

МО України, військова частина А1906, 2003. – С. 149-158. 11. Питерсон Дж. Теория сетей Петри и моделирование систем: Пер. с англ. – М.: Мир, 1984. – 263 с. 12. Popek G., Farber D. A model for verification of data security in operating systems // Communications of the ACM. – 1978. – V. 21, № 9. – P. 737-749.

УДК 004.56.021.2: 510.22 (043.2)

ЭКСПЕРТИЗА В СИСТЕМЕ ТЗИ НА ОСНОВЕ НЕЧЕТКИХ МНОЖЕСТВ

Александр Корченко, Вячеслав Потапов, Виктория Рындюк

Национальный авиационный университет

Аннотация: На основе нечетких множеств предлагается методология оценки соответствия гарантий защищенности информации требованиям стандартов безопасности для систем ТЗИ в программно-управляемых автоматических телефонных станциях (АТС).

Summary: Proposed methods of evaluating quality relevant of documentation supporting to security standards requirements for technical defenses at computer-controlled automatic telephone stations on fuzzy-sets basis.

Ключевые слова: Критерии оценки, уровни гарантий, нечеткие множества, нечеткие числа.

I Введение

Для эффективного решения ряда проблем в области безопасности информационных технологий используются различные мероприятия, из которых можно выделить следующие: анализ угроз; разработка, выбор и применение мер и средств безопасности, адекватных угрозам; сертификация и аккредитация систем безопасности; планирование и организация действий в непредвиденных обстоятельствах [1]. В различных организациях (в частности, правительственных) важным элементом управления риском является экспертиза, как техническое подтверждение того, что меры безопасности и контроля, подобранные для определенного средства защиты информации, соответствуют стандартам и нормально функционируют.

II Постановка задачи

Стандартами по технической защите информации (ТЗИ) Украины, содержащими различные критерии оценки защищенности информации, являются [2 – 5]. Данные критерии определяют уровни реализованных услуг в сочетании с уровнем гарантий.

Эксперты, однако, при практическом использовании существующих стандартов не всегда могут четко детерминировать оцениваемые параметры и, таким образом, в процесс решения вносятся элементы нечеткости, размытости. Поэтому для эффективного использования данных нормативных документов дополнительно требуется разработка методик, осуществляющих оценку защищенности информационных ресурсов с учетом качественных показателей. Отсюда также следует, что теоретическая база, которая может применяться для решения задач защиты информационных ресурсов автоматизированных систем, недостаточно развита. Это особенно важно в тех случаях, когда нет полной информации о системе, а исходные данные, подлежащие обработке, связаны с суждениями и интуицией человека. Наиболее подходящим инструментом для решения указанных задач является аппарат теории нечетких множеств, оперирующий такими понятиями, как нечеткие числа (НЧ), нечеткие операции и др.

На программно-управляемых АТС оценке подлежат [3] корректность реализации системы ТЗИ и уровень доверия к заключению о корректности ее реализации. Процесс оценки уровня доверия состоит, в основном, в последовательном пересмотре и перепроверке результатов и условий разработки, изготовления, испытаний, поставки, введения в действие и эксплуатации оцениваемой АТС на соответствие заданным в [5] критериям доверия. Перечень, содержание и форма необходимых для анализа документов, уровень детализации, обоснований и доказательств, прилагаемых заявителем относительно разных аспектов реализованной на АТС систем ТЗИ, однозначно зависят от заявленного уровня доверия к корректности реализации системы защиты. Эта зависимость отображена в соответствующих требованиях [4, 5].

Особого внимания при проведении экспертизы ТЗИ на АТС заслуживает вопрос проверки выполнения нормативных гарантий защищенности информации с целью оценки уровня доверия к корректности реализации системы ТЗИ, поскольку методика качественного оценивания автоматизированных систем описана лишь в общих чертах и нет реального инструмента для подобной оценки. Следует также отметить, что рассматриваемый стандарт основан на принципе минимальности, и не позволяет учитывать промежуточные оценки и максимумы в оценках уровней гарантий.

В [4] даны спецификации гарантий защиты информационных ресурсов функционирования автоматизированных систем. Гарантии специфицированы по пяти аспектам: 1) гарантии безопасности среды персонала; 2) гарантии стандартизации технологической среды (ТС); 3) гарантии обеспечения наблюдаемости и управляемости ТС; 4) гарантии обеспечения конфиденциальности и целостности информационных ресурсов ТС; 5) гарантии качества документационного обеспечения (ДО).

