

Методы оценки риска

**ГОСТ Р ИСО/МЭК 31010-2011. Менеджмент риска.
Методы оценки риска**

Оценка риска обеспечивает:

- понимание потенциальных опасностей и воздействия их последствий на достижение установленных целей организации;
- получение информации, необходимой для принятия решений;
- понимание опасности и ее источников;
- идентификацию ключевых факторов, формирующих риск, уязвимых мест организации и ее систем;
- возможность сравнения риска с риском альтернативных организаций, технологий, методов и процессов;

- обмен информацией о риске и неопределенностях;
- информацию, необходимую для ранжирования риска;
- предотвращение новых инцидентов на основе исследования последствий произошедших инцидентов;
- выбор способов обработки риска;
- соответствие правовым и обязательным требованиям;
- получение информации, необходимой для обоснованного решения о принятии риска в соответствии с установленными критериями;
- оценку риска на всех стадиях жизненного цикла продукции.

Таблица 1 - Характеристика применимости методов оценки риска
(SA – строго применим, A – применим, NA – не применим)

[Наименование метода]	Процесс оценки риска				
	Идентификация риска	Анализ риска			Сравнительная оценка риска
		Последствие	Вероятностные характеристики	Уровень риска	
Мозговой штурм	SA	NA	NA	NA	NA
Структурированные или частично структурированные интервью	SA	NA	NA	NA	NA
Метод Дельфи	SA	NA	NA	NA	NA
Контрольные листы	SA	NA	NA	NA	NA
Предварительный анализ опасностей (PHA)	SA	NA	NA	NA	NA
Исследование опасности и работоспособности (HAZOP)	SA	SA	A	A	A
Анализ опасности и критических контрольных точек (HACCP)	SA	SA	NA	NA	SA
Оценка токсикологического риска	SA	SA	SA	SA	SA
Структурированный анализ сценариев методом «что, если?» (SWIFT)	SA	SA	SA	SA	SA
Анализ сценариев	SA	SA	A	A	A

Анализ воздействия на бизнес (BIA)	A	SA	A	A	A
Анализ первопричины (RCA)	NA	SA	SA	SA	SA
Анализ видов и последствий отказов (FMEA)	SA	SA	SA	SA	SA
Анализ дерева несправностей (FTA)	A	NA	SA	A	A
Анализ дерева событий (ETA)	A	SA	A	A	NA
Анализ причин и последствий	A	SA	SA	A	A
Причинно-следственный анализ	SA	SA	NA	NA	NA
Анализ уровней защиты (LOPA)	A	SA	A	A	NA
Анализ дерева решений	NA	SA	SA	A	A
Анализ влияния человеческого фактора (HRA)	SA	SA	SA	SA	A
Анализ «галстук-бабочка»	NA	A	SA	SA	A
Техническое обслуживание, направленное на обеспечение надежности	SA	SA	SA	SA	SA
Анализ скрытых дефек-	A	NA	NA	NA	NA

тов (SA)					
Марковский анализ	A	SA	NA	NA	NA
Моделирование методом Монте-Карло	NA	NA	NA	NA	SA
Байесовский анализ и сети Байеса	NA	SA	NA	NA	SA
Кривые FN	A	SA	SA	A	SA
Индексы риска	A	SA	SA	A	SA
Матрица последствий и вероятностей	SA	SA	SA	SA	A
Анализ эффективности затрат (CBA)	A	SA	A	A	A
Мультикритериальный анализ решений (MCDA)	A	SA	A	SA	A

1. Анализ видов и последствий отказов и анализ видов, последствий и критичности отказов

Анализ видов и последствий отказов (**FMEA** - Failure Mode Effect Analysis)) является методом, используемым для идентификации способов отказа **компонентов, систем или процессов**, которые могут привести к невыполнению их назначенной функции.

Расширенной версией метода **FMEA** является **FMECA**, позволяющий оценить критичность и значимость каждого идентифицированного вида отказа.

Критичность отказа - это совокупность признаков, характеризующих последствия отказа.

2. Анализ дерева неисправностей

Анализ дерева неисправностей (**FTA**- Fault Tree Analysis) - метод идентификации и анализа факторов, которые могут способствовать возникновению исследуемого нежелательного события (называемого конечным событием).

