УДК 629.162.658

СОВРЕМЕННАЯ МЕТОДОЛОГИЯ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ АЭС

В. И. Пампуро[1], В. И. Борисенко[2]

[1] *Институт геохимии окружающей среды НАН и МЧС Украины, Киев*
[2] *Институт проблем безопасности АЭС НАН Украины, Киев*

В основе современной методологии управления безопасностью АЭС лежит концепция максимальной безопасности при минимуме возможных затрат (МБМЗ) [1, 2]. Реализация этой концепции базируется на основных положениях, изложенных в работе.

Ключевые слова: управление безопасностью, вероятностный анализ безопасности, глубокоэшелонированная защита, виртуальная авария.

1. Современное управление безопасностью АЭС предполагает сочетание технической эффективности (обеспечения максимальной безопасности) с практической возможностью ее реализации на основе экономической эффективности (минимизацией суммарных затрат на безопасность и их оптимального распределения). Такое сочетание предполагает оптимальное управление безопасностью АЭС [3 - 6]. Оптимальное управление безопасностью АЭС, прежде всего, связано с обоснованием оптимального значения показателя риска аварии.

Необходимо подчеркнуть, что безопасность есть цель оптимального управления, а практические возможности определяют затраты на обеспечение безопасности. Минимизация затрат на безопасность является необходимым условием конкурентоспособности атомной энергетики. Взятый сам по себе тезис «максимальная безопасность» не имеет ни теоретического, ни практического смысла. В условиях конкуренции атомная энергетика может эффективно существовать только при условии обеспечения необходимой прибыли и себестоимости вырабатываемой энергии. В себестоимость входят и расходы на обеспечение безопасности, включая страхование. Иначе, необходимым условием практического обеспечения безопасности является минимизация затрат на нее. Принцип выбора оптимального значения показателя риска аварии показан на рис. 1.

Основные принципы концепции глубокоэшелонированной защиты (ГЭЗ) [7] «*предотвращение и ослабление аварий*», которым соответствует кривая *1* (см. рис. 1), являются недостаточными для оптимального управления безопасностью.

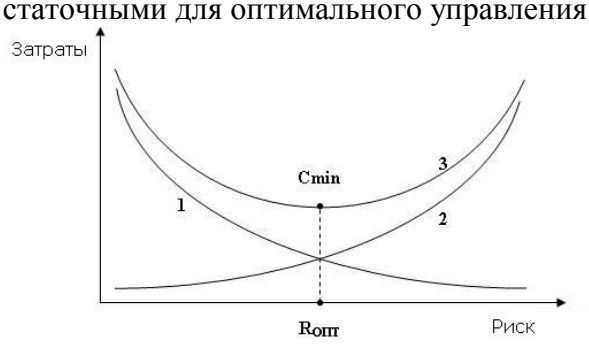


Рис. 1. Зависимость суммарных затрат на безопасность от показателя риска аварии:
1 – затраты на технологию предупреждения и ослабления аварии; *2* – затраты на страхование последствий возможной аварии; *3* – суммарные затраты на обе технологии *(1* и *2)*; C_{min} – минимальные суммарные затраты на безопасность; $R_{опт}$ – оптимальное значение показателя риска виртуальной аварией.

Из кривой *1* следует, что уменьшение значения риска аварии требует увеличения затрат. Согласно ей нельзя обосновать оптимальное значение показателя риска аварии, а также соответствующий ему минимум затрат на безопасность.

Концепция ГЭЗ стремится к предупреждению и ослаблению аварии, но не учитывает последствия аварии. Без такого учета невозможно разработать основы оптимального управления безопасностью при условии минимизации затрат на максимальную безопасность. Они включают в себя как затраты на предупреждение и ослабление аварии, так и затраты на страхование последствий возможной аварии.

Таким образом, концепция МБМЗ принципиально отличается от концепции ГЭЗ, так как в основе последней отсутствует методология экономической эффективности, а также принципы ее реализации методами оптимального управления безопасностью АЭС.

2. Оценка риска аварии согласно концепции ГЭЗ [7] производится с помощью вероятностной модели аварии. На этих методологически основополагающих положениях базируются методы анализа риска [8 - 10]. Погрешность такого постулата подробно рассмотрена в работах [6, 11, 12].

Теория вероятностей, как известно, изучает стохастические закономерности массы (совокупности) однотипных явлений (событий, объектов) в условиях статистической устойчивости. Условие статистической устойчивости для модели случайного события аварии означает постоянство частоты события аварии. Иначе, оно означает периодическую повторяемость обстоятельств и причин появления аварии на части объектов из всей совокупности. Поэтому принятие вероятностной модели события аварии теоретически равносильно постулированию вероятностной закономерности (т.е. априорной неизбежности) появления аварии в течение срока службы АЭС.

