

---

# Методы менеджмента рисков

---

# **FMEA**

## **(Failure Modes and Effects Analysis)**

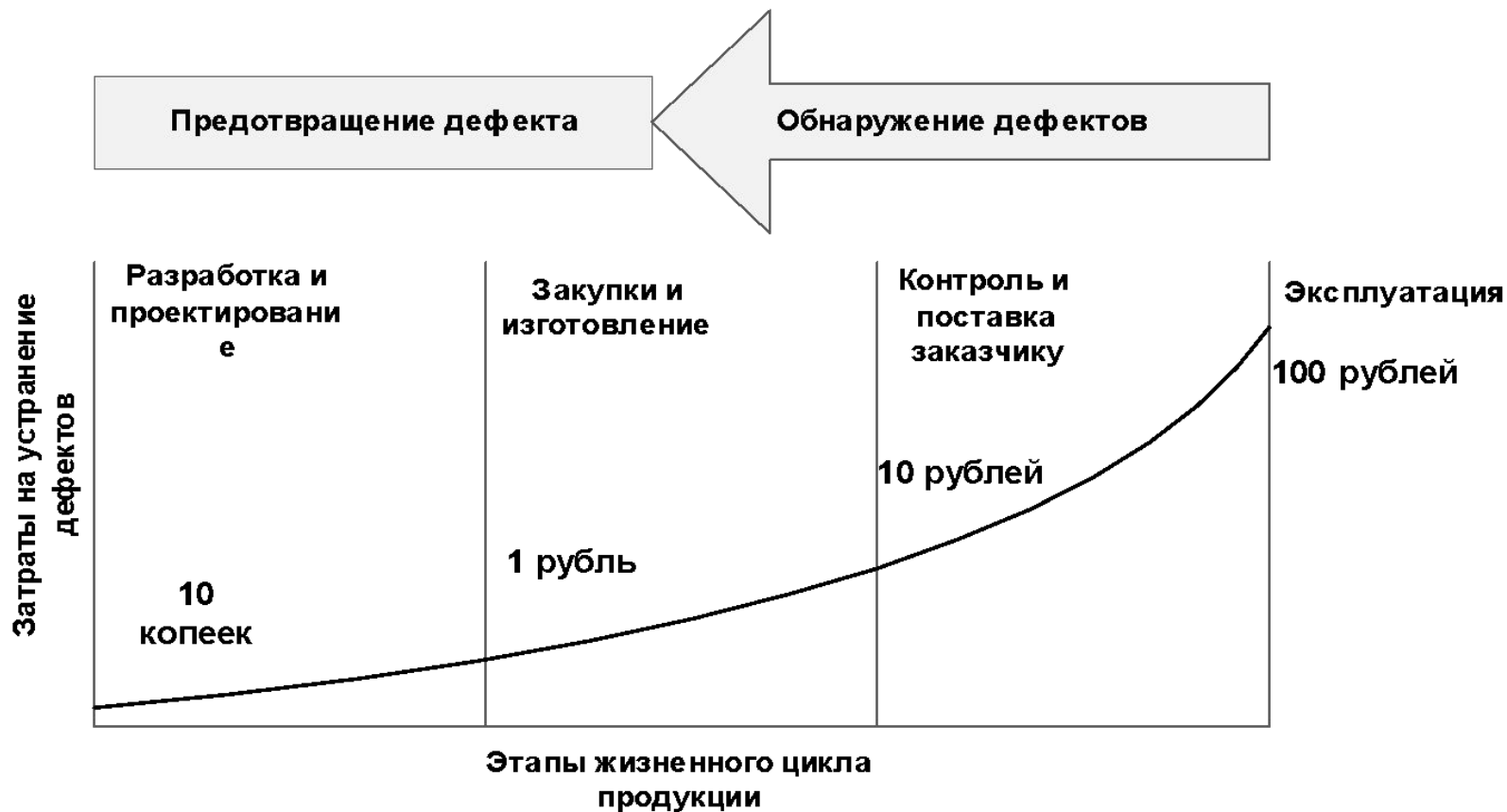
**Анализ видов и последствий  
потенциальных отказов**