Символы



Логический элемент «И» – отказ произойдет, если все события на входе истинны



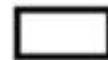
Логический элемент «ИЛИ» – отказ произойдет, если любое из событий на входе истинно



Базовое событие – дальнейший анализ нецелесообразен



Событие далее не анализируют



Событие подлежит дальнейшему анализу



Анализ события приведен на другой странице или в другом месте



Пример метода "Анализ дерева неисправностей"

3. Анализ дерева событий

Метод (**ETA**-Event Tree Analysis) является графическим методом представления взаимоисключающих последовательностей событий, следующих за появлением исходного события, в соответствии с функционированием и нефункционированием систем, разработанных для смягчения последствий опасного события

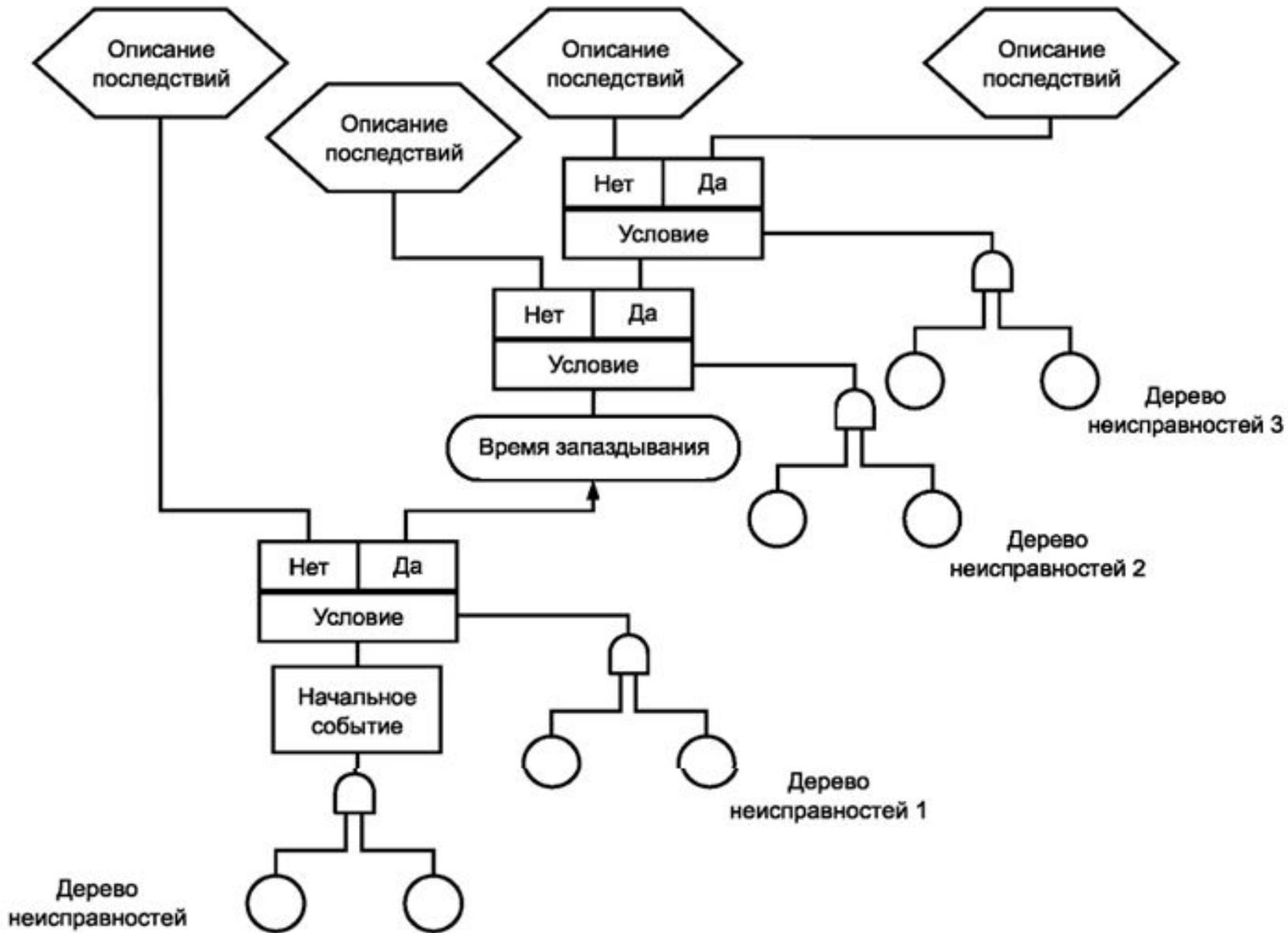


Пример метода "Анализ дерева событий"

4. Анализ причин и последствий

Анализ причин и последствий является сочетанием методов дерева неисправностей и дерева событий.

