

**ЛЕКЦИИ ПО КУРСУ**  
**«Надежность и диагностика машин и оборудования нефтегазовых промыслов»**

ВВЕДЕНИЕ .....	2
ЛЕКЦИЯ 1. ТЕХНОГЕННЫЙ РИСК И КОНЦЕПЦИЯ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ ТС.....	3
ЛЕКЦИЯ 2 ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ ТЕОРИИ НАДЕЖНОСТИ.....	11
ЛЕКЦИЯ 3 ПОКАЗАТЕЛИ НАДЕЖНОСТИ И БЕЗОПАСНОСТИ ТЕХНИЧЕСКОЙ СИСТЕМЫ .....	15
ЛЕКЦИЯ №4 СТРУКТУРНЫЕ МОДЕЛИ НАДЕЖНОСТИ СЛОЖНЫХ СИСТЕМ.....	21
ЛЕКЦИЯ 5 РАСЧЕТ НАДЕЖНОСТИ ТЕХНИЧЕСКИХ СИСТЕМ.....	28
ЛЕКЦИЯ 6. ОСНОВНЫЕ МЕТОДИКИ ОЦЕНКИ ОПАСНОСТЕЙ .....	31
ЛЕКЦИЯ 7 . ПРОЦЕДУРА ПРОВЕДЕНИЯ АНАЛИЗА НАДЕЖНОСТИ ТЕХНИЧЕСКОГО ОБЪЕКТА (ТО).....	38
ЛЕКЦИЯ 8. ОСНОВНЫЕ НАПРАВЛЕНИЯ, МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ НАДЕЖНОСТИ И БЕЗОПАСНОСТИ ТЕХНИЧЕСКИХ СИСТЕМ.....	43
ЛЕКЦИЯ 9 ДИАГНОСТИКА ОПАСНЫХ СИТУАЦИЙ В ТЕХНИЧЕСКИХ СИСТЕМАХ .....	50

## **ВВЕДЕНИЕ**

Безопасность является одной из наиболее социально-значимых характеристик деятельности производств, связанных с риском нанесения вреда людям, материальным ценностям, природе в ходе выполнения общественно полезных работ. Из этого следует необходимость тщательного изучения условий возникновения такого вреда, разработки и реализации мер по его минимизации. Причем, речь идет не только о проведении специальных исследований в этом вопросе, а о формировании так называемой культуры безопасности за счет передачи накапливаемых знаний широкому кругу специалистов.

Изучение курса «Надежность и диагностика технологических систем» имеет целью познакомить студентов с существующей концепцией управления безопасностью технологических систем на основе оценки рисков этой деятельности, представить сложившиеся методические приемы исследования рисков, порожденных отказами технических систем, показать роль человеческого фактора в природе техногенных катастроф.

Теоретические основы надежности включены в курс в том объеме, в котором они могут оказаться полезными при рассмотрении проблем управления безопасностью сложных человеко-машинных систем.

# Лекция 1. Техногенный риск и концепция управления безопасностью ТС

*Понятия «риск», «опасность». Классификация риска по объектам риска, основные классификационные признаки и источники риска. Анализ риска. Основные принципы и постулаты проведения анализа риска в целях управления безопасностью Цель и основные методы проведения оценки риска. Цель управления риском. Основные виды ущерба из-за реализации техногенных опасных факторов. «F/N диаграммы». Техногенный риск. Цели и формы моделирования процесса возникновения и развития техногенного риска*

## **Толкования понятий «риск», «опасность».**

В соответствии с современными взглядами **риск** обычно понимается как вероятностная мера возникновения опасных техногенных или природных явлений, а также характеристика размера нанесенного при этом социального, экономического, экологического и других видов ущерба и вреда.

Иными словами под риском следует понимать ожидаемую частоту или вероятность возникновения опасностей определенного класса, или же размер возможного ущерба (потерь, вреда) от нежелательного события, или же некоторую комбинацию этих величин.

Применение понятия риск позволяет переводить **опасность** в разряд измеряемых категорий. **Риск**, фактически, есть мера опасности. Часто используемое понятие "степень риска" (Level of risk), по сути, не отличается от понятия риск, но лишь подчеркивает, что речь идет об измеряемой величине.

Все интерпретации термина "риск" используются в настоящее время при анализе опасностей и управлении безопасностью (риском) технологических процессов.

Возникновение опасных ситуаций является результатом проявления определенной совокупности факторов риска, порождаемых теми или иными источниками, обстоятельствами, условиями. (примеры источников, обстоятельств, последствий .....)

## **Классификация риска по объектам риска, основные классификационные признаки и источники риска.**

Вид риска	Объект риска	Источник риска	Нежелательное событие
Индивидуальный	Человек	Условия жизнедеятельности человека	Заболевание, травма, инвалидность, смерть
Технический	Технические системы и объекты	Техническое несовершенство, нарушение правил эксплуатации - технических систем и объектов	Авария, взрыв, катастрофа, пожар, разрушение
Экологический	Экологические системы	Антропогенное вмешательство в природную среду, техногенные чрезвычайные ситуации	Антропогенные экологические катастрофы стихийные бедствия.
Социальный	Социальные группы	Чрезвычайная ситуация, снижение качества жизни	Групповые травмы, заболевания, гибель людей, рост смертности -
Экономический	Материальные ресурсы	Повышенная опасность производства или природной среды -	Увеличение затрат на безопасность, ущерб от недостаточной защищенности

**Технический риск** - комплексный показатель надежности элементов техносферы. Он выражает вероятность аварии или катастрофы при эксплуатации машин, механизмов, реализации технологических процессов:

$$R_T = \frac{\Delta T(t)}{T(f)}$$

где  $R_T$  - технический риск;  $\Delta T$  - число происшествий вследствие отказов техники в единицу времени  $t$  на идентичных технических системах и объектах;  $T$  - число идентичных технических систем и объектов, подверженных общему фактору риска  $f$ .

Источник ТР	Наиболее распространенные факторы технического риска
Низкий уровень научно-исследовательских работ	Ошибочный выбор направлений развития техники и технологии по критериям безопасности
То же. опытно-конструкторских работ	Выбор потенциально опасных конструктивных схем и принципов действия технически* систем. Ошибки в определении эксплуатационных нагрузок. Неправильный выбор конструкционных материалов. Недостаточный запас прочности. Отсутствие в проектах технических средств безопасности
Опытное производство новой техники	Некачественная доводка конструкций, технологии документации по критериям безопасности
Серийный выпуск небезопасной техники	Отклонение от заданного химического состава конструкционных материалов. Недостаточная точность конструктивных размеров. Нарушение режимов термической и химико-термической обработки деталей. Нарушение регламентов сборки и монтажа конструкций и машин
Нарушение правил безопасной эксплуатации технических систем	Использование техники не по назначению. Нарушение паспортных, проектных режимов эксплуатации. Несвоевременные профилактические осмотры и ремонты. Нарушение требований транспортирования и хранения
Ошибки персонала	Слабые навыки действий в сложной ситуации. Неумение оценивать информацию о состоянии процесса. Слабое знание сущности происходящего процесса. Отсутствие самообладания в условиях стресса. Недисциплинированность

### ***Анализ риска***

**Анализ риска или риск-анализ** (risk analysis) - процесс идентификации (выявления) опасностей и оценки риска для людей, материальных объектов, окружающей природной среды и др.

При этом под опасностью понимается источник потенциального ущерба или вреда или ситуация с возможностью нанесения ущерба, а под идентификацией опасности - процесс выявления ее, а также определение ее характеристик.

Анализ риска - субъективный процесс, в ходе которого учитываются не только количественные показатели, но и показатели, не поддающиеся формализации, такие, как позиции и мнения различных общественных групп, возможность компромиссных решений, экспертные оценки и т.д.

Особенность анализа технологического риска заключается в том, что в ходе его рассматриваются потенциально негативные последствия, которые могут возникнуть в результате отказа в работе технических систем, сбоев в технологических процессах или ошибок со стороны эксплуатационного персонала. Это не исключает необходимости рассмотрения негативных воздействий на людей и окружающую природную среду при безотказном функционировании производства в т.ч. технологической системы (за счет наличия вредных для здоровья людей примесей в воздухе, утечки вредных или опасных веществ, неочищенных стоков, воздействия солнечной радиации и т.д.).

### ***Общие положения анализа риска.***

Анализ риска имеет ряд общих положений независимо от конкретной природы изучаемых факторов риска, методики анализа и специфики решаемых задач.

*Во-первых*, общей является задача определения допустимого уровня риска, стандартов безопасности персонала, потребителей опасной продукции или услуг и защиты окружающей природной среды.

*Во-вторых*, определение уровня риска происходит, как правило, в условиях недостаточной или неточной (непроверенной) информации, особенно когда это касается новых технологических процессов или новой техники.

*В-третьих*, в ходе анализа обычно приходится решать вероятностные задачи, что может приводить к расхождениям в получаемых результатах.

*В-четвертых*, анализ риска нужно рассматривать, как процесс решения многокритериальных задач, которые обычно возникают из-за необходимости нахождения компромисса между сторонами, заинтересованными в определенных результатах анализа.

### ***Основные принципы и постулаты проведения анализа риска в целях управления безопасностью***

При проведении анализа уровня риска необходимо руководствоваться следующими принципами (или их сочетаниями):

- - принцип безусловного приоритета безопасности, сохранения жизни и здоровья над любыми другими критериями качества жизни людей;
- - принцип приемлемых опасности и риска, в соответствии с которым устанавливаются нижний (допустимый) и верхний (желаемый) уровни безопасности и в этом интервале — приемлемый уровень безопасности и риска с учетом социально-экономических факторов;
- - принцип минимальной опасности, в соответствии с которым уровень риска устанавливается настолько низким, насколько это реально достижимо в конкретных социально-экономических условиях;
- - принцип последовательного приближения к абсолютной безопасности.

В большинстве стран мирового сообщества в настоящее время принята концепция «приемлемого риска» (**ALARA** — as low as risk acceptable), позволяющая использовать принцип «предвидеть и предупредить». Эта общепризнанная концепция нашла отражение в четырех основных постулатах:

- первый постулат — оправданность деятельности по управлению риском, формулируется как стремление к обеспечению материальных и духовных благ при обязательном соблюдении условия: практическая деятельность не может быть оправдана, если выгода от этой деятельности в целом не превышает вызываемого ею ущерба.

- второй постулат — оптимизация защиты по критерию среднестатистической ожидаемой продолжительности предстоящей жизни в обществе. Оптимальным считается вариант сбалансированных затрат на продление жизни за счет снижения уровня риска и за счет выгоды, получаемой от хозяйственной деятельности.

- третий постулат — необходимость учета всего спектра существующих опасностей; вся информация о принимаемых решениях по управлению риском должна быть доступна широким слоям населения.

- четвертый постулат — учет требований о непревышении предельно допустимых экологических нагрузок на экосистемы. Он состоит в том, что обеспечение безопасности человека, живущего сегодня, следует достигать путем реализации таких решений, которые не снижают способность природы обеспечить безопасность и потребности человека будущего поколения.

### ***Цель и основные методы проведения оценки риска.***

С анализом риска тесно связан процесс оценки риска. Оценка риска это процесс, используемый для определения величины (меры) риска для здоровья человека, материальных ценностей, окружающей природной среды и других ситуаций, связанных с реализацией опасности. Оценка риска - обязательная часть анализа.

На этом этапе установленные опасности должны быть оценены ***с целью выделения опасностей с неприемлемым уровнем риска.*** Этап служит основой для разработки рекомендаций и принятия мер по уменьшению опасностей. При этом и критерии приемлемого риска, и результаты оценки риска могут быть выражены как качественно, так и количественно. Оценка риска включает в себя анализ частоты и анализ последствий.

Однако, когда последствия незначительны и частота крайне мала, достаточно оценить лишь один из указанных параметров.

### ***Существуют разные методы оценки риска.***

Первый из них - ***инженерный.*** Он опирается на статистику реализовавшихся опасностей, на вероятностный анализ безопасности, который обычно включает построение и расчет так называемых деревьев событий и деревьев отказов. С помощью первых прогнозируют возможные последствия развития той или иной опасности, а деревья отказов, наоборот, помогают проследить все причины, которые способны вызвать какое-то нежелательное событие. Когда деревья построены, рассчитывается вероятность реализации каждого из сценариев (каждой ветви), а затем - общая вероятность небезопасных событий в анализируемой системе.

Второй подход, ***модельный,*** - основан на рассмотрении моделей воздействия вредных факторов на человека и окружающую среду. Эти модели

могут оценивать воздействия как в ходе работы систем в штатном режиме, так и при возникновении в них особых ситуаций.

Оба подхода основаны на расчетах, однако, для таких расчетов далеко не всегда хватает надежных исходных данных. В этом случае приемлем третий подход - **экспертный**: вероятности различных событий, связи между ними и последствиями определяют не вычислениями, а опросом опытных специалистов.

Наконец, в рамках четвертого подхода - **социологического** - исследуется отношение людей к разным видам риска, например с помощью социологических опросов.

### ***Цель управления риском.***

Под термином «управление риском» понимается совокупность действий, направленных на **снижение уровня технологического риска, уменьшение потенциальных потерь и других негативных последствий** нежелательных событий. По сути дела, речь идет о предотвращении возникновения происшествий в ходе производственной деятельности и мерах по локализации негативных последствий в тех случаях, когда нежелательные события произошли.

### ***Основные виды ущерба из-за реализации техногенных опасных факторов.***

Последствия неблагоприятных событий можно разделить на три группы ущерба: • причинение ущерба жизни и здоровью людей; • экономические ущербы: —из-за повреждения и разрушения технических объектов, включая объекты авиационной инфраструктуры; —косвенные убытки из-за выхода их из эксплуатации и остановки производства; • ущерб и неблагоприятные последствия для окружающей среды.

При рассмотрении социальных, экономических и экологических сторон неблагоприятных событий целесообразно оперировать понятиями прямого, косвенного и полного ущерба.

### ***Общность и различие процедур оценки и управления риском.***

**Общим** в оценке риска и управлении риском является то, что они представляют собой две стадии единого процесса управления безопасностью деятельности. Целью этой деятельности является определение приоритетов действий, направленных на уменьшение риска до приемлемой величины. Это становится возможным, когда известны как источники опасности - (анализ риска), так и наиболее эффективные пути их устранения или локализации (управлением риском).

Основное различие между двумя понятиями заключается в том, что оценка риска строится на естественнонаучном и инженерном изучении источника (например, надежность воздушного судна) и факторов риска (например, техническое обслуживание ВС) и механизма взаимодействия между ними.

### ***Причины перехода от концепции «абсолютной безопасности» к концепции «приемлемого риска».***

Традиционный подход к обеспечению безопасности при эксплуатации технических систем и технологий базируется на концепции "абсолютной

безопасности" – ALAPA (аббревиатура от "As Low As PracticabLe AchievabLe": "настолько низко, насколько это достижимо практически"). То есть внедрение всех мер защиты, которые практически осуществимы. Как показывает практика, такая концепция неадекватна законам техносферы. Эти законы имеют вероятностный характер, и абсолютная безопасность достигается лишь в системах, лишенных запасенной энергии. Требование абсолютной безопасности, подкупающее своей гуманностью, оборачивается трагедией для людей, потому что обеспечить нулевой риск в действующих системах невозможно, и человек должен быть ориентирован на возможность возникновения опасной ситуации, т.е. ориентирован на соответствующий риск.

В настоящее время на смену концепции абсолютной безопасности пришла концепция "приемлемого" (допустимого) риска. Это понятие произошло от принятого в современной научной литературе термина "принцип приемлемого риска", известного как принцип ALAR (аббревиатура от "As Low As ReasonabLe AchievabLe": "настолько низко насколько это достижимо в пределах разумного", учитывая социальные экономические факторы). То есть если нельзя создать абсолютно безопасные технологии, обеспечить абсолютную безопасность, то, очевидно, следует стремиться к достижению, хотя бы такого уровня риска, с которым общество в данный период времени может согласиться.

