МЕТОДИЧЕСКИЕ УКАЗАНИЯ К КУРСОВОЙ РАБОТЕ

Содержание

[1. Введение 6](#_Toc464375825)

[2. Термины и определения 6](#_Toc464375826)

[3. Риски и менеджмент риска 6](#_Toc464375827)

[3.1. Общие определения 6](#_Toc464375828)

[3.2. Анализ рисков 10](#_Toc464375829)

[4. Методы оценки риска 11](#_Toc464375830)

[4.1. Структурная схема надежности и булевы методы. 11](#_Toc464375831)

[4.2. Анализ деревьев неисправностей 12](#_Toc464375832)

[4.3. Анализ деревьев событий 14](#_Toc464375833)

[4.4. Анализ «галстук-бабочка» 15](#_Toc464375834)

[4.5. Анализ видов и последствий отказов (FMEA) 16](#_Toc464375835)

[4.5.1. Основы анализа видов и последствий отказов 16](#_Toc464375836)

[5. Примеры оценки рисков с использованием программных модулей Windchill Quality Solutions 48](#_Toc464375837)

[5.1. Оценка методом анализа видов и последствий отказов АВПКО (FMЕСА), АВПО (FMEA) подсистемы 48](#_Toc464375838)

[5.2. Оценка комбинированным методом (системы изделия / отдельного агрегата) 49](#_Toc464375839)

[Выводы 65](#_Toc464375840)

[Приложение А. Пример применения метода анализа дерева событий 66](#_Toc464375841)

[Приложение Б. Описание логических элементов дерева отказов. Вентили и события 68](#_Toc464375842)

[Приложение В. Блок схема примерного бизнес-процесса оценки риска невыполнения требований к функционированию системы методом FMEA (FMECA) 72](#_Toc464375843)

[Приложение Г. Блок схема примерного бизнес-процесса оценки производственного риска 73](#_Toc464375844)

[Приложение Д. Блок схема примерного бизнес-процесса экспертной оценки производственных рисков (FMEA, FMECA) 74](#_Toc464375845)

[Приложение Е. Блок схема примерного бизнес-процесса экспертной оценки надежности и безопасности 75](#_Toc464375846)

[Приложение Ж. Блок схема примерного бизнес-процесса экспертной оценки показателей надежности и безопасности методом FMEA (FMECA) 76](#_Toc464375847)

[Список литературы 77](#_Toc464375848)

Приложение В. Блок схема примерного бизнес-процесса оценки риска невыполнения требований к функционированию системы методом FMEA (FMECA) 57

Приложение Г. Блок схема примерного бизнес-процесса оценки производственного риска 58

Приложение Д. Блок схема примерного бизнес-процесса экспертной оценки производственных рисков (FMEA, FMECA). 59

Приложение Е. Блок схема примерного бизнес-процесса экспертной оценки надежности и безопасности. 60

Приложение Ж. Блок схема примерного бизнес-процесса экспертной оценки показателей надежности и безопасности методом FMEA (FMECA)

Список литературы. 62

**Список сокращений**

|  |  |
| --- | --- |
| Сокращение | Расшифровка |
| FMEA АВПО | Failure Mode and Effects Analysis, Анализ видов и последствий отказов Анализ видов и последствий отказов |
| FMECA АВПКО | Failure mode, effects, and criticality analysis, Анализ видов, последствий и критичности отказов Анализ видов, последствий и критичности отказов |
| PFMEA | Process Failure Mode and Effects Analysis, Анализ видов и последствий отказов процесса |
| DFMEA | Design Failure Mode and Effect Analysis, Анализ видов и последствий отказов проектирования |
| FTA ДН | Fault tree analysis, Анализ дерева неисправностей Дерево неисправностей |
| ETA ДС | Event tree analysis, Анализ дерева событий Дерево событий |
| ССН (СФС) | Структурная (структурно-функциональная) схема надежности |
| WQS | Windchill Quality Solutions |

# Введение

Определены понятия риска. Приводятся сведения о возможности применения экспертных оценок АВПО, АВПКО совместно с методами логических схем деревьев событий и неисправностей (ДН, ДС). Рассматривается применение методики оценок рисков АВПО, АВПКО, ДН и ДС при анализе надежности и безопасности технической системы (ТС) на этапе проектирования.

Приведены:

- Методические рекомендации по решению задачи оценки рисков сложных событий.

- Сведения о принципах использования методики оценок рисков АВПО, АВПКО.

- Подробная информация о проведении АВПО, АВПКО.

- Сведения о возможности использования методики ДН, ДС для уточнения оценки рисков, полученной в результате анализа структурной схемы.

- Алгоритм и пример применения комбинированной методики оценки рисков.

# Термины и определения

**Риск** -  Сочетание вероятности события и его последствий  
**Оценка риска -** Общий процесс анализа риска и оценивания риска

**Событие -** Возникновение или изменение специфического набора условий

**Опасность –** Источник потенциального вреда

**Вероятность -**Мера возможности появления события, выражаемая действительным числом из интервала от 0 до 1, где 0 соответствует невозможному, а 1 - достоверному событию.

**Частота -**Количество событий или их последствий за определенный период времени

**Уровень риска -**Мера риска или комбинации нескольких видов риска, характеризуемая последствиями и их правдоподобностью/вероятностью**.**

# Риски и менеджмент риска

# Общие определения

Проектное управление жизненного цикла изделий тесно связано с управлением рисками и системной инженерией. Разработанная к настоящему времени нормативная база проектного управления, управления рисками и системной инженерией [1,3,4] определяет их основные понятия и принципы построения. Так комплекс стандартов «Менеджмент риска»[1, 5-21] определяет в качестве основных методов управления рисками методы деревьев неисправностей, марковский метод, методы структурных схем, анализа видов и последствий отказов.

Риск определяется как сочетание вероятности события и его последствий [1]. Кроме того в стандарте [1] даны определения следующих терминов:

* Событие;
* Вероятность события;
* Последствие;
* Идентификация риска и источников;
* Критерий риска;
* Анализ и оценка риска;
* Количественная оценка риска, как процесс присвоения значений вероятности и последствий риска;
* Менеджмент риска.

В стандарте [20] вводится понятие неопределенности и риск определяется как влияние неопределенности на цели, причем неопределенность формулируется как состояние, заключающееся в недостаточности информации, понимания или знания относительно события, его последствий или возможности.

Неопределенность в организационно-экономических, технических системах может рассматриваться в следующих качествах [22]:

1. Неопределенность как мера информации; характеристики определенности и «информированности» организационно-экономической системы принято связывать с энтропией.
2. Неопределенность отражает состояние системы по отношению к «идеальным условиям», когда знание полностью детерминировано.
3. Неопределенность воспринимается как возможность выбора альтернатив и множественность данного выбора (вариативность выбора).
4. Неопределенность определяет качество информации (достоверность, полноту, ценность, актуальность, ясность).
5. Неопределенность является атрибутивным источником риска.
6. Неопределенность предполагает неоднозначность реализации событий, порождаемая факторами неизвестной природы.
7. Неопределенность является естественным ограничителем управляемости и стабильности системы.

В стандарте [5], посвященном менеджменту риска при проектировании, менеджмент риска определяется как системное применение политики, процедур и методов управления к задачам определения ситуации, идентификации, анализа, оценки, обработки, мониторинга риска и обмена информацией, относящейся к риску, для обеспечения снижения потерь и увеличения рентабельности.

Процессы менеджмента риска при проектировании включают (рис. 1, 2):

* Определение ситуации;
* Идентификация риска;
* Оценка риска;
* Обработка риска;
* Исследование и мониторинг риска.

Цель идентификации риска состоит поиске и характеристике всех видов риска, которые могут влиять на выполнение проекта в целом или на достижение целей отдельных стадий проекта.

Цель оценки риска состоит в анализе и оценке идентифицированных видов риска. Анализ риска может выполняться качественными, количественными или смешанными методами.

Оценивание риска определяется как процесс сравнения уровня риска с приемлемыми критериями и установки начальных приоритетов для обработки риска.

Цель процесса обработки риска (рис. 3) состоит в идентификации и осуществлении действий, которые позволят сделать риск допустимым. Процесс обработки риска может включать в себя действия, направленные на:

* полное устранение риска;
* уменьшение вероятности появления опасного события;
* уменьшение последствий опасного события;
* перемещение или распределение риска;
* сохранение риска и разработку планов устранения последствий.

Обработка риска может выявлять новые виды риска.

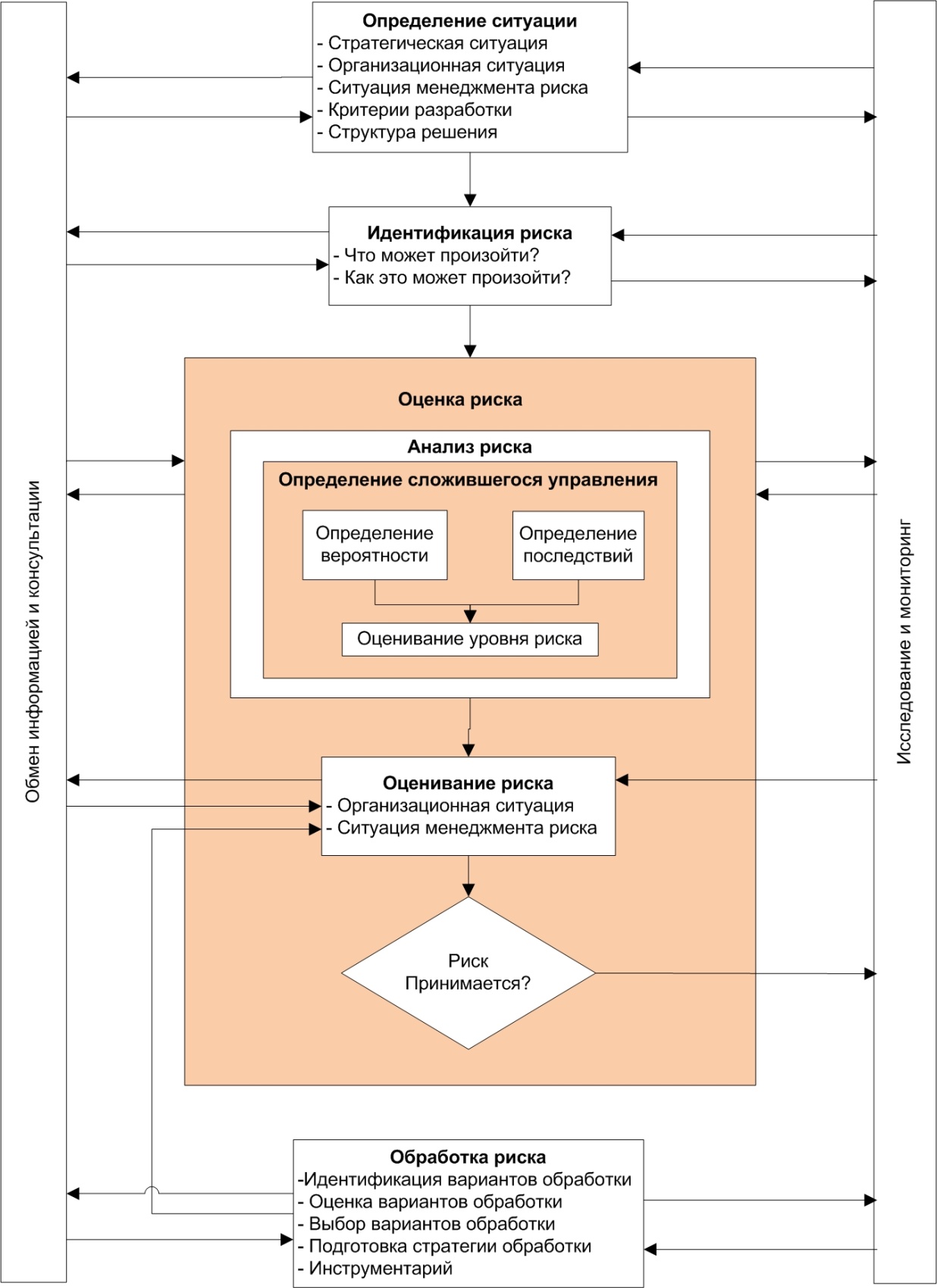


Рис. 1. Процесс менеджмента риска

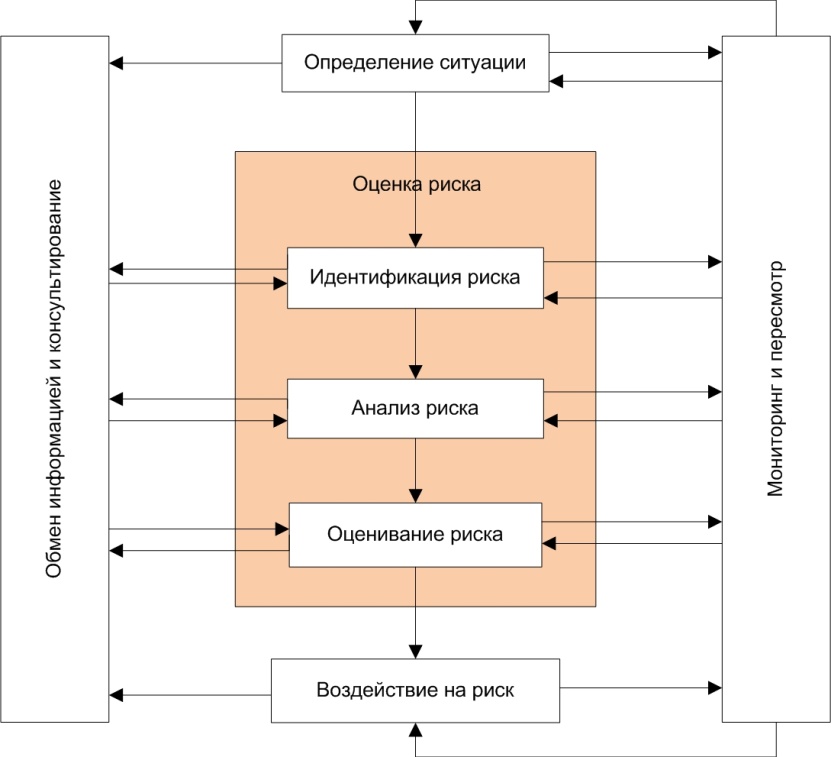


Рис. 2. Процесс менеджмента риска

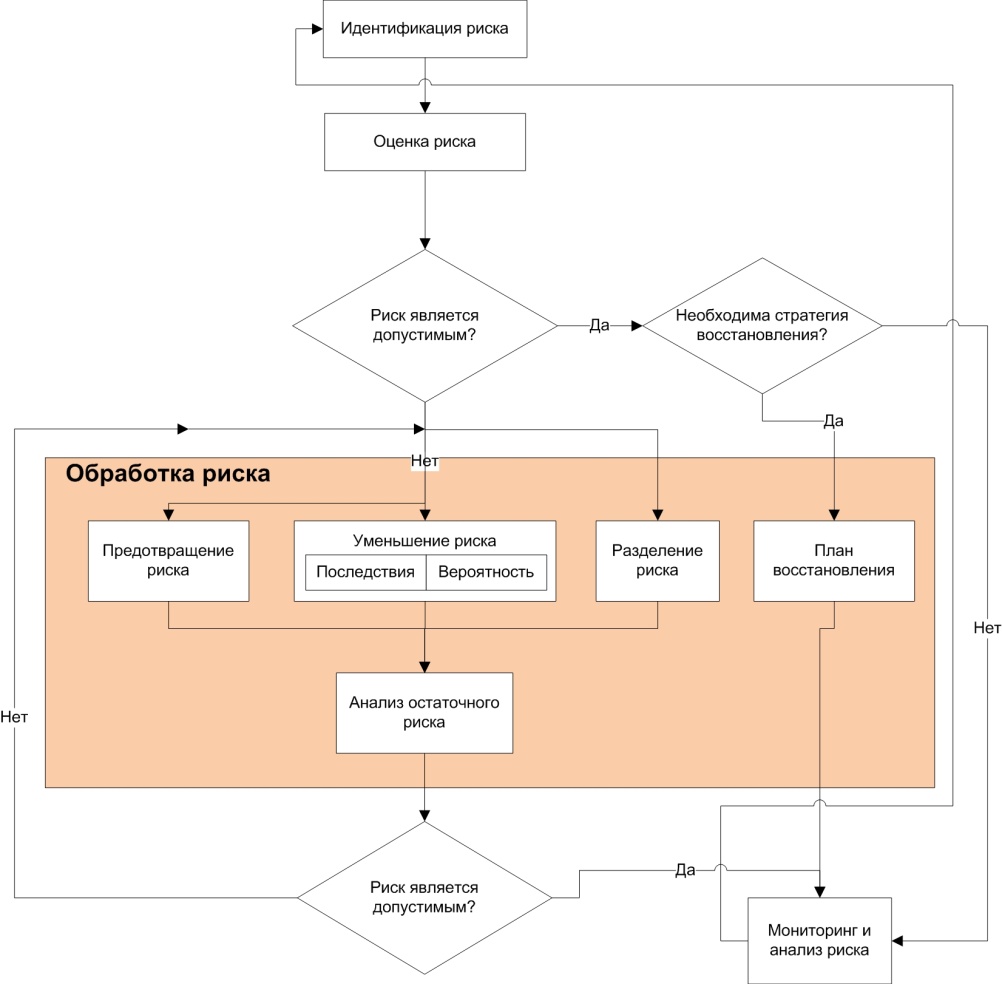


Рис. 3. Процесс обработки риска

Цель исследования и мониторинга риска состоит в идентификации любых новых видов риска и гарантированном сохранении эффективности обработки риска.

# Анализ рисков

В дальнейшем рассматриваются риски как сочетание вероятностей событий, в том числе, связанных с надежностью (безотказностью, долговечностью, ремонтопригодностью, сохраняемостью) оборудования, и вероятностей возникновения негативных последствий событий (аварий) с возможными потерями (снижением безопасности).

Цель управления рисками формулируется следующим образом: оценить эффективность средств и мероприятий по снижению негативных последствий событий, снизить (исключить) потери, связанные с рисками, и таким образом обеспечить заданный уровень безопасности, безаварийности.

Анализ риска – процесс идентификации и оценки риска. При анализе рисков особое значение имеет оценка и достоверность определения уровня риска.

В стандарте [21] способ реализации процесса оценки риска ставится в зависимость от методов оценки риска (рис. 4), анализ риска определяется как анализ вероятности и последствий идентифицированных опасных событий с учетом применяемых способов управления. Данные вероятности событий и их последствий используют для определения уровня риска.

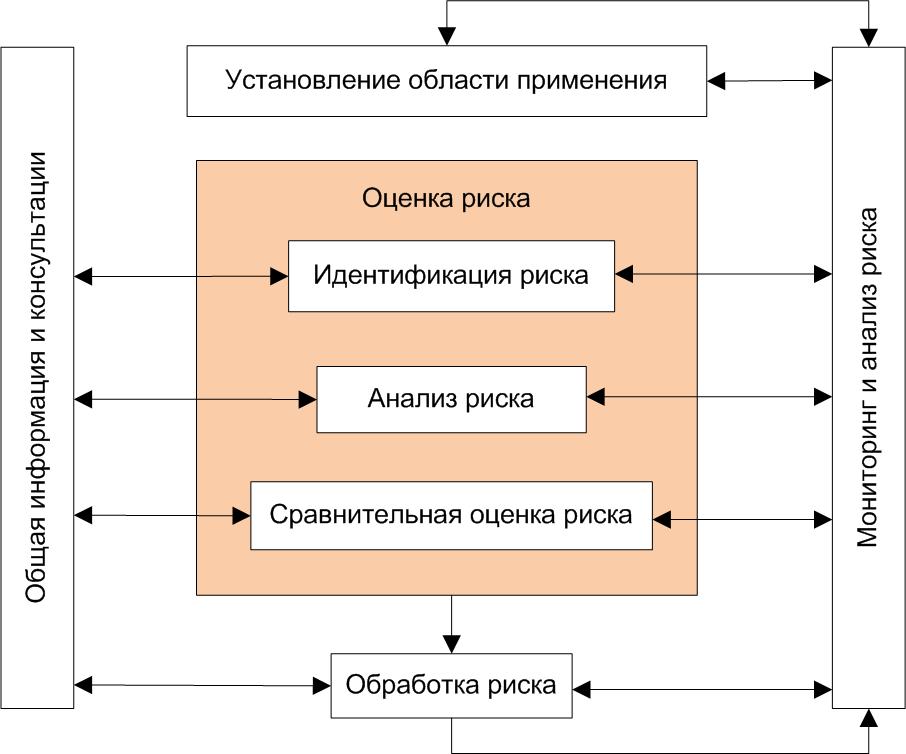


Рис.4. Процесс общей оценки риска

Классификацию методов связывают с этапами процесса оценки риска:

* идентификация риска;
* анализ риска - анализ последствий;
* анализ риска - качественная, смешанная или количественная оценка вероятностных характеристик риска;
* анализ риска - оценка эффективности существующих средств управления;
* анализ риска - количественная оценка уровня риска;
* сравнительная оценка риска.

Для каждого этапа процесса оценки риска применимость метода оценки определяется по шкале: строго применим, применим и не применим (таблица 1). Методы, приведённые в классификационной таблице, призваны обеспечить высокий уровень достоверности на всех этапах оценки риска, в частности количественной оценки вероятностных характеристик риска.

Таблица 1

Характеристика применимости методов оценки риска

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование метода | Процесс оценки риска | | | | |
| Идентификация  риска | Анализ риска | | | Сравнительная оценка  риска |
| Последствие | Вероятностные  характеристики | Уровень  риска |
| Структурная схема надежности и булевы  методы. [14] | применим | не применим | строго применим | не применим | не применим |
| Анализ видов и  последствий отказов  (FMEA) [12,25] | строго применим | строго применим | строго применим | строго применим | строго применим |
| Анализ дерева  неисправностей (FTA) [13,26] | применим | не применим | строго применим | применим | применим |
| Анализ дерева  событий (ETA) [27] | применим | строго применим | применим | применим | не применим |
| Анализ "галстук-  бабочка" [8] | не применим | применим | строго применим | строго применим | применим |
| Марковский анализ. [15] | применим | строго применим | не применим | не применим | не применим |
| Моделирование  методом Монте-Карло | не применим | не применим | не применим | не применим | строго применим |
| Байесовский анализ и  сети Байеса | не применим | строго применим | не применим | не применим | строго применим |
|  |  |  |  |  |  |

# Методы оценки риска

# Структурная схема надежности и булевы методы.

Структурные или структурно-функциональные схемы надежности (Таблица 1) обеспечивают определение показателей, включая вероятности выполнения заданных функций, проекта, заказа, систем, подсистем, схем, оборудования, позволяет идентифицировать элементы, отказ которых приводит невыполнению функций.

