Лекция 5.6 Анализ дерева отказов/неисправностей

Цель лекции – обеспечить слушателей глубоким пониманием методологии Анализа Дерева Отказов (АДО/FTA) как ключевого дедуктивного инструмента в инженерии надежности и безопасности, а также развить практические навыки для его применения в анализе причинно-следственных связей системных отказов.

Задачи лекции:

- понять сущность и принцип работы АДО как метода "сверху вниз", отличающегося от индуктивных подходов (например, FMEA);
- изучить историю возникновения и области наиболее эффективного применения FTA (например, в критически важных отраслях);
- правильно использовать графические символы для событий (верхнее, базовое, промежуточное) и логических операторов (вентили И, ИЛИ).
- научиться последовательно строить диаграмму дерева отказов, начиная с четкого определения верхнего события и заканчивая базовыми событиями.
- определить понятие «минимальное сечение» (Minimal Cut Set) и освоить методику их идентификации.
- научиться использовать минимальные сечения для выявления единичных точек отказа и наиболее критических комбинаций событий.
- понять принципы использования теории вероятностей и булевой алгебры для расчета вероятности верхнего события;
- изучить, какие входные данные (надежность компонентов) необходимы для количественных расчетов, и оценить их влияние на результат.

Анализ Дерева Отказов (АДО, англ. Fault Tree Analysis, FTA) - это системный, дедуктивный (сверху вниз) метод анализа надежности и безопасности, используемый для определения причинно-следственных связей, которые могут привести к определенному нежелательному событию, называемому «верхним событием» или «главным событием». Этот метод использует логические схемы, представленные в виде древовидной диаграммы, для визуализации путей отказа системы.

Эффективность развития любой системы менеджмента включает в себя систему показателей результативности и эффективности стратегии, мониторинг процессов ее выполнения, оценку результатов выполнения, разработку и выполнение корректирующих действий и управленческих решений.

АДО является одним из наиболее мощных инструментов в управлении рисками, надежностью и безопасностью сложных систем в таких критически важных отраслях, как аэрокосмическая, ядерная энергетика, нефтегазовая промышленность, здравоохранение, а также в разработке программного обеспечения.

Ключевая цель АДО:

- идентифицировать все возможные комбинации элементарных событий (отказов компонентов, человеческих ошибок, внешних факторов), которые могут привести к верхнему событию;

- визуализировать логическую структуру причин и следствий;

- провести качественный и количественный анализ для оценки вероятности или частоты возникновения верхнего события и определения наиболее критических «слабых мест» системы.

В отличие от индуктивных методов (например, Анализ Видов и Последствий Отказов, FMEA), которые начинаются с компонента и предсказывают последствия его отказа, АДО является дедуктивным - он начинает с нежелательного системного отказа и ретроспективно исследует его первопричины.

Одно из важнейших направлений при оценке эффективности и результативности управления качеством на предприятии является оценка сопутствующих рисков.