Основанное на вероятностной модели аварии, нормируемое допустимое значение частоты тяжелого повреждения активной зоны (АкЗ) равно 10^{-4} (10^{-5}) реактор/год [13]. Как показано в [11, 12], согласно нормированному значению вероятности тяжелой аварии 10^{-5} реактор/год, среднее значение времени плавления АкЗ $T^0 = 10^5$ лет. Это значение не имеет практического смысла. Действительно, плавление АкЗ возможно только при эксплуатации реактора. В связи с этим статистическое среднее значение времени плавления АкЗ T^0_{CT} не может быть больше срока эксплуатации АЭС τ. Срок эксплуатации АЭС τ измеряется десятками лет и меньше значения 10^2 лет. Поэтому всегда имеет место неравенство $T^0_{CT} \le \tau << T^0$. Следовательно, нормируемое допустимое значение вероятности риска тяжелой аварии 10^{-5} реактор/год и вытекающее из него значение среднего времени наступления аварии $T^0 = 10^5$ лет не имеют ни теоретического, ни, тем более, практического смысла.

Таким образом, постулирование вероятностной модели аварии (следовательно, и ее статистической закономерности) делает теоретически бесполезной любую концепцию обеспечения безопасности АЭС. Тогда концепция защиты теряет смысл, так как теоретически она не в состоянии устранить априори принятую статистическую закономерность аварии.

3. Управление безопасностью АЭС согласно концепции МБМЗ опирается на научном обосновании фундаментальных причин, которые лежат в основе предполагаемой (теоретически возможной, но практически не обязательной) аварии [1, 2, 12]. Необходимо учитывать две фундаментальные причины, которые лежат в основе априорной возможности аварии и не позволяют полностью исключить ее.

Первая фундаментальная неустранимая причина связана с принципиальной ограниченностью наших знаний и вытекающего из этого отсутствия априорных знаний о природе локальных (статистически неустойчивых, виртуальных) аварий.

Теоретически нельзя исключить возможность появления виртуальной аварии. Возможна виртуальная авария, для которой отсутствуют статистические закономерности в настоящем, и, в принципе, их нельзя определить в будущем. Поэтому всегда нужен оптимальный компромисс между технологией предупреждения и ослабления аварии (для которой известны детерминистические и стохастические закономерности), с одной стороны, и страхованием (технологией устранения последствий) виртуальной аварии, с другой стороны.

В концепции МБМЗ учитывается технологически наиболее важная *вторая фундаментальная неустранимая причина виртуальной аварии.* Она вызвана ограниченной точностью и надежностью как систем управления и защиты от аварии, так и технологией эксплуатации (в частности, ограниченной надежностью оператора). Эти подсистемы никогда не будут идеальными из-за ограниченной точности их изготовления и ограниченной надежности технологии эксплуатации, связанной с человеческим фактором.

Таким образом, в отличие от концепции ГЭЗ, в концепции МБМЗ учтены фундаментальные постоянно действующие причины возможности появления виртуальной аварии. Без учета и минимизации влияний этих причин на надежность АЭС невозможно обосновать пути качественного повышения безопасности АЭС с помощью наукоемких технологий.

4. Управление безопасностью АЭС *в условиях отсутствия закономерностей аварии* является принципиально новым положением, впервые использованным в концепции МБМЗ [1, 2, 12]. Это положение объясняется отсутствием статистически устойчивых данных о тяжелых авариях, с одной стороны, и неприемлемостью постулата о статистической устойчивости аварии как теоретического обоснования статистической закономерности (неизбежности) аварии на АЭС, с другой стороны. Это управление основывается на понятии о виртуальной аварии.

Виртуальная авария (*событие виртуальной аварии Ф*) – такая предполагаемая авария, для которой невозможно установить закономерности (повторяемость причин и следствий), которая гипотетически возможна (теоретически не может быть исключена) из-за двух рассмотренных выше ее фундаментальных причин, но *практически необязательна*.

В основе определения виртуальной аварии лежит понятие *возможности аварии.*

Возможность аварии априори предполагаемое событие (последовательность событий как предполагаемых причин аварии), которое не имеет априори устойчивых статистических данных появления этого события. Теоретически это событие можно трактовать как непустое множество, вероятность которого равна нулю.

Понятие *возможности* имеет принципиально отличное значение от понятия *случайность*. Теоретически *случайность* – есть статистическая закономерность, учитывающая свойство массы однотипных элементов (явлений) в условиях статистической устойчивости.

Статистическая устойчивость определяет физические законы (причины), которые определяют экспериментальные условия проявления случайности.

Анализ возможностей аварии является основополагающим в обеспечении безопасности. Этот анализ позволяет учесть причины, которые могут привести к аварии в условиях отсутствия ее закономерности. Он служит основой для разработки технологии предупреждения аварии. В частности, на его основе разрабатываются симптомно-ориентированные инструкции (СОИ) для предупреждения аварии. По сути метод дерева событий также содержит совокупность возможностей аварии, из которых эксперт выбирает наиболее значимые [8 - 10].

