УДК 621.039.058

А.Л. КЛЕВЦОВ

Государственный НТЦ по ядерной и радиационной безопасности, Украина

МОДЕЛЬ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ И УПРАВЛЯЮЩИХ СИСТЕМ АЭС ПРИ ЭКСПЕРТИЗЕ ЯДЕРНОЙ И РАДИАЦИОННОЙ БЕЗОПАСНОСТИ

В статье описывается общая модель оценки безопасности информационных и управляющих систем (ИУС) АЭС при экспертизе ядерной и радиационной безопасности (ЯРБ), построенная с учетом практического опыта нормирования и оценки безопасности ИУС АЭС в рамках выполнения экспертиз ЯРБ в Харьковском филиале ГНТЦ ЯРБ. Также в статье рассматриваются принципы диверсной оценки надежности ИУС АЭС при экспертизе ЯРБ.

информационные и управляющие системы, атомные электростанции, оценка безопасности, экспертиза ядерной и радиационной безопасности, надежность, регулирующие требования

Введение

Для ИУС АЭС проводится оценка безопасности в рамках выполнения Государственной экспертизы ядерной и радиационной безопасности (ЯРБ) [1]. Оценка безопасности ИУС осуществляется экспертной организацией (например, ГНТЦ ЯРБ) при их разработке, испытаниях и внедрении на АЭС.

При выполнении государственной экспертизы ядерной и радиационной безопасности (ЯРБ) объектом оценки безопасности являются конкретные новые/модернизируемые ИУС и их компоненты: программно-технические комплексы (ПТК); технические средства автоматизации (ТСА); программное обеспечение (ПО).

Предметом оценки безопасности могут быть проектные, конструкторские, технологические, программные, организационно-распорядительные и иные документы, относящиеся к объекту оценки и содержащие необходимые сведения, на основании которых производится оценка безопасности (далее – документы, обосновывающие безопасность).

Оценка безопасности при экспертизе состоит в проверке соответствия ИУС АЭС (на основе информации приведенной в документах, обосновывающих безопасность) требованиям действующих в Украине нормативных документов (далее – НД) по ЯРБ.

В настоящее время проведение оценка безопасности ИУС АЭС основана на логическом анализе документов и не автоматизирована. В связи с этим представляет интерес построение математических моделей, описывающих оценку выполнения требований при экспертизе ЯРБ. Создание таких моделей направлено на разработку автоматизированных систем поддержки экспертной деятельности.

Общая модель оценки безопасности ИУС АЭС при экспертизе ЯРБ

Опыт оценки безопасности ИУС АЭС, накопленный специалистами ХФ ГНТЦ ЯРБ, позволяет формализовать этот процесс и построить общую математическую модель.

Процедуру оценки безопасности ИУС АЭС можно условно разбить на два больших этапа.

Этап 1. Формирование критериев оценки для проведения экспертиз ЯРБ

На этом этапе с учетом опыта нормирования и оценки безопасности ИУС АЭС на основе действующих в Украине норм, правил и стандартов, а также на основе международных стандартов (IAEA,

IEC, ISO, IEEE и т.д.), формируется множество $M_{НД}$, которое содержит полный набор НД по ЯРБ:

$$M_{НД} = \{c_1, c_2, ..., c_p\},$$

где $c_1, c_2, \ldots, c_p$ – НД по ЯРБ.

На экспертизу представляются обосновывающие безопасность документы разного типа (например, техническое решение, технические условия, техническое задание, программы и методики испытаний, отчет по анализу безопасности и т.д.). Для оценки и анализа каждого типа документа, обосновывающего безопасность, при экспертизе используется определенный набор НД.

Представляемые документы относятся к определенному типу ИУС (система аварийной и предупредительной защит, система внутриреакторного контроля, система управления машиной перегрузочной, и т.д.). Оценка и анализ безопасности конкретного типа ИУС АЭС проводится на основе требований соответствующего набора НД.

Исходя из этого, можно ввести функцию $F_{НДЭ}$ для установления соответствия между типом экспертируемого документа и относящимися к нему НД, а также между типом ИУС АЭС и НД, в которых установлены требования к данному типу систем. При этом должны также учитываться дополнительные факторы, которые позволяют сформировать множество $M_{НДЭ}$, содержащее перечень НД, непосредственно используемых при экспертизе:

$$M_{НДЭ} = F_{НДЭ}(M_{НД}, K_Б, E_О, S_{ЖЦ}, T_{ИУС}, T_Д),$$

где $K_Б$ – класс безопасности ИУС АЭС (2 или 3);

$E_О$ – объект экспертизы (ИУС/ПТК, ТСА или ПО);

$S_{ЖЦ}$ – этап жизненного цикла ИУС;

$T_{ИУС}$ – конкретный тип ИУС АЭС;

$T_Д$ – конкретный тип документа, обосновывающего безопасность.