Стандарт [14] устанавливает методы построения модели надежности системы и использования этой модели для вычисления показателей ее безотказности и готовности. Основой для построения структурной схемы надежности восстанавливаемых систем является понимание вариантов функционирования системы. Структурная схема надежности может быть построена на различных уровнях:

* системы в целом,
* подсистемы/модуля,
* сборочных единиц.

Если структурную схему надежности разрабатывают для дальнейшего анализа системы (например, методом анализа видов и последствий отказов АВПО (FMEA)), то должен быть выбран уровень, подходящий для такого анализа. Кроме того, должны быть четко описаны:

* выполняемые функции;
* эксплуатационные параметры и их допустимые предельные значения;
* условия эксплуатации и окружающей среды.

При разработке структурной схемы надежности допускается использовать методы качественного анализа. Поэтому должно быть установлено определение для успеха/отказа системы (или несколько определений успеха/отказа). На следующем этапе в соответствии с целями анализа для каждого определения успеха/отказа системы систему необходимо разделить на логические блоки. Блоки могут представлять собой подсистемы, которые в свою очередь могут быть представлены собственными структурными схемами надежности. Вычисления могут быть проведены с применением методов теории надежности, аналитических методов или моделирования Монте-Карло. Так как структурная схема надежности описывает логические отношения, необходимые для описания функционального состояния системы, она не обязательно отражает способ физического соединения аппаратных средств, хотя обычно в максимально возможной степени учитывает физические связи в системе. Рассматриваемый объект может функционировать в нескольких режимах. Если для каждого режима используют отдельную систему, то каждый такой режим необходимо рассматривать независимо от других и использовать при этом свои модели функционального состояния системы. Если все функции выполняет одна система, то для каждого типа функционирования, следует использовать свою структурную схему надежности. При этом необходимо наличие четких описаний (логических утверждений) успеха/отказа системы для каждой ее функции.

Требования к функционированию системы должны сопровождаться описанием внешних условий системы. В описание внешних условий должно быть включено описание условий, воздействию которых система будет подвергаться при транспортировании, хранении и эксплуатации. Обычно часть оборудования предназначена для использования в нескольких внешних условиях. В этом случае оценки показателей безотказности могут быть выполнены с помощью одной и той же структурной схемы надежности и интенсивностей отказов, соответствующих каждой внешней среде.

# Анализ деревьев неисправностей

Дерево неисправностей (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). Анализ  дерева неисправностей часто используют для анализа безопасности систем при идентификации рисков, определении их вероятностей (Таблица 1). Анализ дерева неисправностей может также использоваться для исследования свойств готовности и ремонтопригодности изделий различных видов.

Метод анализа деревьев неисправностей [26] заключается в определении и анализе условий и факторов, которые приводят или могут привести к возникновению негативных завершающих событий - полной или частичной утрате функций, деградации рабочих характеристик изделия, ухудшению безопасности или других важных рабочих свойств.   В анализе реализован дедуктивный метод (причины - следствия), что позволяет осуществлять поиск корневых причин событий для статичных систем, так как дает наглядную и подробную схему взаимосвязей элементов и событий, влияющих на их надежность.

Существуют  два метода проведения анализа дерева неисправностей - качественный и количественный. При  качественном методе вероятности событий или частоту их возникновения не рассматривают. Этот метод заключается в детальном анализе совокупности событий/ неисправностей и его применяют, когда необходимо выявить возможные причины отказов безотносительно реальной вероятности их возникновения. Иногда некоторые события, рассматриваемые при проведении качественного анализа, оценивают и количественно, но такие расчеты не связаны с попытками расчета общей безотказности.

При  количественном методе в процессе детального анализа дерева неисправностей полностью моделируют изделие, процесс или систему и оценивают вероятности возникновения базисных событий, отказов или событий, выявленных в ходе анализа. В этом случае окончательный результат представляет собой вероятность появления завершающего события, свидетельствующего о вероятности возникновения неисправности или отказа.

Дерево неисправностей 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 5).

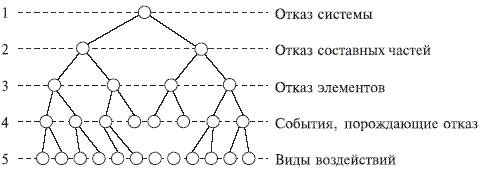


Рис. 5. Структура дерева неисправностей

Чтобы наглядно представить причинную взаимосвязь с помощью дерева неисправностей, необходимы элементарные блоки, подразделяющие и связывающие большое число событий: логические символы (знаки) и символы событий. Логические символы (знаки) связывают события в соответствии с их причинными взаимосвязями (Приложение В, Таблица В1). Логический символ (знак) может иметь один или несколько входов, но только один выход, или выходное событие.

Преимуществом дерева неисправностей (по сравнению с другими методами) является то, что анализ ограничивается выявлением только тех элементов системы и событий, которые приводят к данному конкретному отказу системы или аварии. При этом к событиям и видам воздействия можно отнести действия (ошибки) персонала (экипажа). Кроме того дерево неисправностей:

* позволяет выявлять отказы в процессе построения;
* позволяет показать в явном виде ненадежные места;
* наглядно показывает поведение системы;
* дает возможность выполнять качественный или количественный анализ надежности системы;
* позволяет специалистам поочередно сосредотачиваться на отдельных конкретных отказах системы;
* обеспечивает глубокое представление о поведении системы;
* помогает дедуктивно выявлять отказы;
* дает конструкторам и руководителям возможность наглядного обоснования конструктивных изменений или установления степени соответствия конструкции системы заданным требованиям и анализа компромиссных решений;
* облегчает анализ надежности сложных систем.

Дерево неисправностей обладает следующими недостатками:

* реализация метода требует значительных затрат средств и времени, так как увеличение детальности рассматриваемой инфраструктуры приводит к геометрическому увеличению числа влияющих событий;
* дерево неисправностей 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;
* дерево неисправностей требует от специалистов по надежности глубокого понимания системы и конкретного рассмотрения каждый раз только одного определенного отказа;
* дерево неисправностей 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.

# Анализ деревьев событий

Анализ дерева событий обеспечивает проведение идентификации и анализа рисков (Таблица 1). В основу анализа положена формула полной вероятности.

Стандарт [27] рассматривает последствия отказа, являющегося результирующим в дереве неисправностей. Как и в случае с моделированием методом построения дерева неисправностей (FTA), анализ дерева событий (Event Tree Analysis, ETA) в качестве отправной точки использует определение нежелательного события-вершины, которое может быть получено в результате ранее проведенного анализа видов, последствий (и критичности) отказов (FMEA). Этот метод позволяет рассчитать вероятности различных исходов и определить степень тяжести последствий рассматриваемого отказа.

Анализ дерева событий может быть использован для описания алгоритма построения последовательности событий, исходящих из основного события (аварийной ситуации), и используется для анализа развития этой аварийной ситуации. Построением для системы дерева событий и последовательным детальным анализом всех уровней защиты системы можно продемонстрировать, что даже при наступлении одного из нежелательных базовых событий безопасность всей системы в целом сохранится на достаточном уровне с достаточной вероятностью (т.е. с достаточной вероятностью не наступит нежелательное событие, являющееся вершиной дерева событий системы).

На рис. 6 показан пример дерева событий. В приложении Б приведена реализация дерева событий.

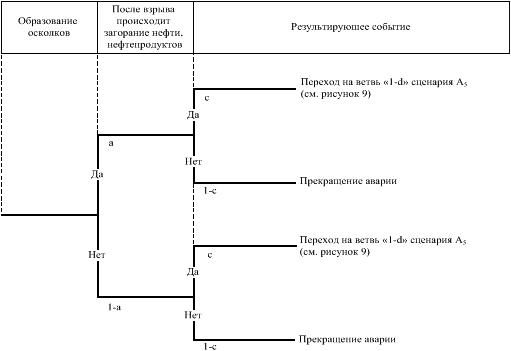


Рис. 6. общий вид дерева событий

# Анализ «галстук-бабочка»

Анализ "галстук-бабочка" [8] представляет собой схематический способ описания и анализа пути развития рискового события от причин до последствий (рис. 7) и применим при анализе рисков (Таблица 1).

Данный метод сочетает исследование причин отказа с помощью дерева неисправностей и анализ последствий с помощью дерева событий. Однако основное внимание метода «галстук-бабочка» сфокусировано на барьерах между причинами и опасными событиями, опасными событиями и последствиями.

Анализ «галстук-бабочка» используют для исследования риска на основе демонстрации диапазона возможных причин и последствий. Данный инструмент является эффективным, если необходимо разобраться в каком-то конкретном риске и понять, как лучше им управлять. Декомпозиция риска на причины и последствия позволяет более адекватно оценить вероятность и уровень ущерба от реализации риска, а также позволяет обнаружить взаимозависимости между рисками. Входными данными метода является информация о причинах и последствиях опасных событий, риске, барьерах и средствах управления, которые могут их предотвратить, смягчить или стимулировать.

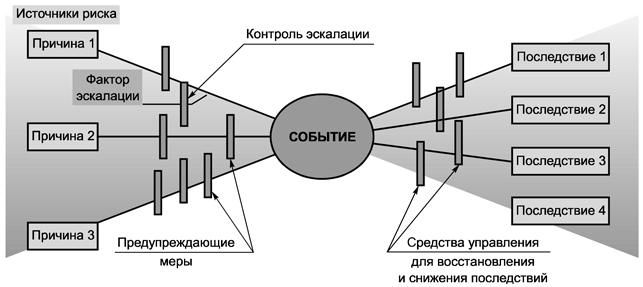


Рис. 7. Метод «галстук-бабочка». Графическая интерпретация размещения схем деревьев неисправностей и деревьев событий

# Анализ видов и последствий отказов (FMEA)

Анализ видов, последствий (и критичности отказов) АВПО, FMEA (Failure modes and effects analysis), АВПКО, FMЕСА (Failure Mode, Effects and Criticality Analysis) применим на следующих этапах оценки риска (Таблица 1):

- идентификация риска;

- анализ риска - анализ последствий;

- анализ риска - качественная, смешанная или количественная оценка вероятностных характеристик риска;

- анализ риска - оценка эффективности существующих средств управления;

- анализ риска - количественная оценка уровня риска;

- сравнительная оценка риска.

Анализ видов, последствий (и критичности отказов) АВПО, FMEA (Failure modes and effects analysis), АВПКО, FMЕСА (Failure Mode, Effects and Criticality Analysis) определены стандартами [12, 25] (рис. 8).

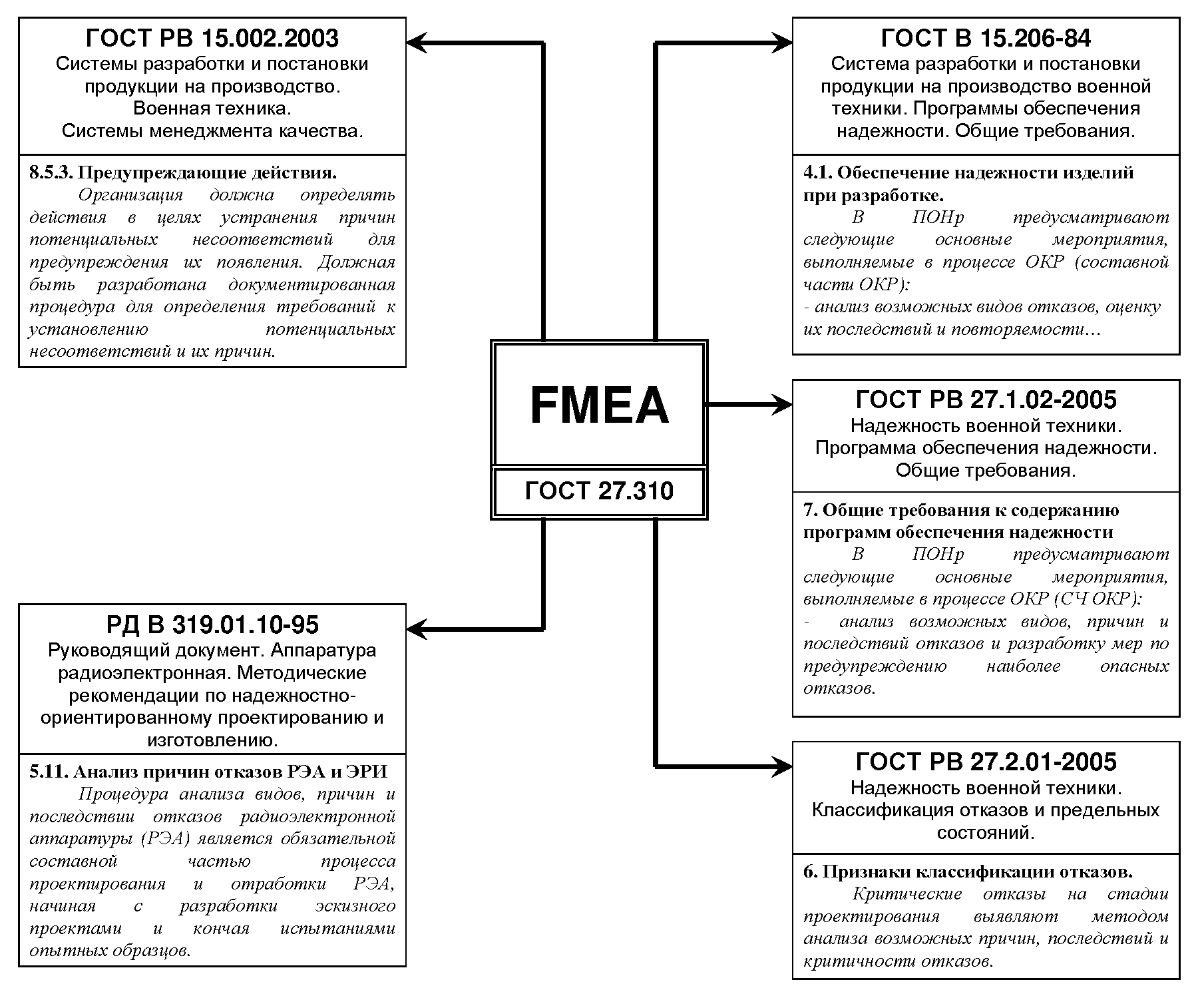


Рис. 8. Взаимосвязь методики FMEA со стандартами и руководящими документами системы ГОСТ РВ.

АВПО (FMEA), АВПКО (FMЕСА) является методом систематического анализа системы с целью идентификации видов потенциальных отказов, их причин и последствий, а также влияния отказов на функционирование и безопасность системы в целом или ее компонентов. АВПО (FMEA), АВПКО (FMЕСА) позволяет идентифицировать тяжесть последствий видов потенциальных отказов и обеспечить меры по снижению риска. В некоторых случаях АВПО (FMEA), АВПКО (FMЕСА) включает оценку вероятности возникновения видов отказов.

АВПО (FMEA) - формализованная, контролируемая процедура качественного анализа проекта, технологии изготовления, правил эксплуатации и хранения, системы технического обслуживания и ремонта изделия, заключающаяся в выделении на некотором уровне разукрупнения его структуры возможных (наблюдаемых) отказов разного вида, в прослеживании причинно-следственных связей, обуславливающих их возникновение, и возможных (наблюдаемых) последствий этих отказов на данном и вышестоящих уровнях, а также - в качественной оценке и ранжировании отказов по тяжести их последствий [25]. В процессе АВПО (FMEA) проводят предварительную количественную оценку и ранжирование выявленных возможных (наблюдаемых) отказов объектов по тяжести их последствий с целью определения необходимости дальнейшего углубленного анализа и оценки их критичности и очередности проведения соответствующих доработок объекта, технологии его изготовления, системы технического обслуживания и ремонта.

АВПКО (FMЕСА) - процедура АВПО (FMEA), дополненная оценками показателей критичности анализируемых отказов. АВПКО (FMЕСА) проводят с целью обоснования, проверки достаточности, оценки эффективности и контроля реализации мероприятий, направленных на совершенствование конструкции, технологии изготовления, правил эксплуатации, системы технического обслуживания и ремонта объекта и обеспечивающих предупреждение возникновения и/или ослабление тяжести возможных последствий его отказов, достижение требуемых характеристик безопасности, эффективности и надежности.

АВПКО (FMECA) расширяет АВПО (FMEA) и включает в себя методы ранжирования тяжести видов отказов, позволяет установить приоритетность контрмер.

В процессе АВПКО (FMECA):

* выявляют возможные виды отказов составных частей и изделия в целом, изучают их причины, механизмы и условия возникновения и развития;
* определяют возможные неблагоприятные последствия возникновения выявленных отказов, проводят качественный анализ тяжести последствий отказов и/или количественную оценку их критичности;
* составляют и периодически корректируют перечни критичных элементов;
* оценивают достаточность предусмотренных средств и методов контроля работоспособности и диагностирования ТС для своевременного обнаружения и локализации его отказов, обосновывают необходимость введения дополнительных средств и методов сигнализации, контроля и диагностирования;
* оценивают достаточность предусмотренных средств и методов проектирования, моделирования, виртуальных и натурных испытаний и обосновывают необходимость использования дополнительных;
* вырабатывают предложения и рекомендации по внесению изменений в конструкцию и технологию изготовления изделия и его составных частей, направленные на снижение вероятности и/или тяжести последствий отказов, оценивают эффективность ранее проведенных конструкторских и технологических доработок;
* оценивают достаточность предусмотренных в системе технологического обслуживания контрольно-диагностических и профилактических операций, направленных на предупреждение отказов ТС в эксплуатации, вырабатывают предложения по корректировке методов и периодичности технического обслуживания.

Основаниями для применения АВПКО (FMECA) и АВПО (FMEA) являются:

* необходимость идентификации отказов, которые имеют нежелательные последствия для функционирования системы, например прекращение или значительное ухудшение работы, влияние на безопасность;
* идентификация для потенциально возможных аварийных ситуаций инициирующих событий и вероятностей их возникновения;
* выполнение требований заказчика, установленных в контракте;
* выполнение разработчиком (поставщиком) системы, оборудования требований ведущего специалиста по проекту;
* повышение надежности или безопасности системы (путем изменения проекта);
* выявление элементов систем, схем, оборудования, отказ которых приводит к невыполнению функций;
* повышение ремонтопригодности системы путем выявления областей риска или несоответствий применительно к ремонтопригодности,

Цели АВПКО (FMECA) и АВПО (FMEA):

* полная идентификация и оценка всех нежелательных для системы последствий и последовательностей событий, вызванных каждым идентифицированным видом отказа общей причины на различных уровнях функциональной структуры системы;
* определение критичности или приоритетности для дополнительных исследований, конструкторской и технологической проработки, диагностики с целью снижения негативных последствий отказов каждого вида, влияющих на правильность функционирования, безопасность и параметры системы;
* классификация идентифицированных видов отказов в соответствии с характеристиками: легкость обнаружения, возможность диагностирования, контролепригодность, условия эксплуатации и ремонта (ремонт, эксплуатация, логистика и т.д.);
* идентификация функциональных отказов системы и оценка тяжести последствий и вероятности возникновения отказа;
* разработка плана улучшения проекта путем сокращения количества и последствий видов отказов за счёт разработки конструкторских, технологических, организационных мероприятий;
* разработка плана эффективной интегральной логистической поддержки (диагностики, технического обслуживания, ремонта) для снижения вероятности возникновения отказов.

Планирование и выполнение расчетов надежности, а также проведение АВПО (FMEA), АВПКО (FMECA) должны являться элементами ПОН, дополнять друг друга, служить взаимными источниками исходных данных. По результатам АВПКО (FMECA) уточняют критерии отказов объекта, модели, применяемые при расчете его надежности, задачи и содержание технического обслуживания и ремонта объекта, а методы и результаты расчетов надежности используют для оценки вероятностей отказов ТС, учитываемых при анализе их критичности.

АВПКО (FMECA) обеспечивает получение исходных данных для:

* уточнения распределения требований надежности между составными частями проекта;
* планирования экспериментальной отработки проектов;
* установления и уточнения требований по приспособленности проекта к диагностированию (контролепригодности) и его ремонтопригодности;
* планирования системы технического обслуживания и ремонта проекта, отработки эксплуатационной и ремонтной документации;
* составления (совершенствования) программ обучения и тренировки эксплуатационного и ремонтного персонала, правил его поведения в аварийных ситуациях.

Результаты АВПКО (FMECA) учитывают при принятии решений о завершении этапов работ на стадиях жизненного цикла ТС, включая приемку ОКР.

**Применение АВПО (FMEA), АВПКО (FMЕСА) в процессе анализа проекта.**

**Методы анализа проведения АВПО (FMEA), АВПКО (FMЕСА).**

АВПО (FMEA), АВПКО (FMЕСА) проводят одним из следующих методов:

* структурным;
* функциональным;
* комбинированным.

Независимо от применяемого метода в качестве первого этапа анализа выполняют следующие процедуры:

* составление перечня и описаний всех задач, выполняемых объектом в эксплуатации, и необходимых для реализации каждой задачи рабочих функций объекта в целом и его элементов вплоть до установленного для данного этапа анализа или предельно возможного уровня разукрупнения. При этом идентифицируют все элементы заданного и вышестоящего уровней, участвующие в выполнении каждой функции объекта;
* кодирование каждой функции и элементов объектов в соответствии с установленной системой кодирования;
* описание режимов и условий выполнения каждой задачи в виде временных диаграмм и циклограмм нагружения объекта и его элементов;
* составление функциональной блок-схемы объекта и структурной (структурно-функциональной) схемы его надежности.

**Структурные методы АВПО (FMEA), АВПКО (FMЕСА)** относят к классу индуктивных методов (восходящий анализ "снизу вверх"), применяются для относительно простых объектов, отказы которых могут быть четко локализованы, а последствия каждого отказа элементов могут быть прослежены на всех вышестоящих уровнях структуры объекта.

Общая схема (алгоритм) АВПО (FMEA), АВПКО (FMЕСА) структурным методом состоит в следующем:

* в соответствии с планом анализа устанавливают минимальный уровень разукрупнения, с которого начинают АВПО (FMEA);
* на основе функциональной блок-схемы объекта идентифицируют все элементы выбранного уровня разукрупнения;
* для каждого идентифицированного элемента данного уровня на основе имеющихся классификаторов отказов, инженерного анализа, имеющихся априорных данных, опыта и знаний составляют перечень возможных видов отказов данного элемента;
* для каждого вида отказов выбранного элемента определяют его возможные последствия на рассматриваемом и следующих уровнях структуры объекта;
* для элементов, отказы определенного вида которых приводят непосредственно к отказу объекта или снижению качества его функционирования, оценивают категорию тяжести последствий отказов (при АВПО (FMEA)) или рассчитывают показатели критичности (при АВПКО (FMЕСА));
* повторяют описанные выше операции последовательно для элементов всех вышестоящих уровней разукрупнения. Последствия отказов элементов нижестоящего уровня, которые не могут быть выражены в виде влияния на функционирование элементов рассматриваемого уровня, рассматривают как самостоятельные виды отказов на этом уровне;
* выделяют отказы, категория тяжести последствий или оценки показателей критичности которых превосходят пределы, установленные планом анализа, а элементы, соответствующие этим отказам, включают в перечень критичных элементов.