Событие виртуальной аварии *Ф* не является статистически устойчивым, оно является априори возможным в связи с наличием предполагаемых причин. Оно не может быть определено так, как это можно сделать для случайного события в рамках теории вероятностей. Это вызывает определенные трудности построения теории управления безопасностью по критерию виртуальной аварии. Событие виртуальной аварии можно очертить, рассматривая предполагаемые причины его появления. Соответствующий подход к определению возможности виртуальной аварии будет рассмотрен ниже.

В результате теоретического положения о виртуальной аварии, тяжелая авария из известной категории статистически закономерного события аварии, принятой в концепции ГЭЗ, переходит в категорию теоретически *априори возможного*, но практически необязательного события. Иначе, *возможность аварии нельзя теоретически исключить полностью, но нельзя также утверждать ее статистическую закономерность*. Это качественно меняет подход к пониманию природы тяжелой аварии и к методам ее предупреждения. В таком подходе вся исходная информация для управления безопасностью черпается из работоспособного состояния объекта, без информации о статистической закономерности аварии.

Необходимо рассматривать все варианты возможности аварии, включая внутренние и внешние экстремальные воздействия. Во всех случаях следует оценивать возможность аварии из-за ограниченной точности предупреждения и ослабления аварии, а также вероятные затраты на устранение последствий возможной (виртуальной) аварии.

Проблема управления при неполных знаниях уже рассматривалась, например в кибернетике согласно энтропийной оценке вероятности аварии. Однако положение о виртуальной аварии требует принципиально нового подхода, который обусловлен отсутствием знаний закономерностей аварии.

Целью управления безопасностью, как известно, является исключение аварии из эксплуатации АЭС. Следовательно, в теории безопасности понятие аварии не должно иметь толкование практической естественности и теоретической неизбежности. Оно не должно быть подобным толкованию понятия отказа в теории надежности, которое рассматривается как практически естественное и теоретически неизбежное событие. Подход к понятию отказа в теории надежности нельзя автоматически переносить на понятие аварии в теории безопасности, как это имеет место в классической теории безопасности [8 - 10]. Такой подход теоретически означает неизбежность аварии. Поэтому понятие виртуальной аварии является естественным теоретическим положением, которое исключает теоретическую неизбежность аварии и согласуется с целью управления безопасностью.

5. Использование закономерности технологии предупреждения аварии (согласно концепции МБМЗ) лежит в основе оптимального управления безопасностью АЭС. Предупреждение виртуальной аварии на основе этих закономерностей сводится к недопущению перехода АЭС в аварийное состояние.

Очевидно, что управление безопасностью (как любое априорное управление) можно осуществить, только используя *закономерности*. Следуя методологии виртуальной аварии (когда отсутствует стохастическая закономерность аварии), наиболее естественной закономерностью обеспечения безопасности, которую целесообразно использовать для управления безопасностью АЭС, является закономерность технологии предупреждения аварии. Эта технология достаточно хорошо разработана и постоянно совершенствуется за счет наукоемких технологий. Поэтому оптимальное управление безопасностью АЭС для модели *виртуальной* аварии целесообразно осуществлять путем оптимизации, прежде всего технологии предотвращения аварии с целью недопущения плавления АкЗ. Оно заключается в минимизации влияния на безопасность двух рассмотренных ранее фундаментальных причин.

С целью предотвращения аварии следует использовать интервал *запаса управляемости безопасностью АЭС*. Этот интервал является одним из основных понятий концепции МБМЗ [1, 2]. Этот запас находится на границе устойчивого безопасного состояния АЭС. Он определяет зону потенциальной опасности перехода АЭС из работоспособного в аварийное состояние за счет неустойчивого управления, вызванного погрешностью технологии предупреждения аварии.

Смысл интервала запаса управляемостью АЭС заключается в переходе от концепции ГЭЗ (включающей в себя предупреждение и ослабление аварии) к идее предупреждения аварии, как основополагающей в управлении безопасностью. Это положение полностью согласуется с международным нормативным руководством по повышению эксплуатационной безопасности [14]. При этом идея ослабления аварии также используется в связи с тем, что теоретически нельзя исключить возможность виртуальной аварии.

С позиции обеспечения безопасности АЭС, предупреждение тяжелой аварии, в первую очередь, связано с предупреждением плавления АкЗ. Если в качестве одного из параметров управляемости безопасностью АЭС принять, например, температуру теплоносителя в АкЗ, то интервал запаса управляемости определим как

$$\Delta_1 = [z_1, z_2] , \qquad (1)$$

где z_2 - верхняя граница интервала, после которой наступает интенсивное парообразование теплоносителя и, как следствие, нарушение теплообмена. Нижняя граница z_1 выбирается из условия запаса по температуре, примерно в 20 ^{o}C. Интервал находится в пределах закономерности технологии предупреждения и ослабления аварии. Длина W_1 интервала запаса управляемости $\Delta_1 = [z_1, z_2]$ определяется как $W_1 = z_2 - z_1$.