---

**FMEA - Формализованная процедура анализа и доработки проектируемого технического объекта, процесса изготовления, правил эксплуатации и хранения, системы технического обслуживания и ремонта данного технического объекта, основанная на выделении возможных (наблюдаемых) дефектов разного вида с их последствиями и причинно-следственными связями, обуславливающими их возникновение, и оценках критичности этих дефектов.**

**FMEA является методом систематического анализа системы для идентификации видов потенциальных отказов, их причин и последствий, а также влияния отказов на функционирование системы**

# Правило десятикратного увеличения затрат



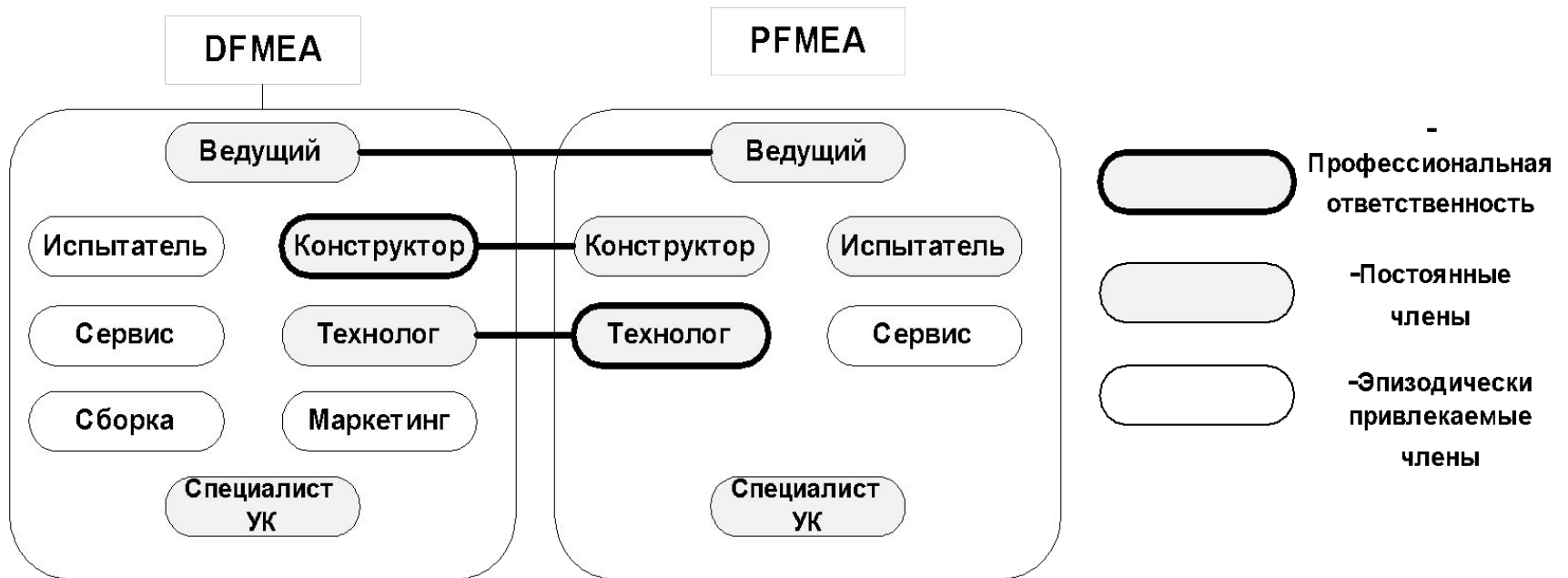
# Виды FMEA

---

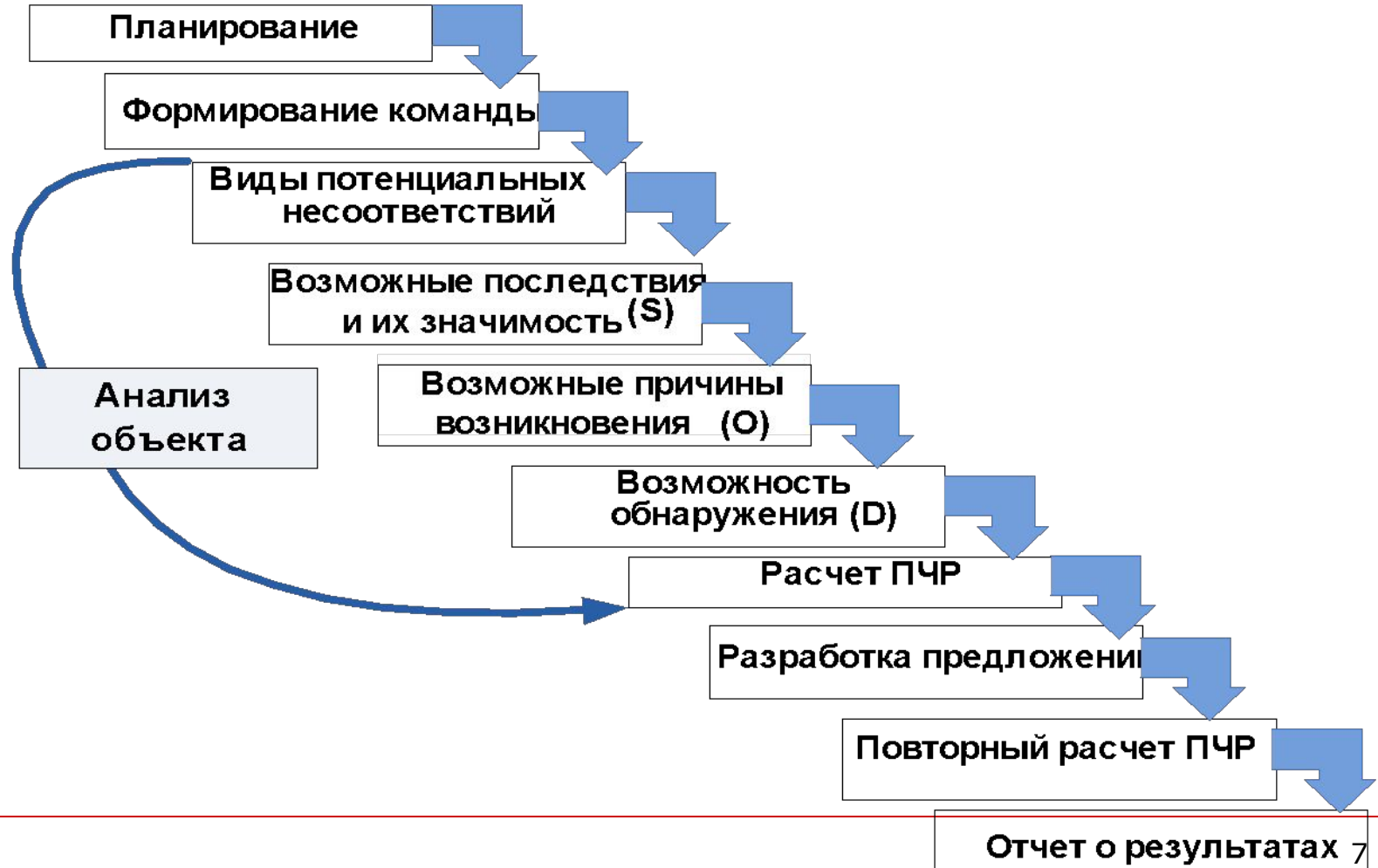
**FMEA анализ бывает трех видов:**

- 1) Общий FMEA;**
- 2) FMEA конструкции (DFMEA - design FMEA);**
- 3) FMEA процесса (PFMEA - process FMEA).**