Для каждого критичного элемента:

* определяют наличие и оценивают достаточность предусмотренных средств и методов обнаружения, локализации и индикации отказов, включая средства проектирования, моделирования, испытаний (виртуальных, натурных);
* определяют возможные меры, обеспечивающие обеспечение (сохранение) работоспособности объекта при возникновении данного отказа (введение резервирования, перестраиваемая структура, изменение алгоритма функционирования) и оценивают целесообразность их введения;
* определяют возможные меры по снижению вероятности отказов (проведение конструкторских и технологических изменении, натурных и виртуальных испытаний, применение в облегченном режиме, введение защиты от перегрузок, дополнительных проверок в процессе изготовления и эксплуатации, введение профилактического обслуживания и плановых замен в эксплуатации и т.п.) и оценивают их эффективность;
* определяют возможные способы предупреждения наиболее опасных последствий отказов (аварийная защита и сигнализация, специальные правила поведения персонала (экипажа) при возникновении отказов и т.п.).

При углубленном анализе возможно рассмотрение на каждом уровне разукрупнения комбинаций отказов двух и более элементов.

Таким образом, АВПО (FMEA), АВПКО (FMЕСА) структурным методом применим на различных уровнях декомпозиции системы - от системы в целом до функций отдельных компонентов или команд программного обеспечения. Анализ начинают с элементов самого нижнего уровня системы и проводят по восходящей схеме, пока не будут определены конечные последствия для системы в целом (рис. 9).

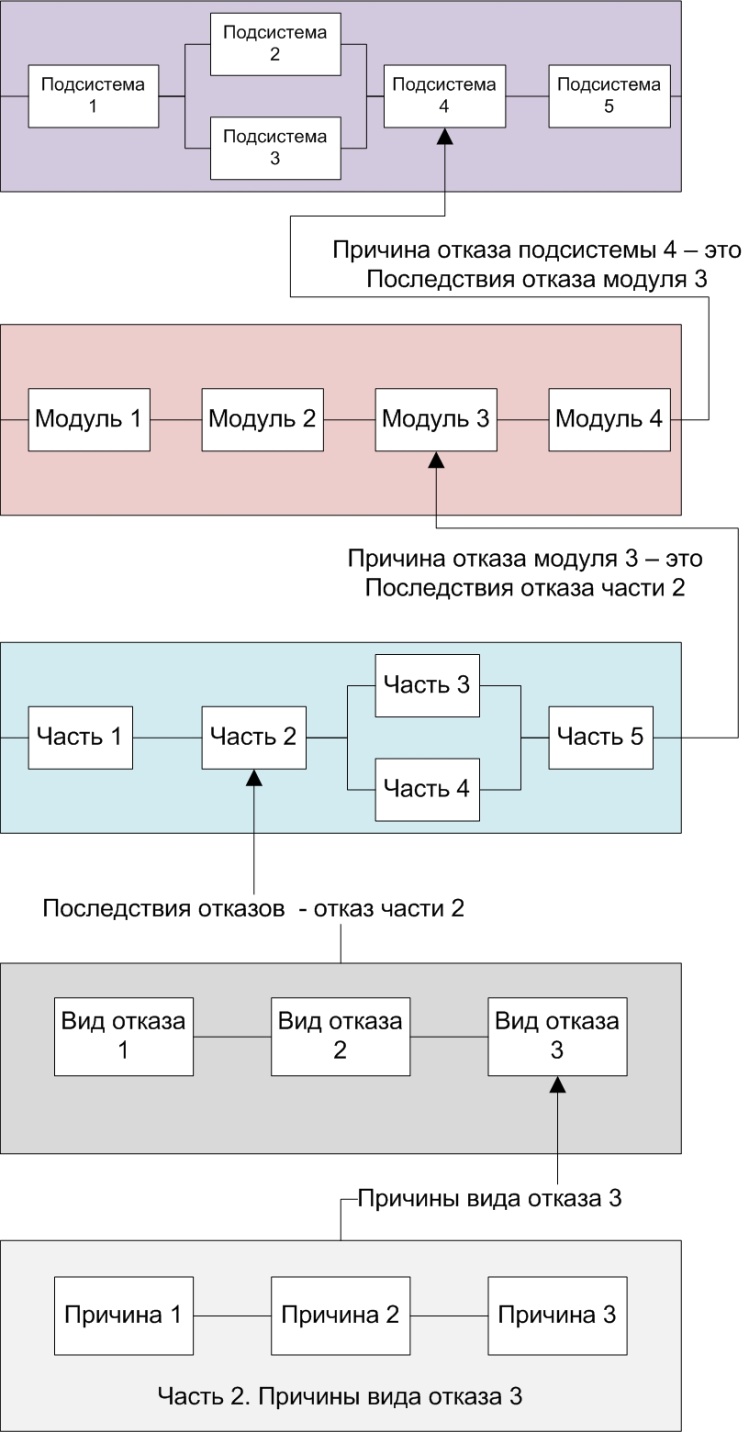


Рис. 9. Взаимосвязь видов и последствий отказов в иерархической структуре системы.

**Понятие декомпозиции системы.**

Декомпозиция рассматривает функционирование комплекса как сложное событие, распадающиеся на элементы согласно структурно-логической схемы надежности рассматриваемой системы (корабля). При декомпозиции выделяют существенно независимые подсистемы, ответственные за определенные функции, либо по принципу расположения в объекте. Декомпозиция исследуемой системы может иметь несколько уровней. Нулевой уровень представляет собой динамическую систему в целом, первый уровень – подсистемами и т. д.

На втором уровне декомпозиции выделяют простые динамические подсистемы. Декомпозиция функциональной и конструктивной схем корабля с выделением подсистем различного уровня позволяет наглядно проводить многоуровневый АВПКО. При анализе структуры корабля или проекта целесообразно выделять 2 вида декомпозиции:

- Декомпозиция по совокупности подсистем низкого уровня, включаемых в подсистемы более высокого уровня по функциональному признаку. Например «Корабль – подсистема - деталь»

- Декомпозиция по принципу расположения на объекте. Например «Корабль – помещение - деталь».

Таким образом, в внутри подсистемы могут быть включены подсистемы более низкого уровня, расположенные в разных помещениях. А, также, внутри определенного помещения могут быть расположены подсистемы низкого уровня и отдельные детали, принадлежащие к различным подсистемам более высокого уровня.

Последствия отказа, идентифицированного на более низком уровне, могут стать видами отказов для более высокого уровня системы. Виды отказов на более низком уровне системы могут стать причинами отказов на более высоком уровне системы. При декомпозиции системы последствия одной или более причины вида отказов создают вид отказа, который в свою очередь является причиной отказов составной части. Отказ составной части является причиной отказа модуля, который в свою очередь является причиной отказа подсистемы. Таким образом, воздействие причины отказа на одном уровне системы становится причиной воздействия на более высоком уровне.

При определении последствий отказа необходимо рассмотреть отказы более высокого уровня и отказы того же уровня, возникшие в результате произошедшего отказа. Анализ должен выявить все возможные комбинации видов отказов и их последовательностей, которые могут быть причиной последствий видов отказа на более высоком уровне. В этом случае необходимо дополнительное моделирование для оценки тяжести или вероятности возникновения таких последствий.

В общем случае АВПО (FMEA), АВПКО (FMЕСА) применяют к отдельным видам отказов и их последствиям для системы в целом. Каждый вид отказа рассматривают как независимый. Таким образом, процедура АВПО (FMEA), АВПКО (FMЕСА) не подходит для рассмотрения зависимых отказов или отказов, являющихся следствием последовательности нескольких событий. Для анализа таких ситуаций необходимо применять марковский анализ [15] и/или анализ дерева неисправностей [13].

**Функциональные методы АВПО (FMEA), АВПКО (FMЕСА)** относят к классу дедуктивных методов (анализ по нисходящей схеме), применяемых для сложных многофункциональных объектов, отказы которых трудно априорно локализовать и для которых характерны сложные зависимые отказы.

Общая схема (алгоритм) АВПО (FMEA), АВПКО (FMЕСА) функциональным методом:

* идентифицируют все функции, выполняемые объектом:

- Требования к функционированию системы должны быть определены так, чтобы обеспечить ясные формулировки критериев отказа и/или работоспособности.

- Требования к готовности или безопасности следует устанавливать на основе заданных минимальных уровней функционирования, необходимых для работы, и максимальных уровней повреждения, допускающих приемку.

* для каждой функции на основе априорных данных, опыта исследователя, инженерного анализа и другими доступными способами определяют перечень возможных нарушений (отклонений) данной функции;
* для каждого нарушения функции оценивают тяжесть возможных последствий этого нарушения (качественно через АВПО (FMEA)) или количественно - ожидаемый ущерб (при АВПКО (FMЕСА)).
* выделяют критические нарушения функции, тяжесть возможных последствий которых или ущерб от которых превосходит пределы, установленные планом анализа;
* для каждого выделенного критического нарушения, принимая его возникновение в качестве "вершинного события", **строят дерево отказов**, охватывающее отказы элементов всех уровней разукрупнения, вплоть до нижнего уровня, установленного планом анализа;
* с помощью построенного дерева выделяют одиночные элементы, приводящие к критическому нарушению функций изделия, и сочетания элементов, совместные отказы которых ведут к указанному нарушению;
* оценивают вероятности отказов одиночных элементов и вероятности выделенных комбинаций отказов элементов, с использованием которых при проведении АВПКО рассчитывают показатели критичности соответствующих отказов (сочетаний отказов);
* составляют перечни критичных элементов.

**Комбинированный метод АВПО (FMEA), АВПКО (FMЕСА).**

Как правило, для сложных объектов АВПО (FMEA), АВПКО (FMЕСА) проводят комбинированными методами, сочетающими элементы структурных и функциональных методов. Например, результаты проведения анализа рисков проекта в целом с помощью структурной (структурно-функциональной) схемы надежности, могут потребовать проведения АВПО (FMEA), АВПКО (FMЕСА) для отдельных единиц оборудования, подсистем.

**Рекомендации по применению АВПО (FMEA), АВПКО (FMЕСА).**

АВПО (FMEA), АВПКО (FMЕСА) может быть применен самостоятельно. Однако, в общем случае анализа сложной системы с несколькими функциями, многочисленными объектами и взаимосвязями между этими объектами АВПО (FMEA), АВПКО (FMЕСА) является необходимым, но недостаточным. Чаще всего в качестве системного индуктивного метода анализа АВПО (FMEA), АВПКО (FMЕСА) используют в качестве дополнения к другим методам, например, дедуктивным, (FTA). Это особенно справедливо, когда решения должны быть найдены в ситуациях с многократными отказами и цепочкой последствий.

На стадии проектирования часто трудно определить, какой метод (индуктивный или дедуктивный) предпочесть.

Если для оборудования и системы идентифицированы уровни риска, предпочтителен дедуктивный метод. На ранних стадиях проектирования, когда известны только функции, общая структура системы и ее подсистемы, успешное функционирование системы можно изобразить с помощью структурной (структурно-функциональной) схемы надежности или дерева неисправностей. Однако для составления этих систем к подсистемам должен быть применен индуктивный процесс АВПО (FMEA), АВПКО (FMЕСА). В этих обстоятельствах метод АВПО (FMEA), АВПКО (FMЕСА) не является всеобъемлющим, но отражает результат в наглядной табличной форме.

Анализ дерева неисправностей (FTA) является дополнительным дедуктивным методом анализа видов отказов и соответствующих им причин. Он позволяет прослеживать причины низкого уровня, приводящие к отказам высокого уровня. Хотя логический анализ иногда используют для качественного анализа последовательностей неисправностей, он обычно предшествует оценке частоты отказов высокого уровня. FTA позволяет моделировать взаимозависимости различных видов отказов в тех случаях, когда их взаимодействие может привести к событию высокой тяжести, Это особенно важно, когда появление одного вида отказа вызывает появление другого вида отказа с высокой вероятностью и высокой тяжестью. Этот сценарий не может быть успешно смоделирован с применением FMEA, где каждый вид отказа рассматривают независимо и индивидуально.

Один из недостатков АВПО (FMEA), АВПКО (FMЕСА) заключается в его неспособности анализировать взаимодействия и динамику возникновения вида отказа в системах. FTA же концентрируется на логике совпадающих (или последовательных) и альтернативных событий, вызывающих нежелательные последствия, позволяет построить правильную модель анализируемой системы, оценки ее безотказности и вероятности отказа, а также позволяет оценить влияние улучшений проекта и уменьшения числа отказов конкретного вида на надежность системы в целом.

Однако если система базируется главным образом на последовательной логике с небольшим резервированием и многочисленными функциями, то FTA является слишком сложным способом представления логики системы и идентификации видов отказов. В таких случаях адекватны АВПО (FMEA), АВПКО (FMЕСА) и метод структурной схемы надежности. В других случаях, когда предпочтителен FTA, он должен быть дополнен описаниями видов, отказов и их последствий.

При выборе метода анализа необходимо руководствоваться в первую очередь специфическими, а не только техническими требованиями проекта, а также требованиями к показателям времени, стоимости, эффективности и использования результатов.

Таким образом, АВПО (FMEA), АВПКО (FMЕСА) поддерживает концепцию анализа проекта и при проектировании подсистем и системы в целом должен применяться как можно раньше. АВПО (FMEA), АВПКО (FMЕСА) применим ко всем уровням системы, но более подходит для низких уровней, характеризующихся большим числом объектов и/или функциональной сложностью. В конце этапа проектирования АВПО (FMEA), АВПКО (FMЕСА) используют для проверки конструкции и демонстрации соответствия разработанной системы установленным требованиям заказчика, требованиям стандартов, инструкций.

АВПО (FMEA), АВПКО (FMЕСА) - метод, который приспособлен к исследованию отказов оборудования и может быть применен к различным типам систем (электрических, механических, гидравлических и т.д.) и их комбинациям для частей оборудования, системы или проекта в целом. АВПО (FMEA), АВПКО (FMЕСА) должен включать в себя исследование программного обеспечения и действий человека, если они влияют на надежность системы.

Информация, полученная на основе АВПО (FMEA), АВПКО (FMЕСА), идентифицирует приоритеты проведения дополнительных исследований и расчетов, моделирования и испытаний, конструкторских, технологических проработок, конструкторских и технологических изменений, выборочного и входного контроля в процессе производства и монтажа, а также для квалификационных, приемо-сдаточных, приемочных и пусковых испытаний. FMEA является источником информации для процедур диагностики, технического обслуживания при разработке соответствующих руководств.

При выборе глубины и способов применения АВПО (FMEA), АВПКО (FMЕСА) к объекту или проекту важно рассмотреть цели, для которых необходимы результаты АВПО (FMEA), АВПКО (FMЕСА), согласованность по времени с другими действиями и установить требуемую степень компетентности и контроля нежелательных видов и последствий отказов.

Если время ограничено, АВПО (FMEA), АВПКО (FMЕСА) должен быть сконцентрирован на тех частях конструкции, которые являются новыми или используют новые методы. АВПО (FMEA), АВПКО (FMЕСА) может быть направлен на области, идентифицированные как критические другими методами анализа.

АВПКО (FMЕСА) системы может быть выполнен вначале для компонентов системы независимо от ее конкретного применения, например, электронный усилитель, электрический двигатель, механический клапан, а затем скорректирован в соответствии с особенностями конструкции системы.

На рис. 10 представлено движение информации в процессе применения комбинированного метода.

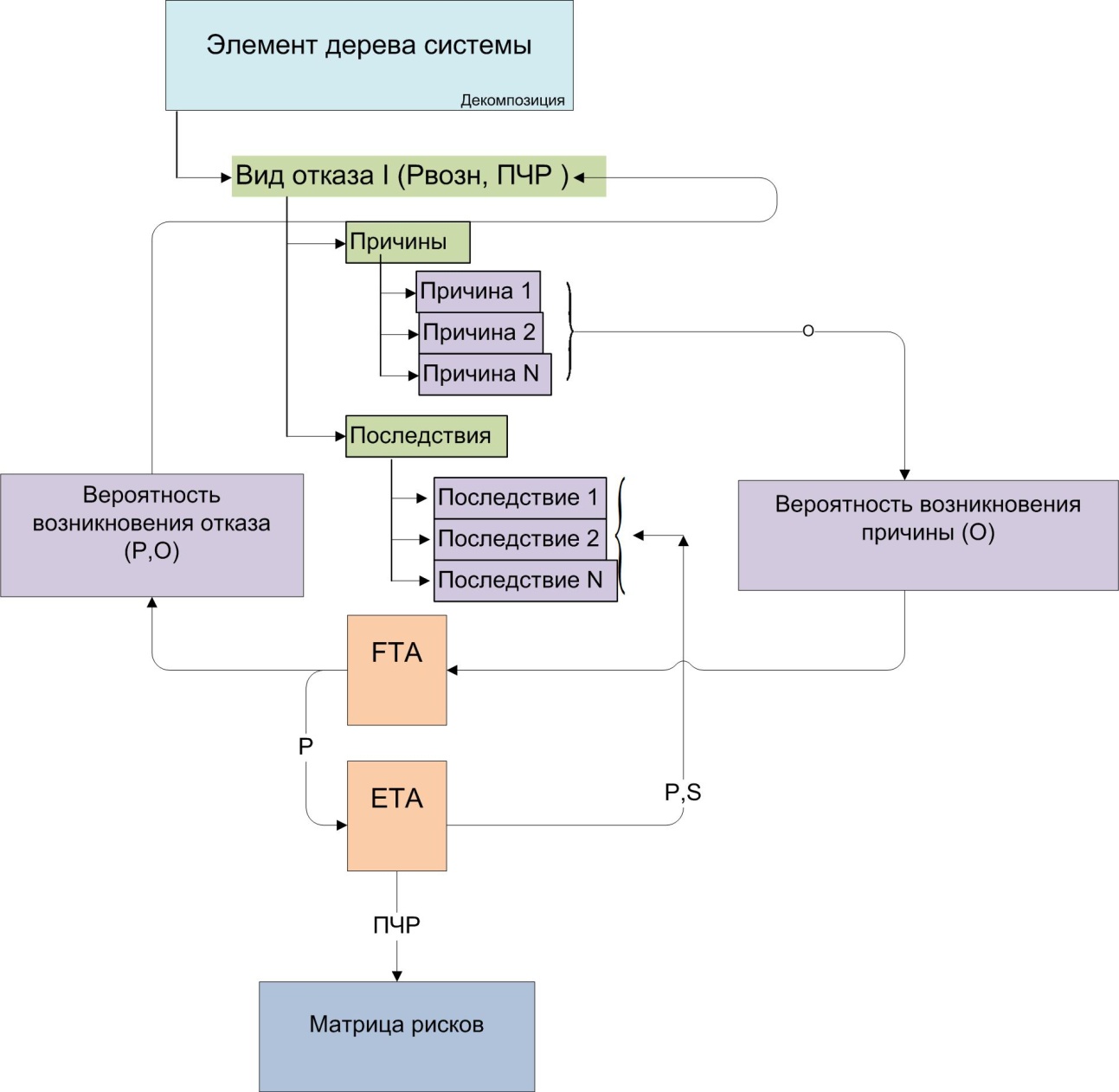


Рис. 10. Применение комбинированного метода анализа рисков

Общие принципы применения методов анализа:

* АВПО (FMEA), АВПКО (FMЕСА) применим, когда требуется всестороннее знание характеристик отказа объекта;
* АВПО (FMEA), АВПКО (FMЕСА) более подходит для небольших систем, модулей или комплексов;
* АВПО (FMEA), АВПКО (FMЕСА) является важным инструментом исследований, разработок, проектирования или решения иных задач, когда недопустимые последствия отказов должны быть идентифицированы и найдены необходимые меры по их устранению или смягчению;
* АВПО (FMEA), АВПКО (FMЕСА) пригоден для объектов, при проектировании которых использованы новейшие достижения, когда характеристики отказов не могут быть известны из предыдущей эксплуатации;
* АВПО (FMEA), АВПКО (FMЕСА) более применим к системам, имеющим большое количество компонентов, которые связаны общей логикой отказов;
* FTA является более подходящим для анализа видов многократных и зависимых отказов со сложной логикой и резервированием, с учетом воздействий персонала.
* FTA может быть использован на более высоких уровнях структуры системы, ранних стадиях проекта и в случае идентификации необходимости детального FMEA на более низких уровнях при углубленной проработке конструкции.

Преимущества АВПО (FMEA), АВПКО (FMЕСА) заключаются в следующем:

* идентификация отказов, которые при появлении по одному и в комбинации имеют недопустимые или существенные последствия, и определение видов отказов, которые могут иметь серьезные последствия для ожидаемой или требуемой функции. Последствия могут включать в себя зависимые отказы;
* определение необходимых методов повышения надежности конструкции (резервирование, оптимальные рабочие нагрузки, отказоустойчивость, выбор компонентов и т.д.);
* обеспечение логической модели для оценки вероятности или интенсивности появления аномальных условий эксплуатации системы при подготовке к анализу критичности;
* выявление проблемных зон безопасности и ответственности за качество выпускаемой продукции или ее несоответствие обязательным требованиям. Для безопасности необходимы самостоятельные исследования;
* разработка программы испытаний, позволяющей обнаруживать потенциальные виды отказов;
* помощь в определении особенностей общей стратегии и графика профилактического технического обслуживания;
* помощь и поддержка в определении критериев испытаний, планов испытаний и диагностических процедур (сравнительные испытания, испытания на надежность);
* поддержка последовательности исключения дефектов конструкции и поддержка планирования альтернативных режимов работы и переконфигурации;
* понимание проектировщиками параметров, влияющих на надежность системы;
* разработка документа, содержащего доказательства предпринятых действий по обеспечению соответствия результатов проектирования требованиям технического задания при обслуживании.