III Основная часть

Учитывая вышеизложенное, на основе методов, применяемых в теории и практике безопасности информации, а также в теории нечетких множеств, предлагается методология оценки защиты информационных ресурсов ТС функционирования автоматизированных систем. Она включает следующие этапы: 1) определение соответствующих ТС в зависимости от оцениваемого аспекта; 2) выбор метода и, на основании мнений одного или группы экспертов, формирование нечетких эталонов лингвистических термов для каждого из определенных видов требований, указанных в спецификации; 3) выбор метода (по усмотрению эксперта и, на основании мнений одного или группы экспертов, формирование нечетких переменных оцениваемых требований); 4) сравнение эталонных и полученных значений; 5) установление соответствия полученных результатов определенному уровню гарантий.

На рис. 1 приведена схема оценки систем ТЗИ на программно-управляемых АТС, в которой использованы обозначения:

- $y=\{1, 2, 3, 4, 6\}$ – показатель оцениваемого аспекта [4]; при $y=1$ оценке подлежит безопасность среды персонала, при $y=2$ – качество ДО, при $y=3$ – стандартизация ТС, при $y=4$ – обеспечение конфиденциальности и целостности информационных ресурсов ТС, а при $y=6$ – обеспечение наблюдаемости и управляемости ТС;

- j – количество нечетких требований в i -ой ТС: $j=\overline{1, J}$, где $J=\overline{1, 7}$ – максимальное количество требований;

- m_q – количество видов требований, $q=\overline{1, M}$, $M=\overline{1, 41}$ – максимальное количество видов требований;

- ЗЭ – завершение экспертизы;

- КЭ – количество экспертов;

- БА – блок анализа;

- ЛП – лингвистические переменные;

- $\Gamma(U_{sp}i - G)$ – уровень гарантий определенного аспекта в i -ой ТС, G – показатель уровня гарантий.

Обозначения для используемых методов, приведенные на рис. 1, такие: СТАТ – статистические, ПАР – параметрические, ИНТ – интервальные, КПС – количественных парных сравнений, УМН – уровневых множеств, ММ – максиминный, ЦТ – центра тяжести, БР – на основе операций “больше или равно”, ФУП – функция упорядочения единичного интервала, УНЧ – упорядочения НЧ, УИО – упорядочения нечетких множеств с использованием отношений, РХ – расстояние Хемминга, АУР – α -уровневое расстояние.

Рассмотрим вопросы организации экспертиз на примере оценки качества ДО. Основные требования к качеству ДО, указанные в спецификациях [4], таковы: 1) требования к полноте (Т2.1), 2) требования к уровню детализации описания среды и (или) технологий (Т2.2), 3) требования к достоверности информации (Т2.3) и 4) требования к качеству оформления (Т2.4).

В свою очередь, требования к полноте включают: а) охват отдельных элементов среды и (или) технологий (Т2.1.1), б) охват критически важных элементов среды и (или) технологий (Т2.1.2), в) охват всех основных подсистем сред и (или) технологий (Т2.1.3), г) полный охват всех элементов среды и технологий (Т2.1.4).

Требования к уровню детализации описания среды и (или) технологий включают: а) описание общих характеристик элементов среды и (или) технологий (Т2.2.1), б) описание среды и (или) технологий на уровне структурных схем и обобщенных алгоритмов работы (Т2.2.2), в) описание среды и (или) технологий на уровне функциональных схем и детальных алгоритмов работы (Т2.2.3), а также г) детальное описание среды и (или) технологий на уровне принципиальных схем, программ ЭВМ, инструкций по эксплуатации (Т2.2.4).

Требования к достоверности информации, содержащейся в ДО, подразумевают: а) не больше одной грамматической ошибки на одну страницу машинописного текста (Т2.3.1), б) не больше одной грамматической ошибки на десять страниц машинописного текста (Т2.3.2), в) отсутствие искажения содержания, которое описывает процессы (отсутствие семантических ошибок) (Т2.3.3) и г) отсутствие ошибок в числовых данных, наименованиях идентификаторов, текстах программ для ЭВМ (Т2.3.4).

Требование к качеству предоставляемого ДО подразумевает оформление соответственно к требованиям нормативных документов (Т2.4.1). В [3] также приведены спецификации уровней гарантий ДО в соответствии с требованиями к его качеству. Выделено четыре уровня гарантий качества (УГК): 1) $\Gamma(\text{УКД}i-0)$ –

нулевой, 2) Г(УКДі-1) – первый, 3) Г(УКДі-2) – второй и 4) Г(УКДі-3) – третий. Здесь УКДі – мнемоническое обозначение логического объекта документированности в і-ой ТС.

Для оценки качества ДО системы ТЗИ в АТС [3-5] подробно опишем методику оценивания.

1. Определение вида ДО (технологическое, конструкторское, эксплуатационное, программное). Пусть число всех видов документации N. Для оценки, в зависимости от описываемого объекта, эксперту предоставляется $p \leq N$ видов ДО и, следовательно, он выделяет соответствующие ТС, которые определяются этапами жизненного цикла описываемого объекта.