# Примерные составы FMEA - команд

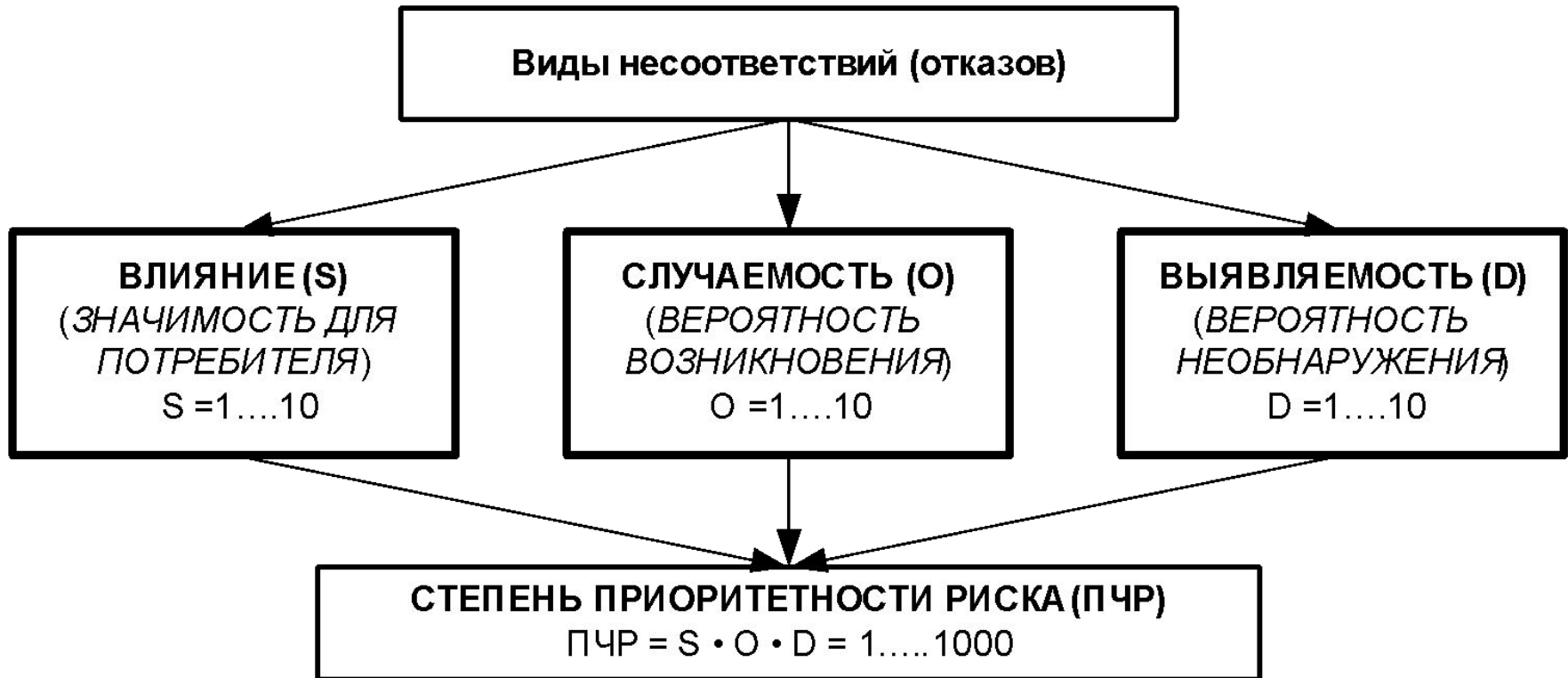


# Алгоритм проведения FMEA-анализа



# Общая методология FMEA – анализа

---





# Бланк FMEA

Изделие, процесс, функция	Вид потенциального несоответствия	Последствие потенциального несоответствия	S	Потенциальная причина несоответствия	O	Действующие меры контроля	D	ПЧР	Рекомендуемое действие	Ответственность, сроки	Результаты				
											Предпринятые действия	O	S	D	ПЧР
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
			7		5		6	210				7	5	1	35

ПЧР  
допуст.-125

Установить  
ПО

Петров В.С.

