

СИСТЕМНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ

УДК 681.5.015:007

АНАЛИЗ НАДЕЖНОСТИ: ОТ ДЕРЕВА ОТКАЗОВ К ДЕРЕВУ КАТАСТРОФ

© 2021 г. Д. И. Кательников^а, Л. В. Пустыльник^б, А. П. Ротштейн^{с,д,*}

^а Винницкий национальный технический ун-т, Винница, Украина

^б Тель-Авивский академический инженерный колледж – Афека, Тель-Авив, Израиль

^с Иерусалимский политехнический ин-т – Махон Лев, Иерусалим, Израиль

^д Донецкий национальный ун-т им. Василя Стуса, Винница, Украина

*e-mail: rothstei@g.jct.ac.il

Поступила в редакцию 06.02.2021 г.

После доработки 25.03.2021 г.

Принята к публикации 31.05.2021 г.

Предлагается метод анализа дерева катастроф, который является аналогом классического метода анализа дерева отказов, не требующим знания вероятностей событий. Вместо понятия “вероятность отказа” используется понятие “возможность бифуркации”, которая оценивается числом в интервале $[0, 1]$ с помощью теории катастроф и соответствует функции принадлежности нечеткого множества. Расчет возможности бифуркации (или катастрофы) системы выполняется с помощью специально введенных правил агрегации возможностей бифуркаций для различных логических операций дерева отказов. Иллюстрация метода анализа катастроф выполнена на примере дерева отказов для дорожной аварии на Т-образном перекрестке.

DOI: 10.31857/S0002338821050115

Введение. Метод дерева отказов (fault tree analysis – FTA), предложенный в 1962 г. и подробно изложенный в [1], до сих пор является одним из основных методов анализа надежности, безопасности и риска не только в технических, но и в социально-экономических, военных и других системах [2, 3].

Вероятностные модели FTA предусматривают бинарную концепцию отказов системы и ее элементов: 1 – нет отказа, 0 – есть отказ. Поэтому событие “отказ” можно трактовать как бифуркацию, т.е. перескок из одного устойчивого состояния (нет отказа) в другое устойчивое состояние (есть отказ). Подход к моделированию и оптимизации надежности на основе вилок бифуркаций из теории хаоса рассмотрен в [4, 5].

Специальным математическим аппаратом моделирования бифуркаций служит теория катастроф [6–8], которая является развитием теории нелинейных колебаний [9]. Несмотря на широкое распространение теории катастроф в различных областях, работы по ее применению в моделях надежности отсутствуют.

В статье предлагается метод анализа дерева катастроф (catastrophe tree analysis – CTA), который есть аналог классического метода FTA, не требующий знания вероятностей событий. Вместо понятия “вероятность отказа” используется понятие “возможность бифуркации”, которая оценивается числом в интервале $[0, 1]$ с помощью теории катастроф и соответствует функции принадлежности нечеткого множества [10–12]. Расчет возможности бифуркации (или катастрофы) системы выполняется с помощью специально введенных правил агрегации возможностей бифуркаций для различных логических операций дерева отказов.

Статья организована следующим образом. В разд. 1 приводятся понятия характеристической функции и функции принадлежности, необходимые для понимания различий между вероятностью и возможностью отказа, которые вычисляются на основе структурной функции надежности. В разд. 2 рассматривается пример описания бифуркации с помощью функции принадлежности нечеткого множества. Раздел 3 содержит основные соотношения теории катастроф, которые используются в методе анализа дерева катастроф. В разд. 4 предлагаются правила агрегации уровней бифуркаций для логических операций дерева катастроф. Раздел 5 иллюстрирует метод дерева катастроф на примере дорожной аварии.

1. Структурная функция: вероятность и возможность отказа. Формальной основой дерева отказов является булева функция, которую в теории надежности принято называть структурной функцией [1]. Она связывает бинарные характеристические функции системы и ее элементов:

$$\chi_S = f_L(\chi_1, \chi_2, \dots, \chi_n), \tag{1.1}$$

где $\chi_i = 1(0)$, если i -й элемент работает (отказал), $\chi_S = 1(0)$, если система работает (отказала).