2. Определение согласно заявленному уровню доверия и соответствующим нормативным документам [3 - 5] в каждой выбранной і-ой ТС ($i = \overline{1, n}$) максимального количества элементов среды k_{ijmax} для каждого из j оцениваемых требований $T_{u,j}$ к качеству ДО (в данном случае количество нечетких требований $j = \overline{1, 2}$, а $u=2$). Здесь и далее под нечеткими требованиями будем понимать размытые, недостаточно детерминированные или формализованные требования, относительно которых при формализации мнений эксперта привлекаются методы нечетких множеств. Требования Т2.3 и Т2.4 соответственно к достоверности и качеству оформления ДО не принимаются во внимание, поскольку они являются четкими.

3. Определение интервалов $[\underline{k}_{ijm}, \overline{k}_{ijm}]$ для каждого из m_q (в данном случае $m_q = m = \overline{1, 4}$) видов требований $T_{2,j,m}$ к документации, т. е. интервалов, задающих количества элементов среды, которые, по мнению эксперта, должны оцениваться для каждого из m видов требований.

4. Формирование лингвистических термов. Для определения лингвистических переменных “Полнота”, “Уровень детализации”, “Достоверность” необходимо для каждого из $T_{2,j,m}$ видов требований к ДО задать базовые терм-множества $T_{jm} = \{T_s\}$ ($s = \overline{1, L}$, где L – количество термов, используемых в качестве нечетких эталонов оцениваемых параметров). Терм-множества каждой из этих лингвистических переменных, например, при $L=3$, можно задать термами с названиями: малый (М), средний (С) и большой (Б), которые представляют собой наименования числовых нечетких переменных, т. е. НЧ. После определения количества термов и их названий необходимо построить их функции принадлежности, определив вид и способ построения.

5. Формирование экспертом НЧ соответствующих видов.

6. Определение оценочных коэффициентов (ОК), образованных в результате сравнения эталонных значений и экспертной оценки.

7. Определение соответствия каждого из полученных требований определенному УГК. Минимальный из УГК выбирается в качестве результирующего уровня.

Пусть оценивается определенный вид документации ($n=1, i=1$) при известном заявленном уровне доверия. Для общего описания методики данные факторы не имеют принципиального значения.

Пусть эксперт определил, что для оценки требования полноты (Т2.1) данной документации должно быть представлено максимум $k_{ijmax} = k_{11max} = 100$ описаний, следовательно, максимальное количество элементов среды равно 100. Рассмотрим методику оценки на примере требования Т2.1 к полноте ($j=1$).

Вначале для всех видов требования Т2.1.m определяются интервалы описанных элементов среды $[\underline{k}_{11m}, \overline{k}_{11m}]$, которые, по мнению эксперта, подлежат оценке при данном виде требований. Например, при рассмотрении требования Т2.1.1 будет оцениваться $[S_{111}^-] = [10, 40]$ элементов среды, при Т2.1.2 – $[S_{112}^-] = [30, 60]$ элементов среды, при Т2.1.3 – $[S_{113}^-] = [50, 80]$ элементов среды, при Т2.1.4 – $[S_{114}^-] = [70, 100]$ элементов среды. При этом нужно заметить, что интервалы оценок могут пересекаться.

Далее можно сформировать базовые терм-множества для каждого из $T_{2.1,m}$ видов требований. Их будем использовать в качестве эталонов. Для требования к полноте базовые терм-множества зададим тремя нечеткими термами с названиями: *малая* (М), *средняя* (С) и *большая* (Б), представляющими собой НЧ. Для построения функций принадлежности этих НЧ используем, к примеру, метод опроса формирования функций принадлежности группой экспертов [6].

В табл. 1, 2, 3 и 4 приведены результаты опроса, например, пяти экспертов соответственно для оценок Т2.1.1, Т2.1.2, Т2.1.3 и Т2.1.4.

