ДОПОВІДІ
НАЦІОНАЛЬНОЇ
АКАДЕМІЇ НАУК
УКРАЇНИ

12 • 2008

ЕКОЛОГІЯ

УДК 629.162.658

В. И. Пампуро

Методологические ограничения метода дерева событий

(Представлено академиком НАН Украины В. П. Кухарем)

A short analysis of the events tree method is given, and the theoretical groundlessness of the method is proved. The incorrectness to postulate a probabilistic model of accidents is shown. The error of accident risk assessments by the events tree method is determined.

Наибольшее практическое распространение анализа безопасности (Risk Assessment) получил метод дерева событий, разработанный в США еще в 1960-х гг. [1]. Он не претерпел принципиальных изменений до настоящего времени [2–6]. Его методология является основой подходов к нормированию безопасности [7, 8].

Метод дерева событий основывается на вероятностной модели аварии и является составной частью анализа безопасности АЭС. Он широко используется в США, России и Украине [6–8]. Технология вероятностного анализа безопасности является частью технологии обеспечения безопасности [1]. В целом эта технология имеет положительное значение как сугубо экспертная, позволяющая повышать безопасность АЭС согласно экспертным рекомендациям, без оптимизации требований к показателю риска аварии и к показателям надежности систем управления и защиты АЭС.

Дерево событий представляет собой логический перебор всех возможных аварийных последовательностей (путей графа событий). Совокупность путей определяет варианты возможной аварии, вызванной исходным событием $\overline{\varepsilon_{\text{а}}}$ с учетом надежности систем, влияющих на развитие аварии. Методику анализа риска аварии по методу дерева событий целесообразно изложить в следующих основных пунктах:

М. 1. Экспертом выбирается исходное событие $\overline{\varepsilon_{\text{а}}}$, инициирующее возможную аварию — событие аварии $\overline{\varepsilon_{\text{п}}}$.

М. 2. Экспертом разрабатывается сценарий аварии. Определяются события работоспособности ε_k и отказа $\overline{\varepsilon_k}$, $k = \overline{1, n}$, систем, с которыми связан сценарий аварии.

М. 3. Все события рассматриваются как независимые, в результате чего в дальнейшем используются только безусловные вероятности событий.

М. 4. Определяется вероятность исходного события $P(\overline{\varepsilon_{\text{а}}}) = R_{\text{а}}$, а также согласно методу дерева отказов определяются вероятности событий работоспособности $P(\varepsilon_k) = P_k$ и вероятности событий отказов $P(\overline{\varepsilon_k}) = R_k$, $k = \overline{1, n}$, систем, определенных сценарием аварии.

М. 5. Строится дерево событий. На входе дерево событий имеет одно ребро, которому приписывается вероятность исходного события $P(\overline{\varepsilon_{\text{а}}}) = R_{\text{а}}$. В общем случае с этим ребром связано 2^n аварийных последовательностей — возможных вариантов развития аварии. Они вместе с ребром исходного события образуют пути. Путь изображается цепочкой ребер, определяющих аварийную последовательность развития аварии, начиная с ребра исходного события и включая последовательность ребер событий работоспособности или отказа соответствующей системы, с которыми связан определенный сценарий аварии. В зависимости от пути, каждому его ребру приписывается вероятность $P(\varepsilon_k) = P_k$ или вероятность $P(\overline{\varepsilon_k}) = R_k$.

М. 6. Определяется вероятность каждого пути (аварийной последовательности) $P_{\text{в}}$, в $= \overline{1, m}$, $m = 2^n$. Она равна произведению вероятностей, приписанных ребрам, образующих путь.

