования.

4.3 Классификация чрезвычайных ситуаций природного и техногенного характера

Аварии – это выход из строя машин, механизмов, устройств, коммуникаций, сооружений и их систем и т.п. вследствие нарушения технологии производства, правил эксплуатации, мер безопасности, ошибок, допущенных при проектировании, строительстве или изготовлении станков, агрегатов и т.д., низкой трудовой дисциплины.

Взрывы, и как их следствие, пожары происходят на объектах, производящих взрывоопасные и химические вещества; в системах и агрегатах, находящихся под большим давлением; на газо- и нефтепроводах и т.п. Наиболее взрывоопасные смеси с воздухом образуются при истечении газообразных и сжиженных углеводородных продуктов метана, пропана, бутана, этилена, пропилена, бутилена и др.

Пожары на предприятиях могут возникать также вследствие повреждения электропроводки и машин, находящихся под напряжением, топок и отопительных систем, емкостей с легковоспламеняющимися жидкостями, нарушений правил техники безопасности.

Аварии с истечением (выбросом) СДЯВ и заражением окружающей среды возникают на предприятиях химической, нефтеперерабатывающей, целлюлозно-бумажной, мясомолочной и пищевой промышленности, водопроводных и очистных сооружений, а также при транспортировке СДЯВ по железной дороге.

Непосредственными причинами являются: нарушение правил хранения и транспортировки, несоблюдение техники безопасности, выход из строя агрегатов, механизмов, трубопроводов, повреждение емкостей и т.п.

Рис.4.2. Классификация чрезвычайных ситуаций

4.4 Статистика аварий и катастроф

Бездумное наращивание энергетически направленных систем способно привести к катастрофическим последствиям.

Вот лишь несколько примеров из истории "катастроф века". Авария 1973 года в Чикаго, когда в результате взрывов и пожаров на заводе по выпуску типографской краски предприятие было полностью разрушено, погиб персонал. Авария 1976 года на химическом заводе в итальянском городе Севезо: из-за выброса диоксина была заражена огромная территория, в воздухе оказалось до 7 тысяч смертельных доз газа. Или более близкое событие – авария на хранилище сжиженных углеводородов в Мехико – 1984 год. От взрывов и пожаров тогда погибло более 500 человек, 7 тысяч получили ранения.

В нашей промышленности подобные по характеру и масштабам разрушения в разное время произошли на 15 предприятиях. За последние 18 лет случилось более 150 тяжелых аварий, каждая из которых в результате цепного развития могла приобрести катастрофические масштабы.

О многих из них общественность не была информирована. Людей, погибших на рабочем месте, хоронили украдкой, как какие-нибудь отходы производства. Но преданные гласности события последнего времени, прежде всего катастрофа в Башкирии, погубившая около тысячи человек, очевидно, дают нам основания не кивать на то, что происходит за рубежом, а получше разобраться в собственном хозяйстве.

В 1974 году в городе Фликсборо в Англии при аварийном выбросе на заводе фирмы «Нипро» произошел взрыв парового облака циклогексана. В итоге – человеческие жертвы, разрушение и повреждение тысяч домов в радиусе до 5 километров от предприятия. Эта авария прогремела тогда на весь мир и, кстати, тоже была занесена в разряд «катастроф века». Но что показательно. В том же году был подписан договор с англичанами и те же самые агрегаты с помощью инофирм были установлены на целом ряде отечественных предприятий!

Результат не замедлил сказаться. В 1978 году при схожих обстоятельствах взорвался агрегат в производственном объединении «Куйбышевазот» вызвав близкие по масштабам разруше-

ния. Сегодня в опасных условиях эксплуатируются аналогичные технологические блоки на других заводах.

1984 г., Индия, город Бхопал. В результате аварии на заводе американской фирмы «Юнион Карбайт» выброшено в атмосферу свыше 40 тонн метилизоцианата, отравлено свыше 60 тыс. человек, лечение одного пострадавшего обошлось фирме в среднем в 14 тыс. долларов.

Наиболее опасными по масштабам последствий являются аварии на атомных станциях (АС) с выбросом в атмосферу радиоактивных веществ (РВ), в результате чего, кроме разрушения энергоблоков, имеет место длительное радиоактивное загрязнение местности на огромных площадях.

Радиоактивное загрязнение местности в случае аварии на АЭС существенно отличается от радиоактивного заражения при ядерном взрыве по конфигурации следа, масштабам и степени заражения, дисперсному составу радиоактивных продуктов, а также своему поражающему действию. Это обусловлено в основном динамикой и изотопным составом радиоактивных выбросов, а также изменением метеорологических условий в период выбросов.

Особенности аварии на ЧАЭС

Авария произошла 26 апреля 1986 года в 01 час 23 мин.; на четвертом энергоблоке произошел взрыв реактора и частичное разрушение реакторного здания, возник пожар. Через проломы в здании было выброшено в атмосферу большое количество твердых материалов из активной зоны реактора. Цепная реакция прекратилась, но произошло расплавление тепловыделяющих сборок и всех элементов конструкции активной зоны. Образовался многокомпонентный расплав делящегося материала. Разрушенный реактор превратился в постоянно действующий источник поступления в атмосферу радиоактивных веществ, выделение которых прекратилось 6 мая 1986 г. Основная масса выброшенных радиоактивных веществ сосредоточилась около стен четвертого реактора и на территории АЭС.

После стабилизации радиационной обстановки к середине мая 1986 года территория вокруг ЧАЭС была разбита на три зоны: зону отчуждения, зону временного отселения и зону жесткого радиационного контроля соответственно с уровнями радиации 20, 5, 2 мР/ч. Эвакуировались более 116 тысяч человек. В результате аварии погиб 31 человек, 28 человек скончались от острой

лучевой болезни. В 1994 г. число жертв Чернобыльской катастрофы превысило 2000 человек.

Гидротехнические аварии

К основным гидротехническим сооружениям, разрушение (прорыв) которых приводит к гидродинамическим авариям, относятся плотины, водозаборные и водосборные сооружения (шлюзы).

Транспортные аварии

Причины аварий на транспорте весьма многообразны. Это может быть нарушение правил транспортировки взрывоопасных, ядовитых и горючих веществ, технические неисправности, низкая подготовка обслуживающего персонала и другие.

Взрыв железнодорожного грузового состава на станции Свердловск-сортировочный 4 октября 1988 г. (тротиловый эквивалент 104000 кг). Основная причина взрыва – халатность диспетчера. Погибло 6 человек, 1021 получили травмы, образовалась воронка глубиной 10 м и диаметром 50 м. Ориентировочный ущерб 236 млн.руб. в ценах 1991 г. (повреждено 642 дома и 72 подлежат сносу).

Взрыв грузового состава на станции Арзамас-1 4 июня 1988 г. (тротиловый эквивалент 117600 кг). Причина взрыва – нарушение правил погрузки и перевозки промышленных ВВ. Погиб 91 человек (12 детей), полностью разрушено 44 жилых дома. Ущерб превысил 120 млн. руб. в ценах 1991 г.

Хроника крупнейших морских катастроф XX века

15 апреля 1912 г. английский лайнер «Титаник» затонул после столкновения с айсбергом. Утонуло 1503 человека.

29 мая 1914 г. канадский пассажирский лайнер «Эмпресс оф айленд» столкнулся с норвежским судном «Сторстард». Погибло 1012 человек.

17 июля 1947 г. в Бенгальском заливе в шторм затонул индийский паром «Рандас». Утонуло 625 пассажиров и членов экипажа.

27 января 1949 г. в Тайваньском проливе столкнулись китайские пароходы «Тайпин» и «Цзинь-Юань». Погибло более 1500 человек.

11 октября 1968 г. у о.Минданао в шторм затонул филиппинский паром «Дамеджиет», который унес в пучину более 500

человек.

31 августа 1986 г. в результате столкновения на выходе из новороссийского порта затонул советский лайнер «Адмирал Нахимов». По официальным данным погибло 423 человека.

20 декабря 1987 г. филиппинский каботажный теплоход «Дона Бас» столкнулся с танкером «Вектор». Произошел пожар, в результате которого оба судна затонули и погибло около 3000 человек.

6 марта 1987 г. английский автопассажирский паром «Геральд оф зе фри Энтерпрайз» опрокинулся при выходе из бельгийского порта Зебрюгге. При этом погибло 193 человека. Причина трагедии – выход в море с приоткрытыми грузовыми воротами – вероятно, чтобы выветривались выхлопные газы с автомобильной палубы.

4.5 Экологические последствия аварий на опасных производствах и применения ядерного оружия

Стихийные бедствия: землетрясения, селевые потоки, оползни, тайфуны, наводнения и т.д. оказывают отрицательное влияние на экологию регионов, где они произошли. Разрушаются города и другие населенные пункты, гибнут леса, выходят их строя сельскохозяйственные угодья, а также гибнут люди и животный мир. Наносится большой материальный ущерб народному хозяйству.

Аварии и катастрофы на промышленных предприятиях, связанные с выбросом в атмосферу СДЯВ наносят большой вред окружающей среде. Образуются зоны заражения СДЯВ, происходит отравление сельскохозяйственных животных, заражаются водоемы, водные источники и т.д.

Большой ущерб наносится растительному миру, сельскохозяйственным угодьям и т.д.

Аварии на радиационно опасных объектах приводят к заражению радиоактивными веществами атмосферы, различных объектов народного хозяйства, растительности, почвы и т.д. При этом люди, животный мир, растения подвергаются облучению, которое вызывает у людей и животных лучевую болезнь. Для ликвидации последствий аварии требуются большие материальные затраты. Нарушается нормальная жизнедеятельность целых районов, областей при проведении эвакуационных мероприятий.

Как повлияет на экологию применение ядерного оружия?

На выставке в мемориальном Центре Мира в Хиросиме среди груд полуоплавленного металла, битого кирпича, обрывков горелой одежды лежит обугливший остов наручных часов. Стрелки на них исчезли, но остались их тени, навечно «впечатанные» в циферблат вспышкой взрыва, поразившего город. Эта картина – зловещее свидетельство: в 8 час. 15 мин. утра 6 августа 1945 г. внезапно оборвалась жизнь владельца этих часов, как и тысячи других жителей Хиросимы.

Бомбардировка Хиросимы, а затем Нагасаки дает нам единственную возможность непосредственно изучить последствия взрывов ядерного оружия в городах. Эти трагические события позволили получить разнообразную информацию о потенциальных физических и социальных последствиях ядерной войны.

В общей сложности сейчас в мире насчитывается около 50 тысяч единиц ядерных боеголовок. Что произойдет, если значительная часть их будет применена? Последствия будут принципиально иными, нежели в Хиросиме и Нагасаки.

Дым от гигантских пожаров, возникших в городах при ядерной бомбардировке, приведет к глобальным изменениям погоды и климата на Земле. Огромные пространства Земли на недели и месяцы охватят сумерки. Наиболее сложная обстановка сложится в Северном полушарии. Средняя температура может упасть на несколько градусов по шкале Цельсия. Во многих районах мира существенно уменьшится количество осадков. Значительные изменения температуры и количества осадков возможны также в тропических районах южного полушария.

Катастрофа не минует мировое сельское хозяйство и главные экосистемы: леса, степи, морские угодья. Популяции растений и животных окажутся в условиях быстрых и драматических изменений привычного климатического режима.

Урожай вряд ли придется собрать. Это неуклонно повлечет за собой глобальный продовольственный кризис как в воюющих, так и в нейтральных странах.

Среди других последствий можно назвать также: выход из строя систем энергоснабжения и связи, уменьшение толщины озонового слоя в верхних слоях атмосферы, защищающего жизнь на Земле от биологически опасного ультрафиолетового облучения, интенсивные радиоактивные осадки и долговременное глобальное радиоактивное загрязнение атмосферы, отравление воды и воздуха вследствие высвобождения большого количества ток-

сичных веществ и газов.

5. ПРИЧИНЫ АВАРИЙНОСТИ НА ПРОИЗВОДСТВЕ

5.1 Распределение причин возникновения аварийных ситуаций

Анализ массива несчастных случаев за последние годы в динамике с учетом классификации несчастных случаев со смертельным исходом на опасных производственных объектах РФ по техническим и организационным причинам позволил выявить некоторые закономерности, приведенные в таблице.

Причины и распределение несчастных случаев

Основные причины	Количество несчастных случаев, %
Травмирование в результате аварии	6,4
Нарушение технологии производства работ, неисправность или умышленное исключение технических устройств, в т.ч. приборов безопасности	28,2
Низкий уровень защиты исполнителей работ	10,2
Недисциплинированность, неосторожность, неправомочные действия исполнителей работ	22,9
Низкий уровень управления производством	28,3
Другие причины, не связанные с промышленной безопасностью (умышленные действия пострадавших, заболевания, не связанные с производством, алкогольное опьянение и др.)	3,9

Эти закономерности сводятся в частности к тому, что частая повторяемость однородных несчастных случаев связана не только с несовершенством технических устройств и приемами работ, которые, как правило, бывают малоизвестными и не отражаются в актах о несчастных случаях, и, следовательно, могут быть мало полезными уроками на будущее. Анализ причин несчастных случаев путем предлагаемой классификации, позволил выявить набор индикаторов опасности, указывающих на возможность возникновения внештатной ситуации и как, следствие, приводящих к несчастному случаю. На основе метода факторного анализа получен следующий набор факторов (индикаторов опасности): 1) уровень знаний по охране труда; 2) обеспеченность средствами индивидуальной защиты персонала; 3) доля неисправного оборудования в подразделении; 4) доля аттестованных ра-

бочих мест в подразделении; 5) доля работающего не по специальности персонала; 6) укомплектованность штатов надзорных органов; 7) степень износа оборудования.

Анализ причин и хода развития аварий и крупных катастроф позволил выделить общие стадии аварийного процесса, независимо от времени, типа производства и региона. Это стадия накопления дефектов или отклонений в регламенте процессов, которые сами по себе не представляют угрозы, но в сочетании с другими факторами приводят к катастрофе. На следующей стадии происходит инициирующее событие, когда уже не остается средств для эффективных действий. И, наконец, на третьей стадии происходит быстрое развитие событий, приводящее к катастрофе. События третьей стадии невозможны без накопления ошибок на первой стадии.

