ДОПОВІДІ
НАЦІОНАЛЬНОЇ
АКАДЕМІЇ НАУК
УКРАЇНИ

12 • 2009

ЕКОЛОГІЯ

УДК 629.162.658

В. И. Пампуро

Структурный анализ систем управления безопасностью

(Представлено академиком НАН Украины В. П. Кухарем)

Надані основні положення структурного аналізу надійності систем керування безпекою АЕС згідно з інформаційною теорією керування. Викладена теорія мінімізації похибки оператора шляхом оптимізації структури систем керування безпекою. Дано теоретичне обгрунтування концепції глибокоешелонованого захисту.

Структурный анализ подсистем управления безопасностью экологически опасных объектов (ЭОО) является важной составляющей теории обеспечения экологической безопасности человеко-машинных систем (объектов). Он включает в себя анализ влияния человеческого фактора на безопасность ЭОО, анализ надежности и безопасности ЭОО с помощью глубокоэшелонированной защиты, анализ влияний надежности элемента на надежность ЭОО, связь структурного анализа с оптимизацией и др.

Теория структурного информационного анализа безопасности ЭОО является обобщением идей анализа, заложенных в классических методах анализа аналоговых систем, а также в классических теориях надежности и безопасности [1, 2]. Принципы построения математической модели структуры детально разработаны в классических технических приложениях. Соответствующие методы построения модели аналоговой системы, основанные на анализе видов соединения ее элементов, рассмотрены в целом ряде структурных детерминистических теорий. К ним относятся такие, как теория электрических цепей, теория автоматического управления, теория информационно-измерительных систем, теория механических систем, теория электронных и радиотехнических систем, теория транспортных задач (связи, электрических сетей и т. п.), теория электрических цепей и т. д. [1, 3, 4].

Методологически структурные *детерминистические* методы построения математической модели аналоговой системы можно разбить на два типа.

Общими для теорий первого типа являются методы построения математических моделей аналоговых линейных систем на основе детерминистических законов связи материальных потоков — вещественных компонент. Общим положением для обоснования любых видов соединений элементов электрической цепи является общая энергетическая основа: по каждому элементу любых соединений проходит поток электрической энергии, связанный

определенными законами с потоком электрической энергии соединения. Примерами таких законов являются законы Кирхгофа, законы связи потоков товаров в транспортных задачах, законы связи потоков энергии в электрических сетях, законы связи потоков сообщений в сетях связи и т. п. В общем случае виды соединений включают в себя последовательное, параллельное, смешанное соединение элементов и соединение элементов по схеме обратной связи. Полный набор видов соединений элементов имеет теория электрических цепей. В ней имеются все виды соединений: последовательное, параллельное, смешанное и по схеме обратной связи. Поэтому теория электрических цепей выступает как методологическая основа методов построения математической модели аналогового объекта.

Второй тип структурного детерминистического подхода к построению математической модели линейных аналоговых систем с однонаправленными элементами содержится в теории автоматического управления. Эта теория рассматривает системы управления, состоящие из объекта управления и подсистем, выполняющих функцию управления. Как правило, объект управления и подсистемы энергетически отличаются друг от друга. Примером системы автоматического управления может быть механический аналоговый объект управления и электронная подсистема управления. Согласно теории автоматического управления структура объекта рассматривается как система управления с многоконтурной обратной связью. Она представляет собой структуру из контуров обратной связи, элементы которых (объект управления и подсистема управления) характеризуются разнородными вещественными потоками. В соответствии с такими принципами построения модели аналоговой системы, теория автоматического управления не исследует связь разнородных вещественных потоков. Поэтому в ней отсутствуют понятия последовательного, параллельного и смешанного соединения элементов, как это имеет место, например, в теории электрических цепей.

В прикладных теориях анализа сложных аналоговых систем используется как теория цепей, так и теория автоматического управления. Наиболее полно теория автоматического управления вошла составной частью в кибернетику для анализа систем как неживой, так и живой природы.

