УДК 685.1

Е.В. Брежнев

Национальный аэрокосмический университет им. Н.Е. Жуковского "ХАИ", Харьков

АНАЛИЗ ПОДХОДОВ К ОЦЕНКЕ БЕЗОПАСНОСТИ КРИТИЧЕСКИХ ИНФРАСТРУКТУР В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ

В статье рассмотрены существующие подходы к риск-анализу безопасности критической инфраструктуры. Проведен анализ видов неопределенности, приведена классификация критических инфраструктур по сложности поведения. Рассмотрены основные сходства и различия между детерминированным, вероятностным и soft подходами. Показана необходимость развития методологии оценки безопасности критической инфраструктуры, интегрирующей данные направления.

Ключевые слова: *критическая инфраструктура, безопасность, риск-анализ, софт-компьютинг.*

Введение

Постановка проблемы и анализ литературы. Энергетические, транспортные, телекоммуникационные, банковские и другие системы, являются примером критических инфраструктур (КИ), обеспечивающих благополучие и экономическое развитие общества [1].

Развитие КИ приводит к углублению взаимосвязей и взаимовлияния между ними, усложнению поведения и характера отказов, приводящих к серьезным последствиям. Сложность и взаимозависимость становятся причинами уязвимости [2, 3] КИ к действию неблагоприятных факторов и увеличения рисков аварий и катастроф.

Безопасность КИ обеспечивается анализом процессов ее функционирования, мониторингом состояния, моделированием и оценкой рисков отказов, оценкой ущерба, разработкой эффективных стратегий безопасности.

Анализ тенденций развития КИ показывает, что риск аварий в результате прямого воздействия неблагоприятных факторов, в будущем будет возрастать [4]. Данная проблема усложняется отсутствием единого комплексного подхода к оценке безопасности КИ. Каждая область человеческой деятельности оперирует своим инструментарием и понятийным аппаратом анализа безопасности.

Различия в понимании проблемы приводят к разнообразию методов, применяемых для оценки безопасности КИ [5 – 9].

Часть этих методов устарела и не удовлетворяет уровню развития КИ и требованиям к ее безопасности, не обеспечивая приемлемый уровень достоверности результатов.

Ввиду значительной сложности и слабой структурированности КИ, доминирования качественной информации в их описании и высокой степени неопределенности, применение классических (вероятностных и детерминированных) методов может стать причиной неадекватности оценок безопасности КИ и неэффективности стратегий риск-менеджмента.

Успешное решение проблемы обеспечения безопасности КИ невозможно без применения новых информационных технологий, частью которых являются интеллектуальные методы обработки информации.

Цель статьи – провести анализ методов оценки безопасности в КИ и показать необходимость совместного использования методов софт-компьютинга и вероятностных методов для риск-анализа КИ в условиях неопределенности для повышения обоснованности результатов оценки безопасности.

Основной материал

Следует отметить, что проблема оценки безопасности КИ является сложной и неоднозначной. Эта сложность обусловлена:

– нечеткостью в определении границ проблемы;

– сложностью поведения КИ, эмерджентностью ее свойств;

– неэргодичностью КИ, невозможностью определения всех ее состояний и переходов между ними;

– отсутствием статистических данных, связанных с крупными авариями и сбоями;

– немонотонностью проблемы, т.е. увеличение знаний не приводит к ее более глубокому пониманию.

Разработка точной и полной модели оценки безопасности является сложной задачей, связанной с недостатком знаний о возможных отказах и поведении КИ, наличием исходных данных, представленных в разных квалиметрических шкалах.

Все это неизбежно приводит к проблеме неопределенности в риск-анализе.

Классификация видов неопределенности, присущей проблеме оценке безопасности критической инфраструктуры, приведена на рис. 1.