Ограничения и недостатки АВПО (FMEA), АВПКО (FMЕСА):

* АВПО (FMEA), АВПКО (FMЕСА) эффективен, если его используют для анализа элементов, которые вызывают отказ системы в целом или нарушение основной функции системы. Однако АВПО (FMEA), АВПКО (FMЕСА) может быть трудоемким и неэффективным для сложных систем, имеющих много функций и состоящих из различных наборов компонентов. Эти сложности увеличиваются при наличии многочисленных режимов эксплуатации, а также нескольких политик технического обслуживания и ремонта.
* Могут возникнуть осложнения и ошибки при попытке охвата исследованиями АВПО (FMEA), АВПКО (FMЕСА) нескольких уровней в иерархической структуре системы, если она предусматривает резервирование.
* Так как главное предположение этого анализа - независимость видов отказов, то взаимосвязи между людьми или группами видов отказов или причинами видов отказов эффективно представлены в АВПО (FMEA), АВПКО (FMЕСА) не могут. Этот недостаток становится еще более явным из-за взаимодействий программного обеспечения и аппаратных средств, когда предположение о независимости не подтверждается. Отмеченное справедливо для взаимодействия человека с аппаратными средствами и моделей этого взаимодействия.
* Предположение о независимости отказов не позволяет уделять должное внимание видам отказа, которые при совместном появлении могут иметь существенные последствия, тогда как каждый из них в отдельности имеет низкую вероятность появления. Взаимосвязи элементов системы легче исследовать, используя для анализа метод дерева отказов FTA [11]. Метод дерева неисправностей FTA предпочтителен для применения в АВПО (FMEA), АВПКО (FMЕСА), поскольку ограничивается связями только двух уровней иерархической структуры, например идентификацией видов отказов объектов и определением их последствий для системы в целом. Эти последствия затем становятся видами отказов на следующем уровне, например для модуля, и т.д.
* неспособность АВПО (FMEA), АВПКО (FMЕСА) оценить общую надежность системы и таким образом оценить степень улучшения ее конструкции или изменений.

**Процедуры анализа видов, последствий и критичности отказов АВПКО (FMECA), АВПО (FMEA)**

Блок-схема (рис. 11) показывает общую процедуру анализа видов, последствий и критичности отказов АВПКО (FMECA), АВПО (FMEA).



Рис. 11. Блок-схема анализа АВПКО (FMECA), АВПО (FMEA)

**Определение видов отказов.**

Для оценки функционирования системы необходимо идентифицировать ее критические элементы, от функционирования которых зависит успешное функционирование системы. Процедура идентификации видов отказов, их причин и последствий требует подготовки списка ожидаемых (потенциальных) видов отказов на основе:

* назначения системы;
* особенностей элементов системы;
* режима работы системы;
* требований к эксплуатации;
* ограничений по времени;
* воздействий окружающей среды;
* рабочих нагрузок.

Разработчики оборудования, систем, схем, поставщики комплектующих должны идентифицировать потенциальные виды отказов для своей продукции.

Данные о видах отказов могут быть получены из следующих источников:

* для новых объектов могут быть использованы данные объектов с аналогичными функцией и структурой, а также результаты испытаний этих объектов с соответствующими нагрузками;
* для новых объектов потенциальные виды отказов и их причины определяют в соответствии с целями проектирования и детальным анализом функций объекта;
* для объектов, находящихся в эксплуатации, могут быть использованы данные отчетов, относящихся к обслуживанию и отказам;
* потенциальные виды отказов могут быть определены на основе анализа функциональных и физических параметров, характерных для работы объекта.

Пример списка общих видов отказов приведен в таблице 2.

Таблица 2

Пример общих видов отказов

|  |  |
| --- | --- |
| Номер вида отказа | Наименование вида отказа |
| 1 | Отказ в процессе функционирования |
| 2 | Отказ, связанный с несрабатыванием в установленное время |
| 3 | Отказ, связанный с невозможностью прекращения работы в установленное время |
| 4 | Преждевременное включение |
| 5 | Превышение значения рабочего параметра 1 в процессе работы |
| 6 | Пониженное значение рабочего параметра 1 в процессе работы |
| 7 | Отказ, связанный с невозможностью запуска в ручном режиме |
| 8 | Отказ, связанный с неисправностью системы более высокого уровня |

Потенциальные виды отказов должны быть идентифицированы и описаны на структурной схеме надежности объекта. Затем определяют возможные отказы для компонентов, подсистем и функций системы (Таблица 3).

Таблица 3

Виды отказов компонентов, подсистем системы

|  |  |  |
| --- | --- | --- |
| Номер вида отказа | Наименование элемента (функции) | Наименование вида отказа |
| 1 | Система газового контроля | Отказ системы газового контроля |
| 2 | Система защиты 1 уровня | Отказ системы защиты |
| 3 | Система азотного пожаротушения (САП) | Отказ САП |
| 4 | Система пожаротушения ТРВ | Отказ системы пожаротушения ТРВ |
| 5 | Система пожарной сигнализации | Отказ системы пожарной сигнализации |
| 6 | Теленаблюдение (ТН) | Отказ ТН |
| 7 | Электрооборудование | Отказ электрооборудования с коротким замыканием |
| 8 | ЭХРВ | 8.1 Возгорание ЭХРВ 1 |
| 8.2 Возгорание ЭХРВ 2 |
| 8.3 Возгорание ЭХРВ 3 |
| 9 | Блокировочный клапан | 9.1 Отказ системы ДУА блокировочного клапана (КБ Х) |
| 9.2 Отказ ручного привода блокировочного клапана КБ |
| 9.3 Отказ блокировочного клапана |
| 10 | Датчики давления ВВД | Отказ датчика ВВД |
| 11 | Датчики температуры | Отказ датчика температуры |

**Определение причин отказов.**

Так как вид отказов может иметь несколько причин, должны быть идентифицированы и описаны наиболее вероятные независимые причины каждого потенциального вида отказов.

Идентификация и описание причин отказов и предложений по их устранению выполняют на основе изучения последствий отказов и их тяжести. Причины отказов могут быть определены на основе анализа эксплуатационных отказов или отказов в процессе испытаний, установлены экспертными методами.

**Определение последствий отказа.**

После выбора видов отказа, пригодных для проводимого анализа, определяют последствия отказов для компонентов, подсистем и функций системы.

Последствие отказа является результатом действия вида отказов. Последствие отказа может быть вызвано одним или несколькими видами отказов одного или нескольких объектов. Должны быть идентифицированы, оценены и зарегистрированы последствия каждого вида отказов для функционирования элементов, функции или системы. Так как последствия отказа могут воздействовать на следующий и на высший уровень анализа системы, на каждом уровне последствия отказов должны быть оценены для следующего, более высокого уровня.

Локальные последствия отказа (последствия вида отказа для рассматриваемого элемента системы) должны быть описаны для каждого возможного отказа на выходе объекта. Цель идентификации локальных последствий состоит в обеспечении оценки существующих или разработки рекомендуемых корректирующих действий. В некоторых случаях локальные последствия отказа отсутствуют.

При идентификации последствий возможного отказа для высшего уровня системы проводят анализ на всех промежуточных уровнях. Последствия высшего уровня могут быть результатом многократных отказов. Необходимо классифицировать последствия отказов системы, например: отказ предохранителя, устранимый отказ, неустранимый отказ, ухудшение выполнения задачи, невыполнение задачи, последствия для отдельных людей, группы или общества в целом.

Типичной является разработка АВПО (FMEA), АВПКО (FMЕСА) для конкретного проекта с конкретными последствиями отказов системы. Возможность учета в АВПО (FMEA), АВПКО (FMЕСА) самых отдаленных последствий отказа системы зависит от конструкции системы и взаимосвязей АВПО (FMEA), АВПКО (FMЕСА) с другими формами анализа, дерево неисправностей, марковский анализ и т.п.

В результате анализа последствий должен быть подготовлен список последствий отказов для конкретной системы. В таблицах 4, 5, 6 и 7 приведен типичный набор последствий отказов на различных уровнях системы.

Таблица 4

Пример последствий отказов

|  |  |
| --- | --- |
| Номер вида отказа | Последствие |
| 1 | Система не функционирует |
| 2 | Значение одной из ключевых технических характеристик системы меньше установленной |
| 3 | Система не выполняет одну из функций |
| 4 | Система срабатывает преждевременно |

Таблица 5

Последствия отказов на рассматриваемом уровне

|  |  |
| --- | --- |
| Вид отказа | Последствие |
| Отказ системы газового контроля | Увеличение концентрации кислорода |
| Отказ системы защиты | Неразвитый пожар |
| Отказ САП | Несрабатывание САП |
| Отказ системы пожаротушения ТРВ | Отказ системы защиты 1 уровня |
| Отказ системы пожарной сигнализации | Необнаружение возгорания |
| Отказ ТН | Необнаружение возгорания |
| Отказ электрооборудования с коротким замыканием | Короткое замыкание электрооборудования |
| 8.1 Возгорание ЭХРВ 1 | Возгорание ЭХРВ |
| 8.2 Возгорание ЭХРВ 2 | Возгорание ЭХРВ |
| 8.3 Возгорание ЭХРВ 3 | Возгорание ЭХРВ |
| 9.1 Отказ системы ДУА блокировочного клапана (КБ Х) | Не закрыть блокировочный клапан |
| 9.2 Отказ ручного привода блокировочного клапана КБ | Не закрыть блокировочный клапан |
| 9.3 Отказ блокировочного клапана | Не закрыть блокировочный клапан |
| Отказ датчика ВВД | Отказ датчиков системы ВВД |
| Отказ датчика температуры | Отказ датчиков системы ВВД |

Таблица 6

Последствия отказов для следующего уровня системы

|  |  |
| --- | --- |
| Вид отказа | Последствие |
| Отказ системы газового контроля |  |
| Отказ системы защиты |  |
| Отказ САП |  |
| Отказ системы пожаротушения ТРВ | Неразвитый пожар |
| Отказ системы пожарной сигнализации | Отказ системы защиты 1 уровня |
| Отказ ТН | Отказ системы защиты 1 уровня |
| Отказ электрооборудования с коротким замыканием | Возгорание |
| 8.1 Возгорание ЭХРВ 1 | Возгорание |
| 8.2 Возгорание ЭХРВ 2 | Возгорание |
| 8.3 Возгорание ЭХРВ 3 | Возгорание |
| 9.1 Отказ системы ДУА блокировочного клапана (КБ Х) | Поступление воздуха от системы ВВД |
| 9.2 Отказ ручного привода блокировочного клапана КБ | Поступление воздуха от системы ВВД |
| 9.3 Отказ блокировочного клапана | Поступление воздуха от системы ВВД |
| Отказ датчика ВВД | Поступление воздуха от системы ВВД |
| Отказ датчика температуры | Поступление воздуха от системы ВВД |

Таблица 7

Последствия отказов для высшего уровня системы

|  |  |
| --- | --- |
| Вид отказа | Последствие |
| Отказ системы газового контроля | Объёмный пожар в отсеке X |
| Отказ системы защиты | Объёмный пожар в отсеке X |
| Отказ САП | Объёмный пожар в отсеке X |
| Отказ системы пожаротушения ТРВ | Объёмный пожар в отсеке X |
| Отказ системы пожарной сигнализации | Объёмный пожар в отсеке X |
| Отказ ТН | Объёмный пожар в отсеке X |
| Отказ электрооборудования с коротким замыканием | Объёмный пожар в отсеке X |
| 8.1 Возгорание ЭХРВ 1 | Объёмный пожар в отсеке X |
| 8.2 Возгорание ЭХРВ 2 | Объёмный пожар в отсеке X |
| 8.3 Возгорание ЭХРВ 3 | Объёмный пожар в отсеке X |
| 9.1 Отказ системы ДУА блокировочного клапана (КБ Х) | Объёмный пожар в отсеке X |
| 9.2 Отказ ручного привода блокировочного клапана КБ | Объёмный пожар в отсеке X |
| 9.3 Отказ блокировочного клапана | Объёмный пожар в отсеке X |
| Отказ датчика ВВД | Объёмный пожар в отсеке X |
| Отказ датчика температуры | Объёмный пожар в отсеке X |

Отчет о последствиях отказов должен быть основан на перечне последствий отказов системы в целом и должен содержать подробности видов отказов, влияющих на каждое последствие отказа. В таблицах 8 и 9 показан пример обзора последствий отказов.

Таблица 8

Пример вероятностей последствий отказов

|  |  |  |  |
| --- | --- | --- | --- |
| Номер последствия вида отказа | Последствие | Виды отказов, приводящие к последствию | Вероятность появления последствия отказа |
| 1 | Система не функционирует | 1,2,7,8 | 8·10-3 |
| 2 | Значение одной из ключевых технических характеристик системы меньше установленной | 6 | 6·10-4 |
| 3 | Система не выполняет одну из функций | 3,5,6 | 1,1·10-5 |
| 4 | Система срабатывает преждевременно | 3,4,8 | 3,6·10-7 |

Такая таблица может быть построена для различных качественных и количественных ранжирований объекта или системы.

Таблица 9

Вероятности последствий отказов для высшего уровня системы

|  |  |  |  |
| --- | --- | --- | --- |
| Номер последствия вида отказа | Последствие | Виды отказов, приводящие к последствию | Вероятность появления последствия отказа |
| 1 | Объёмный пожар в отсеке X | 1, 2, 3, 4 | 8·10-2 |
| 2 | Объёмный пожар в отсеке X | 5, 6 | 6·10-2 |
| 3 | Объёмный пожар в отсеке X | 7, 8, 9 | 1,1·10-3 |
| 4 | Объёмный пожар в отсеке X | 10, 11, 12, 13, 14, 15 | 3,6·10-4 |

**Определение методов обнаружения отказов.**

В процессе АВПКО (FMЕСА), АВПО (FMEA) для каждого вида отказа необходимо определить способ обнаружения отказа в процессе проектирования, испытаний, средства технического обслуживания для диагностики отказа. В процессе проектирования потенциальные отказы могут быть идентифицированы с помощью анализа надежности, в том числе структурного, численного, имитационного, объемного моделирования, виртуальных, макетных, натурных испытаний и т.д.

Диагностика отказов может быть выполнена с применением технических средств, автоматически устройствами, предусмотренными в конструкции (встроенное тестирование), введением специальной процедуры контроля до начала работы системы или при техническом обслуживании, при запуске системы в процессе ее функционирования или через установленные интервалы времени. После диагностики отказа должен быть устранен опасный режим эксплуатации.

При обнаружении отказов исследуют также, с какой вероятностью, когда и как недостаток конструкции, технологии будет идентифицирован и устранён.

**Определение условий компенсации отказа.**

Под компенсацией отказа понимают идентификацию всех особенностей проекта, конструкции на данном уровне системы, этапе разработки проекта или других мер, которые могут предотвратить или уменьшить последствия видов отказа. В анализе АВПКО (FMЕСА), АВПО (FMEA) должны быть зарегистрированы меры, препятствующие отказу:

* альтернативные схемные, конструкторские и технологические решения;
* альтернативные способы функционирования и компоненты, в том числе альтернативные комплектующие;
* резервированные компоненты, которые допускают длительную работу, если один или несколько компонентов отказали;
* мониторинг технического состояния или сигнальные устройства;
* другие методы и средства ликвидации и ограничения ущерба.

**Определение тяжести конечных последствий отказов. Классификация тяжести отказа.**

В соответствии с АВПО (FMEA) каждое идентифицированное последствие отказа относят к соответствующему классу тяжести (Таблицы 10 и 11). До проведения АВПО (FMEA), АВПКО (FMЕСА) должна быть выработана система классификации отказов по категориям тяжести их возможных последствий. При категорировании отказов по тяжести их последствий должны учитываться следующие факторы:

* характеристики системы в соответствии с возможными отказами, особенностями эксплуатации или окружающей среды;
* функциональные параметры системы;
* требования ТТЗ, требования, установленные в контракте;
* влияние отказа на качество функционирования объекта и полноту выполнения им назначенных функций, возможный ущерб (материальный, военный и др.), обусловленный снижением качества функционирования объекта или невыполнением объектом определенных функций (поставленных задач);
* опасность отказа (с учетом немедленных и отдаленных последствий) для жизни людей, для целостности и сохранности самого объекта;
* скорость развития неблагоприятных последствий отказа, определяющая возможность принятия соответствующих мер защиты от них.
* законодательные требования и требования безопасности;
* требования, связанные с гарантийными обязательствами.

Таблица 10

Пример классификации тяжести последствий отказа

|  |  |  |
| --- | --- | --- |
| Номер класса тяжести отказа | Наименование класса тяжести отказа | Описание последствия отказа для людей или окружающей среды |
| IV | Катастрофический | Вид отказа может привести к прекращению выполнения первичных функций системы и вызывает тяжелые повреждения системы и окружающей среды и/или гибель и тяжелые травмы людей |
| III | Критический | Вид отказа может привести к прекращению выполнения первичных функций системы и вызывает значительное повреждение системы и окружающей среды, но не представляет собой серьезной угрозы жизни или здоровью людей |
| II | Минимальный | Вид отказа может ухудшить выполнение функций системы без заметного повреждения системы или угрозы жизни или здоровью людей |
| I | Ничтожный | Вид отказа может ухудшить выполнение функций системы, но не вызывает повреждений системы и не создает угрозы жизни и здоровью людей |

Таблица 11

Классификация тяжести последствий отказа

|  |  |  |  |
| --- | --- | --- | --- |
| Номер класса тяжести отказа | Наименование класса тяжести отказа | Описание последствия отказа для людей или окружающей среды | Описание конкретного последствия отказа |
| IV | Катастрофический | Вид отказа может привести к прекращению выполнения первичных функций системы и вызывает тяжелые повреждения проекта (заказа) и окружающей среды и/или гибель и тяжелые травмы людей | Объёмный пожар в отсеке X |
| III | Критический | Вид отказа может привести к прекращению выполнения первичных функций системы и вызывает значительное повреждение заказа и окружающей среды, но не представляет собой серьезной угрозы жизни или здоровью людей | Неразвитый пожар  Возгорание |
| II | Некритический отказ | Вид отказа может ухудшить выполнение функций системы без заметного повреждения заказа или угрозы жизни или здоровью людей | Отказ системы защиты 1 уровня |
| I | Отказ с пренебрежимо малыми последствиями | Вид отказа может ухудшить выполнение функций системы, но не вызывает повреждений заказа и не создает угрозы жизни и здоровью людей | Поступление воздуха от системы ВВД |

**Анализ критичности.** **Определение частоты или вероятности появления отказов.**

Определение критичности подразумевает использование качественной или количественной меры последствий видов отказа. Смысл критичности, его определение и способ измерения формулируются как воздействие или значимость вида отказа, который необходимо устранить или смягчить его последствия. Цель анализа критичности состоит в качественном или количественном определении относительной величины каждого последствия отказа. Значения этой величины используют для установления приоритетности действий по устранению отказов или снижению их последствий на основе комбинаций критичности отказов и тяжести их последствий.

Для оценки тяжести последствий или критичности отказов, построения очередности необходимых доработок проекта с целью их предупреждения определяют частоту или вероятность появления каждого вида отказа. Частоту появления событий вычисляют на основе данных об отказах или оценивают для исследуемой составной части.

Вероятность появления видов отказов для системы можно оценивать с использованием:

* данных ресурсных испытаний;
* баз данных об интенсивностях отказов;
* результатов расчетов надежности, в том числе методом структурных схем;
* данных эксплуатационных отказов;
* данных об отказах аналогичных объектов или компонентов аналогичного класса.

Оценки вероятности появления отказа относят к определенному периоду времени, гарантийный период или установленный срок службы.

В процессе АВПО (FMEA) проводят предварительную качественную оценку и ранжирование выявленных возможных отказов по тяжести их последствий с целью определения необходимости дальнейшего углубленного анализа и оценки их критичности и очередности проведения соответствующих доработок объекта, системы технического обслуживания и ремонта. Например, при АВПО (FMEA) может проводиться предварительная качественная оценка ожидаемой частоты наступления отказов разных категорий тяжести при эксплуатации объектов. Указанные оценки используют:

* для ранжирования отказов по очередности необходимых доработок объекта с целью их предупреждения с использованием матриц "вероятность отказа - тяжесть последствий", (таблицы 12, 13);
* для построения шкал балльных оценок критичности отказов (таблицы 14, 15, 16).

Таблица 12

МАТРИЦА "ВЕРОЯТНОСТЬ ОТКАЗА - ТЯЖЕСТЬ ПОСЛЕДСТВИЙ" ДЛЯ РАНЖИРОВАНИЯ ОТКАЗОВ ПРИ АВПО

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Тяжесть последствий | | | |
| Ожидаемая частота возникновения | Катастрофический отказ (категория IV) | Критический отказ (категория III) | Некритический отказ (категория II) | Отказ с пренебрежимо малыми последствиями (категория I) |
| Частый отказ | А | А | А | С |
| Вероятный отказ | А | А | В | С |
| Возможный отказ | А | В | В | D |
| Редкий отказ | А | В | С | D |
| Практически невероятный отказ | В | С | С | D |

Ранги отказов:

А - обязателен углубленный количественный анализ критичности,

В - желателен количественный анализ критичности,

С - можно ограничиться качественным анализом,

D - анализ не требуется.