В общем случае АЭС интервал (1) определяет границы физической величины (нейтронного потока, давления, расхода, активности и др.), по которой оценивают безопасность и/или ведут управление безопасностью.

Обеспечение приведенного запаса по температуре и соответствующего интервала $\Delta_1 = [z_1, z_2]$ недостаточно для управления безопасностью. С целью минимизации риска аварии и определения соответствующего запаса по показателю риска аварии, необходимо обеспечить запас по значению показателя риска аварии. Чтобы обеспечить такой запас, следует использовать другую форму записи интервала запаса управляемости. Он определяется размахом значений показателя риска R для предаварийного состояния

$$\Delta_2 = [R_1, R_{10}\ ], \tag{2}$$

где R_{10} - начальное значение показателя риска перехода АЭС в аварийное состояние (без учета запаса на погрешность управления); R_1 - уточненное новое значение показателя риска перехода АЭС в аварийное состояние (нижняя граница показателя риска перехода в предаварийное состояние).

Уточненное значение показателя риска перехода АЭС в аварийное состояние R_1 определяет вероятность события попадания температуры теплоносителя η в интервал запаса управляемости, т.е. при условии ($z_2 \geq \eta \geq z_1$).

Длина интервала запаса управляемости $\Delta_2 = [R_1, R_{10}\ ]$ определяется как

$$W_2 = R_{10} - R_1 \tag{3}$$

Эта длина выбирается так, чтобы ее значение было равно наиболее вероятному размаху W_2 значений случайной погрешности χ технологии предупреждения аварии.

Соответственно значение R_1 на длину W_2 меньше начального показателя риска R_{10}:

$$R_1 = P(z_2 \geq \eta > z_1) = R_{10} - W_2, \tag{4}$$

$$R_{10} = P(\eta > z_2). \tag{5}$$

Здесь $(\eta > z_2)$ - критерий отказа технологии предупреждения виртуальной аварии.

Обычно $R_{10} \leq .10^{-4}$. Уменьшение начального значения показателя риска R_{10} достигается за счет соответствующего увеличения надежности системы предупреждения аварии.

Таким образом, запас управления безопасностью состоит как в обеспечении интервала запаса по температуре $\Delta_1 = [z_1, z_2]$, так и в уменьшении начального значения показателя риска R_{10} на длину интервала запаса управляемости W_2 за счет увеличения надежности систем предупреждения аварии и перехода к устойчивому управлению безопасностью [1, 2, 12]

Подчеркнем, что устойчивое управление безопасностью АЭС осуществляется в пределах интервала безопасности $\exists_1 = [0, z_1]$, верхняя граница которого равна нижней границе z_1 интервала запаса управляемости безопасностью АЭС $\Delta_1 = [z_1, z_2]$. При этом значение показателя риска виртуальной аварии должно находиться в пределах интервала безопасности $\exists_2 = [0, R_1]$, которое обеспечивается за счет соответствующего повышения надежности систем предупреждения аварии.

Положение о первостепенном значении принципов предупреждения аварии в управлении безопасностью экологически опасного объекта (ЭОО) полностью согласуется с методологией комплексной системы управления качеством [14].

6. Как было отмечено во втором положении, нормируемое допустимое значение частоты тяжелого повреждения АкЗ 10^{-5} реактор/год не имеет практического смысла. Согласно концепции МБМЗ теория управления безопасностью АЭС основывается на конструктивных принципах, позволяющих оценивать безопасность по реальным контролируемым данным. С этой целью используются максимально возможное значение дозы всей совокупности продуктов деления и допустимое количество выбросов, определяемое соответствующей норма-

тивно-технической документацией и, в частности, НРБУ-97/Д-2000 [15]. В работах [12, 16] приведено подробное обсуждение и обоснование максимально допустимого значения показателя риска экологической опасности

$$R_M \le q/h, \tag{6}$$

где q – максимальное значение допустимой согласно НРБУ-97/Д-2000 [15] дозы выбросов, h - максимальное значение дозы всей совокупности продуктов деления.

Расчеты максимально допустимого значения показателя риска экологической опасности согласно формуле (6) могут использоваться на любых этапах жизненного цикла обеспечения безопасности ЭОО, включая АЭС. Особо формула (6) удобна при определении максимально допустимого значения показателя риска экологической опасности на этапе проектирования, когда отсутствуют эксплуатационные данные об авариях [12, 16]

7. Согласно концепции МБМЗ управление безопасностью требует соответствующей теории [4, 12, 18, 19]. Необходимость теории управления надежностью безопасностью вызвана непригодностью существующих методов анализа надежности безопасности для управления надежностью и безопасностью ЭОО. Покажем эту необходимость на примере анализа методологических ограничений метода дерева событий, наиболее распространенного метода анализа риска аварии [8, 9].