### 1.12. Цели построения «F/N диаграмм».

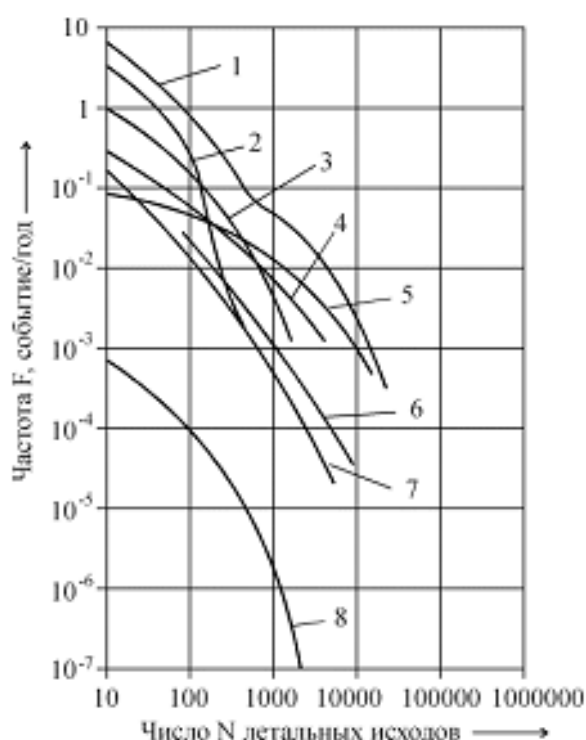


Рис. 1.1 Частота и количество катастроф связанных с техникой 1 - суммарная кривая; 2 - общее число катастроф ВС; 3 - пожары; 4 - взрывы; 5 – прорывы плотины; 6 - выбросы вредных химических веществ; 7 – катастрофы самолетов (без пассажиров); 8 - 100 атомных реакторов

Ключевое значение в установлении границ допустимого риска получила идея, предложенная Фармером в 1967 году. Смысл ее заключался в установлении зависимости между средним количеством нежелательных (небезопасных) событий и вероятностью (средняя частота в год) их наступления. Примером использования таких диаграмм могут служить графики (см. рис.1.1), на которых подобные зависимости применяются для сравнения различных техногенных и природных опасностей. За такими графиками закрепилось название "F/N - диаграмма".

Подобные графики с горизонтальной осью N - "число событий со смертельным исходом" и вертикальной осью F - "частота событий" в случае, если количество данных и диапазон их изменений очень велик, обычно строятся в логарифмическом масштабе. Они могут быть аппроксимированы непрерывной функцией.



### ***Основные условия возникновения техногенного риска.***

Риск летального исхода существует на уровне  $10^{-7}$  и выше на человека в год. Таким образом, при проектировании и эксплуатации технических устройств риск на уровне  $10^{-7}$  чел/год может быть принят допустимым **при следующих условиях:** - проблема риска проанализирована глубоко и всесторонне; - анализ проведен до принятия решений и подтвержден имеющимися статистическими данными в определенном временном интервале; - после наступления неблагоприятного события анализ и заключение о риске, полученные на основании имевшихся данных, не меняются; - анализ показывает, и результаты контроля все время подтверждают, что угроза не может быть уменьшена ценой оправданных затрат.

### ***Цели и формы моделирования процесса возникновения и развития техногенного риска***

Для оценки динамики возникновения и развития причин происшествий, прогнозирования их последствий обычно требуется создавать математические модели, позволяющие осмыслить поведение технической системы и с ее помощью оценить различные стратегии риска. Модель должна отражать важнейшие черты явления, т. е. в ней должны быть учтены все существенные факторы, от которых в наибольшей степени зависит функционирование системы. Вместе с тем она должна быть по возможности простой и понятной пользователю, целенаправленной, надежной (гарантия от абсурдных ответов), удобной в управлении и обращении, достаточно полной, адекватной, позволяющей легко переходить к другим модификациям и обновлению данных.

При построении математической модели может быть использован математический аппарат различной сложности - алгебраические и дифференциальные уравнения, как обыкновенные, так и с частными производными. В наиболее трудных случаях, если функционирование системы зависит от большого числа сложно сочетающихся между собой случайных факторов, может применяться метод статистического моделирования.

**Моделирование социального риска.** Социальный риск - зависимость частоты возникновения событий, вызывающих ущерб определенного масштаба, от масштаба ущерба. Результаты анализа изображаются в виде графиков (так называемых F—N диаграмм). Социальный риск  $R = F(N)$  характеризует масштаб реализации возможных опасностей. Социальный риск может быть рассчитан по формуле

$$R_c(N) = \sum_{m=1}^M \sum_{i=1}^I P(N/Q_m) P(Q_m/A_i) F(A_i)$$

где  $P(N/Q_m)$ — вероятность гибели (травмирования)  $N$  людей от  $Q_m$ -го фактора угрозы;  $P(Q_m/A_i)$  - вероятность возникновения  $Q_m$ -го фактора угрозы при реализации  $A_i$  -го события (аварии, опасного природного явления, катастрофы, стихийного или иного бедствия).

Для оценки риска происшествий, наряду с аналитическими методами, представляется возможным использование метода Монте-Карло. Большинство методов, используемых при анализе рисков, позволяют решать вероятностные проблемы, сводя их к задачам теории вероятностей и математического анализа, решение которых, в свою очередь, можно получить аналитически или численно. Метод Монте-Карло, называемый также методом статистического моделирования, позволяет решать вероятностные проблемы статистическими средствами.

## ЛЕКЦИЯ 2 ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ ТЕОРИИ НАДЕЖНОСТИ

*Надежность, безотказность, долговечность, ремонтпригодность, сохраняемость технических систем. Классификация состояний технического объекта. Виды надежности. Отказы объекта и их классификация.*

Применительно к опасным промышленным и транспортным объектам целесообразно рассматривать проблемы безопасности как проблемы надежности сложных человеко-машинных систем по отношению к здоровью и жизни людей, состоянию окружающей среды.

Во-первых, при определенных условиях эти понятия тесно связаны (например, когда нарушение работоспособного состояния технических элементов системы может привести к аварийным или катастрофическим последствиям). Во-вторых, такой подход позволяет использовать количественные показатели безопасности, подобные в математическом отношении принятым показателям теории надежности, методы которой разработаны достаточно полно и широко используются на практике.

При этом вводится понятие «технический риск» (или функция риска) как дополнение до единицы функции безопасности, определяемой по аналогии с функцией надежности как вероятностью безопасной работы. Технический риск не включает измерение размеров потерь или ущерба, эта характеристика позволяет оценивать вероятность критического (опасного) отказа.

**Надежность** - свойство объекта сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, ремонтов, хранения и транспортировки. К параметрам, характеризующим способность выполнять требуемые функции, относят геометрические, кинематические и динамические параметры, показатели конструкционной прочности, показатели точности функционирования, производительности, скорости и т. п. С течением времени значения этих параметров могут изменяться, характеризуя то или иное состояние объекта.

### ***Свойства технической системы***

Надежность - комплексное свойство, определяемое через ***безотказность, долговечность, ремонтпригодность, сохраняемость*** технических систем. Для конкретных объектов и условий их эксплуатации эти свойства могут иметь различную значимость.

**Безотказность** - свойство объекта непрерывно сохранять работоспособность в течение некоторой наработки или в течение некоторого времени.

**Ремонтпригодность** - свойство объекта быть приспособленным к предупреждению и обнаружению отказов и повреждений, к восстановлению работоспособности и исправности в процессе технического обслуживания и ремонта.

**Долговечность** - свойство объекта сохранять работоспособность до наступления предельного состояния с необходимым прерыванием для технического обслуживания и ремонтов.

**Сохраняемость** - свойство объекта непрерывно сохранять исправное и работоспособное состояние в течение (и после) хранения и (или) транспортировки.

**Наработка** — продолжительность или объем работы объекта. Нарботка может быть как непрерывной величиной (продолжительность работы в часах) так и целочисленной величиной (число рабочих циклов, запусков, полетов и т.п.).

**Наработка до отказа** — наработка объекта от начала эксплуатации до возникновения первого отказа.

**Ресурс** — суммарная наработка объекта от начала его эксплуатации или ее возобновления после ремонта до перехода в предельное состояние.

**Срок службы** — календарная продолжительность эксплуатации от начала эксплуатации объекта или ее возобновления после ремонта до перехода в предельное состояние.

**Остаточный ресурс** — суммарная наработка объекта от момента контроля его технического состояния до перехода в предельное состояние. Аналогично вводятся понятия «остаточная наработка до отказа» и «остаточный срок службы».

**Назначенный ресурс** - суммарная наработка, при достижении которой эксплуатация объекта должна быть прекращена независимо от его технического состояния.

**Назначенный срок службы** — календарная продолжительность эксплуатации, при достижении которой эксплуатация объекта должна быть прекращена независимо от его технического состояния.

### ***Классификация состояний технического объекта***

В теории надежности обычно рассматриваются ***исправное, неисправное, работоспособное, неработоспособное*** и ***предельное*** состояния.

**Исправное состояние** (исправность) — состояние объекта, при котором он соответствует всем требованиям нормативно-технической и (или) конструкторской (проектной) документации.

**Неисправное состояние** (неисправность) — состояние объекта, при котором он не соответствует хотя бы одному из требований нормативно-технической и (или) конструкторской (проектной) документации.

**Работоспособное состояние** (работоспособность) — состояние объекта, при котором значения всех параметров, характеризующих способность выполнять заданные функции, соответствуют нормативно-технической (проектной) документации.

**Неработоспособное состояние** (неработоспособность) — состояние объекта, при котором значение хотя бы одного параметра, характеризующего способность выполнять заданные функции, не соответствует требованиям нормативно-технической и (или) конструкторской (проектной) документации.

**Предельное состояние** — состояние объекта, при котором его дальнейшая эксплуатация недопустима или нецелесообразна либо восстановление его работоспособного состояния невозможно или нецелесообразно. Критерий предельного состояния — признак или совокупность признаков предельного состояния объекта, установленные нормативно-технической и (или) конструкторской (проектной) документацией. В зависимости от условий эксплуатации и назначения для одного и того же объекта могут быть установлены различные критерии предельного состояния.

### ***Виды надежности***

Многоцелевое назначение оборудования и систем приводит к необходимости исследовать те или другие стороны надежности с учетом причин, формирующих надежность объектов. Это приводит к необходимости подразделения надежности на виды. Различают:

- **аппаратурную надежность**, обусловленную состоянием технических элементов сложных систем; в свою очередь она может подразделяться на надежность конструктивную, схемную, производственно-технологическую;
- **функциональную надежность**, связанную с выполнением некоторой функции (либо комплекса функций), возлагаемых на объект, систему;
- **эксплуатационную надежность**, обусловленную качеством использования и обслуживания;
- **программную надежность**, обусловленную качеством программного обеспечения (программ, алгоритмов действий, инструкций и т.д.);
- **надежность системы "человек-машина"**, зависящую от характеристик взаимодействия человека-оператора и технического устройства.

### ***Отказы объекта и их классификация***

Одним из основных понятий теории надежности является понятие отказа (объекта, элемента, системы). Ошибка оператора может также рассматриваться как отказ функционального элемента сложной полиэнергетической (человеко-машинной) системы.

Отказ объекта - событие, заключающееся в том, что объект полностью или частично перестает выполнять заданные функции. При полной потере работоспособности возникает **полный отказ**, при частичной - **частичный**.

Понятия полного и частичного отказов каждый раз должны быть четко сформулированы перед анализом надежности, поскольку от этого зависит количественная оценка надежности.

По **причинам возникновения** отказов различают:

- отказы из-за конструктивных дефектов;
- отказы из-за технологических дефектов;
- отказы из-за эксплуатационных дефектов;
- отказы из-за постепенного старения (износа).

Отказы по **причинным схемам возникновения** подразделяются на следующие группы:

- отказы с мгновенной схемой возникновения;
- отказы с постепенной схемой возникновения;
- отказы с релаксационной схемой возникновения;

- отказы с комбинированными схемами возникновения.

**По времени развития и степени предсказуемости** отказы подразделяются на внезапные и постепенные.

**По характеру устранения с течением времени** различают устойчивые (окончательные) и самоустраниющиеся (кратковременные) отказы. Кратковременный отказ называется сбоем. Характерным признаком сбоя является то, что восстановление работоспособности после его возникновения не требует ремонта системы. Примером может служить кратковременно действующая помеха при приеме сигнала связного оборудования, дефекты программы навигационного комплекса и т.п.

Отказы могут возникать в результате: первичных отказов; вторичных отказов; ошибочных команд (инициированные отказы).

**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, значение которых находится в пределах, лежащих в расчетном диапазоне, а отказы объясняются естественным старением элементов.

**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 действия этих напряжений могут выходить за пределы допусков и вызываются различными источниками энергии: термической, механической, электрической, химической, магнитной, радиоактивной и т.п. Эти напряжения вызываются соседними элементами или окружающей средой, например - метеорологическими (ливень, ветровая нагрузка), воздействием со стороны других технических систем.

**Инициированные отказы** (ошибочные и ложные команды). Люди, например, операторы и обслуживающий технический персонал, также являются возможными источниками вторичных отказов, если их действия приводят к выходу элементов из строя. Ошибочные и ложные команды представляются в виде элемента, находящегося в нерабочем состоянии из-за выработки неправильного сигнала управления или помех.

**Критерии отказа** — признак или совокупность признаков нарушения работоспособного состояния объекта, установленные в нормативно-технической и (или) конструкторской (проектной) документации.

**Причина отказа** — явления, процессы, события и состояния, вызвавшие возникновение отказа объекта.

**Последствие отказа** - явления, процессы, события и состояния, обусловленные возникновением отказа объекта.

**Критичность отказа** - совокупность признаков, характеризующих последствия отказа.

**Повреждение** — событие, заключающееся в нарушении исправного состояния объекта при сохранении его работоспособного состояния.

## ЛЕКЦИЯ 3 ПОКАЗАТЕЛИ НАДЕЖНОСТИ И БЕЗОПАСНОСТИ ТЕХНИЧЕСКОЙ СИСТЕМЫ

*Вероятность безотказной работы, функция надежности, срок службы, функция безопасности, интенсивность отказов, средний ресурс, Связь между показателями безопасности и технического риска.*

К показателям надежности и безопасности относят количественные характеристики, которые вводят и определяют согласно правилам теории надежности, теории вероятностей и математической статистики. Область применения этих теорий ограничена крупносерийными объектами, которые изготавливают и эксплуатируют в статистически однородных условиях и к совокупности которых применимо статистическое истолкование вероятности.

Применение статистической теории надежности к уникальным и малосерийным объектам (такowymi являются, как правило, потенциально опасные производственные и транспортные объекты) ограничено. Эта теория применима для единичных восстанавливаемых или ремонтируемых объектов, в которых допускаются многократные отказы, для описания которых применяют модель потока случайных событий (в том числе редких событий, когда проводится анализ критических или аварийных отказов). Статистическую теорию применяют также к уникальным и малосерийным объектам, которые, в свою очередь, состоят из объектов массового производства. В этом случае расчет показателей надежности и безопасности объекта проводят методами статистической теории по известным показателям надежности и безопасности компонентов и элементов.

Рассматривая отказ как случайное событие, *мерой надежности технических объектов признается вероятность безотказной работы* системы и, соответственно, *мерой безопасности - вероятность безаварийной работы*.

**Вероятность безотказной работы** — вероятность того, что в пределах заданной наработки отказ объекта не возникает.

Вероятность безотказной работы определяется в предположении, что в начальный момент времени (начало исчисления наработки) объект находился в работоспособном состоянии.

