УДК 685.1

Е.В. Брежнев

Национальный аэрокосмический университет имени Н. Е. Жуковского «ХАИ», Харьков

МЕТОД ОЦЕНИВАНИЯ РИСКОВ КАСКАДНЫХ АВАРИЙ (ОТКАЗОВ) С ИСПОЛЬЗОВАНИЕМ ДИНАМИЧЕСКИХ МАТРИЦ КРИТИЧНОСТИ

Каскадные (цепочные) аварии (отказы) представляют риски для критических инфраструктур (КИ) и их информационно-управляющих систем (ИУС). Каскадные аварии (отказы) характеризуются высокой тяжестью последствий, неопределенностью механизма возникновения. В статье предлагается метод оценивания рисков каскадных аварий (отказов) в условиях неопределенности, связанной с недостатком статистических данных для определенияих вероятностных характеристик. Метод основан на использовании лингвистической аппроксимации (ЛА), позволяющей провести эвристическое прогнозирование развития аварий. Неопределенность выбора функции принадлежности лингвистических термов состояния снижается за счет использования интервальных нечетких множеств. В статье предложены стратегии снижения рисков каскадных аварий (отказов) в КИ.

***Ключевые слова**: каскадные аварии (отказы), риск, критическая инфраструктура, лингвистическая аппроксимация, интервальные нечеткие множества.*

Введение

Каскадные (цепочные)аварии (отказы) представляют опасность для КИ и их ИУС. Каскадные аварии (отказы) характеризуются высокой тяжестью последствий. Так, например, в ходе аварии на АЭС Фукусима-1, отказы насосов подачи морской воды и системы аварийного энергоснабжения привели к аварии реактора с потерей теплоносителя, к частичному расплавлению реактора, нагреву хранилища отработанного топлива, пожарам, а также выбросу радиации в атмосферу. Каскадные аварии возникают из-за уязвимостей КИ к природным катастрофам, ошибок оператора, сбоев программных и аппаратных средств ИУС, пр. Стремление владельцев КИ к максимизации прибыли приводит к функционированию КИ с параметрами, близкими к пределам безопасности. Внешние негативные факторы приводят к нарушению нормальной работы систем в КИ. При переходе систем в неработоспособное состояние ИУС перераспределяет ресурсы и задачи между работоспособными системами, что приводит к увеличению рисков каскадных аварий в КИ.

Возникновение каскадных аварии (отказов)также обусловлено нарушениями взаимосвязей между системами в КИ. Так, подобная ситуация произошла на Саяно-Шушенской (СШ) ГЭС, в 2009 г. Отключение от нагрузки Братской ГЭС привело к передаче нагрузки на СШ ГЭС и, как результат, к увеличению локальной нагрузки на все ее гидроагрегаты. При этом риски отказов гидроагрегатов увеличились, что и привело к аварии с тяжелыми последствиями.

При оценивании рисков каскадных аварий возникают трудности, связанные с определением инициирующего отказа (события), каскадной цепочки (последовательности отказов и аварий), оценки прогнозной тяжести аварии. Отсутствие статистики затрудняет оценивание законов распределения каскадных отказов. Кроме того, каскадные аварии (отказы) могут быть отнесены к классу редких событий с большой тяжестью последствий (*blackswan* события), для которых даже наличие статистики не позволяет достоверно определить характеристики распределения.

Подходы к анализу рисков каскадных отказов

Существует ряд подходов к анализу рисков каскадных отказов в КИ [1 – 5]. Так, например, в работе [1] рассмотрена возможность использования алгебры причинно-следственных комплексов для построения автоматной и стохастической моделей каскадных отказов в КИ. Подход предполагает наличие полной информации о развитии аварии, идентификацию всех причинно-следственных связей, что не всегда возможно в рамках сложной системы. Для анализа каскадных отказов также используются подходы, основанные на: кластерном анализе [2]; анализе наиболее вероятных путей каскада [3]; анализе универсальных выборок [4]; анализе исторических данных [5]. В табл. 1 приведены основные характеристики методов риск анализа каскадных аварий (отказов).