Данный метод начинают с рассмотрения критического события и анализа его последствий посредством применения сочетания логических элементов ДА/НЕТ.



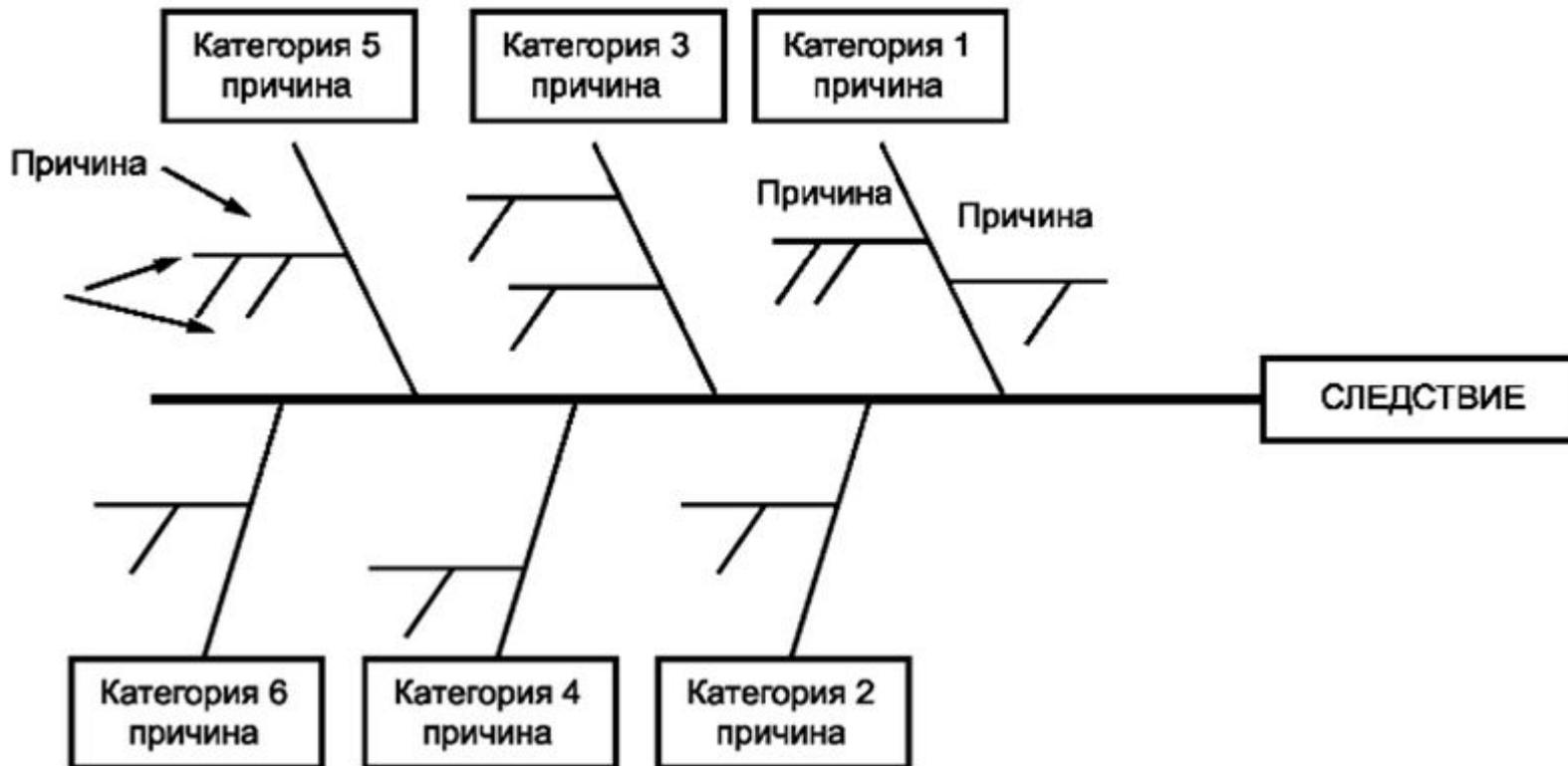
Пример анализа причин и последствий