Дерево событий представляет собой логический метод перебора всех возможных аварийных последовательностей (путей графа событий). Совокупность путей определяет варианты события возможной аварии $\overline{\varepsilon_{\text{п}}}$, вызванной исходным событием $\overline{\varepsilon_A}$ с учетом надежности подсистем, влияющих на развитие аварии. На основе экспертного анализа, дерево, состоящее из m исходных вариантов аварии, делится на две части, события которых соответственно Н и $\overline{\text{H}}$. Сумма этих событий равна достоверному событию I:

$$\text{H} + \overline{\text{H}} = \text{I}. \tag{7}$$

Событие Н 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 $\overline{\text{H}}$ и исключаются как те, которые не могут привести к аварии. Тем самым теоретически постулируется несовместность исходного события $\overline{\varepsilon_{\text{A}}}$ с событием исключенной части $\overline{\text{H}}$, т.е. произведение $\overline{\varepsilon_{\text{A}}}\,\overline{\text{H}} = \varnothing$. Это замечание имеет важное значение для последующего анализа методологических ограничений метода дерева событий.

Вычисляется вероятность события риска аварии $R = P(\overline{\varepsilon_{\text{п}}})$, равного сумме вероятностей несовместных событий путей (аварийных последовательностей) P_B, по формуле

$$R = R_A \sum_{B \in T_B} P_B, \tag{8}$$

где T - множество индексов вариантов, входящих в событие Н. При этом не учитывается изменения значений вероятностей P_B, что необходимо сделать при переходе к преобразованному (упрощенному) графу в связи с условием $\overline{\varepsilon_{\text{A}}}\,\overline{\text{H}} = \varnothing$.

Ключевыми к пониманию основного методологического ограничения метода событий являются положения, вытекающие из условия $\overline{\varepsilon_{\text{A}}}\,\overline{\text{H}} = \varnothing$. Они состоят в следующем.

Когда анализируется зависимость события аварии $\overline{\varepsilon_{П}}$ от исходного события $\overline{\varepsilon_A}$

$$\overline{\varepsilon_{П}} = H\overline{\varepsilon_A} \tag{9}$$

с учетом несовместности события $\overline{\varepsilon_A}$ и события исключенной части графа $\overline{H}$, т.е. справедливо равенство $\overline{\varepsilon_A}\,\overline{H} = \varnothing$, тогда при наступлении исходного события $\overline{\varepsilon_A}$, т.е. при условии $\overline{\varepsilon_A} = I$, событие исключенной части дерева событий $\overline{H}$ является невозможным:

$$\overline{H} = \varnothing. \tag{10}$$

Из выражений (7) и (10) следует, что событие H достоверное: H = I.

С учетом последнего равенства и выражения (9) следует, что событие аварии равно исходному событию [17]

$$\overline{\varepsilon_П} = \overline{\varepsilon_A}. \tag{11}$$

Таким образом, при корректном теоретическом анализе метод дерева событий не учитывает влияния систем управления и защиты на безопасность АЭС.

Отсутствие анализа методологических ограничений метода дерева событий приводит к ошибочному анализу безопасности. Это наглядно видно на широко используемом классическом примере анализа тяжелой аварии АЭС с потерей теплоносителя [8, 9]. Из анализа этого примера следует, что событие аварии равно исходному событию [17].

Согласно логико-вероятностному методу анализа надежности и безопасности, *когда справедлива вероятностная модель аварии*, 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. Логически из этого следует, что авария может наступить только тогда, когда откажут обе компоненты. Соответственно событие аварии

$$\overline{\varepsilon_П} = \overline{\varepsilon_{ji}}\ \overline{\varepsilon_{ij}}, \tag{12}$$

и, соответственно, для независимых событий вероятность аварии

$$P(\overline{\varepsilon_П}) = P(\overline{\varepsilon_{ji}})P(\overline{\varepsilon_{ij}}). \tag{13}$$

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]

$$P_A = \frac{P(\overline{\varepsilon_{ji}})P(\overline{\varepsilon_{ij}})}{1 - P(\varepsilon_{ij})P(\overline{\varepsilon_{ji}})}. \tag{14}$$

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

$$P(\overline{\varepsilon_{ji}})P(\overline{\varepsilon_{ij}}) < \frac{P(\overline{\varepsilon_{ji}})P(\overline{\varepsilon_{ij}})}{1 - P(\varepsilon_{ij})P(\overline{\varepsilon_{ji}})}. \tag{15}$$

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 $P(\overline{\varepsilon_{ji}})P(\overline{\varepsilon_{ij}})$ (13) мало отличается от точного значения, полученного согласно формуле (14): погрешность оценки составляет около 0,1 %. Однако, в преобразованном дереве событий согласно формуле (8) 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 (8) значение показателя риска, в лучшем случае, можно рассматривать только как верхнюю оценку показателя риска аварии.