Таблица 1

Основные характеристики
методов риск анализа каскадных аварий (отказов)

Подход	Преимущества	Недостатки
Анализ исторических данных	Нет допущений	Необходимость наблюдений
Стохастическое моделирование	Позволяет получить оценки риска	Много допущений, ограничен. сценариев
Высокоуровневое статистическое моделирование	Простота анализа, понятность результатов	Не учитывает детали каскадных отказов

Сложный характер взаимовлияния приводит к увеличению рисков каскадных аварий (отказов). Приведенные методы не учитывают связи между состояниями безопасности систем, не рассматривают их нарушение как причину возникновения каскадных аварий (отказов) в КИ. Динамические матрицы критичности (ДМК)[6], которые учитывают взаимовлияние между системами, связи между состояниями их безопасности (уровнем критичности) могут быть использованы для прогнозирования рисков каскадных аварий (отказов)в условиях ограниченности статистических данных.

Цель статьи – разработка метода к оцениванию рисков каскадных аварий (отказов) с использованием ДМК.

Основной материал

Основными этапами оценивания рисков каскадных аварий с использованием ДМК являются:

1. Построение иерархии ДМК для анализируемой системы с использованием алгоритма, приведенного в [6].

2. Выявление типов взаимовлияний между системами КИ. Для КИ выделяют: физическое влияние $I^{physic}(S_1 \to S_2)$, обусловленное потоками энергии между системами; информационное влияние $I^{inf\,or}(S_1 \to S_2)$, обусловленное информационным обменом между системами; географическое влияние $I^{geogr}(S_1 \to S_2)$, обусловленное близостью систем между собой (распространение последствий), пр.

3. Построение матрицы влияния (МВ) между системами. МВ содержит оценки степени влияния между состояниями безопасности систем в КИ. Величина влияния представляется в виде лингвистической переменной (ЛП), которая демонстрирует степень уверенности эксперта в том, что отказ одной из систем приведет к росту критичности другой системы.

Пример МВ приведен в табл. 2.

Таблица 2

Пример матрицы влияния

	S_{12}	S_{21}	S_{32}	S_{41}	S_{52}	S_{61}
S_{12}	-	High				
S_{21}		-	High			High
S_{32}			-			High
S_{41}				-		
S_{52}					-	High
S_{61}				High		-

4. Формирование множества сценариев каскадных аварий. Анализируются все возможные цепочки каскадных аварий с учетом существующих взаимовлияний. Определяется система (множество систем), отказ которой может инициировать развитие каскада. Далее выявляются все системы, связанные с инициирующей системой, и т.д.

5. Ранжирование каскадов по интегральной тяжести последствий. Из общего множества сценариев выделяется подмножество, характеризующееся наиболее высокой интегральной тяжестью последствий. Тяжесть последствий рассматривается для всех уровней иерархии КИ.

6. Прогнозирование развития каскадной аварии с использованием ЛА и управление рисками. На этом этапе проводится обновление критичностей систем с учетом отказов систем, инициирующих каскад.

Этапы оценивания рисков каскадных аварий (отказов) приведены на рис. 1.

