FTA. ДЕРЕВО ОТКАЗОВ, КАК МЕТОД СТРУКТУРНОГО АНАЛИЗА.

03 марта 2009 года

Антон Алексеев,
тренер-консультант
IT Expert

Общая информация

В 1940 - 50-х годах теория надежности, как самостоятельная область знаний, получает распространение в основном в авиации, военной и ядерной индустрии. Фактически "родиной" теории надежности становятся в 1950 году США, что, прежде всего, связано с развитием электроники. Именно тогда министр обороны США выявил, что поддержание в работоспособном состоянии электронного оборудования стоимостью в 1 доллар обходится за год в 2 доллара. Стало очевидным, что следовало разрабатывать элементы системы изначально надежными. При этом системы были настолько сложными, а элементы системы влияли на такое большое число различных функций, что только самые четкие и неукоснительные действия обученного обслуживающего инженерного персонала могли обеспечивать минимально необходимый уровень надежности. В итоге, министр обороны при объявлении тендера на поставку электронного оборудования потребовал, чтобы производители оборудования по итогам длительных испытаний доказали надежность своего оборудования. Результаты этих испытаний и составили первую известную базу данных по надежности "Military Standard 217. Reliability prediction of electronic equipment".

Тогда же в 1962 году впервые был использован метод анализа дерева отказов (**fault tree analysis, FTA**) компанией Bell Labs для Военно-воздушных сил США, который на

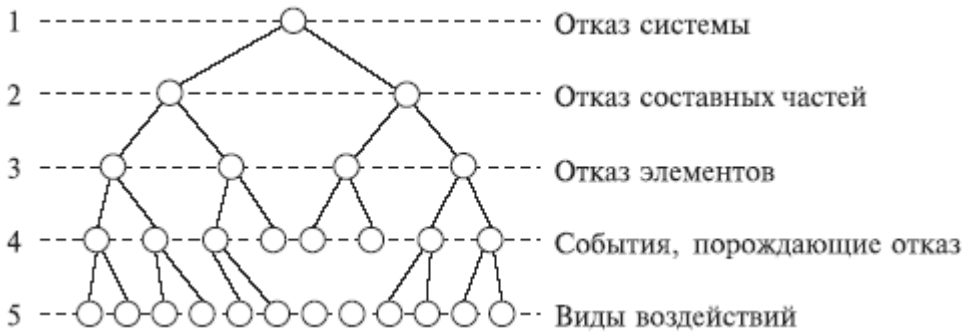
сегодняшний день получил широкое распространение для анализа причин отказов статичных систем.

Данный метод является частью национальных стандартов таких, например, как стандарт США «MIL-HDBK-217 Reliability prediction of electronic equipment» или российских «Методических указаний по проведению анализа риска опасных производственных объектов №РД 03-418-01»

Предназначение и область применения

Дерево отказов (аварий, происшествий, последствий, нежелательных событий и пр.) лежит в основе логико-вероятностной модели причинно-следственных связей отказов системы с отказами ее элементов и другими событиями (воздействиями). При анализе возникновения отказа, дерево отказов состоит из последовательностей и комбинаций нарушений и неисправностей, и таким образом оно представляет собой многоуровневую графологическую структуру причинных взаимосвязей, полученных в результате прослеживания опасных ситуаций в обратном порядке, для того чтобы отыскать возможные причины их возникновения (Рисунок 1. Условная схема построения дерева отказов).

Рисунок 1. Условная схема построения дерева отказов



Преимущества и ограничения применения

В этом способе реализован дедуктивный метод (причины - следствия), что наделяет метод самыми серьезными возможностями по поиску корневых причин событий для статичных систем, так как дает наглядную и подробную схему взаимосвязей элементов инфраструктуры и событий, влияющих на их надежность.

Ценность дерева отказов заключается в следующем:

- анализ ориентируется на нахождение отказов;
- позволяет показать в явном виде ненадежные места;
- обеспечивается графикой и представляет наглядный материал для той части ИТ специалистов, которые принимают участие в обслуживании системы;
- дает возможность выполнять качественный или количественный анализ надежности системы;
- метод позволяет специалистам поочередно сосредотачиваться на отдельных конкретных отказах системы;
- обеспечивает глубокое представление о поведении системы и проникновение в процесс ее работы;

- являются средством общения специалистов, поскольку они представлены в четкой наглядной форме;
- помогает дедуктивно выявлять отказы;
- дает конструкторам, пользователям и руководителям возможность наглядного обоснования конструктивных изменений или установления степени соответствия 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 или аварии.