5. Причинно-следственный анализ

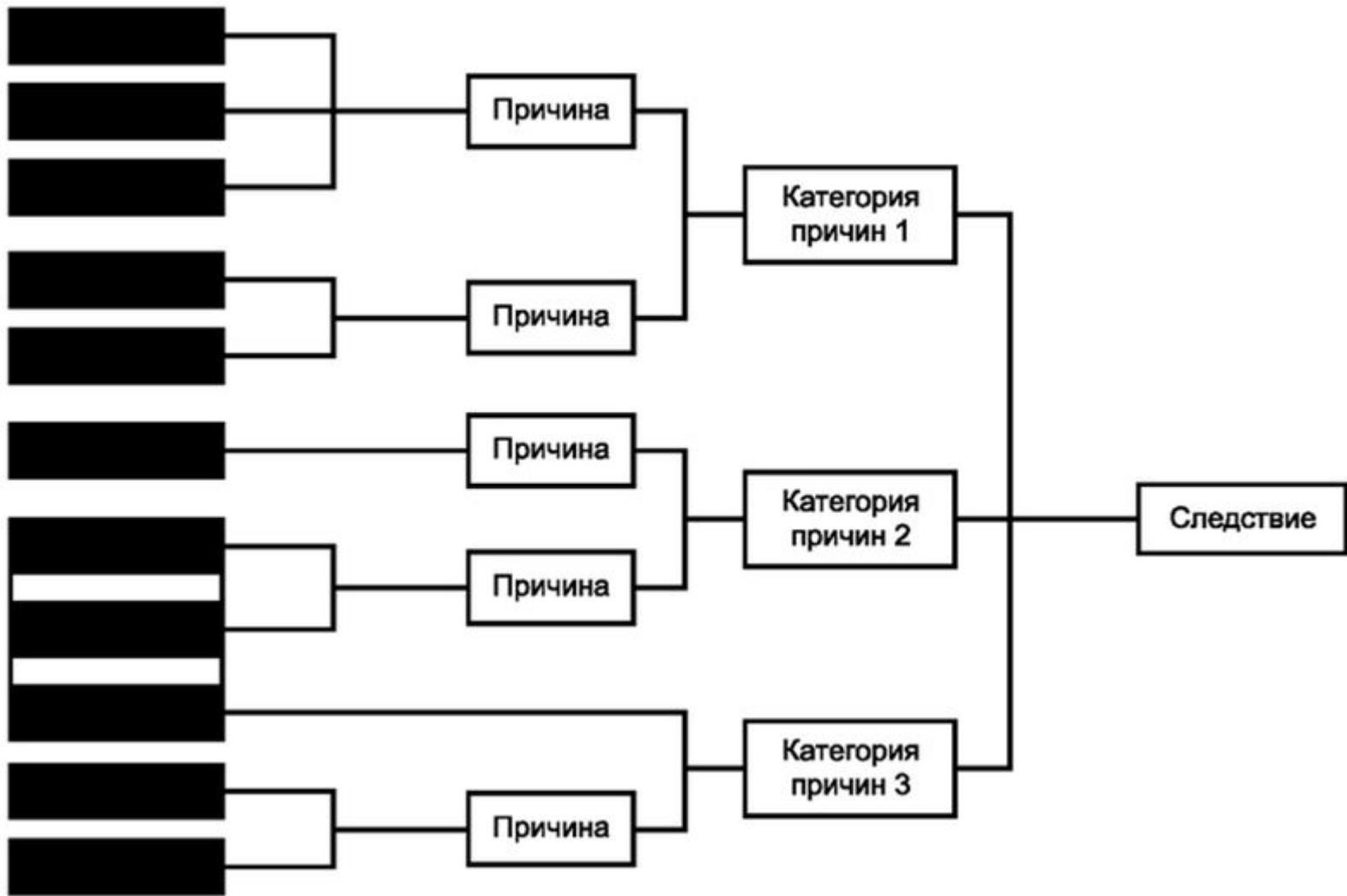
Причинно-следственный анализ является структурированным методом идентификации возможных причин нежелательного события или проблемы.