М. 7. На основе экспертного анализа, дерево, состоящее из m исходных вариантов аварии, делится на две части, события которых соответственно H и $\overline{H}$. Сумма этих событий равна достоверному событию:

$$H + \overline{H} = I. \tag{1}$$

Событие H включает в себя только t вариантов аварийных последовательностей (путей), $t < m$, которые, по мнению эксперта, имеют практическую возможность привести к аварии. Остальные $(m - t)$ вариантов относятся к событию $\overline{H}$ и исключаются. Поэтому событие

$$\overline{H} = \varnothing. \tag{2}$$

Соответственно событие аварии

$$\overline{\varepsilon_{\text{п}}} = \overline{\varepsilon_{\text{а}}} H. \tag{3}$$

М. 8. Вычисляется вероятность события риска аварии $R = P(\overline{\varepsilon_{\text{п}}})$, равного сумме вероятностей несовместных событий путей (аварийных последовательностей) $P_{\text{в}}$, по следующей формуле:

$$R = R_{\text{а}} \sum_{B \in T_{\text{в}}} P_{\text{в}}, \tag{4}$$

где $T_{\text{в}}$ — множество индексов вариантов B, входящих в событие H. При этом не учитывается изменение значений вероятностей $P_{\text{в}}$, что необходимо сделать при переходе к преобразованному (упрощенному) графу.

Несомненное достоинство метода дерева событий заключается в его практической направленности, основанной на экспертном анализе возможных вариантов развития аварии, а также возможных последствий аварии. В то же время метод дерева событий имеет ряд существенных методологических ограничений, не позволяющих использовать его для оптимального управления безопасностью АЭС. Эти ограничения заключаются в следующем:

I. Постулирование вероятностной модели аварии ведет к теоретической (статистически закономерной) неизбежности аварии в течение срока службы АЭС [9]. Следствием этого является теоретическая бесполезность любой (в том числе и глубокоэшелонированной) концепции обеспечения безопасности АЭС, так как концептуально эта концепция не в состоянии устранить априори принятую статистическую закономерность аварии.

II. Метод дерева событий не позволяет определить оптимальное значение показателя риска аварии, исходя из максимальной безопасности при минимуме возможных затрат. В методе дерева событий отсутствует методология экономической эффективности, а также принципы ее реализации методами оптимального управления безопасностью АЭС [10, 11].

III. Одним из очевидных методологических ограничений метода дерева событий является допущение о независимости ε-событий, отмеченное в пункте М. 3. Это допущение нарушается в пункте М. 7, согласно которому из всех m исходных вариантов аварии выбираются только t вариантов (путей), $t < m$. Из-за этого нарушения полученные с помощью метода дерева событий результаты анализа безопасности становятся теоретически некорректными. Докажем это важное утверждение.

Исходный (полный) граф событий описывается событиями первой H и второй $\overline{H}$ частей. Эти события образуют полную группу несовместных событий. Поэтому их сумма согласно (1) равна достоверному событию I. В результате перехода от анализа всего дерева событий, описываемого событиями первой H и второй $\overline{H}$ частей, к преобразованному графу событий, описываемому только событие первой H части, событие второй части $\overline{H}$ согласно (2) становится невозможным. Следовательно, в результате преобразований с учетом выражения (1) событие первой части H становится достоверным:

$$H = I \qquad \text{при} \qquad \overline{H} = \varnothing. \tag{5}$$

Из этого и выражения (3) вытекает, что событие аварии равно исходному событию:

$$\overline{\varepsilon_{\text{п}}} = \overline{\varepsilon_{\text{а}}}, \tag{6}$$

т. е. системы обеспечения безопасности не участвуют в предотвращении аварии.

Приведенный вывод подтверждается следующим логическим анализом. Действительно, если рассматривать полное дерево событий, совокупность всех его ветвей (без учета ветки исходного события) определяет все возможные варианты аварии, т. е. если наступает исходное событие, то авария должна произойти по одному из вариантов (ветки) полного дерева событий. А так как совокупность всех вариантов полного дерева событий является достоверным событием, то событие аварии равно исходному событию. При переходе к упрощенному дереву событий логически ситуация не изменяется, так как согласно экспертному условию упрощенное дерево учитывает все возможные варианты аварии при наступлении исходного события. Поэтому событие аварии равно исходному событию.

В то же время, несмотря на теоретические погрешности метода дерева событий, требуется объяснение причин многолетнего его использования в практике обеспечения безопасности. Ниже остановимся на объяснении этого феномена, учитывая тот факт, что согласно методу событий показатель риска аварии для усеченного дерева событий без коррекции исходных значений вероятностей определяется по формуле (4).