В общем случае обеспечение безопасности труда, несмотря на различие объектов и технологий, связано с решением трех задач. Во-первых, необходимо принять все возможные меры по предупреждению аварийности и травматизма. Однако даже при высокой надежности производств и машин, проектных решений и регламентах, способных обеспечить безопасную работу, из-за дефектов оборудования, нарушений регламента или человеческих ошибок, в работе возникают те или иные отклонения, которые можно рассматривать как инциденты или аварийные ситуации. Эти ситуации еще не ведут к катастрофическим последствиям, но требуют быстрых действий по их устранению. Это можно отнести ко второй задаче обеспечения промышленной безопасности. Для этого проектируются различные дублирующие системы и защитные устройства, системы обнаружения опасных веществ. Однако сами эти устройства и системы сложны, дороги и не безотказны. Поэтому эффективность действия таких систем в промышленности не всегда высока. Так в нашей стране не зарегистрировано ни одного случая тушения пожара резервуара с помощью системы автоматических установок пожаротушения, хотя до 20% общих затрат на резервуарные парки приходится на системы АУП. В то же время применение систем технической диагностики, исключающих развитие проектных и режимных аварийных ситуаций, необходимо в сложных уникальных системах, эксплуатация которых осуществляется на предельных параметрах и практически носит опытный или экспериментальный характер. В случае неэффективной работы защитных систем дело может дойти до катастрофы. В этом случае третья задача промышленной безопасности и охраны труда – спасение пострадавших и ликвидация последствий. Здесь вступают в действие различные спасательные службы – скорая помощь, горноспасатели, газоспасатели, пожарные, восстановительные поезда, спасатели МЧС и т.д. На данном этапе борьба идет за спасение конкретных пострадавших. Однако

на этой стадии эффективность действий совсем невелика. По данным МЧС, эффективность действий спасательных служб близка к максимальной и достичь большей защищенности на этом пути уже не удастся. Поэтому основным направлением обеспечения промышленной безопасности и охраны труда является предупреждение аварийности и травматизма. Именно на предупреждение аварий ориентирует в первую очередь закон «О промышленной безопасности опасных производственных объектов».

Для инспекторов Ростехнадзора России нарушения правил и норм промышленной безопасности и охраны труда, выявленные в ходе их надзорной и контрольной деятельности, являются указанием на возможность возникновения аварий и несчастных случаев на подконтрольных объектах. Так в течение года почти на 15 тысячах предприятий и организаций, имеющих более двух миллионов поднадзорных объектов и технических единиц, проводится более 30 тысяч обследований, в ходе которых выявляется более двух миллионов нарушений правил и норм. По результатам проверок и выявленных нарушений инспектора совместно с руководством обследуемых объектов принимают соответствующие меры по предотвращению возможных аварий и несчастных случаев. Принимаемые меры зависят от серьезности нарушений и степени опасности, вызываемой этими нарушениями. Инспектора имеют право дать предписание к устранению нарушений, предписание приостановить производства, объекты, работы (таких предписаний к приостановке продолжительностью более смены выдается более 100 тысяч в год). Более 100 тысяч работников привлекаются ежегодно к ответственности за нарушения правил и норм, из них до 10 тысяч освобождается или понижается в должности, более 20 тысяч подвергаются штрафным санкциям, сотни дел передаются в следственные органы. До 10 тысяч руководителей предприятий заслушиваются на советах региональных органов Ростехнадзора России. Инспектора принимают участие в проверке знаний требований правил и норм почти миллиона работников предприятий (порядка восьми процентов из них оказываются неподготовленными).

В качестве примера можно привести повышенное внимание Ростехнадзора России к положению в угольной промышленности, где многочисленные нарушения правил и норм прямо указывали на возможность катастроф. Обращает на себя внимание факт, что предпринятыми мерами удалось предупредить катастрофы на самых опасных шахтах (например, «Комсомольская»). Однако прогноз реализовался на других, относительно благополучных шахтах («Баренцбург», «Зыряновская», «Центральная»). Данный пример иллюстрирует соотношение между прогнозом и предупреждением аварий в деятельности Ростехнадзора России.

5.2 Основы математической статистики, используемые в процессе прогнозирования возникновения аварийной ситуации

Характерным примером ситуации, требующей прогнозных оценок, является продление ресурса безопасной эксплуатации потенциально опасных объектов. Для этих целей разработаны и утверждены специальные указания, регламентирующие порядок определения остаточного ресурса прогнозированием его технического состояния по определяющим параметрам до достижения предельного состояния. При этом в качестве основного показателя остаточного ресурса в результате прогноза должен определяться гамма-процентный ресурс, задаваемый двумя численными значениями: наработкой и выраженной в процентах вероятностью, того что в течение этой наработки предельное состояние не будет достигнуто.

Для такого разрушительного вида горных катастроф, как горный удар, прогноз предусматривает осуществление мероприятий, направленных на установление удароопасности месторождений, региональный прогноз удароопасности в пределах шахтного поля, прогноз степени удароопасности отдельных участков угольных пластов, рудного и породного массивов. С использованием методов прогноза определяют степень удароопасности отдельных участков горных выработок, основанных на относительной оценке напряженного состояния угля, руды или породы. После обнаружения службой прогноза опасных мест они приводятся в неопасное состояние имеющимися способами с оценкой эффективности этих работ теми же методами прогноза. Как видно, и здесь основное внимание уделяется не предсказанию времени проявления горных ударов, а выяснению места их возможного проявления и принятию превентивных мер с учетом воздействия на массив.

Методические указания по проведению анализа риска опасных промышленных объектов, которые регламентируют порядок оценки частоты и возможных последствий аварий на опасных производствах, также относятся к нормативным документам по прогнозированию. Однако и в этих методических указаниях основное внимание уделяется вопросам выявления (идентификации) и разработке мер, направленных на уменьшение риска.

Таким образом, в своей деятельности по профилактике аварийности и травматизма надзорные органы России используют методы прогнозирования аварийных ситуаций и осуществляют нормативное регулирование этой деятельности. Основными показателями возможности аварийной ситуации являются нарушения правил и норм, а методами предупреждения аварий – меры, принятые по выявленным на-

рушениям. Поэтому целевой функцией прогнозирования и предупреждения аварийности и травматизма является научно обоснованная система нормативных документов, регулирующих правовые, организационные, социально-экономические и технические аспекты безопасности производств, нарушения требований которых являются параметрами, определяющими приближение опасной ситуации.

Эмпирическим источником знаний о промышленной безопасности и охране труда служат прежде всего данные об аварийности и травматизме в стране и в мире, данные об отдельных авариях и катастрофах. В науке о промышленной безопасности и охране труда данные об авариях служат исходным материалом по всем вопросам. Как правило, аварии происходят неожиданно, информация об их причинах, ходе развития и даже последствиях специально не фиксируется и даже скрывается владельцами производств. Поэтому совершенствование системы расследования аварий, сбора данных по ним и их анализу является определяющей для создания базиса эмпирических сведений по промышленной безопасности и охране труда. Первым принципом, на котором строится методология прогнозирования и предупреждения аварийности и травматизма – создание эффективной системы расследования, сбора и анализа данных по аварийности и травматизму, обобщение данных по аварийности и травматизму за предыдущие годы. Анализ этих данных, особенно по причинам аварийности и травматизма, служит основой для совершенствования нормативно-технической документации и тем самым для предупреждения аварий, принятых проектных и конструктивных решений, а также разработки предложений для научных исследований.

Следующий шаг, который необходимо пройти на пути предупреждения аварий и катастроф – создание методов прогнозирования аварий и катастроф. Прогнозирование во времени является весьма сложной задачей. Как указывалось выше, прогнозирование, как правило, служит лишь промежуточной целью для предупреждения инцидентов. Для прогнозирования необходим анализ опасностей производств на основе не только данных о произошедших инцидентах, но и на основе моделирования аварийных процессов.

Для моделирования аварийных процессов необходимы знания о закономерностях и механизмах основных физико-химических процессов, происходящих во время аварий. К таким процессам, определяющим инициирование, развитие и исход аварии относятся горение и взрыв конденсированных и паро-воздушных сред, распространение опасных веществ в различных средах, разрушения различных объектов. Именно необходимость исследования механизмов и закономерностей таких процессов и является вторым принципом создания научно-методических основ прогнозирования аварийности и травматизма.

Результаты исследования имеющих отношение к авариям процессов используются при моделировании аварийных процессов и создании методов анализа опасностей. Моделирование аварийных процессов – третий принцип создания научно-методических основ предупреждения аварийности и травматизма.

Анализ опасностей промышленного объекта обычно строится на вероятностном подходе. И здесь встает проблема использования вероятностного подхода к анализу опасности и детерминированного подхода, который используется в нормативно-технической документации. В этом направлении используется метод категорирования производств и объектов по степени опасности, что является четвертым принципом, на которых основана методология предупреждения аварийности и травматизма. Категорирование опасных производств и объектов строится на основе выбора необходимых критериев риска, алгоритмов и методов категорирования взрыво- и токсически опасных объектов.

При разработке нормативно-технической документации и на стадии категорирования опасных объектов и производств как одной из промежуточных стадий нормирования необходимо учесть необходимость согласования отечественных и зарубежных норм и требований в связи со стремлением России стать членом Всемирной торговой организации. Учет международных норм и требований при разработке нормативной документации – пятый принцип, на котором строится методология прогнозирования и предупреждения аварийности и травматизма.

И, наконец, доведение всех научно-технических разработок до нормативных документов – шестой принцип создания научно-методических основ предупреждения аварийности и травматизма.

Несмотря на значительный резонанс, который вызывают в обществе крупные аварии и катастрофы, глубокого анализа положения с аварийностью и производственным травматизмом, как правило, не проводится и конкретные цели в этой области не ставятся.

Для формулировки целей и задач необходимо уяснить место аварийности и производственного травматизма в экономике страны и отдельных отраслей промышленности. Также необходимо определить место производственного травматизма в ряду других причин смерти и инвалидности, после чего определить допустимые уровни инцидентов и устанавливать цели. Для этого необходим тщательный и полный анализ и обобщение фактов. Такой подход совсем не противоречит принципиальной позиции Ростехнадзора России, рассматривающего аварийность и травматизм как недопустимые явления на каждом конкретном промышленном объекте.

Несчастные случаи являются одной из основных причин смерти населения трудоспособного возраста. Так, по данным Совета нацио-

нальной безопасности США для людей в возрасте до 38 лет несчастные случаи в ряду причин смерти стоят на первом месте. Всемирная организация здравоохранения собирает информацию о состоянии здоровья населения из 61 страны. По ее данным уровень смертности от несчастных случаев (количество несчастных случаев на 100000 населения в год) изменяется от 10,7 на острове Сан Томе и Принсипи у западного берега Африки до 81,2 в Венгрии. По данным Российского статистического ежегодника смертность от несчастных случаев в России составила в 1994 году 368,4 тысяч человек, а уровень смертности 251 превосходя в несколько раз (вплоть до порядка) аналогичные показатели других стран. В последующие годы уровень смертности от несчастных случаев в России снизился и в 1997 г. достиг значения 188.

Значительную долю смертности от несчастных случаев дает травматизм на рабочих местах. В табл. 1 приведены сведения о смертельном травматизме на рабочих местах из Годовой книги рабочей статистики Международной организации труда (МОТ), членами которой являются 70 стран.

Таблица 1 Смертельный травматизм на рабочих местах

Страна	*Год*	*Количество*	*Частота*	*База для расчета частоты*
Австрия	*1990*	*198*	*0,077*	1000 занятых
Бразилия	*1991*	*4523*	*0,200*	1000 застрахованных
Великобритания	*1990*	*339*	*0,015*	1000 занятых
Венгрия	*1991*	*362*	*0,183*	1000 занятых ручным трудом
Германия	*1990*	*2272*	*0,070*	1000 занятых
Гонконг	*1990*	*244*	*0,099*	1000 занятых
Греция	*1988*	*79*	*0,049*	1000 застрахованных
Дания	*1989*	*81*	*0,030*	1000 занятых
Египет	*1989*	*223*	*0,160*	1000 занятых
Испания	*1991*	*1360*	*0,132*	1000 застрахованных
Италия	*1988*	*1366*	*0,112*	1000 рабочих
Канада	*1990*	*809*	*0,078*	1000 занятых
Колумбия	*1990*	*352*	*0,013*	1000 застрахованных рабочих
Корея	*1991*	*2299*	*0,290*	1000 застрахованных
Мексика	*1989*	*993*	*0,160*	1000 застрахованных рабочих
Нидерланды	*1988*	*54*	*0,013*	1000 застрахованных рабочих
Новая Зеландия	*1990*	*84*	*0,057*	1000 занятых
Норвегия	*1991*	*58*	*0,030*	1000 занятых
Перу	*1990*	*780*	*0,050*	1000 застрахованных
Польша	*1991*	*800*	*0,065*	1000 занятых
Россия	*1994*	*6770*	*0,133*	1000 занятых
Сингапур	*1991*	*68*	*0,128*	1000 занятых ручным трудом
США (Совет национальной безопасности)	*1990*	*10100*	*0,090*	1000 рабочих
Филиппины	*1989*	*56*	*0,206*	1000 рабочих
Финляндия	*1990*	*74*	*0,035*	1000 занятых
Франция	*1989*	*1177*	*0,084*	1000 занятых
Чехословакия	*1991*	*467*	*0,063*	1000 занятых
Швейцария	*1989*	*141*	*0,042*	1000 подверженных риску рабочих
Швеция	*1990*	*117*	*0,038*	1000 рабочих
Южная Африка	*1988*	*1762*	*0,341*	1000 застрахованных
Япония	*1990*	*2550*	*0,020*	1000 рабочих

По данным МОТ ежегодно на производстве происходит примерно 140 миллионов случаев травмирования и погибает 180 тысяч человек. Эти данные следует рассматривать как ориентировочные из-за различий в системах государственной статистики разных стран, в частности относящихся к использованию различных показателей уровня травматизма.

Состояние производственного травматизма в России хотя и ус-

тупает развитым странам, однако не так сильно, как общие показатели по несчастным случаям, включающие несчастные случаи в быту. Это говорит об определенной защищенности работников в части техники безопасности по сравнению с трагическими цифрами смертности от несчастных случаев в быту. Динамика производственного травматизма представлена в табл. 2.

