

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

**КАФЕДРА «БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ И ЗАЩИТА
ОКРУЖАЮЩЕЙ СРЕДЫ»**

**Системный анализ безопасности. Вероятностные методы оценки
безопасности. Дерево отказов**

Методические рекомендации к выполнению расчетной части раздела
«Безопасность и экологичность проекта»
для студентов очной и заочной форм обучения по направлениям подготовки
бакалавров и специалистов

Ростов – на – Дону
2017

Составители: доцент, к.т.н. Богданова И.В.

УДК 621.8

Системный анализ безопасности. Вероятностные методы оценки безопасности. Дерево отказов.

Вероятностные методы оценки безопасности. Дерево отказов

Широко используемым в настоящее время является метод анализа безопасности эргатических систем методом так называемого «дерева отказов» («дерево событий», «дерево происшествий»).

Широкому применению этих моделей в зарубежных исследованиях аварийности и травматизма способствует целый ряд достоинств, присущих диаграммам типа "дерево". Основные из них проявляются в следующем: сравнительная простота построения, дедуктивный характер выявления причинно-следственных связей исследуемых явлений. направленность на их существенные факторы, легкость преобразования таких моделей, наглядность реакции изучаемой системы на изменение структуры, декомпозируемость "дерева" и процесса его изучения, возможность качественного анализа исследуемых процессов, легкость дальнейшей формализации и алгоритмизации, приспособленность к обработке на средствах ЭВТ, доступность для статистического моделирования и количественной оценки изучаемых явлений, процессов и их свойств.

Приведенные и другие достоинства моделей типа "дерево" обеспечили их приемлемость для исследования процесса возникновения и предупреждения происшествий в ведущих отраслях народного хозяйства - ядерной энергетике, химической промышленности, аэрокосмической индустрии и на транспорте.

По своей сути, представление процессов возникновения или предупреждения происшествий в виде дерева является графической иллюстрацией т.н. *булевых условий* (вспомним элементы булевой алгебры), направленных либо на появление предпосылок и перерастание их в причинную цепь происшествия, либо на обеспечение таких свойств исследуемого объекта и системы обеспечения безопасности его функционирования, которые исключают указанные условия.

1. Методика количественного анализа безопасности с использованием дерева отказов

Дерево отказов представляет собой графическое представление причинных взаимосвязей, полученных в результате прослеживания опасных ситуаций в системе в обратном порядке (от конечного нежелательного события до начальных), чтобы отыскать возможные причины их возникновения. При построении дерева отказов используются определенные понятия и правила, а также графическая символика.

1.1 Основные понятия, используемые при построении дерева отказов

1.1.1 Событие: в вашем случае событие - это авария. травма, отказ какого-либо устройства, элемента. Частота этих событий связана с

продолжительностью работы и количеством работающих. События эти следуют одно за другим в случайные моменты времени, скачкообразно меняя состояние системы. Говоря о вероятности перехода системы в то или иное состояние, мы имеем в виду вероятность появления события в потоке за отрезок времени от t до $t+\Delta t$.

Теория вероятностей определяет случайное событие как исход опыта. Для удобства рассуждений в нашем случае можно трактовать опыт как отрезок Δt на интервале времени, в течение которого наблюдалось состояние системы. Обычно на производстве таким интервалом времени является год, выраженный в часах (1800 рабочих часов) или, с учетом количества работающих, в человеко-часах.

Табличные значения вероятностей отказов различных устройств даются обычно за определенное количество часов и при расчетах вероятностей по дереву отказов необходимо приводить исходные данные к единому интервалу оценивания.