Согласно логико-вероятностному методу анализа надежности и безопасности, можно утверждать, что система, состоящая из двух компонент (объекта ji и подсистемы защиты ij), описывается соответственно событиями ε_{ji}, ε_{ij}. Система считается безопасной, если безотказно функционирует одна из компонент. Это практически очевидное положение означает, что авария может наступить только тогда, когда откажут обе компоненты, т. е. событие аварии

$$\overline{\varepsilon_{\text{п}}} = \overline{\varepsilon_{ji}\varepsilon_{ij}}. \tag{7}$$

Соответственно, для независимых событий вероятность аварии

$$P(\overline{\varepsilon_{\text{п}}}) = P(\overline{\varepsilon_{ji}})P(\overline{\varepsilon_{ij}}). \tag{8}$$

Рассмотренная модель является симметрической функцией. Она справедлива, когда компоненты системы равноправны в обеспечении безопасности [13]. Так как объект ji и подсистема защиты ij имеют разное значение в обеспечении безопасности, то их взаимодействие необходимо учитывать в контуре управления безопасностью [13, 14]. С учетом этого контура управления вероятность аварии [14]

$$P_{\text{a}} = \frac{P(\overline{\varepsilon}_{ij})P(\overline{\varepsilon}_{ji})}{1 - P(\varepsilon_{ij})P(\overline{\varepsilon}_{ji})}. \tag{9}$$

Из сравнения выражений (8) и (9) следует неравенство

$$P(\overline{\varepsilon_{ji}})P(\overline{\varepsilon_{ij}}) < \frac{P(\overline{\varepsilon}_{ij})P(\overline{\varepsilon}_{ji})}{1 - P(\varepsilon_{ij})P(\overline{\varepsilon}_{ji})}. \tag{10}$$

Современные АЭС имеют следующие значения вероятности безотказной работы: $P(\varepsilon_{ij}) \approx 0{,}9999$, $P(\varepsilon_{ji}) \approx 0{,}999$. Для этих значений вероятностей безотказной работы значение оценки $P(\overline{\varepsilon_{ji}})P(\overline{\varepsilon_{ij}})$ (8) мало отличается от точного значения, полученного согласно (9): погрешность оценки составляет около 0,1%. Однако в преобразованном дереве событий согласно (4) суммируются вероятности ряда событий путей возможной аварии, среди которых наименьшее значение имеет произведение $P(\overline{\varepsilon_{ji}})P(\overline{\varepsilon_{ij}})$. Поэтому определенное согласно формуле (4) значение показателя риска можно рассматривать только как верхнюю оценку показателя риска аварии.

IV. Оценить погрешность верхней оценки показателя риска аварии (вероятности аварии), получаемой на основе метода дерева событий в пределах этого метода невозможно. Следует учесть, что анализ риска аварии с помощью метода событий связан с проблемой размерности. Так, для системы с n элементами исходное дерево содержит 2^n путей. Например, для структурной схемы управления балансом нейтронной и тепловой мощностей, содержащей восемнадцать элементов, соответствующее ей дерево событий должно содержать 2600000 путей (ветвей) [15]. Провести анализ всех путей и выбрать наиболее значимые для последующего анализа безопасности практически невозможно. Поэтому согласно методу дерева событий такую схему расчленяют на части, находят оценку сверху показателя риска аварии для каждой части, а общую оценку получают как сумму оценок всех частей [3, 5]. Как само расчленение на части, так и принцип суперпозиции (суммирования показателей риска аварии для каждой части) содержат неучтенные ошибки. В результате получаемое значение показателя риска аварии будет существенно превышать точное значение, определяемое согласно (9).

Учитывая проделанный анализ, получаемые согласно методу дерева событий значения оценки показателя риска можно рассматривать только как приближенную верхнюю оценку, для которой отсутствует оценка погрешности приближения.

Оценивая метод дерева событий в целом, заметим следующее.