Таблица 2 Динамика производственного травматизма в России

Годы	Число н/с на производстве		Число н/с со смертельным исходом	
	всего, тыс.	на 1000 работающих	всего	на 1000 работающих
1975	689	10,8	11766	0,185
1980	570	8.4	12349	0,183
1985	456	6,5	9819	0,142
1990	432	6,6	8393	0,129
1991	406	6,5	8032	0,128
1992	364	6,2	7653	0,131
1993	343	6,3	7574	0,139
1994	330	5,9	6770	0,133
1995	271	5,5	6789	0,138
1996	213	6,1	5378	0,155
1997	185	5,8	4734	0,148
1998	159	5,3	4399	0,142

Видно, что с 1975 года наблюдается постоянное снижение числа пострадавших при несчастных случаях на производстве с временной утратой трудоспособности и со смертельным исходом. Что касается частоты несчастных случаев со смертельным исходом, то этот показатель подвержен значительным колебаниям – имеются достаточно длительные периоды его роста или снижения. Наименьшее его значение (0,128) было зафиксировано в 1991 году, к 1998 году оно выросло до 0,142. С учетом падения производства за этот период можно сделать вывод об ухудшении производственной безопасности.

Очевидно, что определение частоты травматизма позволяет проводить сравнение отдельных отраслей промышленности, производств и работ по уровню опасности, пока уровень травматизма сохраняет статистическую значимость. Однако для такого сравнения необходима отработанная система сбора и анализа данных по аварийности и травматизму.

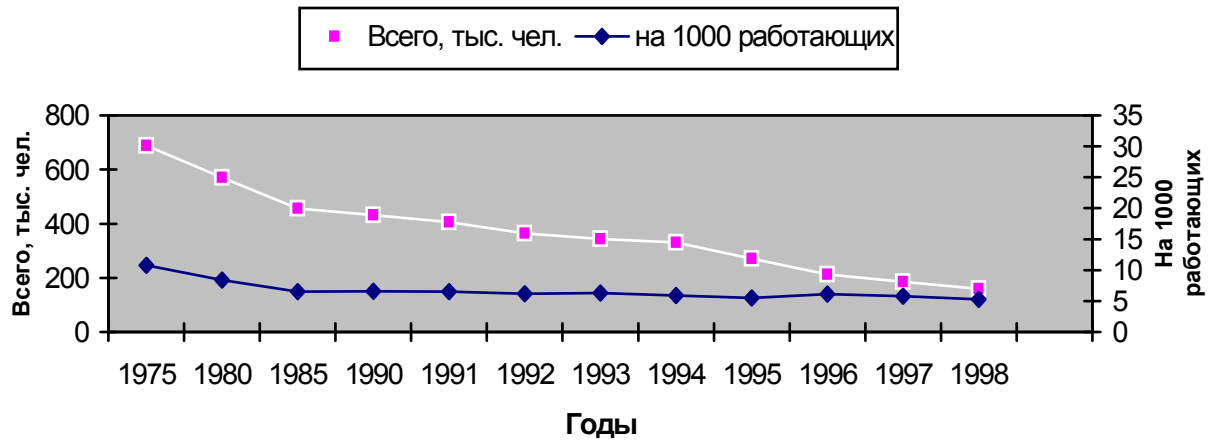


Рис. 5.1. Число пострадавших при несчастных случаях на производстве с утратой трудоспособности на 1 рабочий день и более со смертельным исходом

Потери рабочего времени по причине производственного травматизма по данным Российского статистического ежегодника 1995 года составили в России в 1993 году 8700000 человеко-дней. В США потери рабочего времени в 1992 году по причине производственного травматизма составляют 105000000 рабочих дней при сравнимом уровне травматизма, из них 65000000 рабочих дней за счет травматизма в текущем году и 40000000 рабочих дней за счет травматизма в прошедшем году. Более того, считается, что травматизм 1992 года привел к потере 110000000 рабочих дней в 1993 году.

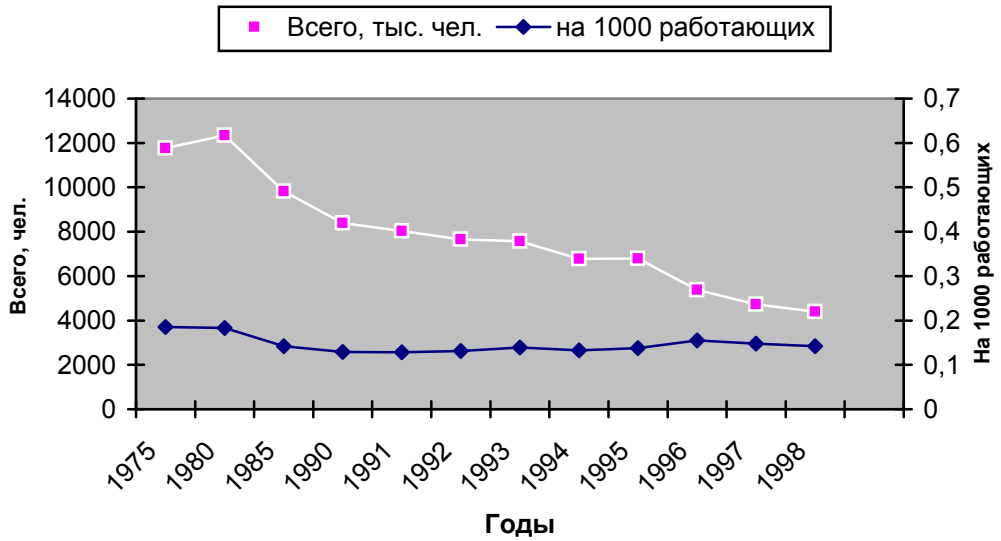


Рис. 5.2. Число пострадавших при несчастных случаях на производстве со смертельным исходом

Эти данные получены из расчета, что несчастный случай со смертельным исходом приводит к потере 150 рабочих дней в текущем году и 5850 рабочих дней в последующих годах, постоянная нетрудоспособность приводит к потере 150 и 565 рабочих дней в текущем и последующих годах, соответственно, а временная нетрудоспособность приводит к потере 17 рабочих дней только в текущем году.

6 ОСНОВЫ ТЕОРИИ РИСКА

6.1. Определение риска, его роль в оценке безопасности опасных объектов, производств и технологий

Термины, *надежность*, *безопасность*, *опасность* и *риск* часто смешивают, при этом их значения перекрываются. В этом курсе термины *анализ безопасности* или *анализ опасности* использованы как равнозначные понятия. Наряду с термином *анализ надежности* они относятся к исследованию как работоспособности, отказов оборудования, потери работоспособности, так и процесса их возникновения. Если в результате анализа требуется определить параметры, характеризующие безопасность, необходимо в дополнение к отказам оборудования и нарушениям работоспособности системы рассмотреть возможность повреждений самого оборудования или вызываемых ими других повреждений. Если на этой стадии анализа безопасности предполагается возможность отказов в системе, то проводится анализ риска для того, чтобы определить последствия отказов в смысле ущерба, наносимого оборудованию, и последствий для людей, находящихся вблизи него.

Примером изучения надежности может быть анализ того, насколько часто перегревается химический реактор из-за нарушений в работе насосов, теплообменников, системы управления и другого связанного с ним оборудования, а также ошибок человека оператора. Если задачу анализа расширить и включить в него оценку риска того, насколько часто изменение температуры приводит к взрыву, то здесь речь уже идет о проблеме безопасности (или опасности). Чтобы завершить изучение вопросов безопасности, необходимо проверить, перегревается ли химический реактор при отсутствии отказов оборудования или нарушений правил его эксплуатации, а также по другим причинам, не относящимся к его конструкции.

Если расширить анализ случаев взрыва химического реак-

тора, включив в него рассмотрение последствий ожидаемую частоту их появления, а также ущерб, вызываемый потерями оборудования и человеческими жертвами, то можно считать анализ риска выполненным. Например, последствиями взрыва из-за изменения температуры могут быть небольшие повреждения за счет разлетевшихся осколков или полная катастрофа вследствие пожара. Одной из целей анализа риска является оценка частоты (вероятности) этих или других возможных последствий из-за отказов в системе.

Конечным результатом изучения степени риска может быть, например, такое утверждение (одно или ряд утверждений): "Возможное число человеческих жертв в течение года в результате взрыва реактора равно 10^{-4}". Таким образом, на каждые 10 тыс. чел. работающих предсказывается гибель одного человека. С точки зрения общества в целом интересно сравнение полученной величины со степенью риска обычных условий человеческой жизни для того, чтобы получить представление о приемлемом уровне риска и иметь основу для принятия соответствующих решений.

Словарным значением слова риск является "*возможность* человеческих жертв и материальных потерь или травм и повреждений". Если бы словарь составлялся специалистом по надежности, данное значение звучало бы так: "*вероятность* человеческих и материальных потерь или повреждений". В технических терминах, например, риск любого человека из 200-миллионного населения США погибнуть в течение года в автомобильных катастрофах составляет

$$\frac{50\ \text{тыс.смертельных исходов в год}}{200\ \text{млн. людей}} = 2{,}5\times10^{-4}\ \frac{\text{смертельных исходов}}{\text{в год на каждого}}$$

т.к. суммарное годовое число смертельных случаев в автомобильных катастрофах в США равняется 50 тыс. Риск может иметь не смертельный исход, поэтому более общим выражением является

$$\text{риск}\left[\frac{\text{последствие}}{\text{время}}\right] = \text{частота}\left[\frac{\text{событие}}{\text{время}}\right]\text{величина}\left[\frac{\text{последствие}}{\text{событие}}\right].$$

Для примера с автомобильными авариями при общем числе аварий, равном в США 50 млн. в год, число катастроф (смертельных исходов/авария) равно 10^{-3}, так как

$$50000\,\frac{\text{смертельных исходов}}{\text{год}} = \left(50\times10^{6}\,\frac{\text{аварий}}{\text{год}}\right)\left(10^{-3}\,\frac{\text{смертей}}{\text{аварий}}\right).$$

Для общества риск понести материальные потери от автомобильных аварий можно выразить так:

$$\text{риск}\left[\frac{\text{потери}}{\text{время}}\right] = \text{частота}\left[\frac{\text{аварий}}{\text{время}}\right]\text{величина}\left[\frac{\text{потери}}{\text{аварий}}\right].$$

Вероятностная величина, равная $2{,}5\cdot10^{-4}$ смертельных исходов на человека в год, означает, что если бы жители США имели равную вероятность погибнуть в автомобильных катастрофах и если бы не было других причин смерти, то все население страны погибло бы в автомобильных катастрофах в течение 4 тыс. лет. Только то, что мы имеем дело с данными большого масштаба, придает смысл сделанным выводам. Любой отдельно взятый водитель мог бы сказать так: "Для меня все это не имеет смысла. Я могу погибнуть в катастрофе завтра". И он будет прав.

При применении данного вероятностного критерия к оценке риска погибнуть, например, в железнодорожной катастрофе имеется существенная разница между тем, относится ли риск, например в 0,1 фатального исхода в год, к 100 погибшим в одной катастрофе за 1000 лет или к гибели одного человека в течение каждых десяти лет. В целом, общественность мало обращает внимание на аварии с единичными жертвами, однако всегда бурно реагирует даже на потенциально опасные объекты, в катастрофах на которых могут погибнуть сотни людей.

Подход к анализу риска, описанный в последующих параграфах, построен на классическом принципе определения относительных частот событий при длительных испытаниях. Однако, если анализ риска, связанный с еще не построенным атомным реактором, дает величину, равную 10^{-6} жертв в год, можно утверждать, что здесь речь идет не об относительных частотах при длительных испытаниях, а о "редких событиях", к которым классический вероятностный подход, основанный на статистических выводах, не может быть применен. Здесь уместно напомнить о традиционном примере с ученым-статистиком, который утонул в ручье, имевшем среднюю глубину в пять сантиметров.

Альтернативный подход к проблеме "редких явлений" основывается на субъективистской логике. Такой подход отвергает по-

нятие об истинной вероятности и основывается на идее представления вероятности как меры субъективных мнений и убеждений. Методы обращения убеждений и мнений в критерий риска включают не тривиальную и подчас противоречивую операцию определения вероятности с использованием опроса экспертов в сочетании с теоремой Бейеса.

6.2 Методы качественной оценки риска, методы количественной оценки риска

Современный уровень знаний в области анализа риска и инструментарий, которым пользуются различные государства, для обеспечения безопасности населения, подтверждают переход от теории "абсолютной безопасности" к концепции приемлемого по экономическим, технологическим и социальным соображениям риска.

Концепция приемлемого риска позволяет:

1) сформулировать цели безопасности, которые органично вписываются в иерархическую систему целей развития общества (в качестве сценария развития общества в работе рассматривается стратегия перехода к устойчивому развитию, провозглашенная в ряде международных и национальных программ и документов);

2) разработать методологию достижения целей безопасности (цели безопасности формулируются количественно и формируются критерии, позволяющие определить степень достижения этих целей);

3) определить процесс управления риском в социо-эколого-экономической системе как целенаправленное воздействие на управляющие параметры для достижения оптимальной траектории развития системы.

Рассматривается модель "объект-среда", где в качестве "объекта" могут выступать: население региона, предприятия, важные сооружения и т.п., а "среда" характеризуется рисками (преждевременной смерти, уничтожения материальных ценностей, непоправимых нарушений в окружающей среде и др.) различной природы: техногенными, социально-экономическими и др.

В качестве целевой функции безопасности может быть выбрана, например, средняя продолжительность времени функционирования "объекта" F (например, жизни населения региона). В качестве управляющих воздействий используются ресурсы

(например, денежные средства), направляемые в снижение различных видов риска для членов общества.

Возникает проблема оценки влияния вкладываемых ресурсов в снижение рисков на продолжительность времени функционирования объекта.

В общем виде функцию безопасности F можно выразить следующим образом

$$F = F\{R_1(x_1), R_2(x_2), ..., R_n(x_n)\},$$

где R_i – риск i-й природы;

x_i – ресурсы, вкладываемые для снижения риска i-й природы.

Представим систему "среда", состоящей из двух взаимодействующих подсистем: "среда" до внедрения рассматриваемой технологии (например, транспортировки взрывоопасной продукции) и сама эта деятельность. Тогда, если предположить, что каждая из подсистем представляет собой относительно устойчивое целое за счет преобладания внутренних связей элементов над внешними, все риски можно разбить на обобщенный риск системы $R_с$ и риск рассматриваемой технологии $R_т$.