Качественно новый подход, отличный от уже рассмотренного детерминистического построения математической модели аналогового объекта, положен в основу классических теорий надежности и безопасности [4–7]. Он объясняется необходимостью построения математических моделей для объектов с избыточностью и восстановлением. Рассмотренные ранее теории не позволяют решить эту задачу. Эта задача решается в классических теориях надежности и безопасности абстрактно (без учета законов связи потоков элементов). В методах теории надежности и безопасности, применяемых для построения структуры объекта с избыточностью или с восстановлением, отсутствуют понятия потоков элементов и соответствующих им видов связи элементов. В частности, отсутствует соединение по схеме обратной связи. В классических теориях надежности и безопасности для построения математических моделей объектов с избыточностью и восстановлением используются математические правила алгебры логики и теория марковских цепей. Согласно алгебре логики, используемой в классических методах теории надежности, математическая модель работоспособного состояния любой системы без избыточности представляется как последовательное соединение ее работоспособных элементов. Это соединение основывается на законе логического произведения высказываний, согласно которому условие безотказности системы без избыточности может выполняться только при совместном выполнении (т. е. при логическом произведении) условий безотказности всех элементов. При таком принципе построения модели безотказности системы без избыточности не учитывается разная степень

влияния каждого элемента на безотказность системы без избыточности. Тем самым постулируется одинаковая степень влияния безотказности любого элемента на безотказность системы, из чего следуют равные оптимальные требования к показателям безотказности элементов при заданном требовании на безотказность системы. В конечном счете это ведет к проблеме размерности, неразрешимой в рамках классической теории надежности. На основе теории марковских цепей разработаны методы учета состояний системы и перехода из одного состояния в другое. Число состояний системы велико. При этом также нет возможности учесть разную степень влияния каждого элемента на безотказность системы без избыточности в зависимости от количества потока информации, что в конечном счете ведет к проблеме размерности.

В целом перечисленные методы не учитывают отличия разных элементов системы, выполняющих различные функции в зависимости от проходящих по ним потоков информации. Они не позволяют построить модели систем без избыточности, отражающих индивидуальные особенности каждой системы с учетом количества проходящих по элементам потоков информации, а также решить проблему размерности, состоящую в следующем. Как отмечалось ранее, модель системы без избыточности представляется последовательным соединением элементов. Число элементов для больших систем $n \succ 10^5$. Чтобы выполнить заданное требование к вероятности безотказности системы p_c, необходимо обеспечить значение вероятности безотказности элемента $p_э \geqslant \sqrt[n]{p_c}$. Обычно требуемое значение вероятности $p_с \geqslant 1-10^{-4}$, тогда требуемое значение вероятности $p_э \geqslant \sqrt[n]{(1-10^{-4})}$. Обеспечить это требование при числе элементов $n \succ 10^5$ практически невозможно.

Чтобы снять проблему размерности, необходимо учесть количество потока информации, проходящего через элемент. Анализ связи потоков информации элементов с потоками информации системы изложен в информационной теории управления надежностью и безопасностью [1, 2]. Для построения моделей управления надежностью и безопасностью с учетом информационной значимости каждого элемента системы в информационной теории управления используются понятия события работоспособности ε_{qr} (события отказа $\overline{\varepsilon}_{qr}$) элемента qr, а также событие потока информации θ_{qr}, проходящего через элемент qr. Использование событий потоков информации качественно расширяет возможности теорий надежности и безопасности. Путем анализа связи потоков информации элементов с потоками информации системы можно обосновать все виды соединений (включая схему обратной связи) элементов и построить математическую модель как надежности, так и безопасности любой системы.

Как отмечалось, вид соединения элементов в информационной структурной схеме (вид соединения координатных ребер графа событий) зависит от законов связи их потоков информации. Анализ вида соединений элементов qr сводится к анализу операций над событиями потоков информации θ_{qr}, поступающих на элементы qr. Все виды соединений элементов основываются на следующем *законе сохранения потоков информации:*

Сумма события собственного потока информации θ'_q, накопленной в вершине q элемента qr, и событий потоков информации θ_{qr}, приходящих в вершину q, равна объединению событий потоков информации θ_{kq}, исходящих из вершины q:

$$\theta'_q + \bigcup_r \theta_{qr} = \bigcup_k \theta_{kq}. \tag{1}$$

Закон сохранения потоков информации (1) является обобщением на информационной основе известных законов сохранения материальных потоков, содержащихся в разных тех-

нических теориях. В частности, в теории цепей — это первый закон Кирхгофа, в транспортных задачах — закон сохранения входящих и исходящих материальных потоков, в энергетике — закон связи входящих и исходящих потоков энергии, в экологически опасных системах — закон связи потоков вредных веществ и т. п.

