Группа Т59

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Менеджмент риска

АНАЛИЗ ДЕРЕВА СОБЫТИЙ

Risk management. Event tree analysis

ОКС 21.020

Дата введения 2015-12-01

Предисловие

1 ПОДГОТОВЛЕН Открытым акционерным обществом "Научно-исследовательский центр контроля и диагностики технических систем" (АО "НИЦ КД") на основе собственного аутентичного перевода на русский язык международного стандарта, указанного в разделе 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 10 "Менеджмент риска"

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 24 октября 2014 г. N 1429-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 62502:2010* "Аналитические методы надежности. Анализ дерева событий (ETA)" (IEC 62502:2010 "Analysis techniques for dependability - Event tree analysis (ETA)").

_____

* Доступ к международным и зарубежным документам, упомянутым здесь и далее по тексту, можно получить, перейдя по ссылке на сайт http://shop.cntd.ru. - Примечание изготовителя базы данных.

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5-2012 (подраздел 3.5).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты Российской Федерации, сведения о которых приведены в дополнительном приложении ДА

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в ГОСТ Р 1.0-2012 *(раздел 8). Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе "Национальные стандарты", а официальный текст изменений и поправок - в ежемесячном информационном указателе "Национальные стандарты". В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя "Национальные стандарты". Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования - на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети*

Интернет (www.gost.ru)

Введение

В настоящем стандарте установлены основные принципы метода анализа надежности называемого "Анализ дерева событий" (ETA). Этот метод используют также для анализа риска и безопасности. Основные принципы метода установлены в 1960 г. Метод ETA впервые был применен для анализа объектов атомной промышленности в США. Затем он получил широкое распространение, как метод анализа надежности и риска и применялся для анализа надежности ядерных установок, аэрокосмических систем, химических процессов, установок по добыче нефти и газа, транспортных систем и др.

В противоположность другим методам анализа надежности, например Марковскому методу, ETA основан на относительно простых математических выводах. Однако применение метода требует наличия специальных навыков, опыта и внимательности. Кроме того обычно полезно использовать взаимосвязь анализа дерева неисправностей (FTA) с количественным и качественным анализом дерева событий.

В настоящем стандарте установлены общие принципы ETA и показано его применение для анализа параметров систем, относящихся к надежности и риску.

1 Область применения

В настоящем стандарте установлены основные принципы метода ETA[1)] (анализ дерева событий) и приведено руководство по моделированию последствий инициирующих событий, а также качественному и количественному анализу показателей надежности и риска.

[1)] ETA - Event tree analysis.

В настоящем стандарте по отношению к анализу дерева событий установлены:

a) основные термины, используемые обозначения и способы графического представления;

b) этапы процедуры построения дерева событий;

c) предположения, ограничения и преимущества анализа ETA;

d) взаимосвязь ETA с другими методами анализа надежности и риска и области применения метода;

e) рекомендации по определению качественных и количественных оценок;

f) практические примеры применения метода.

Настоящий стандарт применим во всех случаях, когда необходимо определить оценки показателей надежности и риска.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты*:

_____

* Таблицу соответствия национальных стандартов международным см. по ссылке. - Примечание изготовителя базы данных.

МЭК 60050-191:1990 Международный электротехнический словарь. Глава 191: Надежность и качество обслуживания (IEC 60050-191:1990, International electrotechnical vocabulary; chapter 191: dependability and quality of service)

МЭК 61025:2006 Анализ дерева отказов (FTA) [IEC 61025:2006, Fault tree analysis (FTA)]

3 Термины, определения, сокращения и обозначения

В настоящем стандарте применены термины по МЭК 60050-191, а также следующие термины с соответствующими определениями.

3.1 Термины и определения

3.1.1 узел (node): Точка в графическом представлении дерева событий, имеющая два или более выходов.

Примечание - Узлу дерева событий может соответствовать вершина событий соответствующего дерева неисправностей.

3.1.2 общая причина (common cause): Причина реализации одновременно нескольких событий (кратных событий).

[МЭК 61025:2006, 3.15]

Примечание - В некоторых случаях должен быть определен период, в течение которого происходят эти события, например, несколько событий происходят одновременно или в течение короткого промежутка времени.

Пример - ***Природные опасности (например, пожар, наводнение), отказы технических систем, заражение инфекцией или действия человека.***

3.1.3 **событие** (event): Возникновение условия или воздействия.

[МЭК 61025:2006, 3.8]

3.1.4 **заголовок** (headings): Фактор защиты, указанный на линии, расположенной над графическим изображением дерева событий.

3.1.5 **инициирующее событие** (initiating event): Событие, которое является отправной точкой дерева событий и последовательности событий, которые могут привести к различным возможным выходам.

3.1.6 **фактор защиты** (mitigating factor): Система, функция или другой косвенный фактор, смягчающий последствия инициирующего события.

Примечание - Во многих отраслях промышленности существуют эквивалентные термины, например, линия обороны, линия защиты, система защиты, барьер безопасности, линия гарантии, фактор снижения риска и т.д.

3.1.7 **выход** (outcome): Возможный результат последовательности событий после всех воздействий

рассмотренных факторов защиты, если дальнейшей разработки дерева событий не требуется.

3.1.8 **последовательность событий** (sequence): Цепочка событий от инициирующего события к последующим событиям, приводящая к определенному выходу.

3.1.9 **главное событие, вершина событий** (top event): Установленное неблагоприятное событие, которое является отправной точкой и главной целью анализа дерева неисправностей. Это событие занимает высшую позицию в структуре дерева неисправностей.

Примечание - Главное событие (вершина событий) является результатом комбинации всех входных событий.

3.1.10 **ветвь** (branch): Графическое представление одного, двух или более возможных выходов из узла.

3.2 Сокращения и обозначения

3.2.1 Сокращения

CCA[1)] - анализ причин и последствий;

[1)] CCA - Cause-Consequence Analysis.

ETA - анализ дерева событий;

FMEA[2)] - анализ видов и последствий отказов;

[2)] FMEA - Failure Mode and Effects Analysis.

FTA[3)] - анализ дерева неисправностей;

[3)] FTA - Fault Tree Analysis.

IRF[4)] - индивидуальный риск гибели человека;

[4)] IRF - Individual Risk of Fatality.

LESF[5)] - комбинация двух методов анализа надежности: больших деревьев событий (LE) и соответствующих небольших деревьев неисправностей (SF);

[5)] LESF - Large Event Trees (LE), Small Fault Trees (SF).

LOPA[6)] - анализ уровней защиты;

[6)] LOPA - Layers Of Protection Analysis.

RBD[7] - метод структурной схемы надежности;

[7] RBD - Reliability Block Diagrams.

PRA[8] - вероятностная оценка риска;

[8] PRA - Probabilistic Risk Assessment.

PRA/PSA[9] - анализ вероятностной оценки риска/безопасности;

[9] PRA/PSA - Probabilistic Risk/Safety Analysis.

SELF[10] - комбинация двух методов анализа надежности: небольших деревьев событий (SE) и больших деревьев неисправностей (LF).

[10] SELF - Small Event Trees (SE), Large Fault Trees (LF).

3.2.2 Обозначения

A - реализовавшееся событие A (прописная буква, записанная курсивом);

$\overline{A}$ - нереализовавшееся событие A (прописная буква, записанная курсивом с черточкой наверху);

I_E - реализовавшееся инициирующее событие (курсив);

$O_{I_E, A,B}$ - выход, получаемый в результате реализации всех событий, указанных в индексе (прописными курсивными буквами, разделенными запятыми) в указанном в индексе порядке (см. пример на рисунке 3);

α,..., σ - выходы дерева событий (строчные греческие буквы);

"+" - логическое "ИЛИ";

"." - логическое "И";

P(A) - вероятность события A. *P(A)* - действительное число из закрытого интервала [0,1], установленное для события A, см. [25];

$P(I_E . A. \overline{B} . \overline{C})$ - вероятность того, что инициирующее событие I_E и событие A произошли, а события B и C не произошли;

$P(A\backslash I_E)$ - вероятность события A, при условии реализации инициирующего события I_E;

f - частота (количество событий в единицу времени, см. [25]);

f_δ - частота выхода δ.

4 Общее описание метода

Анализ дерева событий является индуктивной процедурой, предназначенной для моделирования возможных выходов, являющихся следствием реализации данного инициирующего события и состояний факторов защиты, а также определения оценок частоты или вероятности возможных выходов данного инициирующего события.

Графическое представление дерева событий требует, чтобы символы, идентификаторы и метки были использованы последовательно. Представление дерева событий зависит от предпочтений пользователя. Наиболее часто используемое графическое представление приведено в приложении А.

Начиная с инициирующего события, в процессе анализа ETA исследователи постоянно ищут ответ на вопрос "Что произойдет, если ...". Опираясь на полученные ответы, аналитик строит дерево возможных выходов. Поэтому крайне важно составить перечень всех возможных инициирующих событий. Это обеспечивает то, что построенные деревья событий отражают все важные последовательности событий для рассматриваемой системы. Используя эту логику, ETA можно трактовать как метод представления применимых факторов защиты для данного инициирующего события.

Анализ ETA помогает идентифицировать все возможные варианты сценария развития неблагоприятного события (выделяя на дереве событий ветви успеха или срабатывания и отказа или несрабатывания фактора защиты), конструкции разрабатываемого объекта и выявить слабые места процедуры. Ветвь успеха является моделью условий, в которых фактор защиты действует в соответствии с его назначением (срабатывает). Как и в случае других аналитических методов, особое внимание следует уделять моделированию зависимости событий, учитывая, что вероятности, используемые в дереве событий, являются условными на последовательности событий, которые произошли до реализации рассматриваемого события. В разделе 8 рассмотрены качественные аспекты анализа, а также основные количественные правила вычисления оценок вероятности или частоты (1/ч) для каждого выхода. Несмотря на то, что теоретически с помощью дерева событий можно моделировать последствия ошибок оператора или программного обеспечения, в настоящем стандарте эти вопросы не рассмотрены. Анализу этих проблем посвящены другие стандарты МЭК, например, МЭК 62508 [23] и МЭК 62429 [22].

Преимущества ETA для анализа надежности и риска, а также его ограничения, рассмотрены в разделе 5. Примером ограничений ETA является исследование временных зависимостей. Оценки в такой ситуации необходимо определять очень осторожно, поскольку это может быть правильно сделано только в отдельных случаях. Для исследования временных зависимостей разработаны специальные методы, такие как метод динамического анализа дерева событий. Метод динамического анализа дерева событий не рассмотрен в настоящем стандарте, однако, соответствующие ссылки включены в библиографию.

Метод ETA тесно связан с методом FTA, поскольку вероятность главного события FTA позволяет определить условную вероятность для узла ETA. Это более полно описано в разделе 6, где рассмотрена связь между ETA и другими аналитическими методами, такими как анализ причин и последствий (CCA) и анализ уровней защиты (LOPA). Метод CCA комбинирует анализ причин с анализом последствий и использует дедуктивный и индуктивный анализ. Метод LOPA был разработан для перерабатывающей промышленности в виде специальной адаптации ETA.

В разделе 7 установлена процедура построения дерева событий, начинающаяся с четкого определения исследуемой системы. Кроме того, в разделе 7 рассмотрены различные аспекты исследуемой системы (технический, человеческий и функциональный) и необходимая глубина анализа. Другой важной задачей является составление перечня соответствующих инициирующих событий.

На рисунке 1 изображены основные этапы выполнения ETA. Следует учитывать, что процесс разработки дерева событий является итерационным.

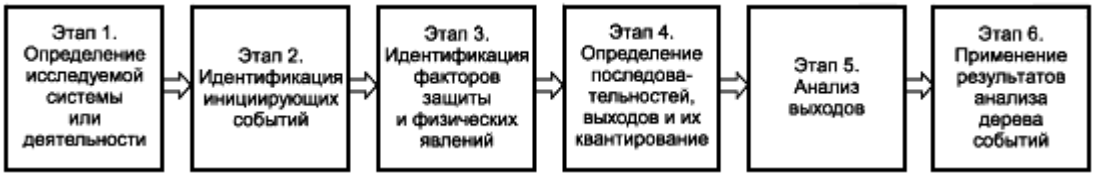


Рисунок 1 - Процесс разработки дерева событий

В разделе 9 кратко указаны требования к документированию анализа и его результатов.

В приложении А приведены наиболее используемое графическое представление дерева событий. В приложение В приведены примеры ETA для характерных областей его использования.

5 Преимущества и ограничения ETA

5.1 Преимущества метода ETA

Метод ETA обладает следующими преимуществами. Метод

a) применим к системам любого типа;

b) обеспечивает визуальное представление последовательности событий после реализации инициирующего события;

c) позволяет получить оценку нескольких одновременных отказов системы (например, дефект системы контроля) или ее отказов (например, неспособность клапана закрываться), а также других зависимых событий;

d) применим для исследования, как успеха (нормального функционирования), так и отказа системы;

e) позволяет идентифицировать конечные события, которые иначе невозможно прогнозировать;

f) позволяет идентифицировать возможные единичные отказы, области уязвимости системы и малоэффективные контрмеры. Метод обеспечивает оптимальное распределение ресурсов и улучшение контроля риска через улучшение процедур и функций безопасности;

g) допускает идентификацию и прослеживаемость путей развития отказа системы;

h) позволяет представлять большие и сложные системы в виде более простых с помощью группировки частей исследуемой системы в функциональные единицы или подсистемы.

Преимуществом ETA по сравнению со многими другими методами анализа риска является его способность моделировать последовательности и взаимодействия различных факторов защиты, сопровождающих появление инициирующего события. Таким образом, система и ее взаимодействия со всеми факторами защиты при развитии неблагоприятного сценария становятся наглядно представленными, что способствует для дальнейшей оценки риска.