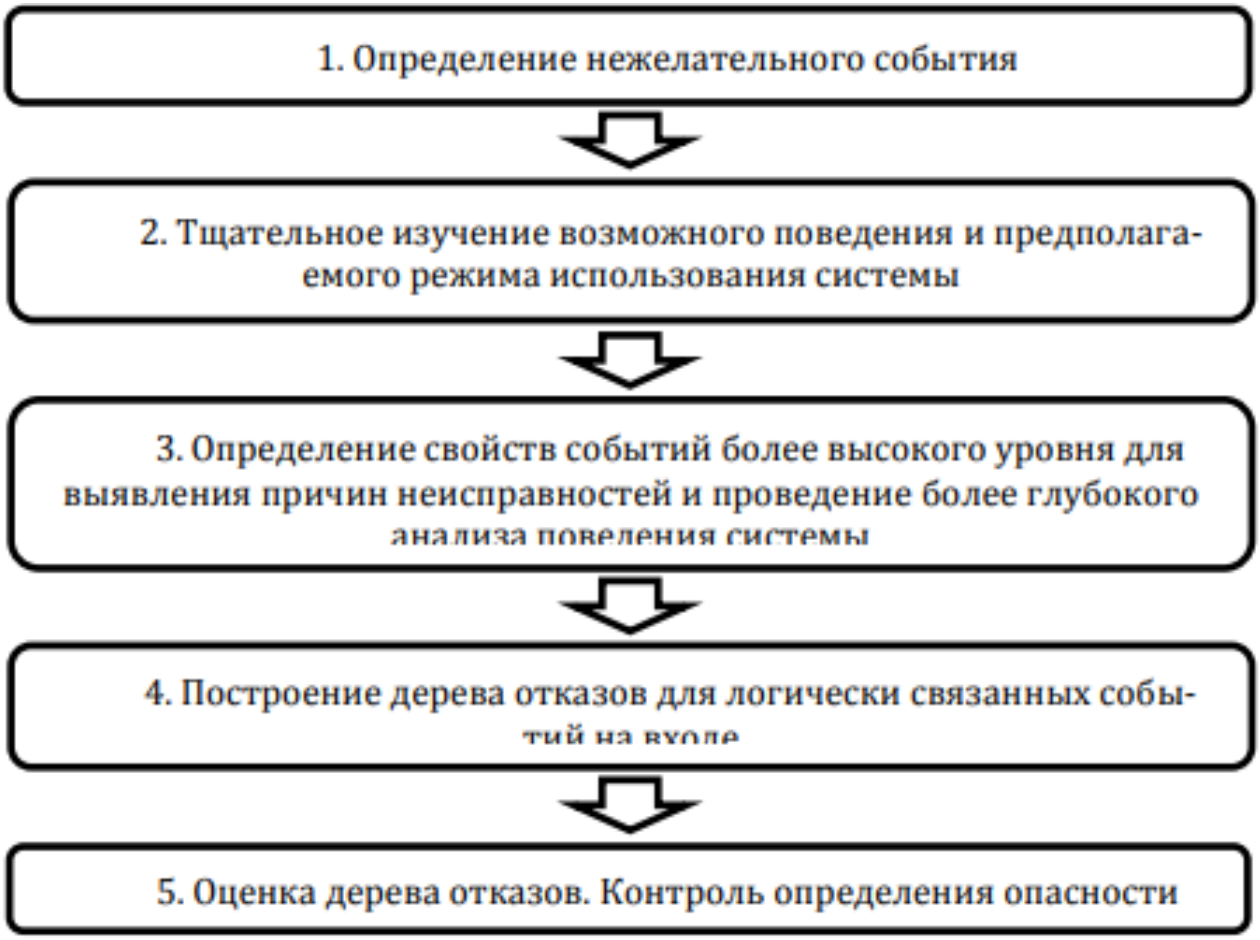


Рисунок 1 - Общий алгоритм с деревом отказов

Наиболее оптимальным методом, не требующим углубленных знаний статистического анализа, является метод построения и анализ дерева отказов.

Дерево отказов/неисправностей – организованное графическое представление условий или других факторов, вызывающих нежелательное

событие, называемое вершиной событий. Представление приводят в форме, которая может быть понята, проанализирована и, по мере необходимости, перестроена таким образом, чтобы облегчить идентификацию.

В 1962 г. впервые был использован метод анализа дерева отказов (fault tree analysis, FTA) компанией Bell Labs для Военно-воздушных сил США, который на сегодняшний день получил широкое распространение для анализа причин отказов различных систем.

Деревья неисправностей могут быть изображены в вертикальном или горизонтальном расположении. Если используется вертикальное расположение, то вершина событий должна быть наверху страницы, а основные события – внизу.

Если используется горизонтальное расположение, то вершина событий может быть слева или справа страницы (рисунок 2, 3).