Для построения модели надежности и безопасности любой системы основополагающим в информационной теории является следующее уравнение связи событий: события работоспособности ε_{ji} элемента ji, а также событие потока информации θ_{ji}:

$$\theta_j = \theta'_j + \bigcup_{i \neq j} \varepsilon_{ji}\theta_{ji}, \qquad j = \overline{1,n}, \tag{2}$$

где θ_j — событие потока информации в вершине j; n — число вершин j в структурной схеме (графе событий) системы, событие собственного потока информации

$$\theta'_j = \theta_j \qquad \text{при} \qquad \theta_{ji} = \varnothing \qquad \forall\, i \neq j. \tag{3}$$

На основе системы уравнений (2) построена система видов соединения элементов, включающая в себя последовательное, параллельное и смешанное, из которых виды соединения элементов в классических теориях надежности и безопасности следуют как частный случай при достоверных событиях потоков информации θ_{ji}.

Принципиальным для теории управления надежностью и безопасностью является соединение по схеме с обратной стохастической связью [1, 2]. Рассмотрим систему с обратной связью, состоящую из управляемого объекта ji и подсистемы управления ij, события функционирования которых соответственно $\varepsilon_{ji} = \varepsilon'_{ji} + \varepsilon''_{ji}$ и ε_{ij}. Вероятность события выходного потока информации системы с обратной связью для независимых событий θ_j, θ'_j, ε'_{ji}, ε''_{ji}, ε_{ji} согласно соотношению (2) равна

$$P(\theta_j) = \frac{P(\varepsilon'_{ji})}{1 - P(\varepsilon_{ij}/\Omega_2)P(\varepsilon''_{ji})} P(\theta'_i), \qquad \varepsilon'_{ji} = \Omega_1\varepsilon_{ji}, \qquad \varepsilon''_{ji} = \Omega_2\varepsilon_{ji}, \tag{4}$$

где

$$\varepsilon_{ji}\Theta'_i = \Omega_1\varepsilon_{ji}\Theta'_i, \quad \Omega_1\varepsilon_{ij} = \varnothing \quad \text{и} \quad (\varepsilon_{ji}\overline{\varepsilon_{ij}}) \neq \varnothing, \quad (\Omega_1 + \Omega_2) = I, \quad \Omega_1\Omega_2 = \varnothing, \tag{5}$$

Ω_1 — событие состояния системы, при котором объект ji функционирует без подсистемы ij; Ω_2 — событие состояния системы, при котором объект ji функционирует с подсистемой ij; $P(\varepsilon_{ij}/\Omega_2)$ — условная вероятность функционирования подсистемы ij в состоянии Ω_2.

Практически при случайных воздействиях цепи обратной связи приходится сохранять работоспособность цепи и в состоянии Ω_1. Поэтому для прикладных задач анализа и особенно синтеза следует положить

$$P(\varepsilon_{ij}/\Omega_2) = P(\varepsilon_{ij}). \tag{6}$$

Вероятность риска аварии системы с обратной связью

$$P(\overline{\theta}_j) = \frac{P(\overline{\varepsilon}_{ji})P(\overline{\varepsilon}_{ij})}{1 - P(\varepsilon_{ij})P(\overline{\varepsilon}_{ji})}, \tag{7}$$

где $\overline{\theta}_j$ — событие потока информации о выбросах РАО; $\overline{\varepsilon}_{ji}$, $\overline{\varepsilon}_{ij}$ — события отказа соответственно объекта и подсистемы управления (защиты).