5.2 Ограничения метода

К ограничениям ETA относятся ограничения, общие для всех методов анализа надежности:

a) инициирующие события не могут быть выявлены с помощью анализа, это задача специалистов, составляющих общий перечень инициирующих событий;

b) при использовании метода необходимо вовлечение специалистов, составляющих общее описание сценариев функционирования системы;

c) могут быть пропущены скрытые системные зависимости, что приводит к излишне оптимистичным оценкам показателей надежности и риска;

d) для правильного вычисления условных вероятностей и корректной обработки зависимых событий необходим практический опыт работы с методом, а также предыдущие результаты исследования системы;

e) оценка и обработка вероятностей, зависящих от времени может быть выполнена только если истинная вероятность или интенсивность отказов системы постоянна или если для восстанавливаемой системы быстро наступает устойчивое неработоспособное состояние. Это следует учитывать в случае периодически проверяемых систем;

f) другой трудный аспект работы с временной зависимостью охватывает быстро меняющиеся ситуации, например, когда критерии успеха факторов защиты изменяются в зависимости от срабатывания предшествующих факторов защиты. Обычно в этом случае делают предположения, обеспечивающие получение гарантированных оценок;

g) ситуации, когда пребывание объекта в некотором состоянии более установленного времени может привести к отказу, трудно смоделировать с помощью дерева событий (например, медленная утечка воздуха из автомобильной камеры);

h) зависимости в дереве событий, например, из-за зависимостей инициирующего события от факторов защиты, необходимо внимательно исследовать. Однако существует лишь несколько методов анализа подходящих для обработки зависимых отказов. Для этого может оказаться подходящей комбинация FTA и ETA;

i) несмотря на то, что может быть идентифицировано несколько последовательностей событий, приводящих к отказу системы, различия в значимости опасностей, связанных с конкретными выходами могут быть не различимы без дополнительного анализа.

6 Взаимосвязь с другими аналитическими методами

6.1 Комбинация ETA и FTA

На практике ETA иногда выполняют как самостоятельный анализ, а в других случаях в комбинации с FTA.

Метод FTA позволяет идентифицировать и анализировать условия и факторы, вызывающие или способствующие реализации конкретного опасного события (см. МЭК 61025).

Использование комбинации ETA и FTA позволяет преодолеть многие из недостатков ETA, например, при количественном анализе могут быть учтены отказы общей причины (отказы по общей причине). Таким образом, комбинация ETA и FTA является мощным методом анализа надежности и риска.

Обычно используют комбинацию ETA и FTA (иногда называемую анализом причин и последствий (CCA)) (см. [30], [36]). Метод FTA может быть использован для определения оценки частоты/реализации инициирующего события в ETA. Следует заметить также, что условные вероятности событий в последовательности событий часто вычисляют с помощью FTA. Одним из примеров, где использованы ETA и FTA, является метод PRA (вероятностная оценка риска), разработанный первоначально для анализа надежности атомной электростанции.

В принципе, развитие любого инициирующего события может быть исследовано с помощью ETA. Однако в некоторых случаях это может быть невозможно по одной из следующих причин:

a) итоговые деревья могут стать очень сложными и необозримыми;

b) иногда легче разработать взаимосвязи причин, чем последовательность событий;

c) часто имеются отдельные команды, выполняющие функциональный и технический анализ. Однако

зависимости между функциональной областью (например, правилами выполнения процедур, технического обслуживания) и технической областью (исследуемой системой) не всегда ясны в начале анализа. Таким образом, на практике, возможные события, связанные с зависимостями функциональной и технической областей определяют в первую очередь. В частности, обычно единичные отказы исключены конструкцией системы, например, вследствие отказоустойчивого проектирования, и таким образом, метод ETA не должен привести непосредственно к тяжелым последствиям при реализации единичного отказа без дальнейших возможных факторов защиты.

Можно выбрать один из двух подходов для объединения дерева событий и дерева неисправностей. Один подход - это подход LESF. Если дерево событий имеет тенденцию становиться необозримо большим, может быть использован подход SELF.

В подходе LESF состояние всех систем, которые поддерживают работу исследуемой системы (далее системы поддержки) представляют в виде деревьев событий. Главные события деревьев неисправностей имеют граничные условия, которые включают предположение о том, что системы поддержки находятся в конкретном состоянии, соответствующем исследуемой последовательности событий. Отдельные деревья неисправностей используют для каждого набора граничных условий исследуемой системы. Эти отдельные деревья неисправностей, полученные из единственного дерева неисправностей, которое включает системы поддержки, связанные с конкретной последовательностью событий, обусловлены состоянием систем поддержки. Этот подход представляет LESF, позволяющий явно представить существующие зависимости. Так как они связаны с меньшими деревьями неисправностей, они требуют меньших компьютерных ресурсов и применения менее сложных компьютерных программ. Однако сложность деревьев событий быстро увеличивается с увеличением количества систем поддержки и состояний каждой системы поддержки, которые представлены в дереве событий. Кроме того, процесс определения количественных оценок является достаточно громоздким и зависит от возможных оплошностей и ошибок человека. Подход LESF не позволяет явно определить, какие комбинации отказов систем поддержки приводят к отказу исследуемой системы (эти комбинации иногда называют "линией фронта системы"). Упрощенный пример такого большого дерева событий представлен на рисунке B.1 (см. также [31]).

В подходе SELF деревья событий с инициирующим событием и функциями защиты, выполняемыми различными системами защиты, указанными в головке таблицы выше изображения дерева событий, сначала разрабатывают, а затем расширяют до деревьев событий со статусом линии фронта системы. Модели дерева неисправностей системы разрабатывают от линии фронта системы к границам с системами поддержки. Деревья неисправностей систем поддержки могут быть разработаны отдельно и затем объединены в моделях линии фронта системы. Такой подход формирует деревья событий, которые являются более краткими и допускают объединенное представление последовательности неблагоприятных событий. Кроме того, небольшие деревья событий более доступны для составления компьютерных программ. Однако, зависимости и значимость соответствующих систем поддержки остаются не выявленными. Теоретический пример такого небольшого дерева событий представлен на рисунке B.3 (см. [4]).

6.2 Анализ уровней защиты (LOPA)

Метод LOPA представляет собой особую стандартизированную форму ETA, которую используют в качестве метода упрощенного анализа риска, адаптированного для конкретных условий. Метод LOPA применяют в форме рабочего листа, аналогично применяемому при выполнении анализа видов и последствий отказов (FMEA). Инициирующие события фиксируют в строках, а различные уровни защиты (представляющие стандартизованные факторы защиты) - в колонках. Таким образом, любую последовательность событий, представленную в соответствии с LOPA, можно также рассматривать как данные для ETA. Для целей анализа риска уровни значимости (или опасности) также объединяют в рабочий лист.

Поэтому LOPA можно рассматривать как ETA с ограниченным набором возможных факторов защиты для конкретных условий. Метод обычно используют в промышленности. Более подробно метод LOPA описан в [1] и [5].

6.3 Комбинация с другими методами

Метод ETA может быть объединен с любым другим методом, пригодным для определения вероятности успеха или отказа соответствующих факторов защиты (например, методом Маркова или блок-схемы надежности (RBD), см. [16]), но в этом случае, другие методы служат только дополнением ETA.

В сложных случаях или при зависимости функционирования системы от времени (см. 8.3.2), можно использовать Марковские методы с учетом всех имеющихся ограничений. Для получения дополнительной информации см. [17].

Другим близким методом анализа надежности является анализ видов и последствий отказов (FMEA) (см. [13]), который является формализованной процедурой анализа системы для выявления возможных видов отказов системы, их причин и последствий. Метод FMEA помогает идентифицировать значимость возможных отказов и установить, какие факторы защиты включает конструкция для снижения вероятности отказов системы до допустимого уровня. Первым этапом разработки дерева событий может быть идентификация основных отказов системы, как возможных инициирующих событий.

Методы Марковского моделирования, RBD и FMEA установлены соответственно в МЭК 61165 [17], МЭК 61078 [16] и МЭК 60812 [15].

7 Разработка дерева событий

7.1 Общие положения

События, определяющие последовательности событий, обычно характеризуют по:

a) функциям: выполнение (не выполнение) функций, как фактор защиты;

b) системам: воздействие (или нет) систем защиты как факторов защиты, которые по предположению должны предотвратить развитие инициирующего события в неблагоприятную ситуацию, уменьшить неблагоприятные последствия или привести к отказу факторов защиты;

c) физическим явлениям: возникновение или не возникновение физических явлений.

Как правило, идентифицируют вначале функции, которые необходимо выполнить после реализации инициирующего события, а затем системы (факторы защиты), которые могут выполнить эти функции. Физические явления описывают развитие неблагоприятного события, имеющее место внутри и снаружи исследуемой системы (например, изменение давления и температуры, появление огня, ядовитых паров и т.п.).

Область применения и цель ETA должны быть четко определены до выполнения действий в соответствии с 7.2.

7.2 Этапы выполнения ETA

7.2.1 Общая процедура

Процедура выполнения ETA (см. рисунок 1) состоит из шести этапов:

Этап 1. Определение исследуемой системы или деятельности (см. 7.2.2)

Устанавливают границы системы или деятельности, для которых необходимо выполнить ETA.

Этап 2. Идентификация исследуемых инициирующих событий (см. 7.2.3)

Проводят общее рассмотрение (скрининг) всех событий для идентификации событий или категорий событий, рассматриваемых в ETA. Категории событий могут включать столкновения, возгорания, взрывы, ядовитые выбросы и т.п.

Этап 3. Идентификация факторов защиты и физических явлений (см. 7.2.4)

Выявляют факторы защиты, которые могут повлиять на развитие инициирующего события до его неблагоприятных последствий. Факторы защиты охватывают как технические системы, так и действия/решения людей. Кроме того, идентифицируют физические явления и вторичные события, такие как возгорание или метеорологические условия, способствующие развитию неблагоприятной ситуации и инициирующего события. Дерево событий должно включать все факторы защиты и физические явления (см. 7.1).

Этап 4. Определение последовательности событий и выходов, определение их количественных параметров (см. 7.2.5)

Для каждого инициирующего события определяют возможные выходы (например, сценарии несчастного случая) и выполняют их количественный анализ на основе построенного дерева событий.

Этап 5. Анализ выходов (см. 7.2.6)

Выходы анализируют в отношении их последствий и воздействий на результаты анализа.

Этап 6. Использование результатов ETA (см. 7.2.7)

На основе качественных и количественных результатов анализа определяют необходимые действия.

7.2.2 Этап 1. Определение исследуемой системы или деятельности

При выполнении ETA рассматривают способы развития инициирующего события в опасное событие, включая отказы различных факторов защиты. Внимательные идентификация и исследование факторов защиты являются важным этапом оценки эффективности.

Очень мало реальных систем работает в изоляции. В большинстве случаев система взаимодействует с другими системами. Четко определяя границы системы, в особенности при наличии систем поддержки, таких как электроснабжение и обеспечение сжатым воздухом, аналитики могут избежать пропуска основных элементов системы в интерфейсах или ошибочного рассмотрения в качестве элементов системы другого оборудования.

Теоретически в ETA можно включать все события и условия, которые могут способствовать реализации определенного выхода или обеспечить некоторый уровень защиты от исследуемого опасного события. Однако включать все возможные выходы в исследование не практично. Во многих исследованиях определяют такие аналитические границы как:

a) предельный уровень анализа (например, аналитик при изучении навигационной системы может принять решение детально не анализировать проблемы системы распределения электроэнергии);

b) исключение из анализа определенных типов событий или условий, таких как саботаж.

Начальное состояние системы, включая оборудование уже вышедшее из строя, связано с комбинацией событий, приводящей к последующим выходам. Например, если защитная блокировка регулярно удаляется из обслуживания, дерево событий должно быть изменено для отражения измененных сценариев, связанных с потенциально более высоким риском.

7.2.3 Этап 2. Идентификация исследуемых инициирующих событий

На этом этапе обычно используют различные методы идентификации опасностей такие как: "что - если", предварительная оценка или предварительный анализ опасности для проведения систематической оценки действий в рамках исследования. Этот этап помогает идентифицировать опасности и возможные инициирующие события, которые являются следствием этих опасностей. Такие методы идентификации направлены на исследования всех действий в области определения анализа и идентификацию всех возможных инициирующих событий и выходов, связанных с этими событиями. Общий список и описание методов приведены в [12]. В результате идентификации обычно формируют список возможных событий и их последствий.

Затем должна быть поставлена общая цель идентификации всего спектра событий, которые могут произойти в области определения ETA. После того, как это сделано, аналитики применяют критерии скрининга (сплошной проверки), чтобы идентифицировать инициирующие события, которые необходимо рассмотреть в деревьях событий. В основном существует два способа отбора инициирующих событий, а именно, исключение событий с маловероятным сочетанием физических свойств (например, не превышение установленных значений давления или температуры при пожаре) или инициирующих событий с низкой частотой реализации при определении гарантированной оценки. Этот этап помогает идентифицировать события, которые должны быть проанализированы далее для понимания сложных взаимодействий систем. В процессе анализа необходимо проверить возможность всех взаимодействий инициирующих событий и факторов защиты, например, могут ли условия, вызванные инициирующим событием, таким как потеря всех энергоресурсов после землетрясения,

оказать негативное влияние на действие факторов защиты.

После анализа начального перечня событий оставшийся перечень инициирующих событий включает события, которые должны быть рассмотрены в деревьях событий. Это события, которые идентифицированы опытными экспертами как достаточный комплекс событий для дополнительного анализа отдельной системы и взаимодействий персонала, которые вызывают различные выходы инициирующего события.

Если имеется много событий, для которых необходимо построить деревья событий, инициирующие события объединяют в несколько категорий, таких как столкновения, пожары, взрывы, ядовитые выбросы и т.п. В некоторых случаях такая классификация может быть не применима. Например, если целью исследования является идентификация диапазона выходов, связанных только с пожаром, на этапе скрининга должна быть проведена сортировка, исключающая все события, не связанные с пожаром.

Инициирующие события, сгруппированные в одну категорию, требуют вмешательства одних и тех же факторов защиты и приводят к аналогичным результатам.