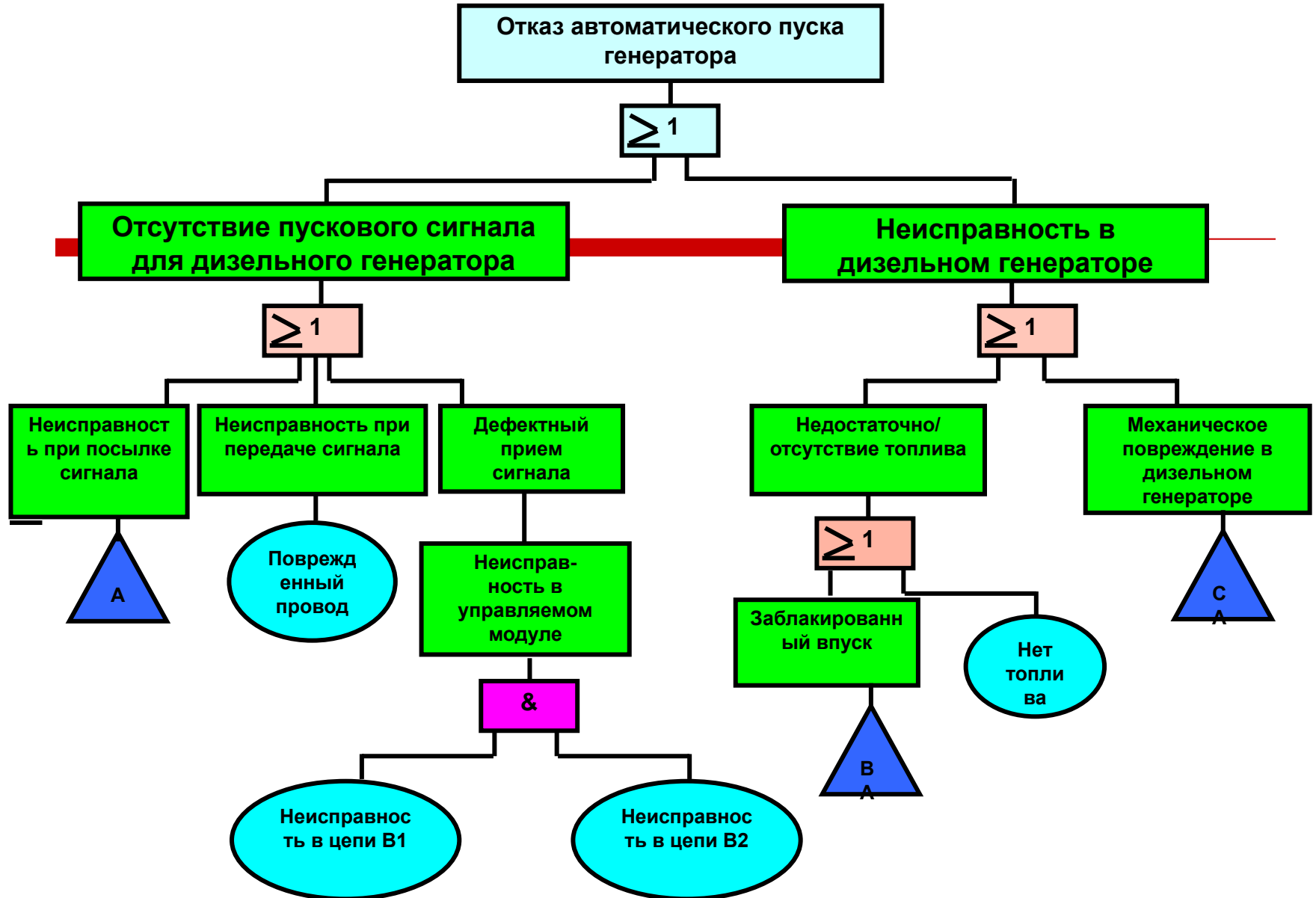
# FTA - анализ «дерева неисправностей»

---


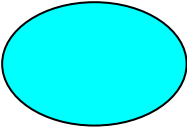
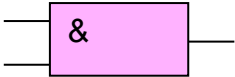
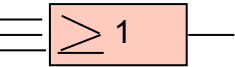
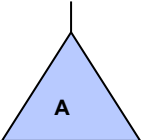
FTA представляет собой совокупность приемов качественных или количественных, при помощи которых выявляются методом дедукции, выстраиваются в логическую цепь и представляются в графической форме те условия и факторы, которые могут способствовать определенному нежелательному событию (называемому вершиной событий).