С точки зрения безопасной эргатической системы необходимо выделить следующие виды событий:

а) нормальное событие [функционирование]: событие, характеризующее ожидаемый [нормальный] ход рассматриваемого процесса. Оно может появиться или не появиться в определенное время. Если нормальное событие произошло не вовремя, оно рассматривается как отказ;

б) отказ: событие, характеризуемое тем, что одно из двух его состояний связано с ненормальной работой, являющейся следствием поломки или дефекта. События “а” и “б” взаимно исключают друг друга и исчерпывают все множество событий, т.е. являются несовместными. Различают три вида отказов:

первичный отказ: событие, вызванное особенностями самого элемента системы, например его износом;

вторичный отказ: отказ, вызванный внешними причинами, т.е. отказом других элементов, отклонениями условий среды, внешних факторов [например электрического напряжения];

- **ошибочная команда:** неправильный сигнал управления, сигналы помех, ошибочные действия оператора;

в) исходное событие: (нормальное функционирование или отказ), которое появляется на элементарном уровне, т.е. на уровне элементов. Под элементом здесь понимается наименьшая анализируемая составная часть системы. Например, если рассматривать вероятность отказов некоторых компонентов, то эти компоненты будут элементами системы, поскольку дальнейшее их разделение не требуется (невозможно или не имеет смысла). В качестве исходных событий - отказов могут выступать повреждения или отказы элементов, ошибки человека, отклонения условий производственной среды;

г) головное событие: событие на вершине дерева отказов, которое затем анализируется с помощью остальной части дерева. Обычно это отказ

системы, т.е. результирующий отказ, выводящий систему (человека или машину) из работоспособного состояния.

1.2. Символика, используемая при построении

Исходные события являются первопричинами, которые прямо или косвенно приводят к головным событиям. Деревья отказов могут также содержать промежуточные события, в том числе причины -реализаторы головного события. События дерева отказов обозначаются условными символами (таблица 1) и соединяются с помощью символов логических операций в соответствии с их причинными взаимосвязями. Символы логических операций представлены в таблице 2.

1.3. Правила построения дерева отказов

1.3.1. События, входные для операции “ИЛИ” должны формулироваться так, чтобы каждое из них способно было вызвать появление выходного события, а вместе они исчерпывали бы все возможные пути появления выходного события.

1.3.2. Для любого события, подлежащего анализу, вначале рассматриваются все события, являющиеся входами операций “ИЛИ”, а затем входы операций “И”.

1.3.3. События, входные для операции “И” должны формулироваться так, чтобы появления выходного события было возможно лишь при совместной их реализации.

1.3.4. Если в системе возможны головные события, различающиеся по характеру и тяжести последствий, для каждого из таких событий строят отдельное дерево отказов. Эти деревья могут объединяться в общее дерево отказов системы.

Таблица 1. Символы событий



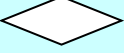
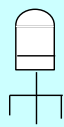
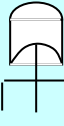
Символ	Содержание события
	Событие, вводимое логическим знаком и анализируемое в дереве отказов (головное или промежуточное событие)
	Исходное событие, обеспеченное достаточными данными
	Событие, недостаточно детально разработанное. Далее в дереве отказов оно не анализируется из-за отсутствия данных или из-за нецелесообразности.

Таблица 2. Символы логических операций

	“И”	Выходное событие происходит, если все входные события происходят одновременно
	“ИЛИ”	Выходное событие происходит, если случается любое из входных событий

1.4. Этапы построения дерева отказов

1.4.1. Выбирается уровень детализации рассматриваемой эргатической системы. Рассматриваются все возможные нежелательные события в системе.

1.4.2. События разделяются на самостоятельные группы.

1.4.3. Для каждой группы выделяется головное событие т.е. событие, к которому в различных комбинациях приводят все события данной группы и которое должно быть предотвращено.

1.4.4. Рассматриваются все первичные и вторичные события которые могли вызвать головное событие,

1.4.5. Устанавливается связь между событиями через соответствующие логические операции (логическое "И", логическое "или").

1.4.6. Рассматриваются события, необходимые для анализа каждого из предыдущих событий, и повторяются пп. 1.4.1, 1.4.2 и т.д., пока все события не будут основными, или прекращаем дальнейший анализ в силу незначительности события, нецелесообразности или отсутствия данных.

1.4.7. События представляются графически в виде дерева отказов.

1.4.8. Выполняется количественный анализ (вычисление вероятностей событий).