Одним из важных разделов структурной теории является анализ влияний вероятностей отказов элементов на вероятность риска аварии системы, который рассмотрен в теории чувствительности [1, 4]. Для анализа влияний используют структурную функцию P, аргументами которой являются вероятности работоспособности элементов P_i, $i = \overline{1,n}$:

$$P = \frac{P(\varepsilon'_{ji})}{1 - P(\varepsilon_{ij}/\Omega_2)P(\varepsilon''_{ji})} = P(P_1, P_2, \ldots, P_n).$$

Используя структурную функцию, согласно теории погрешности получаем линейное уравнение

$$\delta P = S_1 \delta P_1 + S_2 \delta P_2 + \cdots + S_n \delta P_n, \tag{8}$$

где относительные погрешности

$$\delta P = \frac{P - P_0}{P_0} \qquad \text{и} \qquad \delta P_i = \frac{P_i - P_{i0}}{P_{i0}}, \qquad i = \overline{1,n}, \tag{9}$$

представляют собой отклонения от ненулевых значений аргументов P_{i0}, $i = \overline{1,n}$, и структурной функции $P_0 = f(P_{10}, P_{20}, \ldots, P_{n0})$. Функции чувствительности

$$S_i = \frac{\partial P}{\partial P_i}\frac{P_{i0}}{P_0}, \qquad i = \overline{1,n}. \tag{10}$$

Линейное уравнение относительной погрешности (8) позволяет порознь оценить вклад отказа каждого i-го элемента на отказ системы. Для этого в выражении (9) функцию чувствительности (10) заменяют ее значением при номинальных значениях аргументов P_{i0}, $i = \overline{1,n}$. Обычно расчетное значение вероятности безопасного функционирования объекта P близко к единице. Например, по рекомендациям нормативных документов значение $P_0 \geqslant 1 - 10^{-5}$. Поэтому $\delta P \approx -(1 - P)$. Значения вероятностей надежной работы элементов P_i значительно меньше значения P. Для оборудования наиболее реальными являются значения $P_i = 0{,}99$. Самыми малыми вероятностями, не превышающими значения 0,9, характеризуются технологические операции, выполняемые оператором. Учитывая это и выражение (9), запишем связь вероятностей отказов элементов $(1 - P_i) = R_i$ со значением вероятности риска $(1 - P) = R_{\text{рис}}$ в следующем виде:

$$R_{\text{рис}} \approx S_1^* R_1 + S_2^* R_2 + \cdots + S_n^* R_n, \tag{11}$$

где из условия $S_i R_i / P_{i0} = S_i^* R_i$ приведенная функция чувствительности

$$S_i^* = \frac{S_i}{P_{i0}}, \qquad i = \overline{1,n}. \tag{12}$$

Принцип структурного обеспечения безопасности объекта состоит в том, что структура системы управления строится из условия минимизации негативного влияния наиболее слабого и ограниченного по надежности элемента системы путем оптимального его расположения. Выбор слабого звена производится с помощью теории чувствительности, путем определения элемента с максимальным модулем функции чувствительности. Слабое звено k

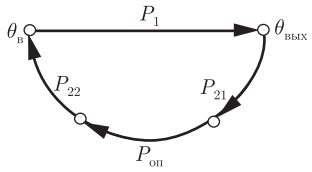


Рис. 1. Граф событий АЭС с подсистемой управления безопасностью для неоптимального расположения оператора

вносит наибольший вклад в значение вероятности риска аварии $R_{\text{рис}}$ (11) и удовлетворяет неравенству

$$|S_k^* R_k| \gg |S_i^* R_i| \qquad \text{при} \qquad R_k = R_i, \qquad (i = \overline{1,n}) \wedge (i \neq k). \tag{13}$$

Линейное уравнение погрешности (9) позволяет достаточно просто найти оптимальные требования к вероятностям безотказной работы элементов. При заданном требуемом значении вероятности безотказной работы системы в виде неравенства $P \geqslant P_{\text{Д}}$ и вытекающего из этого условия $\delta P \geqslant \alpha$ оптимальные требования к вероятностям безотказной работы элементов определяются согласно следующим неравенствам:

$$\delta P_i \geqslant \frac{\alpha}{nS_i}, \qquad i = \overline{1,n}. \tag{14}$$