Во-первых. Несомненное достоинство метода дерева событий заключается в его практической направленности, основанной на знаниях специалиста по атомной энергетике, анализе возможных вариантов развития аварии, а также возможных последствий аварии. Необходимая исходная информация не может быть получена формальным теоретическим путем. Ею

владеет только специалист, который хорошо разбирается в технологии функционирования АЭС и систем обеспечения безопасности. Специалист рассматривает не только варианты (пути) возможной аварии, но и возможные последствия, замыкая тем самым контур управления безопасностью. Дерево событий не содержит контуров управления безопасностью. Оно позволяет лишь упорядочить анализ вариантов опасности АЭС, расчленив общую задачу анализа на части (варианты).

Во-вторых. Метод дерева событий имеет неустранимые методологические ошибки, исключающие корректный анализ безопасности АЭС. В целом он позволяет получить приближенные оценки сверху показателя риска аварии без учета значения погрешности приближения.

Лежащий в основе метода событий качественный подход не позволяет учесть основные скрытые причины виртуальной аварии (неполноту знаний и погрешность технологии обеспечения безопасности).

В-третьих. Метод дерева событий не пригоден для оптимального управления безопасностью из-за проблемы размерности и отсутствия контуров управления безопасностью АЭС. В целом он является качественным методом оценки показателя риска аварии АЭС.

1. *Haasl D.* Advanced concepts in fault tree analysis // System Safety Symposium. – Seattle, Washington, 1965. – P. 234–239.
2. *Хенли Э. Д., Кумато Х.* Надежность технических систем и оценка риска. – Москва: Машиностроение, 1979. – 528 с.
3. *Уивер Л.* Риск от аварии на АЭС с легководными реакторами // Безопасность ядерной энергетики. – Москва: Атомиздат, 1980. – С. 114–133.
4. *Швыряев Ю. В.* Вероятностный анализ безопасности атомных станций. Методика выполнения. – Москва: ИАЭ им. Курчатова, 1992. – 266 с.
5. *Вероятностный* анализ безопасности атомных станций / В. В. Бегун, О. В. Горбунов, И. Н. Каденко и др. – Киев, 2000. – 568 с.
6. *Probabilistic* risk Assessment: Applications for Nuclear Reactor Inspection // O. L. Kelly, T. J. Leahy, H. S. Blackman et al. – Idaho Fails, ID: Idaho National Engineering Laboratory, 1992. – P. 207.
7. *Нормы* радиационной безопасности Украины НРБУ – 97/Д – 2000.
8. *Общие* положения обеспечения безопасности атомных станций ОПБ АЭС – 2000.
9. *Пампуро В. И.* Управление безопасностью объектов атомной энергетики согласно концепции виртуальной аварии // Доп. НАН України. – 2007. – № 11. – С. 180–185.
10. *Пампуро В. И.* Максимальная безопасность атомных станций при минимально возможных затратах // Доп. НАН України. – 2006. – № 5. – С. 186–192.
11. *Пампуро В. И.* Концепция максимальной безопасности при минимальных затратах // Двадцать лет Чернобыльской катастрофы. Взгляд в будущее. – Киев, 2006. – Сб. докл. – Т. 22 – Т. 26.
12. *Основные* принципы безопасности атомных станций. Отчет междунар. консультативной группы по ядерной безопасности // Серия безопасности. INSAG – 3, Rev. 1 INSAG – 12. – 1975. – С. 53.
13. *Пампуро В. И.* Структурная информационная теория надежности систем. – Киев: Наук. думка, 1992. – 324 с.
14. *Пампуро В. И.* Метод разработки математических моделей управления экологической безопасностью объектов // Доп. НАН України. – 1999. – № 1. – С. 197–203.
15. *Pampuro V. I., Borisenko V. I.* Management of Individual Ecological Safety of Potentially Hazardous Object // The third American Nuclear International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2000), November 13–17, 2000. – Washington, D. C., 2000. – P. 707–722.

Институт электродинамики НАН Украины, Киев *Поступило в редакцию 19.03.2008*