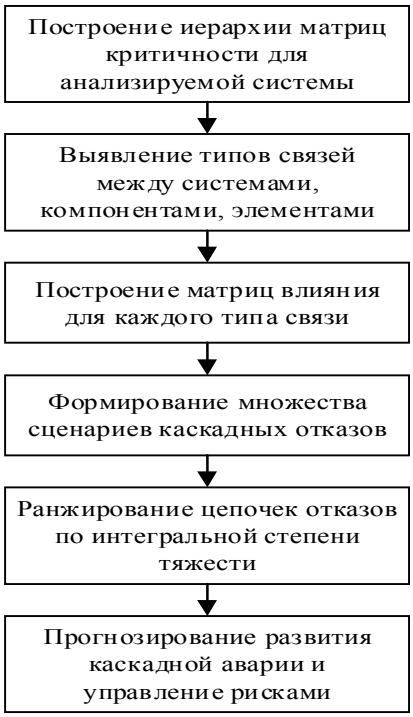

Рис. 1. Этапы оценивания рисков каскадных отказов

Рассмотрим пример использования метода оценивания рисков каскадных аварий с использованием ДМК. В рамках примера, рассмотрим два сценария каскадных аварий: $S_{12} \to S_{21} \to S_{61} \to S_{41}$;$S_{52} \to S_{61} \to S_{41}$. Рассмотрим каскад вида $S_{12} \to S_{21} \to S_{32} \to S_{61} \to S_{41}$, как каскад с наиболее высокой интегральной тяжестью последствий.

Этап прогнозирования каскадной аварии с использованием ЛА.

Прогнозирование развития каскада проводится в условиях неопределенности, связанной с отсутствием статистической информации о каскадных отказах систем КИ, а также наличием экспертной информации о связях между состояниями безопасности, представленной в виде выражений лингвистических переменных. ЛА позволяет обрабатывать входные данные для анализа, представленных в виде ЛП.

ЛА может рассматриваться как разновидность эвристического прогнозирования с использованием лингвистических оценок. Эвристическое прогнозирование используется в случаях, когда применение строгих математических моделей не обеспечивает

достоверных результатов прогноза из-за того, что лежащие в их основе предпосылки не соответствуют реальным свойствам поведения прогнозируемого процесса или объекта.

Проведение ЛА для прогнозирования каскадной аварии включает этапы: представление знаний об объекте в виде ЛП; представление ЛП в виде нечетких чисел; вычисления с нечеткими числами для определения нового значения критичности системы; представление результирующих нечетких чисел в виде ЛП, обновление критичности систем с учетом рассматриваемого сценария.

Таким образом, новая (прогнозная)величина критичности (оценки безопасности) может быть получена путем мультипликации двух нечетких чисел, описывающих семантику нечетких оценок критичности и влияния отказа.

Как правило эта оценка не совпадает с первоначальными термами исходного множества лингвистических оценок критичности Si. Для представления полученных результатов в первоначальных термах, применяется ЛА, основанная на оценке Евклидова расстояния вида:

$$d(S_i, C_j) = \sqrt{P_1(a_i - a_j)^2 + P_2(b_i - b_j)^2 + P_3(c_i - c_j)^2},$$

где (a_i, b_i, c_i) – параметры функции принадлежности первоначального лингвистического терма S_i; (a_j, b_j, c_j) – функция принадлежности полученного нечеткого множества (НМ), характеризующего семантику новой лингвистической оценки критичности (С)системы;

Трудности построения функции принадлежности приводят к целесообразности использования НМ интервального типа для ЛА.

Особенности ЛА при использовании нечётких интервальных множеств – близость между НМ будем находить на основе правила сходства [7].

Под интервальным нечетким множеством А на универсальном множестве $U \neq 0$ есть отображение A: $U \to L([0,1])$, такое, что функция принадлежности $u \in U$ имеет вид $A(U) = [\underline{A}(U), \overline{A}(U)] \in L([0,1])$, где $\underline{A} : U \to [0,1]$ и $\overline{A} : U \to [0,1]$ есть отображения, определяющие нижнюю и верхнюю границы функции принадлежности A(U).