Зная вероятности этих состояний

$$P_i = \text{Prob}(\chi_i = 1), \quad P_S = \text{Prob}(\chi_S = 1),$$

из структурной функции (1.1) получается вероятностная функция надежности системы:

$$P_S = f_P(P_1, P_2, \dots, P_n), \tag{1.2}$$

где Prob – символ вероятности, P_i и P_S – вероятности безотказной работы i -го элемента ($i = 1, 2, \dots, n$) и системы соответственно.

При этом используются следующие правила перехода к вероятности:

$$\chi_i \wedge \chi_j \Rightarrow P_i \cdot P_j,$$

$$\chi_i \vee \chi_j \Rightarrow P_i + P_j - P_i \cdot P_j.$$

Если в (1.1) характеристические функции χ_i и χ_S заменить функциями принадлежности нечетких множеств, то получаем нечетко-логическую функцию

$$\pi_S = f_L(\pi_1, \pi_2, \dots, \pi_n), \tag{1.3}$$

которая позволяет оценивать возможность безотказной работы системы $\pi_S \in [0, 1]$ на основе возможностей $\pi_i \in [0, 1]$ безотказной работы ее элементов. При этом используются следующие правила вычислений:

$$\pi_i \wedge \pi_j \Rightarrow \min(\pi_i, \pi_j),$$

$$\pi_i \vee \pi_j \Rightarrow \max(\pi_i, \pi_j).$$

Взаимосвязь возможности и вероятности в моделях надежности показана на рис. 1, где z – параметр, от которого зависит надежность элемента, $z \in [z, \bar{z}]$, z (\bar{z}) – нижнее (верхнее) значение интервала допустимых значений; A – нечеткое множество “возможность надежной работы элемента в зависимости от параметра z ”; $\pi_A(z)$ – функция принадлежности параметра z к нечеткому множеству A . Согласно [10], функция $\pi_A(z)$ трактуется как распределение возможности надежной работы элемента; α – число в интервале $[0, 1]$, которое задает минимально необходимый уровень возможности надежной работы; A_α – множество α -уровня, определяющее значения параметра z , для которых возможность надежной работы не ниже α , т.е.

$$A_\alpha = \{z \in [z, \bar{z}], \pi_A(z) \geq \alpha\};$$

$\chi_A(z)$ – характеристическая функция, такая, что

$$\chi_A(z) = \begin{cases} 1, & \text{если } z \in A_\alpha, \\ 0, & \text{если } z \notin A_\alpha, \end{cases}$$

q – вероятность отказа элемента, которая оценивается статически:

$$q = \frac{N - N_\alpha}{N},$$

где N – общее число испытаний, N_α – число испытаний, в которых $z \in A_\alpha$.

2. Функция принадлежности к бифуркации. Событие “отказ” нами трактуется как бифуркация, т.е. потеря устойчивости. В теории колебаний [9] принято использовать определение устойчивости по Ляпунову, которое требует внутреннего описания системы с помощью дифференциальных уравнений.

Покажем, что при отсутствии внутреннего описания устойчивость можно определить с помощью нечетких множеств, которые лежат в основе теории возможностей [10].