Рассмотрим достаточно простой, но имеющий принципиальное значение пример анализа слабого звена, когда слабым звеном является оператор. Будем анализировать замкнутую структуру управления безопасностью АЭС (рис. 1), состоящую из объекта — активной зоны АЭС (АкЗ) 2.1, вероятность работоспособного состояния которого P_1, и подсистемы управления, состоящую из следующих элементов: подсистемы диагностирования 3.2, вероятность работоспособного состояния которой P_{21}, оператора 4.3, вероятность работоспособного состояния которого $P_{\text{оп}}$, и подсистемы регулирования — дистанционного расхолаживания активной зоны 1.4, вероятность работоспособного состояния которого P_{22}.

Для независимых ε-событий и равенства $\theta_j = \theta_{\text{вых}}$ вероятность работоспособного состояния (отсутствия риска аварии) согласно формуле (4) и рис. 1 равна

$$P(\theta_{\text{вых}}) = \frac{P_1}{1 - P_{21}P_{\text{оп}}P_{22}(1 - P_1)} P(\theta_{\text{в}}), \tag{15}$$

где $\theta_{\text{в}}$ — событие входного, $\theta_{\text{вых}}$ — событие выходного потоков информации. Значения вероятностей безотказной работы элементов 3.2 и 1.4 контура управления обычно больше 0,99. Значение вероятности функционирования оператора $P_{\text{оп}} \leqslant 0{,}9$ в связи с эргономическими ограничениями оператора. Можно показать, что произведение $S_{\text{оп}}R_{\text{оп}}$ (где $S_{\text{оп}}$ — чувствительность оператора, $R_{\text{оп}} = 1 - P_{\text{оп}}$) удовлетворяет условию (13). Поэтому из-за низкой надежности оператора надежность управления — вероятность совместного функционирования элементов контура управления мала и удовлетворяет неравенству

$$P_{21}P_{\text{оп}}P_{22} \leqslant 0{,}9. \tag{16}$$

Увеличение надежности управления является основным стратегическим направлением повышения безопасности модернизируемых АЭС.

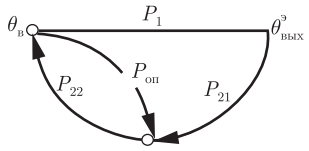


Рис. 2. Граф событий АЭС с подсистемой управления безопасностью для оптимального расположения оператора

Чтобы увеличить надежность управления, оператор из контура непосредственного управления безопасностью АЭС целесообразно перенести в контур управления за элементом регулирования 1.4, как это показано на рис. 2.

Согласно формуле (4), вероятность безотказной работы АЭС, граф событий которой приведен на рис. 2, равна

$$P(\theta^{\text{э}}_{\text{вых}}) = \frac{P_1}{1 - P_{21}P^{\text{э}}_{22}(1 - P_1)}P(\theta_{\text{в}}), \qquad P^{\text{э}}_{22} = \frac{P_{22}}{1 - P_{\text{оп}}(1 - P_{22})}. \tag{17}$$

В результате надежность управления безопасностью $P^{\text{э}}_{22}$ существенно возросла и удовлетворяет неравенству

$$P^{\text{э}}_{22} \gg P_{\text{оп}}P_{22}. \tag{18}$$

Для оценки эффективности структурной оптимизации системы управления безопасностью АЭС путем перехода от структуры, изображенной на рис. 1, к структуре, приведенной на рис. 2, найдем функции чувствительностей $S^{(1)}_{\text{оп}}$ и $S^{(2)}_{\text{оп}}$ согласно выражениям (15), (17) и (12) соответственно:

$$S^{(1)}_{\text{оп}} = \frac{P_{21}P_{22}(1 - P_1)}{1 - P_{21}P_{\text{оп}}P_{22}(1 - P_1)}, \tag{19}$$

$$S^{(2)}_{\text{оп}} = \frac{P_{21}P^{\text{э}}_{22}(1 - P_1)(1 - P_{22})}{[1 - P_{21}P^{\text{э}}_{22}(1 - P_1)][1 - P_{\text{оп}}(1 - P_{22})]}. \tag{20}$$