Введем следующую характеристику (параметр) "объекта": $C_с$ – стоимость продления времени функционирования "объекта" в системе.

Другими словами: $C_с$ – прирост годового дохода, в связи с увеличением на один год средней продолжительности времени функционирования "объекта" в системе. Введение указанной характеристики позволяет оценить влияние рассматриваемой технологии на безопасность, оценив ее вклад в доход системы (например, в валовой национальный продукт).

В соответствии с универсальным законом уменьшения эффективности экономической отдачи $C_с$ растет по мере развития системы. Если предположить ограниченность ресурсов системы ($x_с + x_т$ = const) и аддитивность рассматриваемых рисков: $F(R_с, R_т) = F(R_с + R_т)$ и $R_с << 1$, $R_т << 1$, – то можно определить предельные затраты на снижение полного риска в системе.

Для аналитической функции $F(R_с, R_т)$:

$$F = \int_{T_1}^{T_2} t \cdot R(t) \cdot e^{\int_0^t R(\tau)\mathrm{d}\tau} \mathrm{d}t,$$

где $R(t)$ – полный риск (например, летальный исход на t-м году жизни, а интегрирование проводится по всей жизни родившегося

поколения от T_1 до T_2), справедливо разложение:

$$dF = \frac{\partial F}{\partial R} dx_{\text{с}} \left(\frac{\partial R_{\text{с}}}{\partial x_{\text{с}}} - \frac{\partial R_{\text{т}}}{\partial x_{\text{т}}} \right).$$

Так как $\frac{\partial R_{\text{с}}}{\partial x_{\text{с}}} = -C_{\text{с}}^{-1}$ получаем следующее необходимое условие максимума функции F:

$$\text{d}F = 0, \text{ если } \frac{\partial R_{\text{т}}}{\partial x_{\text{т}}} = -C_{\text{с}}^{-1},$$

т.е. предельные затраты на снижение риска должны быть равны стоимости продления времени функционирования объекта в системе (принцип предельных затрат).

Достаточным условием максимума функции безопасности является выпуклость “эластичностей” всех рисков:

$$\frac{d^2 R_{\text{с}}}{dx_{\text{с}}^2} > 0, \frac{d^2 R_{\text{т}}}{dx_{\text{т}}^2} > 0.$$

Необходимое условие максимума функции F связывает стоимость единицы риска с уровнем технологического, экономического и социального развития “объекта” и позволяет оценить насколько затраты на снижение различных рисков далеки от оптимальных.

Если к $R(t)$ в выражении для аналитической функции F добавить “маленький” риск от рассматриваемой технологии ($R_{\text{т}} << R_{\text{с}}$), то можно получить линейный по риску вклад данной технологии в сокращение продолжительности функционирования системы.

Так как в общем случае стоимость единицы риска для субъектов, участвующих в реализации некоторой технологии, разная, то возникает проблема оптимального управления рисками. Решению этой проблемы отвечает справедливость утверждения о том, что при отсутствии у субъектов связей иерархического характера (т.е. прямой подчиненности) существует эффективное (неулучшаемое) кооперативное соглашение, которое является следствием принципа предельных затрат, сформулированного выше.

Действительно, рассмотрим два субъекта, различающиеся по уровню развития технологии и экономики и, следовательно, по уровню безопасности. Пусть оба субъекта управляют своими рисками наиболее эффективным образом, т.е. в соответствии с

принципом предельных затрат. При этом каждый субъект достигает максимально возможного для него уровня безопасности. Рассмотрим ситуацию, когда первый субъект начинает чувствовать риск второго, связанный с внедрением последним новой технологии. Для первого субъекта встает вопрос: должен ли он вкладывать свои ресурсы в источник опасности, порожденный вторым субъектом? Представим полный риск первого субъекта в виде суммы двух слагаемых: $R_1(A)$, который зависит только от его ресурсов A и R_{12}, в снижение которого он не вкладывает пока средств. Допустим, что небольшая доля ресурсов dx первого субъекта будет вложена в риск, порожденный технологией второго субъекта. Тогда вариация его полного риска составит:

$$\delta R = \left(\frac{\mathrm{d}R_1}{\mathrm{d}x_{x=A}} - \frac{\mathrm{d}R_{12}}{\mathrm{d}x_{x=0}} \right) \delta x .$$

Если $\delta R<0$, тогда вкладывание ресурсов в источник риска второго субъекта является оправданным (даже при условии, когда второму субъекту не выгодно вкладывать ресурсы в снижение риска, например, он беднее субъекта первого).

В силу закона об уменьшении эффективности отдачи имеем следующее соотношение:

$$\left| \frac{\mathrm{d}R_1}{\mathrm{d}x_{x=A}} \right| < \left| \frac{\mathrm{d}R_{12}}{\mathrm{d}x} \right| < \left| \frac{\mathrm{d}R_2}{\mathrm{d}x_{x=B}} \right| .$$

Таким образом, возникает задача об управлении рисками, а именно, о вкладывании ресурсов обоими субъектами в снижение риска от общего источника с целью минимизации уровня общего риска.

Величины ресурсов и соответствующих им рисков могут быть найдены из совместного решения системы уравнений:

$$\begin{cases} \dfrac{\mathrm{d}R_{12}}{\mathrm{d}x_{x=A_2+B_2}} = \dfrac{\mathrm{d}R_1}{\mathrm{d}x_{x=A-A_2}} \\ \dfrac{\mathrm{d}R_{12}}{\mathrm{d}x_{x=A_2+B_2}} = \dfrac{\mathrm{d}R_2}{\mathrm{d}x_{x=B-B_2}} \end{cases} .$$

Первое уравнение – это условие минимума полного риска для первого субъекта, второе уравнение – минимум полного риска для второго субъекта. Любое отступление от условий компромисса приведет к возрастанию риска хотя бы одного из субъектов. A_2 и B_2 обозначают вложения в снижение рассматриваемого

риска со стороны обоих участников.

Смысл предлагаемого подхода состоит в том, что решение системы уравнений оказывается взаимовыгодным (кооперативным по терминологии теории игр с непротивоположными интересами). Заметим, что компромисс может и не достигаться (система несовместна), если субъекты различаются по уровню технологического и социально-экономического развития (например, интервалы управляемых рисков могут не перекрываться).

6.3. Матрица распределения риска по критериям тяжести последствий аварии, по экономическим критериям

Полная безопасность не может быть гарантирована никому, независимо от образа жизни. Каждый из нас живет от одного дня до другого, избегая риска или преодолевая опасности, такие, например, как приведенные в табл. 6.1. При уменьшении риска ниже уровня 10^{-6} в год общественность не выражает чрезмерной озабоченности, и поэтому редко принимаются специальные меры для снижения степени риска; мы, например, не проводим свою жизнь в страхе погибнуть от удара молнии. Основываясь на этой предпосылке, многие специалисты принимают величину 10^{-6} как тот уровень, к которому следует стремиться, устанавливая степень риска, обусловленную деятельностью промышленных предприятий.

Таблица 6.1 Индивидуальный риск преждевременного фатального исхода, обусловленный различными причинами

Причина или место Несчастного случая	Общее число жертв за 1969 г.	Приблизительный уровень риска. Вероятность преждевременного фатального исхода в год[1]
1	2	3
Автомобильный транспорт	55791	$3 \cdot 10^{-4}$
Падение	17827	$9 \cdot 10^{-5}$
Пожар и ожог	7451	$4 \cdot 10^{-5}$
Утопление	6181	$3 \cdot 10^{-5}$
Отравление	4516	$2 \cdot 10^{-5}$

1	2	3
Огнестрельное оружие	2309	$1 \cdot 10^{-5}$
Станочное оборудование (1968 г.)	2054	$1 \cdot 10^{-5}$
Водный транспорт	1743	$9 \cdot 10^{-6}$
Воздушный транспорт	1778	$9 \cdot 10^{-6}$
Падающие предметы	1271	$6 \cdot 10^{-6}$
Электрический ток	1148	$6 \cdot 10^{-6}$
Железная дорога	884	$4 \cdot 10^{-6}$
Молния	160	$5 \cdot 10^{-7}$
Торнадо	118[2]	$4 \cdot 10^{-7}$
Ураган	90[3]	$4 \cdot 10^{-7}$
Все прочие	8695	$4 \cdot 10^{-5}$
Общее число жертв	115000	$6 \cdot 10^{-4}$
Катастрофы[4], связанные с ядерной энергией (100 реакторов)	–	$2 \cdot 10^{-10}$

[1] – Основаны на данных, относящихся ко всему населению США, за исключением случаев, указанных отдельно.

[2] – Среднее значение за 1953-1971 гг.

[3] – Среднее значение за 1901-1972 гг.

[4] – Основано на данных для населения $15 \cdot 10^5$ человек, связанных с видом риска.

Интересный обзор повседневной деятельности человека, носящей по своей природе случайный характер, был составлен Б.Буллахом из отделения "Монд" (Mond) фирмы "Империал кемикал индастриз" (Imperial chemical Industries).

По оси ординат на рис. 6.1 отложена частота несчастных случаев с фатальным исходом, т.е. среднее число погибших в результате несчастных случаев в течение 10 ч при определенных видах деятельности. Вопреки общественному мнению, которое сложилось в результате некоторых газетных статей, описывающих химическую промышленность, по меньшей мере, как причиняющую постоянные хлопоты или, в худшем случае, как скопление большого количества отравляющих веществ, на самом деле химическое предприятие является исключительно безопасным местом работы со средним уровнем риска, лежащим в нижней части спектра. Более того, примерно половина жертв (равная для

химической промышленности 3,5) обусловлена дорожными и другими транспортными происшествиями, падениями и т.п., т.е. несчастными случаями, не связанными с технологическим процессом.

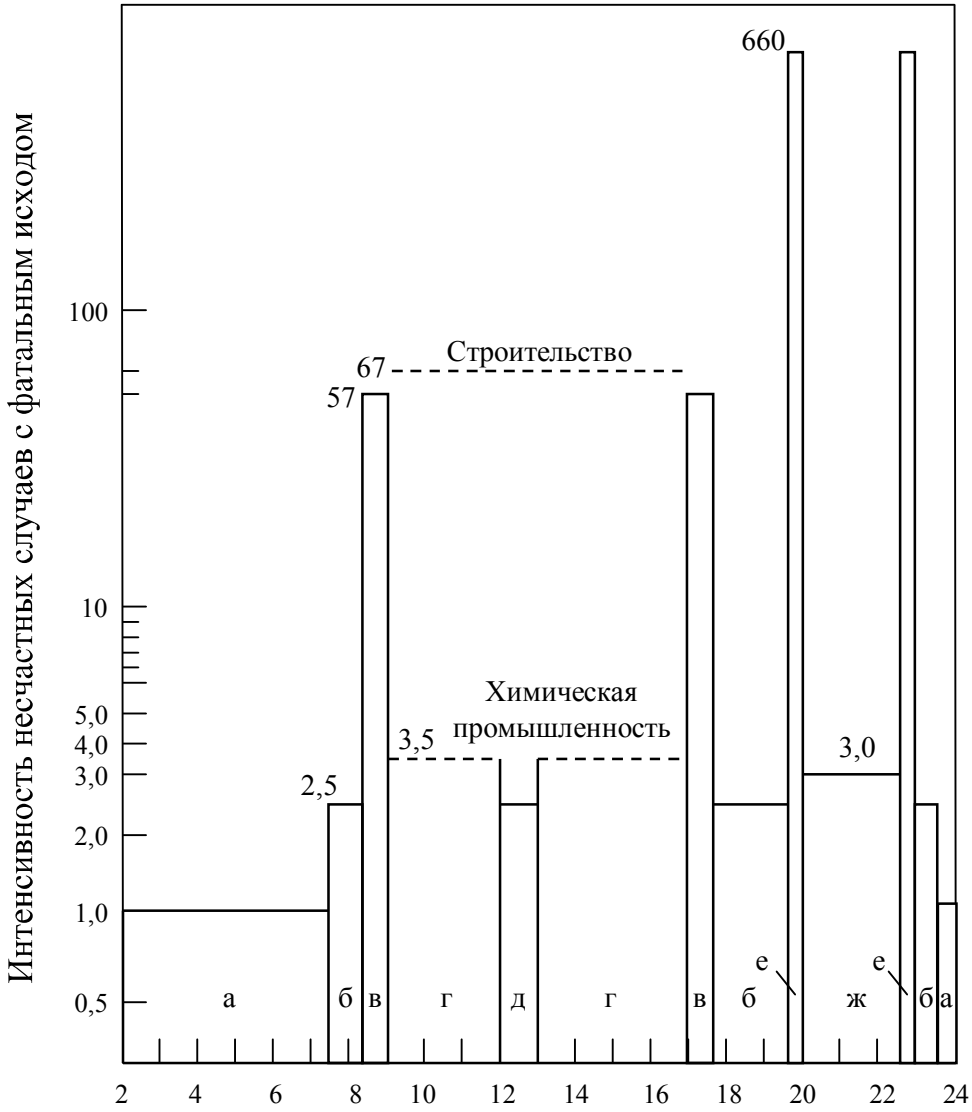


Рис.6.1. **Повседневные опасности:**

а – сон; *б* – домашний туалет и принятие пищи; *в* – поездка на работу и с работы за рулем автомобиля; *г* – дневная работа; *д* – обеденный перерыв; *е* – езда на мотоцикле; *ж* – развлечения

7. АНАЛИЗ РИСКА. НОРМАТИВНЫЕ ЗНАЧЕНИЯ РИСКА. СНИЖЕНИЕ РИСКА

7.1 Анализ риска и его нормативные значения

Анализ риска аварий на опасных производственных объектах (далее - анализ риска) является составной частью управления промышленной безопасностью. Анализ риска заключается в систематическом использовании всей доступной информации для идентификации опасностей и оценки риска возможных нежелательных событий.

Результаты анализа риска используются при декларировании промышленной безопасности опасных производственных объектов, экспертизе промышленной безопасности, обосновании технических решений по обеспечению безопасности, страховании, экономическом анализе безопасности по критериям «стоимость-безопасность-выгода», оценке воздействия хозяйственной деятельности на окружающую природную среду и при других процедурах, связанных с анализом безопасности.