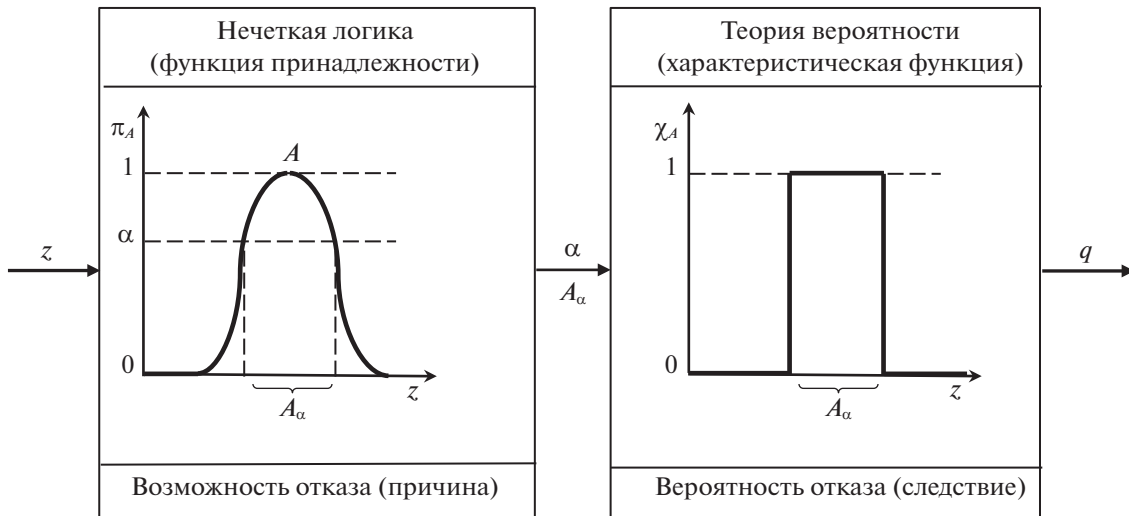


Рис. 1. Взаимосвязь возможности и вероятности отказа

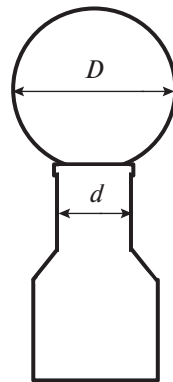


Рис. 2. Шарик на бутылке

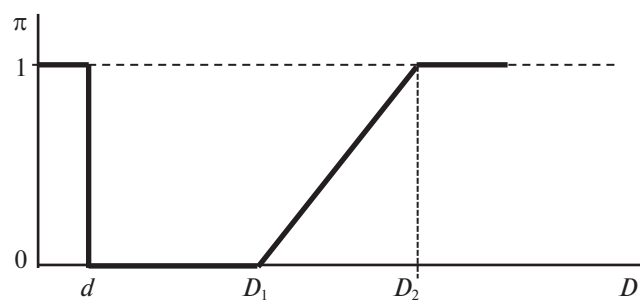


Рис. 3. Функция принадлежности к бифуркации

На рис. 2 показан шарик диаметром D , который сохраняет устойчивость на горлышке бутылки диаметром d . Предполагается, что величина диаметра D может изменяться.

Бифуркация, т.е. падение шарика с бутылки, описывается функцией принадлежности (рис. 3), где имеются следующие области:

(а) как только $D < d$, то шарик проваливается в бутылку и степень принадлежности к бифуркации $\pi = 1$.

Таблица 1. Возможности бифуркаций для различных потенциальных функций

Модель катастрофы	Потенциальная функция	Число входов	Нормализованные формулы
C (Cusp)	$V(x) = x^4 + ax^2 + bx$	2	$x_a = \sqrt{a}, x_b = \sqrt[3]{b}$
S (Swallowtail)	$V(x) = x^5 + ax^3 + bx^2 + cx$	3	$x_a = \sqrt{a}, x_b = \sqrt[3]{b}, x_c = \sqrt[4]{c}$
B (Butterfly)	$V(x) = x^6 + ax^4 + bx^3 + cx^2 + dx$	4	$x_a = \sqrt{a}, x_b = \sqrt[3]{b}, x_c = \sqrt[4]{c}, x_d = \sqrt[5]{d}$

(б) если $D \in [d, D_1]$, то шарик сохраняет устойчивость, $\pi = 0$.

(в) при $D \in [D_1, D_2]$ шарик находится на нечетком переходе “устойчиво – не устойчиво”, что соответствует возрастанию π от 0 к 1.

(г) при $D > D_2$ шарик падает с бутылки и $\pi = 1$.