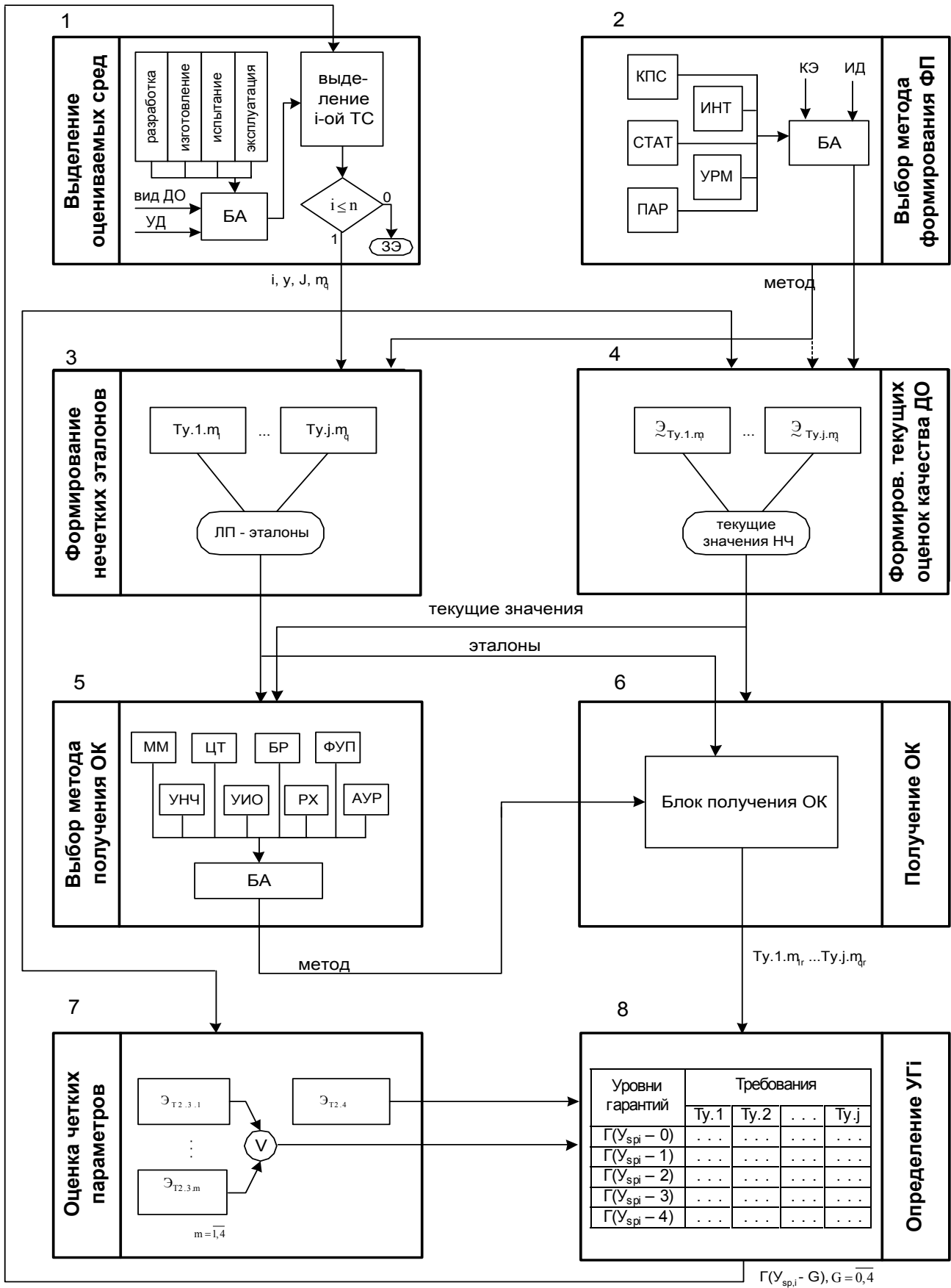


Рисунок 1 – Методика оценки системы ТЗИ на программно-управляемых АТС

Таблица 1 – Результаты опроса экспертов для T2.1.1

Значение лингвистической переменной	Количество элементов ТС			
	10	20	30	40
М	5	4	1	0
С	2	5	3	1
Б	0	3	4	5

Таблица 2 – Результаты опроса экспертов для T2.1.2

Значение лингвистической переменной	Количество элементов ТС			
	30	40	50	60
М	5	4	2	0
С	1	3	5	2
Б	0	1	4	5

На основании формул и по аналогии с примером [6] для каждого из видов требований получим значения НЧ: $\underline{M}_{T2.1.1}=\{1/10, 0.8/20, 0.2/30, 0/40\}$; $\underline{C}_{T2.1.1}=\{0.4/10, 1/20, 0.6/30, 0.2/40\}$; $\underline{B}_{T2.1.1}=\{0/10, 0.6/20, 0.8/30, 1/40\}$.

Аналогично получим НЧ для T2.1.2: $\underline{M}_{T2.1.2}=\{1/30, 0.8/40, 0.4/50, 0/60\}$; $\underline{C}_{T2.1.2}=\{0.2/30, 0.6/40, 1/50, 0.4/60\}$; $\underline{B}_{T2.1.2}=\{0/30, 0.2/40, 0.8/50, 1/60\}$.