Таблица 13

# КАЧЕСТВЕННЫЕ ОЦЕНКИ ЧАСТОТЫ ОТКАЗОВ

|  |  |  |
| --- | --- | --- |
| Виды отказов по частоте | Качественное описание частоты для: | |
|  | индивидуального изделия | совокупности изделий |
| Частый отказ | Вероятно частое возникновение | Наблюдается постоянно |
| Вероятный отказ | Будет наблюдаться несколько раз за срок службы изделия | Вероятно частое возникновение |
| Возможный отказ | Возможно одно наблюдение данного отказа за срок службы | Наблюдается несколько раз |
| Редкий отказ | Отказ маловероятен, но возможен хотя бы один раз за срок службы | Вполне возможен хотя бы один раз |
| Практически невероятный отказ | Отказ настолько маловероятен, что вряд ли будет наблюдаться даже один раз за срок службы | Отказ маловероятен, но возможен хотя бы один раз |

Таблица 14

Оценки вероятностей отказов в баллах

|  |  |  |
| --- | --- | --- |
| Виды отказов по вероятности возникновения за время эксплуатации | Ожидаемая вероятность отказов, оцененная расчетом или экспериментальным путем | Оценка вероятности отказа в баллах, O |
| Отказ практически невероятен | Менее 0,00005 | 1 |
| Отказ маловероятен | От 0,00005 до 0,001 | 2 |
| Отказ имеет малую вероятность, обусловленную только точностью расчета | От 0,001 до 0,005 | 3 |
| Умеренная вероятность отказа | От 0,005 до 0,001 | 4 |
| Отказы возможны, но при испытаниях или в эксплуатации аналогичных изделий не наблюдались | От 0,001 до 0,005 | 5 |
| Отказы возможны, наблюдались при испытаниях и в эксплуатации аналогичных изделий | От 0,001 до 0,005 | 6 |
| Отказы вполне вероятны | От 0,005 до 0,01 | 7 |
| Высокая вероятность отказов | От 0,01 до 0,10 | 8 |
| Вероятны повторные отказы | Более 0,11 | 10 |

Таблица 15

Оценки последствий отказов

|  |  |
| --- | --- |
| Описание последствий отказов | Оценка последствий в баллах, S |
| Отказ не приводит к заметным последствиям, в процессе эксплуатации вероятно не обнаружится наличие неисправности | 1 |
| Последствия отказа незначительны, но в процессе эксплуатации может возникнуть нежелательная ситуация в связи с его появлением | 2-3 |
| Отказ приводит к заметному снижению эксплуатационных характеристик и/или к затруднению эксплуатации технической системы | 4-6 |
| Техническая система не может быть использовано по назначению, но угрозы безопасности отказ не представляет | 7-8 |
| Отказ представляет угрозу безопасности людей или окружающей среды | 9-10 |

Таблица 16

Оценка вероятности обнаружения отказа в результате ошибки разработки (комплектации) оборудования на этапе оценки заказа (проекта)

|  |  |  |
| --- | --- | --- |
| Виды отказов по вероятности обнаружения до поставки | Вероятность обнаружения отказа, оцененная расчетным или экспертным путем | Оценка вероятности в баллах, D |
| Очень высокая вероятность выявления отказа при разработке, проектировании, моделировании, проектной оценке надежности, виртуальных и натурных испытаниях, контроле параметров комплектующих | Более 0,95 | 1 |
| Высокая вероятность выявления отказа при разработке, проектировании, моделировании, проектной оценке надежности, виртуальных и натурных испытаниях, контроле параметров комплектующих | От 0,95 до 0,85 | 2-3 |
| Умеренная вероятность выявления отказа при разработке, проектировании, моделировании, проектной оценке надежности, виртуальных и натурных испытаниях, контроле параметров комплектующих | От 0,85 до 0,45 | 4-6 |
| Высокая вероятность пропуска дефектного оборудования, системы, схемы к производству и сборке заказа | От 0,45 до 0,25 | 7-8 |
| Очень высокая вероятность пропуска дефектного оборудования, системы, схемы к производству и сборке заказа | Менее 0,25 | 9-10 |

Для определения вероятности появления вида отказа, помимо информации об интенсивности отказов, опубликованной в справочниках, необходимо учитывать реальные условия функционирования каждого компонента (механические и/или электрические нагрузки), характеристики которого вносят свой вклад в вероятность появления отказа.

Достоверность оценки частот и вероятностей определяет достоверность оценки тяжести последствий и критичности отказов.

**Определение интенсивности отказов**

Если известны интенсивности отказов для видов отказов аналогичных объектов, определенные для внешних и эксплуатационных условий, аналогичных принятым для исследуемой системы, эти частоты событий могут быть непосредственно использованы в АВПО (FMEA), АВПКО (FMECA). На стадиях разработки и проектирования при отсутствии данных по показателям надёжности составных частей изделия (разрабатываемых и комплектующих узлов и деталей) оценка надежности изделия проводится с использованием отечественных и зарубежных стандартов и справочников. Справочники представляют собой сводные данные по испытаниям и эксплуатации аналогичных изделий в различных условиях. Стандарт позволяет получать требуемые показатели надёжности составной части с учётом условий эксплуатации и конструкторско-технологических характеристик составной части. Рекомендации по выбору значений этих показателей можно найти в соответствующих публикациях по надежности [28].

Для определения вероятности возникновения отказа в случае количественных методов анализа вместо интенсивности отказов i-го вида отказов λi используют значение критичности вида отказа С. Значение критичности отказа связано с условной частотой отказа и временем эксплуатации и может быть использовано для получения более реалистичной оценки риска, соответствующего конкретному виду отказа, в течение заданного времени использования продукции.

*Ci* = λ*itj*

где: *tj* - время работы компонента в течение всего заданного времени исследований АВПКО (FMECA), для которого оценена вероятность, т.е. время активной работы *j*-го компонента. Значение критичности для *j*-го компонента, имеющего *т* видов отказов, определяют по формуле

,

где: λi - оценка интенсивности отказов i-гo вида отказов (интенсивность отказов предполагается постоянной);

λj - интенсивность отказов j-го компонента;

αi - отношение количества i-ro вида отказов к общему количеству видов отказов, т.е, вероятность того, что объект будет иметь i-й вид отказа;

βi - условная вероятность последствия i-ro вида отказа.

Вероятность Pi появления отказа i-го вида за время tj для полученной критичности:

.

Если интенсивности видов отказов и соответствующие значения критичности малы, то с грубым приближением можно утверждать, что для вероятностей появления меньше 0,2 (критичность равна 0,223) значения критичности и вероятности отказа очень близки.

В случае переменных интенсивностей отказов или частот появления отказа необходимо вычислять вероятность появления отказа, а не критичность, которая основана на предположении о постоянстве интенсивности отказов.

**Риск R, значение приоритетности риска (RPN) и анализ риска**

АВПКО (FMЕСА) представляет сочетание качественного анализа видов и последствий отказов с количественными оценками критичности выявляемых при АВПО возможных отказов.

Одним из методов количественной оценки критичности является определение значения приоритетности риска [Risk Priority Number (RPN)] - величины, характеризующей тяжесть последствий. В этом случае риск оценивают субъективной мерой тяжести последствий и вероятностью возникновения отказа в течение заданного периода времени. В тех случаях, когда этот способ неприменим, необходимо обратиться к более простой форме неколичественного АВПО (FMEA).

При АВПКО (FMЕСА) критичность отказов оценивают с использованием показателей, учитывающих для каждого анализируемого отказа:

* вероятность его возникновения за время эксплуатации;
* условные вероятности наступления всех возможных неблагоприятных последствий отказа, если он может сопровождаться несколькими различными по характеру и тяжести последствиями;
* размер возможного ущерба в результате наступления каждого из ожидаемых последствий отказов.

В общем случае показатель критичности отказа представляет произведение его вероятности на размер ущерба от отказа, средневзвешенный по условным вероятностям проявления последствий отказа .

*Ck* =

Возможно применение других способов измерения критичности отказов.

Значения вероятностей отказов , учитываемые при оценке их критичности, рассчитывают (прогнозируют) принятыми в расчетах надежности методами с учетом структуры объекта, уровней нагруженности и режимов работы его элементов по имеющимся справочным или экспериментальным данным об их надежности.

Возможные последствия каждого отказа определяют по результатам АВПО (FMEA) объекта, а соответствующие условные вероятности наступления каждого последствия рассчитывают на основе моделей типа "дерева событий" или прогнозируют экспертными методами.

Для определения возможного ущерба от наступления определенных последствий каждого отказа в АВПКО (FMЕСА) применяют показатели, представляющие числовые характеристики соответствующих функций потерь, например распределения ущерба от отказов в натуральном выражении, и оцениваемые методами прогнозирования по априорным данным или путем моделирования возникающих в результате отказа аварийных ситуаций (пожаров, взрывов, выбросов отравляющих или радиоактивных веществ и др.).

Для объектов, абсолютные оценки последствий отказов которых невозможны или нецелесообразны по техническим или экономическим соображениям, применяют относительные балльные оценки возможного ущерба от отказов с использованием соответствующей шкалы, разработанной применительно к конкретному объекту и установленной в методике АВПКО (FMЕСА).

Степень риска можно представить как математическое ожидание величины ущерба от нежелательного события:

*R*(*m*)=,

где *pi*  – вероятность наступления события, связанного с ущербом;

*mi* – случайная величина ущерба.

В контексте анализа и обоснования безопасности энергетических установок степень риска – суммарная вероятность конечных аварийных состояний с радиационно-опасными последствиями.

В некоторых типах АВПКО (FMECA), АВПО (FMEA) в качестве общей меры потенциального риска R используют величину

R = SP,

где: S - значение тяжести последствий, т.е. степени влияния отказа на систему или экипаж (в безразмерных единицах);

Р - вероятность появления отказа. Если Р меньше 0.2, то ее можно заменить значением критичности С, которое используют в некоторых количественных методах АВПО (FMEA), (оценка вероятности появления последствий отказа).

Если в процессе применения АВПКО (FMECA), АВПО (FMEA) дополнительно выделяют уровень обнаружения отказа для системы в целом, то в этом случае при формировании значения приоритетности риска *RPN* используют значение вероятности обнаружения отказа D

RPN = SOD,

где: О - вероятность появления отказа для заданного или установленного периода времени (величина может быть определена как ранг, а не значение вероятности появления отказа);

D - характеризует процесс обнаружения отказа и представляет собой оценку вероятности идентифицировать и устранить отказ в процессе проектирования, разработки конструкторской документации, испытаний до проявления последствий для системы или в эксплуатации у заказчика. Значения D обычно ранжированы в обратном порядке по отношению к вероятности появления отказа или тяжести отказа. Чем выше значение D, тем менее вероятно обнаружение отказа.

Таким образом, более низкая вероятность обнаружения соответствует более высокому значению RPN и более высокой приоритетности вида отказа и значение приоритетности риска R, RPN можно использовать для установления приоритетов при сокращении идентифицированных видов отказа.

Кроме значения приоритетности риска в процессе принятия решения о сокращении видов идентифицированных отказов учитывают, прежде всего, значение тяжести видов отказа, подразумевая, что при равных или близких значениях RPNв первую очередь это решение следует применять к видам отказов с более высокими значениями тяжести отказов. Эти значения могут быть оценены в числовом виде с применением непрерывной или дискретной шкалы (конечное число заданных значений). Затем виды отказов ранжируют в соответствии с их RPN*.* Высокий приоритет назначают для высоких значений RPN*.* В некоторых случаях последствия для видов отказов с RPN, превышающим установленный предел, являются неприемлемыми, в то время как в других случаях высокие значения тяжести отказа устанавливают независимо от значений RPN*.*

Описанные типы АВПКО (FMECA), АВПО (FMEA) обычно применяют для анализа проекта. Различные типы АВПКО (FMECA), АВПО (FMEA) используют различные шкалы значений для *S*, *О* и *D*, например от 1 до 4 или 5. Некоторые АВПКО (FMECA), АВПО (FMEA), используемые для анализа конструкции, так называемые DFMEA и PFMEA, назначают шкалу от 1 до 10.

Ранг тяжести последствий назначают для каждого вида отказа на основе влияния последствий отказа на систему в целом, ее безопасность, выполнение требований, целей и ограничений, а также вида системы.

В отличие от шкалы тяжести последствий шкала вероятности появления отказов нелинейна и не является логарифмической. Поэтому необходимо учитывать, что соответствующее значение *RPN* после вычислений оценок также нелинейно и его необходимо использовать с особой осторожностью.

Концепция RPN предусматривает оценку вероятности обнаружения отказа, т.е. вероятности того, что с помощью процедур верификации, предусмотренных в процессе проектирования, а также в проекте изделия будут обнаружены возможные виды отказов за время, достаточное для предотвращения отказов на уровне системы в целом. Вероятность обнаружения трудно оценить для изделий, которые могут быть использованы в других системах.

Оценка поRPN обладает следующими недостатками:

* наличие пустых промежутков в диапазонах значений: 88 % диапазонов пусты, только 120 из 1000 значений использованы;
* неоднозначность RPN: несколько комбинаций различных значений параметров приводят к одинаковым значениям RPN;
* чувствительность RPN к небольшим изменениям: малые отклонения одного параметра оказывают большое влияние на результат, если другие параметры имеют большие значения (например, 9·9·3 = 243 и 9·9·4 = 324, в то время как 3·4·3 = 36 и 3·4·4 = 48);
* неадекватная шкала RPN: таблица появления отказов является нелинейной (например, отношение между двумя последовательными рангами может быть и 2,5, и 2);
* неадекватный масштаб RPN: разница в значениях для RPN может казаться незначительной, в то время как фактически является весьма существенной. Например, значения S = 6, О = 4, D = 2 дают RPN = 48, а значения S = 6, О = 5 и D = 2 дают RPN = 60. Второе значение RPN не вдвое больше, в то время как фактически для О = 5 вероятность появления отказа вдвое больше, чем для О = 4. Поэтому исходные значения для RPN не следует сравнивать линейно;

**Анализ риска**

Сочетание критичности и тяжести последствий характеризует риск, который отличается от обычно применяемых показателей риска меньшей строгостью и требует меньше усилий для оценки. Различия заключаются не только в способе прогноза тяжести последствий отказа, но также и в описании взаимодействий между вносящими вклад факторами с помощью обычной восходящей процедуры АВПКО (FMECA).

Можно выделить два основных метода оценки критичности: матрицу критичности и концепцию приоритетности риска RPN*.*

**Матрица критичности**

Критичность может быть представлена в виде матрицы критичности (рис. 12). В матрице критичности предполагается, что тяжесть последствий увеличивается с увеличением ее значения. В этом случае IV соответствует наивысшей тяжести последствий (гибель человека и/или потеря функции системы, травмы людей). Кроме этого, предполагается, что на оси ординат вероятность появления вида отказа возрастает снизу вверх.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Вероятность появления |  |  |  |  |
| 5(А) |  |  |  | Высокий риск |
| 4(В) |  | Вид отказа 1 |  |  |
| 3(С) |  |  |  |  |
| 2(D) |  |  | Вид отказа 2 |  |
| 1(Е) | Низкий риск |  |  |  |
| Тяжесть последствий | I | II | III | IV |

Рис. 12. Матрица критичности

Если самая высокая вероятность появления не превышает значения 0,2. то вероятность появления вида отказа и значение критичности приблизительно равны друг другу. Часто при составлении матрицы критичности применяют следующую шкалу:

* значение критичности 1 или Е. Практически невероятный отказ, вероятность его появления изменяется в интервале: 0 ≤ *Pi* < 0,001;
* значение критичности 2 или D. Редкий отказ, вероятность его появления изменяется в интервале: 0,001 ≤ *Pi* < 0,01;
* значение критичности 3 или С. Возможный отказ, вероятность его появления изменяется в интервале: 0,01 ≤ *Рi* <0,1;
* значение критичности 4 или В. Вероятный отказ, вероятность его появления изменяется в интервале: 0,1 ≤ *Рi* < 0,2;
* значение критичности 5 или А. Частый отказ, вероятность его появления изменяется в интервале: 0,2 ≤ *Рi* < 1.

Вид отказа 1 (рисунок 12) имеет более высокую вероятность появления, чем вид отказа 2, который имеет более высокую тяжесть последствий. Решение о том, какому виду отказа соответствует более высокий приоритет, зависит от вида шкалы, классов тяжести и частоты и используемых принципов ранжирования. Хотя для линейной шкалы вид отказа 1 (как обычно в матрице критичности) должен иметь более высокую критичность (или вероятность появления), чем вид отказа 2, могут быть ситуации, когда тяжесть последствий имеет абсолютный приоритет над частотой. В этом случае вид отказа 2 является более критичным видом отказа.

Только виды отказа, относящиеся к одному уровню системы, можно обоснованно сравнивать в соответствии с матрицей критичности, поскольку виды отказа систем низкой сложности на более низком уровне обычно имеют более низкую частоту. Матрица критичности (рис. 12) может быть использована и качественно, и количественно. Для критичности и тяжести последствий могут использоваться другие обозначения и определения.

**Приоритетность риска RPN**

Интуитивный метод должен сопровождаться ранжированием приоритетности действий, направленных на обеспечение наивысшего уровня безопасности для заказчика. Вид отказа с высоким значением тяжести, низкой интенсивностью появления и очень высоким значением обнаружения (например, значения S, O, D соответственно 2, 3 и 10) может иметь намного более низкий RPN (в приведенном случае 60), чем вид отказа со средними значениями всех перечисленных величин (например, 5 в каждом случае), и, соответственно, RPN = 125. Поэтому часто используют дополнительные процедуры для гарантии того, чтобы видам отказов с высоким рангом тяжести (например, 9 или 10) было придано первостепенное значение и приняты в первую очередь меры по их устранению. В этом случае для принятия более обоснованного решения следует руководствоваться не только RPN, а и рангом тяжести.

Значения RPN, вычисленные в соответствии с таблицами, часто используют для руководства при сокращении видов отказов. Применение анализа на основе RPN требует анализа значений тяжести, появления и обнаружения до формирования заключения и проведения корректирующих мер.

**Оценка приемлемости риска**

Если необходимо построить матрицу критичности, то может быть составлена схема распределения тяжести последствий и частот появления событий. Приемлемость риска определяют субъективно или руководствуются решениями в зависимости от типа системы. В таблице 17 приведены примеры классов приемлемого риска и модифицированной матрицы критичности.

Таблица 17

Матрица риска/критичности

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Частота появления отказа | Уровни тяжести последствий | | | |
| 1 Ничтожный | 2 Минимальный | 3 Критический | 4 Катастрофический |
| 1. Практически невероятный отказ | Незначительные последствия | Незначительные последствия | Терпимые последствия | Терпимые последствия |
| 2. Редкий отказ | Незначительные последствия | Терпимые последствия | Нежелательные последствия | Нежелательные последствия |
| 3. Возможный отказ | Терпимые последствия | Нежелательные последствия | Нежелательные последствия | Неприемлемые последствия |
| 4. Вероятный отказ | Терпимые последствия | Нежелательные последствия | Неприемлемые последствия | Неприемлемые последствия |
| 5. Частый отказ | Нежелательные последствия | Неприемлемые последствия | Неприемлемые последствия | Неприемлемые последствия |

В Приложении В приведен пример блок схемы бизнес-процесса оценки риска невыполнения требований к функционированию системы методом FMEA (FMECA). Блок схема бизнес процесса оценки производственных рисков с использованием методов FMEA (FMECA), дерева неисправностей и дерева событий приведена в Приложении Г. В Приложении Д раскрыт бизнес процесс экспертной оценки производственных рисков методом FMEA, FMECA. Бизнес-процесса экспертной оценки надежности и безопасности методами СФСН, марковских диаграмм, деревьев неисправностей и деревьев событий, методом FMEA (FMECA) приведен в Приложении Е. В Приложении Ж более подробно раскрыт бизнес-процесс экспертной оценки показателей надежности и безопасности методом FMEA (FMECA).

**Рабочие таблицы АВПКО (FMECA), АВПО (FMEA)**

Рабочие таблицы АВПКО (FMECA), АВПО (FMEA) (таблица 18,19) описывают детали анализа в табличной форме.

Таблица 18

Пример рабочей таблицы АВПО (FMEA)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | Последствия отказа | | | Способы и | Рекомендации |  |
| Код элемента (функции) | Наименование элемента (функции) | Вид (описание) отказа | Возможные причины отказа | на рассматриваемом уровне | на вышестоящем уровне | на уровне изделия | средства обнаружения и локализации отказа | по предупреждению (снижению) тяжести последствий отказа | Категория тяжести последствий отказа |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |

Таблица 19

Пример рабочей таблицы АВПКО (FMECA)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | Последствия отказа | | | Способы и | Рекомендации |  |  |
| Код элемента (функции) | Наименование элемента (функции) | Вид (описание) отказа | Возможные причины отказа | на рассматриваемом уровне | на вышестоящем уровне | на уровне изделия | средства обнаружения отказа | по предупреждению (снижению) тяжести последствий отказа | Вероятность отказа | Критичность отказа |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |

# Пример оценки рисков с использованием программных модулей Windchill Quality Solutions

В случае, когда событие FMECA является сложным, т.е. причина появления события является комбинацией причин, соединенных в сложную логическую структуру, применяется анализ методом деревьев неисправностей (FTA). Кроме того возникновение несоответствий или отказов может приводить к целому ряду нежелательных последствий. Развитие последствий может протекать в зависимости от внешних факторов, имеющих случайную природу, поэтому целесообразно обратиться к методике дерева событий (ETA) для подробного анализа всех возможных эффектов (последствий).

Совокупность вышесказанного указывает на возможность реализации комплексной методики оценки рисков с использованием всех обозначенных в этой работе видов анализа. В разделе разбирается прикладная задача комплексного применения методики экспертных оценок в отношении рисков в надежности и безопасности АВПКО (FMЕСА), АВПО (FMEA) с привлечением FTA и ETA.

**Описание задачи**

В задаче рассматривается подсистема, являющаяся частью большой технической системы. В этой подсистеме рассмотрено, как центральное, нежелательное событие/авария/отказ – «объемный пожар в отсеке Х». Оцениваются риски связанные с возникновением этого события. А именно:

- Вероятность возникновения;

- Оценка тяжести последствий в случае возникновения события;

- Возможность анализа этого события для его учета на этапе проектирования и поиска упреждающих проектных решений;

- Выработка последовательности действий при возникновении аварии.

**Решение задачи**

Началом анализа является составление декомпозиции подсистемы, подвергаемой анализу. Следует отметить, что в задаче рассматривается ситуация аварии в определенном помещении и декомпозиция строится по принципу расположения на объекте. Например «Корабль – помещение - деталь».

На высшем уровне декомпозиции технической системы одним из возможных несоответствий или отказов будет несанкционированное возгорание. В соответствии с алгоритмом АВПКО, проводят анализ функций каждого компонента подсистемы, результаты которого сводят в таблицу АВПКО (FMECA). Для одного элемента декомпозиции может быть определено множество видов отказов. В свою очередь для каждого вида отказа может быть установлено несколько видов вызывающих его причин и несколько видов последствий (эффектов). Под действием понимаются меры, которые следует принять в случае возникновения отказа или несоответствия (рис. 13).

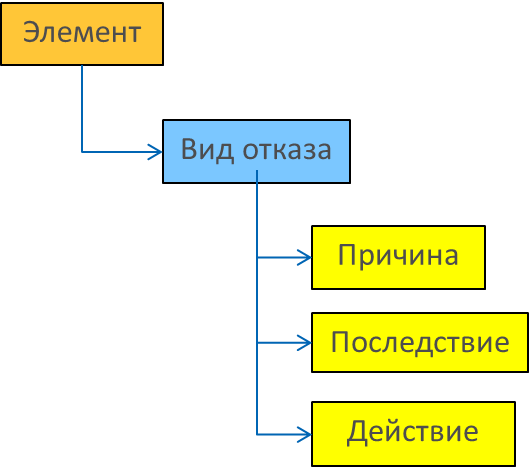
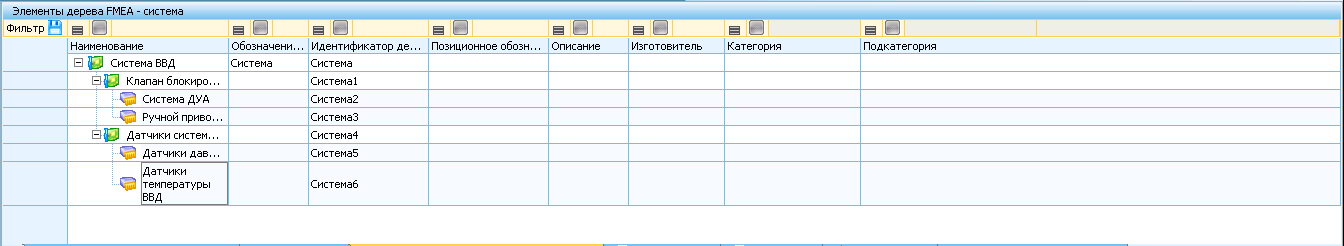


Рис. 13. Свойства элемента декомпозиции системы

**Комплексная оценка рисков в системе WQS**

Ниже представлена реализация комплексной методики оценки рисков поэтапно. Каждый рисунок относится к пункту, обозначенному порядковым номером, внутри которого он находится, поэтому нумерация этих рисунков опускается.