Обозначим через  $t$  время или наработку объекта. Возникновение первого отказа — случайное событие, а наработка от начального момента до возникновения этого события  $\tau$  - случайная величина. Вероятность безотказной работы объекта в интервале времени от 0 до  $t$  включительно определяют как

$$P(t) = P\{\tau > t\}.$$

Здесь  $P\{\tau > t\}$  — вероятность события, заключенного в скобки. Очевидно, что эта величина является функцией времени или наработки  $P(t)$ . В

технической литературе эту функцию называют **функцией надежности**. Аналогично можно определить вероятность безаварийной работы:

$$S(t) = S(T > t),$$

рассматривая происшествие как отказ из-за перехода объекта в предельное состояние (устанавливаемого из соображений безопасности), а наработку (или время) от начального момента до достижения предельного состояния как **ресурс Т (или срок службы)**. Функцию  $S(t)$  в этом случае называют (по аналогии с функцией надежности) **функцией безопасности**.

В более общем случае, когда состояние объекта характеризуется набором параметров, функция безопасности  $S(t)$  определяется вероятностью случайного события, состоящего в том, что на отрезке времени  $[0, t]$  ни разу не возникнет особая ситуация, вызванная отказом и приводящая к происшествию.

Функция безопасности  $S(t)$  связана с функцией распределения  $H(t)$  и плотностью распределения  $h(t)$  случайной величины  $T$  соотношениями

$$H(t) = 1 - S(t), \quad h(t) = dH(t)/dt = -dS(t)/dt.$$

Дополнение функции безопасности  $S(t)$  до единицы (т.е. функция распределения случайной величины  $T$  в теории вероятностей)

$$1 - S(t) = H(t)$$

в теории безопасности и риска называется функцией риска или **техническим риском**.

Эту функцию особенно удобно использовать применительно к отказам или совокупностям отказов, последствия которых представляют опасность для людей, окружающей среды, а также связаны с серьезным материальным и (или) моральным ущербом.

Статистическую оценку  $\hat{h}(t)$  для плотности распределения  $h(t)$  случайной величины  $T$  принимают в виде

$$\hat{h}(t) = \frac{n(t + \Delta t / 2) - n(t - \Delta t / 2)}{N \Delta t}$$

где  $N$  - число объектов, работоспособных в начальный момент времени;

$n(t + \Delta t / 2)$  — число объектов, переходящих в предельные состояния на отрезке от 0 до  $t + \Delta t / 2$ ;

$n(t - \Delta t / 2)$  — число объектов, переходящих в предельные состояния на отрезке от 0 до  $t - \Delta t / 2$ .

Время  $t$  при оценке риска происшествий обычно исчисляют в годах, поэтому величина  **$\hat{h}(t)$  имеет смысл годовой относительной частоты происшествий  $V(t)$** .

Показатели **средний ресурс, средний срок службы** равны математическим ожиданиям соответствующих случайных величин (ресурса, срока службы).

С учетом формул (2.2) средний ресурс вычисляют по формуле



$$T_c = \int_0^{\infty} t \cdot h(t) dt = \int_0^{\infty} [1 - H(t)] dt$$

**Интенсивность технического риска  $\lambda(t)$  (аналог интенсивности отказов в теории надежности)** определяют по формуле

$$\lambda(t) = h(t)/[1 - H(t)] = -S'(t)/S(t).$$

Отсюда, после преобразований, вероятность безаварийной работы на отрезке времени от начала эксплуатации до некоторого момента  $t$  определится по формуле

$$S(t) = S(0) \exp \left[ - \int_0^t \lambda(t_1) dt_1 \right]$$

Все вышеприведенные характеристики взаимосвязаны, что иллюстрируется таблице.

Таблица. Связь между показателями безопасности и технического риска

Показатель	S(t)	H(t)	h(t)	$\lambda(t)$
S(t)	-	$1 - H(t)$	$1 - \int_0^t h(t_1) dt_1$	$\exp \left[ - \int_0^t \lambda(t_1) dt_1 \right]$
H(t)	$1 - S(t)$	-	$\int_0^t h(t_1) dt_1$	$1 - \exp \left[ - \int_0^t \lambda(t_1) dt_1 \right]$
h(t)	$- S'(t)$	$H'(t)$	-	$\lambda(t) \exp \left[ - \int_0^t \lambda(t_1) dt_1 \right]$
$\lambda(t)$	$\frac{S'(t)}{S(t)}$	$\frac{H'(t)}{1 - H(t)}$	$\frac{h(t)}{1 - \int_0^t h(t_1) dt_1}$	-

Интенсивность технического риска  $\lambda(t)$  является важной характеристикой в теории безопасности, так как она определяет вероятность того, что после безотказной работы до момента времени  $t$  происшествие произойдет в последующем отрезке времени  $\Delta t$ .

Этот показатель и его приближенные статистические оценки широко используются при анализе безопасности и риска объектов в процессе эксплуатации.

Статистическую оценку для интенсивности технического риска принимают в виде

$$\hat{\lambda}(t) = \frac{n(t + \Delta t / 2) - n(t - \Delta t / 2)}{[N - n(t)]\Delta t}$$

Практически для оценки интенсивности риска  $\lambda(t)$  используют приближенные оценки исходя из того, что для высоконадежных систем  $S(t) \approx 1$ . Поэтому интенсивность риска приближенно равна плотности распределения ресурса, что приводит к следующим приближенным оценкам:

$$\lambda(t) \approx h(t) \approx \hat{h}(t) = \nu(t)$$

Так как время  $t$  при оценке риска обычно исчисляют в годах, то величина  $\lambda(t)$  **имеет** смысл годового технического риска и фактически имеет **значение** условно индивидуального риска **за** год. Таким образом, в случае редких событий условный индивидуальный риск (**годовой**) приближенно равен годовой относительной частоте происшествий.

В технической литературе имеются статистические данные по частотам и интенсивностям отказов (в том числе критическим), которые **могут** использоваться (с учетом их полноты и достоверности) для априорных и **прогнозных** оценок интенсивностей технических рисков и тем самым - индивидуальных рисков.

Можно использовать также средний годовой технический риск как отношение  $H(T)/T$ . Такие показатели безопасности нередко используются в авиации и атомной энергетике.

### **Определение количественных характеристик надежности по статистическим данным об отказах изделия**

*Вероятность безотказной работы* по статистическим данным об отказах оценивается выражением

$$P(t) = \frac{n(t)}{N} \quad (1)$$

где  $n(t)$  – число изделий, не отказавших к моменту времени  $t$ ;  $N$  – число изделий, поставленных на испытания;  $P(t)$  – статистическая оценка вероятности безотказной работы изделия.

Для *вероятности отказа* справедливо соотношение

$$q(t) = \frac{N - n(t)}{N} = 1 - P(t) \quad (2)$$

где  $N - n(t)$  – число изделий, отказавших к моменту времени  $t$ ;  $q(t)$  – статистическая оценка вероятности отказа изделия.

*Частота отказов* определяется выражением

$$f(t) = \frac{\Delta n(t)}{N \cdot \Delta t} \quad (3)$$

где  $\Delta n(t)$  – число отказавших изделий на участке времени  $(t, t + \Delta t)$ ;  $f(t)$  – статистическая оценка частоты отказов изделия;  $\Delta t$  – интервал времени.

Интенсивность отказов по статистическим данным об отказах определяется формулой

$$\lambda(t) = \frac{\Delta n(t)}{\Delta t \cdot n(t)} \quad (4)$$

где  $n(t)$  – среднее число изделий, не отказавших к моменту времени  $t$ ;  $\Delta n(t)$  – число отказавших изделий на участке времени  $(t, t+\Delta t)$ ;  $\lambda(t)$  – статистическая оценка интенсивности отказов изделия.

Среднее время безотказной работы изделия по статистическим данным оценивается выражением

$$m_t = \frac{1}{N} \sum_{i=1}^N t_i \quad (5)$$

где  $t_i$  – время безотказной работы  $i$ -го изделия;  $N$  – общее число изделий, поставленных на испытания;  $m_t$  – статистическая оценка среднего времени безотказной работы изделия.

Для определения  $m_t$  по формуле (5) необходимо знать моменты выхода из строя всех  $N$  изделий.

**Задача 1.** На испытание поставлено 1000 однотипных изделий, за 3000 час. отказало 80 изделий. Требуется определить вероятность безотказной работы  $P(t)$ , вероятность отказов  $q(t)$  для отрезка времени от начала эксплуатации до  $t = 3000$  час.

Решение. В данном случае  $N = 1000$ ;  $n(t) = 1000 - 80 = 920$ ;  $N - n(t) = 1000 - 920 = 80$ . По формулам (1) и (2) определяем

$$P^*(3000) = \frac{n(t)}{N} = \frac{920}{1000} = 0.92,$$

$$q^*(3000) = \frac{N - n(t)}{N} = \frac{80}{1000} = 0.08,$$

$$q^*(3000) = 1 - P^*(3000) = 1 - 0.92 = 0.08.$$

**Задача 2.** На испытание было поставлено 1000 изделий. За первые 3000 час. отказало 80 шт. изделий, а за интервал времени 3000÷4000 час. отказало еще 50 шт. Требуется определить статистическую оценку частоты и интенсивности отказов изделий в промежутке времени 3000÷4000 час.

Решение.  $N = 1000$ ;  $t = 3000$  час;

$$\Delta t = 4000 - 3000 = 1000 \text{ час};$$

$$\Delta n(t) = 50; \quad n(t) = 920.$$

По формулам (3) и (4) находим

$$f^*(t) = f^*(3000) = \frac{\Delta n(t)}{N \cdot \Delta t} = \frac{50}{1000 \cdot 1000} = 5 \cdot 10^{-5} \text{ 1 / час}$$

$$\lambda^*(t) = \lambda^*(3000) = \frac{\Delta n(t)}{\Delta t \cdot n(t)} = \frac{100}{100 \cdot 920} = 5 \cdot 10^{-3} \text{ 1/час}$$

**Задача 3.** На испытание поставлено  $N = 400$  изделий. За время  $t = 3000$  час отказало 200 изделий, т.е.  $n(t) = 400 - 200 = 200$ . За интервал времени  $(t, t + \Delta t)$ , где  $\Delta t = 100$  час, отказало 100 изделий, т.е.  $\Delta n(t) = 100$ . Требуется определить  $P^*(3000)$ ,  $P^*(3100)$ ,  $f^*(3000)$ ,  $\lambda^*(3000)$ .

Решение. По формуле (1) находим

$$P^*(3000) = \frac{n(t)}{N} = \frac{200}{400} = 0,5.$$

$$P^*(3100) = \frac{n(t)}{N} = \frac{100}{400} = 0,25.$$

Используя формулы (3) и (4), получим

$$f^*(t) = f^*(3000) = \frac{\Delta n(t)}{N \cdot \Delta t} = \frac{100}{400 \cdot 100} = 2,5 \cdot 10^{-3} \text{ (1/час)}$$

$$\lambda^*(t) = \lambda^*(3000) = \frac{\Delta n(t)}{\Delta t \cdot n(t)} = \frac{100}{100 \cdot 200} = 5 \cdot 10^{-3} \text{ (1/час)}$$

## ЛЕКЦИЯ №4 Структурные модели надежности сложных систем

*Сложная система; положительные и отрицательные свойства; группы элементов системы; последовательные, параллельные, смешанные системы; надежность системы, горячее холодное резервирование; поканальное и поэлементное резервирование; пример расчета смешанной системы*

Большинство технических систем являются сложными системами, состоящими из отдельных узлов, деталей, агрегатов, систем управления и т.п. ***Под сложной системой понимается объект, предназначенный для выполнения заданных функций, который может быть расчленен на элементы (компоненты), каждый из которых также выполняет определенные функции и находится во взаимодействии с другими элементами системы.***

С позиций надежности сложная система обладает как отрицательными, так и положительными свойствами.

Факторы, отрицательно влияющие на надежность сложных систем, следующие:

- во-первых, ***это большое число элементов, отказ каждого из которых может привести к отказу всей системы;***
- во-вторых, ***оценить работоспособность сложных систем весьма затруднительно с точки зрения статистических данных, т.к. они часто являются уникальными или имеются в небольших количествах;***
- в-третьих, даже у систем одинакового предназначения каждый экземпляр имеет свои незначительные вариации свойств отдельных элементов, что сказывается на выходных параметрах системы. **Чем сложнее система, тем большими индивидуальными особенностями она обладает.**

Однако сложные системы обладают и такими свойствами, которые положительно

влияют на их надежность:

- во-первых, сложным системам **свойственна самоорганизация, саморегулирование или самоприспособление, когда система способна найти наиболее устойчивое для своего функционирования состояние;**
- во-вторых, для сложной системы часто **возможно восстановление работоспособности по частям, без прекращения ее функционирования;**
- **в-третьих, не все элементы системы одинаково влияют на надежность сложной системы.**

Анализ работоспособности сложной системы связан с изучением ее структуры и тех взаимосвязей, которые определяют ее надежное функционирование.

**При анализе надежности сложных систем их разбивают на элементы (компоненты) с тем, чтобы вначале рассмотреть параметры и характеристики элементов, а затем оценить работоспособность всей системы. Под элементом можно понимать составную часть сложной**

системы, которая может характеризоваться самостоятельными входными и выходными параметрами. При исследовании надежности системы элемент не расчленяется на составные части, и показатели безотказности и долговечности относятся к элементу в целом. При этом возможно восстановление работоспособности элемента независимо от других частей и элементов системы.

Анализ надежности сложных систем имеет свои специфические особенности. Влияние различных отказов и снижение работоспособности элементов системы по-разному скажутся на надежности всей системы.

При анализе надежности сложной системы все ее элементы и компоненты целесообразно разделить на следующие группы.

1) Элементы, отказ которых практически не влияет на работоспособность системы (деформация ограждающего кожуха машины, изменение окраски поверхности и т.п.). Отказы (т.е. неисправное состояние) этих элементов могут рассматриваться изолированно от системы.

2) Элементы, работоспособность которых за рассматриваемый период времени практически не изменяется (станины и корпусные детали, малонагруженные элементы с большим запасом прочности).

3) Элементы, ремонт или регулировка которых возможна при работе изделия или во время остановок, не влияющих на его эффективность (подналадка и замена режущего инструмента на станке, регулировка холостого хода карбюратора автомобильного двигателя).

4) Элементы, отказ которых приводит к отказам системы.

Таким образом, рассмотрению и анализу надежности подлежат лишь элементы последней группы. Как правило, имеется ограниченное число элементов, которые в основном и определяют надежность изделия. Эти элементы и подсистемы выявляются при рассмотрении структурной схемы параметрической надежности.

Модели надежности устанавливают связь между подсистемами (или элементами системы) и их влиянием на работу всей системы.

Структурная схема надежности определяет функциональную взаимосвязь между работой подсистем (или элементов) в определенной последовательности. Эту схему составляют по принципу функционального назначения соответствующих подсистем (или элементов) при выполнении ими определенной части работы, выполняемой системой в целом.

Техническая система может быть сконструирована таким образом, что для успешного ее функционирования необходима исправная работа всех ее элементов. В этом случае ее называют последовательной системой.

Есть также системы, в которых при отказе одного элемента другой элемент способен выполнить его функции. Такую систему называют параллельной.

Очень часто системы обладают свойствами как параллельных, так и последовательных систем — системы со смешанным соединением. При расчете надежности необходимо исследовать действия системы, основываясь на ее функциональной структуре и используя вероятностные соотношения.

Такое исследование структуры позволяет выявить узкие места в конструкции системы с точки зрения ее надежности, а на этапе проектирования разработать конструктивные меры *по устранению подобных узких мест*. Например, можно заранее подсчитать, сколько резервных элементов необходимо для обеспечения заданного уровня надежности системы. Далее можно рассчитать надежность системы, построенной из элементов с известной надежностью, или наоборот, исходя из требования к надежности системы, предъявить требования к надежности элементов.