Таблица 3 – Результаты опроса экспертов для T2.1.3

Значение лингвистической переменной	Количество элементов ТС			
	50	60	70	80
М	5	4	2	0
С	3	5	4	1
Б	0	1	3	5

Таблица 4 – Результаты опроса экспертов для T2.1.4

Значение лингвистической переменной	Количество элементов ТС			
	70	80	90	100
М	5	3	2	0
С	1	2	5	3
Б	0	1	4	5

Для T2.1.3 НЧ будут иметь вид: $\underline{M}_{T2.1.3}=\{1/50, 0.8/60, 0.4/70, 0/80\}$; $\underline{C}_{T2.1.3}=\{0.6/50, 1/60, 0.8/70, 0.2/80\}$; $\underline{B}_{T2.1.3}=\{0/50, 0.2/60, 0.6/70, 1/80\}$. Для T2.1.4 НЧ будут иметь вид: $\underline{M}_{T2.1.4}=\{1/70, 0.6/80, 0.4/90, 0/100\}$; $\underline{C}_{T2.1.4}=\{0.2/70, 0.4/80, 1/90, 0.6/100\}$; $\underline{B}_{T2.1.4}=\{0/70, 0.2/80, 0.8/90, 1/100\}$.

Аналогичным образом можно сформировать значения эталонов для требования T2.2.m.

Рассмотрим пример оценки эксплуатационного ДО. Пусть группа из пяти экспертов, используя метод опроса, получила следующее НЧ, характеризующее полноту ДО: $\underline{Z}_{T2.1} = \{0.4/ 40, 0.8/50, 1/60, 0.2/70\}$. Полученное НЧ

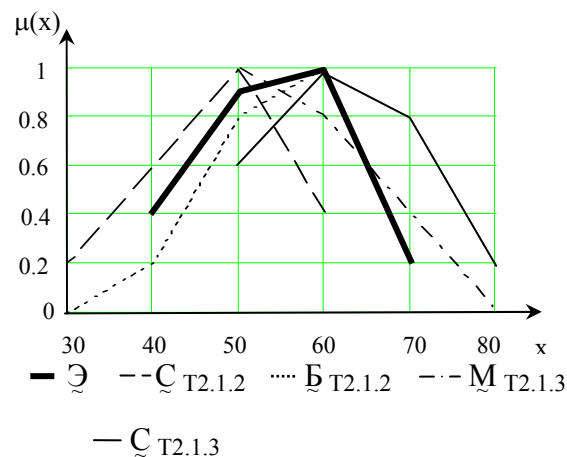


Рисунок 2 – Графики сравниваемых НЧ

сравним с эталонными. Для выполнения этой процедуры используем расстояние Хемминга [7] как наиболее подходящий метод для данного вида НЧ [8]. Заметим, что носители этого НЧ принадлежат интервалу [40, 60] и, значит, его следует сравнивать с НЧ, построенными для T1.2.2 и T1.2.3. Графики сравниваемых НЧ представлены на рис. 2. Сравнивая НЧ, получим, что $\underline{Z}_{T2.1}$ наиболее близко к $\underline{B}_{T2.1.2}$ и, следовательно, полнота ДО соответствует виду требования T2.1.2.

Пусть, например, в результате дальнейшей оценки получили для требования к детализации значение T2.2.3. Тогда, при условии выполнения требований T2.3.1, T2.3.3 и T2.4.1, являющихся четкими, данному ДО будет присвоен первый уровень гарантий: Г(УКДі-1), поскольку ему соответствует наименьшее из полученных видов требований (T2.1.2).

Данная методология обладает гибкостью, т. к. непосредственная оценка качества ДО может производиться как группой экспертов, например, с использованием метода опроса, так и одним экспертом, используя, например, треугольные или трапециевидные методы построения функций принадлежности [9]. При этом значение параметра k_{ijmax} может быть изменено (по усмотрению экспертов) и это не повлечет за

собой необходимости проведения новых экспертных опросов для формирования эталонных значений. В данном случае достаточно использовать переход к так называемым “универсальным шкалам” [10].

При проведении экспертиз встречаются случаи, когда представляют несколько изделий одного класса, которым в результате оценки был присвоен одинаковый уровень доверия и, соответственно, ДО получило одинаковые УГК. В таком случае возникает вопрос: какое из представленных изделий лучше выбрать для практического использования. Для решения подобных задач предлагается интегрированная оценка уровней гарантий. Она состоит из следующих этапов (рис. 3): 1) выделение для каждой из n сред p -ой АТС ($p = \overline{1, P}$) нечетких показателей $((T^{11}y.1.m_1, T^{11}y.j.m_q) \dots (T^{1n}y.1.m_1, T^{1n}y.j.m_q)) \dots ((T^{p1}y.1.m_1, T^{p1}y.j.m_q) \dots (T^{pn}y.1.m_1, T^{pn}y.j.m_q))$, определяющих уровень гарантий в данной среде; 2) выбор метода получения суммарного нечеткого показателя в зависимости от классов выделенных нечетких показателей; 3) определение суммарных нечетких показателей $\underline{S}_1 \dots \underline{S}_p$ всех ТС каждой из АТС; 4) перевод полученных значений суммарных нечетких показателей в универсальные шкалы; 5) выбор методов определения ОК; 6) определение ОК, образованных в результате сравнения суммарных нечетких показателей АТС; 7) сортировка АТС по ОК и выбор наилучшего варианта АТС.