Процесс проведения анализа риска включает следующие основные этапы:

планирование и организацию работ;

идентификацию опасностей;

оценку риска;

разработку рекомендаций по уменьшению риска.

Всесторонняя оценка риска аварий основывается на анализе причин (отказы технических устройств, ошибки персонала, внешние воздействия) возникновения и условий развития аварий, поражения производственного персонала, населения, причинения ущерба имуществу эксплуатирующей организации или третьим лицам, вреда окружающей природной среде. Чтобы подчеркнуть, что речь идет об «измеряемой» величине, используется понятие «степень риска» или «уровень риска». Степень риска аварий на опасном производственном объекте, эксплуатация которого связана со множеством опасностей, определяется на основе учета соответствующих показателей риска. В общем случае показатели риска выражаются в виде сочетания (комбинации) вероятности (или частоты) и тяжести последствий рассматриваемых нежелательных событий.

Ниже даны краткие характеристики основных количественных показателей риска.

1. При анализе опасностей, связанных с отказами технических устройств, выделяют **технический риск**, показатели которого определяются соответствующими методами теории надежности.

2. Одной из наиболее часто употребляющихся характеристик опасности является **индивидуальный риск** - частота поражения от-

дельного индивидуума (человека) в результате воздействия исследуемых факторов опасности. В общем случае количественно (численно) индивидуальный риск выражается отношением числа пострадавших людей к общему числу рискующих за определенный период времени. При расчете распределения риска по территории вокруг объекта (картировании риска) индивидуальный риск определяется потенциальным территориальным риском (см. ниже) и вероятностью нахождения человека в районе возможного действия опасных факторов. Индивидуальный риск во многом определяется квалификацией и готовностью индивидуума к действиям в опасной ситуации, его защищенностью. Индивидуальный риск, как правило, следует определять не для каждого человека, а для групп людей, характеризующихся примерно одинаковым временем пребывания в различных опасных зонах и использующих одинаковые средства защиты. Рекомендуется оценивать индивидуальный риск отдельно для персонала объекта и для населения прилегающей территории или, при необходимости, для более узких групп, например для рабочих различных специальностей.

3. Другим комплексным показателем риска, характеризующим пространственное распределение опасности по объекту и близлежащей территории, является **потенциальный территориальный риск** - частота реализации поражающих факторов в рассматриваемой точке территории. Потенциальный территориальный, или потенциальный, риск не зависит от факта нахождения объекта воздействия (например, человека) в данном месте пространства. Предполагается, что условная вероятность нахождения объекта воздействия равна 1 (т.е. человек находится в данной точке пространства в течение всего рассматриваемого промежутка времени). Потенциальный риск не зависит от того, находится ли опасный объект в многолюдном или пустынном месте и может меняться в широком интервале. Потенциальный риск, в соответствии с названием, выражает собой потенциал максимально возможной опасности для конкретных объектов воздействия (реципиентов), находящихся в данной точке пространства. Как правило, потенциальный риск оказывается промежуточной мерой опасности, используемой для оценки социального и индивидуального риска при крупных авариях. Распределения потенциального риска и населения в исследуемом районе позволяют получить количественную оценку социального риска для населения. Для этого нужно рассчитать количество пораженных при каждом сценарии от каждого источника опасности и затем определить частоту событий *F,* при которой может пострадать на том или ином уровне N и более человек.

4. **Социальный риск** характеризует масштаб и вероятность (частоту) аварий и определяется функцией распределения потерь (ущерба), у которой есть установившееся название - ***F/N*-кривая** (в

зарубежных работах - кривая Фармера).

В общем случае в зависимости от задач анализа под *N* можно понимать и общее число пострадавших, и число смертельно травмированных или другой показатель тяжести последствий. Соответственно критерий приемлемого риска будет определяться уже не числом для отдельного события, а кривой, построенной для различных сценариев аварии с учетом их вероятности. В настоящее время общераспространенным подходом для определения приемлемости риска является использование двух кривых, когда, например, в логарифмических координатах определены F/N-кривые приемлемого и неприемлемого риска смертельного травмирования. Область между этими кривыми определяет промежуточную степень риска, вопрос о снижении которой следует решать, исходя из специфики производства и региональных условий.

5. Другой количественной интегральной мерой опасности объекта является **коллективный риск**, определяющий ожидаемое количество пострадавших в результате аварий на объекте за определенное время.

6. Для целей экономического регулирования промышленной безопасности и страхования важным является такой показатель риска, как статистически **ожидаемый ущерб** в стоимостных или натуральных показателях.

Ключевым принципом в анализе риска является идея, предложенная Фармером в 1967 г. и заключающаяся в установлении случайной, но тщательно подобранной зависимости между средним количеством радиоактивной утечки в атмосферу из ядерного реактора и вероятностью (средняя частота в год или соответствующая величина среднего отрезка времени между этими событиями) наступления такого события. Таким способом определяется *предельная кривая частоты случайных утечек*, которая может использоваться прежде всего в качестве исходных данных проектировщиками новой станции и специалистами по оценке безопасности. Существующая форма предельной кривой частоты аварийных утечек, которая в настоящее время используется управлением по атомной энергии Великобритании, показана на рис.7.1. Считается, что кривая отделяет верхнюю область недопустимо большого риска от области приемлемого риска, расположенной ниже и левее кривой. Кривую, таким образом, можно использовать в качестве критерия безопасности, определяющего верхнюю границу допустимой вероятности. Если это условие выполняется, основная цель достигнута, а интуиция подсказывает, что она правильная, а

именно: аварии, вызывающие небольшие утечки и приводящие к незначительным последствиям, отражающимся на здоровье людей и чистоте окружающей среды, могут случаться сравнительно часто (например, каждые 10 или 100 лет в среднем для одного реактора); чем больше утечка, тем меньше должна быть вероятность или частота ее появления, а для очень больших утечек вероятность действительно должна быть чрезвычайно низкой.

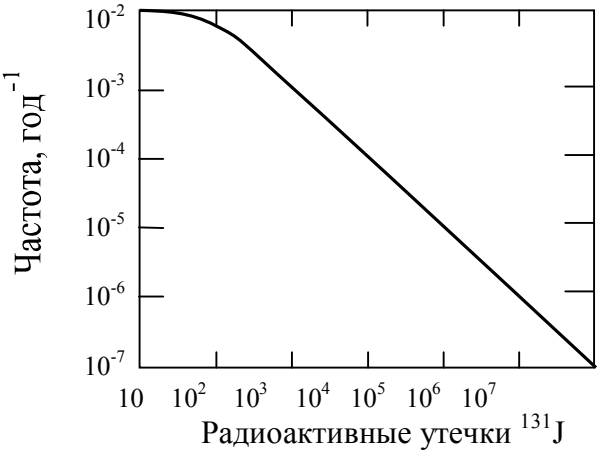


Рис.7.1. Предельная кривая интенсивности утечек для йода

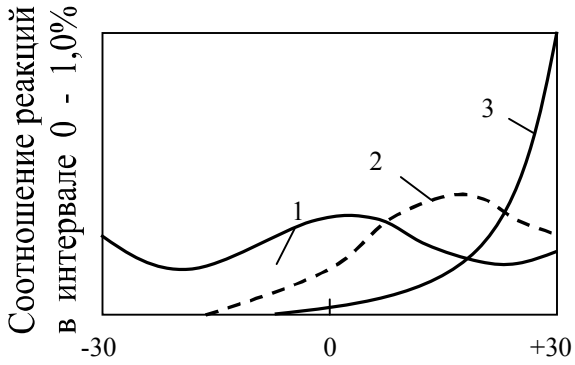


Рис.7.2. Распределение частоты благоприятного отношения общественности к различным видам энергии: *1* – ядерная; 2 – уголь и нефть; 3 – солнечная и гидравлическая

В наше время "полной гласности" выявление и количественная оценка риска, которая выполняется квалифицированными специалистами, являются предметом обсуждения общественности. Схема прохождения информации показана на рис. 7.3.

Рис.7.3. Структурная схема проведения анализа риска

В нее включены психологические и социальные аспекты, иными словами, такие понятия, как психологическое благополучие индивидуума в соответствии с его пониманием социального риска и воздействие этих факторов на общество в целом и его отдельных членов. Широко известно, что общественность поразному реагирует на риск: приемлемая степень смертельного риска при добровольном участии на три порядка (10^3) выше, чем при вынужденном участии.

Поэтому можно ожидать, что средства железнодорожного транспорта в 1000 раз "безопаснее", чем защитное снаряжение альпиниста. Точно так же известно, что общество считает одиночные, но с тяжелыми последствиями события менее приемлемыми, чем большое количество малых происшествий при той же степе-

ни риска. Приведенные примеры иллюстрируют раздел "общественное мнение" на рис. 7.3.

Подобные наблюдения являются результатом применения методологии, которая основана на учете отношения общества и которая служит для выявления определяющих факторов восприятия людьми технических систем. Обычно считается, что положительное отношение направлено на принятие риска, а отрицательное – на его отвергание.

На рис.7.2. показано распределение частоты благоприятного отношения общественности к пяти основным видам энергии. Было выявлено только три вида распределения. К гидравлической и солнечной энергии отношение исключительно благоприятное; отношение к углю и нефти умеренно благоприятное; что касается ядерной энергии, явно обнаруживается нормальный закон распределения отношения за исключением дополнительных всплесков существенно отрицательного и положительного характера. Последний вид распределения отражает степень поляризации взглядов по отношению к радиоактивным отходам. Анализ, подобный приведенному, представляет определенный интерес, однако результаты далеки от того, чтобы сделать окончательные выводы. Действительно, они выражают лишь интуитивные мнения людей и отражают определенную тенденцию, высказанную в интервью. В США когда бы людям не предоставлялась возможность проголосовать по вопросу ядерной энергии, они голосовали преимущественно в пользу ее применения в мирных целях. Противники ядерной энергии иногда успешно запугивают судебный и административный аппарат. В этой связи интересно отметить, что недавно проведенный в стране опрос общественного мнения показал, что американцы больше доверяют инженерам, чем адвокатам или врачам. Конечно, информация в прессе, относящаяся к аварии на атомной электростанции "Три майл айленд" (Three Mile Island), может полностью изменить эту картину.

При проведении анализа (второй квадрат на рис. 7.3. в колонке "Анализ риска") может быть применена теория использования или метод оценки затрат – результатов. Когда при анализе проекта учитываются возможность человеческих жертв или меры для их исключения, количественные задачи приводят к необходимости оценить безопасность человеческой жизни в стоимостном выражении.

В принципе имеется пять подходов, которые были предло-

жены для придания денежного выражения мерам по обеспечению безопасности для использования при оценках затрат – результатов. К ним относятся (по данным Отвейя) следующие:

Косвенная стоимость. Безопасность человека оценивается в соответствии со стоимостью мероприятий, проводимых с целью уменьшения смертельного риска.

Личный капитал. Безопасность оценивается как часть заработка индивидуума, связанного с риском.

Страхование. Безопасность оценивается на основе суммы личного страхования.

Судебные выплаты. Выплаты по решению суда в качестве компенсации за потерю жизни берутся за основу для определения размера стоимости безопасности.

Добровольные платы. Оценивается уменьшение риска по величине добровольной платы за меры безопасности.

Денежные выражения, полученные с помощью этих методов, сведены в табл. 7.1 с указанием ограничений, присущих данным методам.

Таблица 7.1 Оценка безопасности с точки зрения анализа доходов и расходов

Виды оценок	Типичная стоимость, тыс.долл.	Ограничения
1	2	3
Косвенная стоимость	9-9000	Принятые меры безопасности предполагаются оптимальными
Личный капитал	100-400	Целиком основан на доходе в течение всей жизни. Не учитывает индивидуальные наклонности. Дискриминируются непроизводительные члены общества
Страховые премии	Широкий диапазон	Не учитывают индивидуальные интересы в части защиты собственной жизни
Судебные выплаты	250	Основаны на потерянных доходах
Добровольная плата	180-1000	С трудом поддается оценке. Зависит от обстоятельств, связанных с риском

Примечания.

Итог: Все варианты оценок в определенной степени зависят от потенциального суммарного дохода индивидуума, связанного с риском, в течение его жизни и не учитывают серьезности последствий.

Вывод: Сумма не может быть определена очень точно. Следует выбирать значения стоимости (например, 300 тыс. долл.) в зависимости от индивидуальных отличий, интересов третьих лиц и психологических факторов.

Все приведенные методы так или иначе зависят от дохода индивидуумов, связанных с риском, и от действующих юридических законодательств. Для того чтобы получить правильную величину, которая используется при анализе затрат – результатов, необходимо уделить внимание причине и времени смерти и связанным с ней трагическим обстоятельствам. В США суд обычно выносит решение о меньших суммах выплаты при разборе смертельных случаев, чем при потерях трудоспособности.

Последний блок на рис. 7.3 "Стратегия управления риском" включает информацию исторического и политического характера, а также данные общего характера. Таким образом, рассматриваются все технические и социальные аспекты в их взаимосвязи. При этом ключевым моментом являются "политические суждения", а выводы обычно неутешительные. Результаты исследований, проведенных Пончином и другими учеными, представлены в табл. 7.2.

Таблица показывает, что потребление природного газа и ядерной энергии – видов топлива, используемых для производства электроэнергии и являющихся предметом острых политических дискуссий, существенно меньше связано с риском, чем другие способы получения электроэнергии.

Таблица 7.2 Оценка числа смертельных случаев, вызванных различными источниками энергии в расчете на 1 гигаватт (1 Гвт)

Виды топлива или энергии	Конечная форма энергии	Число жертв на 1 Гвт		Суммарное
		профессиональных	населения	
Метанол, биопродукты	м	110	0	110
Энергия ветра	э	20 – 30	2 – 40	22 – 70
Солнечная, фотоэлектрическая	э	16 – 21	1 – 40	17 – 61
Уголь	э	2 – 10	3 – 150	5 – 160
Солнечная (тепловая)	э	7 – 10	1 – 40	8 – 50
Нефть	э	0,2 – 2	1,4–140	1,6 – 142
Солнечная (нагрев помещения)	т	9 – 10	0,4	9 – 10
Гидроэлектрическая	э	2 – 4	1 – 2	3 – 6
Океан (тепловая)		2 – 3	0,1	2 – 3
Атомная	э	0,2 – 1,3	0,04–0,24	0,25 – 1,5
Природный газ	э	0,1 – 0,4	0	0,1 – 0,4

Конечная форма энергии: э – электрическая; м – механическая; т –тепловая

7.2. Снижение риска за счет приоритетного снижения вероятности возникновения аварийной ситуации и разработка рекомендаций по снижению ожидаемого ущерба

Подобно анализам воздействия промышленных предприятий на окружающую природную среду, большинство исследований по оценке безопасности и риска в настоящее время выполняется с целью удовлетворения лишь запросов общественности и государственных органов надзора, но не с целью уменьшения самого риска.