7.2.4 Этап 3. Идентификация факторов защиты и физических явлений

Как только инициирующее событие определено, все факторы защиты при развитии опасного события должны быть определены и организованы в соответствии с их временем действия. Они состоят из технических компонентов, таких как система предупреждения, блокирующие устройства, автоматические клапаны, административная система и персонал (например, пожарная команда, аварийная бригада, а также обнаружение опасности человеком посредством наблюдений, осязательных, слуховых, вкусовых и обонятельных ощущений).

Функции, выполняемые вышеупомянутыми компонентами или факторами защиты, структурируют в форме заголовков в функциональном дереве событий. Для каждой функции должны быть идентифицированы, перечислены и пронумерованы возможные успехи и отказы. Каждый набор успехов или отказов, связанный с фактором защиты дает узел дерева событий, не обязательно ограниченный двумя ветвями.

Физические явления также могут влиять на выход инициирующего события. Например, на случай выброса огнеопасной жидкости могут быть предусмотрены технические средства обеспечения безопасности для изоляции утечки. Однако, если утечка не изолирована, то окончательный выход, связанный с выбросом, зависит от таких физических явлений, как мгновенное возгорание, отсроченное возгорание или особенности разброса жидкости. Эти физические явления также моделируют в виде узлов дерева событий.

В системном анализе, требующем большого количества деревьев событий для инициирующих событий, возникающих одновременно в течение короткого периода времени, может быть упрощено объединением их в категории в соответствии с их фактором защиты. Это позволяет одни и те же элементы дерева событий (т.е. факторы защиты с одним и тем же отказом или успехом) использовать для различных исследуемых инициирующих событий. Если факторы защиты адекватно реагируют на события, то частоты отдельных событий могут быть просуммированы по всем событиям класса. Более детальная информация приведена в 8.3.

7.2.5 Этап 4. Определение последовательностей событий, выходов и их количественных параметров

Одним из преимуществ ETA является способность метода моделировать порядок воздействия и взаимодействия различных систем, реагирующих на инициирующее событие. Таким образом, воздействия различных систем могут быть смоделированы "одно за другим". При выполнении соответствующих расчетов для этих взаимодействий аналитик должен:

- определить логическое развитие инициирующего события через различные факторы защиты к возможным выходам и сценариям опасного события;

- идентифицировать зависимости факторов защиты;

- подсчитать условные вероятности успеха/отказа одной системы с учетом действия или состояния предыдущих систем;

- построить дерево событий.

Конечно, не все инициирующие события (в том числе отказы системы) приводят к катастрофическим результатам. Также не каждый фактор защиты или блокирующее устройство используют при реализации события. Логическое развитие инициирующего события происходит в виде последовательности реализации событий во времени до появления опасных последствий (выхода). В процессе реализации последовательности

событий их последствия становятся все более значимыми. Системы на это реагируют по-разному. Понимание развития событий и синхронизация реакций системы и физического отклика важны для разработки логики дерева событий. Например, при воспламенении отходов, реакцией персонала являются действия по их тушению с помощью огнетушителей, если персонал присутствует и огнетушители доступны. Полную систему противопожарной защиты и пожарную команду не задействуют, если значимость опасности не велика.

Большая часть систем связана или взаимодействует с другими элементами и процессами. Эти взаимодействия или зависимости влияют, как правило, в худшую сторону на уровень защиты, обеспечиваемый резервирующими системами, которые совместно используют некоторое оборудование. В примере нефтяного танкера с резервированным управлением двигательными установками, отказы каждой системы, скорее всего, являются зависимыми, если системы управления используют общую гидравлическую систему.

Для определения количественных оценок дерева событий используют условные вероятности. Таким образом, вероятность определенного события (например, успеха или отказа) для фактора защиты является условной в зависимости от предшествующих событию реакций факторов защиты.

Рекомендуемый процесс построения дерева событий состоит из следующих этапов:

a) инициирующее событие размещают сначала в левой стороне дерева событий;

b) факторы защиты и физические явления размещают в направлении развития дерева событий в хронологическом (или) функциональном порядке, в котором они влияют на развитие опасного события;

c) определяют успех (обычно ему соответствует верхняя ветвь) и отказ (обычно ему соответствует нижняя ветвь) для каждого фактора защиты в каждом узле, учитывая следующее:

1) некоторые узлы могут иметь более двух результатов и должны иметь соответствующее количество ветвей (см. приложение А);

2) некоторые узлы могут иметь только один результат; в этом случае через такой фактор защиты проходит прямая линия. В этом случае условная вероятность равна 1,0. Фактор защиты не зависит от предыдущего успеха или отказа другого фактора защиты.

Эти этапы иллюстрированы в приложении А и на рисунках В.1 и В.4 на примерах железнодорожного переезда и электростанции.

Количественный анализ более подробно приведен в 8.3 и в примере В.2.6.

7.2.6 Этап 5. Анализ выходов

Выходами ETA являются конечные ветви дерева событий. Каждый выход может быть оценен качественно или количественно. В рассмотренном случае выходы идентифицируют различные последовательности событий, возникающие при реализации исследуемого инициирующего события. Количественная оценка обеспечивает лучшее понимание относительной значимости факторов защиты, поскольку выходы в этом случае характеризуют частотой. Для количественной оценки ETA необходимы соответствующие достоверные данные о реализации события.

Иногда удобно разделить возможные выходы на несколько категорий в соответствии с типом последствий (потеря жизни, материальные потери, вред окружающей среде и т.п.). Количество выходов дерева событий зависит от того, какие типы выходов должны быть проанализированы, например:

a) отказ или нарушение функционирования системы;

b) разрушение системы;

c) значимые воздействия на окружающую среду;

d) гибель людей.

Для практической оценки большого количества выходов полезно классифицировать и группировать выходы так, чтобы упростить результаты.

7.2.7 Этап 6. Использование результатов ETA

Результаты ETA могут быть использованы для принятия решения, которое может способствовать повышению надежности и уменьшению риска на основе известных методов и организационных действий. Корректирующие действия могут включать изменение архитектуры системы, рабочих процессов, правил технического обслуживания и т.д.

В частности, решения, которые основаны на выполнении анализа, могут быть следующими:

a) риск является допустимым или нет: решение принимают с учетом последствий соответствующих риску на основе критериев приемлемости риска;

b) возможные улучшения системы: выявляют факторы снижения риска и необходимые изменения архитектуры исследуемой системы для обеспечения соответствия критерию приемлемости;

c) рекомендации по улучшению: разрабатывают предложения по улучшению функционирования системы, включая:

1) модификацию оборудования;

2) изменение рабочих и организационных процедур;

3) изменение административной политики в области планирования задач технического обслуживания, обучения персонала и т.п.;

d) обоснование распределения ресурсов: определение воздействия выполнения рекомендаций по улучшению функционирования системы.

Так как исследуемая система может претерпеть изменения в процессе эксплуатации, ETA необходимо поддерживать в рабочем состоянии в течение всего срока службы системы, что обеспечивает процесс принятия решений. Этот процесс регулярной периодической модификации в некоторых отраслях промышленности называют "живой PRA/PSA" (Вероятностный анализ риска/безопасности). Необходимое применение ETA в общем процессе менеджмента риска описано в [12].

8 Оценка

8.1 Предварительные замечания

До начала количественного анализа частоты или вероятности выходов для различных последовательностей событий должен быть проведен тщательный качественный анализ дерева событий, которое может включать инициирующие события, главные события, а также промежуточные и основные события соответствующих деревьев неисправностей.

Для описания основных принципов анализа для наглядности использовано основное графическое представление дерева событий, представленное на рисунке 2.

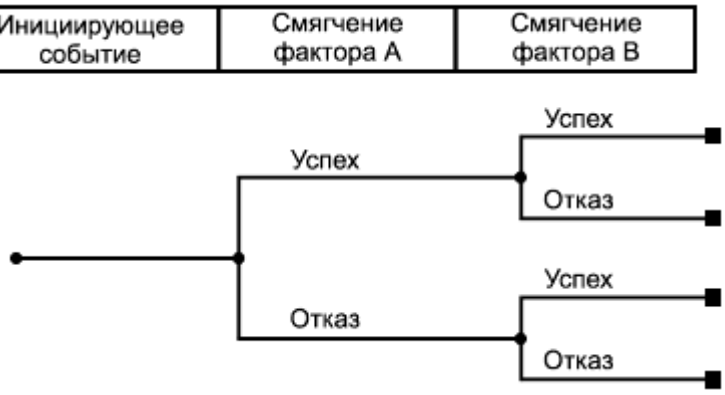


Рисунок 2 - Основное графическое представление дерева событий

8.2 Качественный анализ. Основные зависимости

8.2.1 Общие положения

Целью качественного анализа является:

a) понимание факторов, которые определяют зависимости между функциями или компонентами системы;

b) идентификация значимых событий зависимых отказов;

c) корректный количественный анализ дерева событий и установление его адекватной связи с деревьями несоответствий.

Качественному анализу и, в частности, анализу зависимостей должно быть уделено внимание, однако его выполняют вместе с анализом последовательностей событий и анализом системы.

Существует два основных вида зависимостей:

- функциональные зависимости (см. 8.2.2);

- структурные или физические зависимости (см. 8.2.3).

Например, зависимость является функциональной, если отказ фактора защиты делает невозможным выполнение своей функции следующим фактором защиты, например, если факторы защиты используют общий компонент, то отказ этого компонента выводит их из работоспособного состояния. Более подробная информация об этих различиях приведена в [40].

Для простоты дерево событий рассмотрено на уровне системы.

8.2.2 Функциональные зависимости

При упорядочивании различных факторов защиты дерева событий в последовательность следует учитывать не только время их воздействия как фактора защиты, но и их логический порядок. Кроме этого необходимо учитывать зависимость успешного срабатывания одного фактора защиты от успешного срабатывания другого. Это может иметь место, например, если:

a) один фактор защиты представляет собой систему поддержки другого;

b) изменения экологических параметров влияют на успешную работу другого фактора защиты.

Например, на рисунке 3 показано дерево событий, в котором последовательные отказы систем A и B (факторы защиты) приводят к показанным выходам. В этом примере система B поддерживает систему A.

После переупорядочения систем A и B в дереве событий (см. рисунок 3) ветвь отказа системы B не нуждается в дальнейшем делении на две ветви для системы A, поскольку отказ системы B предполагает, что система A не может выполнять свою функцию. Такое представление упрощает дерево событий. Так как для формирования дерева событий в основном используют компьютерные программы, главной задачей аналитика является анализ различных зависимостей в модели.

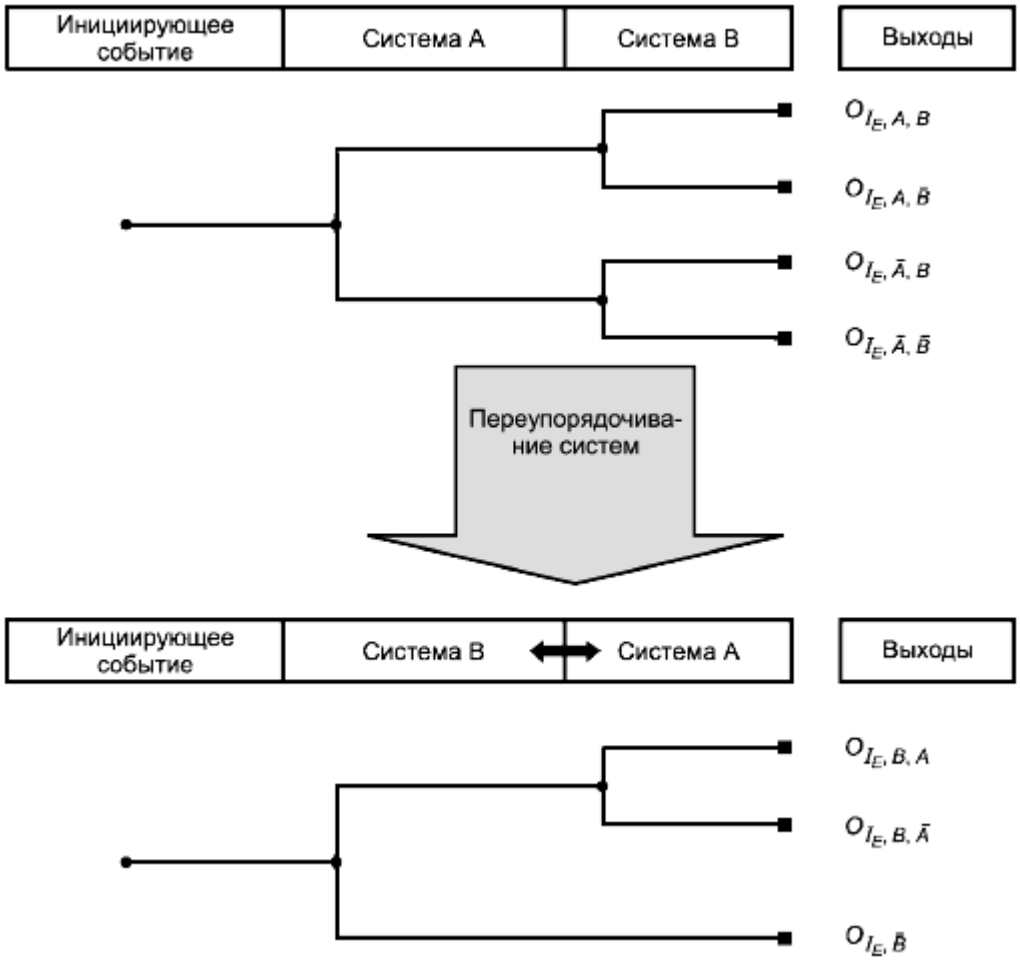


Рисунок 3 - Функциональные зависимости дерева событий

Прежде чем применять переупорядочение, необходимо учесть, что на основе описания дерева событий может быть смоделирована последовательность моментов отказов системы. Таким образом, конкретное дерево событий не моделирует все возможные временные последовательности после реализации инициирующего события. Это следует учитывать при его объединении с деревом неисправностей или Булевыми методами (8.3.2, B.2).