Рассмотрим пример интегрированной оценки качества ДО. Тогда пункт 1 данной методики будет интерпретирован так: выделение для каждой из n сред p -ой АТС ($p = \overline{1, P}$) пары нечетких показателей $((T^{12.1.1.m_1, T^{12.2.1.m_2}) \dots (T^{1n.1.1.m_1, T^{1n.2.1.m_2})) \dots ((T^{p1.1.1.m_1, T^{p1.2.1.m_2}) \dots (T^{pn.1.1.m_1, T^{pn.2.1.m_2}))$, определяющих УГК ДО в данной среде. Требования Т2.3 и Т2.4 для данных АТС не рассматриваются, поскольку являются четкими и, по условию, выполненными для данных АТС, ДО которых имеет одинаковые УГК.

Пример 1. Пусть две оцениваемых АТС одного класса получили одинаковый УГК ДО – $\Gamma(\text{УКД}i-1)$. Для ДО₍₁₎ первой АТС и при $k_{ij\max}=100$, согласно описанной выше методике оценки качества ДО, были получены следующие НЧ: для требования к полноте $\underline{B}_{T2.1.2}=\{0/30, 0.2/40, 0.8/50, 1/60\}$, для требования к детализации $\underline{C}_{T2.2.3}=\{0.2/50, 0.6/60, 1/70, 0.4/80\}$, а для ДО₍₂₎ второй АТС ($k_{ij\max}=60$) соответственно $\underline{C}_{T2.1.3}=\{0.6/30, 1/36, 0.8/42, 0.2/48\}$, $\underline{M}_{T2.2.2} = \{1/18, 0.6/24, 0.2/30, 0/36\}$. Требования Т2.3 и Т2.4 выполнены и соответствуют второму УГК. Для данных АТС УГК были определены в первом случае – по показателю требования к полноте, который оказался минимальным, а во втором случае – по требованию к детализации.

Определим суммарный нечеткий показатель полученных оценок каждой из АТС. Для выполнения этой операции выберем метод ЛАЛМ при $\Omega_2=1$, описанный в [11]. Получим: $\underline{S}_1 = \underline{B}_{T2.1.2} \tilde{+} \underline{C}_{T2.2.3} = \{0/80, 0.2/90, 0.2/100, 0.6/110, 0.8/120, 1/130, 0.4/140\}$, $\underline{S}_2 = \underline{C}_{T2.1.3} \tilde{+} \underline{M}_{T2.2.2} = \{0.6/48, 1/54, 0.8/60, 0.6/66, 0.2/72, 0.2/78, 0/84\}$. Поскольку значения $k_{ij\max}$ различны для каждого из объектов, то для сравнения полученных величин используем переход к универсальным шкалам.

Получим следующие НЧ (см. рис. 4): $\underline{S}_{1u} = \{0/0.55, 0.2/0.65, 0.2/0.7, 0.6/0.8, 0.8/0.85, 1/0.9, 0.4/1\}$, $\underline{S}_{2u} = \{0.6/0.6, 1/0.65, 0.8/0.7, 0.6/0.8, 0.2/0.85, 0.2/9, 0/1\}$.

Исходя из классификации НЧ [8] и требований, предъявляемых к дискретизированным по α -уровням НЧ, для определения ОК применим метод ЦТ [9]. Получим следующие коэффициенты: ОК(\underline{S}_{1u})=0.856 и ОК(\underline{S}_{2u})=0.714. Имеем: $0.856 > 0.714$. Согласно условиям метода, это означает, что $\underline{S}_{1u} > \underline{S}_{2u}$, следовательно, первая АТС является более предпочтительной по сравнению со второй.

Проведем еще один эксперимент и изменим нечеткие показатели ДО₍₂₎, а четкие оставим прежними.