Рассмотрим систему, состоящую из двух или более элементов.

Пусть  $A$  — событие, состоящее в том, что система работает безотказно.

Пусть  $A_i$  ( $i=1, 2, \dots, n$ ) — события, состоящие в исправной работе всех элементов системы  $A$ . Далее предположим, что событие  $A$  имеет место тогда и только тогда, когда имеют место все события  $A_i$ , т.е. система исправна тогда и только тогда, когда исправны все ее элементы. В этом случае систему называют *последовательной системой*.

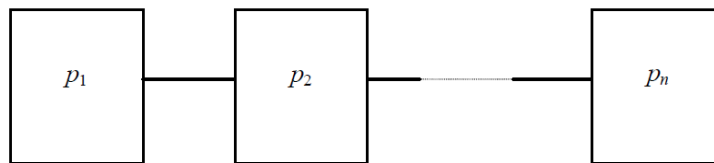


Рис. Структурная схема надежности системы с последовательным соединением элементов

Известно, что отказ любого элемента такой системы приводят, как правило, к отказу системы. Поэтому вероятность безотказной работы системы определяют как произведение вероятностей для *независимых событий*.

Таким образом, надежность всей системы равна произведению надежностей подсистем или элементов:

$$P(A) = \prod_{i=1}^n P(A_i)$$

Обозначив  $P(A) = P$ ;  $P(A_i) = p_i$ , получим

$$P = \prod_{i=1}^n p_i$$

где  $P$  — **надежность (вероятность безотказной работы) системы**.

Сложные системы, состоящие из элементов высокой надежности, могут обладать низкой надежностью за счет наличия большого числа элементов. Например, если узел состоит всего из 50 деталей, а вероятность безотказной работы каждой детали за выбранный промежуток времени составляет  $p_i = 0,99$ , то вероятность безотказной работы узла будет

$$P(t) = 0,99^{50} = 0,55.$$

Если же узел с аналогичной безотказностью элементов состоит из 400 деталей, то  $P(t) = 0,99^{400} = 0,018$ , т.е. узел становится практически неработоспособным.

**Пример 1.** Определить надежность автомобиля (системы) при движении на заданное расстояние, если известны надежности следующих подси-

стем: системы зажигания  $p_1 = 0,99$ ; системы питания топливом и смазкой  $p_2 = 0,999$ ; системы охлаждения  $p_3 = 0,998$ ; двигателя  $p_4 = 0,985$ ; ходовой части  $p_5 = 0,997$ .

Решение. Известно, что отказ любой подсистемы приводит к отказу автомобиля. Для определения надежности автомобиля используем формулу

$$P = p_1 p_2 p_3 p_4 p_5 = 0,99 \cdot 0,999 \cdot 0,998 \cdot 0,985 \cdot 0,997 = 0,979.$$

Ответ:  $P = 0,979$ .

В практике проектирования сложных технических систем часто используют схемы с *параллельным соединением элементов* (рис. 2.), которые построены таким образом, что отказ системы возможен лишь в случае, когда отказывают все ее элементы, т.е. система исправна, если исправен хотя бы один ее элемент. Такое соединение часто называют *резервированием*. В большинстве случаев резервирование оправдывает себя, несмотря на увеличение стоимости. Наиболее выгодным является *резервирование отдельных элементов*, которые непосредственно влияют на выполнение основной работы. При конструировании технических систем в зависимости от выполняемой системой задачи применяют горячее или холодное резервирование.

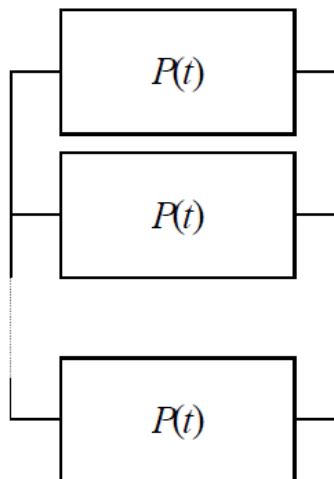


Рис. 2. Структурная схема надежности системы с параллельным соединением элементов

**Горячее резервирование** применяют тогда, когда не допускается прерыв в работе на переключение отказавшего элемента на резервный с целью выполнения задачи в установленное время. Чаще всего горячему резервированию подвергают отдельные элементы. Используют горячее резервирование элементов и подсистем, например источников питания (аккумуляторные батареи дублируются генератором и т.п.).

**Холодное резервирование** используют в тех случаях, когда необходимо увеличение ресурса работы элемента, и поэтому предусматривают **время на переключение отказавшего элемента на резервный**.

Существуют технические системы с *частично параллельным резервированием*, т. е. системы, которые оказываются работоспособными даже в случае отказа нескольких элементов.

Рассмотрим систему, имеющую ряд параллельных элементов с надежностью  $p(t)$  и соответственно ненадежностью  $q(t) = 1 - p(t)$ . В случае, если си-



стема содержит  $n$  элементов, которые соединены параллельно, вероятность отказа системы равна:

$$Q = [q(t)]^n,$$

а вероятность безотказной работы

$$P(t) = 1 - [q(t)]^n.$$

При частично параллельном резервировании вероятность безотказной работы системы, состоящей из общего числа элементов  $n$ , определяют по формуле:

$$P(t) = \sum_{k=j}^n C_n^k \cdot p(t)^k \cdot q(t)^{n-k}$$

где  $p(t)$  — вероятность безотказной работы одного элемента;  $j$  — число исправных элементов, при котором обеспечивается работоспособность системы;  $C_n^k = n!/[k!(n-k)!]$  — число сочетаний из  $n$  элементов по  $k$ .

В случае  $j = 1$  система будет полностью параллельной, в остальных случаях — частично параллельной.

Следует отметить, что в практике проектирования технических систем часто используют структурные схемы надежности с *параллельно-последовательным соединением* элементов. Так, например, часто при проектировании систем с радиоэлектронными элементами применяют схемы, работающие по принципу два из трех, когда работоспособность обеспечивается благодаря исправному состоянию любых двух элементов. Надежность такой схемы соединения определяют по формуле

$$P(t) = P^3(t) + 3P^2(t)Q(t).$$

где  $p(t)$  — надежность каждого элемента за время работы  $t$  одинакова;  $q(t) = 1 - p(t)$ .

Широкое применение в проектировании нашли так называемые *мостиковые схемы*. Надежность такой схемы определяют из соотношения вида

$$P(t) = p^5(t) + 5p^4(t)q(t) + 8p^3(t)q^2(t) + 2p^2(t)q^3(t).$$

Здесь все элементы также имеют одинаковую надежность.

Различают структурные схемы надежности с поканальным и поэлементным резервированием. Структурная схема надежности с поканальным резервированием показана на рис. 3.

Формула надежности выглядит так:

$$P = [1 - (1 - p_{11} p_{12} \dots p_{1n})(1 - p_{21} p_{22} \dots p_{2n}) \dots (1 - p_{k1} p_{k2} \dots p_{kn})]$$

При  $p_{ij} = p_j$   $P = 1 - (1 - p_1 p_2 \dots p_n)^k$

Если  $p_{ij} = p$ , то  $P = 1 - (1 - p^n)^k$

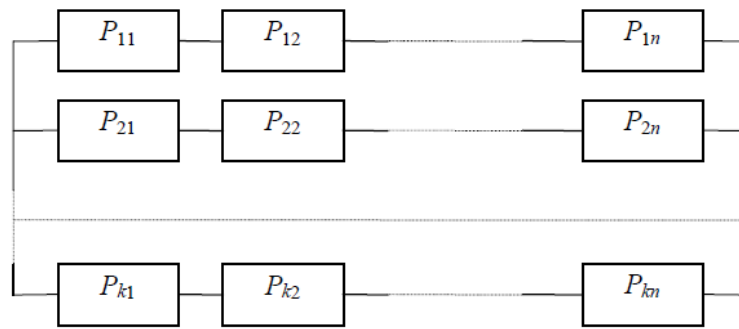


Рис.3. Структурная схема надежности с поканальным резервированием

В практике проектирования часто используют структурную схему надежности с поэлементным резервированием

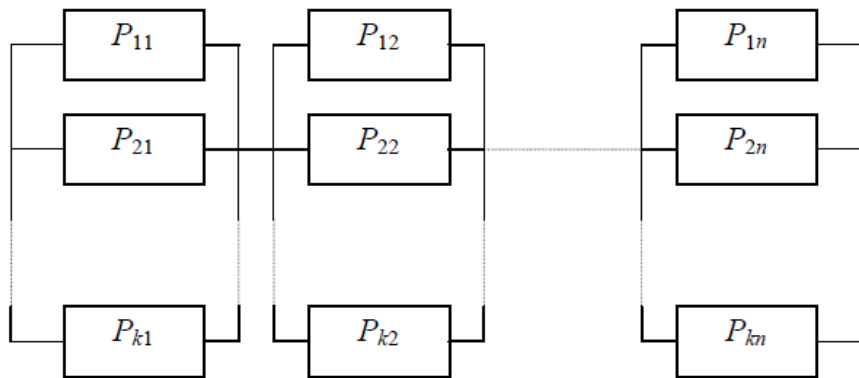


Рис.4. Надежность такой системы определяют по формуле:

$$P = [1 - (1 - p_{11})(1 - p_{21}) \dots (1 - p_{k1})][1 - (1 - p_{12})(1 - p_{22}) \dots (1 - p_{k2})] \dots [1 - (1 - p_{1n})(1 - p_{2n}) \dots (1 - p_{kn})].$$

При  $p_{ij} = p_j$   $P = [1 - (1 - p_1)^k][1 - (1 - p_2)^k] \dots [1 - (1 - p_n)^k].$

Если  $p_{ij} = p$ , то  $P = [1 - (1 - p)^k]^n.$

Анализ последних двух схем показывает, что структурная схема с поэлементным резервированием имеет более высокую надежность по сравнению с поканальным резервированием.

**Пример 2.** Техническая система предназначена для выполнения некоторой задачи. С целью обеспечения работоспособности система спроектирована со смешанным соединением элементов (рис. 5.).

Определить надежность системы, если известно, что надежность ее элементов равна:

$$p_1=0,99; p_2=0,98; p_3=0,9; p_4=0,95; p_5=0,9; p_6=0,9; p_7=0,8; p_8=0,75; p_9=0,7.$$

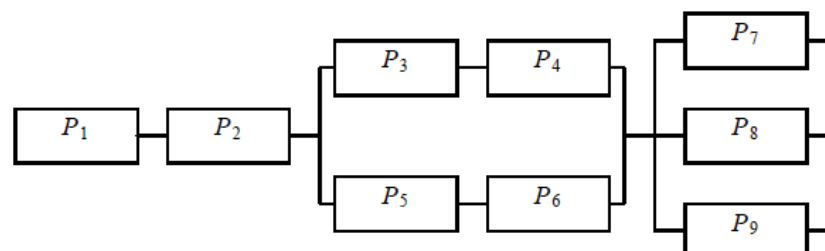


Рис.4. Структурная схема надежности технической системы

Решение. При расчете надежности воспользуемся формулами, как для последовательного, так и для параллельного соединения элементов:

$$P = p_1 p_2 [1 - (1 - p_3 p_4)(1 - p_5 p_6)] [1 - (1 - p_7)(1 - p_8)(1 - p_9)] = \\ = 0,99 \cdot 0,98 [1 - (1 - 0,9 \cdot 0,95)(1 - 0,9 \cdot 0,9)] [1 - (1 - 0,8)(1 - 0,75)(1 - 0,7)] = 0,927.$$

При расчете схемной надежности данную систему представляют в виде структурной схемы, в которой элементы, отказ которых приводит к отказу всей системы, изображаются последовательно, а резервные элементы или цепи – параллельно. Следует иметь в виду, что конструктивное оформление элементов, их последовательное или параллельное соединение в конструкции еще не означает аналогичного изображения в структурной схеме надежности.

## ЛЕКЦИЯ 5 РАСЧЕТ НАДЕЖНОСТИ ТЕХНИЧЕСКИХ СИСТЕМ

*Классификация расчетов надежности; Алгоритм расчета надежности; Формулировка задания на расчет надежности, Инженерные методы оценки опасностей, качественные и количественные методы анализа надежности систем.*

Расчеты надежности - расчеты, предназначенные для определения количественных показателей надежности. Они проводятся на различных этапах разработки, изготовления и эксплуатации объектов.

### ***Классификация расчетов надежности***

***На этапе проектирования*** расчет надежности производится с целью прогнозирования (предсказания) ожидаемой надежности проектируемой системы. Такое прогнозирование необходимо для обоснования предполагаемого проекта, а также для решения организационно-технических вопросов:

- выбора оптимального варианта структуры объекта;
- способа резервирования элементов;
- глубины и методов контроля;
- количества запасных элементов;
- периодичности профилактики.

***На этапе испытаний и эксплуатации*** расчеты надежности проводятся для оценки количественных показателей надежности. Такие расчеты носят, как правило, характер констатации. Результаты расчетов в этом случае показывают, какой надежностью обладали объекты, прошедшие испытания или используемые в некоторых определенных условиях эксплуатации. На основании этих расчетов разрабатываются меры по повышению надежности, определяются слабые места объекта, даются оценки его надежности и влияния на нее отдельных факторов.

Многочисленные цели расчетов привели к большому их разнообразию. На рисунке изображены основные виды расчетов.



Рис. 2.3 Классификация расчетов надежности

**Элементный расчет** - определение показателей надежности объекта, обусловленных надежностью его комплектующих частей (элементов). В результате такого расчета оценивается техническое состояние объекта (вероятность того, что объект будет находиться в работоспособном состоянии, средняя наработка на отказ и т.п.).

**Расчет функциональной надежности** - определение показателей надежности выполнения заданных функций (например, вероятность того, что система подачи топлива в двигатели будет работать заданное время, в заданных режимах эксплуатации с сохранением всех необходимых параметров топливообеспечения). Поскольку такие показатели зависят от ряда действующих факторов, то, как правило, расчет функциональной надежности более сложен, чем элементный расчет.

#### **Алгоритм расчета надежности**



**Рис. 2.4. Алгоритм расчета надежности**

Выбирая на рис 2.3 варианты перемещений по пути, указанному стрелками, могут быть получены новые виды расчета.

#### **Формулировка задания на расчет надежности**

Прежде всего, четко следует сформулировать задание на расчет надежности. В нем должны быть указаны:

- 1) назначение системы, ее состав и основные сведения о функционировании;

- 2) показатели надежности и признаки отказов, целевое назначение расчетов;
- 3) условия, в которых работает (или будет работать) система;
- 4) требования к точности и достоверности расчетов, к полноте учета действующих факторов.

На основании изучения задания делается вывод о характере предстоящих расчетов. В случае расчета функциональной надежности осуществляется переход к этапам 4-5-7, в случае расчета элементов (аппаратурной надежности) - к этапам 3-6-7.

**Инженерные методы оценки опасностей** могут быть основаны на качественном и количественном подходах. Качественный анализ, как правило, предшествует количественному. Идентификация (выявление) опасностей выполняется только на основе качественного их анализа. Обычно анализ проводится по результатам наблюдения за изучаемой системой (например, техническим состоянием ВС, или технологией работы экипажа). Задача - выделить опасности, нуждающиеся в более подробном рассмотрении. В любых видах деятельности, включая выполнение и обеспечение полетов, можно выявить источники повышенной опасности в т.ч. ненадежные компоненты технических систем.

В технике и технологиях встречаются разнообразные источники опасности и если они оказываются связанными со значительными запасами энергии, то опасные точки обнаружить относительно просто. Чаще всего это достигается **качественным анализом**.

Применение **количественных методов** анализа требует выбора критериев, как меры для сравнения количественных показателей исследуемых альтернатив решения проблемы в отношении затрачиваемых ресурсов и получаемых результатов (показатели типа "цена/качество").