8.2.3 Структурные или физические зависимости

Структурные или физические зависимости обычно приводят к отказам, вызванным общей причиной (отказам общей причины), а такие отказы приводят к реализации нескольких событий одновременно или за короткий промежуток времени (см. определение 3.1.2). Примерами отказов общей причины являются отказы, вызванные

такими событиями, как пожар, землетрясение, ураган, отказы технических систем (например, отказ системы электроснабжения высокой мощности или короткое замыкание) или действия человека, такие как ошибки или акты саботажа.

Поэтому анализ общей причины выполняют для определения подверженности различных факторов защиты последствиям отказа под воздействием внешних или внутренних условий, систем или функций.

Одним из важных вопросов является наличие влияния реализации инициирующего события (например, землетрясения) на условные вероятности реализации всех вершин событий соответствующих деревьев неисправностей (см. 8.3.2).

Другим вопросом качественного анализа является идентификация общих систем или общих функций, которые влияют на различные факторы защиты. Например, в дереве событий (рисунок 3) отказ системы, вызванный отказом системы В, приводит к нежелательному выходу. Если для функционирования системы А необходимо функционирование части системы В, в дереве событий необходимо рассмотреть три системы: систему А* и систему В*, которые являются системами А и В без общих частей, и систему С, представляющую собой общие части систем А и В. Этот сценарий представлен на рисунке 4.

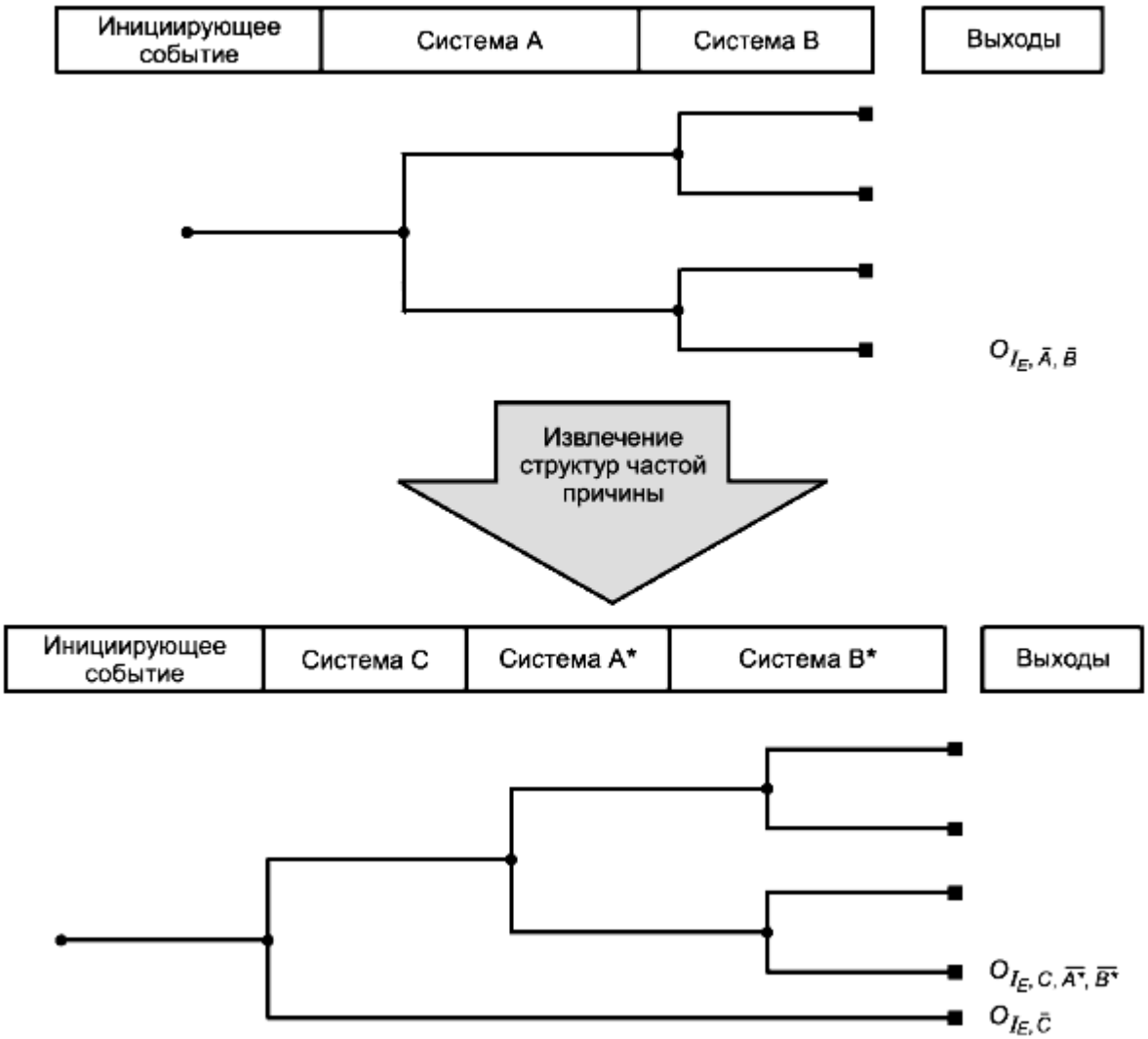


Рисунок 4 - Моделирование структурных или физических зависимостей

В большинстве случаев зависимости намного более сложны, чем показанные выше.

Например, отказы, вызванные действиями по техническому обслуживанию, выполняемыми бригадой

технического обслуживания, не могут быть так легко смоделированы, как показано выше. В случае большого количества комбинаций зависимых систем и их компонентов, можно использовать так называемое сопряжение деревьев неисправностей (см. 8.3.2).

8.3 Количественный анализ

8.3.1 Последовательность независимых событий

Если все условные вероятности успеха или отказа факторов защиты не зависят друг от друга, количественный анализ становится очень простым.

На рисунке 5 представлено дерево событий с тремя факторами защиты: системами A, B и C. Пунктиром на рисунке 5 показана последовательность событий в дереве событий, где система A функционирует, а системы B и C отказали. В следующих разделах установлены основные принципы определения оценок частоты или вероятности выхода этой конкретной последовательности δ. Практические примеры деревьев событий приведены ниже.

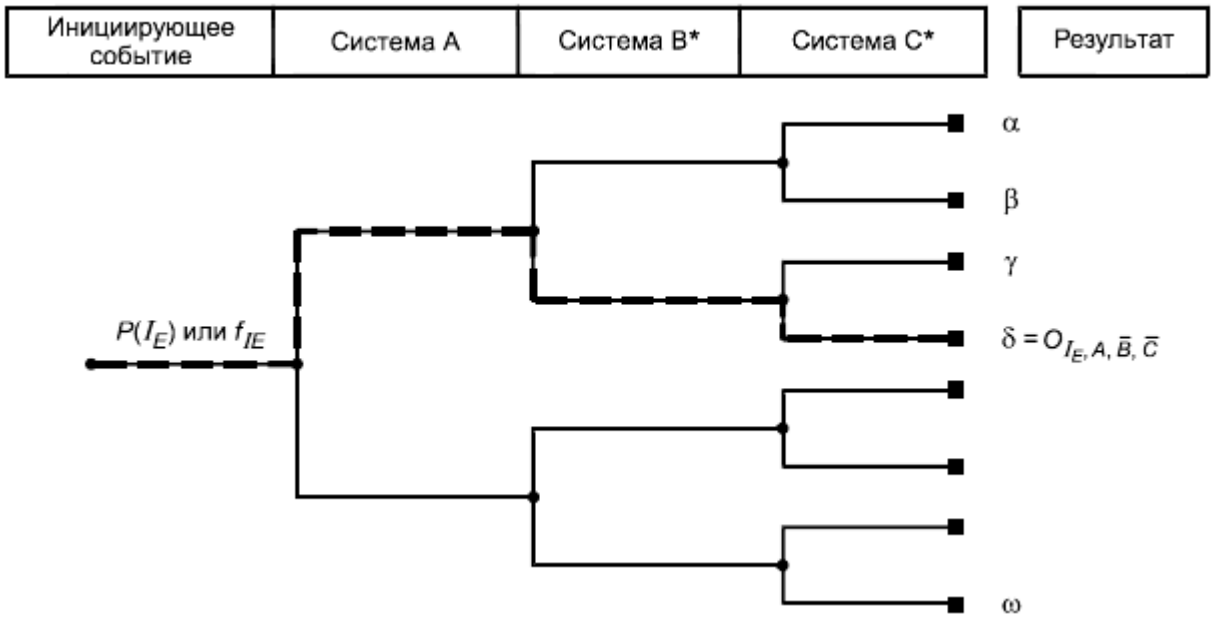


Рисунок 5 - Последовательность событий

Для вывода формулы (1) для вероятности P(δ) последовательности δ необходимо использовать теорему условной вероятности и определения, приведенные в разделе 3:

$$P(\delta) = P(I_E \cdot A.\ \bar{B}.\ \bar{C}) = P(I_E) \cdot P(A \backslash I_E) \cdot P(\bar{B} \mid I_E .A) \cdot P(\bar{C} / I_E .A.\ \bar{B}), \quad (1)$$

где P(I_E) - вероятность реализации инициирующего события I_E;

P($A|I_E$) - вероятность успеха системы A при реализации данного инициирующего события I_E (условная вероятность).

Если успехи и отказы одной системы не зависят от таковых для других систем, можно использовать условные вероятности, связанные только с реализацией события I_E. В этом случае выражение (1) может быть упрощено:

$$P(\delta) = P(I_E) \cdot P(A|I_E) \cdot P(\overline{B}|I_E) \cdot P(\overline{C}|I_E). \quad (2)$$

Инициирующее событие может быть описано или с помощью безразмерной вероятности реализации события $P(I_E)$, или с помощью частоты f_{IE} (1/время). Если оценивают частоту, эта математическая модель может быть использована для вычисления частоты f_δ последовательности δ:

$$f_\delta = f_{IE} \cdot P(A|I_E) \cdot P(\overline{B}|I_E) \cdot P(C|I_E), \quad (3)$$

где f_{IE} - частота инициирующего события.

Выражение (3) использовано в примерах, приведенных в В.1.3, В.2.5 и В.2.6.

Выполняя расчеты для всех возможных последовательностей α, β, γ, δ, ..., ω, получают количественную оценку всех выходов инициирующего события.

Если данных о реализации инициирующих событий недостаточно или их достоверность вызывает сомнение, не следует полностью полагаться на такие количественные оценки. В этом случае следует использовать анализ чувствительности для выявления наиболее критичных последовательностей.

8.3.2 Объединение дерева неисправностей и булевой редукции

В соответствии с 6.1 и 5.2 при вычислении условной вероятности для отказов факторов защиты могут быть использованы деревья неисправностей.

На рисунке 6 показано дерево событий с двумя факторами защиты системами А и В. Вероятности отказа систем А и В обозначены соответственно $P(F_A)$ и $P(F_B)$ и вычислены. На этом рисунке они изображены рядом с их главными событиями с помощью логических операций "И" и "ИЛИ" в соответствии с МЭК 61078 [16].

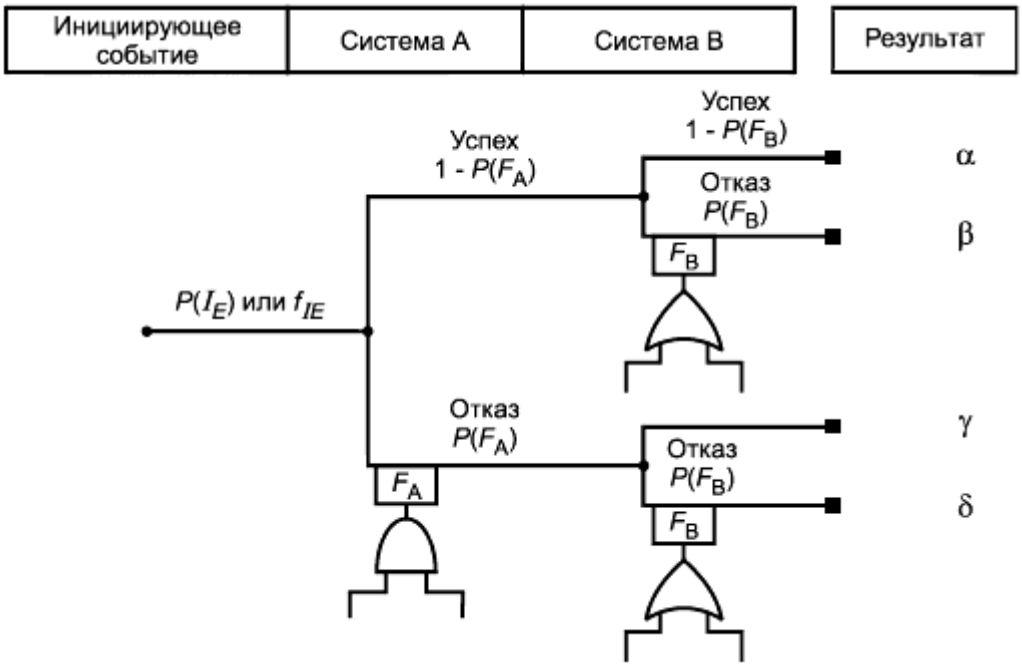


Рисунок 6 - Соединение с деревом неисправностей

Вероятности соответствующих главных событий F_A и F_B использованы в дереве событий в качестве условных вероятностей $P(F_A)$ и $P(F_B)$ отказов систем A и B соответственно. Условные вероятности успеха систем равны соответственно (1 - $P(F_A)$) и (1 - $P(F_B)$).

Если на факторы защиты воздействуют события общей причины, для уменьшения дерева событий и идентификации этих событий может быть использована Булева алгебра.

Для определения выходов в каждой последовательности дерева событий используют понятия, приведенные в [14]. Необходимую Булеву редукцию и анализ простой импликаты проводят в соответствии с [16].

В B.3 приведен подробный пример Булевой редукции и простой импликаты для конкретного дерева событий.