© Е.В. Брежнев

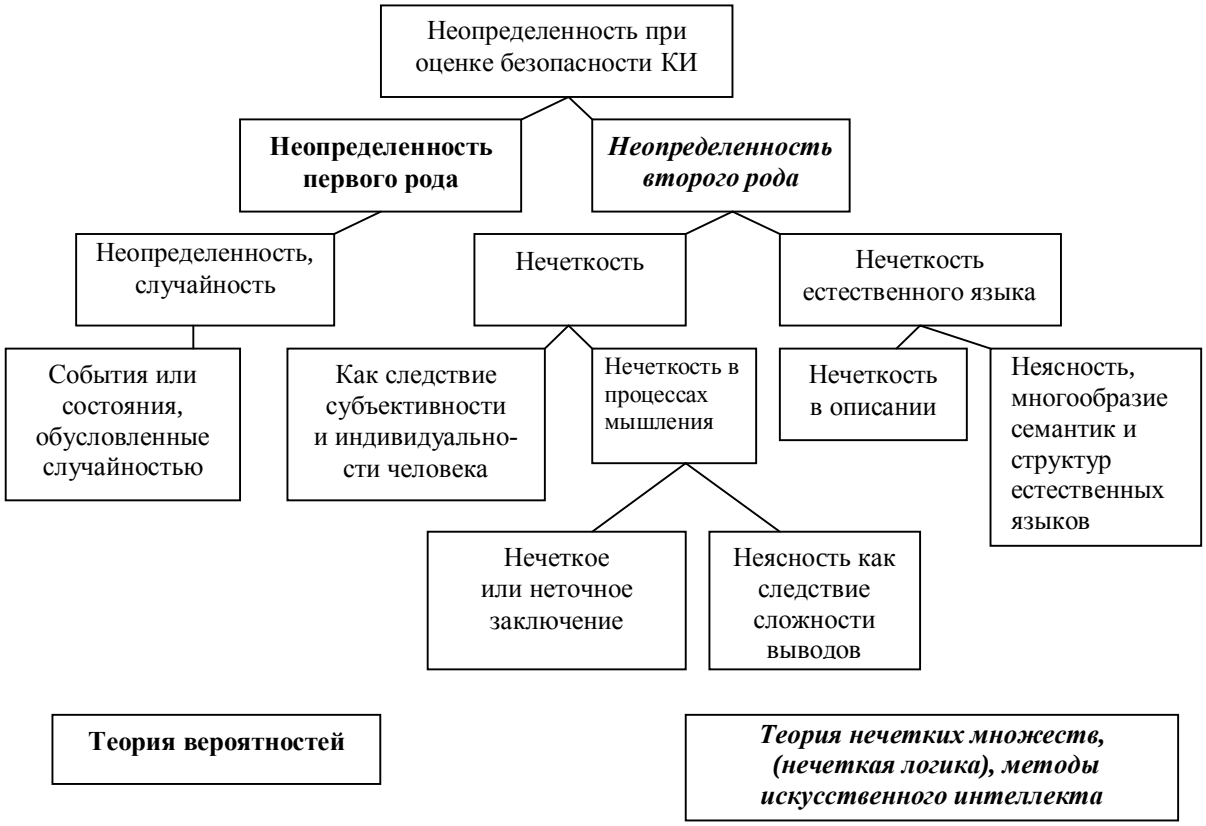

Рис. 1. Классификация видов неопределенности
при оценке безопасности критической инфраструктуры

По характеру поведения КИ могут быть классифицированы на:

– детерминированные системы, поведение которых определено известными правилами и законами. Множество состояний каждого компонента, подсистемы и системы в целом известно;

– вероятностные системы, поведение которых может быть описано методами теории вероятностей;

– хаотические системы. Данные системы характеризуются тем, что небольшие изменения в их текущем состоянии могут приводить к непредсказуемым и значительным изменениям в последующем состоянии.

Классификация критической инфраструктуры, построенная по сложности поведения, представлена на рис. 2.

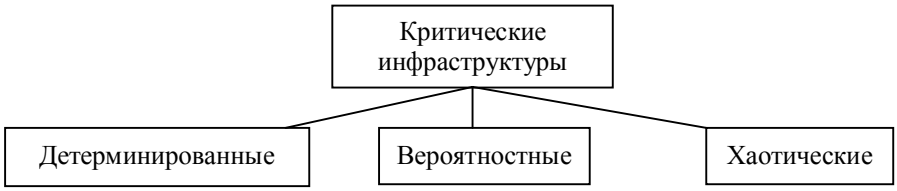

Рис. 2. Классификация критических систем по сложности поведения

Анализ методов, применяемых для оценки риска в критических инфраструктурах. Детерминированный анализ (DSA).