Недостатки дерева отказов состоят в следующем:

- реализация метода требует значительных затрат средств и времени, так как увеличение детальности рассматриваемой инфраструктуры приводит к геометрическому увеличению числа влияющих событий;
- 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, содержащие 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 понимания системы и конкретного рассмотрения каждый раз только одного определенного отказа;
- дерево отказов описывает систему в определенный момент времени (обычно в установившемся режиме), и последовательности событий могут быть показаны с большим трудом, иногда это оказывается невозможным. Это справедливо для систем, имеющих сложные контуры регулирования, в таких случаях, как правило, обращаются к методам, основанным на стохастических (случайных) процессах.

Принцип использования

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

Логические символы. Логические символы (знаки) связывают события в соответствии с их причинными взаимосвязями. Обозначения логических знаков приведены в Таблица 1. Значение логических символов дерева отказов 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 стоящее справа зависело от появления стоящего слева. Таким образом, появление выходного события будет определяться появлением последнего события в ряду N - 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?".

Таблица 1. Значение логических символов дерева отказов

№	Символ логического знака	Название логического знака	Причинная взаимосвязь
1		И	Выходное событие происходит, если все входные события случаются одновременно
2		ИЛИ	Выходное событие происходит, если случается любое из входных событий
3		Запрет	Наличие входа вызывает наличие выхода тогда, когда происходит условное событие
4		Приоритетное И	Выходное событие случается, если все входные события происходят в нужном порядке слева направо
5		Исключающее ИЛИ	Выходное событие случается, если случается одно (но только одно) из выходных событий
6		«m из n» (голосования или выборки)	Выходное событие случается, если случается m из n входных событий

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?".

Порядок применения логических знаков И и ИЛИ. Для любого события, подлежащего дальнейшему анализу, вначале рассматриваются все возможные события, являющиеся входами операций ИЛИ, затем входы операций И. Это справедливо как для головного события, так и для любого события, анализ которого целесообразно продолжить.

Примеры этих двух логических знаков показаны на рис. Рисунок 5. Пример схемы построения дерева отказов с указанием вероятности событий.

Причинные связи, выраженные логическими знаками И и ИЛИ, являются детерминированными, так как появление выходного события полностью определяется входными событиями.

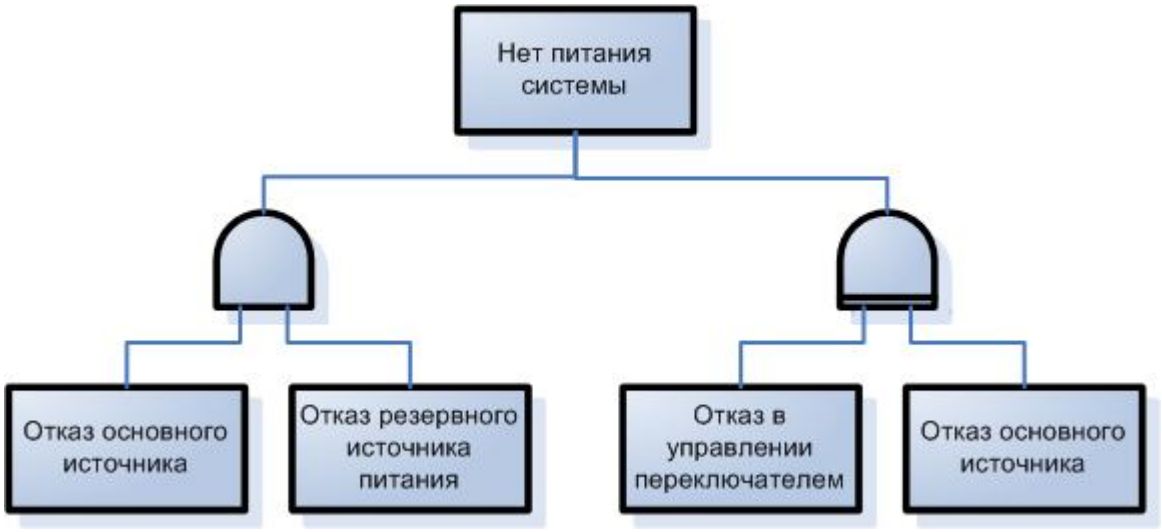
Логический знак запрета. Шестиугольник, являющийся логическим знаком запрета и расположенный в строке 3 Таблица 1. Значение логических символов дерева отказов, используется для представления вероятностных причинных связей. Событие, помещенное под логическим знаком запрета называется входным событием, в то время, как событие, расположенное сбоку от логического знака, называется условным событием. Условное событие принимает форму события при условии появления входного события. Выходное событие происходит, если и входное и условное событие имеют место. Другими словами, входное событие вызывает выходное событие с вероятностью (обычно постоянной) появления условного события. Логический знак запрета часто появляется в тех случаях, когда событие вызывается по требованию. Он используется главным образом для удобств и может быть заменен логическим знаком И.