## ЛЕКЦИЯ 6. Основные методики оценки опасностей

*Предварительный анализ опасностей; Методы проверочного листа (CHECK-LIST) и "что будет если ...?" ("WHAT - IF"); 5.3 Дерево отказов - ДО (fault tree analysis - FTA), Карта общего анализа опасностей; Граф дерева отказов; Логические символы взаимосвязей*

### ***Предварительный анализ опасностей***

Целью предварительного анализа опасностей (ПАО) является определение топографии (состава) системы, ее части или отдельного элемента, выявление потенциальных опасностей или опасных состояний, которые могут создавать система или ее элементы в ходе работы и которые могут привести к опасным событиям, т.е. определение той части системы, где требуется провести более подробный анализ.

В машиностроении риск происшествия, прежде всего, связан с бесконтрольным высвобождением энергии движущихся частей оборудования.

Поскольку одни части системы (воздушного судна, системы «экипаж-ВС» и т.д.) представляют большую опасность, чем другие, в самом начале анализа следует разбить систему или технологический процесс на подсистемы (этапы), для того чтобы выполнить предварительный анализ опасностей в следующей последовательности:

Шаг 1. Выявление потенциальных источников опасностей (системы, части системы или элементов), которые могут вызвать наступление неблагоприятных последствий.

Шаг 2. Определение степени опасности вероятных последствий - возможные пожары, взрывы, разрушение конструкции, утечки горючих веществ и т.д., в т.ч. тех которые маловероятны и ранее не приводили к происшествиям.

Шаг 3. Исключение из списка тех опасностей, проявление которых практически неосуществимо.

Процедура ПАО нередко включает в себя не только предварительное выявление элементов системы или событий, которые могут привести к опасным ситуациям. Задачи анализа расширяются с использованием количественных (формализованных) приемов сравнения, включением в рассмотрение последовательности событий, превращающих опасности в происшествия, а также корректирующих мероприятий (контрмер) для устранения опасности.

Таким образом, результатом ПАО будут: перечень опасностей, причинно-следственные цепочки наступления неблагоприятных последствий и корректирующие воздействия. На этой основе в дальнейшем разворачивается детальный количественный анализ. Другими словами - выявляются приоритеты и виды опасностей, которые следует рассматривать более подробно.

***Методы проверочного листа (CHECK-LIST) и "что будет если ...?" ("WHAT - IF")***

Эти методы, способствуют выявлению на практике критических точек системы, способных вызвать отказ системы (элемента) или обусловить аварийное состояние технологического процесса. Эти методы (чаще - их комби-

нация) относятся к группе качественных методов оценки опасности, основанных на изучении соответствия условий эксплуатации системы (объекта) действующим требованиям безопасности. Они дают представление об отклонении от нормы и могут служить основой для более подробных (в т.ч. и количественных) методов анализа, позволяют выработать корректирующие воздействия не только в отношении условий эксплуатации, но и внести коррективы в содержание технологического процесса или модернизировать конструкцию системы. Метод использует промежуточные признаки состояния системы и способствует предотвращению опасных событий.

На рис. 6.1 приводится схема использования промежуточных признаков для предотвращения развития опасной ситуации, приводящей к происшествию. В методическом плане эту схему можно применить к любому технологическому процессу.



Рис 6.1 Методика использования промежуточных признаков для предотвращения происшествий

Метод проверочного листа отличается от "Что будет, если...?" более обширным представлением исходной информации и результатов о последствиях нарушений безопасности. Исследование безопасности существенно упростится, если процесс исследования обеспечить вспомогательными формами, унифицированными бланками, облегчающими на практике сбор информации, проведение анализа и представление результатов. Методы недороги и наиболее эффективны при исследовании безопасности хорошо изученных объектов с известной технологией эксплуатации или объектов с незначительным риском крупных происшествий.

Примером тому могут служить карты контрольных проверок, широко используемые в различных технологических процессах при эксплуатации (технической и летной) авиационной техники.

В каждом конкретном случае используются собственные признаки. Опытный специалист по безопасности может заметить промежуточный признак, который не виден лицу, эксплуатирующему оборудование, так же как и оператор технической системы или технолог могут увидеть отклонения от нормы, которые не понятны специалисту по безопасности. Например, в качестве промежуточного признака может выступать повышенная вибрация, шум в отдельных частях агрегата и др. Форма проверочного листа - перечень вопросов и ответов о соответствии исследуемой системы требованиям безопасности и указания по обеспечению безопасности (контрмеры).



Описание каждой из контролируемых опасностей следует заносить в карту (табл. 6.1).

Таблица 6.1. Карта общего анализа опасностей

Подготовил _____ Дата _____			
Описание опасности _____			
Участок системы _____			
Серьезность	Вероятность	Затраты	Действия
Вызывающая беспокойство	Небольшая	Допустимые	Несрочные
Предельно допустимая	Умеренная	Предельные	Анализ
Критическая	Значительная	Значительные	Немедленные
Катастрофическая			

На карте проставляется дата, что дает возможность устанавливать хронологию выявления (развития) опасностей, указывается элемент системы, что дает возможность проследить топографию опасностей. Остальная часть разбита на четыре рубрики. Каждая из них представлена несколькими категориями. Категории располагаются так, что те из них, которые требуют наибольшего внимания, находятся внизу перечня. Например, если серьезность опасности катастрофическая, вероятность происшествия - неминуемое, а затраты - номинальные, то необходимо немедленное корректирующее действие.

Детальный анализ проводится по совокупности собранных контрольных карт и состоит в следующем:

1. Опасности систематизируются по месту и времени действия в технологической операции, что позволяет лучше оценить серьезность и продолжительность опасности.
2. Выявляются изначальные причины возникновения опасности, (вместо использования промежуточных признаков выявляемых на этапе общего анализа).
3. Подробно оценивается влияния контрмер, что трудно сделать в общем анализе.
4. Прослеживается влияние каждой контрмеры на все элементы системы с целью выявления таких состояний системы, при которых опасность происшествия возрастает из-за негативного влияния корректирующих мер на работу других элементов системы.

Следующий этап детального анализа - матричное представление результатов анализа. Его цель - представить информацию о затратах и эффективности контрмер в сжатой и логичной форме. При этом информация не обрабатывается, не формализуется, а только лишь представляется в удобном виде для принятия правильного решения. Как правило, производится сравнение альтернативных вариантов контрмер и различных типов опасностей.

В матрице элементы опасности, выявленные в ходе детального анализа, располагаются в порядке важности. Альтернативные варианты указываются в вертикальном столбце и тут же указываются затраты на данную контрмеру. В поле матрицы в местах пересечения опасностей и контрмер указываются

символы: "-" - устранение элемента опасности, R - снижение опасности, X - опасность не изменилась, I - опасность увеличилась.

Экономическая эффективность мероприятий представляет собой дополнительную переменную, определенную в ходе детального анализа. Матричное представление не гарантирует оптимальность решения, поскольку предназначено только для облегчения процесса принятия управленческого решения за счет упорядочения результатов качественной оценки опасностей.

### ***Дерево отказов - ДО (fault tree analysis - FTA)***

Анализу причин отказов и выработке мероприятий, наиболее эффективных для их устранения, способствует построение дерева отказов и неработоспособных состояний. Такой анализ следует проводить для каждого периода функционирования, каждой части или системы в целом.

Дерево отказов (аварий, происшествий, последствий нежелательных событий и пр.) лежит в основе логико-вероятностной модели причинно-следственных связей отказов системы (как вида проявления опасности) с отказами ее элементов и другими событиями (воздействиями). При анализе возникновения отказа системы (происшествия) событие представляется последовательностью и комбинацией нарушений и неисправностей, и таким образом оно представляет собой многоуровневую графологическую структуру причинных взаимосвязей, полученных в результате прослеживания динамики развития опасных ситуаций в обратном порядке, для того чтобы отыскать возможные причины их возникновения (рис. 6.2).

Ценность дерева отказов заключается в следующем:

- анализ ориентируется на нахождение отказов элементов, приведших к отказу системы;
- позволяет показать в явном виде ненадежные места;
- обеспечивается графикой и представляет наглядный материал для той части работников, которые принимают участие в эксплуатации системы;
- дает возможность выполнять качественный или количественный анализ надежности системы;
- метод позволяет специалистам поочередно сосредотачиваться на отдельных конкретных отказах системы;
- обеспечивает наглядное представление о поведении системы и повышает эффективность контроля над ее работой

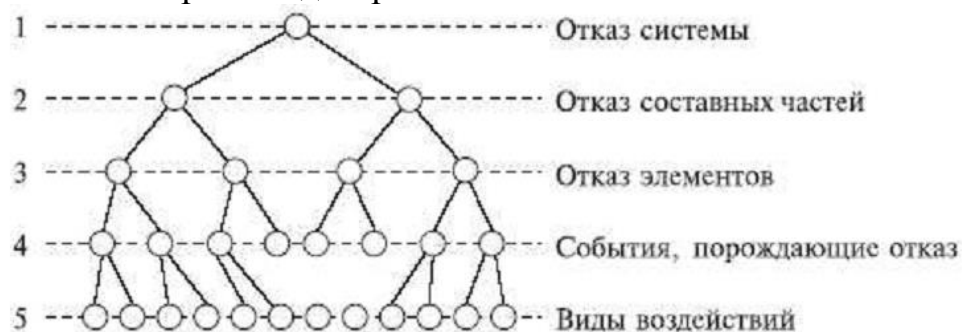


Рис. 6.2. Граф дерева отказов

- помогает дедуктивно выявлять отказы;
- дает конструкторам, пользователям и руководителям возможность наглядного обоснования конструктивных изменений или установления степени ответственности конструкции системы заданным требованиям и анализа компромиссных решений;
- облегчает анализ надежности сложных систем.

Главное преимущество дерева отказов (по сравнению с другими методами) заключается в том, что анализ ограничивается выявлением только тех элементов системы и событий, которые приводят к данному конкретному отказу системы (происшествию).

Недостатки дерева отказов состоят в следующем:

- реализация метода требует значительных затрат средств и времени;
- дерево отказов представляет собой схему булевой логики, на которой показывают только два состояния: рабочее и отказавшее;
- трудно учесть состояние частичного отказа элементов, поскольку при использовании метода, как правило, считают, что система находится либо в исправном состоянии, либо в состоянии отказа;
- трудности в общем случае аналитического решения для деревьев, содержащих резервные узлы и восстанавливаемые узлы с приоритетами, не говоря уже о тех значительных усилиях, которые требуются для охвата всех видов множественных отказов;
- требует от специалистов по надежности глубокого знания системы и конкретного рассмотрения каждый раз только одного определенного отказа;
- дерево отказов описывает систему в определенный момент времени (обычно в установившемся режиме), и реальные последовательности событий (переходные процессы) могут быть показаны с большим трудом, иногда это оказывается невозможным. Это справедливо для систем, имеющих сложные контуры регулирования.



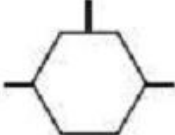



Чтобы отыскать и наглядно представить причинную взаимосвязь с помощью дерева отказов, необходимы элементарные блоки, подразделяющие и связывающие большое число событий. В инженерной практике принято использовать два типа блоков: логические символы (знаки) и символы событий.

**Логические символы.** Логические символы (знаки) связывают события в соответствии с причинами их возникновения. Обозначения логических знаков приведены в табл. 6.2 Логический символ (знак) может иметь один или несколько входов, но только один выход, или выходное событие.

Логический знак "И" (схема совпадения). Выходное событие логического знака И наступает в том случае, если все входные события появляются одновременно. Правило формулирования событий. События, входные по отношению к операции И, должны формулироваться так, чтобы второе было условным по отношению к первому, третье условным по отношению к первому и второму, а последнее - условным ко всем предыдущим. Кроме того, по крайней мере, одно из событий должно быть связано с появлением выходного события. Полная характеристика события не требуется.

Иногда она даже мешает графической ясности диаграммы. Требуется лишь упорядочить события так, чтобы событие стоящее справа зависело от появления события стоящего слева. Таким образом, появление выходного события будет определяться появлением последнего события в ряду N - событий.

Таблица 6.2 Логические символы

Стро- ка	Символ логи- ческого знака	Название логического знака	Причинная взаимосвязь
1		<b>И</b>	Выходное событие происхо- дит, если все входные собы- тия случаются одновременно
2		<b>ИЛИ</b>	Выходное событие происхо- дит, если случается любое из входных событий
3		<b>«Запрет»</b>	Наличие входа вызывает на- личие выхода тогда, когда происходит условное событие
4		<b>«Приоритетное И»</b>	Выходное событие случается, если все входные события происходят в нужном поряд- ке слева направо
5		<b>«Исключающее ИЛИ»</b>	Выходное событие происхо- дит, если случается одно (но не оба) из входных событий
6		<b>«m из n» (голосования или выборки)</b>	Выходное событие происхо- дит, если случается m из n входных событий

Правило применения логического знака И. Если имеются несколько причин, которые должны появиться одновременно, то обычно, используют операцию И. Входы операции должны отвечать на вопрос: "Что необходимо для появления выходного события?".

Логический знак "ИЛИ" (схема объединения). Выходное событие логического знака ИЛИ наступает в том случае, если имеет место любое из входных событий.

Правило формулирования событий. События, входные по отношению к операции ИЛИ, должны формулироваться так, чтобы они вместе исчерпывали все возможные пути появления выходного события. Кроме того, любое из входных событий должно приводить к появлению выходного события. Правило не дает способа описания событий, но оно должно выполняться при построении дерева отказа.

Правило применения логического знака ИЛИ. Если любая из причин приводит к появлению выходного события, следует использовать операцию ИЛИ. Входы операции отвечают на вопрос: "Какие события достаточны для появления выходного события?".

Примеры этих двух логических знаков показаны на рис. 6.3. Событие "возникновение пожара" имеет место, если два события - "утечка горючей жидкости" И "очаг воспламенения вблизи горючей жидкости", происходят одновременно. Последнее (критическое) событие случается, если происходит одно из двух событий - "наличие искры" ИЛИ "открытое пламя".



Рис. 6.3 Пример использования логических знаков И и ИЛИ

## Лекция 7 . Процедура проведения анализа надежности технического объекта (ТО)

*Анализ "сверху вниз" – этапы проведения; виды событий дерева отказов; последовательность построения дерева отказов; пример анализа надежности ТО; Дерево событий - ДС (event tree analysis - ETA); Дерево решений; Логический анализ;*

Суть метода заключается в построении структурной схемы - дерева отказов системы и ее анализе. Основной принцип построения дерева отказов (ДО) заключается в последовательной постановке вопроса, по каким причинам может произойти отказ системы или элемента. Анализ осуществляется "сверху вниз".

Обычно предполагается, что инженер, прежде чем приступить к построению дерева отказов, тщательно изучает строение системы. Поэтому описание системы должно быть частью документации, составленной в ходе анализа ДО.

Процедура построения дерева отказов включает, как правило, следующие этапы: 1. Определение критического (завершающего) события в рассматриваемой системе. 2. Тщательное изучение предполагаемого режима использования системы и ее реального поведения. 3. Проведение углубленного анализа работы системы с целью выявления событий, способных привести к отказу системы. 4. Собственно построение дерева отказов. Эти события должны определяться в терминах независимых первичных отказов.

Чтобы получить количественные оценки завершающего нежелательного события (происшествия), необходимо задать вероятности отказов, их интенсивность, интенсивность восстановлений и другие показатели, характеризующие первичные события, при условии, что эти события дерева отказов не являются избыточными (т.е. не приводящими к происшествию).

Более детальный анализ предусматривает выполнение таких процедур, как определение небезопасных границ системы, построение дерева неисправностей, качественная оценка, количественная оценка.

Основой построения дерева отказов является символическое представление существующих в системе условий - событий, способных вызвать отказ.