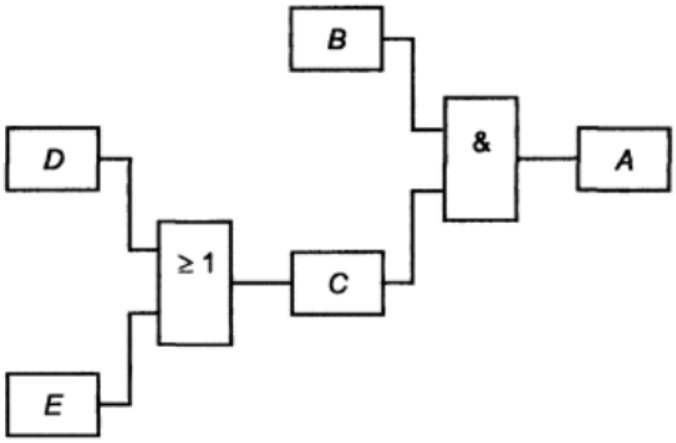


Рисунок 2 - Пример дерева неисправностей

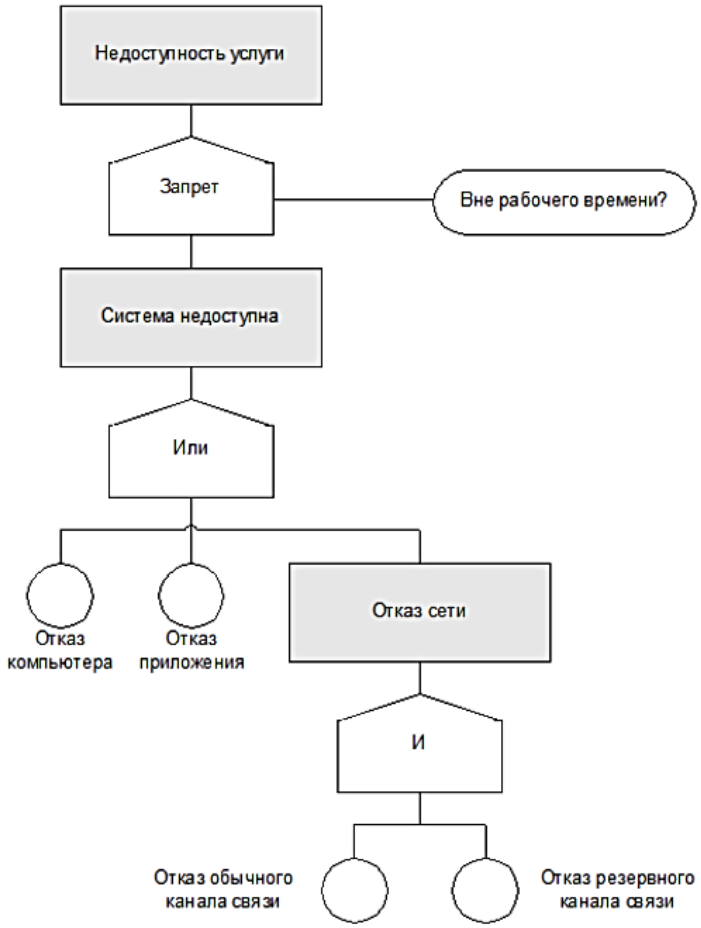
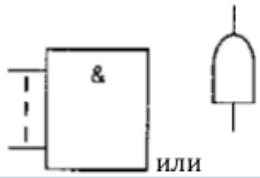
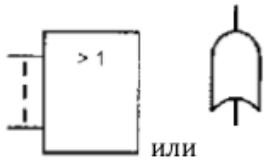
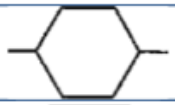
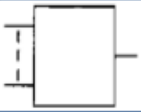


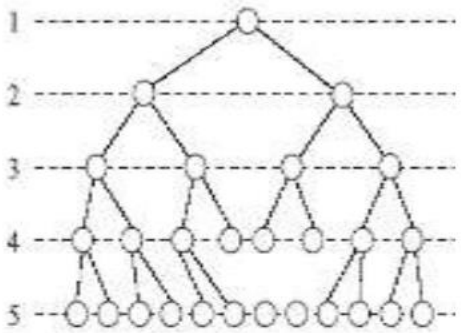
Рисунок 3 - Пример дерева неисправности «дефектов/сбоев»

При построении в дерево неисправностей должны включаться события, являющиеся следствием всех причин. Такие причины должны включать результаты воздействия всех условий окружающей среды или других условий, которые могут воздействовать на элемент, в том числе те, появление которых возможно в процессе работы, даже если они не предусмотрены.

Дерево, как правило, строится с использованием логических символов. Маршрут между событием и инициатором события называется «сечение». Самый короткий путь от неисправности до исходного события называется «минимальное сечение». Символы, используемые при построении дерева отказов приведены в таблице.

Логические символы, используемые при построении дерева отказов

Символ	Описание	
	Клапан «И»	Выходное событие происходит, когда имеют место все входные события
	Логический знак «ИЛИ»	Выходное событие происходит, если имеется одно или несколько входных событий
	Логический знак «Запрет»	Входное событие вызывает выходное, если происходит условное событие
	Клапан (общая форма)	Общий символ клапана, функция которого указывается внутри символа
	Блок описания события	Название или описание события, код события и вероятности появления (при необходимости) должны быть указаны внутри символа



Принцип построения дерева отказов следующий:

1-й уровень – устанавливается «нежелательное событие», которое необходимо предотвратить

2-й уровень – устанавливается отказ составных частей вызывающее основное нежелательное событие

3-й уровень – отказ элементов, вызывающих отказ уровня 2

4-й уровень – устанавливаются причины вызывающие отказ уровня 3

5-й уровень – устанавливаются различные виды воздействий, порождающие причины, отраженные на уровне 4

FTA – дедуктивный, нисходящий метод, направленный на анализ последствий возникновения неисправностей и событий в сложной системе.