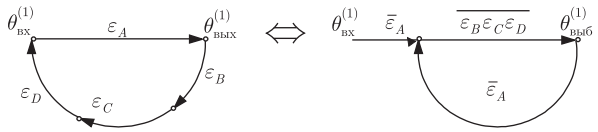
Отношение функций чувствительностей

$$\frac{S^{(2)}_{\text{оп}}}{S^{(1)}_{\text{оп}}} \approx \frac{1 - P_{22}}{P_{22}}. \tag{21}$$

Для вероятности $P_{22} = 0{,}99$ отношение $S^{(2)}_{\text{оп}}/S^{(1)}_{\text{оп}} \approx 0{,}01$. Это означает, что степень влияния ошибки оператора на риск аварии в структуре, приведенной на рис. 2, на два порядка меньше, чем степень влияния ошибки оператора в структуре, приведенной на рис. 1. Структура, изображенная на рис. 1, будет равноценной по безопасности структуре, изображенной на рис. 2, если вероятность функционирования оператора вместо $P_{\text{оп}} \approx 0{,}9$ станет $P_{\text{оп}} \approx 0{,}999$. Понятно, что из-за эргономических ограничений человека в принципе нельзя обеспечить такую вероятность функционирования оператора.

Применение структурной оптимизации является необходимым направлением повышения безопасности модернизируемой АЭС, в контуре управления которой обязательно присутствие оператора.

Заметим, что рассмотренную задачу структурной оптимизации оператора нельзя решить классическими методами анализа риска аварии (с помощью метода дерева событий)



Граф безопасности Граф опасности

Рис. 3. Графы безопасности и опасности с учетом первого контура защиты АЭС

и надежности (методом марковских цепей), так как они не позволяют учесть различие структур, приведенных на рис. 1 и на рис. 2 [4–7].

Теория управления надежностью и безопасностью позволяет дать теоретическое обоснование обеспечения безопасности АЭС согласно концепции глубоко эшелонированной защиты. Эта концепция базируется на двух положениях: на предупреждении аварии и на ослаблении влияния аварии. Теорию реализации этих двух положений рассмотрим на методологическом примере двухконтурного управления безопасностью АЭС. Первый контур управления предназначен для предупреждения аварии, а второй — для ослабления ее негативных последствий.

На рис. 3 приведен информационный граф событий первого контура эшелонированной защиты АЭС. Первый контур эшелонированной защиты служит для недопущения плавления активной зоны (АкЗ) путем регулирования теплообмена реактора между нейтронной и тепловой мощностями. На рис. 3 приняты следующие обозначения: ε_A — событие безопасности АкЗ реактора; ε_B — событие функционирования подсистемы диагностирования; ε_C — событие функционирования оператора; ε_D — событие функционирования регулирующего АкЗ органа; $\theta^{(1)}_{\text{вх}}$ — событие входного потока информации, определяющее совокупность радиоактивных веществ (РАО) в АкЗ до аварии (отказа первого контура); $\theta^{(1)}_{\text{вых}}$ — событие выходного потока информации, определяющее совокупность РАО в АкЗ после аварии (отказа первого контура), $\theta^{(1)}_{\text{выб}}$ — событие выброса продуктов деления, определяющее совокупность РАО, вышедших за пределы АкЗ в результате ее плавления (отказа первого контура). Чертой сверху обозначены противоположные события.

Граф безопасности (см. рис. 3) первого контура защиты АЭС согласно формуле (4) описывается выражениями

$$P(\theta^{(1)}_{\text{вых}}) = P(\varepsilon_{k1})P(\theta^{(1)}_{\text{вх}}), \qquad P(\varepsilon_{k1}) = \frac{P(\varepsilon_A)}{1 - P(\varepsilon_B\varepsilon_C\varepsilon_D)P(\overline{\varepsilon}_A)}, \tag{22}$$

где ε_{k1} — событие безопасности системы, состоящей из АкЗ и элементов подсистемы управления безопасностью.