В качестве доказательства этого утверждения предлагается наблюдение, что, по-видимому, только 10% сооружаемых в настоящее время предприятий были подвергнуты анализу с целью определения связанного с ними риска (или воздействия на окружающую среду). Существующая тенденция в законодательстве,

относящемся к риску, состоит в формулировании требований к количественным оценкам. Документ комиссии по контролю за ядерной энергетикой *RG*1.115 под названием "*Защита против газотурбинных низколетающих аппаратов*" (с. 1.115-3) утверждает, что "Персонал этой комиссии считает уровень 10^{-7} в год допустимой степенью риска с выходом из строя одной из основных систем для единичного происшествия". Другой интересный принцип количественной оценки риска предложен в документе *RG* 1.110 "*Анализ затрат - результатов для систем радиоактивных отходов* (с. 1.110-6): Любой претендент на получение разрешения на строительство ядерного реактора с водяным охлаждением должен продемонстрировать с помощью анализа затрат – результатов, что дальнейшее снижение совокупной дозы облучения, получаемой населением в 80-километровой окрестности вблизи места нахождения реактора, не может быть обеспечено за счет мероприятий годовой стоимостью в 1000 долл. на 1 бэр (100 бэр=13 в) в расчете на одного человека (или меньше этой стоимости, являющейся приемлемой для данного конкретного случая)".

США первенствовали во введении такого, носящего не практичный характер законодательства, относящегося к атомной энергии и вопросам окружающей среды. Однако страны Европы быстро ликвидируют отставание в части подобных законодательств, основанных на количественных критериях, и обещают обогнать Соединенные Штаты путем распространения этих принципов на оформление прав и правил инспекции химических предприятий. Такие законодательства уже приняты в Нидерландах, за которыми вскоре должны последовать законодательные органы Великобритании и Франции.

Нет уверенности в том, что подобные законодательства положат конец несчастным случаям; они лишь увеличат расходы для населения. Действительно если единственным побуждением при проведении исследования риска является удовлетворение правительственных требований, то оно направлено лишь на снятие персональной ответственности с исследователя и не стимулирует его конструктивного вклада в решение проблемы обеспечения безопасности.

8. АВАРИЙНАЯ ПОДГОТОВЛЕННОСТЬ. АВАРИЙНОЕ РЕАГИРОВАНИЕ. УПРАВЛЕНИЕ РИСКОМ. ДОПУСТИМЫЙ РИСК

8.1 Система подготовки специалистов в направлении обеспечения безопасности производственных объектов

8.1.1 Нахождение аварийного события

Имеется два подхода при анализе причинных связей: *прямой анализ* и *анализ с обратным порядком*. Анализ с прямым порядком начинается с определения перечня отказов и развивается в прямом направлении с определением последствий этих событий. Анализ с обратным порядком начинается с отыскания опасного состояния системы, от которого в обратном направлении прослеживаются возможные причины возникновения этого состояния.

При построении дерева событий (ДС), проведении анализа видов отказов и последствий (АВОП), анализа критичности (АК) и предварительного анализа опасностей (ПАО) используется прямой подход. Обратный порядок характерен для анализа с помощью дерева отказов (АДО). Комбинированное использование обоих подходов необходимо, чтобы полностью решать задачу анализа риска и надежности.

Обратный подход, т.е. анализ с помощью дерева отказов, используется для определения причинных связей, ведущих к данному опасному состоянию системы. Само опасное состояние становится конечным событием дерева отказов. Данное конкретное конечное событие является лишь одним из многих возможных опасных состояний системы, представляющих интерес для анализа; дерево отказов само по себе не выявляет возможных опасных событий в системе. Большие системы могут иметь много самых различных конечных событий и соответствующих им деревьев отказов.

При выполнении анализа в прямом порядке принимается ряд определенных последовательностей событий и составляются соответствующие этим последствиям сценарии, оканчивающиеся опасными состояниями системы. Информация, которая должна быть собрана и обработана для написания хорошего сценария, состоит из сведений по *взаимосвязи элементов* и *топографии системы*, а также включает данные по отказам элементов и другим *детальным характеристикам системы*. Эти

сведения оказываются полезными и для построения деревьев отказов.

8.1.2 Взаимосвязи элементов и топография системы

Система состоит из таких элементов, как единицы оборудования, материалы, персонал предприятия (необязательно, чтобы эти элементы были самыми мелкими в системе; они могут быть блоками или целыми подсистемами), которые находятся в определенной окружающей и социальной среде и подвержены старению.

Опасные состояния вызываются одним или несколькими элементами, приводящими к отказам в системе. Окружающая среда, персонал и старение могут влиять на систему только через ее элементы (рис. 8.1).

Рис. 8.1. Воздействия и взаимосвязи элементов

Каждый элемент системы связан с другими элементами специфическим образом, а идентичные элементы могут иметь различные характеристики в различных системах. Поэтому необ-

ходимо уточнять взаимосвязи и топографию системы.

Взаимосвязи и топографию определяют, например, путем изучения системы трубопроводов данного предприятия, электрических схем, механических соединений, потоков информации, а также физического расположения элементов. Эти связи наилучшим образом можно представить в виде различных схем системы; технические описания системы и карты логических переходов также оказываются полезными в данной работе.

Например, гидравлический удар, который вызывается быстрым закрытием клапана и который, в свою очередь, приводит к потере герметичности фланцевого соединения, выявляют при изучении схемы трубопроводов. Взаимовлияние двух близко расположенных емкостей возможно в случае пожара. Возможные изменения состояния элементов системы, возникающие в результате других причин, следует также включать в технические описания или в карты логических переходов.

8.1.3 Характеристики отказов элементов

Отказы элементов являются основополагающими данными при анализе причинных связей. Они классифицируются на *первичные отказы*, *вторичные отказы* и *ошибочные команды*.

Первичный отказ элемента определяют как нерабочее состояние этого элемента, причиной которого является он сам, и необходимо выполнить ремонтные работы для возвращения элемента в рабочее состояние. Первичные отказы происходят при входных воздействиях, значения которых находятся в пределах, лежащих в расчетном диапазоне, а отказы объясняются естественным старением элементов. Разрыв резервуара вследствие усталости материала служит примером первичного отказа.

Вторичный отказ такой же, как первичный, за исключением того, что сам элемент не является причиной отказа. Вторичные отказы объясняются воздействием предыдущих или текущих избыточных напряжений на элементы. Амплитуда, частота, продолжительность действий этих напряжений могут выходить за пределы допусков или иметь обратную полярность и вызываются различными источниками энергии: термической, механической, электрической, химической, магнитной, радиоактивной и т.п. Эти напряжения вызываются соседними элементами или окружающей средой, например, метеорологическими и геологическими условиями, а также воздействием со стороны других технических систем. Лю-

ди, например операторы и контролеры, также являются возможными источниками вторичных отказов, если их действия приводят к выходу элементов из строя. Примерами вторичных отказов служит "срабатывание предохранителя от повышенного электрического тока", "повреждение емкостей для хранения при землетрясении". Следует отметить, что устранение источников повышенных напряжений не гарантирует возвращения элемента в рабочее состояние, так как предыдущая перегрузка могла вызвать необратимое повреждение в элементе, требующее в этом случае ремонта. Когда точный вид первичного или вторичного отказа определен и данные по этому отказу получены, события с первичными и вторичными отказами оказываются одинаковыми, они рассматриваются как исходные отказы, которые в дереве отказов помещаются в круглые блоки.

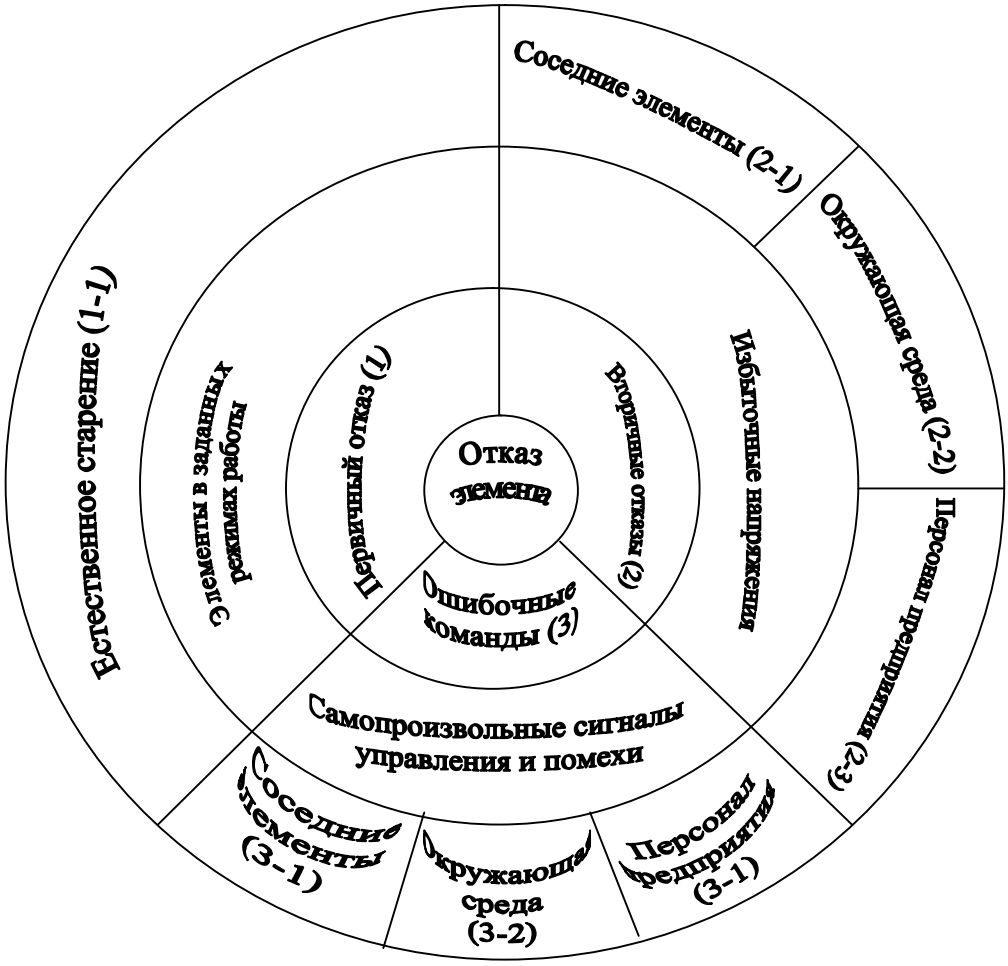


Рис. 8.2 Характеристики отказов элементов

Ошибочные команды представляются в виде элемента, находящегося в нерабочем состоянии из-за неправильного сигнала управления или помехи, при этом часто не требуется ремонт для возвращения данного элемента в рабочее состояние. Самопроизвольные сигналы управления или помехи часто не оставляют последствий (повреждений), и в последующих нормальных режимах элементы работают в соответствии с заданными требованиями. Типичными примерами ошибочных команд являются: "напряжение приложено самопроизвольно к обмотке реле", "переключатель случайно не разомкнулся из-за помех", "помехи на входе контрольного прибора в системе безопасности вызвали ложный сигнал на остановку", "оператор не нажал аварийную кнопку" (ошибочная команда от аварийной кнопки).

Как показано во внутреннем кольце (рис.8.2), расположенном вокруг "отказа элементов", отказы могут возникнуть в результате 1) первичных отказов, 2) вторичных отказов или 3) ошибочных команд. Отказы всех этих категорий могут иметь различные причины, приведенные в наружном кольце.

8.1.4. Технические характеристики системы

Только главные, наиболее вероятные или критичные события должны рассматриваться на начальной стадии анализа. Для определения этих событий можно использовать анализ критичности (АК). По мере продвижения аналитической работы можно включать все более редкие или менее вероятные события или предпочесть не принимать их в расчет. В принципе, окружающие условия – это весь мир, в котором находится данная система. Таким образом, чтобы не отклоняться от намеченной цели, необходимо установить разумные пределы влияния окружающей среды при проведении исследования с помощью дерева событий или анализа последствий, поскольку эти два подхода предусматривают детальную разработку развития начальных аварийных событий в системе и окружающей ее среде.

При определении системы требуется тщательно установить *начальные состояния элементов*. Все элементы, которые имеют более одного рабочего состояния, создают различные начальные условия. Например, начальное количество жидкости в баке может быть регламентировано. Событие "бак полный" становится одним начальным состоянием, а "бак пустой" является другим

состоянием. Необходимо также точно установить *рабочий отрезок времени*: например, условия при пуске и остановке могут создавать другого рода опасные условия, отличающиеся от установившихся режимов работы.

Когда достаточное количество информации по системе собрано, можно составить описания вариантов развития процесса (сценариев) и определить конечные события. Затем устанавливают причинные взаимосвязи, ведущие к каждому конечному событию, при помощи дерева отказов.

8.1.5 Процедура построения дерева отказов

Дерево отказов является графическим представлением причинных взаимосвязей, полученных в результате прослеживания опасных ситуаций в системе в обратном порядке, для того чтобы отыскать возможные причины их возникновения. В этом случае опасная ситуация в системе является конечным событием в дереве отказов.

8.1.6 Пример построения дерева отказов

В качестве первого примера построения дерева отказов рассмотрим конечное событие "отказ запуска электродвигателя" для системы, представленной на рис. 8.3.