3. Необходимые соотношения теории катастроф. Теория катастроф – это математическая дисциплина для моделирования нелинейных объектов “вход–выход”, в которых незначительные изменения входов (причин) приводят к большим изменениям выходов (следствий) [6–8]. Эта теория позволяет напрямую изучать прерывистое поведение системы без знания ее внутренней структуры. Для этого используется понятие *потенциальной функции*, которая в механике называется *энергетической функцией* или *функцией Ляпунова* в теории устойчивости (второй метод Ляпунова).

В каждый момент времени система стремится минимизировать свой потенциал, который меняется в зависимости от внешних (управляющих) параметров (минимизация локальная). При изменении этих параметров некоторые локальные минимумы могут “исчезать”, что приводит к скачкам, которые соответствуют бифуркациям или катастрофам. Наглядной моделью этой ситуации служит шарик на неровной поверхности, который под воздействием силы тяжести стремится в самое нижнее положение среди других, находящихся поблизости.

В табл. 1 приведены потенциальные функции, которые будут использованы при построении дерева катастроф, соответствующего дереву отказов.

В каждой потенциальной функции $V(x)$ имеется переменная состояния системы (x) и управляемые (входные) переменные (a, b, c, d), которые изменяются в интервалах их допустимых значений. При стремлении потенциальной функции к минимуму могут возникать бифуркации, множество которых определяется из системы уравнений: $V'(x) = 0, V''(x) = 0$. Множеству бифуркаций соответствуют нормализованные формулы, позволяющие вычислить уровни бифуркации (x_a, x_b, \dots, x_d) по входным переменным (a, b, \dots, d). Вывод нормализованных формул описан в работе [13]. Они получены исходя из требования, что входные переменные и уровни бифуркаций изменяются в интервале $[0, 1]$. Это допускает интерпретацию в терминах теории возможности [10]:

a, b, \dots, d – возможности событий, соответствующих входным переменным;

x_a, x_b, \dots, x_d – возможности бифуркаций по входным переменным.

Следует отметить, что операциям извлечения корней в нормализованных формулах соответствуют лингвистические модификаторы (*достаточно, более-менее* и др.), которые используются для растяжения функций принадлежности в теории нечетких множеств. Этим достигается увеличение функции при небольших значениях аргумента.

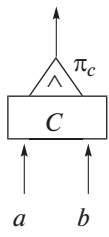
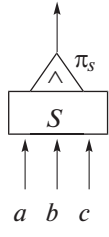
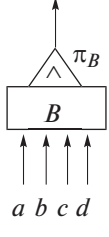
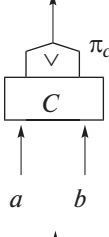
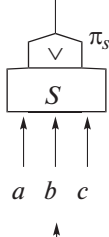
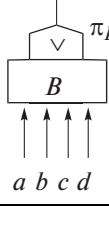
Например, пусть $\pi_p(y) = y$ – функция принадлежности переменной $y \in [0, 1]$ к нечеткому множеству “перфектность (p)”. Тогда модифицированные нечеткие множества “достаточно перфектно (fp)” и “более-менее перфектно (mfp)” описываются функциями принадлежности:

$$\pi_{fp}(y) = y^{1/2}, \quad \pi_{mfp}(y) = y^{1/4}.$$

Поскольку входные переменные a, b, c, d в потенциальных функциях (табл. 1) изменяются в интервале $[0, 1]$ и имеют смысл степеней принадлежности, то операции извлечения корней (правый столбец табл. 1) можно трактовать как растяжение степеней принадлежности с помощью лингвистических модификаторов.