Событие на выходе появляется, если события на входе происходят в определенной последовательности (слева направо). Появление событий на входе в другом порядке не вызывает события на выходе. Рассмотрим, например, систему, имеющую основной источник питания и резервный. Резервный источник питания включается в работу автоматически переключателем, когда отказывает основной источник. Питание в системе отсутствует, если:

- отказывают как основной, так и резервный источники;
- сначала выходит из строя переключатель, а затем отказывает основной источник питания.

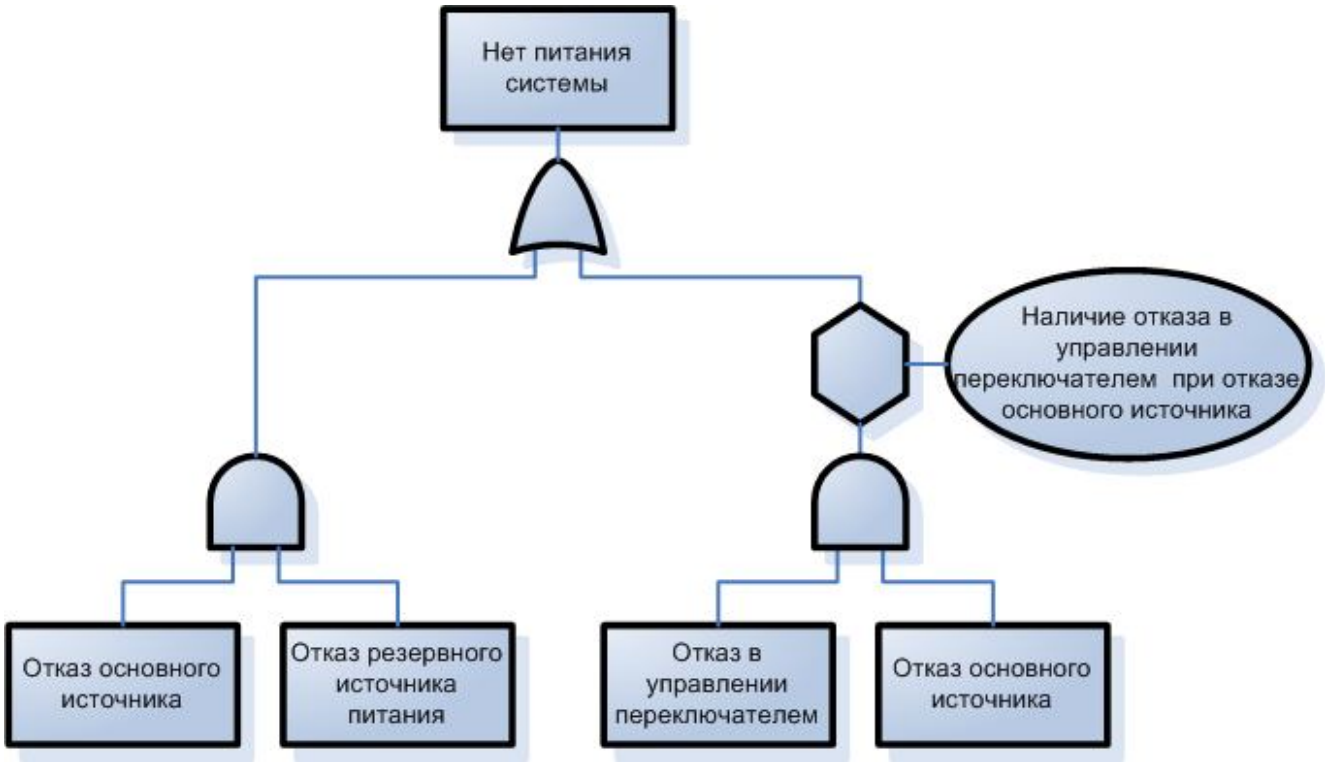
Предполагается, что, если за отказом переключателя следует отказ основного источника, это не приведет к потере питания при условии нормальной работы резервного источника. Логический символ "приоритетное И" может быть представлен сочетанием "логического И" и знака "запрета", а следовательно, эти логические знаки являются эквивалентом "логического И". Условным событием для "логического запрета" является то, что входные события логического знака И происходят в определенной последовательности. Пример показан на Рисунок 22. Пример использования логического знака «приоритетное И».