В исходной форме главное событие дерева неисправностей, связанного с различными факторами защиты, позволяет определить вероятность конкретного состояния (например, успеха или отказа) фактора защиты. Эти вероятности, вычисленные с применением FTA, могут быть объединены с вероятностью или частотой реализации инициирующего события (см. 8.3.1). Если главное событие характеризовано с помощью интенсивности или частоты отказов, то эти показатели реализации главного события не могут быть объединены с частотой реализации инициирующего события. Следовательно, в этом случае необходимо применять другие аналитические методы, такие как Марковское моделирование (см. [17]). Если для различных факторов защиты использованы стратегии восстановления или ремонта, Марковское моделирование может помочь в разработке более адекватной модели. Более детальные методы анализа различных моделей функционирования системы и соответствующих показателей надежности приведены в [18].

Более детальная информация об основных математических расчетах для дерева событий приведена в [32].

Основные правила определения количественных оценок просты и могут быть выполнены на компьютере. Существует много пакетов программ для качественного и количественного анализа дерева событий. Однако конкретный пакет программ не может быть рекомендован.

Практические примеры, иллюстрирующие теоретические положения данного подраздела, приведены в приложении B.

Кроме теоретических положений, связанных с переупорядочиванием и логическими операциями дерева неисправностей, важно установить четкие рекомендации для определения целей и требований к выполнению анализа. Более всесторонний подход к установлению краткой процедуры ETA приведен в [3].

9 Документация

Документация ETA должна включать некоторые основные элементы. Для разъяснения аспектов сложных систем может быть предоставлена дополнительная информация. Документация должна всесторонне освещать все выполненные этапы и действия. Это требование является ключевым.

Указанные ниже номера подразделов в скобках относятся к примеру, приведенному в B.2:

a) цель и область применения анализа (B.2.2), (B.2.4);

b) описание системы (B.2.3):

1) описание конструкции,

2) описание функционирования системы,

3) подробное определение границ системы;

c) предположения (B.2.3), (B.2.4):

1) предположения, относящиеся к конструкции системы,

2) предположения, относящиеся к функционированию, техническому обслуживанию, испытаниям и контролю системы,

3) предположения, относящиеся к моделированию надежности и доступности системы;

d) ETA (B.2.5), (B.2.6):

1) обоснования и источники, использованные при составлении перечня инициирующих событий,

2) анализ, включая графическое представление,

3) источники использованных данных;

e) результаты, выводы и рекомендации (B.2.7).

Более общие рекомендации по документации приведены в [13].

Приложение A
(справочное)

Графическое представление дерева событий

Наиболее часто используемое графическое представление дерева событий приведено на рисунке A.1.

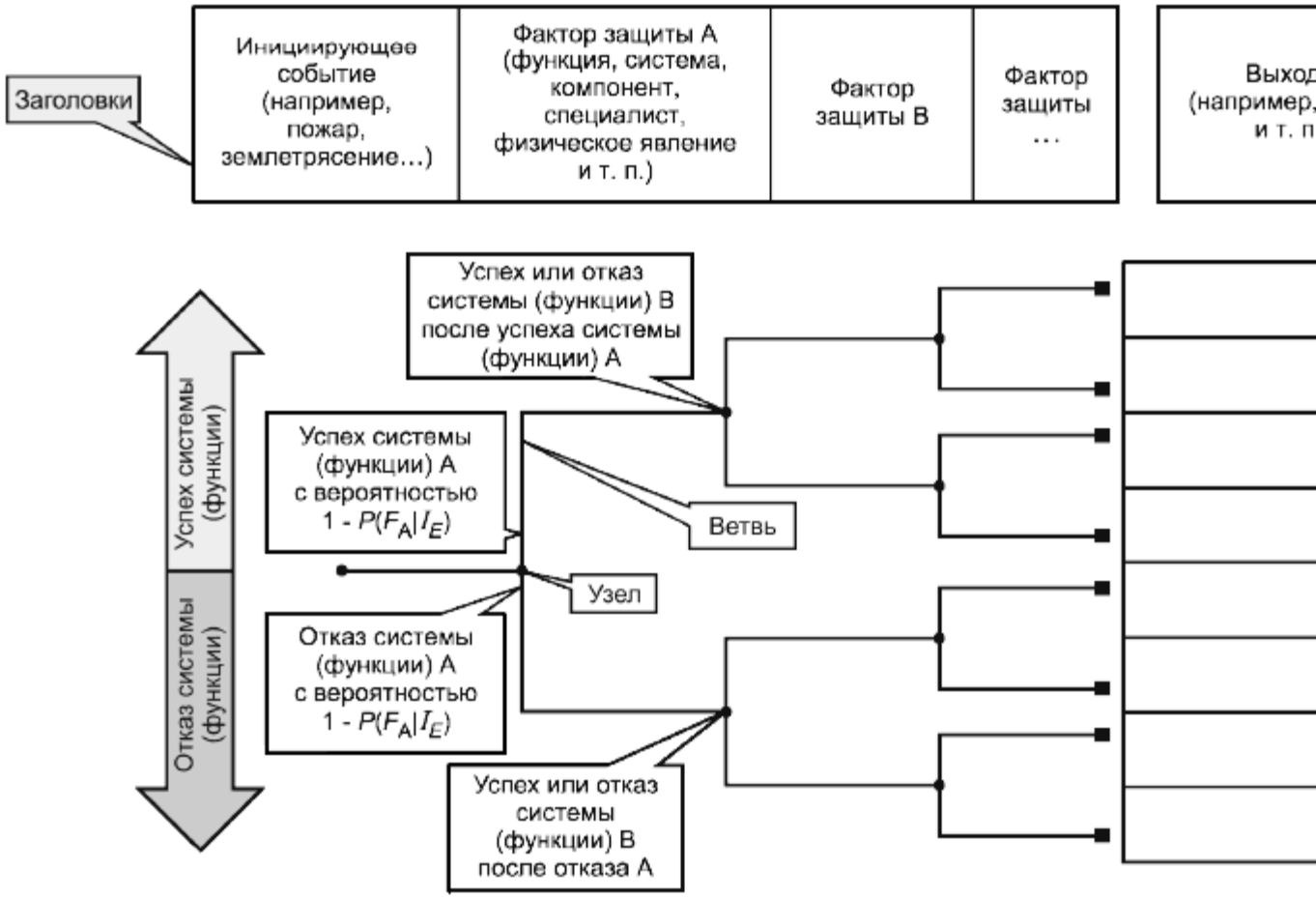


Рисунок А.1 - Наиболее часто используемое графическое представление дерева событий

Пояснение элементов графического представления дерева событий, представленного на рисунке А.1, приведено в таблице А.1.

Таблица А.1 - Пояснения к элементам А.1

Элемент	Примечания
Ветвь	См. 3.1.10. Может быть две или более ветви, исходящие из узла (см. также 7.2.5 с) 1). Необходимо помнить, что только в случае двух ветвей могут быть применены Булевы методы (см. В.3)
Заголовок	См. 3.1.4
Инициирующее событие	См. 3.1.5
Фактор защиты	См. 3.1.6
Узел	См. 3.1.1
Результат	См. 3.1.7
$P(F_A \mid I_E)$	Вероятность отказа фактора защиты А при условии реализации инициирующего события I_E
Успех/отказ	Чтобы нанести на схему возможные выходы, связанные с успехом или отказом системы или функции, необходимо установить четкие критерии

	успеха и отказа, соответственно

Приложение B
(справочное)

Примеры

B.1 Пожар на атомной электростанции

B.1.1 Краткий обзор

Опыт эксплуатации атомных электростанций за последние 40 лет показал, что риск пожара на атомной электростанции должен быть учтен при анализе факторов совокупного риска серьезной аварии.

Далее приведен вероятностный анализ риска пожароопасности, выполненный с двумя целями:

a) выявление критических зон электростанции, дающих наибольший вклад в общую вероятность повреждения атомной электростанции в процессе скрининга;

b) установление последовательности событий развития пожара, отражающих возникновение и обнаружение огня, изоляцию помещения, подавление пожара и разрушение (повреждение) оборудования при устранении пожара.

В процессе количественного анализа ETA должна быть определена частота инициирующих событий, вызывающих пожар, и различные основные повреждения.

Главными задачами являются количественный анализ и качественный анализ в процессе скрининга для идентификации критических по отношению к возникновению пожара помещений.

B.1.2 Анализ на основе скрининга

На первом этапе проводят сбор подробных данных обо всех помещениях станции и классифицируют их по важности и функциям. Далее приведены примеры элементов конкретного анализа.

Область пожара определена как здание или часть здания, достаточно защищенного барьерами, которые предотвращают распространение огня в смежные части здания или соседние здания.

Помещение, в котором возможно возникновение пожара, представляет собой часть зоны возможного пожара. При этом нежелательные последствия не распространяются на другие подразделения.

Существенным по отношению к возникновению пожара является помещение (далее существенное помещение), которое содержит оборудование, связанное с энергообеспечением, обеспечением безопасности, постоянным или временным размещением горючих материалов.

Критическим по отношению к пожару помещением (далее критическое помещение) является существенное помещение, в котором пожар может привести к разрушению (нарушению) хотя бы одного, связанного с безопасностью компонента или системы, это вызывает инициирующее событие, приводящие к нарушению безопасности атомной электростанции.

Процесс скрининга начинают с идентификации всех помещений, для которых выполнен хотя бы один из следующих трех критериев:

a) огневая нагрузка более 7 кВт·ч/м^2;

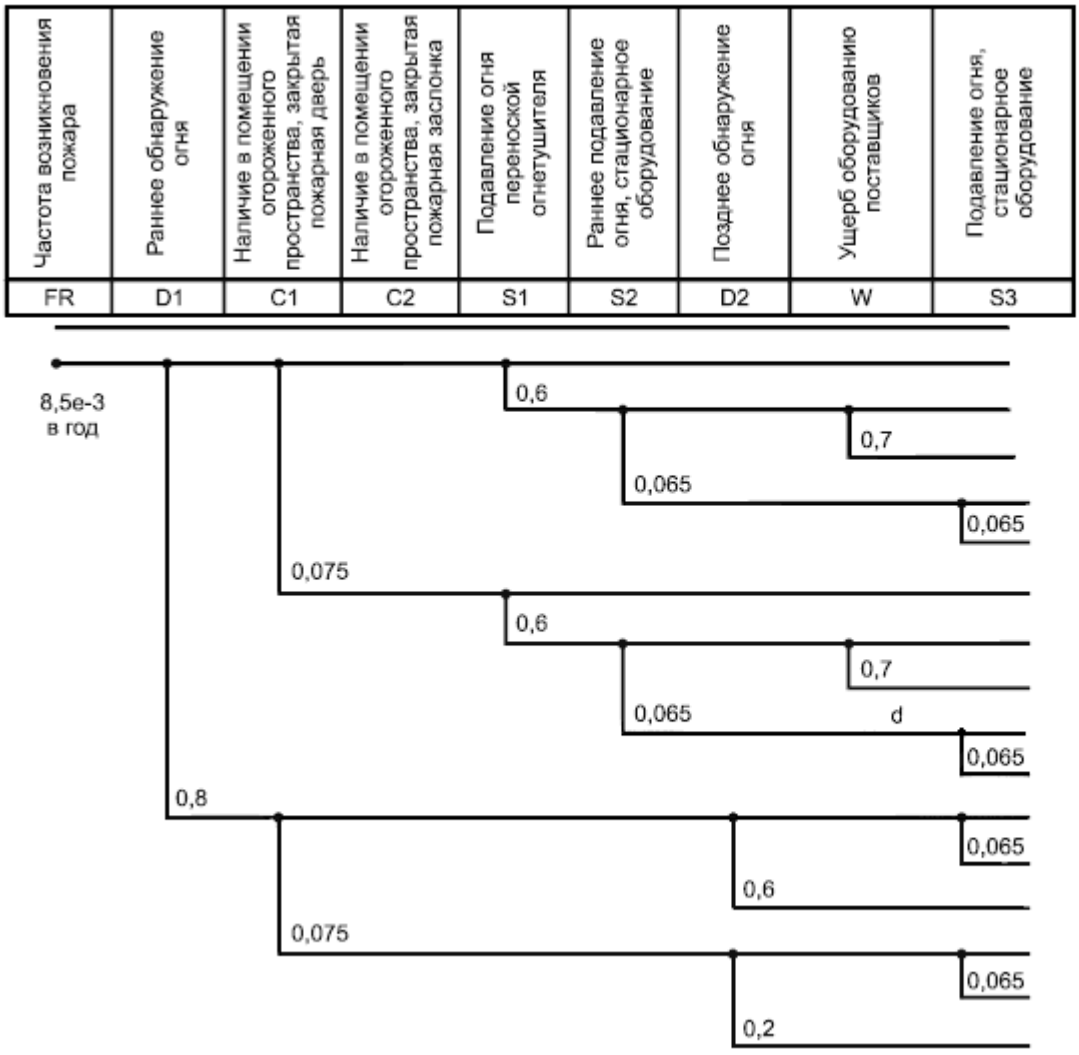
b) помещение содержит оборудование, связанное с обеспечением безопасности, или кабели такого оборудования;

c) помещение содержит функциональное оборудование или датчики системы защиты реактора (системы контроля безопасности).

B.1.3 Количественный анализ

Для каждого критического помещения дерево событий должно включать узлы, связанные с инициацией пожара, вентиляцией помещений, обнаружением огня, подавлением и распространением огня. Все факторы защиты в дереве событий рассматривают как независимые друг от друга (см. ограничения в 5.2). На рисунке B.1 показано типовое дерево событий для возгорания масла в помещении дизельного генератора.

Для определения частоты возгораний различных узлов должны быть использованы соответствующие данные. Такие данные должны в максимально возможной степени быть установлены организацией. Однако в случае недостатка данных некоторые данные могут быть получены из международных баз данных, таких как база данных заводов США. Для вычисления частоты возгораний в одноместной комнате в здании необходимо использовать дополнительно коэффициенты, основанные на количестве источников воспламенения, весе кабельной изоляции, количестве зон возгорания и специальных коэффициентов для источников воспламенения.