4. Дерево катастроф. Будем предполагать, что известно дерево отказов, в котором используются только два логических узла: AND (\wedge) и OR (\vee). Кроме того, ограничимся случаем, когда в

Таблица 2. Правила агрегации на дереве катастроф

Логический узел	Катастрофа	Обозначение на дереве катастроф	Формула агрегации
AND (\wedge)	C		$\pi_C = \begin{cases} \min(\sqrt{a}, \sqrt[3]{b}), \\ \sqrt{\sqrt{a} \cdot \sqrt[3]{b}} \end{cases}$
	S		$\pi_S = \begin{cases} \min(\sqrt{a}, \sqrt[3]{b}, \sqrt[4]{c}), \\ \sqrt[3]{\sqrt{a} \cdot \sqrt[3]{b} \cdot \sqrt[4]{c}} \end{cases}$
	B		$\pi_B = \begin{cases} \min(\sqrt{a}, \sqrt[3]{b}, \sqrt[4]{c}, \sqrt[5]{d}), \\ \sqrt[4]{\sqrt{a} \cdot \sqrt[3]{b} \cdot \sqrt[4]{c} \cdot \sqrt[5]{d}} \end{cases}$
OR (\vee)	C		$\pi_C = \begin{cases} \max(\sqrt{a}, \sqrt[3]{b}), \\ \frac{1}{2}(\sqrt{a} + \sqrt[3]{b}) \end{cases}$
	S		$\pi_S = \begin{cases} \max(\sqrt{a}, \sqrt[3]{b}, \sqrt[4]{c}), \\ \frac{1}{3}(\sqrt{a} + \sqrt[3]{b} + \sqrt[4]{c}) \end{cases}$
	B		$\pi_B = \begin{cases} \max(\sqrt{a}, \sqrt[3]{b}, \sqrt[4]{c}, \sqrt[5]{d}), \\ \frac{1}{4}(\sqrt{a} + \sqrt[3]{b} + \sqrt[4]{c} + \sqrt[5]{d}) \end{cases}$

каждый из логических узлов входит не более четырех аргументов (стрелок). Методика построения дерева катастроф будет показана на примере в разд. 5.

При переходе от дерева отказов к дереву катастроф будем использовать следующие модели, представленные в табл. 2:

Сборка (C) – для логических узлов с двумя входными стрелками;

Ласточкин хвост (S) – для логических узлов с тремя входными стрелками;

Бабочка (B) – для логических узлов с четырьмя входными стрелками.