1. Выстраивают древовидную структуру (декомпозицию) анализируемого изделия (системы изделия / отдельного агрегата) в модуле FMEA.



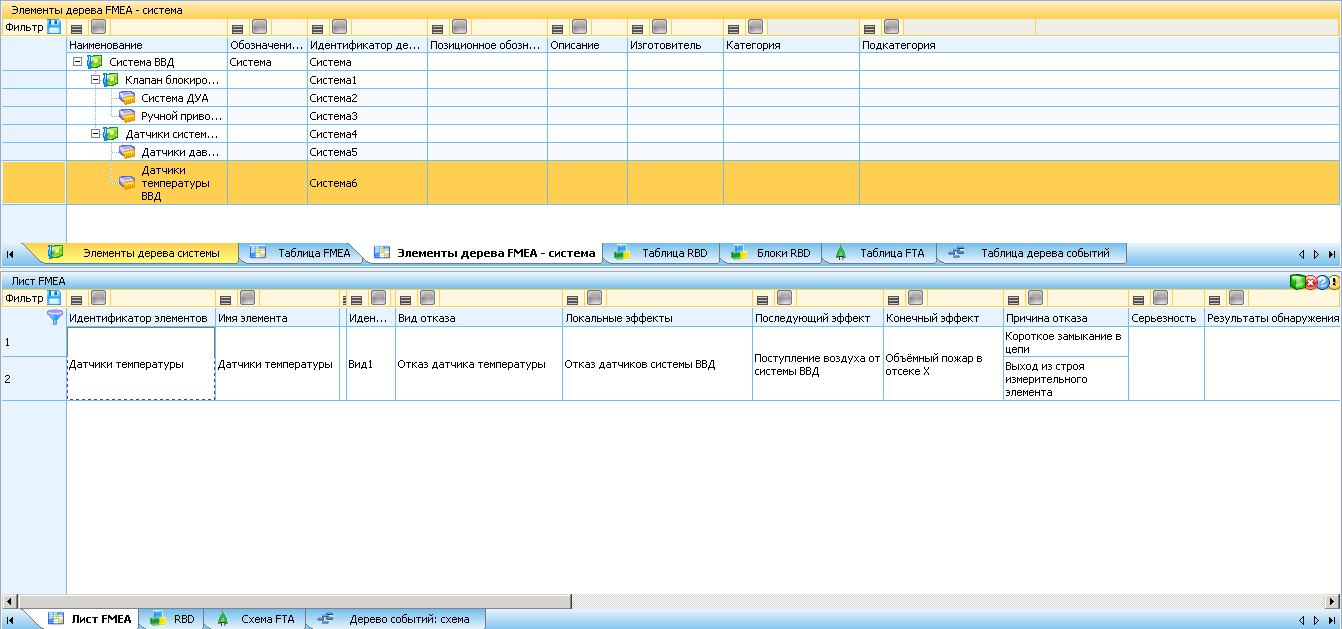
1. Настраивают вид таблицы АВПКО (FMECA), АВПО (FMEA).

Вид таблицы определяется исходя из принятых на предприятии традиций и из соображений рационального хранения информации. У таблицы помимо обязательных для анализа столбцов, обозначенных в табл. 18, могут быть так же дополнительные столбцы со справочной или навигационной информацией.

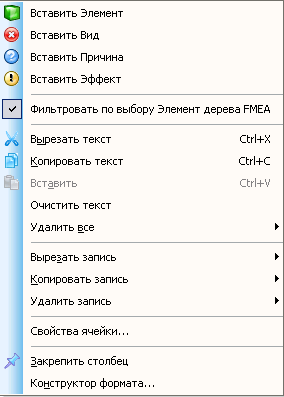
1. Заполняют виды отказов для выбранного элемента структуры изделия.

Для каждого вида отказов заполняют последствия отказов, причины и другие необходимые данные. На данном этапе могут быть обозначены связи причина-последствие для различных уровней, описанные на рисунках 9 и 10.

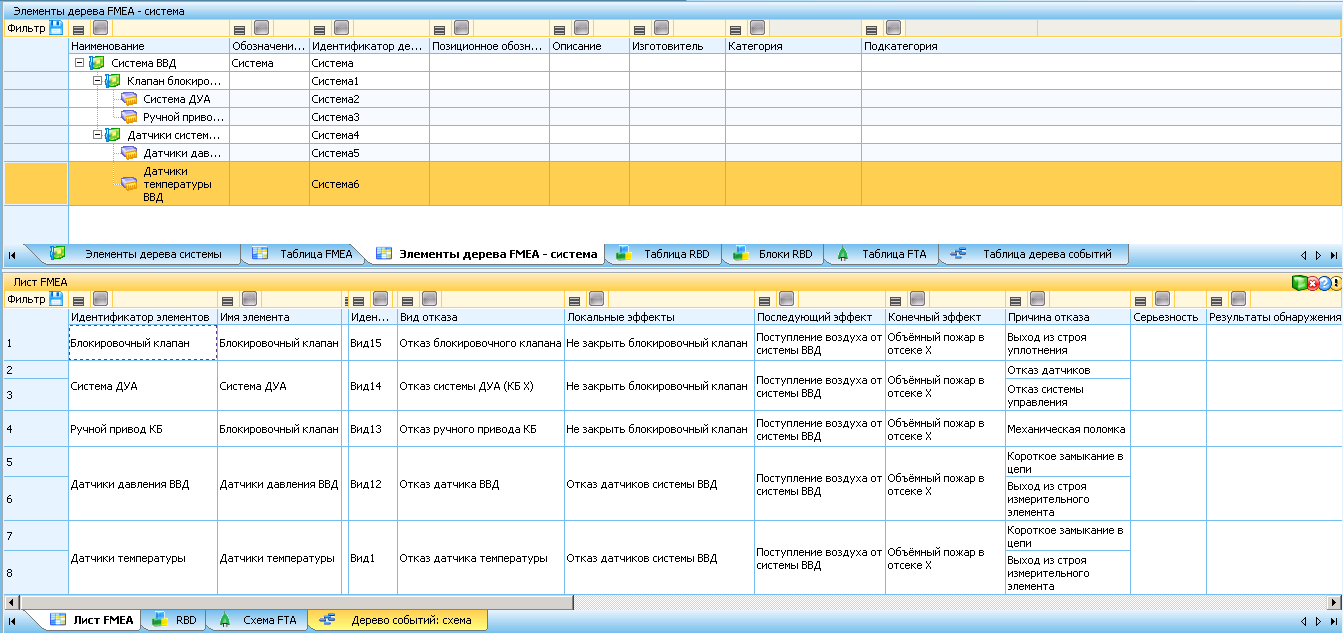
1. Вводят значения весовых коэффициентов критичности, возможности обнаружения и вероятности возникновения каждого вида отказа. Приоритетное число риска вычисляется автоматически. Здесь стоит заметить, что в WQS некоторые весовые коэффициенты вводятся в качественной форме. Для правильного подбора коэффициентов следует обратится в таблицы раздела 4.5.

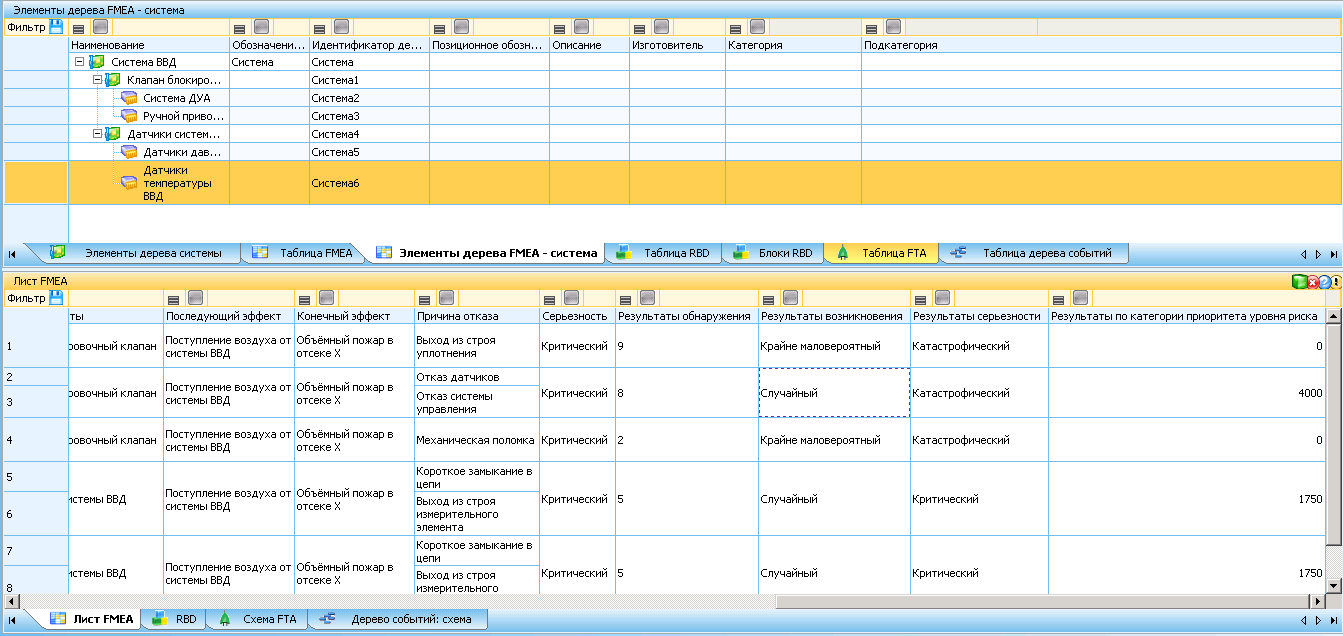


1. При необходимости, выводят виды отказов по всем элементам системы, без деления

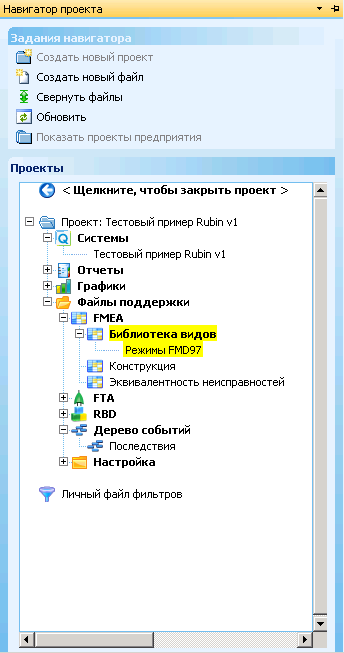


1. Полная база данных проекта WQS АВПКО (FMECA), АВПО (FMEA) для рассматриваемой системы

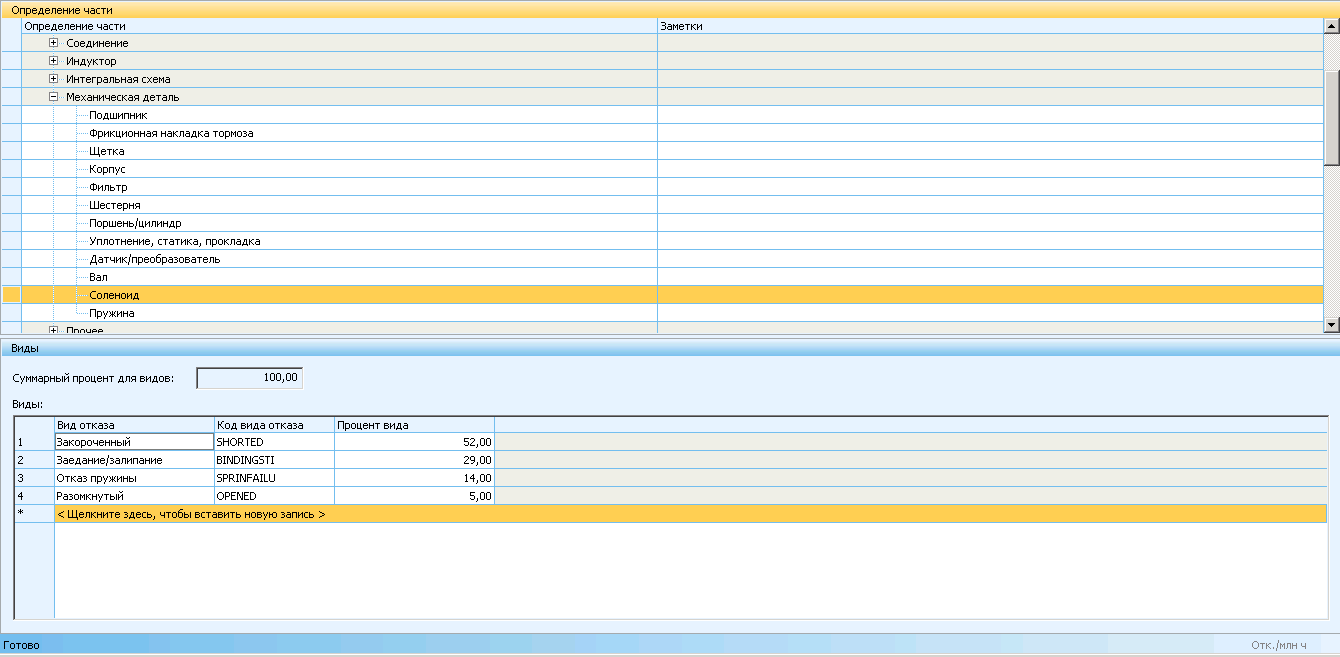




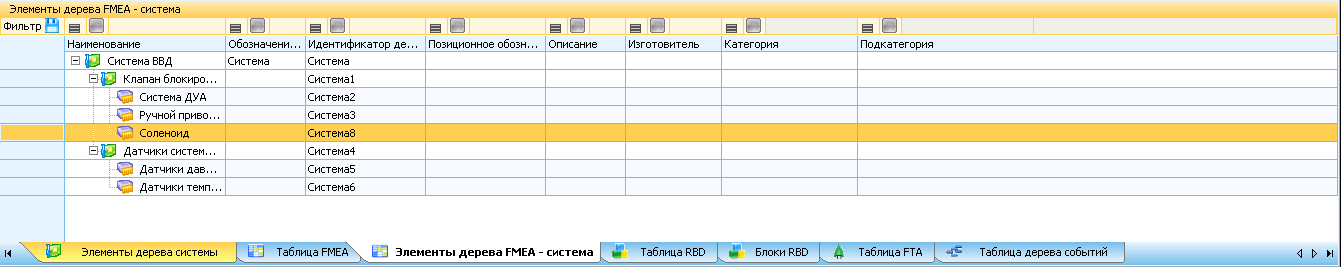
1. При наличии в системе элементов, по которым информация о видах отказов отсутствует (новые типы элементов), можно использовать встроенные базы данных по видам отказов. Виды отказов можно найти в файле поддержки «Режимы FMD97», либо другом файле, в зависимости от выбранного стандарта АВПКО (FMECA), АВПО (FMEA).



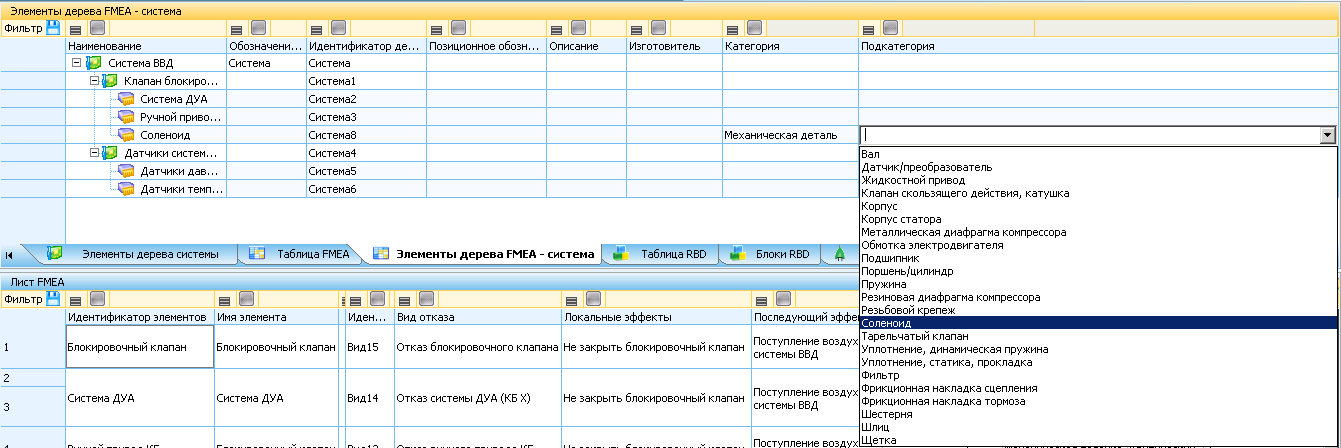
1. В файле отображены виды отказов по классификатору стандартных элементов.



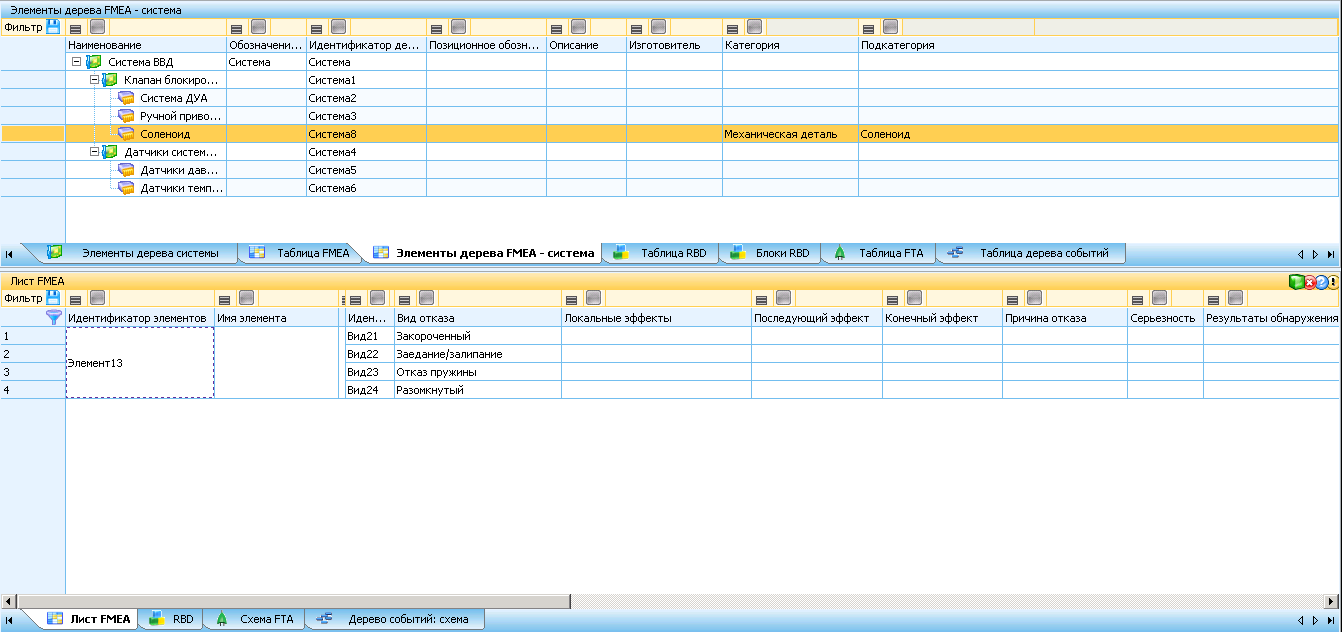
1. Для добавления видов отказов из встроенной базы данных следует выполнить следующие действия:
   1. Добавить новый элемент



* 1. Провести классификацию нового элемента



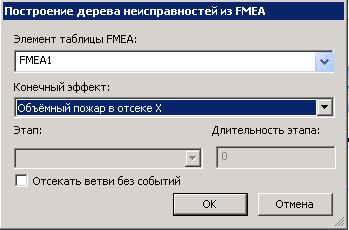
* 1. Стандартные виды отказов будут добавлены автоматически



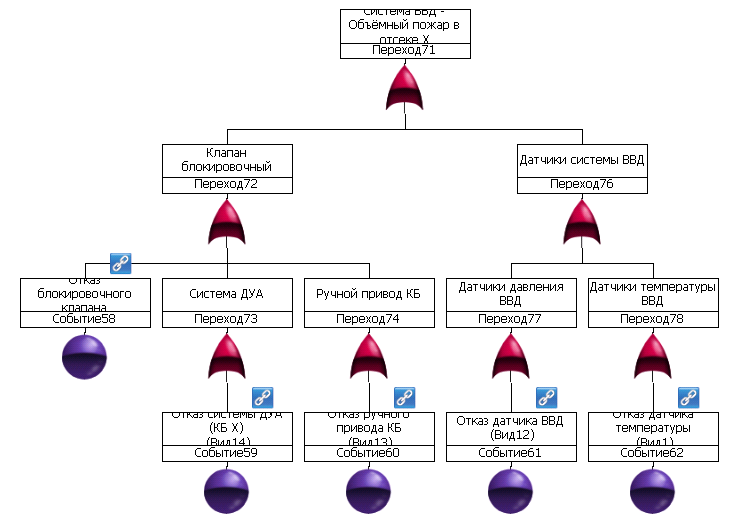
Предварительное построение таблицы АВПКО (FMECA)окончено. Далее данные, полученные по результатам анализа, могут быть использованы для проведения анализа ДО (FTA), и, в дальнейшем, учтены в той же таблице АВПКО (FMECA).