Получаемое с помощью функции $F_{НДЭ}$ множество $M_{НДЭ}$ является подмножеством множества $M_{НД}$:

$$M_{НДЭ} \subset M_{НД};$$

$$M_{НДЭ} = \{d_1, d_2, ..., d_s\};$$

где $d_1, d_2, \ldots, d_s$ – НД, на основании требований, которых производится анализ и оценка определенного типа документов, обосновывающих безопасность соответствующей ИУС АЭС.

Из каждого НД, который является элементом множества $M_{НДЭ}$, может быть выделено множество установленных в нем требований по ЯРБ:

$$d_1 \Rightarrow R_1,\ d_2 \Rightarrow R_2,\ \ldots,\ d_s \Rightarrow R_s,$$

где $R_1, R_2, \ldots, R_s$ – множества требований каждого отдельно взятого НД.

Путем объединения указанных множеств формируется множество M_T требований всех НД, используемых при экспертизе

$$M_T = R_1 \cup R_2 \cup \ldots \cup R_s.$$

Следует отметить, что в общем случае полученное множество M_T содержит как те требования, которые относятся к экспертируемому документу и оцениваемой ИУС, так и те требования, которые не имеют к ним непосредственного отношения.

Это объясняется тем, что НД, как правило, аккумулируют в себе требованиям к множеству различных ИУС и документов, обосновывающих безопасность, а при проведении экспертизу необходимо выделить из них только требования, которые регламентированы строго для конкретной ИУС АЭС и для конкретного типа документа, обосновывающего безопасность.

Применяя функцию $F_{ТЭ}$ из всего множества M_T можно выделить подмножество $M_{ТЭ}$, содержащее только требования, которые имеют непосредственное отношение к представленному на экспертизу документу, обосновывающему безопасность конкретной ИУС АЭС:

$$M_{ТЭ} = F_{ТЭ}(M_T, K_Б, E_О, S_{ЖЦ}, T_{ИУС}, T_Д);$$

$$M_{ТЭ} \subset M_T;$$

$$M_{ТЭ} = \{y_1, y_2, ..., y_m\},$$

где $y_1, y_2, \ldots, y_m$ – требования НД, которые используются для анализа и оценки конкретного документы, обосновывающего безопасность ИУС АЭС.

В результате описанного выделения множества требований $M_{TЭ}$, сформированы критерии экспертной оценки представленного документа, обосновывающего безопасность ИУС АЭС.

Формирование рассмотренных множеств является задачей верхнего уровня, поскольку они должны создаваться не для каждой отдельной экспертизы, а являются общими и могут быть использоваться при проведении экспертиз различных документов и различных ИУС. Реализация указанных множеств в виде таблиц баз данных (БД) [2 3] позволит автоматизировать выборку необходимых НД и регулирующих требований.

Этап 2. Выполнение анализа и оценки документа, обосновывающего безопасность ИУС АЭС, на соответствие требованиям НД по ЯРБ

На втором этапе осуществляется оценка представленного документа, обосновывающего безопасность конкретной ИУС АЭС, на соответствие регулирующим требованиям НД по ЯРБ. Для этого, прежде всего, описанным выше способом формируются множества $M_{НДЭ}$ и $M_{TЭ}$.

Далее введем множество $M_{TД}$, которое содержит требования, отраженные в оцениваемом документе.

$$M_{TД} = \{x_1, x_2, \ldots, x_n\}$$

где $x_1, x_2, \ldots, x_n$ – регулирующие требования, отраженные в оцениваемом документе.

При проведении экспертизы осуществляется сопоставление и оценка соответствия требований НД (элементы множества $M_{TЭ}$) требованиям, отраженным в экспертируемом документе (элементы множества $M_{TД}$). Таким образом, может быть получено множество M_{TC} отраженных в экспертируемом документе требований, которые соответствуют требованиям НД. Множество M_{TC} является пересечением множеств $M_{TЭ}$ и $M_{TД}$:

$$M_{TC} = M_{TЭ} \cap M_{TД}.$$

Результат экспертизы является положительным только в том случае, если выполнение всех предъявляемых требования НД в достаточной степени отражено в оцениваемом документе, т.е. если $M_{TC} = M_{TД}$. Если же выполнение хотя бы части обязательных требований НД не отражено в оцениваемом документе, т.е. $M_{TC} \neq M_{TД}$, то результат экспертизы будет отрицательным.