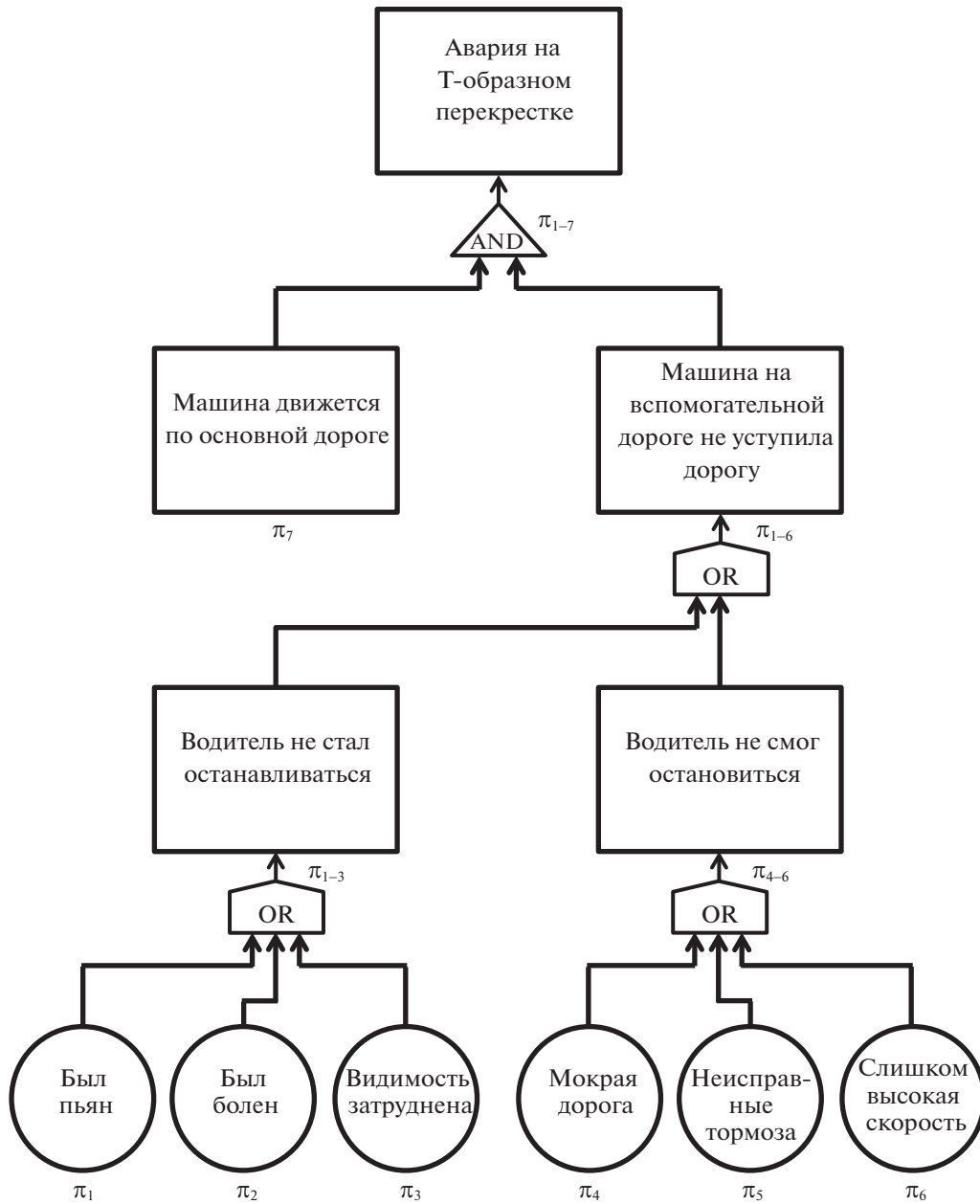


Рис. 4. Дерево отказов

Каждый из узлов дерева катастроф представляет собой преобразователь “входы–выход” по правилам агрегации “вектор–скаляр”, которые приведены в табл. 2. В теории нечетких множеств используются различные методы агрегации функций принадлежности, над которыми выполняются операции AND и OR. Применение каждого из этих методов может давать различные результаты. В частности, в [14] рассмотрен пример необходимости замены операции **min** операцией умножения. Окончательное решение о результатах анализа дерева катастроф для конкретного объекта целесообразно принимать путем сравнения нескольких методов агрегации “вектор–скаляр”. Поэтому в табл. 2, наряду с традиционными для теории нечетких множеств операциями **min** и **max**, приводятся среднее геометрическое и среднее арифметическое. Однако это не исключает возможности применения других известных методов агрегации.

Предполагается, что при нумерации входных стрелок дерева катастроф, соответствующих терминальным вершинам дерева отказов, соблюдается условие $a \leq b \leq c \leq d$. Это необходимо для получения **min** и **max** при выполнении операций AND и OR.

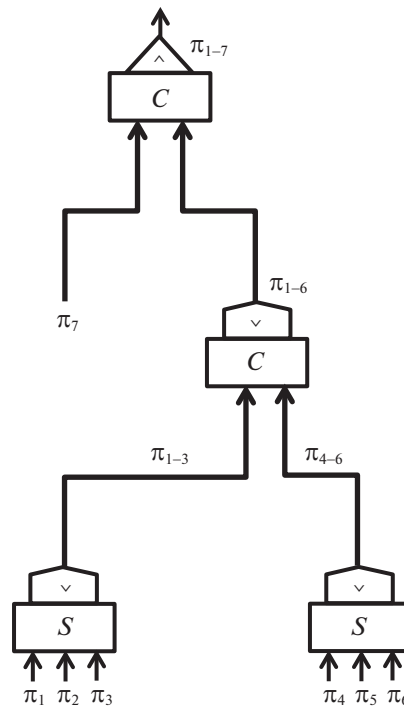


Рис. 5. Дерево катастроф

5. Пример применения. На рис. 4 представлено дерево отказов, для аварии на Т-образном перекрестке, где обозначены: $\pi_1, \pi_2, \dots, \pi_6, \pi_7$ – возможности первичных событий, которые соответствуют терминальным вершинам дерева; $\pi_{1-3}, \pi_{4-5}, \pi_{1-6}$ – возможности промежуточных (не терминальных) событий; π_{1-7} – возможность аварии.