Номер выхода	Частота (1/a)	
1	2,9e-3	a
2	1,2e-3	c
3	2,8e-3	b
4	2,6e-4	d
5	1,8e-5	e
6	2,3e-4	a
7	9,9e-5	c
8	2,3e-4	b
9	2,1e-5	d
10	1,5e-6	e
11	2,4e-4	d
12	1,6e-5	e
13	3,8e-4	e
14	3,8e-5	d
15	2,7e-6	e
16	1,0e-5	e

Рисунок B.1 - Дерево событий для пожара в помещении дизельного генератора

Выход относят к одной из пяти категорий повреждений (a), (b), (c), (d) и (e). Худшая категория (e) "Полное разрушение и распространение огня" происходит, когда все меры противопожарной защиты не могут предотвратить распространение огня в смежные комнаты. В соседних помещениях повреждено все, связанное с обеспечением безопасности оборудования.

Для каждого критического помещения получены следующие результаты:

a) частота и источник огня, быстро охватывающего всю атомную электростанцию;

b) список поврежденного оборудования, в соответствии с категориями повреждений (a)-(e);

c) частота по категориям повреждений.

На рисунке B.2 приведен аналогичный вариант дерева событий. Частоту изоляции огня с последующей недоступностью обнаружения огня вычисляют, умножая частоту инициирующего события (1,0 e-4 в год) на вероятность невозможности обнаружения пожара (1,0 e-3 в год). Полученная частота равна (1,0 e-7 в год).

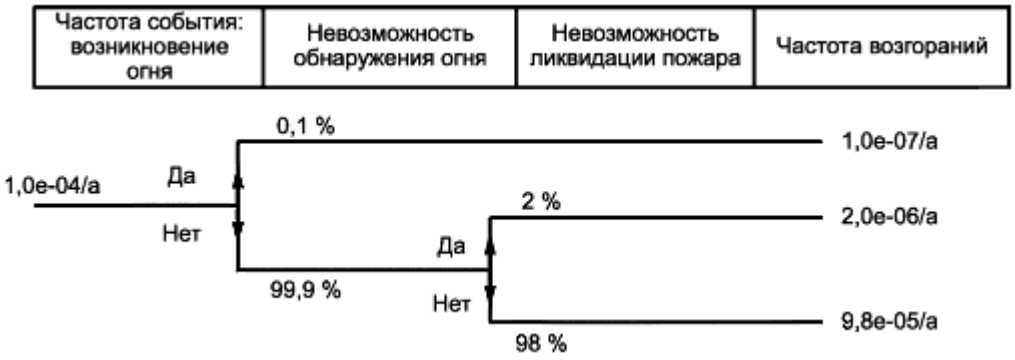


Рисунок B.2 - Дерево событий для пожара

B.1.4 Результаты

Метод ETA является методом учета, оценки и исследования возможных недостатков и ранжирования мероприятий по улучшению противопожарной защиты. Дополнительные исследования затрат/выгод могут быть основаны на результатах ETA.

B.2 ETA для железнодорожного переезда

B.2.1 Обозначения и сокращения

Используемые далее обозначения приведены в таблице B.1.

Таблица B.1 - Обозначения, используемые в B.2

Символ	Описание
A_k	*k*-й сценарий опасного события

C_k	Вероятность, соответствующая *k*-му выходу
D	Продолжительность действия опасности
E	Общая экспозиция за период использования
F_k	Вероятность гибели
IRF	Индивидуальный риск гибели человека
H	Опасность
H_R	Интенсивность реализации опасности (аналогичная "мгновенной интенсивности отказов", см. 6.1.3 из МЭК 61703:2001 [20])
k	Номер сценария
LX	Железнодорожный переезд
N	Количество пересечений автомобилем железнодорожного переезда
THR	Допустимый уровень опасности (в смысле "мгновенной интенсивности отказов", см. 6.1.3 МЭК 61703:2001 [20])
P_c	Вероятность столкновения автомобиля с поездом
P_{EA}	Вероятность того, что водитель автомобиля может избежать столкновения с поездом в результате быстрой реакции
P_N	Вероятность своевременного уведомления водителя о приближении поезда
P_{T_r}	Вероятность отсутствия приближающегося поезда
TIR	Целевое значение приемлемого риска для автомобилиста

B.2.2 Цель

Для иллюстрации применения ETA ниже приведен пример ориентируемого на риск распределения требований общей безопасности между элементами системы железнодорожного переезда.

Цель анализа состоит в определении целей безопасности для конкретного инициирующего события с учетом всех функциональных, экологических и архитектурных условий. Эта цель может быть достигнута посредством "обратного" ETA (см. B.2.6). "Обратный ETA" в данном случае означает определение приемлемой частоты для инициирующего события с помощью инверсии вычислений дерева событий (от выходов).

Рассматриваемый в примере железнодорожный переезд является гипотетическим и приведен для пояснения метода. Все числовые значения, используемые в вычислениях, являются примерами и не могут быть использованы для сопоставления с фактическими.

B.2.3 Определение системы

Для иллюстрации приведен следующий пример.

Автоматический железнодорожный переезд функционировал в течение 25 лет. На переезде использованы световые сигналы предупреждения автомобилистов и удаленный сигнал для предупреждения машиниста переезда.

Схема железнодорожного переезда (LX) приведена на рисунке B.3.

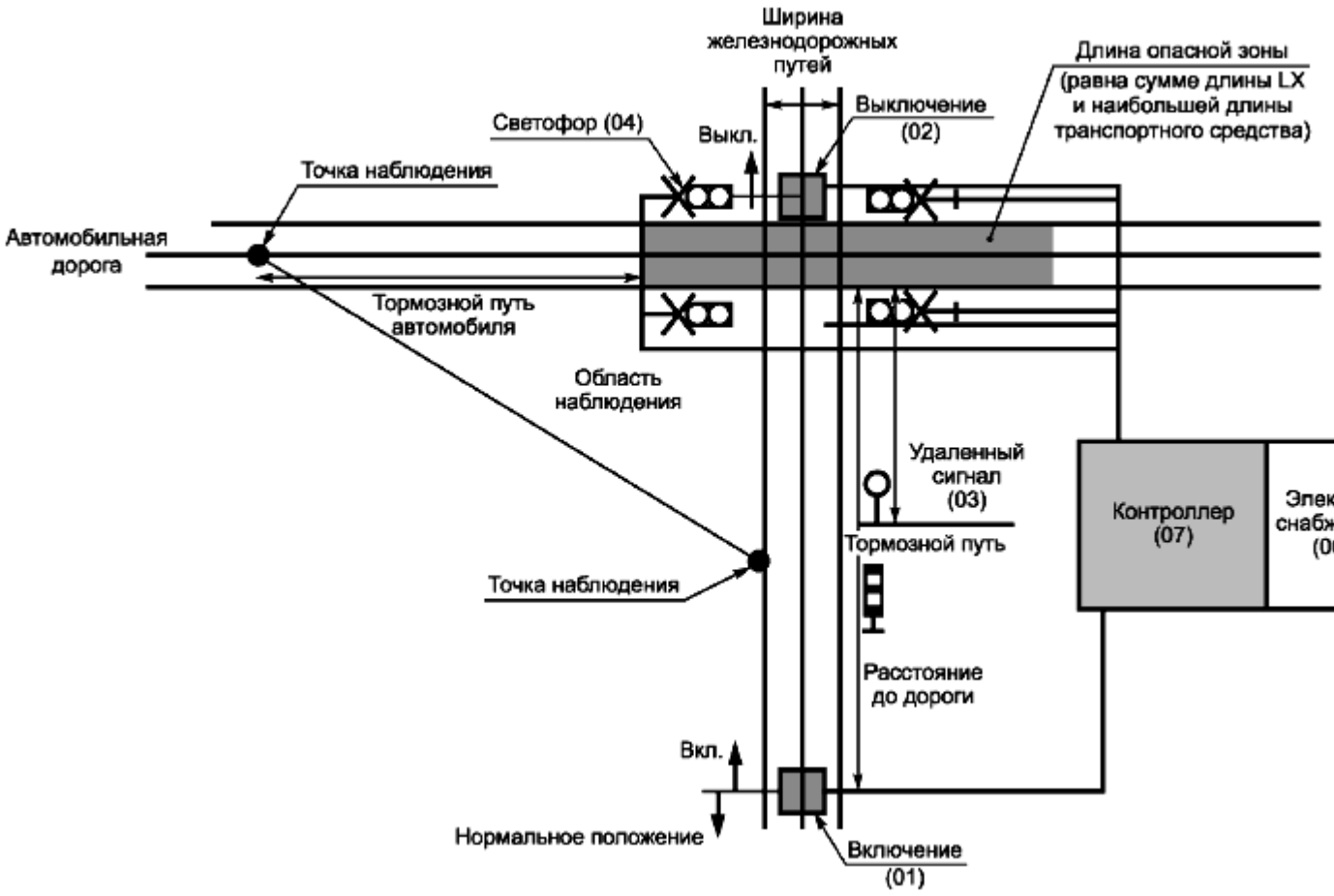


Рисунок В.3 - Система железнодорожного переезда (LX)

В таблице В.2 приведено краткое описание основных функциональных единиц железнодорожного переезда.

Таблица В.2 - Краткое описание системы

N	Функциональная единица	Описание
01	Включение LX	Активация выключения LX при приближении поезда (осуществляется посредством обнаружения колеса поезда)
02	Выключение LX	Выключение LX сразу после того, как поезд покинул переезд (осуществляется посредством не обнаружения колеса поезда)
03	Удаленный сигнал	Показывает состояние LX машинисту поезда
04	Светофор	Показывает состояние LX пользователям автомобильной дороги
05	Нормальное положение	Возвращает LX в нормальное положение (переезд свободен), если оно включено и затем не выключено в пределах определенного времени (необходимого, например, для обнаружения отказа датчика, который продолжает показывать наличие поезда, даже когда он прошел переезд или когда поезд остановился перед переездом и т.д.)

06	Электропитание	Состоит из обычной системы электропитания или батареи, обеспечивающей действие LX в течение ограниченного времени, например 2 ч. Напряжение батареи проверяют блокировкой
07	Контроллер	Управляет LX. Программируемое электронное устройство, включающее программное обеспечение и необходимые данные

Краткое описание функционирования железнодорожного переезда:

a) Приближающийся поезд обнаруживает элемент (01) и передает сигнал на контроллер (07). Расстояние элемента (01) от железнодорожного переезда обозначено как "расстояние до дороги".

b) Контроллер дает команду активизировать светофор (04) и ждет сигнал успешного включения. Расстояние между точкой наблюдения и железнодорожным переездом обозначено как "тормозной путь автомобиля".

c) Контроллер дает команду активизировать удаленный сигнал (03), изображенный маленьким кружком на вертикальном перпендикуляре к небольшому горизонтальному отрезку. Положение по умолчанию - выкл. (опасность). Когда удаленный сигнал выключен, приближающийся поезд должен остановиться на железнодорожном переезде, тогда машинист может включить железнодорожный переезд вручную, используя ключ.

d) Пересечение железнодорожного переезда поездом обнаружено элементом (02) и соответствующий сигнал передан на контроллер.

e) Контроллер дает команду выключить удаленный сигнал. После задержки выключены также светофоры.

B.2.4 Идентификация опасности

На железнодорожном транспорте инициирующие события считают опасными в соответствии со стандартами CENELEC.

Полный анализ возможных опасностей в рассмотренном примере не выполнялся. Рассмотрена только опасность H.

H - отказ железнодорожного переезда, не обеспечивающий защиту автомобилей от столкновения с поездом.

Эта опасность охватывает все ситуации, в которых железнодорожный переезд должен известить автомобилистов о приближении поезда, но не выполняет это действие.

Цель состоит в определении интенсивности опасности (1/время) для H, которая является приемлемой в соответствии с критерием приемлемого риска. Термин "интенсивность" использован в смысле "мгновенной интенсивности отказов" (см. МЭК 61703:2001, 6.1.3 [20]).

B.2.5 ETA

При определении возможных выходов для опасности H необходимо изучить сценарий, в соответствии с которым реализуется опасность H. Следовательно, в конкретном случае, когда к железнодорожному переезду приближается автомобиль, можно рассматривать P_{T_r} (вероятность отсутствия приближающегося поезда), P_N (вероятность своевременного уведомления водителя о приближении поезда), P_{EA} (вероятность того, что водитель автомобиля сможет избежать столкновения с поездом в результате быстрой реакции) и P_C (вероятность столкновения автомобиля с поездом).

Таким образом, имеется два типа опасных событий ("Столкновение поезда с автомобилем" и "Наезд автомобиля на шлагбаум"). На рисунке B.4 показаны внешние факторы снижения риска (т.е. факторы защиты, см.

3.1.6) между инициирующим событием и выходами.