В [7] предложено использовать в качестве величины сходства между двумя нечеткими множествами интервального типа $\widetilde{A}$, $\widetilde{B}$ величину вида:

$$s_Z(\widetilde{A}, \widetilde{B}) = 1 - \frac{1}{2n}\sum_{i=1}^{n}\left(\left|\underline{\mu}_{\widetilde{A}}(x_i) - \underline{\mu}_{\widetilde{B}}(x_i)\right| + \right.$$

$$\left. + \sum_{i=1}^{n}\left(\left|\overline{\mu}_{\widetilde{A}}(x_i) - \overline{\mu}_{\widetilde{B}}(x_i)\right|\right)\right),$$

где $\underline{\mu}_{\widetilde{A}}(x_i)(\underline{\mu}_{\widetilde{B}}(x_i))$ - левая (нижняя) граница интервала функции принадлежности нечеткого множества $\widetilde{A}(\widetilde{B})$; $\overline{\mu}_{\widetilde{A}}(x_i)(\overline{\mu}_{\widetilde{B}}(x_i))$ - правая (верхняя) граница интервала функции принадлежности нечеткого множества $\widetilde{A}(\widetilde{B})$.

Ниже приведены результаты использования ЛА для обновления оценок критичностей состояния систем с учетом связей и отказов в КИ.

1. Для цепочки отказов $S_{12} \to S_{21} \to S_{32} \to S_{61} \to S_{41}$ с учетом МВ, приведенной в табл. 2.

Первоначальные критичности состояний систем, рассматриваемых в рамках каскадного отказа (до отказа), приведены в табл. 3.

Таблица 3

Первоначальные критичности состояний систем

Система	S_{12}	S_{21}	S_{32}	S_{61}	S_{41}
Исходная критичность	High	High	Medium	Low	Low

С учетом ЛА обновленные критичности состояний систем, рассматриваемых в рамках каскадного отказа (после отказа), приведены в табл. 4.

Таблица 4

Обновленные критичности состояний систем

Система	S_{12}	S_{21}	S_{32}	S_{61}	S_{41}
Новый уровень критичности	Failure	*Failure*	High	Medium	Low

2. Для цепочки отказов вида $S_{21} \to S_{61} \to S_{41}$

Первоначальные критичности состояний систем, рассматриваемых в рамках каскадного отказа (до отказа), приведены в табл. 5.

Таблица 5

Первоначальные критичности состояний систем

Система	S_{21}	S_{61}	S_{41}
Исходная критичность	High	Low	Low

Обновленные критичности состояний систем, рассматриваемых в рамках каскадного отказа (после отказа), приведены в табл. 6.

Таблица 6

Обновленные критичности состояний систем

Система	S_{21}	S_{61}	S_{41}
Новый уровень критичности	Failure	Medium	Low

Превентивное управление рисками каскадных отказов

Для превентивного управления рисками каскадных аварий возможны следующие стратегии:

первая стратегия – определить цепочку с наибольшей интегральной тяжестью последствий. Для цепочки выявляется система, отказ которой может инициировать появление каскада. Выделяются средства для снижения критичности состояния этой системы;

вторая стратегия – снизить риски каскадных отказов последовательно, т.е. выделить ресурсы для последовательного снижения рисков с учетом величин интегральной тяжести последствий для каждой цепочки;

третья стратегия – снизить риски одновременно, для всех цепочек.

Управление каскадными авариями возможно при условии мониторинга уровня критичностей систем, и выявления взаимосвязей между ними.

Использование стратегий предполагает наличие определенного внешнего и внутреннего ресурса в КИ. Так, например, в условиях аварии на СШ ГЭС, при нормальном функционировании систем защиты гидроагрегата от перегрузок и вибрации, второй гидроагрегат должен быть выключен. Отказ гидроагрегата может быть компенсирован увеличением нагрузки на другие гидроагрегаты (внутренние ресурсы) или снижением мощности станции и передачи регулировочной функции на другую ГЭС (внешние ресурсы). Для снижения последствий отказов системе необходимо располагать некоторым ресурсом, которым она будет компенсировать последствия отказов подсистем.