При построении ДО учитывают и используют следующие основные виды событий:

- результирующее событие (происшествие) - нежелательное событие (конкретный вид отказа системы из перечня возможных отказов, приводящий к недопустимому ущербу), анализ которого проводится;
- промежуточное событие - сложное событие, возникающее при определенных условиях и являющееся одной из возможных причин результирующего события. Его выявляют в ходе анализа причин возникновения результирующего события и подвергают дальнейшему анализу;

- базовое событие - простое исходное событие, означающее первичный отказ, которое дальше не анализируется в связи с определенностью и наличием достаточного числа данных;
- неполное событие - недостаточно детально исследованное событие, которое дальше не анализируется, из-за невозможности или отсутствия необходимости проведения его анализа;

Исходными событиями при построении ДО являются перечни возможных видов событий - отказов и их причин, нерасчетные значения внешних воздействующих факторов и др. Соответственно, каждому виду события и оператора присваиваются символы, которые используются для графического построения дерева отказов. Логические символы связывают события в соответствии с их причинными взаимосвязями.

Построение дерева и анализ исследуемого объекта (системы) производят следующим образом.

1. Определяют аварийное (предельно опасное, конечное) событие - происшествие, которое образует вершину дерева. Данное событие четко определяют, устанавливают условия его появления, дают признаки для его распознавания. Определяют возможные первичные и вторичные отказы, которые могут вызвать аварийное событие, рассматривают их комбинации.
2. Используя стандартные символы событий и логические символы (табл. 3.2-3.4), строят ДО в соответствии со следующими правилами: а) конечное (аварийное) событие помещают вверху (уровень 1); б) дерево состоит из последовательности событий, которые ведут к конечному событию; в) последовательности событий образуются с помощью логических знаков И, ИЛИ и др.; г) событие, определяемое логическим знаком помещают в прямоугольнике, а текстовое описание события вписывают в этот прямоугольник; д) первичные события (исходные причины) располагают внизу.
3. Определяют минимальные аварийные сочетания и минимальную траекторию прохождения отказа для построенного дерева. Первичные и неразлагаемые события соединяются с событиями первого уровня маршрутами (ветвями). Сложное дерево имеет различные наборы исходных событий, при которых достигается событие в вершине. Эти наборы называются аварийными сочетаниями. Минимальным аварийным сочетанием (МАС) называют наименьший набор исходных событий, приводящих к событию в вершине. Полная совокупность аварийных сочетаний конкретного дерева представляет собой все варианты сочетаний первичных отказов, при которых может возникнуть происшествие (отказ системы в целом).
4. На уровне качественных и количественных оценок исследуют дерево отказов с использованием найденных минимальных аварийных сочетаний. Качественный анализ заключается в сопоставлении различных маршрутов и начальных условий с целью определения критических (наиболее опасных) путей, приводящих к происшествию. При количественном исследовании рассчитывают вероятность происшествия в течение заданного интервала времени при всех возможных маршрутах распространения отказов.

5. Разрабатывают рекомендации по введению изменений в конструкцию и технологию эксплуатации объекта, системы контроля и управления для улучшения показателей его безаварийности.

В зависимости от конкретных целей анализа, деревья могут быть построены для любых видов отказов - первичных, вторичных и инициированных отказов.

Случай первичного отказа. Отказ элемента называется первичным, если он происходит в расчетных условиях функционирования системы. Построение ДО на основе учета лишь такого рода отказов не представляет большой сложности, так как дерево строится только до той точки, где идентифицируемые первичные отказы элементов вызывают отказ системы.

**ПРИМЕР.** Требуется построить ДО для простой системы - электросети, выключателя и электрической лампочки. Считается, что завершающим событием является отсутствие освещения.

Дерево отказов для этой системы показано на рис.6.1. Основными (первичными) событиями ДО являются (1) отказ источника питания E1, (2) отказ предохранителя E2, (3) отказ выключателя E3 и (4) перегорание лампочки E4.

Промежуточным событием является прекращение подачи энергии. Исходные отказы представляют собой входы схем ИЛИ: при наступлении любого из четырех первичных событий осуществляется завершающее событие - отсутствие освещения.

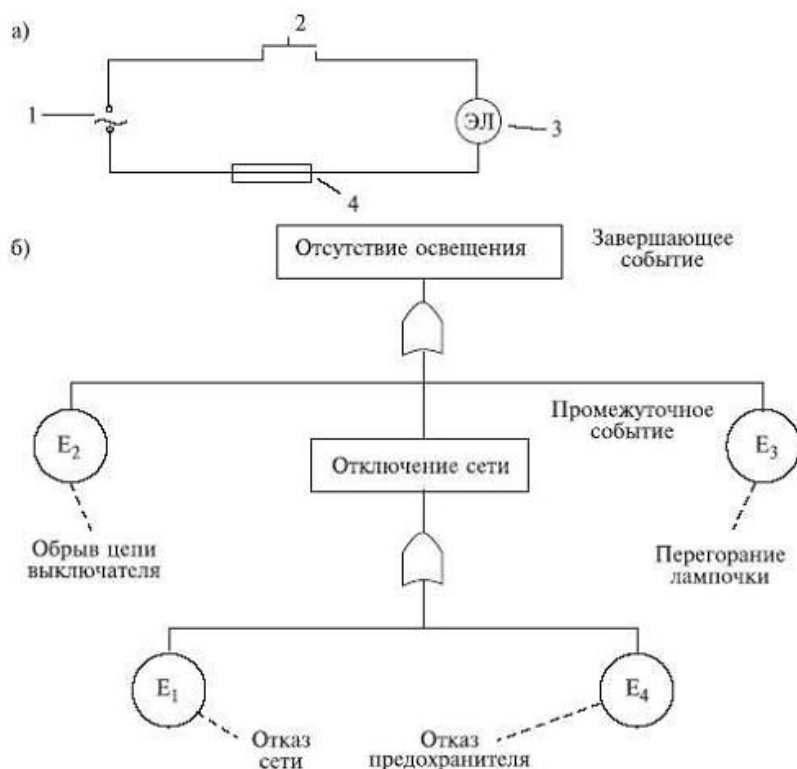


Рис. 7.1. Электрическая схема системы "сеть - электрическая лампочка" (а) и дерево (б) для случая первичных отказов: 1 - сеть; 2 - выключатель; 3 - электролампа; 4 - предохранитель

Случай вторичного отказа. В этом случае требуется более глубокое исследование системы. При этом анализ выходит за рамки рассмотрения си-



системы на уровне отказов ее основных элементов, поскольку вторичные отказы вызываются неблагоприятным воздействием внешних условий или чрезмерными нагрузками на элемент системы в процессе ее эксплуатации.

### **Дерево событий - ДС (event tree analysis - ETA)**

Дерево событий (ДС) используется для анализа последовательности (вариантов, сценариев) развития отказа системы (происшествия), включающей сложные взаимосвязи между техническими элементами обеспечения безопасности. Вероятность каждого сценария развития аварийной ситуации рассчитывается путем умножения вероятности первичного события на вероятность конечного события.

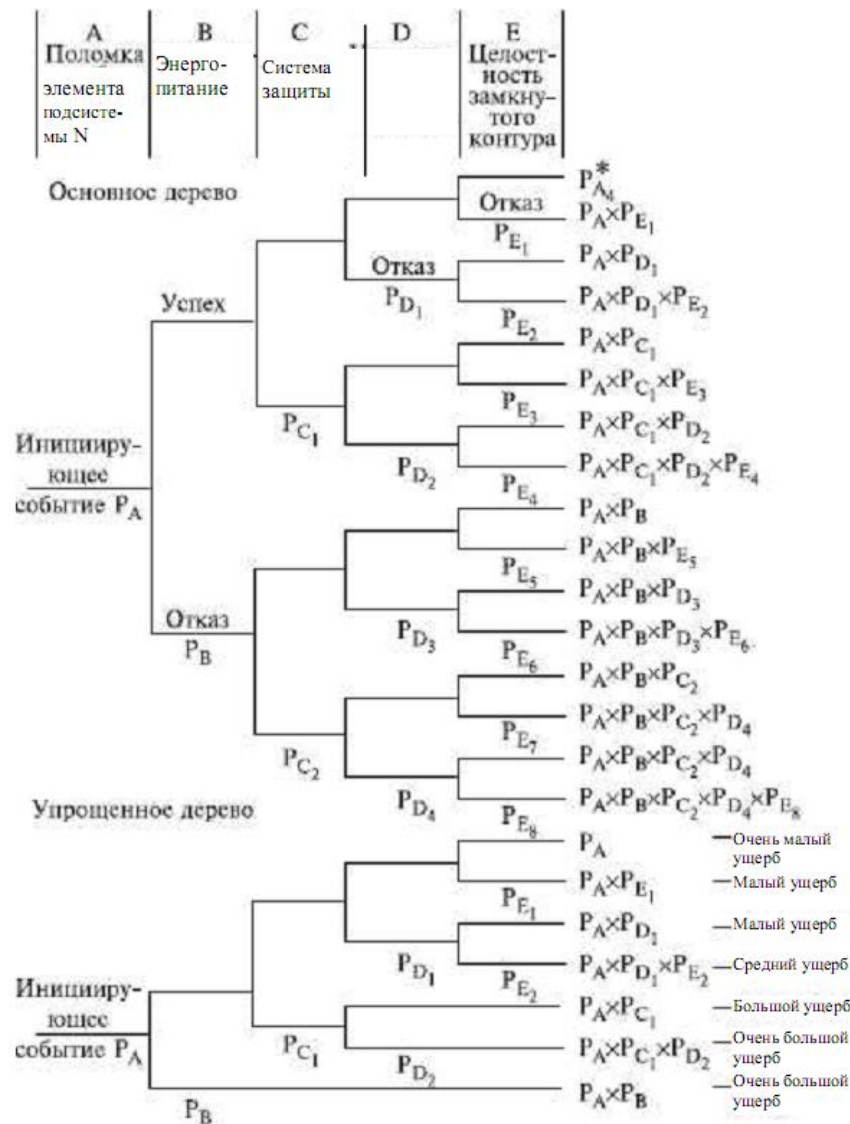


Рис. 7.2 Дерево событий

Рассмотрев все варианты дерева событий, можно получить спектр возможных ущербов и соответствующие вероятности для различных последовательностей развития происшествия (рис. 6.2).

### **Дерево решений**

Дерево решений является разновидностью дерева событий. В дереве событий работоспособные состояния системы не рассматриваются, так что

сумма вероятностей всех событий не равна единице. В дереве решений все возможные состояния системы необходимо выразить через состояния элементов. Таким образом, все состояния системы взаимно увязаны, и их вероятность в сумме должна равняться единице. Деревья решений могут использоваться, если отказы всех элементов независимы или имеются элементы с несколькими возможными состояниями, а также есть односторонние зависимости. Они не могут использоваться при наличии многосторонних зависимостей.

### *Логический анализ*

Логический анализ опасностей основан на понятиях булевой алгебры (алгебры логики).

В алгебре логики переменные, обозначаемые заглавными буквами, имеют, как правило, смысл некоторых событий или факторов. Например, можно обозначить символом А событие, состоящее в повреждении какой-то части технической системы. Если это происходит, то мы говорим, что  $A=T$  или что А истинно. Если это событие не происходит, говорим, что  $A=F$  или что А ложно. Такие высказывания справедливы для некоторого определенного интервала времени и вероятности, связанной с появлением события. Переменные в алгебре логики принимают два значения: истина или ложь (появление или неоявление). Аналогично и функции, образуемые этими переменными, принимают два значения в зависимости от комбинации логических переменных. Функции образуются с помощью операций И (логическое умножение), ИЛИ (логическое сложение) и НЕ (логическое отрицание). Смысл этих операций определяется таблицами истинности.

Истинное значение функции определяется значениями переменных, входящих в нее. Например, пусть функция А имеет вид

$$A = BC + DE.$$

Чтобы определить истинное значение А, надо знать истинные значения четырех переменных. Вычисление значения отдельных членов функции ведется в определенной последовательности: (1) НЕ, (2) И и (3) ИЛИ. Таким образом, если, например  $B=\text{ЛОЖЬ}$ ,  $C=\text{ИСТИНА}$ ,  $D=\text{ИСТИНА}$  и  $E=\text{ЛОЖЬ}$ , то, используя таблицы, получим:

$$A = FT + TF = FT + T = F + T = T.$$

При определенных навыках такие вычисления производятся достаточно быстро. Особый интерес представляет применение алгебры логики для анализа вероятных опасностей.

## Лекция 8. ОСНОВНЫЕ НАПРАВЛЕНИЯ, МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ НАДЕЖНОСТИ И БЕЗОПАСНОСТИ ТЕХНИЧЕСКИХ СИСТЕМ

*Предупредительные, контрольные защитные мероприятия; Техническая поддержка и обеспечение работ по безопасности сложных технических систем; Технические средства предупреждения отказов, контроля надежности в производстве Защитная автоматика; Автоматический контроль и измерения. Сигнализация; Блокировка.*

Для снижения опасности отказов систем из-за конструктивных, производственных или эксплуатационных причин существует ряд типовых мероприятий предупредительного, контролирующего и защитного характера, обеспечивающих надежность и безопасность технических систем. Их применяют на различных этапах жизненного цикла систем - в процессе проектирования, на стадиях изготовления и эксплуатации.

**На стадии проектирования и изготовления технических систем предупредительные мероприятия** обычно включают:

- использование отработанных методов и средств обеспечения надежности;
- анализ альтернативных проектно-конструкторских решений и выбор наилучших;
- создание запасов работоспособности по нагрузкам и отказам различных видов;
- использование резервирования; выбор высоконадежных комплектующих элементов, материалов;
- создание контролепригодных и ремонтпригодных элементов;
- обучение конструкторов, испытателей передовым методам и способам обеспечения надежности;
- установление проектных норм надежности и типовых испытаний при экспериментальной отработке;
- разработка новых средств контроля и диагностики.

### **Контрольные мероприятия:**

- экспериментальная проверка технических решений, особенно новых;
- проверка всех режимов функционирования;
- целевые и комплексные испытания;
- контроль и корректировка конструкторской документации;
- экспериментальная проверка запасов работоспособности на всех режимах функционирования;
- контроль надежности; контроль качества труда исполнителей, самоконтроль.

### **Защитные мероприятия:**

- анализ видов и последствий отказов;
- введение специальных элементов в состав системы, обеспечивающих безопасность при возникновении отказов;

- отработка основных отказных режимов функционирования;
- тренировка эксплуатационного персонала;
- реализация технических решений по локализации отказов;
- применение оперативного контроля и управления функционированием;
- обеспечение сохранения работоспособности системы при отказах элементов;
- разработка системы обслуживания и восстановления техники.

**На стадии эксплуатации технических систем предупредительные мероприятия:**

- использование автоматизированных средств контроля и поиска неисправностей;
- отработка эксплуатационно-технической документации;
- проведение регламентных работ;
- оценка и прогнозирование технического состояния и надежности;
- обучение и аттестация персонала.

**Контрольные мероприятия:**

- автоматизированная регистрация и обработка информации об отказах и неисправностях;
- контроль качества;
- самоконтроль;
- гарантийный надзор.

**Защитные мероприятия:**

- проведение доработок по документации разработчиков;
- использование автоматических средств защиты;
- использование запасных частей, обменного фонда;
- анализ последствий произошедших отказов и реализация защитных мероприятий;
- обучение и аттестация персонала для работы при возникновении отказов.

***Техническая поддержка и обеспечение работ по безопасности сложных технических систем***

Технические средства (элементная база, экспериментальные и производственные возможности) представляют наиболее важную часть активных средств обеспечения безопасности и эффективности сложных технических систем. Отсутствие материально-технической основы создания надежной техники и поддержания ее в работоспособном состоянии на протяжении всего жизненного цикла, не может быть заменено другими мерами (организацией работ, реализацией программного подхода, методического, нормативного или информационного обеспечения).