**Оценка методом деревьев неисправностей (FTA) в системе WQS**

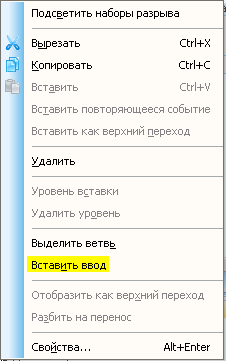
1. По результатам АВПКО (FMECA), АВПО (FMEA) по определённому конечному эффекту отказа строят дерево неисправностей:
   1. Выбирают в меню пункт «Построить дерево неисправностей из FMEA». В открывшемся окне выбирают процесс АВПКО (FMECA), АВПО (FMEA) и конечный эффект, который в итоге станет верхним (конечным) событием дерева неисправностей. При необходимости, можно не учитывать ветви деревьев неисправностей, у которых нет базовых событий (которые в АВПКО (FMECA), АВПО (FMEA) являются видами отказов)

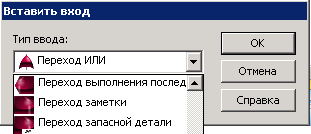


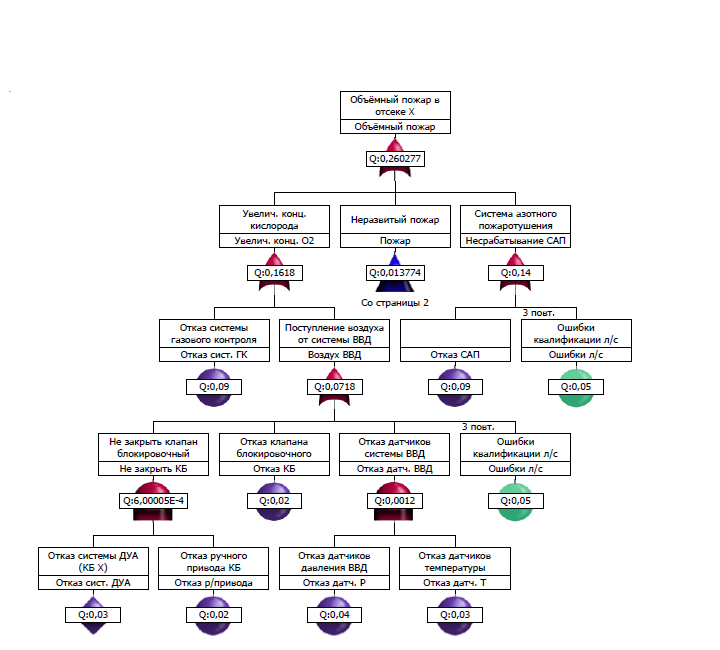
* 1. В результате на основе базы данных АВПКО (FMECA), АВПО (FMEA) выстраивают дерево неисправностей для выбранного конечного эффекта, которое может существовать отдельно, а также входить в иерархию выстраиваемых вручную деревьев неисправностей.

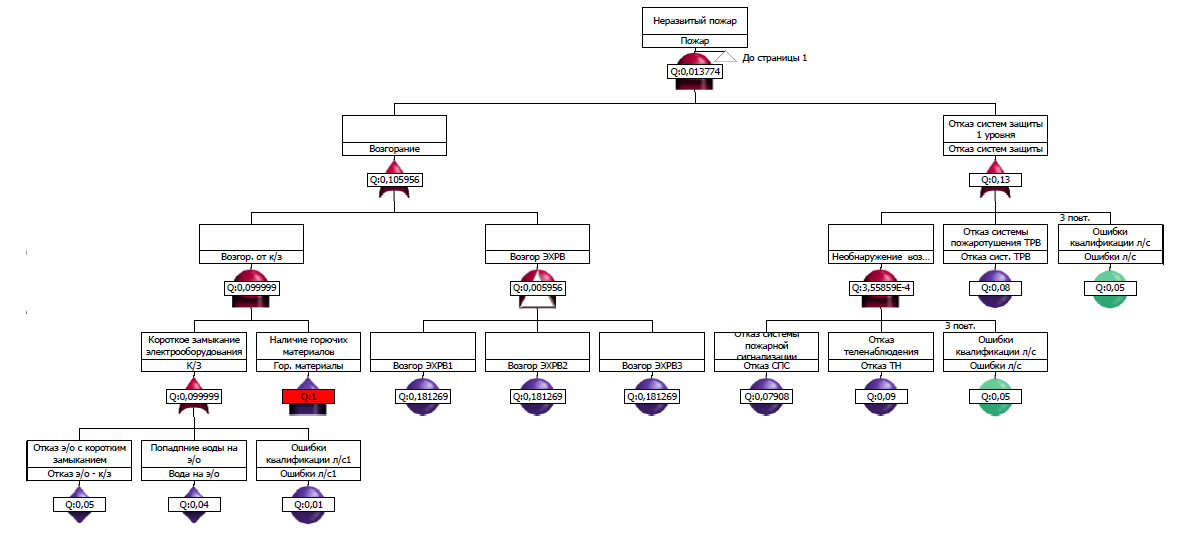


1. Анализ деревьев неисправностей (FTA) в системе WQS.
   1. Построение дерева неисправностей начинают с события верхнего уровня, которое с помощью логических вентилей соединяется с базовыми событиями. При построении можно деревья неисправностей использовать деревья, построенные в процессе АВПКО (FMECA), АВПО (FMEA).

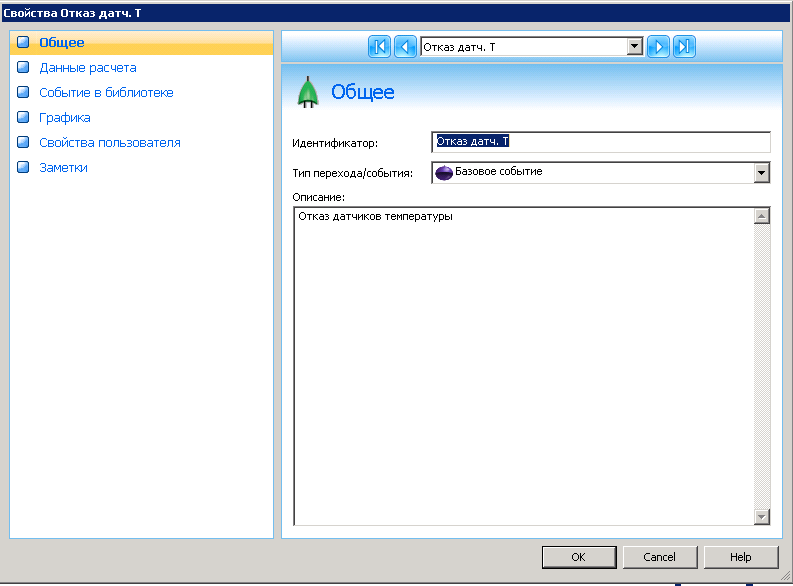


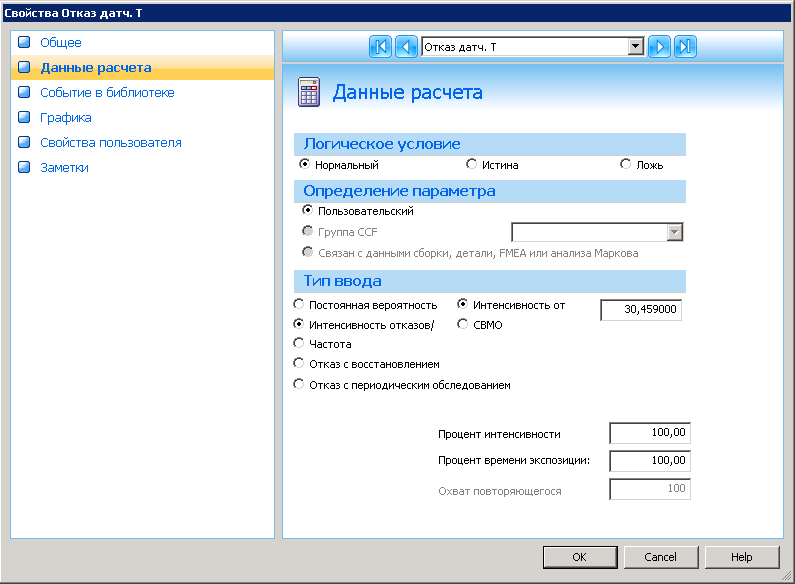




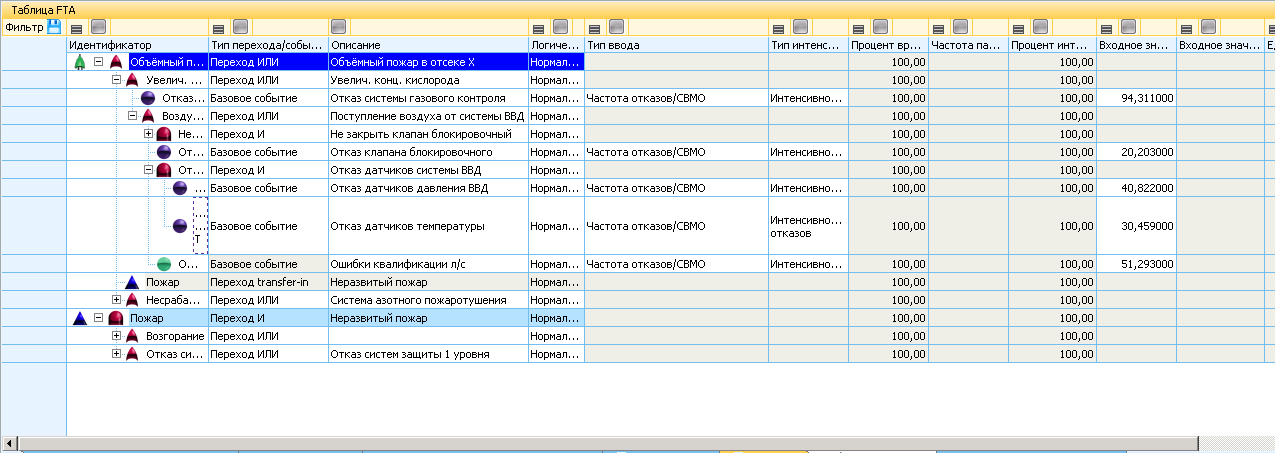


* 1. Для каждого базового события указывают свойства расчёта

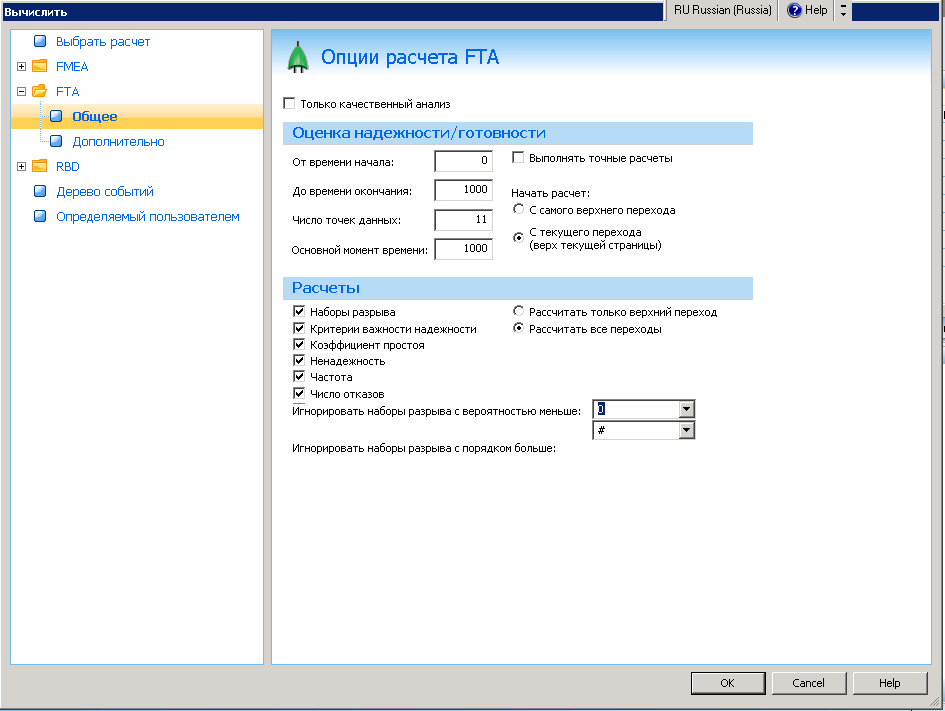


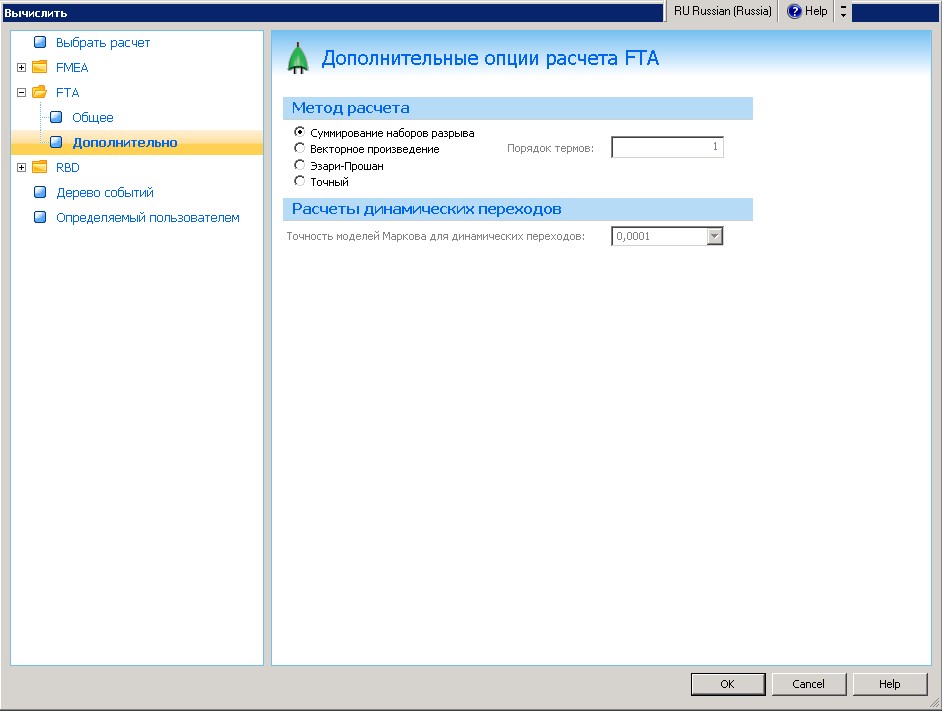


* 1. Графически дерево неисправностей может отображаться в виде в виде диаграммы или в виде таблицы, связанной с структурой.

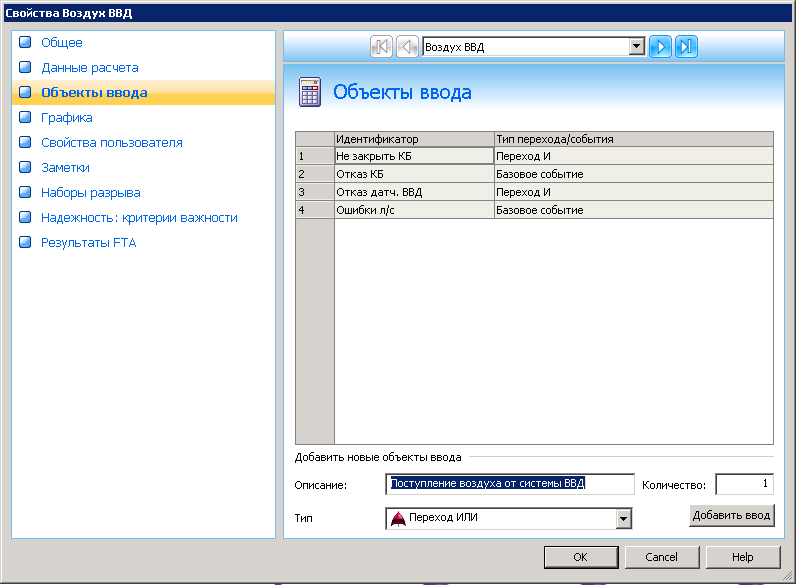


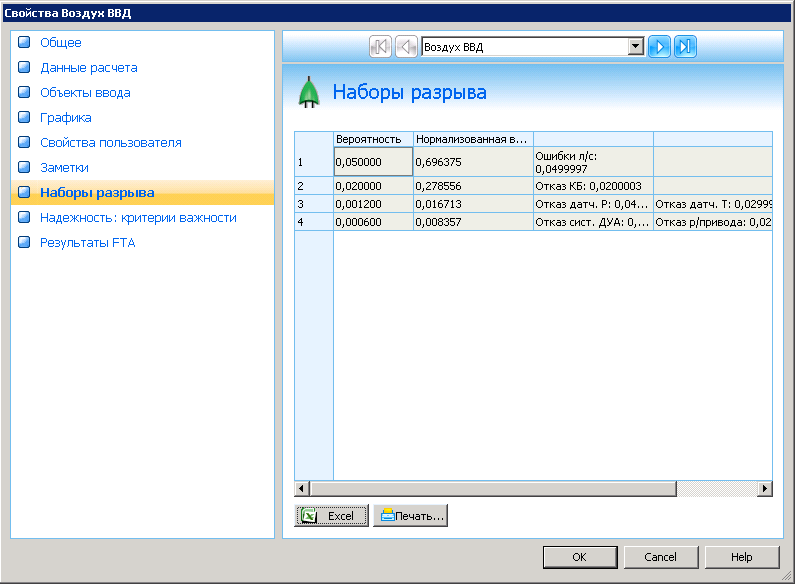
* 1. Проводят расчёт дерева неисправностей. Перед расчётом указывают необходимые опции настройки расчета.

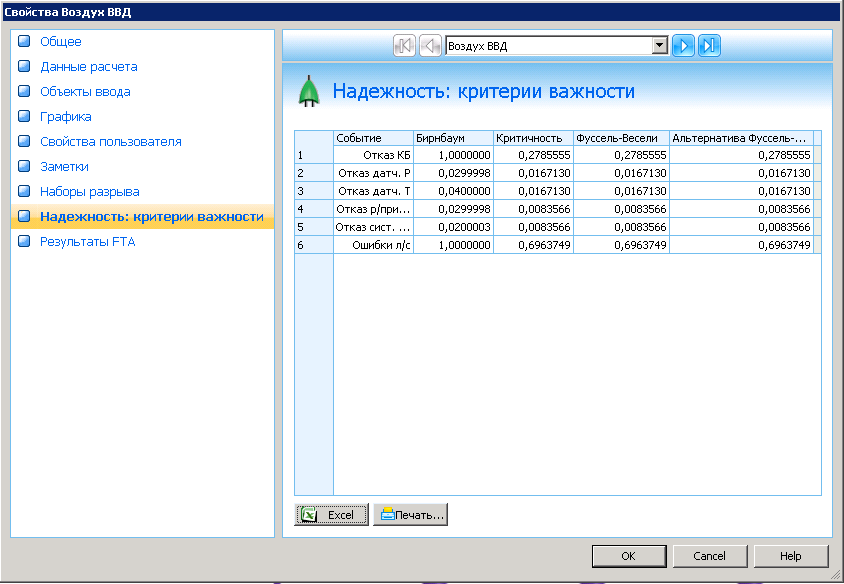


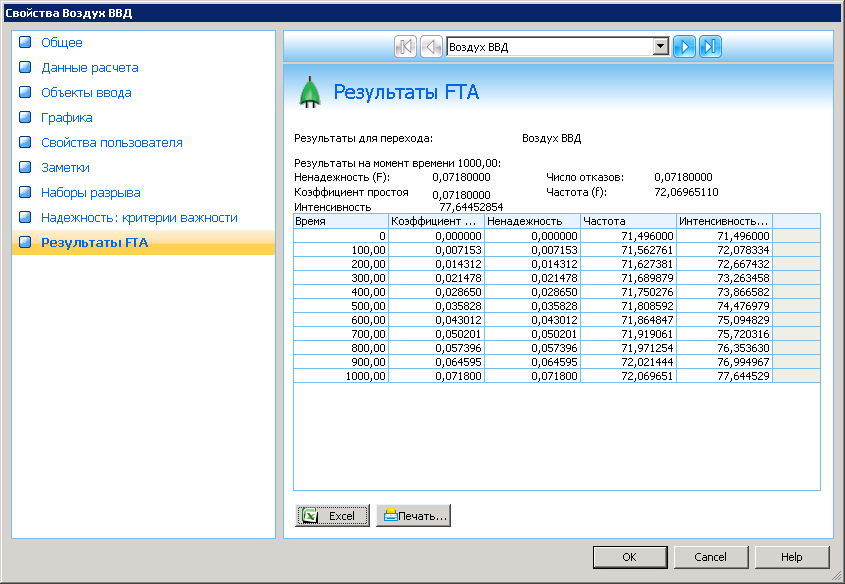


* 1. Результаты расчёта для каждого вентиля дерева неисправностей





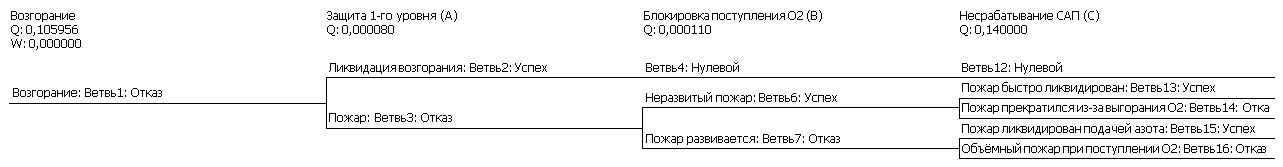




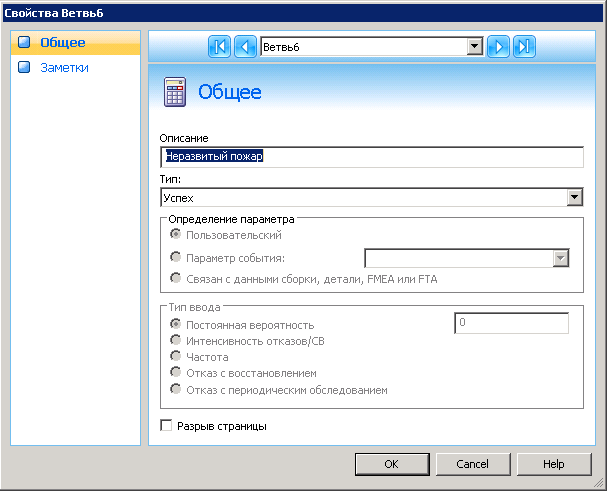
В таблице представлены результаты анализа ДО для базовых событий и связей, описанных в модуле FMEA. Получены оценки вероятностных характеристик возникновения аварии (центрального события). Далее будут оценены характеристики критичности последствий этой аварии методом ДС(ETA)

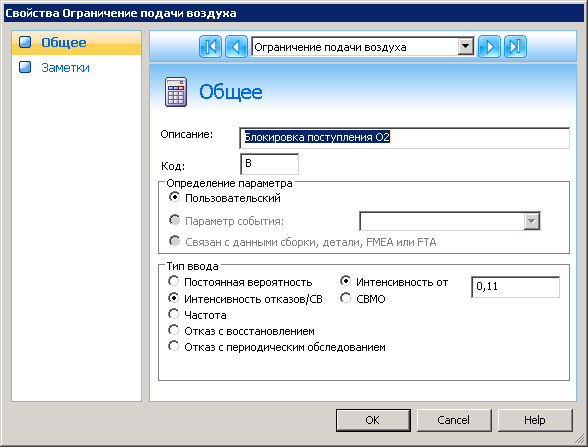
**Оценка методом деревьев событий (ETA) в системе WQS**

1. Устанавливают уровни критичности для конечных событий. Уровень критичности выбирается исходя из ранее установленных бальных оценок уровня критичности для более высокого уровня декомпозиции в АВПКО(FMECA).
2. В качестве исходного события можно использовать вентиль дерева неисправностей. Далее от исходного события начинают выстраивать дерево событий, заканчивая конечными событиями. Оценки вероятности реализации того или иного сценария могут быть так же взяты из таблицы FMEA.