Граф опасности (см. рис. 3) первого контура защиты АЭС согласно формуле (7) описывается выражениями

$$P(\theta^{(1)}_{\text{выб}}) = P(\theta^{(1)}_{\text{вх}}) - P(\theta^{(1)}_{\text{вых}}) = P(\overline{\varepsilon}_{k1})P(\theta^{(1)}_{\text{вх}}), \qquad P(\overline{\varepsilon}_{k1}) = \frac{P(\overline{\varepsilon}_A)P(\overline{\varepsilon_B\varepsilon_C\varepsilon_D})}{1 - P(\varepsilon_B\varepsilon_C\varepsilon_D)P(\overline{\varepsilon}_A)}. \tag{23}$$

Второй контур эшелонированной защиты служит для недопущения выбросов радиоактивных веществ за пределы реактора в случае плавления АкЗ. Граф событий, учитывающий два контура защиты АЭС, приведен на рис. 4. Здесь сохранены вышеуказанные обозначения (см. рис. 3), а также введены следующие: ε_E — событие безотказности герметичной оболочки (контайнмента); $\overline{\varepsilon}_E$ — событие отказа контайнмента; $\theta^{(2)}_{\text{выб}}$ — событие выброса РАО за пределы реактора (контайнмента).

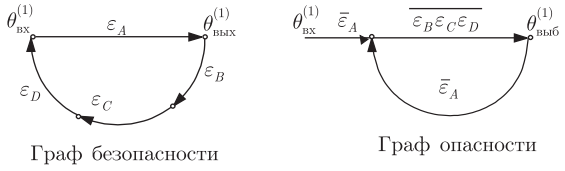


Рис. 4. Графы безопасности и опасности с учетом двух контуров защиты АЭС

Граф безопасности (см. рис. 4) второго контура защиты АЭС согласно формуле (4) описывается выражениями

$$P(\theta^{(2)}_{\text{выб}}) = P(\varepsilon_{k2})P(\theta^{(1)}_{\text{вх}}), \qquad P(\varepsilon_{k2}) = \frac{P(\varepsilon_{k1})}{1 - P(\varepsilon_E)P(\overline{\varepsilon}_{k1})}. \tag{24}$$

Граф опасности (см. рис. 4) второго контура защиты АЭС согласно формуле (7) описывается выражениями

$$P(\theta^{(2)}_{\text{выб}}) = P(\theta^{(1)}_{\text{вх}}) - P(\theta^{(2)}_{\text{вых}}) = P(\overline{\varepsilon}_{k2})P(\theta^{(1)}_{\text{вх}}), \qquad P(\overline{\varepsilon}_{k2}) = \frac{P(\overline{\varepsilon}_{k1})P(\overline{\varepsilon}_E)}{1 - P(\varepsilon_E)P(\overline{\varepsilon}_{k1})}. \tag{25}$$

Повышение безопасности АЭС за счет двухконтурной защиты (путем предупреждения и ослабления аварии) покажем на численных значениях показателей безопасности и опасности. Для иллюстрации эффективности двухконтурной защиты, учитывая эргономические ограничения оператора, примем следующие пессимистические значения надежности элементов подсистемы управления безопасностью: $P(\varepsilon_A) = P(\varepsilon_B) = P(\varepsilon_C) = P(\varepsilon_D) = 0{,}9$. Учитывая эти значения, согласно формуле (22) находим значение вероятности безопасности первого контура защиты АЭС: $P(\varepsilon_{k1}) = 0{,}9708$. Соответственно, значение вероятности опасности с учетом первого контура защиты согласно формуле (23) равно $P(\overline{\varepsilon}_{k1}) = 0{,}0292$.

Для двух контуров защиты АЭС и значения вероятности безотказности контайнмента $P(\varepsilon_E) = 0{,}9$ значение вероятности безопасности с учетом второго контура защиты согласно формуле (24) равно $P(\varepsilon_{k2}) = 0{,}997$. Соответственно, значение вероятности опасности с учетом второго контура защиты согласно формуле (25) равно $P(\overline{\varepsilon}_{k2}) = 0{,}003$.