Длительное время при анализе безопасности КИ применялась парадигма детерминизма, представленная группой DSA методов. Так, например, в атомной индустрии DSA применялся до аварии Three Mile Island, произошедшей в 1979 году. Результат DSA считается определенным с учетом предполагаемых граничных условий [5].

При проведении DSA не используются количественные вероятностные данные для описания событий или их сочетаний. Определяются возможные сценарии, включающие базовое множество событий и их последствия для КИ. Сценарии описываются с использованием выражений естественного языка. DSA обычно проводится с пессимистическим уклоном, т.е. он ориентирован на наихудшие сценарии развития аварий. В связи с этим его результаты являются пессимистическими и не оптимальными. С

точки зрения рациональности использования ресурсов, стратегии DSA риск-менеджмента, являются неэффективными.

Для достижения требуемого уровня безопасности планируется большее количество средств, чем требуется.

При проведении детерминированного риск-анализа безопасности КИ определяется число категорий вероятности и тяжести последствий наступления неблагоприятных событий. Также могут быть приведены количественные характеристики этих категорий, однако подход не предполагает их обязательного применения.

Применительно к FMECA анализу детерминированный подход предполагает определение категорий частоты и тяжести последствий отказов.

Классификация тяжести последствий приведена в табл. 1.

Таблица 1

Категории тяжести последствий

Категории	Качественное описание	Количественное описание (число в год)
1	Катастрофические	Многочисленные жертвы
2	Значительные	Единичные жертвы, множественные ранения
3	Очень серьезные	Ранения длительные
4	Серьезные	Серьезные ранения, возможно полное восстановление
5	Незначительные	Незначительные ранения, временная нетрудоспособность

Классификация частоты отказов представлена в табл. 2.

Таблица 2

Детерминированный риск-анализ частоты отказов

Категории	Качественное описание	Количественное описание (число в год)
A	Возможно	0,3 – 3
B	Вероятно	0,03 – 0,3
C	Маловероятно	0,003 – 0,03
D	Очень маловероятно	0,0003 – 0, 003
E	Практически невозможно	0,00003 – 0,0003

Риск, связанный с конкретной угрозой, определяется как комбинация категории тяжести последствий отказа и его частоты. Например, B3 означает, что вероятность реализации угрозы B и ее последствия относятся к третьей категории. Идея состоит в одновременном анализе вероятности и последствий без использования сложных математических вычислений.

Матрица риска в рамках детерминированного анализа безопасности, приведенная в табл. 3, может быть определена как матрица 5 на 5. Каждая клетка матрицы содержит вероятность и последствия для каждой категории угроза (опасностей). Чем ближе результат к красной зоне, тем более необходимы меры по снижению опасности.

Таблица 3

Матрица риска для детерминированного риск-анализа

Категории частоты	Категория тяжести последствий				
	5	4	3	2	1
A					
B					
C					
D					
E					

Главным недостатком детерминированного подхода является неучет неопределенностей. Поэтому адекватность результатов анализа фактической оценки безопасности сомнительна. Для критических инфраструктур, для которых отказ приводит к серьезным последствиям, например, для АЭС, данный подход не может быть применим по причине не соответствия требованиям безопасности.

Вероятностный анализ (PSA).

Если поведение системы не может быть описано набором определенных правил соотношений для определения характеристик системы, то для риск-анализа используется подход, характеризующийся использованием вероятностных оценок [6, 7].

В соответствии с этим подходом рассматриваются все возможные аварии, а также любое количество одновременных отказов.

Основой вероятностного подхода является системный анализ возможных сценариев, а также последовательное исследование аварий, включая исходные события, пути развития аварийных ситуаций с учетом наложения отказов систем. При этом важным элементом является количественный анализ надежности систем.

Применение вероятностного подхода облегчает установление приоритетов и выбор стратегии обеспечения безопасности. Следует отметить, что крупные аварии являются редкими событиями. Это ограничивает возможности применения классического вероятностного подход, основанного на статистических выводах, к анализу безопасности КИ. Вероятностные методы не приводят к удовлетворительным результатам, когда исходное описание проблемы является неточным и неполным.

Подход для анализа безопасности, основанный на применении Soft-computing.