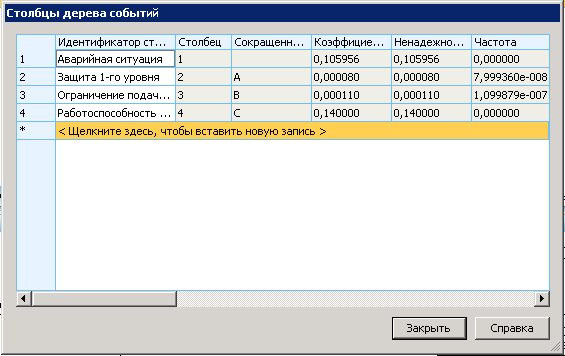


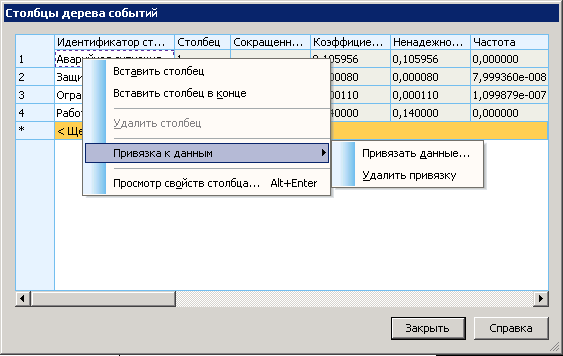
1. Для каждой ветви дерева событий указывают логические свойства и свойства расчёта. Помимо этого, данные ветвей можно привязать к элементам деревьев неисправностей

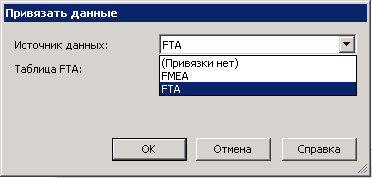




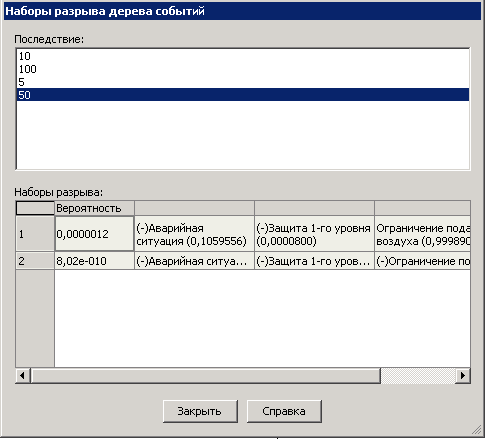
1. Указывают свойства факторов защиты, либо «привязывают» фактор защиты к одному из элементов деревьев неисправностей







1. Проводят расчёт дерева событий. Результаты расчёта по каждому уровню критичности.



**Результаты**

Результатами анализа являются вероятностные характеристики последствий, которые могут иметь место при возникновении центрального события (аварии). Эти характеристики можно использовать как исходные вероятности возникновения причин несоответствий/отказов на более высоких уровнях декомпозиции системы (рисунки 9 и 10). А, так же, для дополнения и коррекции бальных оценок вероятности возникновения и серьезности последствий на текущем уровне декомпозиции.

Для оценки рисков связанных с аварией в этом примере целесообразно обратится к матрице критичности (рисунок 12). Использование этой матрицы позволяет определить наиболее актуальные (с точки зрения соотношения вероятность\*критичность) последствия.

Таким образом, используя описанные в главах 3 и 4 соображения, представляется возможным оценить риски принятия тех или иных проектных решений на этапе эскизного и технического проектирования сложных технических систем.

# Выводы

В отчёте рассмотрены аспекты применения методики АВПКО (FMECA), АВПО (FMEA) при прогнозировании рисков в процессе разработки и проектирования сложных технических систем. Даны рекомендации по применению на различных уровнях декомпозиции технической системы. Методика, изложенная в отчете, позволяет оценить риски возникновения нежелательных событий и их последствий, в том числе, логически сложных, на этапе проектирования с использованием экспертных оценок

Даны определения и раскрыты понятия риска, способов его анализа и оценки, приведены описания алгоритмов применения методики АВПКО (FMECA), АВПО (FMEA), вспомогательные таблицы для оценки коэффициентов, алгоритм применения совмещенной методики оценки рисков. Рассмотрена связь методики АВПКО (FMECA), АВПО (FMEA) с анализом деревьев неисправностей и событий.

# Приложение А. Пример применения метода анализа дерева событий

Допустим, что в ходе выполнения планового осмотра было выявлено, что критической частью системы M, создающей риск аварии, является подсистема N. Анализ начинается с просмотра последовательности возможных событий при отказе элемента подсистемы N, (инициирующего события), вероятность наступления которого равна PA (рисунок Б1), т.е. конечное событие (происшествие) начинается с события A – отказа (разрушения, поломки) элемента подсистемы N.

Далее анализируются возможные варианты развития событий (B, C, D и E), которые могут последовать за разрушением этого элемента. На рисунке Б.1 изображено дерево состояний, отображающее возможные альтернативы развития отказа А. На первой ветви рассматривается состояние системы при разрушении по причине I. Далее подвергается анализу причина II и т.д. При использовании в анализе двоичной системы счисления, т.е. в предположении, что элементы системы либо выполняют свои функции (работоспособны), либо отказывают (неработоспособны), число потенциальных неисправностей равно 2n-1, где n – число элементов подсистемы N. На практике исходное дерево событий можно упростить с помощью инженерной логики и свести к более простому дереву, изображенному в нижней части рисунка Б1.

В первую очередь представляет интерес вопрос о работоспособности подсистемы N. Вопрос заключается в том, какова вероятность PВ отказа этой подсистемы и какое действие ее отказ оказывает на другие подсистемы. Например, если к подсистеме нет подвода энергии, фактически никакие действия, предусмотренные на случай происшествия с использованием этой подсистемы, не могут производиться. В результате упрощенное дерево событий не содержит выбора в случае отсутствия подвода энергии (т.е. управления), и может произойти происшествие, вероятность которого равна PA(PB).

В случае, если отказ в подводе энергии происходит из за повреждения коммуникаций (энергопровода) системы, вероятность PB следует считать как условную вероятность, чтобы учесть эту зависимость. Если подвод энергии обеспечивается, то последующие варианты анализа дерева событий зависят только от состояния подсистемы N. Система защиты подсистемы N может работать или не работать, и ее отказ с вероятностью PC1 ведет к последовательности событий, изображенной на рисунке Б1

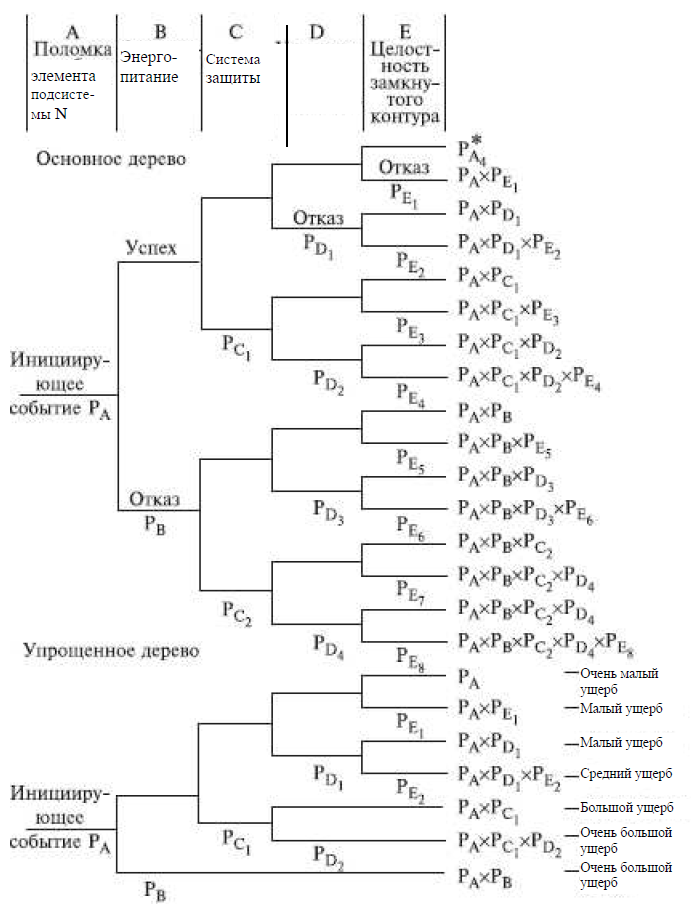


Рисунок А1. Пример применения метода анализа дерева событий

# Приложение Б. Описание логических элементов дерева отказов. Вентили и события

Таблица Б1

Значение логических элементов дерева отказов

| Тип элемента | Значение элемента [13] | Описание элемента | Выражение и таблица истинности (Если A, B ,… - входящие объекты; T - правда; F - ложь) |
| --- | --- | --- | --- |
| Вентили | 1. И | Выходное событие наступает, если наступают все входные события | T=A\*B   |  |  |  | | --- | --- | --- | | A | B | Выходное событие | | T | T | T | | T | F | F | | F | T | F | | F | F | F | |
| 1. ИЛИ | Выходное событие наступает, если наступает любое из входных событий | T=A+B   |  |  |  | | --- | --- | --- | | A | B | Выходное событие | | T | T | T | | T | F | T | | F | T | T | | F | F | F | |
| 1. Исключительное ИЛИ | Событие происходит, если происходит только одно из входных событий (используется обычно с двумя входными событиями) | T=(A\*[~B])+ ( [~A]\*B)   |  |  |  | | --- | --- | --- | | A | B | Выходное событие | | T | T | F | | T | F | T | | F | T | T | | F | F | F | |
| 1. ---- | Если хотя бы одно входное событие не происходит, основное событие происходит | T=~(A\*B)= (~A)+ (~B)   |  |  |  | | --- | --- | --- | | A | B | Выходное событие | | T | T | F | | T | F | T | | F | T | T | | F | F | T | |
| 1. ---- | Если хотя бы одно из входных событий происходит, событие не происходит | T=~(A+B)= (~A)\* (~B)   |  |  |  | | --- | --- | --- | | A | B | Выходное событие | | T | T | F | | T | F | F | | F | T | F | | F | F | T | |
| 1. НЕ | Выходное событие наступает, если не наступает входное событие | T=~A   |  |  | | --- | --- | | A | Выходное событие | | T | F | | F | T | |
| 1. ЗАПРЕТ | Выходное событие наступает, если наступают все входные события, одно из которых условное. Данный вентиль является практически идентичным вентилю И, отличием является обязательное наличие условного входного события. | Для двух входных событий (I1, I2) и одного условного события (C):  T=(I1,I2)\*C   |  |  |  |  | | --- | --- | --- | --- | | A | B | C | Выходное событие | | T | T | T | T | | T | T | F | F | | T | F | T | F | | T | F | F | F | | F | T | T | F | | F | T | F | F | | F | F | T | F | | F | F | F | F | |
| 1. Мажоритарный (Избыточная структура) | Выходное событие наступает, если наступают m или более входных событий из n общего числа | Для трёх событий при условии (2/3): T=(A\*B)+(B\*C)+(C\*A)   |  |  |  |  | | --- | --- | --- | --- | | A | B | C | Выходное событие | | T | T | T | T | | T | T | F | T | | T | F | T | T | | T | F | F | F | | F | T | T | T | | F | T | F | F | | F | F | T | F | | F | F | F | F | |
| 1. И с приоритетом | Выходное событие наступает, если входные события наступают последовательно слева направо | T=A\*B, где A происходит раньше, чем B (в ДН событие A располагается левее, чем событие B)   |  |  |  | | --- | --- | --- | | A | B | Выходное событие | | T(1) | T(2) | T | | T(2) | T(1) | F | | T | F | F | | F | T | F | | F | F | F | |
| 1. Очерёдность | Завершающее событие наступает, если все исходные события наступают поочередно слева направо. Этот вентиль идентичен вентилю И с приоритетом, если число входов вентиля И с приоритетом не менее двух | Все входящие события должны произойти в определённой последовательности (A>B>C) для того, чтобы основное событие произошло.   |  |  |  |  | | --- | --- | --- | --- | | A | B | C | Выходное событие | | F | F | F | F | | F | F | T | Невозможно | | F | T | F | Невозможно | | F | T | T | Невозможно | | T | F | F | F | | T | F | T | Невозможно | | T | T | F | F | | T | T | T | T | |
| 1. Резерв | Завершающее событие наступает, если число запасных компонентов меньше требуемого числа.  Данный вентиль используется как показатель резервирования или запасных частей. Сам вентиль является объектом, а все входные события являются ветвями резервирования или запасными частями. Левая из входящих ветвей является основной, работающей по умолчанию. Остальные входящие ветви являются резервом. При отказе основной ветви, включается в работу первая резервная (расположенная правее). При отказе первой резервной ветви, включается вторая резервная и так далее. При выходе из строя последней резервной ветви, объект считается отказавшим. | Все входящие события должны произойти для того, чтобы основное событие произошло.   |  |  |  | | --- | --- | --- | | A | B | Выходное событие | | T | T | T | | T | F | F | | F | T | F | | F | F | F | |
| 1. Вентиль переноса | Вентиль, указывающий на то, что данная часть системы разрабатывается в другой части страницы или диаграммы | Ссылка на другую часть диаграммы / другую диаграмму |
| События | 1. Базисное событие | Событие самого низкого уровня, для которого имеются данные, касающиеся вероятности его появления |  |
| 1. Условное событие | Событие, которое является результатом появления другого события, при этом для развития завершающего события должны состояться оба события. Условное может быть добавлено только для вентиля запрета. Это дополнительное событие, которое должно произойти для того, чтобы вентиль запрета произошёл для выходного события | См. описание вентиля «ЗАПРЕТ» |
| 1. Неразвитое событие | Первичное событие, относящееся к неразработанной части системы |  |
| 1. Собственное событие | Событие, которое произошло или обязательно произойдет. Вероятность возникновения события равна 1. Также возможно выключение данного события, в этом случае оно станет нулевым и вероятность данного события будет равна 0. |  |
|  | 1. Нулевое событие |  |  |

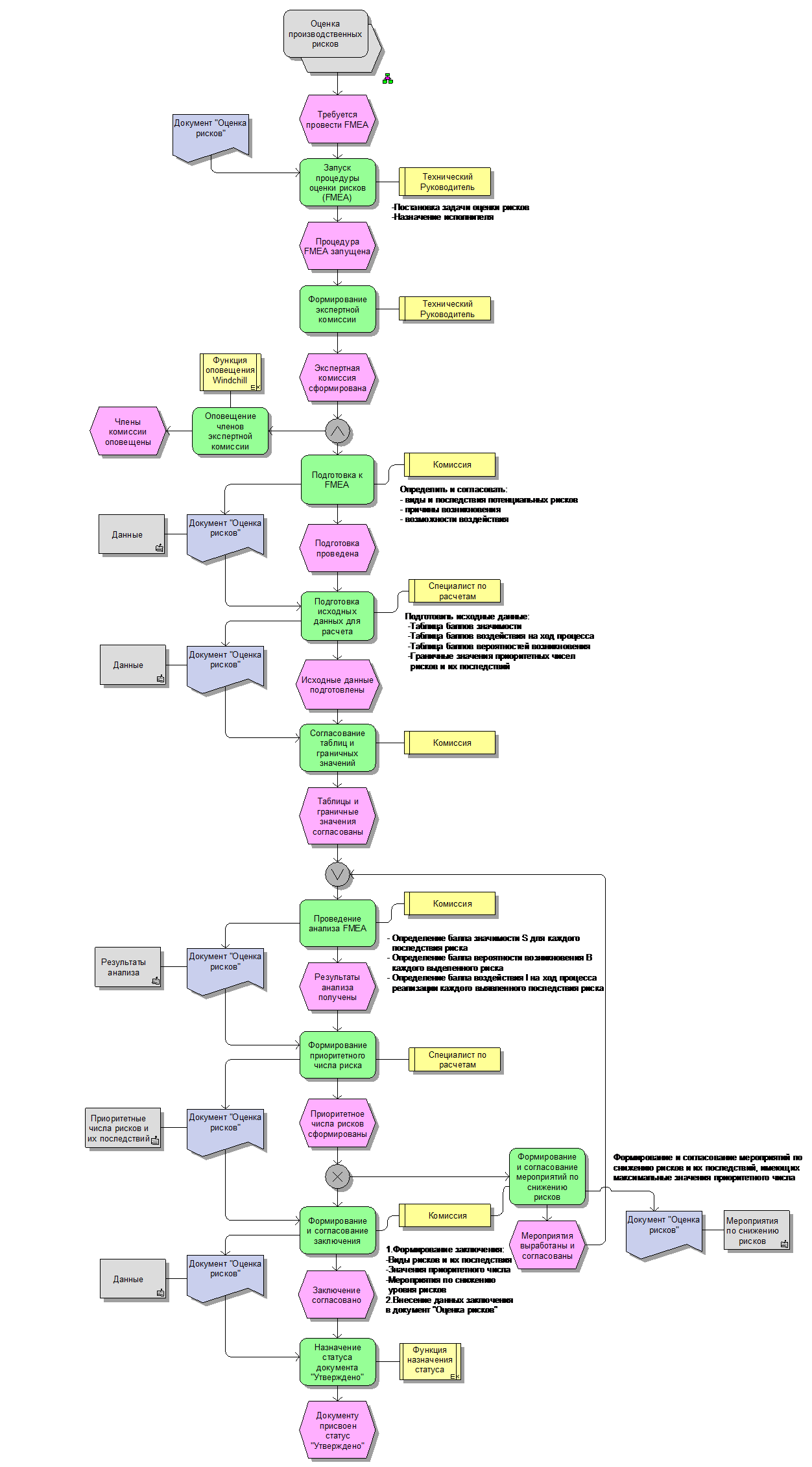
# Приложение В. Блок схема примерного бизнес-процесса оценки риска невыполнения требований к функционированию системы методом FMEA (FMECA)



# Приложение Г. Блок схема примерного бизнес-процесса оценки производственного риска



# Приложение Д. Блок схема примерного бизнес-процесса экспертной оценки производственных рисков (FMEA, FMECA)



# Приложение Е. Блок схема примерного бизнес-процесса экспертной оценки надежности и безопасности



# Приложение Ж. Блок схема примерного бизнес-процесса экспертной оценки показателей надежности и безопасности методом FMEA (FMECA)



# Список литературы

1. ГОСТ Р 51897-2011. Менеджмент риска. Термины и определения.
2. ГОСТ Р 27.002-2009. Надежность в технике. Термины и определения.
3. ГОСТ Р 54869-2011 Проектный менеджмент. Требования к управлению проектом
4. ГОСТ Р ИСО/МЭК 15288-2005 Информационная технология. Системная инженерия. Процессы жизненного цикла систем
5. ГОСТ Р 51901.4-2007 Менеджмент риска. Руководство по применению при проектировании
6. ГОСТ Р 51901.21-2012 Менеджмент риска. Реестр риска. Общие положения
7. ГОСТ Р 51901.22-2012 Менеджмент риска. Реестр риска. Правила построения
8. ГОСТ Р 51901.23-2012 Менеджмент риска. Реестр риска. Руководство по оценке риска опасных событий для включения в реестр риска
9. ГОСТ Р 51901.2-2005 Менеджмент риска. Системы менеджмента надежности
10. ГОСТ Р 51901.3-2007 Менеджмент риска. Руководство по менеджменту надежности
11. ГОСТ Р 51901.5-2007 Менеджмент риска. Руководство по применению методов анализа надежности
12. ГОСТ Р 51901.12-2005 Менеджмент риска. Метод анализа видов и последствий отказов.
13. ГОСТ Р 51901.13-2005 Менеджмент риска. Анализ дерева неисправностей
14. ГОСТ Р 51901.14-2007 Менеджмент риска. Структурная схема надежности и булевы методы.
15. ГОСТ Р 51901.15-2005 Менеджмент риска. Применение марковских методов.
16. ГОСТ Р 51901.16-2005 Менеджмент риска. Повышение надежности. Статистические критерии и методы оценки.
17. ГОСТ Р 51901.6-2007 Менеджмент риска. Программа повышения надежности
18. ГОСТ Р 51901.1-2002 Управление надежностью. Анализ риска технологических систем
19. ГОСТ Р 51901.11-2005 Менеджмент риска. Исследование опасности и работоспособности. Прикладное руководство.
20. ГОСТ Р ИСО 31000-2009 Менеджмент риска. Принципы и руководство.
21. ГОСТ Р ИСО/МЭК 31010-2011 Менеджмент риска. Методы оценки риска.
22. Кузьмин Е.А. Неопределенность в экономике: понятия и положения. Научно-информационный журнал «Вопросы управления». №4(21), декабрь 2012
23. Надежность технических систем и техногенный риск. Под ред. М.И.Фалеева, Москва, ДЭ, 2002
24. А.Н.Бычкова, Г.А.Рудаковская, Анализ характера и последствий отказов, Лекция, Пенза ПГУ, каф. МСК, 2004
25. ГОСТ 27.310-1995 Надежность в технике. Анализ видов, последствий и критичности отказов. Основные положения
26. ГОСТ P 27.302-2009 Надежность в технике. Анализ дерева неисправностей
27. ГОСТ Р МЭК 62502-2014. Менеджмент риска. Анализ дерева событий
28. Методические рекомендации по применению модуля WQS «Prediction» для прогнозирования надежности. 2015