Рассмотрим процесс построения дерева отказов на примере работы на заточном станке. Предположим, что рассматриваемой системой является операция заточки инструмента.

В соответствии с этапом 1.4.1 перечислим нежелательные события - аварийные ситуации, которые должны быть предотвращены.

- а) касание кистью или пальцами наждачного круга.
- б) контакт локтевой части руки с кругом.
- в) попадание одежды в станок.
- г) попадание металлической крошки в глаз.
- д) поражение током из-за плохого заземления.
- е) воспламенение из-за перегрузки двигателя.

Подробный список опасных ситуаций можно составить на основе данных о несчастных случаях за прошедшее время.

На этапе 1.4.2 разделяем перечисленные события на независимые группы. Здесь трудно сформулировать определенный алгоритм, и успех этого этапа во многом зависит от опыта и способностей человека, проводящего анализ, но в рассматриваемом примере можно дать некоторые рекомендации.

Так события "а" и "б", тесно связаны и могут анализироваться совместно. То же можно сказать о событиях "д" и "е". Событие "г" обособлено и должно рассматриваться отдельно. Событие "в" можно рассматривать как часть группы, в которую входят события "а" и "б", но оно относится к захвату одежды движущимися частями, а не к прямому контакту, поэтому также может быть изучено отдельно.

Итак, для четырех групп мы можем сформировать четыре головных события.

Для каждого из этих головных событий можно построить дерево отказов в соответствии с 1.4.4 - 1.4.8. Рассмотрим построение дерева отказов для головного события "г" (рис. 1). Согласно правилу 1.3.1 построения дерева отказов вначале анализируем вход операции "ИЛИ". При этом целесообразно рассмотреть две несовместные категории лиц: рабочий, работающий на станке (оператор), и постороннее лицо (неоператор). Следует также предположить, что если на человеке защитные очки, то попадания частиц в глаз не происходит.

Таблица 3

№ события	Головное событие
1,2	Контакт человека с кругом
3	Попадание одежды в станок
4	Попадание частицы в глаз
5	Аварии двигателя