Сущность “мягких вычислений” [8] при оценке безопасности КИ состоит в том, что в отличие от

традиционных, детерминированных (жестких) вычислений, они нацелены на приспособление к неточности реального мира. Руководящим принципом мягких вычислений является терпимость к неточности, неопределенности и частичной истинности для достижения удобства манипулирования, робастности, низкой стоимости решения и лучшего согласия с реальностью.

Математическая основа искусственного интеллекта – "soft computing" ("мягкое вычисление") – интенсивно развивалась в последнее десятилетие. Управление безопасностью КИ происходит в условиях неопределенности (неточности, нечеткости) информации, связанной с их функционированием. Наличие неточности и неопределенности данных требует применения "мягких вычислений".

Кроме того, традиционные точные двузначные логические системы, исследования в области теории множеств и теории вероятностей являются недостаточно адекватными, чтобы оперировать с неточностью, сложностью критической инфраструктуры.

С развитием концепции нейронных сетей [9] и нечеткой логики "мягкое вычисление" лидирует в управлении сложными динамическими системами, по сравнению с классическими методами, включая в себя следующие направления:

нечеткие множества (первого и второго рода);

генетические алгоритмы;

искусственный интеллект;

моделирующие системы;

вероятностное рассуждение;

изучение алгоритмов интеллектуального управления;

распознание образов;

самоорганизацию сложных систем;

нечеткое управление;

нечеткий информационный поиск и др.

"Мягкое вычисление" основано на нейронной сети (NN – Neural Network), нечеткой логике (FL – Fuzzy Logic) и вероятностном описании (PR – Probabilistic Reasoning). Функции нейронных сетей – изучение степени соответствия данных, идентификация параметров, а также систем и образов. Нечеткая логика (FL) оперирует с неточностью и вероятностным описанием процессов. В последнее время FL сливается с информационной генетикой, оценивает неуверенность, систематизирует случайный поиск и оптимизацию.

Одной из интереснейших и перспективных областей современных высоких технологий для анализа критических инфраструктур является нечеткое моделирование.

Актуальность новой технологии обусловлена сложностью существующих математических и формальных моделей КИ, связанной с желанием повысить адекватность результатов и учесть большее число факторов, влияющих на риски аварий.

Генетические алгоритмы являются мощным средством решения задач оптимизации параметров критических инфраструктур, для обеспечения требуемого уровня безопасности. Этот метод имитирует процесс естественного отбора в природе. Поиск оптимального решения при этом похож на эволюцию популяции индивидов, представленных наборами хромосом.

В эволюции действуют три механизма: отбор сильнейших – наборов хромосом, которым отвечают оптимальные решения; скрещивание – производство новых индивидов с помощью смешивания хромосомных наборов отобранных индивидов; и мутации – случайные изменения генов у некоторых индивидов популяции.

В результате изменения поколений вырабатывается решение задачи, которое уже не может быть дальше улучшено.

В настоящее время начинают находить широкое применение так называемые нечеткие системы управления (fuzzy-системы), основанные на нечеткой логике, разработанной Лотфи Заде в 1965 году [10]. Особенно эффективно применение нечетких систем управления там, где объект управления достаточно сложен для его точного описания и существует дефицит априорной информации о поведении системы.

Основные характеристики рассмотренных методов приведены в табл. 4.

Выводы

Мягкие вычисления могут быть положены в основу создания методологии риск-анализа безопасности критической инфраструктуры. В этой связи, для решения проблемы анализа и синтеза безопасных критических систем необходимо объединение различных направлений и методов анализа, существующих в настоящее время. Главными партнерами в этом объединении являются нечеткая логика, нейровычисления, генетические вычисления и вероятностные вычисления с более поздним включением хаотических систем, сетей доверия и разделов теории обучения.

Главным достоинством этой методологии является то, что ее составляющие являются в большей степени синергетическими и взаимодополняющими, чем соперничающими.

Таким образом, при решении задач связанных с оценкой риска, обеспечения безопасности в критических инфраструктурах, наилучшего результата можно достигнуть путем совместного использования FL, NC, GC и PC, чем путем их применения по отдельности.