FTA эффективно используются, чтобы:

- понимать логику, ведущую к верхнему событию/нежелательному состоянию (отказу системы);
- показать соответствие с системой безопасности/требованиям к надежности;
- ранжировать участников, ведущих к вершине (создание важного оборудования/запчастей/списков событий);
- мониторить и контролировать показатели состояния сложных систем;
- минимизировать и оптимизировать ресурсы.

Кроме того, FTA может быть использован в качестве диагностического инструмента для выявления и исправления причин верхнего события. Это может помочь с созданием диагностических руководств/процессов.

Качественный анализ направлен на выявление критических путей отказа и минимальных сочетаний базовых событий, приводящих к верхнему событию.

- Минимальные Сечения (Minimal Cut Sets): это наименьшие комбинации базовых событий, при одновременном возникновении которых обязательно происходит верхнее событие. Например, если минимальное сечение состоит всего из одного базового события, это означает, что отказ этого единственного компонента приводит к полному отказу системы - единичная точка отказа (single point of failure).
- Минимальные Пути (Minimal Path Sets): это наименьшие наборы базовых событий, не отказ которых (т.е. их нормальное функционирование) гарантирует, что верхнее событие **не произойдет**.
- Ранжирование: Минимальные сечения ранжируются по степени их важности, что позволяет определить, на каких базовых событиях нужно сосредоточить усилия по предотвращению.

Количественный анализ использует вероятности возникновения базовых событий для расчета вероятности (или частоты) верхнего события.

$$P(G) = P(A \cup B) = P(A) + P(B) - P(A)P(B)$$ (для вентиля ИЛИ)

$$P(G) = P(A \cup B) = P(A)P(B)$$ \(для вентиля И при независимых событиях)

где P(G) - вероятность выходного события, P(A) и P(B) - вероятности входных событий.

- Входные данные: требуются данные о надежности (вероятность отказа, частота отказов, среднее время между отказами) для каждого базового события. Эти данные берутся из статистики, исторических данных, баз данных надежности или экспертных оценок.
- Расчет: используя логику дерева и вероятности базовых событий, рассчитывается общая вероятность или частота верхнего события.
- Чувствительность: оценивается, насколько сильно изменение вероятности конкретного базового события влияет на вероятность верхнего события.

На основе результатов анализа (как качественного, так и количественного) разрабатываются и внедряются меры по снижению риска, направленные в первую очередь на устранение или смягчение последствий наиболее критичных минимальных сечений. Это может включать:

- улучшение конструкции или компонентов;
- внедрение дополнительного резервирования;

- повышение качества технического обслуживания;
- разработка процедур для предотвращения человеческих ошибок.

Контрольные вопросы по лекции 5.6

1. В чем состоит фундаментальное различие между дедуктивным подходом Анализа Дерева Отказов (FTA) и индуктивным подходом Анализа Видов и Последствий Отказов (FMEA)? Обоснуйте, в каких случаях предпочтительнее использовать каждый из них.
2. Почему четкое и конкретное определение «верхнего события» является критически важным первым шагом в АДО? Приведите примеры плохо и хорошо сформулированных верхних событий и объясните разницу.
3. Объясните, как вентили «И» (AND) и «ИЛИ» (OR) используются для моделирования резервирования и единичных точек отказа соответственно в логической структуре дерева.
4. Опишите, какие два основных результата дает качественный анализ дерева отказов (FTA) и как эти результаты соотносятся с целями количественного анализа.
5. Что такое «минимальное сечение» (Minimal Cut Set) и почему его идентификация является главным результатом качественного анализа? Как минимальные сечения используются для принятия решений по повышению надежности?
6. Какие типы данных необходимы для проведения количественного анализа АДО? Объясните, как недостаток или недостоверность этих данных может повлиять на итоговую оценку вероятности верхнего события.
7. Почему перед построением дерева важно четко определить границы системы и уровень детализации анализа? К каким ошибкам или неточностям может привести несоблюдение этого принципа?
8. Каким образом человеческие ошибки (операторские ошибки, ошибки обслуживания и т.д.) моделируются и представляются в диаграмме дерева отказов?
9. Опишите ключевые ограничения методологии АДО. В каких ситуациях или для анализа каких типов систем АДО может оказаться неэффективным?
10. Как результаты АДО (в частности, ранжирование минимальных сечений по критичности) используются для обоснования инвестиций и приоритизации мероприятий по модернизации и техническому обслуживанию сложной технической системы?