Данный метод позволяет скомпоновать возможные причинные факторы в обобщенные категории так, чтобы можно было исследовать все возможные гипотезы.

Информацию представляют в виде диаграммы «рыбьего скелета» (метод также называют диаграммой Исикавы) или в виде древовидной схемы.



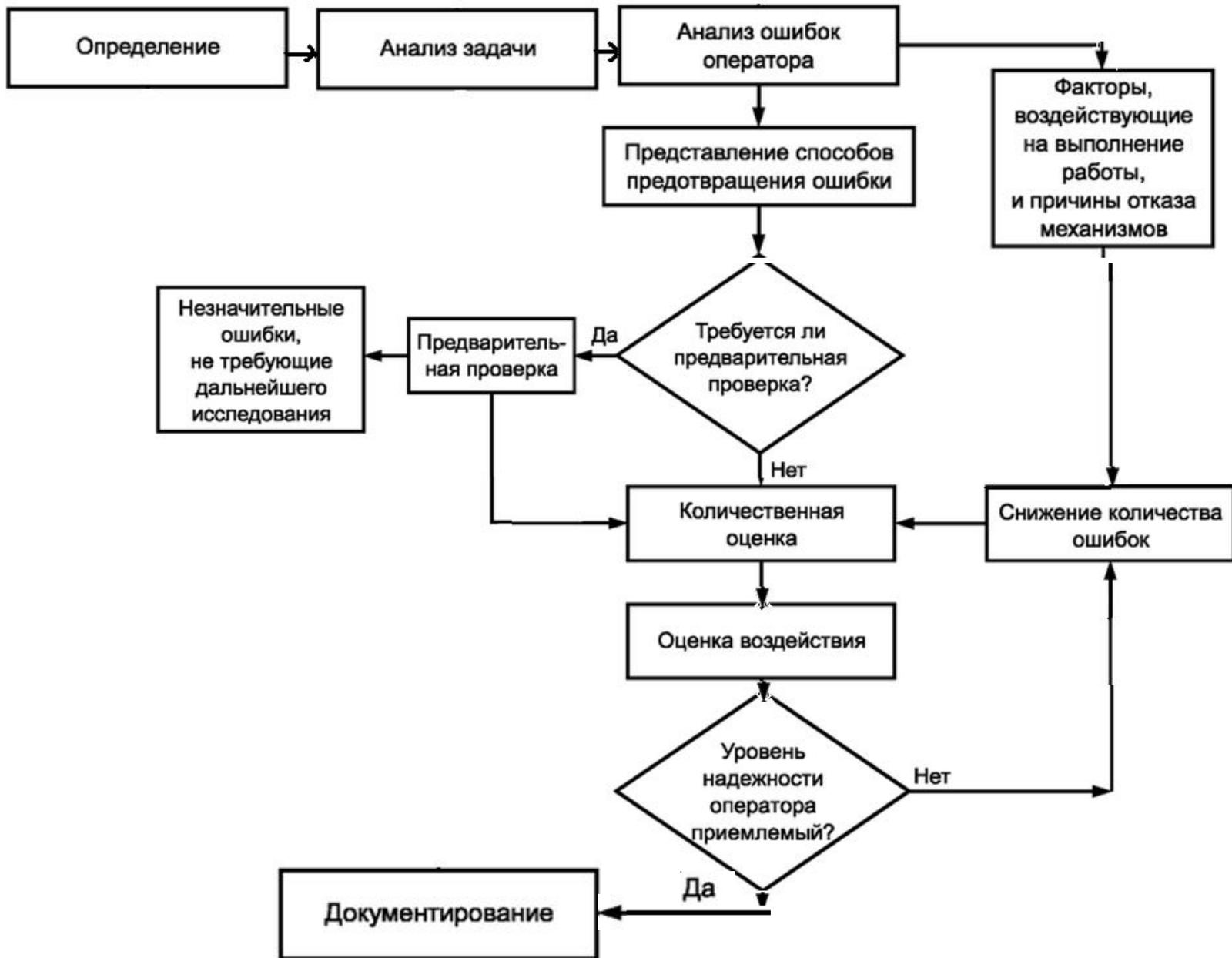
Пример диаграммы Исикавы, или «рыбьего скелета»



Пример представления причинно-следственного анализа в виде древовидной структуры

6. Анализ влияния человеческого фактора

Метод (HRA - Human Reliability Assessment) применяют для оценки влияния действий человека, в том числе ошибок оператора, на работу системы.