---

# Пример «дерева неисправностей»»



# Символы «дерева неисправностей»

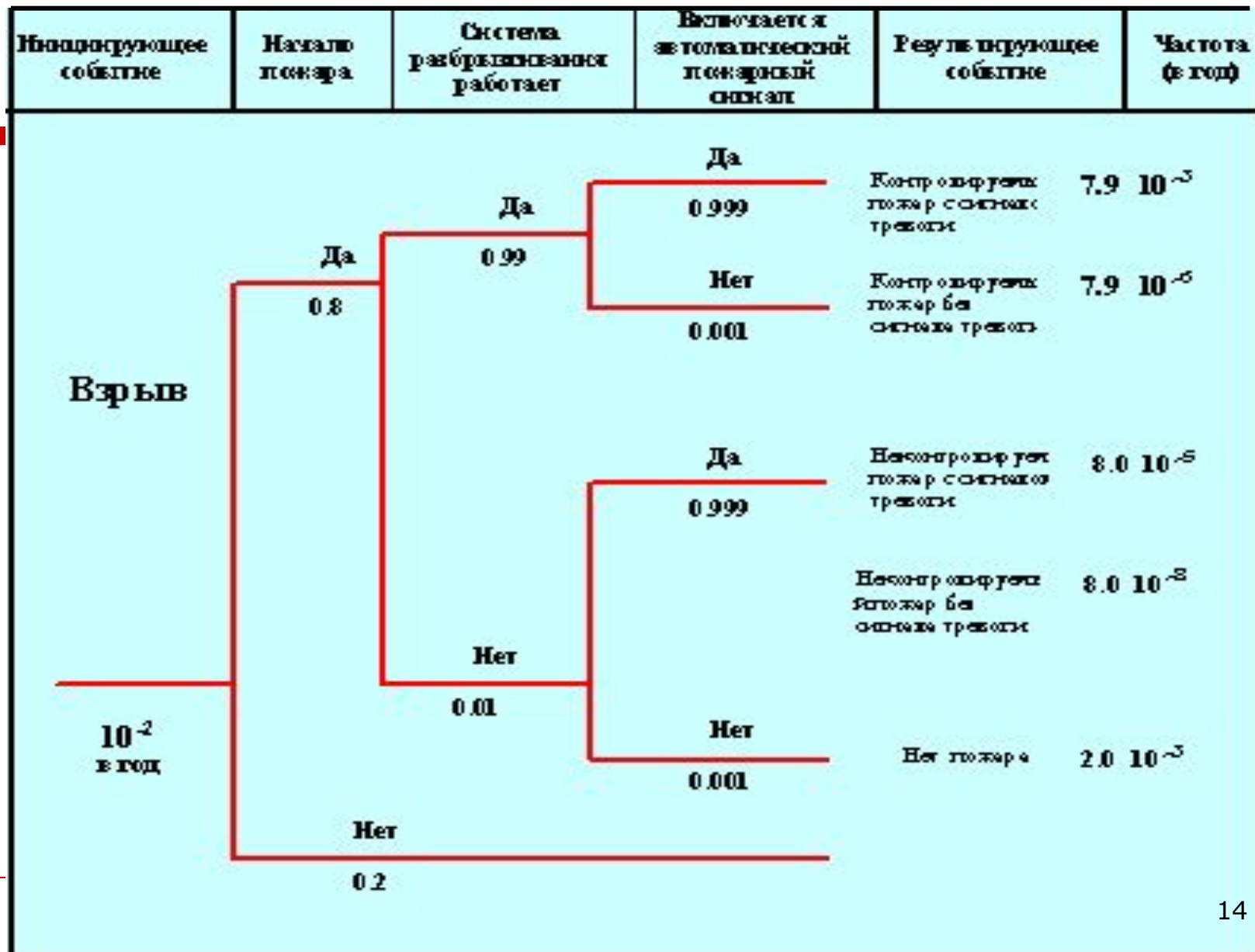
Символ	Функция	Описание
	Блок описания события	Наименование или описание события, код события и вероятность его появления (по мере необходимости) должны быть включены в рамку символа
	Базовое событие	Событие, которое не может быть подразделено
	Переключатель И	Событие происходит только в том случае, если одновременно происходят все составляющие события
	Переключатель ИЛИ	Событие происходит в том случае, если происходит любое из составляющих событий либо в единственном числе, либо в любом из сочетаний
	Вход в блок	Событие, определяемое где-нибудь в другом месте «дерева неисправностей»

Примечание – Символы взяты из МЭК 61025 и использованы на рис. 14. Существуют также альтернативные условные обозначения символов «дерева неисправностей»