Рисунок 22. Пример использования логического знака «приоритетное И»



Логический символ "исключающее ИЛИ" (строка 5 в Таблица 1. Значение логических символов дерева отказов) описывает ситуацию, в которой событие на выходе появляется, если одно из двух (но не оба) событий происходят на входе. В качестве примера рассмотрим систему, питаемую от двух генераторов. Частичная потеря мощности может быть представлена элементом "исключающее ИЛИ". "Исключающее ИЛИ" может быть заменено комбинацией логических элементов И и ИЛИ, что проиллюстрировано на Рисунок3. Эквивалентное представление логического знака «исключающее ИЛИ. Обычно в дереве отказов избегают использования работоспособных состояний, таких как "генератор работает", так как они в значительной степени усложняют количественный анализ. Разумным подходом является замена логического знака "исключающее ИЛИ" комбинацией знаков И и ИЛИ.

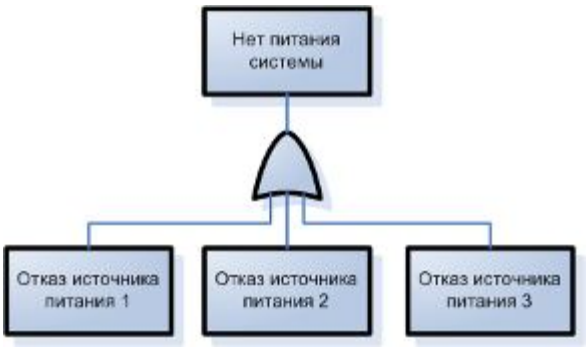
Рисунок3. Эквивалентное представление логического знака «исключающее ИЛИ»



Логический знак голосования m из n (строка 6 в Таблица 1. Значение логических символов дерева отказов) имеет n событий на входе, а событие на выходе появляется, если происходят по меньшей мере m из n событий на входе. Рассмотрим отказ системы, которая сохраняет работоспособность до отключения двух из трех источников питания. Предположим, что выключение системы происходит тогда и только тогда, когда два из трех источников питания вышли из строя. Таким образом, ненужное выключение системы происходит, если два или большее число контрольных приборов подадут ложный сигнал на выключение, в то время как система находится в нормальном состоянии.