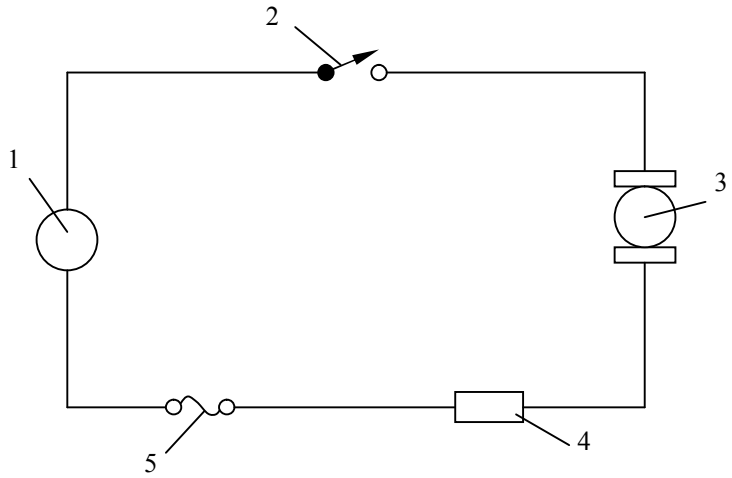


Рис.8.3. Электрическая схема системы:
1 – генератор; *2* – переключатель; *3* – электродвигатель;
4 – кабель; *5* – предохранитель

Четкое определение конечного события необходимо, даже если событие описано на дереве отказов в сокращенной форме. В

данном случае полным конечным событием является "отказ запуска электродвигателя при включении переключателя в заданный момент времени *t*" (переменная *t* может быть выражена не только в единицах времени, но и в другой размерности. Например, данные по надежности транспортных средств обычно задаются в виде пробега. Иногда эта переменная означает число циклов работы.

Классификация отказов элементов, которая приведена на рис. 8.2, полезна при построении дерева отказов, показанного на рис.8.4. Следует отметить, что термины *первичное событие* и *исходный отказ* становятся синонимами, когда отказ (и данные по нему) детально определен, и что вторичные отказы, расположенные над ним, будут в конечном итоге или исключены, или станут исходными событиями.

Конечное событие "отказ запуска электродвигателя" может быть вызвано тремя причинами: первичный отказ электродвигателя, вторичный отказ и ошибочная команда. Первичные отказы – это отказы самого электродвигателя, который соответствует техническим условиям, возникающие в результате естественного старения. Вторичные отказы возникают из-за причин, которые лежат за пределами, заданными техническими условиями, таких как:

а) переработка (например, переключатель остался включенным после предыдущей работы, что вызвало перегрев обмотки электродвигателя, приведший, в свою очередь, к короткому замыканию или обрыву цепи;

б) выход условий работы за установленные пределы (такие, как механические вибрации, термические нагрузки и т.д.);

в) неправильное обслуживание (например, некондиционная смазка подшипников электродвигателя).

Ошибочные команды вызываются самопроизвольными управляющими сигналами или помехами; в данном случае этот отказ заключается в "отсутствии напряжения на электродвигателе".

Первичные и вторичные отказы вызываются причинами, приведенными в крайнем наружном кольце на рис.8.2. Элемент может быть в нерабочем состоянии в момент времени *t*, если предыдущие возмущения вывели элемент из строя, и он не был отремонтирован. Возмущения могли возникнуть в любое время до момента *t*.

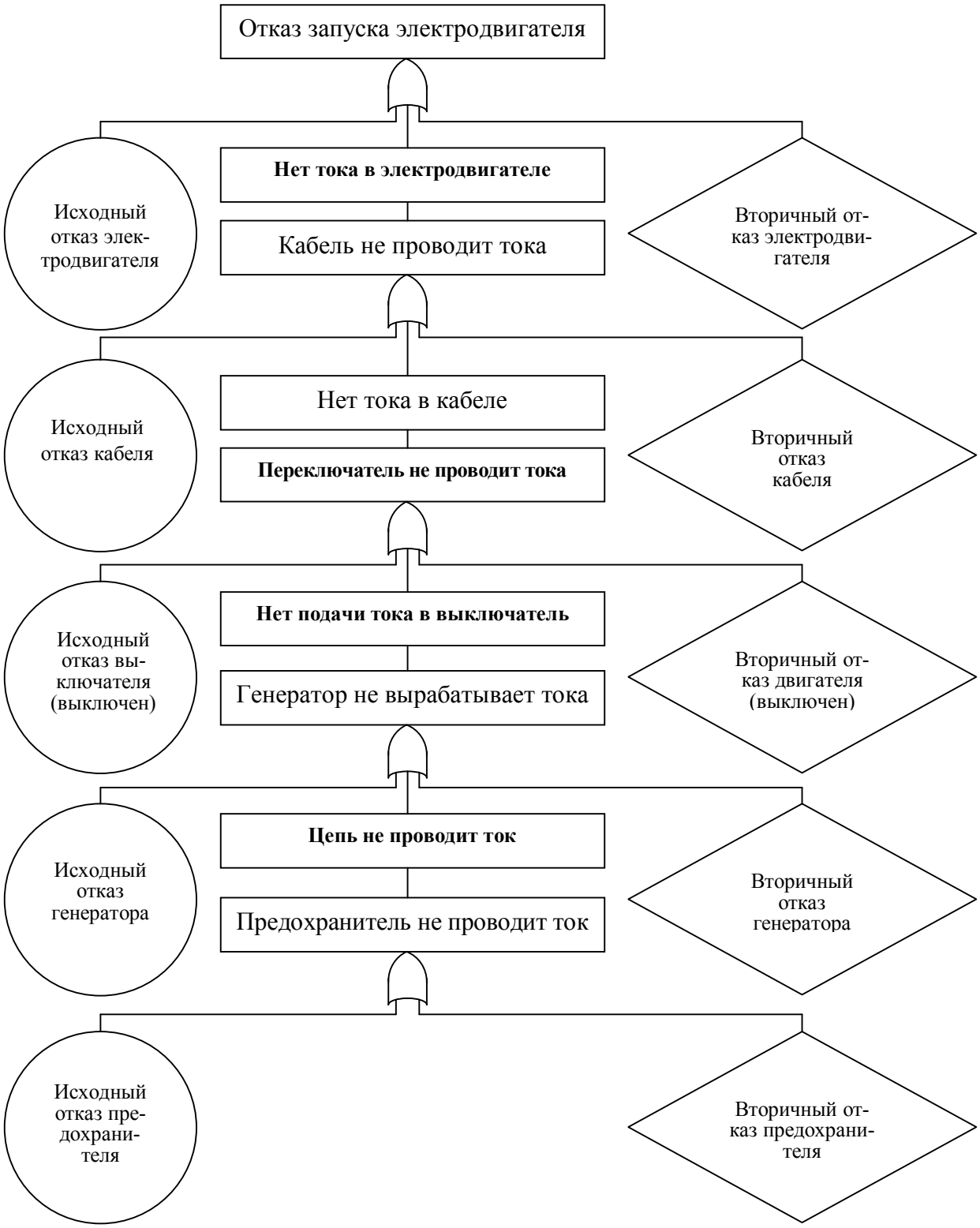


Рис. 8.4. *Дерево отказов для системы, изображенной на рис.8.3*

Однако процесс во времени не рассматривается, таким образом первичный или вторичный отказы в момент *t* являются конечными событиями, и более детальный анализ не проводится. Другими словами, дерево отказов является мгновенным "снимком" системы в момент *t*. Возмущения являются факторами, управляющими переходом из исправного состояния элемента к нарушенному. Точнее говоря, эти возмущения определяют вероятность перехода элементов из одного состояния в другое.

Первичное событие заключено в круге, так как оно является исходным событием, для которого имеются детальные данные по отказу. Вторичное событие является не полностью разработанным, поэтому оно помещено в ромбе. Количественные характеристики вторичных отказов следует оценивать соответствующими методами, после чего они также становятся исходными событиями.

Как было показано на рис. 8.2, ошибочная команда "нет напряжения на электродвигателе" возникает при отказе соседних элементов. На рис. 8.4 имеется событие "нет тока в цепи". Возможна более детальная разборка этого события, которое в итоге приводит к событию "нет тока через предохранитель". Имеется первичный отказ предохранителя "обрыв предохранителя из-за естественного старения" и вторичный отказ "предохранитель размыкается избыточным током". Можно ввести ошибочную команду "нет напряжения на предохранителе", которая относится к категории 3 (рис. 8.2). Однако все элементы были рассмотрены ранее и не было обнаружено отказов, вызывающих событие "нет напряжения на предохранителе". Таким образом, можно не учитывать данную ошибочную команду; в результате дерево отказов построено полностью.

Вторичный отказ предохранителя может быть вызван избыточным током, протекающим в данный момент или перед этим и возникающим в результате отказа соседних элементов. Избыточный ток в любое время до момента *t* может повредить предохранитель. Нельзя ввести событие "избыточный ток возник до момента *t*", так как тогда нужно рассматривать неопределенное число моментов в прошлом. Однако можно ввести событие "избыточный ток в данный момент *t*", и в результате окончательный вариант дерева отказов будет иметь вид, представленный на рис. 8.5 (следует заметить что логический знак запрета здесь эквивалентен знаку "И").

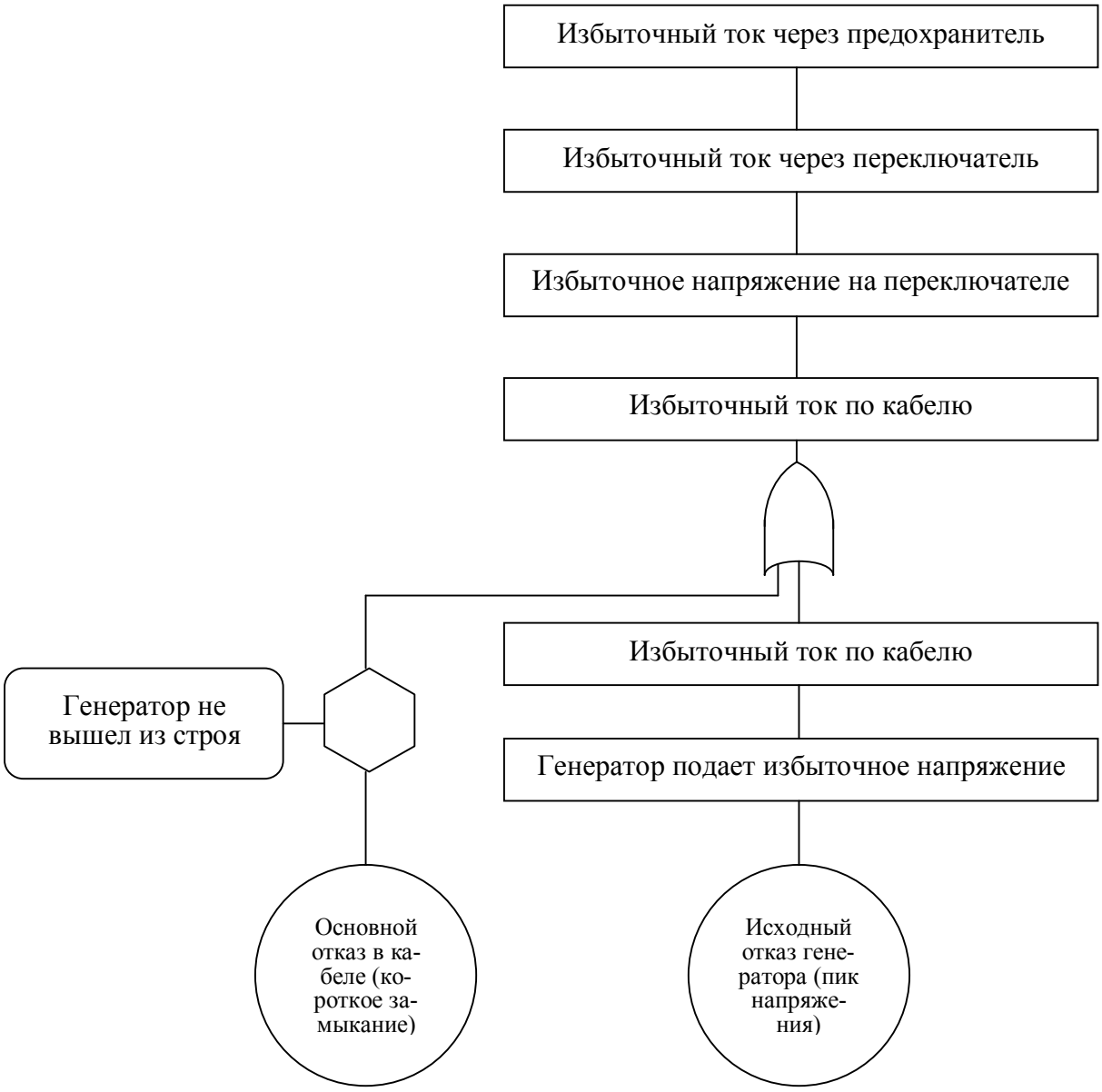


Рис. 8.5. Дерево отказов с конечным событием "избыточный ток предохранителя" (вторичные отказы не учитываются)

Необходимо отметить, что вероятность события "генератор не вышел из строя" очень высока, например равна 0,9999. Будем называть такие события "событиями с очень большой вероятностью", и ими можно пренебречь на входе в логический знак "И" (или знак запрета), существенно не изменяя вероятность конечного события (события с очень большой вероятностью, как подчеркивалось выше, не должны включаться в дерево отказов). Только при очень детальном анализе "события с очень большой вероятностью" сохраняются в дереве отказов. На рис. 8.6 представлен упрощенный

вариант дерева отказов, изображенного на рис.8.5; конечным событием в этом варианте является "избыточный ток".