Следует подчеркнуть, что анализ риска аварии с помощью метода событий связан с проблемой размерности. Так, для системы с *n* элементами исходное дерево содержит 2^n пу-

тей. Например, для структурной схемы управления балансом нейтронной и тепловой мощностей, содержащей 18 элементов, соответствующее ей дерево событий должно содержать 260000 путей (ветвей) [20]. 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 превышать точное значение, в соответствии с (14).

Метод дерева событий принципиально непригоден для реализации структурной оптимизации и поиска слабого звена в системе управления надежностью (безопасностью) АЭС. Это объясняется как уже отмеченной проблемой размерности, так и невозможностью структурного анализа систем без избыточности, что более подробно рассмотрено в [11, 18 - 20]. 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 ядерной энергетике. Необходимая исходная информация для анализа безопасности 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 ее последствия, замыкая тем самым контур управления безопасностью. Дерево событий не содержит контуров управления безопасностью. Оно позволяет лишь упорядочить анализ безопасности АЭС, расчленив общую задачу анализа на части;

во-вторых, метод дерева событий имеет неустранимые методологические ошибки, исключающие корректный анализ безопасности АЭС. В целом он позволяет получить приближеннее оценки сверху показателя риска, в случае, если справедлива ее вероятностная модель, без учета значения погрешности приближения. Лежащий в основе метода событий качественный подход, основанный на знаниях специалиста, не позволяет учесть основные скрытые причины виртуальной аварии (неполноту знаний и погрешность технологии обеспечения безопасности);

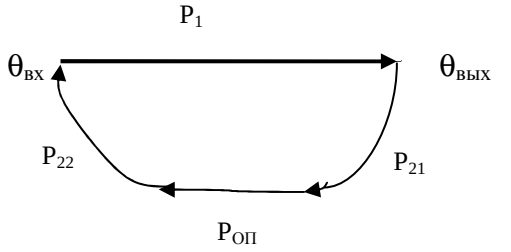
в-третьих, метод дерева событий непригоден для оптимального управления безопасностью из-за погрешности постулирования вероятностной модели аварии, а также из-за проблемы размерности и отсутствия контура управления безопасностью. В целом он является качественным методом оценки показателя риска аварии на АЭС.

Другие ограничения метода событий приведены в [20].

8. Суть проблемы структурного анализа состоит в том, что в классической теории анализа безопасности (в частности, в методе дерева событий) и в классической теории надежности отсутствует необходимая информация для структурного анализа систем без избыточности. В этих теориях используется только свойства элемента в виде событий его безотказности или отказа. Законы связи элементов в системе без избыточности отсутствуют. В системной теории управления безопасностью кроме событий безотказности и отказа используются законы связи событий потоков информации [11, 18 - 20]. Связь событий потоков информации элементов с событиями потоков информации системы определяет все возможные виды соединений элементов. В многообразие видов входят последовательное, совокупность параллельных, смешанных соединений элементов, включающее в себя как частный случай известные в классических теориях надежности и безопасности соединения элементов случай, когда события потоков информации считаются достоверными. Разработанное в структурной теории управления соединение по схеме обратной стохастической связи послужило основой теории управления надежностью и безопасностью. Кроме того, совокупность указанных видов соединения элементов позволяет разработать математическую модель любой системы (как с избыточностью, так и, что особенно важно, без избыточности). В результате снята

проблема размерности. Например, для системы с n элементами дерево событий содержит 2^n путей. Так, для структурной схемы, содержащей 18 элементов, соответствующее ей дерево событий содержит 260000 путей [20]. Из этого множества путей (вариантов возможной аварии) эксперт должен выбирать те, которые, по его мнению, могут привести к аварии. Преимущество системной теории, которое наглядно иллюстрируется данным примером, очевидное. Согласно системной теории управления, любая система описывается числом уравнений $m \le (n+1)$ и имеет одно решение, которое дает однозначную оценку вероятности риска, не требующую экспертного анализа. Это иллюстрируется и примером, приведенным в [9, 17, 22, 23].