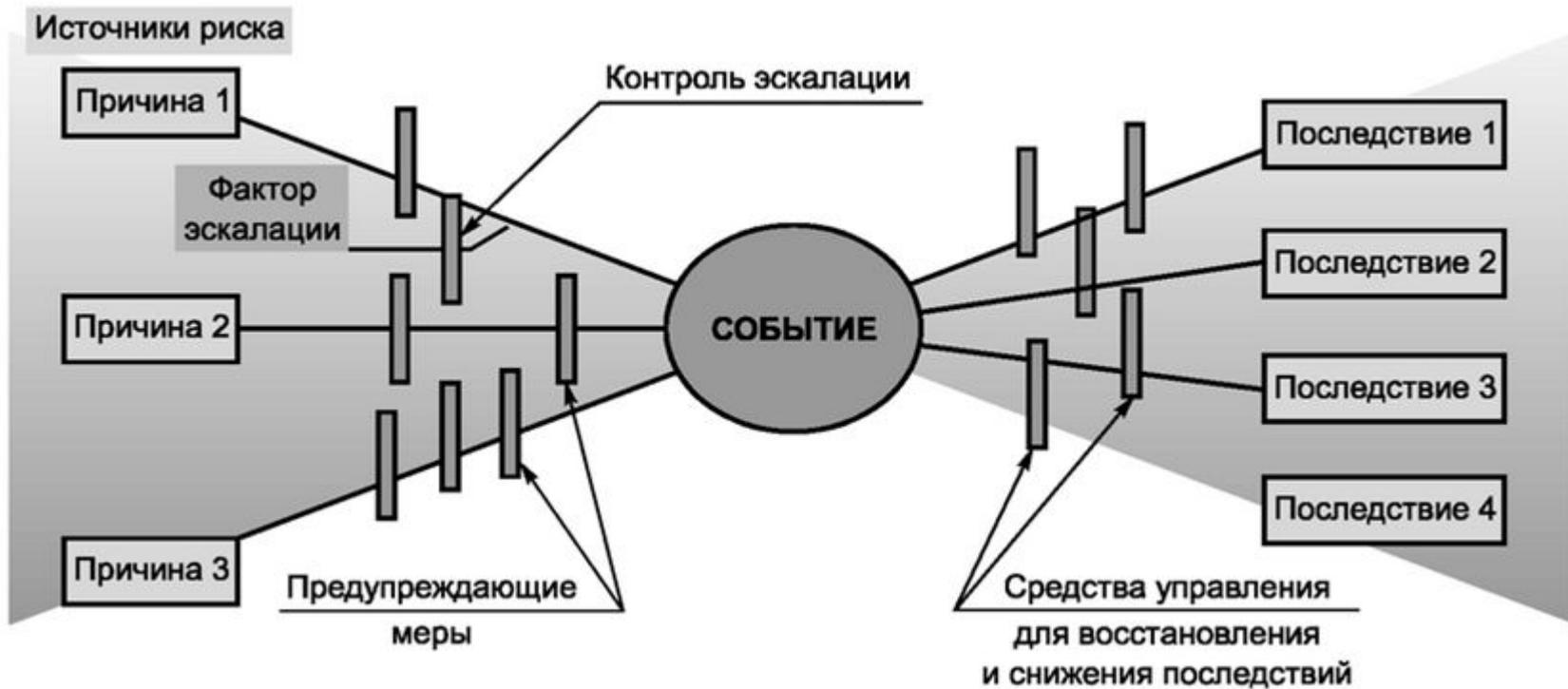
Пример анализа влияния человеческого фактора

7. Анализ «галстук-бабочка»

Анализ «галстук-бабочка» представляет собой схематический способ описания и анализа пути развития опасного события от причин до последствий.

Метод сочетает исследование причин события с помощью дерева неисправностей и анализ последствий с помощью дерева событий.

Основное внимание метода «галстук-бабочка» сфокусировано на барьерах между причинами и опасными событиями и опасными событиями и последствиями.



Пример диаграммы