Пользуясь табл. 2, от дерева отказов (рис. 4) переходим к дереву катастроф (рис. 5), которому соответствуют расчетные формулы:

$$\pi_{1-3} = \begin{cases} \max(\sqrt{\pi_1}, \sqrt[3]{\pi_2}, \sqrt[4]{\pi_3}), \\ \frac{1}{3}(\sqrt{\pi_1} + \sqrt[3]{\pi_2} + \sqrt[4]{\pi_3}), \end{cases}$$

$$\pi_{4-6} = \begin{cases} \max(\sqrt{\pi_4}, \sqrt[3]{\pi_5}, \sqrt[4]{\pi_6}), \\ \frac{1}{3}(\sqrt{\pi_4} + \sqrt[3]{\pi_5} + \sqrt[4]{\pi_6}), \end{cases}$$

$$\pi_{1-6} = \begin{cases} \max(\sqrt{\pi_{1-3}}, \sqrt[3]{\pi_{4-6}}), \\ \frac{1}{2}(\sqrt{\pi_{1-3}} + \sqrt[3]{\pi_{4-6}}), \end{cases}$$

$$\pi_{1-7} = \begin{cases} \min(\sqrt{\pi_7}, \sqrt[3]{\pi_{1-6}}), \\ \sqrt{\sqrt{\pi_7} \cdot \sqrt[3]{\pi_{1-6}}}. \end{cases}$$

Исходные данные для расчета по этим формулам задаются экспертно либо с помощью функций принадлежности по известным количественным значениям параметра, влияющего на возможность события. При выборе функций принадлежности можно воспользоваться методом нечеткой перфектности [14].

В табл. 3 приведены результаты расчета возможности аварии π_{1-7} для семи сценариев, каждый из которых представляет собой вектор возможностей ($\pi_1, \pi_2, \dots, \pi_7$) терминальных событий дерева отказов (рис. 4).

Таблица 3. Возможность аварии для различных сценариев

Сценарии	π_1	π_2	π_3	π_4	π_5	π_6	π_7	π_{1-7}	
								(1)	(2)
1	0.0	0.0	0.0	0.0	0.0	0.0	0.5	0.00	0.00
2	0.1	0.0	0.0	0.0	0.0	0.0	0.1	0.32	0.42
3	0.0	0.1	0.0	0.0	0.0	0.0	0.2	0.45	0.51
4	0.0	0.0	0.1	0.0	0.0	0.0	0.3	0.55	0.57
5	0.0	0.0	0.0	0.1	0.0	0.0	0.4	0.63	0.63
6	0.0	0.0	0.0	0.0	0.1	0.0	0.5	0.71	0.68
7	0.0	0.0	0.0	0.0	0.0	0.1	0.6	0.77	0.71

По табл. 3 необходимо сделать пояснение: столбец (1) соответствует агрегации с использованием \min и \max , а столбец (2) – применению среднего геометрического и среднего арифметического. Из табл. 3 видно, что если машина движется по основной дороге ($\pi_7 \neq 0$), то отсутствие аварии ($\pi_{1-7} = 0$) возможно только при $\pi_1 = \pi_2 = \dots = \pi_6 \approx 0$, т.е. когда нет нарушений, связанных с водителем, видимостью, дорогой, тормозами и скоростью. Наличие хотя бы одного из таких нарушений приводит к резкому возрастанию возможности аварии.

Заключение. Статья является первой работой, в которой теория катастроф применяется для моделирования возможности нежелательных событий на основе известного в задачах надежности и безопасности метода деревьев отказов.