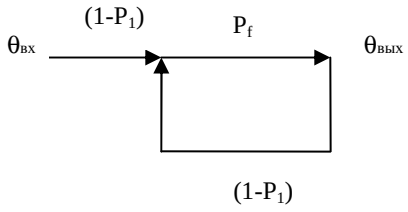
2.1. Модель надежности с оператором ($P_{ОП}$) в контуре управления



$$P(\theta_{вых}) = \frac{P_1}{1 - P_{21} P_{ОП} P_{22} (1 - P_1)} P(\theta_{вх})$$

$$(P_{ОП} < 0{,}9) \rightarrow P_{21} P_{ОП} P_{22} \approx P_{ОП}$$

2.2. Модель анализа риска с оператором в контуре управления

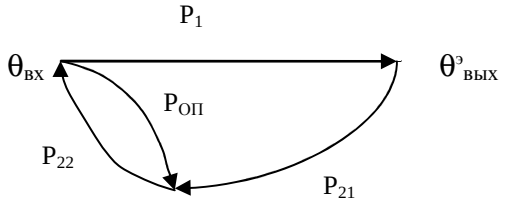


$$\overline{\theta}_{вых} = \theta_{вх} - \theta_{вых}$$

$$P_f = 1 - P_{21} P_{ОП} P_{22}$$

$$P(\overline{\theta}_{вых}) = \frac{(1 - P_1) P_f}{1 - P_{21} P_{ОП} P_{22} (1 - P_1)} P(\theta_{вх})$$

2.3. Модель надежности с оператором в контуре контроля

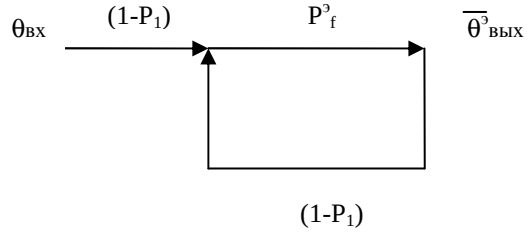


$$P(\theta^{э}_{вых}) = \frac{P_1}{1 - P_{21} P^{э}_{22} (1 - P_1)} P(\theta_{вх})$$

$$P^{э}_{22} = \frac{P_{22}}{1 - P_{ОП} (1 - P_{22})}$$

$$P^{э}_{22} >> P_{ОП} P_{22}$$

2.4. Модель анализа риска с оператором в контуре контроля



$$\overline{\theta}^{э}_{вых} = \theta_{вх} - \theta^{э}_{вых}$$

$$P^{э}_{f} = 1 - P_{21} P^{э}_{22}$$

$$P(\overline{\theta}^{э}_{вых}) = \frac{(1 - P_1) P^{э}_{f}}{1 - P_{21} P^{э}_{22} (1 - P_1)} P(\theta_{вх})$$

$$P(\overline{\theta}^{э}_{вых}) << P(\overline{\theta}_{вых})$$

Рис. 2. Анализ влияния оператора в контуре управления надежностью и безопасностью АЭС.

Рассмотрим достаточно простой, но имеющий принципиальное значение пример анализа слабого звена [21]. Будем анализировать структуру, состоящую из объекта и подсистемы управления безопасностью. Согласно системной теории управления безопасностью, информационный граф событий структуры приведен на рис. 2.1. Структура состоит из объекта 21 (активной зоны АЭС), вероятность безотказной работы которого P_1, и подсистем управ-

ления, которые вместе с объектом образуют контур управления. Система управления состоит из следующих элементов:

подсистемы диагностирования, вероятность безотказной работы которой P_{21};

оператора, вероятность безотказной работы которого $P_{ОП}$;

подсистемы регулирования - дистанционного расхолаживания активной зоны, вероятность безотказной работы которой P_{22}.

Элементы структуры описываются событиями работоспособности ε_{21}, ε_{32}, ε_{43}, ε_{14} соответственно, где вероятности

$$P(\varepsilon_{21}) = P_1, \quad P(\varepsilon_{32}) = P_{21}, \quad P(\varepsilon_{43}) = P_{ОП}, \quad P(\varepsilon_{14}) = P_{22}.$$

Из-за ограниченной надежности оператора система управления надежностью, рис. 2.1 (безопасностью, рис. 2.2) неэффективна.

В результате изменения структуры системы управления надежностью, рис. 2.3 (безопасностью, рис. 2.4) , надежность системы управления качественно повышается, что, в свою очередь, ведет к повышению надежности и безопасности АЭС в целом.

Следует заметить, что обосновать повышение надежности и безопасности АЭС за счет структурной оптимизации системы управления с помощью метода дерева событий принципиально невозможно, так как дерево событий зависит только от количества элементов, и поэтому оно одинаково для всех рассмотренных структур, приведенных на рис. 2. Эту задачу нельзя решить и с другими методами анализа надежности и безопасности, которые не учитывают событий потоков информации.

Учитывая изложенное, заметим, что корректный структурный анализ возможен только с учетом событий потоков информации, который корректно изложен в теории управления надежностью и безопасностью [12, 18, 20, 22].