Уровень технического обеспечения зависит от следующих факторов:

- уровней качества и надежности материалов, полуфабрикатов, комплектующих элементов, агрегатов и изделий общего назначения,
- выпускаемых промышленностью и используемых в составе технических систем;

- технического уровня, номенклатуры, производительности, степени автоматизации технических средств для проектирования, отработки производства и эксплуатации сложных изделий;
- - уровня автоматизации систем и средств оперативного сбора, обработки, обмена информацией для координации и контроля хода создания и применения технических изделий и технологий.

Чем сложнее создаваемые технические системы, тем больше в них потенциальных источников отказов, тем проблематичнее становится обеспечение их надежности при достигнутом научно-техническом уровне проектирования, экспериментальной отработки, производства и эксплуатации.

Все технические средства обеспечения надежности и безопасности, которые используют при создании и эксплуатации технических систем, могут быть условно разделены на три класса: средства предупреждения, средства контроля и средства защиты.

К числу технических средств, используемых для предупреждения отказов конструктивного характера, относят:

- автоматизированные цифровые и аналого-цифровые комплексы моделирования, имеющие необходимое математическое обеспечение и позволяющие проектантам разрабатывать большое число альтернативных вариантов элементов системы, режимов их работы и выбирать наиболее надежные и эффективные;
- средства автоматизированной разработки конструкторской и технологической документации, позволяющие исключить ошибки в документации и значительно ускорить её разработку;
- современное экспериментальное оборудование, позволяющее своевременно отрабатывать новые технические решения, обеспечить высокую надежность элементов;
- технические средства обучения и повышения квалификации конструкторов, технологов, экспериментаторов и других сотрудников предприятий-разработчиков;
- автоматизированную систему информации по вопросам качества и надежности элементов технических систем.

К числу технических средств, предупреждающих отказы и отклонения производственного характера, относят:

- прогрессивное автоматизированное производственно-технологическое оборудование, средства контроля и управления технологическими процессами;
- технические средства входного неразрушающего контроля и диагностики, исключающие попадание в производство недостаточно качественных материалов, полуфабрикатов и комплектующих элементов;
- автоматизированные средства обучения рабочих и инженерно-технических работников предприятий-изготовителей;
- автоматизированную систему информации по качеству и надежности систем в производстве.

К числу технических *средств предупреждения отказов в эксплуата-*

**ции относят:**

- технические средства для отработки эксплуатационной документации (стенды, макеты) и обучения эксплуатирующего персонала;
- автоматизированные средства контроля, диагностики и поиска неисправностей;
- технические средства для проведения предупредительных и регламентных работ.

К числу технических средств, обеспечивающих **контроль и выявление отказов конструктивного характера**, относят:

- экспериментальную базу, достаточную для контроля правильности заложенных технических решений, проверки запасов работоспособности элементов во всех режимах функционирования, контроля надежности;
- технические средства контроля и корректировки конструкторской документации, качества труда исполнителей.

***Технические средства контроля надежности в производстве***

технических систем предназначены для осуществления следующих функций:

- проведения эффективного входного, пооперационного и приёмочного контроля качества элементов;
- проверки режимов функционирования, запасов работоспособности, проведения контрольно-технологических испытаний;
- контроля качества сборки и совместного функционирования групп элементов;
- контроля качества технологической документации, стабильности технологических процессов, качества труда исполнителей.

***Технические средства контроля надежности в эксплуатации:***

- технические средства неразрушающего контроля и диагностики;
- автоматизированные средства регистрации и обработки информации о результатах функционирования элементов систем, об отказах и неисправностях;
- технические средства прогнозирования работоспособности элементов, контроля и поиска неисправностей;
- автоматизированные средства контроля качества работы операторов.

К **числу технических средств защиты**, предназначенных для устранения условий возникновения отказов, а также последствий их появления, относят:

- технические средства локализации отказов, вводимые непосредственно в состав системы;
- технические средства оперативного контроля и управления системой при возникновении опасных ситуаций;
- блокировки в ответственных технологических процессах, исключающие возможности разрушения элементов системы при нарушении технологического процесса;

В конструкции технических систем для уменьшения ущерба от возможных отказов предусматривают следующие технические средства:

- пожаро-взрывобезопасности и пожаротушения; - автоблокировки, исключающие прохождение и выполнение ошибочных команд;
- предупреждения ошибочных действий операторов.

При разработке новых технических систем в них должны быть включены:

- средства предупреждения отказов и отклонений от установленного хода технологических процессов;
- средства оперативного контроля и выявления причин отказов и отклонений;
- средства защиты от опасных последствий отказов и отклонений.

К числу современных средств защиты технических систем от действия опасных отказов относят защитную автоматику.

**Защитная автоматика** - это совокупность организационных и технических средств, используемых в системах для поддержания заданного режима технологического процесса, предотвращения аварийных ситуаций и (или) повреждения элементов систем.

Защитная автоматика должна обеспечивать определение состояния оборудования (например, "включено или выключено"), степени его загрузки, режима работы и значений технологических параметров.

По функциональному признаку в защитной автоматике выделяют блоки автоматического контроля, измерения, сигнализации, защиты и блокировки.

**Автоматический контроль и измерения** могут проводиться дискретно или непрерывно. В зависимости от места представления показаний различают контроль местный и централизованный (дистанционный). При местном контроле измерительные приборы и индикаторы устанавливаются на объекте контроля, при централизованном, индикаторы выносят на диспетчерский пульт. При контроле предельных положений регистрируются только параметры, соответствующие этим положениям, при непрерывном контроле происходит непрерывное измерение параметров.

**Сигнализация** предназначена для передачи контрольных, управляющих (командных) и информационных сигналов по каналам и линиям связи, например оператору или диспетчеру.

Различают сигнализацию предупредительную - для предупреждения персонала о пуске тех или иных механизмов, распорядительную - для пуска и отключения систем оператором, исполнительную - для контроля выполнения распоряжений, аварийную - для оповещения персонала о нарушении нормального хода процессов. Для сигнализации о состоянии распределенных объектов используют телекоммуникацию.

**Блокировка** - совокупность методов и средств, обеспечивающих фиксацию рабочих частей (элементов) технической системы в определенном состоянии (положении), которое сохраняется независимо от того, устранено или нет блокирующее воздействие, чем достигается как безопасность оборудования, так и безопасность обслуживания.

### ***Техническое обслуживание, ремонтные работы и инспектирование***

Надежность и безопасность функционирования технических систем существенно зависит от качества технического обслуживания и ремонта этих

систем. По этой причине должны быть разработаны технологии обслуживания, как самих технических систем, так и относящихся к ним систем безопасности. Техническое обслуживание (ТО) систем безопасности должно обеспечивать решение следующих задач:

- проверку условий работы систем безопасности, как в тестовых режимах, так и в рабочих процессах;
- проверку исправности оборудования систем безопасности на рабочих местах, например, путем визуального осмотра или дистанционного контроля;
- мониторинг питающих устройств;

Ошибки и нарушения персонала при выполнении ТО и ремонтных работ, могут стать причиной возникновения опасностей. Поэтому должны быть разработаны подробные инструкции проведения таких работ. В них должны быть отражены квалификационные требования к обслуживающему персоналу, а также требования по контролю за проведением этих работ.

Необходимо разработать план инспекций и испытаний сложных технических систем, сроки проведения которых должен строго соблюдаться. Инспекторской проверке должны быть подвергнуты технические средства и меры организации контроля над опасностями. Инспекции и испытания должны соответствовать общепринятой практике и проводиться с периодичностью, рекомендованной изготовителем, а при необходимости (устанавливается по предшествующему опыту эксплуатации), и чаще.

Технический персонал, осуществляющий эксплуатацию систем, должен устранить неисправности или перед дальнейшим использованием системы, или по плану-графику, если немедленно были предприняты необходимые меры для обеспечения безопасности эксплуатации.

### ***Управление изменениями в технологическом процессе***

Перед тем как вносить какие-либо изменения в технологию процесса эксплуатации технических систем, в другие объекты, работа которых влияет на технологический процесс, необходимо рассмотреть и оценить:

- - техническую базу для предлагаемого изменения;
- - влияние изменения на безопасность этой и других систем, включая экологическую безопасность;
- - изменение эксплуатационных процедур;
- - срок, необходимый для реализации изменений;

Персонал, вовлеченный в эксплуатацию систем и техническое обслуживание, должен до внесения изменений и запуска модернизированного технологического процесса быть проинформирован об изменениях, и пройти соответствующее обучение. Если изменение затрагивает информацию и инструкции по эксплуатации систем, то они должны быть соответствующим образом откорректированы.

### ***Обучение***

Несмотря на то, что в обеспечении безопасности важное место занимают технические средства, без участия человека никакое производство работать не будет. Поскольку на уровень безопасности люди могут оказывать как позитивное, так и негативное влияние, крайне необходимо снизить по-



следнее и всячески поддержать первое. Обе цели могут быть достигнуты путем правильного подбора персонала, его первоначального обучения и последующего поддержания профессиональных навыков. В ходе обучения до слушателей должна быть доведена следующая информация:

- об опасностях, связанных с производственными процессами и уровнях риска;
- об инструкциях, которые необходимо строго соблюдать в ходе выполнения работы;
- о возможных условиях работы;
- о рекомендуемом поведении при нарушении режимов работы системы;
- о ситуациях, близких к аварийным, на других аналогичных производствах.

Повторное обучение должно проводиться, по крайней мере, каждые три года (или чаще, по мере необходимости) для каждого работника, включенного в эксплуатацию технических систем, для подтверждения того, что работник понимает и твердо придерживается действующих эксплуатационных инструкций.

Руководитель должен определить во время консультаций с работниками, вовлеченными в эксплуатацию технических систем, периодичность повторного обучения. Руководителю необходимо удостовериться, что каждый работник, вовлеченный в процесс, получил и усвоил требуемые знания и навыки.

Результаты обучения и аттестации персонала должны быть оформлены соответствующим образом.

## ЛЕКЦИЯ 9 Диагностика опасных ситуаций в технических системах

*Техническое состояние системы; системы технического диагностирования; достоверность результатов диагностирования; функциональное и тестовое диагностирование; АСУТП, АСД, задача акустического диагностирования; алгоритм обеспечения эксплуатационной надежности технических систем*

Определение технического состояния систем в ходе эксплуатации или после ремонта называют техническим диагностированием. С помощью технической диагностики прогнозируют возможные отклонения в состоянии систем и устройств, а также разрабатывают методы и средства обнаружения и локализации неисправностей в них. Различным нарушениям в работе систем соответствуют определенные технические состояния.

Техническим состоянием называют совокупность свойств системы, подверженных изменениям в процессе ее эксплуатации. Эти свойства характеризуются признаками (требованиями, параметрами), устанавливаемыми нормативно-технической документацией на систему. Введение переменной состояния функционирования  $h$  позволяет каждому значению  $h$  ставить в соответствие определенное техническое состояние.

Совокупность средств, правил и алгоритмов диагностирования образует систему технического диагностирования (СТД).

Основные задачи диагностирования при проектировании - проверка соответствия разработанной системы исходному заданию на проектирование и обеспечение высокого качества диагностики системы на последующих этапах жизненного цикла на предмет установления возможных отказов.

Одновременно с проектированием системы создают СТД. Так как значительная доля происшествий связана с ошибками при проектировании, а стоимость каждой пропущенной ошибки исключительно велика, то диагностированию необходимо уделять большое внимание.

При изготовлении, монтаже систем техническое диагностирование - неотъемлемая часть выполняемых работ. Основная цель диагностирования на этих этапах - проверка работоспособности. Возможны два технических состояния системы: работоспособное ( $h_0$ ) и неработоспособное. При ремонте с помощью диагностики можно выявить, содержит ли система дефектные элементы, действительно ли устранены все неисправности. Алгоритмы технического диагностирования должны обеспечивать требуемую достоверность результатов определения состояния системы.

При эксплуатации системы с помощью технического диагностирования определяют состояние функционирования (допустимое, предаварийное, аварийное), осуществляют поиск неисправности. Число состояний, различаемых в результате поиска неисправности, определяется глубиной поиска дефекта и требуемой достоверностью результатов диагностирования. Глубина поиска задается указанием элементов системы, с точностью, до которых определяют место неисправности.

**Достоверность результатов диагностирования** - степень соответствия состояния, оцененного по этим результатам, истинному состоянию системы. Количественно достоверность характеризуется вероятностью совпадения оцененного и истинного состояний.

Определение состояний, предшествующих происшествию, а следовательно, и первопричины его возникновения, исключительно важно для их устранения в будущем и на аналогичных системах.

Классификация методов технического диагностирования при эксплуатации системы и в нерабочем состоянии показана на рис. 8.1.



Рис. 9.1 Методы, технического диагностирования

При эксплуатации технических систем наиболее распространено функциональное и тестовое диагностирование (рис. 8.2).

В первом случае состояние системы определяют по результатам текущего контроля за входными «х» и выходными «у» переменными. Во втором случае на систему подают специальные тестовые воздействия «х<sub>т</sub>».

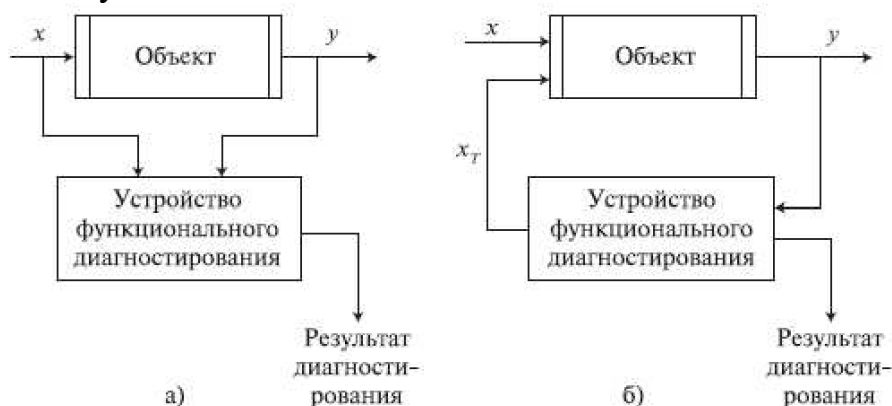


Рис. 9.2. Структурные схемы диагностирования: а - функционального; б – тестового

Для производственного технологического оборудования используют в основном функциональное диагностирование, для автоматических устройств контроля, управления и защиты применяют оба вида диагностирования, вычислительные средства, программное обеспечение проверяют с помощью тестов.

При тестовом контроле на вход проверяемого устройства подаются специально подобранные совокупности входных воздействий (проверяющие

тесты). Полученную на выходе реакцию сравнивают с эталонной. Если они совпадают, то устройство на момент контроля находится в работоспособном состоянии. В противном случае устройство неисправно. Разработаны специальные методы построения оптимальных тестов, позволяющих за минимальное время проверять работоспособность устройства в целом, а также алгоритмы автоматического решения задач синтеза проверяющих и диагностических тестов. Тесты разрабатывают одновременно с проектированием объекта.

Роль технической диагностики возрастает с увеличением мощности и сложности систем, для которых интуитивные методы и ручные способы определения состояний непригодны. Задачи диагностики сложных систем решают с использованием ЭВМ в рамках автоматизированных систем управления технологическими процессами (АСУТП) или автоматизированных систем диагностики (АСД).

Например, применительно к технологическому комплексу АСД выполняет следующие функции:

- определение текущего состояния работоспособности, обнаружение предаварийных и аварийных состояний;
- локализация неисправностей до уровня отдельных агрегатов, элементов систем контроля, управления и защиты;
- регистрация моментов обнаружения неисправностей и их устранения;
- прогнозирование значений переменных технологических процессов в различных состояниях работоспособности;
- прогнозирование предельного значения времени восстановления работоспособности системы;
- регистрация фактического времени восстановления работоспособного состояния;
- отображение оперативной информации о неисправностях на экране дисплея оператора;
- запись, накопление и хранение на магнитных дисках информации о неисправностях;
- выдача накопленной информации о неисправностях системы. АСД, с помощью которой решают данные задачи, может быть реализована на ЭВМ.