Необходимо отметить, что каждое из базовых требований НД может подразделяться на несколько требований более низкого уровня иерархии, а те в свою очередь могут включать в себя требования еще более низкого уровня и т.д.

В общем случае оценка выполнения каждого конкретного регулирующего требования самого нижнего уровня иерархии в экспертируемом документе может осуществляться путем проверки соответствия на основе двухместного предиката [4] следующего вида:

$$P_N(x, y_N) = \text{“}x \text{ соответствует } y_N\text{”}$$

где y_N – требование НД;

x – требование, отраженное в документе обосновывающем безопасность;

N – нижний уровней иерархии требований НД.

Для оценки соответствия требований уровня иерархии *(N-1)* на основе соответствия требований уровня иерархии N можно ввести функцию вида:

$$F_{N-1}(x, y_N) = \begin{cases} 0, \forall y_{Ni} \neg \exists x_j : P_N(x_j, y_{Ni}); \\ (0, 1), \exists y_{Ni} \exists x_j : P_N(x_j, y_{Ni}); \\ \qquad \wedge \exists y_{Ni} \neg \exists x_j : P_N(x_j, y_{Ni}); \\ 1, \forall y_{Ni} \exists x_j : P_N(x_j, y_{Ni}), \end{cases}$$

где $i = \overline{1,n}$ (n – количество требований НД на уровне иерархии N); $j = \overline{1,m}$, (m – общее количество требований, отраженных в экспертируемом документе).

Вышеприведенную формулу можно интерпретировать следующим образом. Функция $F_{N-1}(x, y_N)$ равна:

– 0, если все предикаты возвращают значение 0, т.е. ни одно из регулирующих требований не отражено в экспертируемом документе;

– 1, если все предикаты возвращают значение 1, т.е. все регулирующие требований полностью отражены в экспертируемом документе;

– числу в диапазоне (0, 1), если часть предикатов возвращает значение 1, а часть – 0, т.е. регулирующие требования отражены в экспертируемом документе частично.

В свою очередь для более высоких уровней иерархии значение функции $F_K(x, y_{K+1})$ рассчитывается следующим образом:

$$F_K(x,y_{K+1}) = \begin{cases} 0, \forall y_{(K+1)i} \forall x_j : F_{(K+1)i}(x_j, y_{(K+1)i}) = 0; \\ (0,\ 1), \exists y_{(K+1)i} \exists x_j : 0 \le F_{(K+1)i}(x_j, y_{(K+1)i}) < 1; \\ 1, \forall y_{(K+1)i} \forall x_j : F_{(K+1)i}(x_j, y_{(K+1)i}) = 1, \end{cases}$$

где K – уровень требования в иерархии требований НД (при этом $K = \overline{1,(N-1)}$).

Самый высокий уровень иерархии (при K=1) соответствует базовым регулирующим требованиям, предъявляемым к документу, обосновывающему безопасность ИУС АЭС.

Иными словами, приведенную выше формулу можно интерпретировать следующим образом. Требование уровня иерархии K можно считать полностью выполненным, только в том случае, если для него выполнены все относящиеся к нему требования уровня иерархии *(K+1)*. В противном случае, требование считается невыполненным или выполненным частично.

При частичном выполнении требования конкретное значение функции $F_K(x, y_{K+1})$ может быть определено, например, следующим образом:

$$F_K(x, y_{K+1}) = \frac{q+s}{m},$$

где q – количество регулирующих требований уровня иерархии *(K+1)*, выполнение которых отражено в документе, обосновывающем безопасность;

m – общее количество требований на уровне иерархии *(K+1)*;

s – поправочный коэффициент, который корректирует значение функции $F_K(x, y_{K+1})$, с учетом степени влияния на безопасность замечаний к тем требованиям, выполнение которых недостаточно отражено в документе, обосновывающем безопасность.

Экспертная оценка отчетов по анализу надежности с применением диверсного расчета

Одним из важных этапов оценки безопасности ИУС/ПТК АЭС является экспертиза отчетов о проектной оценке надежности (ПОН). Оценка этого типа документов не в полной мере может быть описана приведенной выше моделью, поскольку при экспертизе ПОН возникает необходимость в проверке правильности проведенных предприятием-разработчиком расчетов надежности ИУС/ПТК.