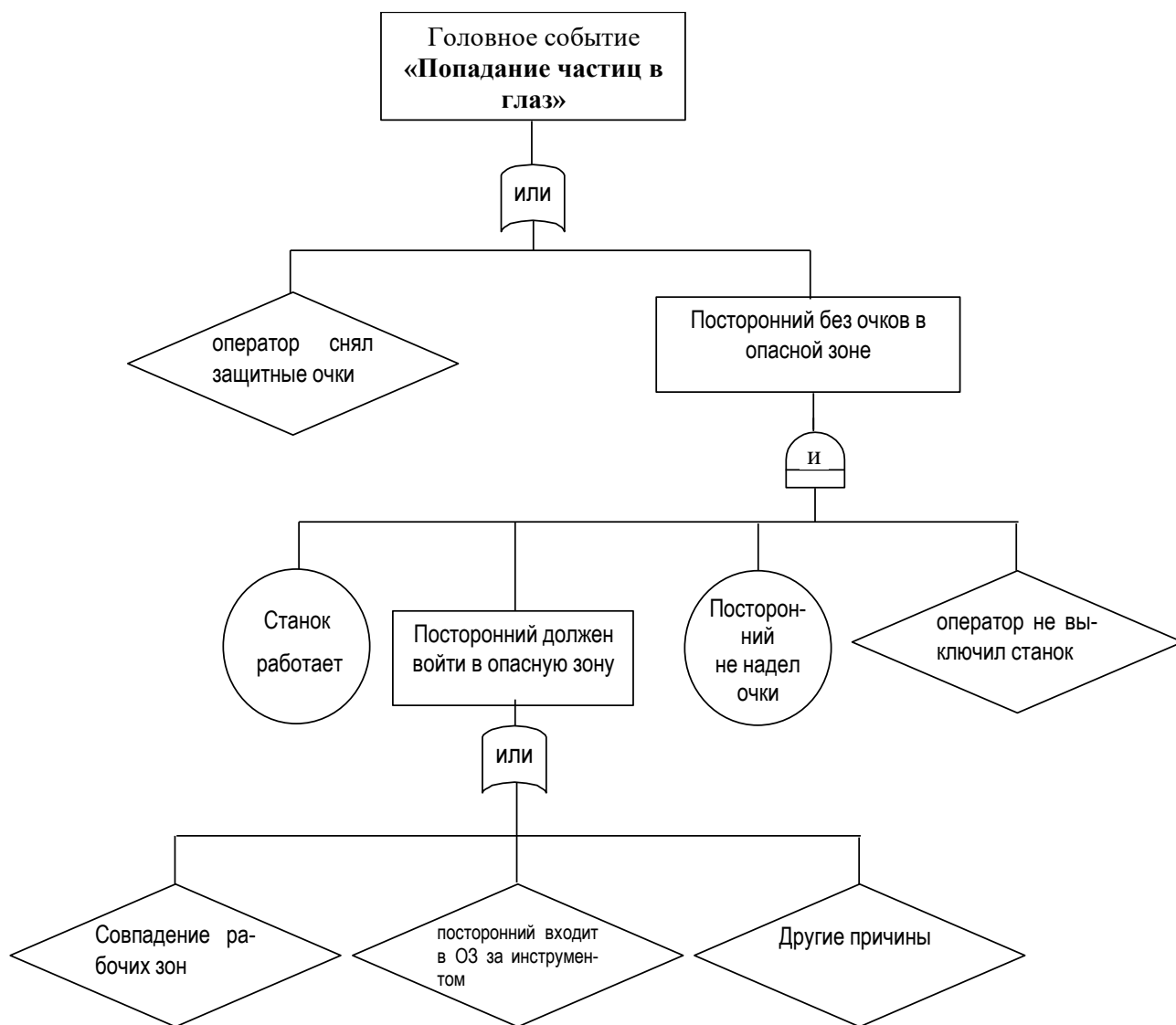


Рис.1

Тогда несчастному случаю предшествуют два показанных на рисунке 1 события А и В. Далее строим дерево отказов, основываясь на логических рассуждениях и знании рабочей обстановки.

Следует отметить, что дерево отказов для данной ситуации не является единственно возможным. В принципе построение дерева может быть продолжено и от события В, однако в данном случае дерево отказов построено в предположении, что в прошлом несчастные случаи, связанные с попаданием частиц в глаза, происходили в основном с посторонними людьми, оказывающимися в опасной зоне во время работы оператора. Анализ показывает, что это может произойти, если у постороннего имеются мотивы войти в опасную зону, и оператор при этом не выключает станка, т.е. имеет место совпадение событий D, E, F и G .

Используя буквенные обозначения событий, представленные на рис. 2 логические связи дерева отказов можно описать, используя уравнения алгебры логики:

$$A = B + C, C = D \cdot E \cdot F \cdot G, E = H + I + J \quad (4.8)$$

1.4. Вычисление вероятностей головных событий

Появление или неоявление события соответствует логическим Т (true - истина) и F (false - ложь).

Любое событие можно представить как логическую функцию, например

$$A = BC + BE \quad (4.9)$$

где A, B, C, D, E - логические переменные, в данном случае - события. Для вычисления A необходимо знать значения B, C, D, E .

Но, в то время как в алгебре логики любое событие является дихотомическим, т.е. может иметь лишь два исхода, а соответствующая логическая (булева) переменная принимать лишь два значения - Т или F, при оценке риска посредством дерева отказов предполагается, что *каждой логической переменной ставится в соответствие некоторая относительная частота, с которой ожидается появление связанного с ней события, т.е. вероятность события A - $P(A)$, вероятность события B - $P(B)$ и т.д..*

Событие A в формуле (3) является сложным. Вероятности сложных событий рассчитываются по формулам, включавшим сложение и умножение вероятностей элементарных событий с учетом их логической взаимосвязи. При этом различаются следующие виды событий:

а) независимые события, если вероятность осуществления одного не зависит от того, осуществилось или нет другое событие, т.е. если выполняется $P(A | B) = P(A)$ и $P(B | A) = P(B)$, где $P(A | B)$ - вероятность события A при условии появления события B (условная вероятность), $P(B | A)$ - вероятность события B при условии появления события A ;

б) зависимые события, $P(A | B) \neq P(A)$ и $P(B | A) \neq P(B)$;

в) несовместные события, если появление события A исключает появление события B и наоборот, т.е. $P(AB) = 0$;

г) противоположные события: противоположным для события A является событие \bar{A} , состоящее в том, что событие A в данном опыте не осуществляется. Вероятности противоположных событий связаны соотношением $P(\bar{A}) = 1 - P(A)$.