Таблица 4

Основные характеристики методов анализа безопасности в критических инфраструктурах

	DSA	PSA	SC
Входные данные	Детерминированные входные данные. Точечная оценка (верхняя или нижняя, средняя)	Вероятностное распределение входных параметров	Нечеткие входные переменные, четкие, нечеткие случайные величины
Множество рассматриваемых событий	Только с наихудшими последствиями	Все прогнозные события	Все прогнозные события
Частота	Достоверные события (P=1)	Вероятность оценивается в соответствии с принятыми законами распределения	Лингвистические оценки, нечеткие числа
Тяжесть последствий	Предполагается известной	Предполагается известной	Лингвистические переменные, нечеткие переменные
Риск оценка	Качественный анализ	Количественный анализ	Нечеткий анализ
Учет неопределенности	Неопределенность не рассматривается	Стохастическая неопределенность (случайные переменные с известным распределением) Неопределенность первого рода	Нестохастическая неопределенность, Неопределенность второго рода

Список литературы

1. Critical Infrastructure: Protecting America's Infrastructure: Report of the President's Commission on Critical Infrastructure Protection / R.T. Marsh, ed. – Washington D.C., USA: United States Government Printing Office, 1997.

2. Ten C.-W. Vulnerability assessment of cybersecurity for SCADA systems / C.-W. Ten, C.-C., M. Govindarasu // IEEE Trans. Power Syst.

3. Vulnerability assessment of cybersecurity for SCADA systems using attack trees // Proc. IEEEC Power Engineers Society General Society General Meeting. – Tampa, FL, Jun. 24-28, 2007.

4. Safety Assessment of Thermal Power Enterprise on BP Neural Network / Yanbin Li, Peng Li et al. // Journal of Information & Computational Science. – 2009. – 6(1). – P. 553-556.

5. Robin K. Deterministic vs. probabilistic earthquake hazard and risks / K. Robin // Engineering Science. – 2001. – 1(10). – P. 63-69.

6. Probabilistic seismic hazard assessment for state of California // Calif. Div. of Mines and Geology, Sacramento, Open-file Rept. 96-08.

7. McGuire R.K. Probabilistic seismic hazard and design earthquakes: closing the loop / R.K. McGuire // Bull. Seism, Soc.Am., 85, 5. – 1995. – P. 1275-1284.

8. Georgilalakis P. On the application of artificial techniques to the quality improvement of industrial processes / P. Georgilalakis, N. Hatziargyrio // SETN Proceeding, Thessaloniki. – 2002. – P. 473-484.

9. Application of Trapezium – cloud Model in Conception Division and Concept Examination / Jiang Jilia-bian, Liang Jia-rong, Jiang Wei, et al. // Computer Engineering and Design. – 2008. – 29(5). – P. 1235-1240.

10. Moulin L. Neural networks and support vector machines applied to power systems transient stability analysis / L. Moulin, A. da Silva, M. El-Sharkawi, R. Marks // Engineering Intelligent system Journal. – Victoria, Australia, 2001.

Поступила в редколлегию 10.02.2011

Рецензент: д-р техн. наук, проф. В.С. Харченко, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.

АНАЛІЗ ПІДХОДІВ ДО ОЦІНКИ БЕЗПЕКИ КРИТИЧНИХ ІНФРАСТРУКТУР В УМОВАХ НЕВИЗНАЧЕНОСТІ

Є.В. Брежнєв

В статті проаналізовано існуючі підходи до ризик-аналізу безпеки критичної інфраструктури. Проведено аналіз видів невизначеності, приведено класифікація критичних інфраструктур за складністю поведінки. Розглянуто схожість та розбіжності між детермінованим, імовірнісним та soft підходами. Показано необхідність розвитку методології аналізу безпеки критичної інфраструктури, який інтегрував би ці напрямки.

Ключові слова: *критична інфраструктура, безпека, ризик-аналіз, софт комп'ютинг.*

THE APPROACHES' ANALYSIS TO CRITICAL INFRASTRUCTURE'S SAFETY ASSESSMENT UNDER UNCERTAINTY

YE.V. Brezhnev

The conventional approaches to critical infrastructure's safety assessment are considered in the paper. The analysis of uncertainty's type, classification of critical infrastructure's behavior is performed. The similarity and differences among deterministic, probabilistic and soft approaches are taken into account. The need of their aggregation for development of new safety assessment methodology is emphasized.

Keywords: *critical infrastructure, safety, risk-analysis, soft-computing.*