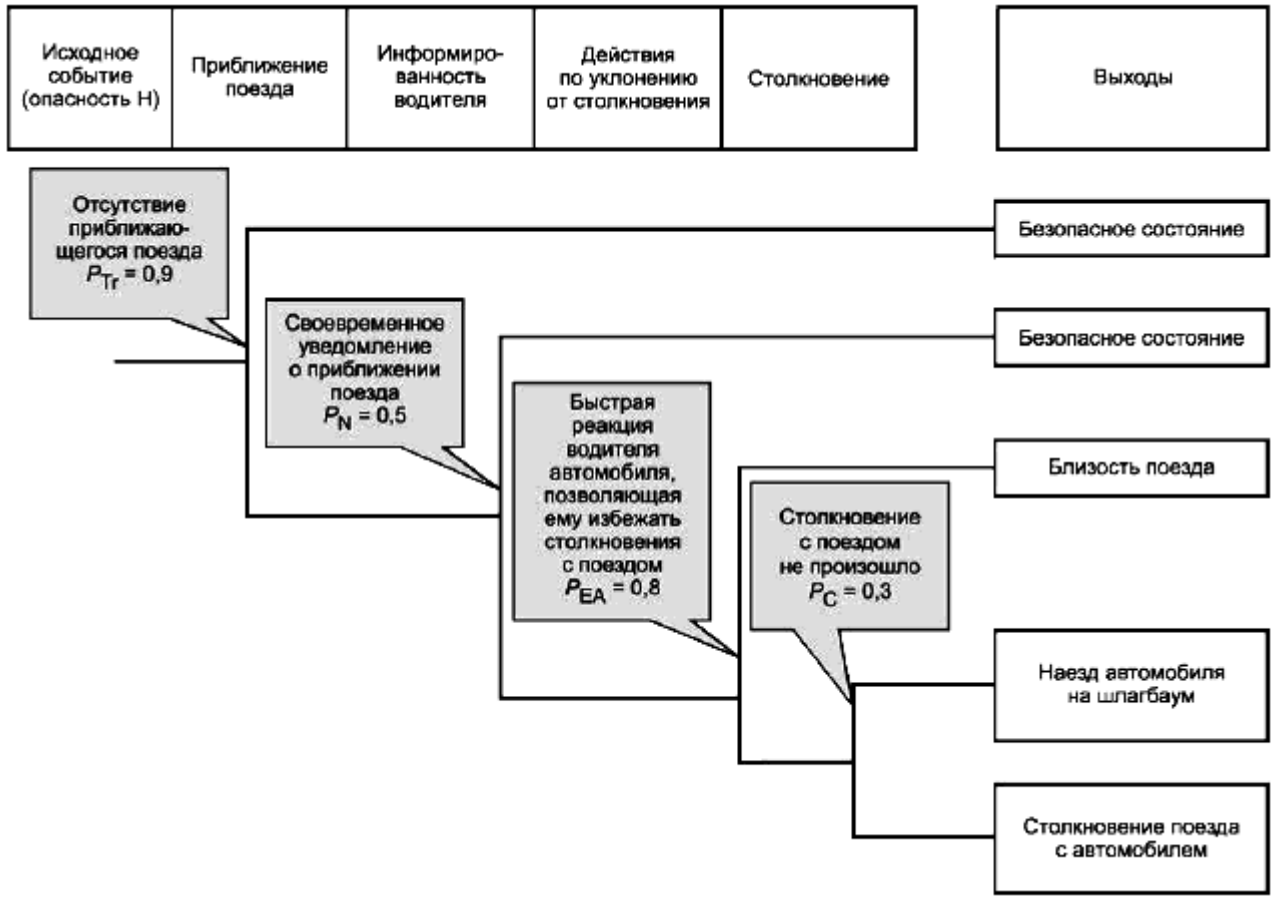


Рисунок В.4 - ETA для железнодорожного переезда

В.2.6 Количественный анализ

Примечание - Принимая во внимание ограничения, указанные в 5.2, приведенный количественный анализ направлен на исследование консервативных (гарантированных) результатов.

В качестве целевого значения риска (TIR) для автомобилиста взяты требования [33]: "Разумно реальные схемы автоматизированных железнодорожных переездов должны обеспечивать водителям транспортных средств риск столкновения с поездом не более чем 1 раз из 100000 пересечений переезда в течение 2000 года" ($R_i < 10^{-5}$).

Для определения более приемлемого риска эта величина была уменьшена в 10 раз. Это означает, что риск должен быть менее 10^{-6} в год. Таким образом, значение TIR установлено равным 10^{-6} в год.

Это означает, что руководство железной дороги должно доказать, что фактический риск автомобилиста на переезде (IRF) меньше или равен TIR. Для определения IRF использована математическая модель [4], учитывающая причинную связь инициирующего события с выходами или последовательностями опасных событий.

а) Предполагается, что автомобилист использует железнодорожный переезд *N* раз в год. Для справки может быть определено общее время использования *E* (т.е. *E* - время, необходимое для пересечения автомобилем

железнодорожного переезда).

b) В данном примере автомобилист подвергается опасности H. Вероятность того, что он подвергается опасности, зависит от продолжительности действия опасности *D* и пребывания *E* автомобилиста в условиях опасности. Эта вероятность представляет собой сумму вероятностей того, что опасность уже существует, когда автомобиль въезжает на железнодорожный переезд (приблизительно $H_R \cdot D$) и вероятность того, что опасность произойдет в то время, пока автомобиль находится на переезде (приблизительно $H_R \cdot E$).

c) Для каждой опасности может существовать одна или более последовательностей событий, приводящих к опасному последствию. Для каждой опасности определяют вероятность выхода C_k. Это вероятность того, что произойдет опасное последствие A_k. Эту вероятность устанавливают для внешних факторов снижения риска (т.е. факторов защиты, см. 3.1.6), полученных с помощью ETA (рисунок B.4). Каждому последствию A_k соответствует определенная значимость. Для конкретного автомобилиста это вероятность несчастного случая со смертельным исходом F_k (см. таблицу B.3). Для данного примера значимость неблагоприятного последствия оценивают, используя данные железной дороги [33].

Таблица B.3 - Параметры снижения риска для рисунка B.4

N *k*	(Опасность) A_k	Фактор снижения риска, C_k	Вероятность гибели человека F_k
1	Столкновение поезда с автомобилем	0,1·0,5·0,2·0,7=0,007	0,2
2	Наезд автомобиля на шлагбаум	0,1·0,5·0,2·0,3=0,003	0,05

Таким образом

$$\text{IRF} = N \cdot H_R \cdot (D+E) \cdot \sum_{A_k} (C_k \cdot F_k). \qquad \text{(B.1)}$$

В формулу (B.1) можно подставлять средние значения или соответствующие параметры (например, процентной) статистических распределений для исходных параметров.

Если риск гибели автомобилиста меньше целевого значения риска, расчетную или оцененную интенсивность опасности (H_R) называют допустимой интенсивностью опасности (THR).

Для данного примера предполагают, что автомобилист неоднократно проезжает по железнодорожному переезду, т.е. N =1000 раз в год. Другие пользователи, такие как пешеходы или велосипедисты, в примере не рассмотрены.

Предполагается, что опасность H, если она реализуется, длится намного дольше времени эксплуатации, т.е. времени пересечения железнодорожного переезда. Это означает, что в уравнении (B.1) можно считать E=0. В качестве пессимистического значения, время продолжительности опасности выбрано D=10 ч, которое представляет собой время отказа LX, приводящего к опасному состоянию системы. Это состояние продолжается до тех пор, пока не будет устранен отказ (ремонт или замена).

Допустимая интенсивность (THR) опасности H может быть вычислена подстановкой параметров в формулу (B.2):

$$\text{IRF} = N \cdot H_R \cdot (D + E) \sum_{A_k} (C_k \cdot F_k) = 1000 \cdot H_R \cdot 10 \cdot (0{,}007 \cdot 0{,}2 + 0{,}003 \cdot 0{,}05) < \text{TIR} = 10^{-6} \text{ (в год)}. \qquad \text{(B.2)}$$

Это допустимая интенсивность инициирующего события, т.е. опасности, которая составляет приблизительно $7 \cdot 10^{-8}$ ч$^{-1}$, что соответствует реализации в среднем одного отказа на железнодорожном переезде в 1600 лет.

B.2.7 Анализ выходов и определение необходимых действий

При завершении анализа важной задачей проектировщика или изготовителя железнодорожного переезда является определение возможности достижения допустимой интенсивности опасности и внесение архитектурных или конструктивных изменений.

B.2.8 Заключение

Данный пример демонстрирует альтернативный подход применения ETA посредством использования обратного подхода для получения допустимых показателей инициирующего события в зависимости от наблюдаемых выходов.

B.3 Объединение дерева неисправностей и Булева редукция

Примечание - В данном подразделе приведены теоретические понятия наиболее используемых программ для Булевой редукции. Для применения программ необходимо понимание основных алгоритмов. Данный подход применим только к деревьям событий, имеющим не более двух ветвей в каждом узле.

Если различные факторы защиты воздействуют на фактор общей причины, можно использовать Булеву алгебру для идентификации этих общих причин при выполнении качественной оценки дерева событий. Полученные в результате качественного анализа основные импликации используют при определении количественной оценки частоты конкретного выхода.

Каждый выход получают с помощью логических операций "И" применительно к вершинам событий соответствующих деревьев неисправностей (см. 8.3.2), связанных с отказами факторов защиты. Аналогично определяют основные импликации.

Минимальная последовательность событий представляет собой наименьшую комбинацию событий, приводящих к опасному выходу. Минимальные последовательности являются фактически специальным случаем основных импликаций. Если дерево неисправностей является понятным (содержит только операции "И" и "ИЛИ"), термин "основные импликации" может быть заменен термином "минимальные последовательности". Для большего количества деталей о теории "основных импликаций" и минимальных последовательностей см. [38].

"Основные импликации" идентифицируют для событий, представляющих собой комбинации событий, объединенных логической операцией "И" и связанных с отказами факторов защиты. Пример Булевой редукции дерева событий представлен на рисунке B.5.

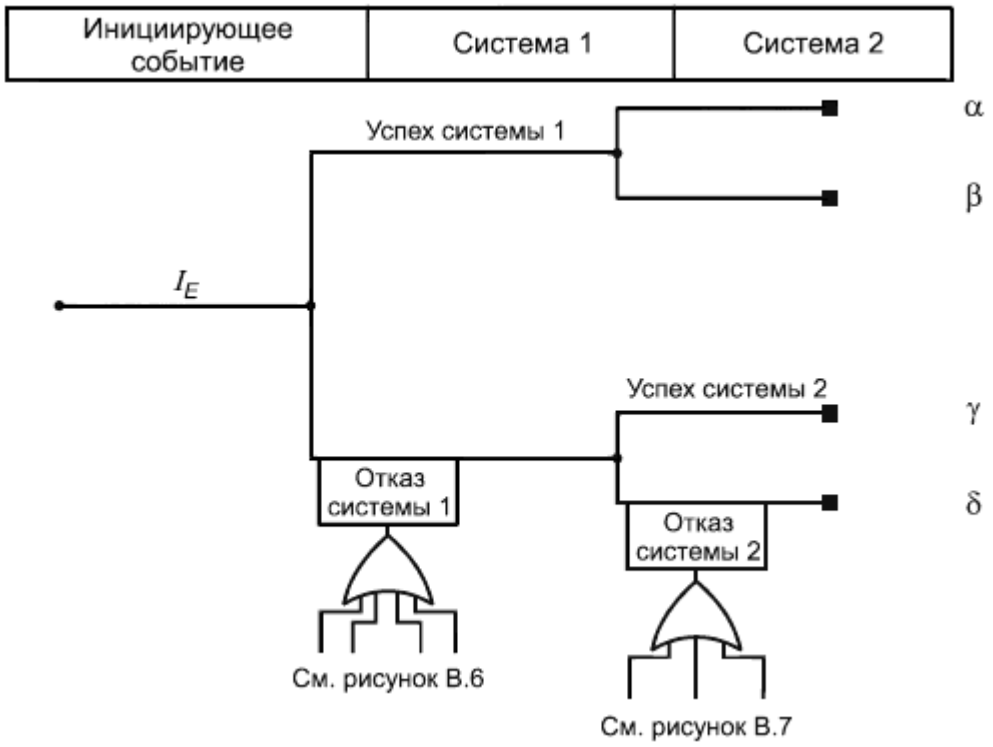


Рисунок В.5 - Простой пример

Вероятности отказов систем 1 и 2 могут быть смоделированы при помощи дерева неисправностей, как описано в 8.3.2.

Следующие теоретические деревья неисправностей представляют собой логическую структуру соответственно для отказа системы 1 (см. рисунок В.6) и системы 2 (см. рисунок В.7), включая семь основных событий A, B, C, D, E, F, и G. Символы используются в соответствии с МЭК 61078 [16].

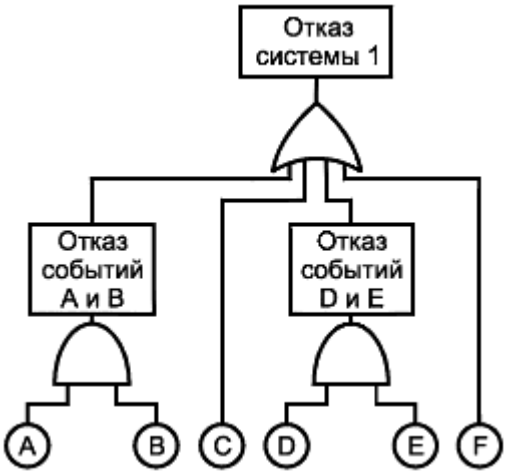


Рисунок В.6 - Дерево неисправностей для системы 1

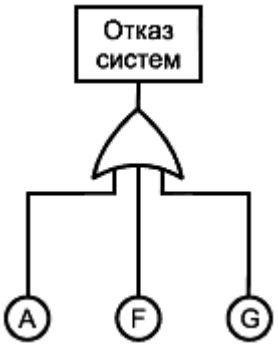


Рисунок В.7 - Дерево неисправностей для системы 2

Для этих деревьев неисправностей и дерева событий выражения для Булевой редукции выходов α, β, γ, δ имеют вид:

$$\alpha = I_E.\left(\overline{A}.\overline{C}.\overline{D}.\overline{F}.\overline{G} + \overline{A}.\overline{C}.\overline{D}.\overline{F}.\overline{G}\right), \quad \text{(B.3)}$$

$$\beta = I_E.\left(A.\overline{B}.\overline{C}.\overline{D}.\overline{F} + A.\overline{B}.\overline{C}.\overline{E}.\overline{F} + \overline{A}.\overline{C}.\overline{D}.\overline{F}.G + \overline{A}.\overline{C}.\overline{E}.\overline{F}.G + \overline{B}.\overline{C}.\overline{D}.\overline{F}.G + \overline{B}.\overline{C}.\overline{E}.\overline{F}.G\right), \quad \text{(B.4)}$$

$$\gamma = I_E.\left(\overline{A}.C.\overline{F}.\overline{G} + \overline{A}.D.E.\overline{F}.\overline{G}\right), \quad \text{(B.5)}$$

$$\delta = I_E.(F+A.B+A.C+G.C+A.D.E+G.D.E). \quad \text{(B.6)}$$

Если δ - исследуемый выход, основными импликациями являются:

$$I_E.F,\ I_E.A.B,\ I_E.A.C,\ I_E.G.C,\ I_E.A.D.E,\ I_E.G.D.E.$$

Основные события A и F характерны для обоих деревьев неисправностей. В соответствии с 8.2.3 они могут быть извлечены для приведения к Системе 1*(S_1) и Системе 2*(S_2), не содержащим события A и F, и представлены в виде новых факторов защиты в новом дереве событий (см. рисунок В.8).