Приведенные расчеты, выполненные на основе теории управления безопасностью [1, 2], иллюстрируют эффективность концепции глубокоэшелонированной защиты. Данная теория позволяет учесть влияние ненадежности каждой компоненты эшелонированной защиты на безопасность АЭС. В частности, на основе формул (10)–(12) для первого контура управления безопасностью АЭС находим показатель риска аварии

$$R(\overline{\varepsilon}_{k1}) \cong S^*_{A1}R(\overline{\varepsilon}_A) + S^*_{B1}R(\overline{\varepsilon}_B) + S^*_{C1}R(\overline{\varepsilon}_C) + S^*_{D1}R(\overline{\varepsilon}_D),$$

где значения вероятностей отказов элементов $R(\overline{\varepsilon}_A) = R(\overline{\varepsilon}_B) = R(\overline{\varepsilon}_C) = R(\overline{\varepsilon}_D) = 0{,}1$, значения чувствительностей (12) $S^*_{A1} = 0{,}3248$; $S^*_{B1} = S^*_{C1} = S^*_{D1} = 0{,}08737$.

С учетом двух контуров защиты показатель риска аварии

$$R(\overline{\varepsilon}_{k2}) \cong S^*_{A2}R(\overline{\varepsilon}_A) + S^*_{\text{B2}}R(\overline{\varepsilon}_B) + S^*_{C2}R(\overline{\varepsilon}_C) + S^*_{D2}R(\overline{\varepsilon}_D) + S_{E2}R(\overline{\varepsilon}_E),$$

Значения чувствительностей $S^*_{A2}0{,}03396$; $S^*_{\text{B2}} = S^*_{C2} = S^*_{D2} = 0{,}008973$; $S_{E2} = 0{,}02999$.

Согласно проведенным расчетам, наибольшей чувствительностью к показателю риска аварии характеризуется АкЗ. Соответственно, при заданном нормативному требованию

к допустимому значению показателя риска $R(\overline{\varepsilon}_{k2}) = 10^{-5}$ реактор/год оптимальное требование к допустимому значению показателя отказа АкЗ согласно формуле (14) равно

$$R_{\text{opt}}(\overline{\varepsilon}_A) = \frac{10^{-5}}{5 \cdot 0{,}03396} = 5{,}89 \cdot 10^{-5} \text{ реактор/год.}$$

Непосредственно обеспечить такие требования к безаварийности АкЗ (без учета эшелонированной защиты) практически невозможно. Поэтому следует учесть реально возможное значение показателя $R(\overline{\varepsilon}_A)$, а затем найти оптимальные требования к значениям безотказности элементов подсистемы защиты с учетом необходимых структурных изменений первого контура защиты для преодоления эргономических ограничений оператора.

1. *Пампуро В. И.* Структурная информационная теория надежности систем. – Киев: Наук. думка, 1992. – 324 с.
2. *Пампуро В. И.* Метод разработки математических моделей управления экологической безопасностью объектов // Доп. НАН України. – 1999. – № 1. – С. 197–203.
3. *Корн Г.* Исследование сложных систем по частям диакоптика. – Москва: Наука, 1972. – 831 с.
4. *Райншке К.* Модели надежности и чувствительности систем / Пер. с нем. под ред. Б. А. Козлова. – Москва: Мир, 1979. – 452 с.
5. *Хенли Э. Д., Кумато Х.* Надежность технических систем и оценка риска. – Москва: Машиностроение, 1979. – 528 с.
6. *Уивер Л.* Риск от аварии на АЭС с легководяными реакторами // Безопасность ядерной энергетики. – Москва: Атомиздат, 1980. – С. 114–133.
7. *Вероятностный* анализ безопасности атомных станций. Методика выполнения / Ю. В. Шыряев и др. – Москва: ИАЭ им. Курчатова, 1992. – 266 с.

Институт электродинамики НАН Украины, Киев *Поступило в редакцию 20.03.2009*

V. I. Pampuro

Structural analysis of safety control systems

The structural analysis of reliability of the safety control system of an NPP according to information control theory is given. The theory of the mistake operator minimization optimizing the structure of a control safety system is presented. The theoretical basis of the protection-in-depth conception is illustrated.