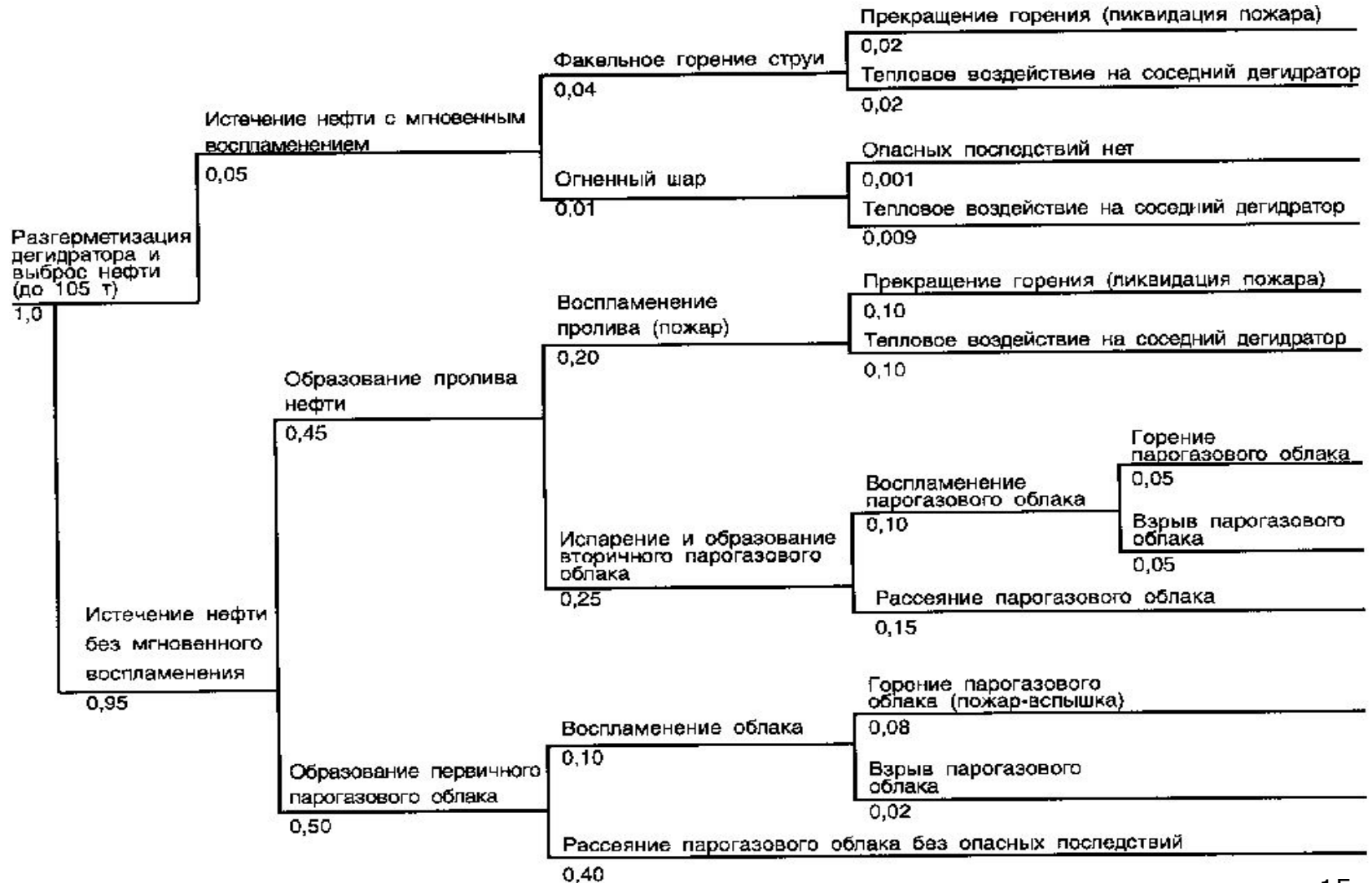
## ETA анализ «дерева событий»

**ETA** представляет собой совокупность приемов количественных или качественных, которые используются для идентификации возможных исходов инициирующего события и, если это требуется, их вероятностей. Предполагается, что каждое событие в последовательности представляет собой либо исправность, либо неисправность.