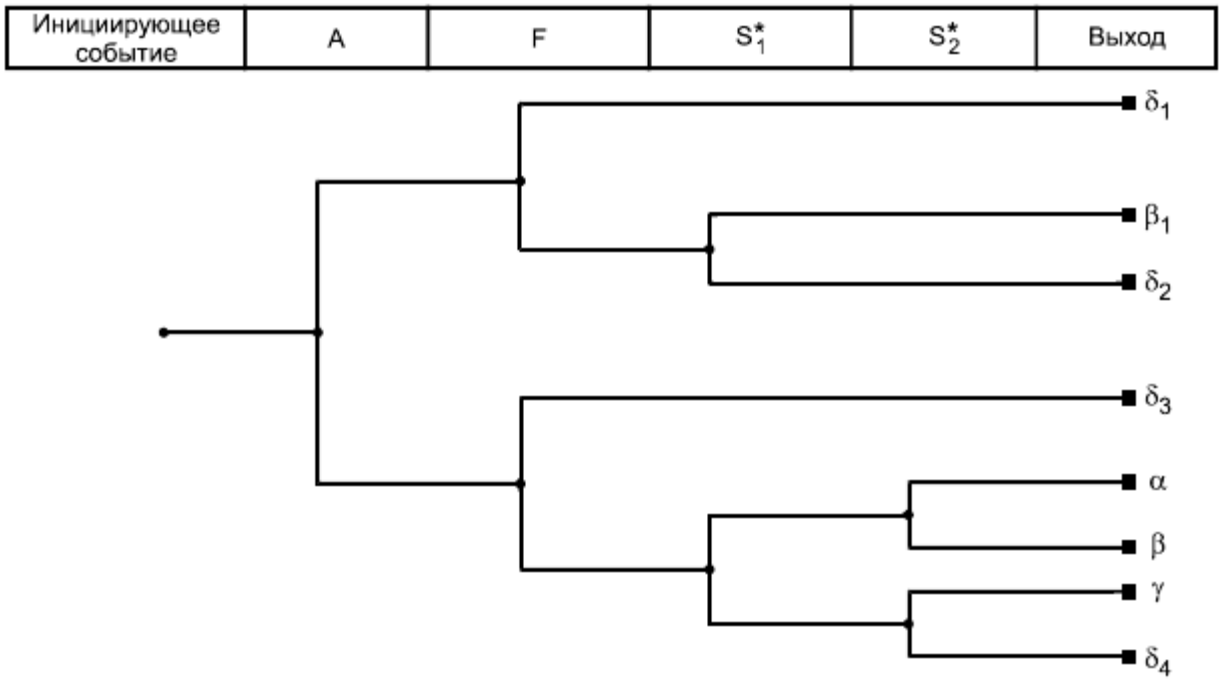


Рисунок В.8 - Модифицированное дерево событий

Примечательно, что в этом конкретном случае A и F, используемые в дереве неисправностей, означают реализацию неисправностей, приводящих к отказу систем (рисунки В.6 и В.7). Таким образом, верхняя ветвь обозначает развитие отказа системы.

Эквивалентность этих двух схем и следующих формул может быть проверена (см. [16]):

$$\beta = \beta_1 + \beta_2, \tag{В.7}$$

$$\delta = \delta_1 + \delta_2 + \delta_3 + \delta_4, \tag{В.8}$$

где $\beta_1 = I_E.\left(A\overline{F}.S_1^*\right)$;

$\beta_2 = I_E.\left(\overline{A}\,\overline{F}.S_1^*.S_2^*\right)$;

$\delta_1 = I_E.\left(A\,F\right)$;

$\delta_2 = I_E.\left(A\overline{F}.\overline{S}_1^*\right)$;

$\delta_3 = I_E.\left(\overline{A}.F\right)$;

$\beta_4 = I_E.\left(\overline{A}\,\overline{F}.\overline{S}_1^*\overline{S}_2^*\right)$.

В (В.9), (В.10), (В.11)дано логическое описание событий: "Отказ системы 1", "Отказ системы 2", "Отказ систем 1 и 2":

$$G_1 = D.E + C, \tag{В.9}$$

$$G_2 = A + G, \tag{В.10}$$

$$G_3 = F + A.B. \quad \text{(B.11)}$$

Дерево событий принимает следующую форму:

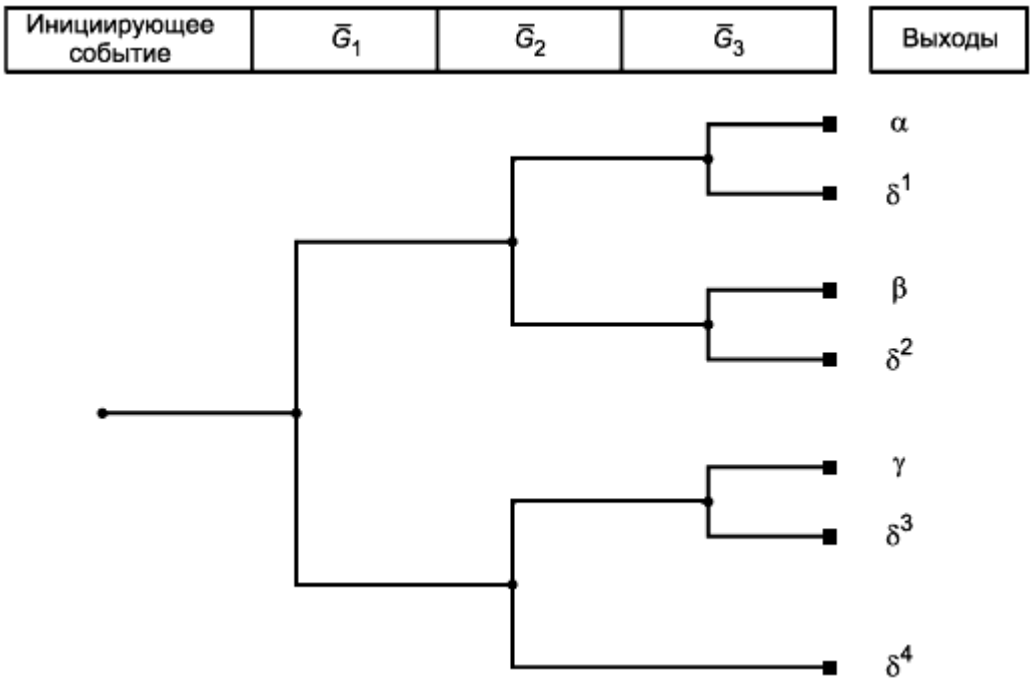


Рисунок В.9 - Дерево событий после "группировки отказов"

Эквивалентность этих схем и следующих выражений может быть проверена (см. МЭК 61078 [16]):

$$\delta = \delta^1 + \delta^2 + \delta^3 + \delta^4, \quad \text{(B.12)}$$

где $\delta^1 = \bar{G}_1.\bar{G}_2.G_3$;

$\delta^2 = \bar{G}_1.G_2.G_3$;

$\delta^3 = G_1.\bar{G}_2.\bar{G}_3$.

$\delta^4 = G_1.G_2$.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
МЭК 60050-191:1990	-	*
МЭК 61025:2006	NEQ	ГОСТ Р 27.302-2009 "Надежность в технике. Анализ дерева неисправностей"

* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде технических регламентов и стандартов.

Примечание - В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:

- NEQ - неэквивалентные стандарты.

Библиография

[1] American Institute of Chemical Engineers, Layer of Protection Analysis - Simplified process risk assessment, New York, USA, October 2001

[2] ANDREWS, J.D., DUNNETT, S.J. Event Tree Analysis using Binary Decision Diagrams, IEEE Trans. Reliability, Vol 49, pp 230-238, 2000

[3] ASME Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME RA-S-2002, 2002, Amended by addenda ASME RA-Sa-2003, ASME RA-Sb2005, and ASME RA-Sc-2007

[4] BRABAND, J., LENNARTZ, K. A Systematic Process for the Definition of Safety Targets for Railway Signalling Applications, Signal+Draht, 9/99

[5] DOWELL, III, A.M., HENDERSHOT, D.C. Simplified Risk Analysis - Layer of Protection Analysis (LOPA), American Institute of Chemical Engineers, Indianapolis, 2002

[6] Expert Group on Probabilistic Safety Analysis for Nuclear Power Plants: "Methods for Probabilistic Safety Analysis for Nuclear Power Plants, Status: August 2005", BfS-SCHR-37/05, Salzgitter, October 2005 (In German)

[7] FULLWOOD, R.; HALL, R. Probabilistic Risk Assessment in the Nuclear Power Industry, NewYork, 1988

[8] GOLDBERG, B.E., EVERHART, K| STEVENS, R., BABBITT III, N., CLEMENS,P| STOUT, L. System Engineering "Toolbox" for Design-Oriented Engineers, NASA Reference Publication 1358,1994

[9] Guidelines on Modeling Common Cause Failures in Probabilistic Risk Assessment, NUREG/CR-5485, NRC 1998

[10] HENLEY, E.J., KUMAMOTO, H. Reliability Engineering and Risk Assessment, 1981

[11] HOFER, E., KLOOS, M., KRZYKACZ-HAUSMANN, B., PESCHKE, J., SONNENKALB, M. Dynamic Event Trees for Probabilistic Safety Analysis, Gesellschaft für Anlagen-und Reaktorsicherheit (GRS), Proceedings EUROSAFE, Berlin 4-5 November 2002

[12] ISO/IEC 31010 Risk management - Risk assessment guidelines

[13] IEC 60300-3-1:2003 Dependability Management - Part 3-1: Application guide-Analysis techniques for dependability - Guide on methodology

[14] IEC 60300-3-9:1995 Dependability management-Part 3: Application guide - Section 9: Risk

analysis of technological systems

[15] IEC 60812:2006 Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)

[16] IEC 61078:2006 Analysis techniques for dependability - Reliability block diagram and boolean methods

[17] IEC 61165:2006 Application of Markov techniques

[18] IEC 61508 (all parts) Functional safety of electrical/electronic/programmable electronic safety-related systems

[19] IEC 61511-3:2003 Functional safety - Safety instrumented systems for the process industry sector - Part 3: Guidance for the determination of the required safety integrity levels

[20] IEC 61703:2001 Mathematical expressions for reliability, availability, maintainability and maintenance support terms

[21] IEC 62425:2007 Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signaling

[22] IEC 62429:2007 Reliability growth - Stress testing for early failures in unique complex systems

[23] IEC 62508:2010 Guidance on human aspects of dependability

[24] IEC 62551 Analysis techniques for dependability- Petri net techniques

[25] ISO 3534-1:2006 Statistics - Vocabulary and symbols - Part 1: General statistical terms and terms used in probability

[26] KLOOS, M., PESCHKE, J., MCDET: A Probabilistic Dynamics Method Combining Monte Carlo Simulation with the Discrete Dynamic Event Tree Approach, Nuclear Science and Engineering: 153,137-156, 2006

[27] LEVESON, N.G. SAFEWARE: System Safety and Computers, Addison-Wesley Publishing Company, 1995

[28] McCORMICK, N.J. Reliability and Risk Analysis - Methods and Nuclear Power Applications, Boston, 1981

[29] Nuclear Regulatory Commission, PRA Procedures Guide, A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants, Final Report, NUREG/CR-2300 Vol. 1, January 1983

[30] NIELSEN, D.S. The Cause/Consequence Diagram Method as a Basis for Quantitative Accident Analysis, Danish Atomic Energy Commission, RISO-M-1374, May 1971

[31] Nuclear Regulatory Commission, Reactor Safety Study: An Assessment of Accident Risks in US Commercial Nuclear Power Plants, Rep. WASH-1400-MR(NUREG-75/014), Washington, DC, 1975

[32] PAPAZOGLOU, I. A. Mathematical foundations of event trees, Reliability Engineering and System Safety 61 (2008) 169-183, Northern Island, 2008

[33] Railtrack, Engineering Safety Management System, Issue 2.0, "Yellow Book", 1997

[34] RAUSAND, M., HOYLAND, A. System Reliability Theory - Models, Statistical Methods and Applications, Hoboken, New Jersey, 2004

[35] SIU, N. Risk Assessment for Dynamic Systems: An Overview, Reliability Engineering and System Safety 43,1994, p. 43-73

[36] SMITH, D.J. Reliability, Maintainability and Risk, Oxford, 2001

[37] Special subject: Common cause failure analysis, Kerntechnik Vol 71, No 1-2, Carl Hanser-Verlag, February 2006, pp 8-62

[38] VILLEMEUR, A. Reliability, Availability, Maintainability and Safety Assessment. Volume 1. Methods and Techniques, Chichester, Wiley, 1992

[39] XU, H.; DUGAN, J.B. Combining Dynamic Fault Trees and Event Trees for Probabilistic Risk Assessment, University of Virginia, January 2004

[40] ZIO, E. An Introduction to the Basics of Reliability and Risk Analysis, Series in Quality, Reliability and Engineering Statistics, Vol. 13, 2007

УДК 62-192:658.562:006.354 ОКС 21.020 Т59

Ключевые слова: событие, вероятность события, частота события, успех события, отказ события, дерево событий, узел, инициирующее событие, последовательность событий, главное событие, ветвь