Понятие “отказ” рассматривается как бифуркация, т.е. перескок между устойчивыми состояниями, и оценивается нормализованными формулами из теории катастроф. Понятие “возможность отказа” оценивается числом в интервале $[0, 1]$ и моделируется по правилам нечеткой логики.

Результатом работы является метод анализа дерева катастроф, которое соответствует дереву отказов. Суть предложенного метода состоит в сформулированных правилах агрегации возможностей бифуркаций для различных логических узлов дерева.

Иллюстрация метода анализа катастроф выполнена на примере дерева отказов, моделирующего дорожную аварию на Т-образном перекрестке.

Метод дерева катастроф не отменяет метод дерева отказов, а дополняет его следующими новыми качествами:

1. Отсутствует необходимость проведения трудоемких экспериментов, связанных с получением вероятностей первичных событий, которые влияют на вероятность отказа системы. Вместо вероятностей используются возможности первичных событий, уровни которых оцениваются экспертно или на основе измеряемых параметров и соответствующих функций принадлежности.

2. Наблюдение за динамикой изменения входных параметров позволяет переходить к on-line мониторингу уровня возможности отказа системы.

3. Применение моделей теории катастроф позволяет наблюдать нелинейные эффекты, связанные с резким увеличением возможности отказа при незначительных изменениях входных параметров.

СПИСОК ЛИТЕРАТУРЫ

1. Barlow R., Proschan F. Statistical Theory of Reliability and Life Testing. Rinehart and Winston: Holt, 1975.
2. Ryabinin I.A. Reliability and Safety of Structurally Complex Systems. St. Petersburg: SPb Polytechnics, 2000.
3. Solozhentsev E.D. Scenario Logic and Probabilistic Management of Risk in Business and Engineering. St. Petersburg: Business-press, 2004.
4. Ротштейн А.П. Интеграция подходов нечеткой логики и теории хаоса в моделировании и оптимизации надежности // Изв. РАН ТИСУ. 2012. № 4 (51). С. 77–87.
5. Rotshstein A.P., Katielnikov D.I., Pustynnik L.V. Reliability Modeling and Optimization Using Fuzzy Logic and Chaos Theory // International J. of Quality, Statistics, and Reliability. 2012. V. 2012. Article ID 847416. 9 p. <https://doi.org/10.1155/2012/847416>

6. *Thom R.* Structural Stability and Morphogenesis. W. A. Benjamin, Reading, Mass, 1975.
7. *Zeeman E.C.* Catastrophe Theory // Scientific American. 1976. V. 234: P. 65–83.
8. *Arnold V.I.* Catastrophe Theory. Berlin: Springer-Verlag, 1992.
9. *Andronov A.A., Vitt A.A., Khaikin S.E.* Theory of Oscillators. Pergamon Press, 1966.
10. *Zadeh L.A.* Fuzzy Sets as a Basis for a Theory of Possibility // Fuzzy Sets and Systems. 1978. V. 1. P. 3–28.
11. *Ротштейн А.П.* Алгебра алгоритмов и нечеткая логика в анализе надежности систем // Изв. РАН ТИСУ. 2010. № 2 (49). С. 87–99.
12. *Кательников Д.И., Ротштейн А.П.* Нечетко-алгоритмическое моделирование надежности: оптимизация ресурсов контроля и коррекции // Изв. РАН ТИСУ. 2010. № 6 (49). С. 138–142.
13. *Ching-Hsue Cheng, Ying-Hua Liu, Yin Lin.* Evaluating a Weapon System Using Catastrophe Series Based on Fuzzy Scales // Soft Computing in Intelligent Systems and Information Processing// Asian Fuzzy Systems Symposium. Kenting, Taiwan, 1996. P. 212–217.
<https://doi.org/10.1109/AFSS.1996.58359>.
14. *Ротштейн А.П.* Выбор условий деятельности человека на основе нечеткой перфектности // Изв. РАН ТИСУ. 2018. № 6 (57). С. 108–119.