СПИСОК ЛИТЕРАТУРЫ

1. *Пампуро В.И.* Максимальная безопасность при минимуме возможных затрат // Доп. НАН України. - 2006. - № 5. - С. 185 - 190.
2. *Пампуро В.И.* Концепция максимальной безопасности АЭС при минимальных затратах // Двадцать лет Чернобыльской катастрофы. Взгляд в будущее. ТЗ-22. 24-26.04.06. Киев, Украина. (Сб. докл.)
3. *Пампуро В.И.* Концепция тяжелой аварии и верхняя оценка ее риска // Доп. НАН України. - 2001. - № 7. - С. 185 - 190.
4. *Пампуро В.И.* Многокритериальная оптимизация технологии предупреждения экологической катастрофы из-за тяжелой аварии объекта // Доп. НАН України. - 2000. - № 10. - С. 200 - 206.
5. *Пампуро В.И.* Оптимизация страхования риска виртуальной тяжелой аварии // Доп. НАН України. - 2002. - № 3. - С. 198 - 204.
6. *Пампуро В.И.* Оптимальное управление безопасностью АЭС и вероятностный анализ риска // Доп. НАН України. - 2001. - № 5. - С. 185 - 191.
7. *Основные* принципы безопасности атомных станций. Отчет Международной консультативной группы по ядерной безопасности. Серия безопасности 75. INSAG-3, Rev.1 INSAG-12
8. *Хенли Э.Д., Кумато Х.* Надежность технических систем и оценка риска.- М.: Машиностроение, 1979. - 528 с.
9. *Уивер Л.* Риск от аварии на АЭС с легководяными реакторами // Безопасность ядерной энергетики. – М.: Атомиздат, 1980. - С. 114 - 133.
10. *Швыряев Ю. В.* Вероятностный анализ безопасности атомных станций. Методика выполнения. - М: ИАЭ им. И. В. Курчатова, 1992. - 265 с.
11. *Пампуро В.И.* Управление безопасностью объектов атомной энергетики согласно концепции виртуальной аварии // Доп. НАН України. - 2007. - № 11. - С. 180 - 185.
12. *Шестопалов В.М, Пампуро В.И., Шибецкий Ю.А.* Проблемы оптимального управления безопасностью геологического захоронения радиоактивных отходов. – К., 2008. - 172 с.
13. *Загальні* положення безпеки атомних станцій. НП 306.2.141-2008.

14. *Руководство* по управлению предупреждения происшествий (путь к повышению эксплуатационной безопасности) // Серия безопасности № 75. - 1991.
15. *Нормы* радиационной безопасности Украины. НРБУ-97/Д-2000.
16. *Пампуро В.И.* Принцип необходимой оптимальной управляемости безопасностью обращения с радиоактивными отходами // Доп. НАН України. - 2003. - № 6. - С. 1182 - 187.
17. *Пампуро В.И.* Методологические ограничения метода дерева событий // Доп. НАН України. - 2008. - № 12. - С. 161 - 165.
18. *Пампуро В.И.* Метод разработки математических моделей управления экологической безопасностью объектов // Доп. НАН України. - 1999. - № 1. - С. 197 - 203.
19. *Пампуро В.И.* Структурная информационная теория надежности систем. – К.: Наук. думка, 1992. – 324 с.
20. *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., p. 707 - 722.
21. *Пампуро В.И.* Анализ эффективности человеческого фактора в технологии оптимального управления экологической безопасностью человеко-машинных систем // Кибернетика и вычислительная техника. - 2002. - Т. 136. - С. 32 - 54.
22. *Ершов Г.А., Козлов Ю.И., Татусьян А.О.* Сравнительный анализ способов моделирования безопасности АЭС с помощью метода ДС-ДО, GO-метода и общего логико-вероятностного метода. Материалы конференции «Практика разработки ВАБ и использования их результатов на действующих и вновь проектируемых АЭС». Москва, 18 - 21 ноября 2002 г.- М.: Атомэнергопроект, 2002.
23. *Пампуро В.И.* Управление безопасностью объектов атомной энергетики согласно концепции виртуальной аварии // Доп. НАН України. - 2007. - № 11. - С. 198 - 204.

СУЧАСНА МЕТОДОЛОГІЯ КЕРУВАННЯ БЕЗПЕКОЮ АЕС

В. І. Пампуро, В. І. Борисенко

В основі сучасної методології керування безпекою АЕС лежить концепція максимальної безпеки при мінімумі можливих витрат. Реалізація цієї концепції базується на основних положеннях, викладених у даній роботі.

Ключові слова: керування безпекою, імовірнісний аналіз безпеки, глибокоешелонований захист, віртуальна аварія.

MODERN METHODOLOGY OF MANAGEMENT OF NPP SAFETY

V. I. Pampuro, V. I. Borysenko

The basis of modern methodology of management of NPP safety - is the concept maximum safety with minimal cost. This concept is based on the main provisions contained in the work.

Keywords: safety management, probabilistic safety analysis, in-depth protection, virtual accident.

Поступила в редакцию 16.11.09