В настоящее время в Украине отсутствуют НД, которые бы жестко регламентировали как методы расчета надежности ИУС/ПТК АЭС, так и методы выполнения экспертизы ПОН ИУС/ПТК АЭС. Классический подход к экспертизе ПОН состоит в проверке правильности выполненного предприятием-разработчиком расчета показателей надежности выполнения функций ИУС/ПТК АЭС. При этом в процессе экспертизы анализируется следующая информация:

– состав и функциональные взаимосвязи между техническими средствами, входящими в ИУС/ПТК АЭС;

– регламентированные в ТЗ требования к надежности выполнения функций ИУС/ПТК АЭС;

– допущения, принятые при расчете надежности;

– методика расчета показателей надежности;

– исходные данные для расчета надежности;

– структурные схемы надежности (ССН) выполнения функций ИУС/ПТК АЭС;

– расчет показателей надежности;

– результаты расчета надежности;

– выводы по результатам расчета надежности.

С целью повышения достоверности результатов экспертной оценки ПОН предлагается применять независимый диверсный расчет надежности. Применение такого подхода расширяет стандартную методику экспертной оценки ПОН.

1. По результатам экспертной оценки в соответствии с проектной документацией уточняется состав и функциональные взаимосвязи между техническими средствами, входящими в ИУС/ПТК АЭС.

2. По результатам экспертной оценки регламентированных в ТЗ требований к надежности выполнения функций ИУС/ПТК АЭС, они уточняются и приводятся в соответствие с действующими НД.