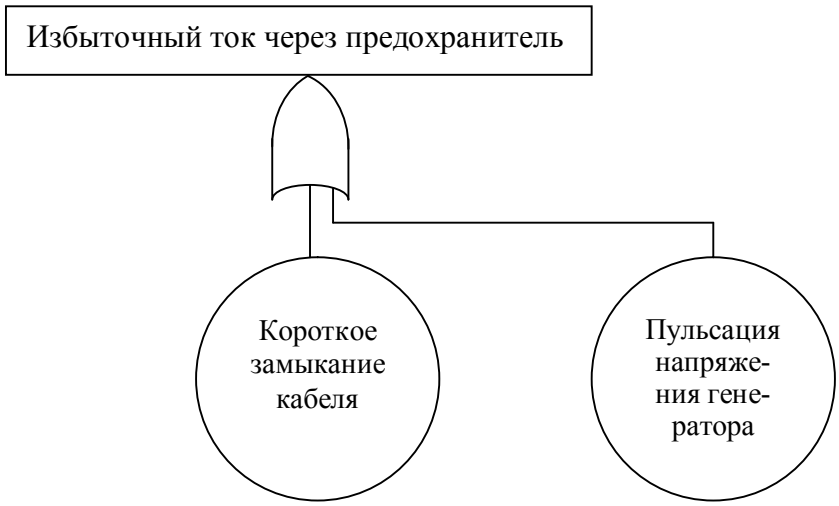
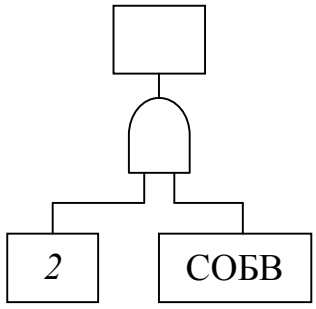


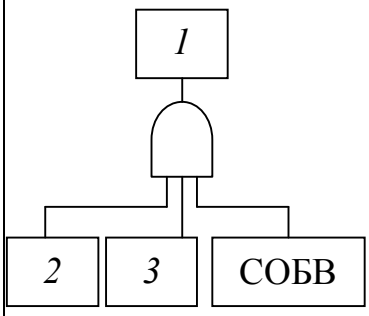
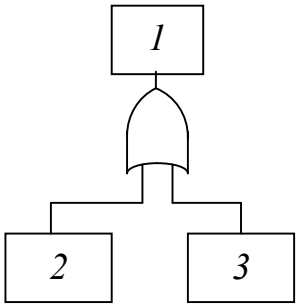
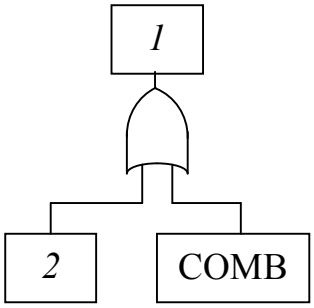
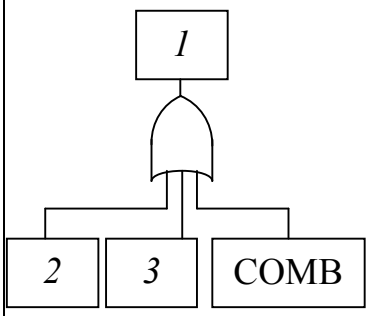
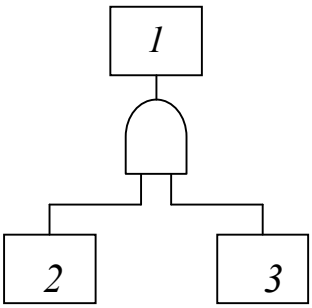
Рис. 8.6. Дерево отказов, полученное при пренебрежении событием с очень высокой вероятностью (генератор не вышел из строя)

Данное дерево отказов можно использовать для количественных оценок с применением методов, описанных в главе 3, для того, чтобы определить частоту возникновения избыточного тока в данной момент t^*. Эта информация, в свою очередь, используется для количественных оценок вторичных отказов предохранителя и в конце концов для подсчета вероятности появления события "нет запуска электродвигателя". Упрощенные методы анализа для событий 1, 2 и 3 очень большой (СОБВ) и очень малой (СОМВ) вероятности появления приведены в табл. 8.1.

Таблица 8.1 Варианты упрощений за счет событий с очень высокой или очень низкой вероятностью

Упрощение за счет события	Причинные связи	
	Первоначальные	упрощенные
1	2	3
С очень высокой вероятностью (логический знак "И" с двумя входами)		

Продолжение табл.8.1

1	2	3
С очень высокой вероятностью (логический знак "И" с тремя или большим числом входов)		
С очень низкой вероятностью (логический знак "ИЛИ" с двумя входами)		
С очень низкой вероятностью (логический знак "ИЛИ" с тремя или большим числом входов)		

8.1.7 Эвристические правила

Ниже описываются некоторые эвристические правила, используемые для построения дерева отказов. Эти правила сведены в табл. 8.2 и проиллюстрированы на рис.8.7. Имеется семь основных правил, согласно которым следует:

1) заменять абстрактные события менее абстрактными, например, событие "Электродвигатель работает слишком долго" на событие "ток через электродвигатель протекает слишком долго";

2) разделять события на более элементарные, например событие "взрыв бака" заменять на событие "взрыв за счет переполнения" или "взрыв в результате реакции, вышедшей из-под контроля";

3) точно определять причины событий, например, событие "вышедшая из-под контроля реакция" заменять на событие "избыточная подача" или "прекращение охлаждения";

4) связывать инициирующие события с событием типа "отсутствие защитных действий", например, событие "перегрев" заменять на событие "отсутствие охлаждения" в сочетании с событием "нет выключения системы";

5) отыскивать совместно действующие причины событий, например, событие "пожар" заменять на два события "утечка горючей жидкости" и "искрение реле";

6) точно указать место отказа элемента, например, событие "нет напряжения на электродвигателе" заменять на событие "нет тока в кабеле"; другой пример: событие "нет охлаждающей жидкости" заменять на событие "главный клапан закрыт" в сочетании с событием "нет открытия обводного клапана";

7) детально разрабатывать отказы элементов в соответствии со схемой, приведенной на рис. 8.7.

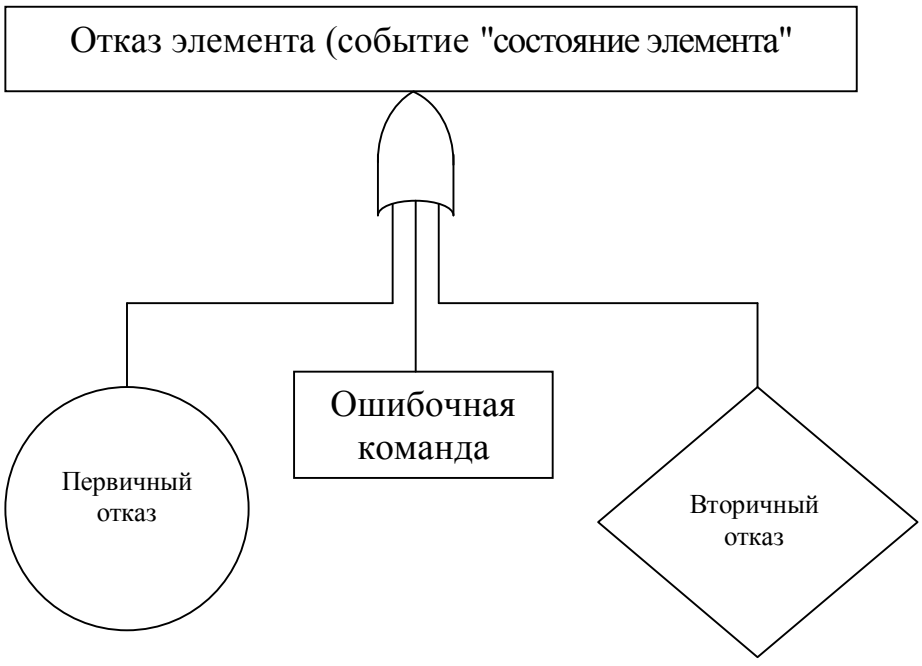
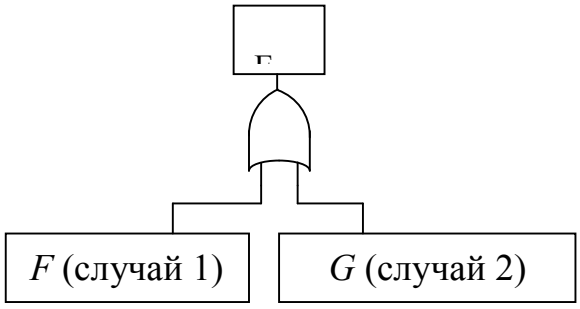
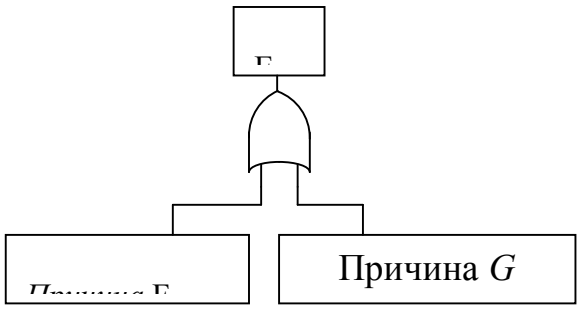
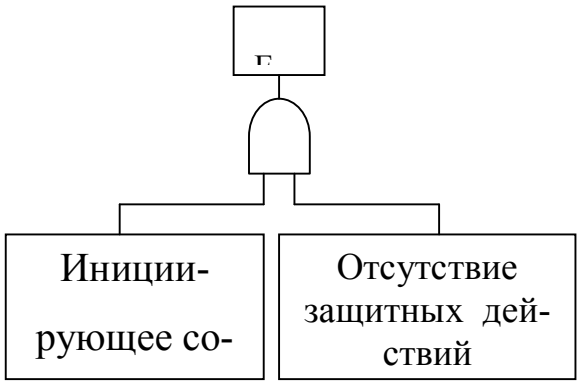
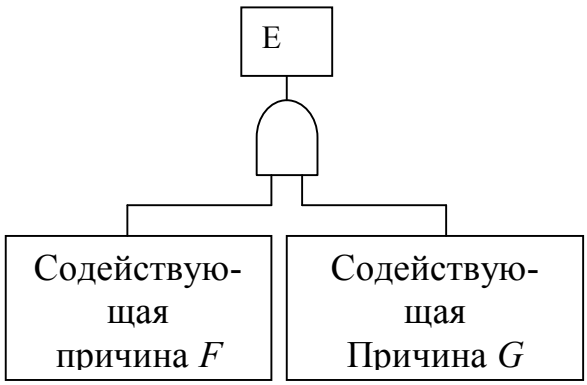
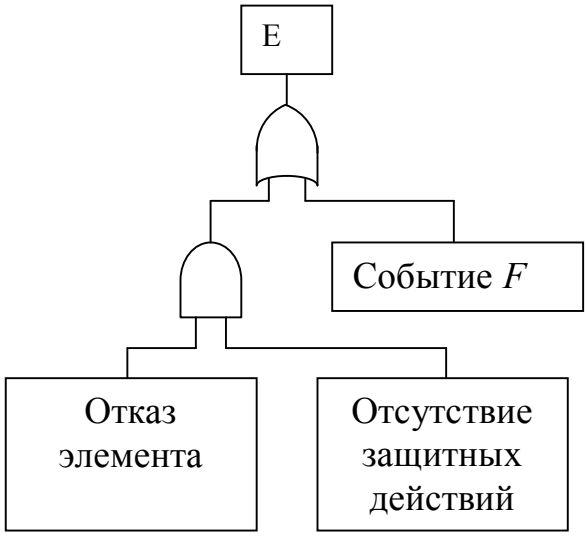


Рис. 8.7. Разработка отказа элемента (событие "состояние элемента")

Таблица 8.2 Эвристические правила для построения дерева отказов

Строка	Принципы построения	Соответствующая часть дерева отказов
1	2	3
1	Эквивалентное, но менее абстрактное событие	
2	Более детальное разбиение события	
3	Явно выраженные причины события	
4	Инициирующее событие при отсутствии защитных действий	

Продолжение табл.8.2

1	2	3
5	Совместно действующие причины	
6	Точное указание отказавшего элемента	

8.2 Допустимый индивидуальный и социальный риск в системе обеспечения пожарной безопасности и взрывобезопасности опасных технологий согласно нормам пожарной безопасности НПБ 105-03

1. Оценку пожарной безопасности технологических процессов повышенной пожарной опасности осуществляют с помощью критериев:

- индивидуального риска;
- социального риска;
- регламентированных параметров пожарной опасности технологических процессов.

2. Пожарная безопасность технологических процессов считается безусловно выполненной, если:

- индивидуальный риск меньше 10^{-8};

- социальный риск меньше 10^{-7}.

Эксплуатация технологических процессов является недопустимой, если индивидуальный риск больше 10^{-6} или социальный риск больше 10^{-5}.

Эксплуатация технологических процессов при промежуточных значениях риска может быть допущена после проведения дополнительного обоснования, в котором будет показано, что предприняты все возможные и достаточные меры для уменьшения пожарной опасности.

3 Оценку пожарной опасности технологических процессов следует проводить на основе оценки их риска.

В случае невозможности проведения такой оценки (например, из-за отсутствия необходимых данных) допускается использование иных критериев пожарной безопасности технологических процессов (допустимых значений параметров этих процессов).

В этом случае действие требований 2 на оценку пожарной опасности технологических процессов не распространяется.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Основная литература

1. Белов, С.В. Безопасность жизнедеятельности: учебник для вузов / С.В.Белов [и др.]; под ред. С.В. Белова. – 5-е изд., испр. и доп. – М.: Высш. шк., 2005. – 606 с.: ил.
2. Русак, О.Н. Безопасность жизнедеятельности: учеб. пособие для вузов / О.Н. Русак, К.Р. Малаян, Н.Г. Занько. – 9-е изд., стер. – СПб. [и др.]: Лань: Омега-Л, 2005. – 448 с.: ил.

2 Дополнительная литература

1. Федосова, Р.Н. Управление рисками промышленного предприятия: опыт и рекомендации / Р.Н. Федосова, О.Г. Крюкова. – М.: Экономика, 2008. – 125 с.
2. Михайлов, Л.А. Безопасность жизнедеятельности: учебник для вузов / Л.А. Михайлов [и др.]; под ред. Л.А. Михайлова: Питер, 2006. – 302 с.
3. Алымов, В.Т. Техногенный риск: Анализ и оценка: учеб. пособие для вузов / В.Т. Алымов, Н.П. Тарасова. – М.: Академкнига, 2004. – 118 с.: ил.

3 Периодические издания

1. Безопасность труда в промышленности/Журнал.

4 Программное обеспечение и Интернет-ресурсы

Общесистемное и прикладное программное обеспечение, базы данных, информационно-справочные и поисковые системы – Интернет ресурсы, отвечающие тематике дисциплины, например:

1. Российская академия наук. – Режим доступа: http://www.ras.ru/.
2. Российский общеобразовательный портал Министерство образования и науки РФ. Система Федеральных образовательных порталов. – Режим доступа: http://www.school.edu.ru/default.asp.
3. Единое окно доступа к образовательным ресурсам. Профессиональное образование / – Режим доступа: http://window.edu.ru/window/catalog p_rubr=2.2.81