Выводы

Таким образом, ДМК могут быть использованы для оценивания рисков каскадных (цепочных) аварий (отказов). Использование ЛА позволит учесть риски, обусловленные взаимовлиянием между системами. ЛА позволяет проводить обновление критичностей состояния систем, связанных с отказами других, зависимых систем. Неопределенность выбора функции принадлежности снижается за счет использования интервального нечеткого множества.

Результаты эвристического прогнозирования с использованием лингвистических вычислений должны уточняться с использованием вероятностных методов по мере накопления необходимой статистики.

Список литературы

1. Иванченко О.В. Метод причинно-следственной декомпозиции аварий и инцидентов критических инфраструктур[Текст] / О.В. Иванченко, В.С. Харченко // Радіоелектронні і комп'ютерні системи. – 2014. – С. 12-17.

2. Physical and Operational Margin Program Manual [Текст] /V&REnergy, Systems, Research, Inc. LosAngeles, CA. – 2010. – 34 p.

3. Rubinstein R.Y., Simulation and the Monte Carlo Method [Текст] / R.Y Rubinstein. – Wiley, 1981. - 278 p.

4. Dobson I. Complex Systems Analysis of Series of Blackouts: Cascading Failure, Critical Points, and Self-Organization / I. Dobson // Chaos. – 2007. – Vol. 17. – P. 123-140.

5. Hines P. Large Blackouts in North America:Historical Trends and Policy Implications[Текст] / P. Hines //Energy Policy. – 2009. – Vol. 37 (12). – P.57 - 67.

6. Безопасность критических инфраструктур: математические и инженерные методы анализа и обеспечения [Текст] / Под ред. В. С. Харченко. –Х.: НАКУ «ХАИ», 2011. – 641 с.

7. Zeng, W. Relations hip between similarity measure and entropy of interval valued fuzzy sets [Текст] / W. Zeng // Fuzzy Sets and Systems. – 2006. – 157. – P. 1477-1484.

Поступила в редколлегию 11.02.2015

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

МЕТОД ОЦІНЮВАННЯ РИЗИКІВКАСКАДНИХ ВІДМОВ (АВАРІЙ) З ВИКОРИСТАННЯМ ДИНАМІЧНИХ МАТРИЦЬ КРИТИЧНОСТІ

Є.В. Брежнєв

Каскадні (ланцюгові) відмови становлять ризики для критичних інфраструктур (КІ) та їх інформаційно-управляючих систем (ІУС). Каскадні відмови характеризуються великою важкістю наслідків, невизначеністю механізмів виникнення. В роботі пропонується метод оцінювання ризиків каскадних відмов (аварій) в умовах невизначеності, що пов'язана з відсутністю потрібних статистичних даних для визначення їх імовірнісних характеристик. Метод ґрунтується на використанні лінгвістичної апроксимації (ЛА), що дозволяє провести евристичне прогнозування розвитку каскадних аварій. Невизначеність вибору функції приналежності лінгвістичних термів стану безпеки знижується за рахунок використання інтервальних нечітких множин. В статті також запропоновано стратегії зниження ризиків каскадних відмов в КІ.

***Ключові слова**: каскадні відмови (аварії), ризик, критична інфраструктура, лінгвістична апроксимація, інтервальні нечіткі множини.*

METHOD OF CASCADING FAILURE (ACCIDENT) RISK ASSESSMENT BASED ON APPLICATION OF DINAMIC CRITICALITY MATRIX

E.V. Brezhnev

Cascading failures (accidents) bring the risks to critical infrastructures and their information and control systems (I&C). These failures are characterized by high severity of consequences, uncertainties of cascading mechanisms, etc. The method of cascading failures risk assessment under uncertainties caused by lack of statistical data is suggested in this paper. This method is based on application of linguistic approximation, which allows performing heuristic prognosis of cascading failures propagation. Uncertainties of selection of membership function are played down by utilization of interval fuzzy sets. The generic strategies of handling these risks are also suggested in the paper.

***Keywords**: cascading failures (accidents), risk, critical infrastructure, linguistic approximation, interval fuzzy sets.*