Пример 2. Рассмотрим данные из примера 1, в котором две оцениваемых АТС одного класса получили одинаковый УГК ДО – $\Gamma(\text{УКД}i-1)$. Пусть для ДО₍₂₎ показателю требования к полноте будет соответствовать эталон $\underline{C}_{T2.1.4}$, а показателю требования к детализации - $\underline{B}_{T2.2.4}$. В результате чего получим следующие нечеткие оценки: для ДО₍₁₎ ($k_{ij\max}=100$) $\underline{B}_{T2.1.2}=\{0/30, 0.2/40, 0.8/50, 1/60\}$ и $\underline{C}_{T2.2.3} = \{0.2/50, 0.6/60, 1/70, 0.4/80\}$, а для ДО₍₂₎ ($k_{ij\max}=60$) $\underline{C}_{T2.1.4}=\{0.2/42, 0.4/48, 1/54, 0.6/60\}$ и $\underline{B}_{T2.2.4}=\{0/42, 0.4/48, 0.6/54, 1/60\}$.

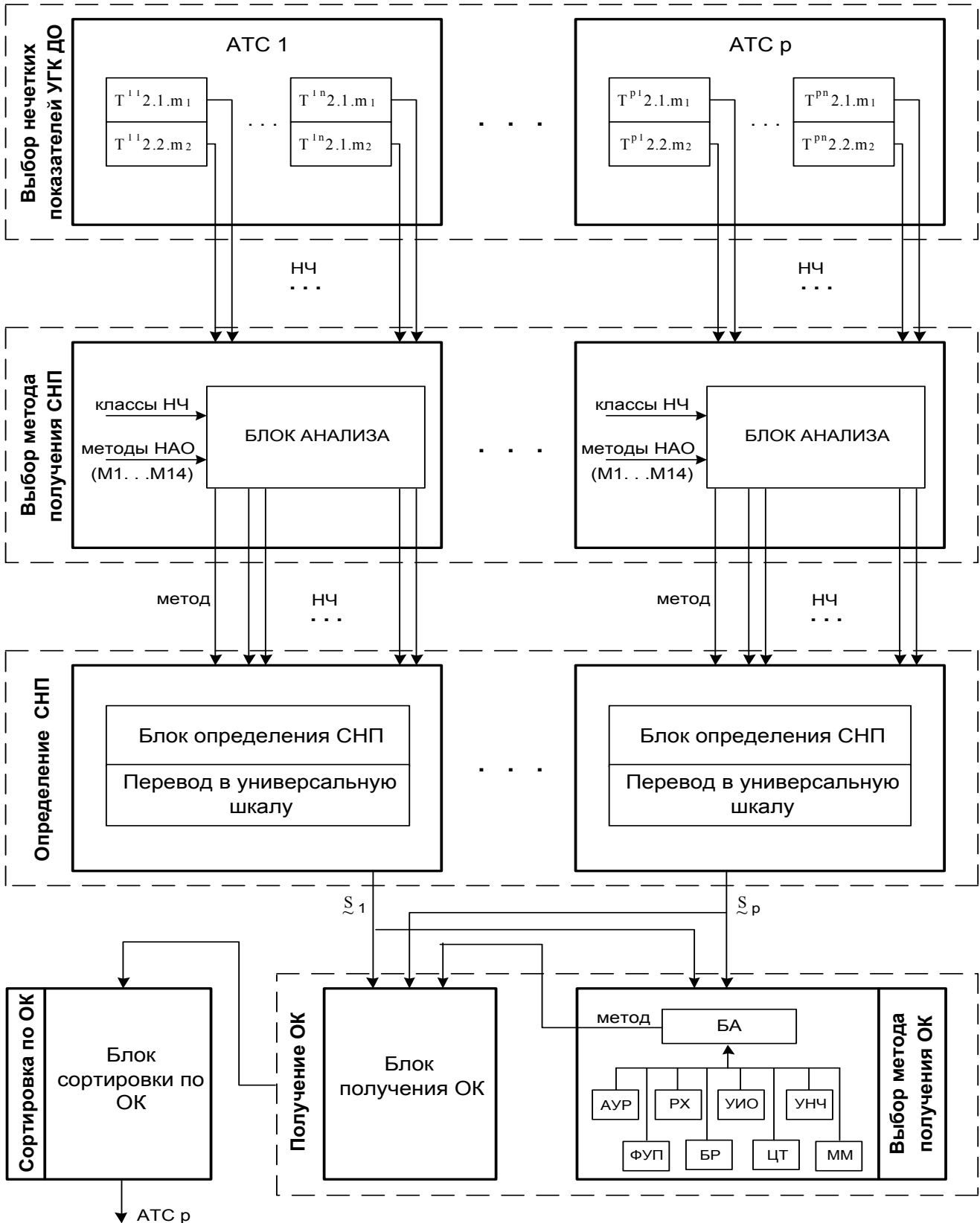


Рисунок 3 – Интегрированная оценка качества ДО

Требования T2.3 и T2.4 для $DO_{(1)}$ и $DO_{(2)}$ выполнены и соответствуют второму УГК ДО. Изменение данных показателей не повлияет на УГК ДО, т. к. они не являются минимальными и для $DO_{(2)}$ определяющими будут четкие показатели T2.3 и T2.4, а для $DO_{(1)}$ – по-прежнему T2.1.