На основе АСД строится автоматизированная система обеспечения безаварийного функционирования. Схема АСД приведена на рис. 7.3. Данная система осуществляет текущий контроль входных «х», выходных «у», переменных и параметров А объекта.

После преобразования сигналов от датчиков в унифицированную форму (блок 2) значения  $x(t)$ ,  $y(t)$ ,  $A(t)$  сопоставляют с допустимыми для нормальной работы (блок 4), т.е. проверяют выполнение условий  $x(t) \in X_{\text{доп}}$ ,  $y(t) \in Y_{\text{доп}}$ ,  $A(t) \in A_{\text{доп}}$ , где  $X_{\text{доп}}$ ,  $Y_{\text{доп}}$ ,  $A_{\text{доп}}$  - области допустимых значений соответственно  $x$ ,  $y$ ,  $A$ . Если какое-либо условие не выполняется, то в блоке 5 принимается решение о выдаче сигнала тревоги  $S(x, y, A)$ , а также выработке корректирующих воздействий управляющими устройствами (блок 11). В блоке 10 по данным о  $x(t)$ ,  $y(t)$ , а иногда и отдельных значений  $h(t)$ ,

оценивают вектор фазовых координат  $z(t)$  и переменную состояния функционирования  $h(t)$ . Значения  $z(t)$  и  $h(t)$  сопоставляют с допустимыми (блок 9), т.е. проверяют условия  $z(t) \leq Z_{\text{доп}}$ ,  $h(t) \leq H_{\text{д}}$ . В блоке 5 анализируется текущее состояние системы в случае опасности и выдается сигнал предупреждения  $S_n(z, h)$  или тревоги,  $S(z, h)$  блоком 3. Блоком 7 производится диагностика имеющихся нарушений, а блоком 6 - проверка работоспособности системы обеспечения безаварийности с помощью специальных тестов.

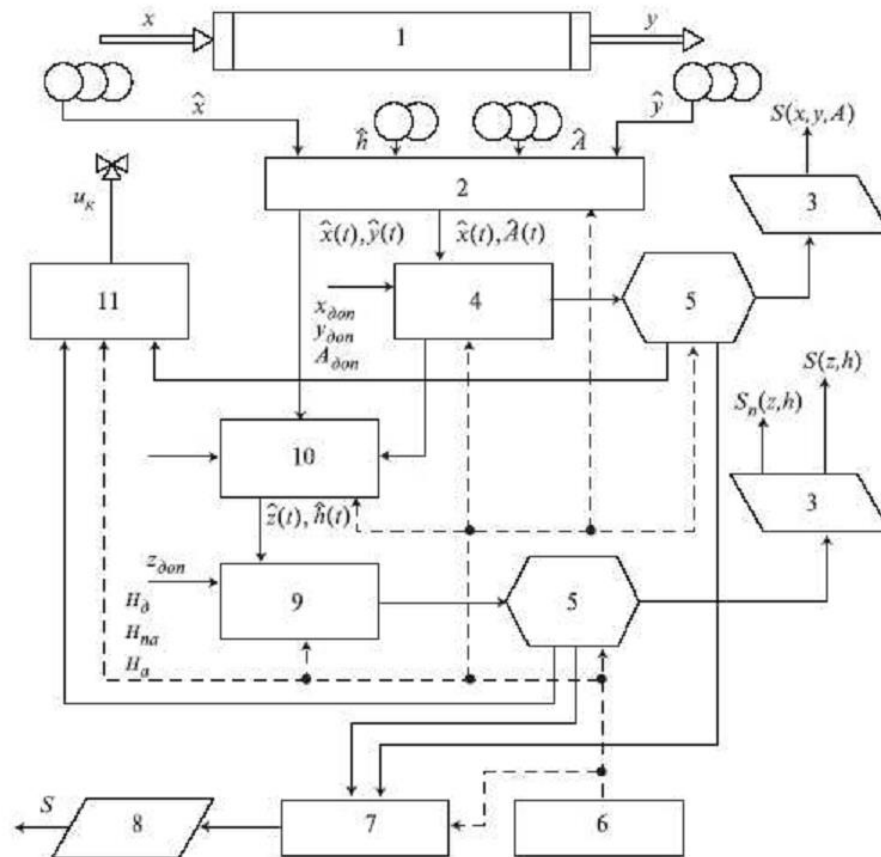


Рис. 9.3. Схема автоматизированной системы диагностики: 1 - объект; 2 - первичные преобразующие и обрабатывающие устройства; 3 - сигнал тревоги; 4 - сопоставление с интервалами, допустимыми для нормальной работы; 5 - анализ и принятие решения; 6 - проверка работоспособности системы; 7 - диагностика нарушения; 8 - сигнал о нарушении; 9 - сопоставление с интервалом  $Z_{\text{доп}}$  и подмножествами состояний  $H_{\text{д}}$ ,  $H_{\text{на}}$ ,  $H_{\text{а}}$ ; 10 - оценка переменных состояния  $z$ ,  $h$ ; 11 - коррекция управляющих воздействий

Например, анализ вибрации позволяет получить важную информацию о процессах в различных механических устройствах, связанных с вращением, качением, скольжением, движением жидкостей, газов и т.д. В настоящее время разработаны датчики вибраций, методы и устройства получения частотного спектра - виброграмм. Схема системы контроля вибраций приведена на рис.7.4а. Расположение дискретных частот виброграммы и их амплитуды позволяют определять состояние работоспособности системы, обнаруживать зарождающиеся отказы, связанные, например, с износом.

Характерный вид виброграмм для различных состояний функционирования показан на рис. 9.4б.

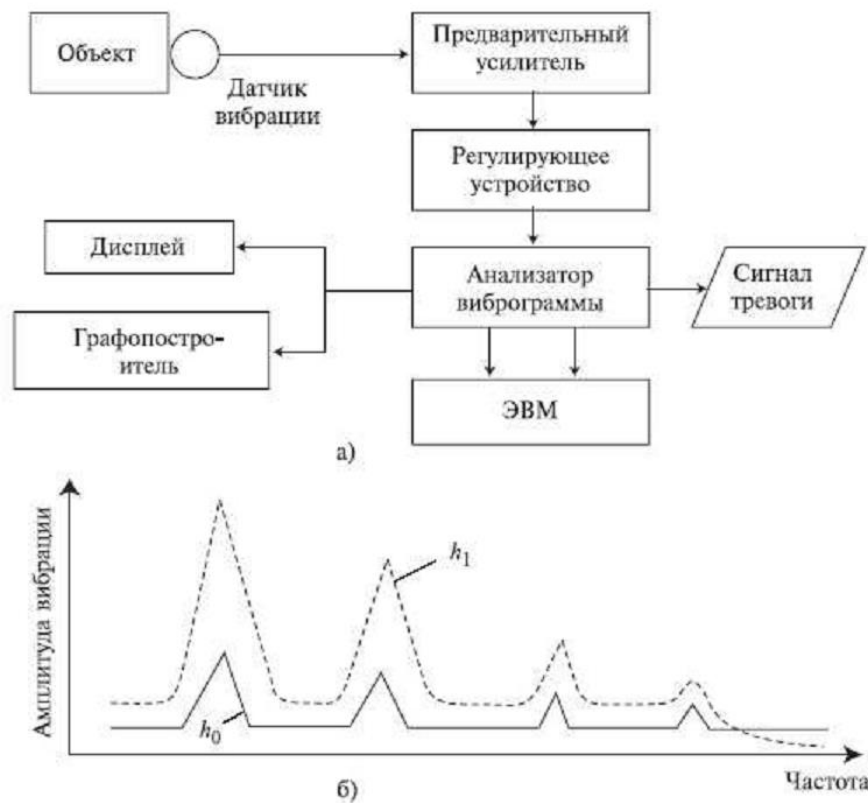


Рис. 9.4 Система контроля вибраций: а - схема; б - виброграммы при различных состояниях работоспособности

Нарушения нормального функционирования, как правило, увеличивают вибрацию (пунктирная линия на рис. 8.4,б для состояния  $h_1$ ).

Многим механическим узлам и устройствам на виброграмме соответствуют определенные дискретные частоты. Для вращательного механизма, например двигателя, компрессора, насоса, вентилятора, турбины, имеется серия дискретных частот, кратных частоте вращения ротора.

Разработан ряд критериев, позволяющих устанавливать допустимые уровни вибрации машин с механизмами вращения. В качестве параметров в критериях используются пики величины вибраций и смещения пиков.

Основные источники вибрации в данном случае деформация или повреждение частей ротора, деформация корпуса и основания, эксцентриситет в подшипниках, повреждение подшипников и др. В меньшей степени исследованы виброграммы механизмов с возвратно-поступательным движением и коробок зубчатых передач.

Для диагностики и предотвращения нарушений в работе технических систем широко используют измерение и анализ характеристик шумов, исходящих от движущихся механизмов, потоков - трубопроводов и теплообменников. С помощью акустических методов выявляют следующие повреждения: трещины в металлических корпусах агрегатов, стенках труб и соединениях, ослабление крепления, отложения на стенках и коррозию, течь в уплотнениях, пропуск газов и др.

Шумы агрегатов и машин характеризуют как общие свойства систем, так и свойства их частей. Производственный шум имеет широкий спектр сигнала, параметры его можно рассматривать как многомерный вектор. Опыт применения акустических методов показывает, что в состоянии нормального функционирования энергия шума в основном концентрируется в области низких частот, а энергия, соответствующая дефектам, располагается на более высоких частотах. Это обстоятельство используют для своевременного обнаружения зарождающихся нарушений.

Каждому состоянию работоспособности системы соответствует свой характерный спектр шума. Задача акустического диагностирования заключается в том, чтобы по зарегистрированному сигналу шума определить техническое состояние контролируемого объекта. Наиболее распространены два способа для решения этой задачи.

Первый способ основан на применении взаимных корреляционных функций, он предполагает предварительную запись в память диагностического устройства временных реализаций сигналов, соответствующих различным состояниям работоспособности. В момент контроля записывается реализация шумового сигнала, излучаемого системой. Данную реализацию используют для расчета взаимных корреляционных функций с сигналами, хранящимися в памяти системы контроля. Считается, что система находится в состоянии, которому соответствует максимальная взаимная корреляция.

Второй способ основан на сравнении статистических характеристик реализаций сигналов, например плотностей распределений, автокорреляционных функций, энергетических спектров. В памяти хранятся статистические характеристики, типовые для возможных состояний функционирования. По реализации сигнала в момент контроля системы вычисляют текущую характеристику, которую сравнивают с типовыми.

Рассчитываемые критерии близости (максимальное отклонение, среднее квадратическое отклонение и т.п.) используют для характеристики технического состояния системы.

Хорошие результаты получают с помощью метода акустической эмиссии. На поверхности системы устанавливают комплект датчиков, которые регистрируют упругие колебания акустического диапазона, источниками колебаний являются развивающиеся макро- и микродефекты материала конструкции. По разности времени прихода импульсов акустической эмиссии к различным датчикам, суммарного числа импульсов, их интенсивности, характера амплитудного распределения сигналов определяют координаты расположения и степень опасности нарушения - источника акустической эмиссии. Спектральный анализ импульсов, корреляционные зависимости между сигналами от датчиков и размерами, конфигурацией и стадией развития макро- и микродефектов для конкретных материалов позволяют оценить техническое состояние конструкции системы, ее остаточный ресурс.

Недостаток большинства акустических методов - необходимость иметь в памяти системы контроля реализации сигналов или статистические характеристики сигналов всех состояний функционирования. При этом они долж-

ны быть получены на контролируемой системе, чтобы учесть его индивидуальные особенности.

### **Алгоритм обеспечения эксплуатационной надежности технических систем**

В процессе обработки информации по анализу последствий отказов технических систем принимают решение либо о немедленном устранении конструктивных недостатков, изменении технологии эксплуатации или технического обслуживания систем (если причина отказа очевидна), либо о проведении необходимых исследований для устранения причины отказа и последующего устранения слабого звена. Окончательные изменения в технологическую документацию вносят только после проверки принятых решений. Процесс этот носит непрерывный характер, что позволяет постоянно поддерживать и даже повышать необходимый уровень эксплуатационной надежности и безопасности таких систем. Таким образом, обеспечение эксплуатационной надежности и безопасности представляет собой замкнутый цикл последовательных операций, один из возможных вариантов которого изображен на рис. 9.5.

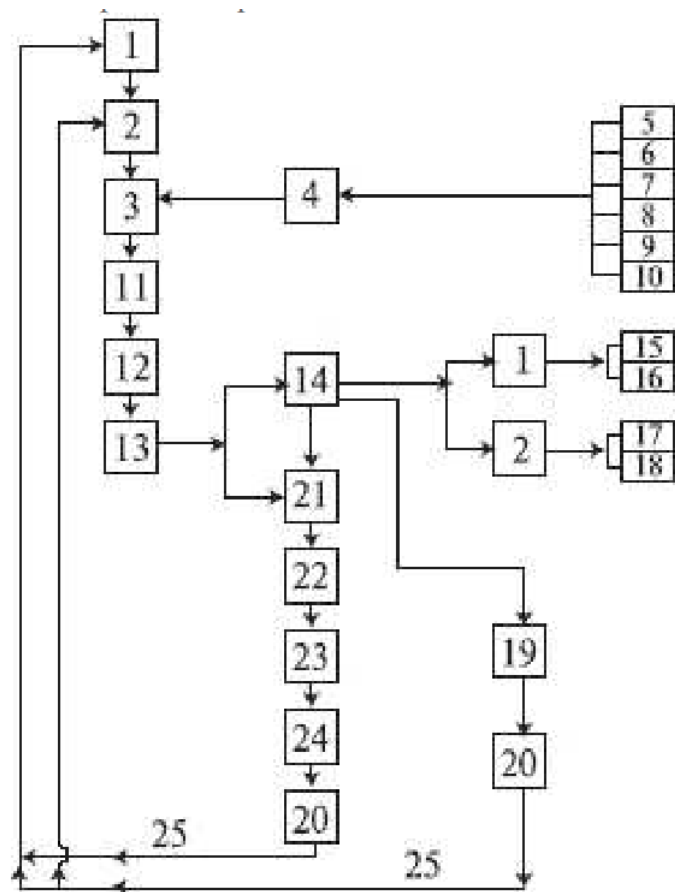


Рис. 9.5. Алгоритм обеспечения эксплуатационной надежности и безопасности системы: 1 - конструкция оборудования; 2 - существующая практика эксплуатации; 3 - информация; 4 - средства получения информации; 5 - причины отказов; 6, 7 - сведения соответственно о расходе запасных частей и частоте их замены и о потерях производства, вызванных простоями; 8 - данные результатов инспекций оборудования; 9 - сведения об изменениях размеров, структуры и свойств материала деталей в процессе эксплуатации; 10 - другие сведения; 11 - обработка информации; 12 - анализ причин отказов и выявление слабых мест; 13 - принятие решения; 14 - решение о немедленном изменении конструкции, практики эксплуатации или технического обслуживания и ремонта оборудования; 15, 16, 17, 18 - изменение соответственно конструкции, материала детали или способа ее

упрочнения, практики эксплуатации, практики технического обслуживания и ремонта; 19 - проверка предложений в промышленной эксплуатации; 20 - данные промышленной эксплуатации после внесенных изменений; 21 - решение о проведении исследований; 22 - разработка методики исследований; 23 - результаты исследований; 24 - усовершенствование конструкции или практики эксплуатации оборудования на основании исследований; 25 - обратная связь