Вероятность независимых событий вычисляется по следующим формулам:

1) логическое "И" (головное событие происходит в случае одновременного появления событий $A_1, A_2, A_3, \dots, A_T$:

$$P(A_1, A_2, A_3, \dots, A_T) = \prod_i^T P(A_i) \quad (4.10)$$

2) логическое “ИЛИ” (головное событие происходит при выполнении любого из событий $A_1, A_2, A_3, \dots, A_T$);

$$P(A_1, A_2, A_3, \dots, A_T) = 1 - \prod_{i=1}^T (1 - A_i). \quad (4.11)$$

1.6. Оценка опасности по экономическим критериям

Построение дерева отказов позволяет провести количественный анализ, конечной целью которого является эффективное распределение средств на обеспечение безопасности. При этом можно рассматривать влияние различных альтернативных мероприятий на дерево отказов и, тем самым на вероятность головного события. Критерием для выбора тех или иных мероприятий является соотношение между затратами и экономией. Определим эти понятия.

Затраты - денежные средства, уплачиваемые за внедрение устройств обеспечения безопасности, методов, процедур и т.п. (капиталовложения, эксплуатационные расходы).

Экономия - ожидаемое сокращение убытков и потерь. Аварии и несчастные случаи вызывают бесполезные затраты в деньгах или потерю трудоспособности, которая также может быть оценена в денежных единицах.

Уровень затрат и потерь непосредственно связан с серьезностью аварий. Каждое головное событие представляет собой аварию или несчастный случай, последствия которых могут быть различны. На основании регистрационных записей можно определить частоту, с которой головное событие приводит, например, к следующим возможным последствиям:

- а) необходимость оказать первую помощь;
- б) временная нетрудоспособность;
- в) частичная инвалидность;
- г) полная инвалидность;
- д) смертельный исход.

Каждому исходу головного события соответствует, таким образом, определенная величина убытков u_i , и средний ожидаемый ущерб от одного несчастного случая может быть записан в виде

$$D = \sum_{i=1}^m p_i u_i, \quad \sum_{i=1}^m p_i = 1, \quad (4.12)$$

где m - количество градаций тяжести исходов, p_i - условная вероятность i -го исхода (последствия) головного события (при условии, что головное событие «несчастный случай» произошло), u_i - средний ущерб от события i -й тяжести.

Средний ожидаемый ущерб при равных вероятностях p_i может быть оценен также по формуле

$$D = \frac{\sum_{j=1}^n u_j}{n} . \quad (4.13)$$

Тогда экономический риск от несчастного случая («критичность события») определяется как

$$R = P \cdot D.$$

Литература

1. Федеральный закон от 24.07.1998 г. № 125-ФЗ "Об обязательном социальном страховании от несчастных случаев на производстве и профессиональных заболеваний".
2. ГОСТ Р 51898-02. Аспекты безопасности. Правила включения в стандарты.
3. Оценка и управление природными рисками// Материалы Общероссийской конференции "Риск-2000". – М.: Анкил, 2000. – 478 с.
4. Хенли Э. Дж., Кумамото Х. Надежность технических систем и оценка риска. –М.: Машиностроение, 1981. –526 с.
5. Профессиональный риск для здоровья работников (Руководство) / Под ред. Н.Ф. Измерова и Э.И. Денисова. М.: Тровант, 2003. 448 с.
6. ГОСТ 11.005-74. Правила определения оценок и доверительных границ для параметров экспоненциального распределения и распределения Пуассона. –29 с