## Пример «дерева событий» для взрыва пыли



# «Дерево событий» при аварии на установке первичной переработки нефти ( $T < 100\text{ }^{\circ}\text{C}$ , $P < 0,98\text{ МПа}$ )



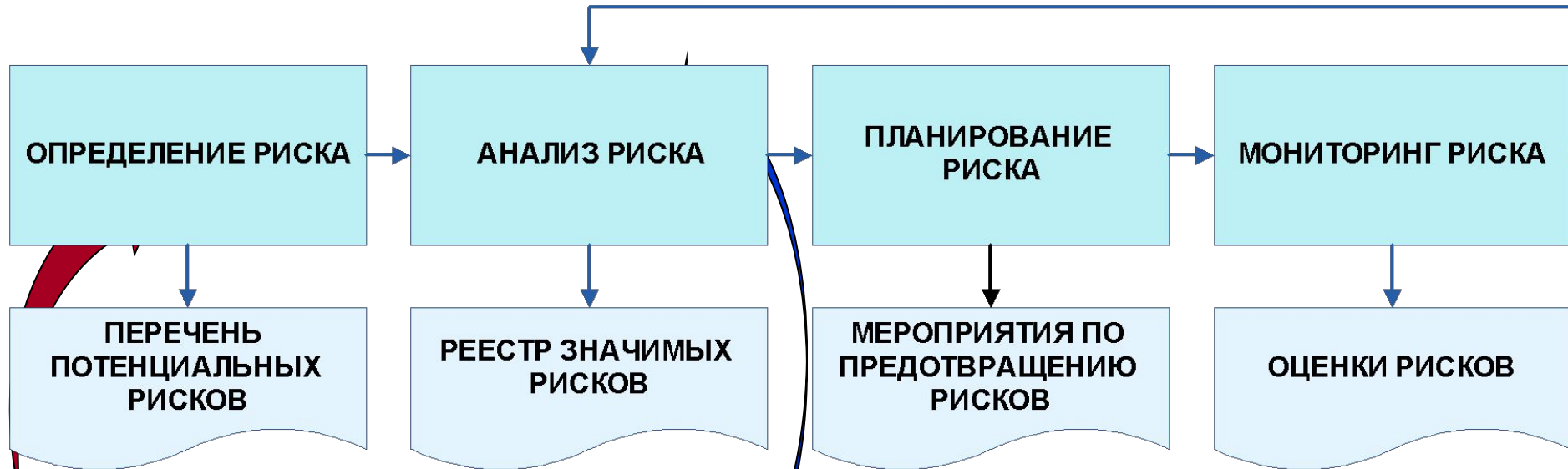
# Другие методы проведения анализа

---

- **Оценка влияния на надежность человеческого фактора (HRA)**
- **Предварительный анализ опасности (PHA)**
- **Исследование опасности и связанных с ней проблем (HAZOP)**



# Процесс управления риском



**Подходы**  
**Мозговой штурм**  
**Опыт менеджера.**

**Подсчитывается вероятность проявления риска и оценивается возможный ущерб.**  
**Вероятность до 10% - очень низкая**

**10% - 25% - низкая**  
**25% - 50% - средняя**  
**50% - 75% - высокая**

## Планирование управления рисками



## Идентификация рисков



## Качественная оценка рисков



## Количественная оценка рисков



## Планирование реагирования



## Возьмем в качестве примера по управлению рисками и безопасностью на предприятиях опыт американских профессионалов:

---

- **6%** их времени уходит на планирование рисков компании и разработку общих мер по их управлению;
- **20%** - на организацию управления безопасностью;
- **5%** - на создание правовых основ защиты информации (составление контрактов и т.п.);
- **14%** - на пресечение потерь от попыток промышленного шпионажа, совершения конкретных преступлений против собственности и другой нежелательной активности конкурентов;
- **14%** - на расследование только что указанных действий;
- **18%** - на контроль безопасности персонала (проверку новых сотрудников и оценку действующих);
- **7%** - на защиту особо уязвимой информации материалов;
- **16%** - на физическую безопасность защищаемых объектов.

**Таким образом, 45% рабочего времени американские специалисты затрачивают на изучение рисков для предприятия и разработку общей системы мер по их контролю.**

---

---

**СПАСИБО ЗА ВНИМАНИЕ**