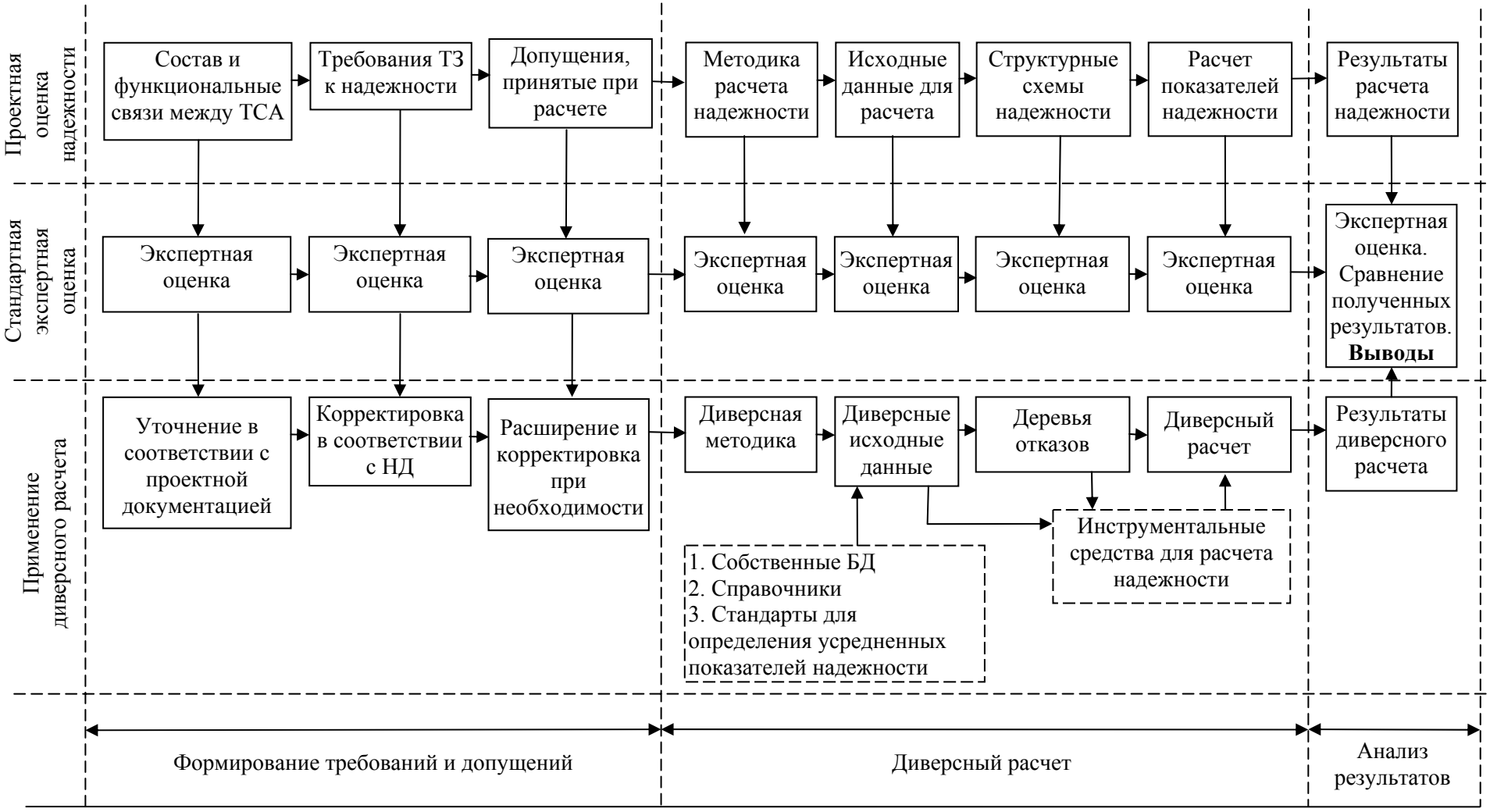

Рис. 1. Схема экспертной оценки отчета по анализу надежности ИУС АЭС

3. По результатам экспертной оценки расширяются и корректируются допущения, принятые при расчете надежности.

4. Предлагается альтернативная методика расчета надежности (если это возможно и необходимо).

5. На основе собственных БД, справочников и стандартов для определения усредненных показателей надежности (например, [5]) задаются диверсные исходные данные для расчета надежности.

6. Вместо ССН для расчета надежности строятся деревья отказов по каждой функции, выполняемой ИУС/ПТК АЭС.

7. С помощью специализированных инструментальных средств (например, RiskSpectrum [6] или Saphire [7]) производится расчет показателей надежности выполнения каждой функции ИУС/ПТК АЭС. Диверсный расчет надежности может проводиться в полном объеме или выборочно для отдельных функций ИУС/ПТК.

8. Проводится анализ полученных результатов и их сравнение с результатами, представленными в экспертируемом ПОН.

9. Формулируются выводы и рекомендации по результатам экспертной оценки с применением диверсного расчета надежности.

Схема экспертной оценки ПОН (с использованием стандартного подхода и с применением независимого диверсного расчета) представлена на рис. 1.

Выводы

1. Предложена общая модель оценки безопасности при выполнении экспертиз ЯРБ, которая в дальнейшем может стать основой для создания автоматизированной системы поддержки экспертной деятельности.

2. Применение диверсного расчета надежности существенно повышает качество и достоверность экспертной оценки ПОН, поскольку он выполняется независимой группой специалистов с использованием альтернативных методов, исходных данных и инструментальных средств расчета надежности.

Литература

1. Ястребенецкий М.А., Васильченко В.Н., Виноградская С.В., Гольдрин В.М., Розен Ю.В., Спектор Л.И., Харченко В.С. Безопасность атомных станций: информационные и управляющие системы (под ред. М.А.Ястребенецкого). – К.: Техника, 2004. – 471 с.

2. Клевцов А.Л. База знаний для оценки безопасности информационных и управляющих систем АЭС // Радіоелектронні і комп'ютерні системи. – 2007 .– № 7. – С. 114-120.

3. Клевцов А.Л. Создание и применение базы знаний для поддержки экспертной деятельности в области ИУС АЭС // Ядерная и радиационная безопасность. К.: ГНТЦ ЯРБ, 2007. – № 1. – С. 86-97.

4. Косовский Н.К., Тишков А.В. Логики конечнозначных предикатов на основе неравенств. – СПб: СПбГТУ, 2000. – 268 с.

5. MIL-HDBK-217F. Military Handbook. Reliability prediction of electronic equipment. USA: Department of Defense, 1991. – 205 p.

6. Guideline for applying Software Tool Risk Spectrum PSA Professional in assessment of NPP I&C reliability. – Kyiv: SSTC NRS, 2005. – 45 p.

7. Saphire – Risk and Reliability Assessment Tool [Электронный ресурс]. – Режим доступа: https://saphire.inl.gov.

Поступила в редакцию 22.02.2008

Рецензент: д-р техн. наук, проф. М.А. Ястребенецкий, Государственный научно-технический центр по ядерной и радиационной безопасности, Харьков.