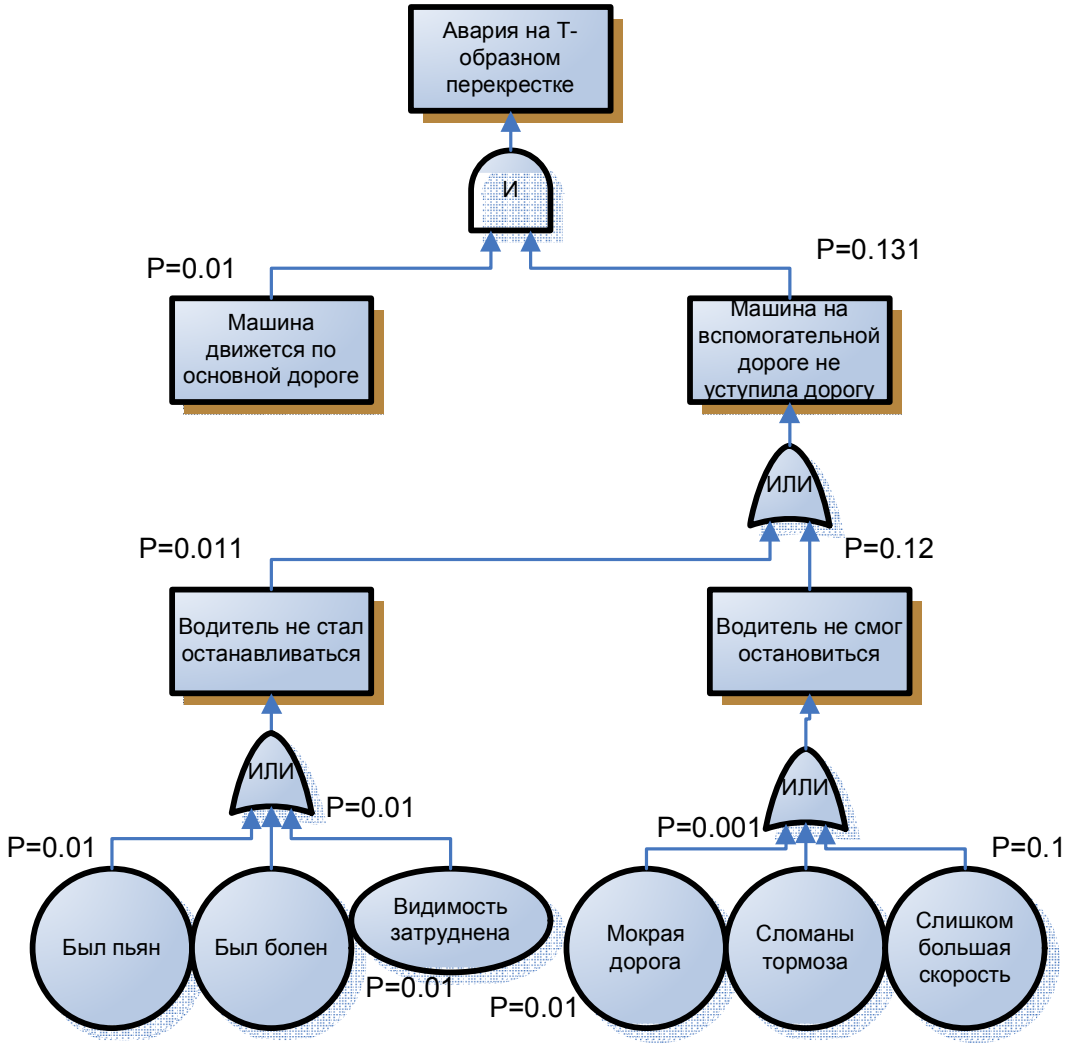
Эту ситуацию можно представить с помощью логического элемента "два из трех", как показано на рис. 4, а. Элемент голосования (выбора) эквивалентен комбинации из логических элементов И и ИЛИ.

Рисунок 4. Пример применения логического знака «два из трех»



Так же удобно использовать дерево отказов в сочетании с вероятностями возникновения тех или иных событий. Пример такого дерева приведен для анализа причин автомобильных аварий на Т-образном перекрестке, который показан на Рисунок 5. Пример схемы построения дерева отказов с указанием вероятности событий

Рисунок 5. Пример схемы построения дерева отказов с указанием вероятности событий



Метод анализа дерева отказов (fault tree analysis, FTA) способствует тщательному анализу причин отказов технических систем и выработке мероприятий, наиболее эффективных для их устранения. Такой анализ проводят для каждого периода функционирования, каждой части или системы в целом.

Вопросы по этой теме обсуждаются на следующих курсах:

- Служба поддержки пользователей: Service Desk, управление инцидентами и проблемами
- ITIL v3 Operational Support and Analysis: поддержка сервисов
- Основы ITIL v3 (ITIL v3 Foundation)
- Основы ITIL (ITIL Foundation)

Данная заметка отражает мнение автора, которое может не совпадать с уважаемыми первоисточниками (ITIL v2, ITIL v3, CobiT, MOF и проч.). Комментарии и предложения темы для следующей заметки можно отправлять на items@itexpert.ru.