Рассмотрим интегрированную оценку ДО. Вначале определим суммарные нечеткие показатели полученных оценок каждой из АТС. Для выполнения этой нечеткой операции, учитывая вид полученных НЧ [8] и исходя из проведенных исследований [11], выберем метод ЛАЛИМ при $\Omega_2=1$ [12]. Получим: $\tilde{S}_1 = \tilde{B}_{T2.1.2} \tilde{+} \tilde{C}_{T2.2.3} = \{0/80, 0.2/90, 0.2/100, 0.6/110, 0.8/120, 1/130, 0.4/140\}$, $\tilde{S}_2 = \tilde{C}_{T2.1.4} \tilde{+} \tilde{B}_{T2.2.4} = \{0/84, 0.2/90, 0.4/96, 0.4/102, 0.6/108, 1/114, 0.6/120\}$. Далее, согласно описанной выше методике проведения интегрированной оценки для сравнения различных величин (рис. 3), используем переход к универсальным шкалам. Получим следующие НЧ (рис. 5): $\tilde{S}_{1u} = \{0/0.55, 0.2/0.65, 0.2/0.7, 0.6/0.8, 0.8/0.85, 1/0.9, 0.4/1\}$, $\tilde{S}_{2u} = \{0/0.7, 0.2/0.75, 0.4/0.8, 0.4/0.85, 0.6/0.9, 1/0.95, 0.6/1\}$. Учитывая вид данных НЧ [8], для определения ОК снова применим метод ЦТ [9]. Получим следующие ОК: $OK(\tilde{S}_{1u})=0.856$ и $OK(\tilde{S}_{2u})=0.913$, а т. к. $0.913 > 0.856$, то $\tilde{S}_{2u} > \tilde{S}_{1u}$.

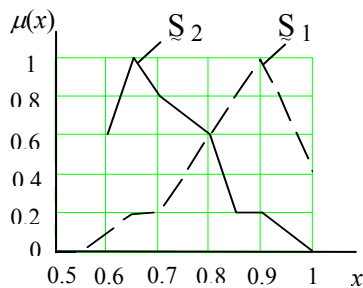


Рисунок 4 – НЧ \tilde{S}_{1u} и \tilde{S}_{2u} из примера 1

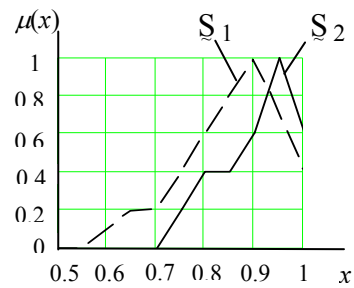


Рисунок 5 – НЧ \tilde{S}_{1u} и \tilde{S}_{2u} из примера 2

Как видим, ОК указывают на превосходство нечетких оценок $DO_{(2)}$, соответствующих $\Gamma(\text{УКД}i-3)$, что говорит о преимуществе второй АТС по сравнению с первой, оценки которой соответствуют $\Gamma(\text{УКД}i-2)$. Однако, согласно оценкам T2.3 и T2.4, являющимися определяющими показателями, в данном случае $DO_{(2)}$, как и $DO_{(1)}$, получит второй УГК.

Анализируя примеры 1 и 2, можно сделать вывод, что применение нечетких оценок дает возможность эксперту сделать предпочтение при выборе АТС, имеющих одинаковые уровни гарантий, поскольку даже при таких условиях интегрированные оценки $DO_{(1)}$ и $DO_{(2)}$ будут отличаться, что, в свою очередь, позволяет оценивающему специалисту более гибко применять данный стандарт.

Теперь проверим адекватность построенной модели.

Пример 3. Улучшим, по сравнению с данными примера 1, один из показателей второй АТС: пусть изменились требования к детализации, которые оказались близки к $\tilde{M}_{T2.2.4}$. В результате получим следующие оценки: для $DO_{(1)}$ $\tilde{B}_{T2.1.2} = \{0/30, 0.2/40, 0.8/50, 1/60\}$ и $\tilde{C}_{T2.2.3} = \{0.2/50, 0.6/60, 1/70, 0.4/80\}$, для $DO_{(2)}$ соответственно $\tilde{C}_{T2.1.3} = \{0.6/30, 1/36, 0.8/42, 0.2/48\}$, $\tilde{M}_{T2.2.4} = \{1/42, 0.8/48, 0.4/54, 0/60\}$. Требования T2.3 и T2.4 для $DO_{(1)}$ и $DO_{(2)}$ выполнены и соответствуют второму УГК. Теперь уровни гарантий для данных АТС определяются по требованиям к полноте, которые в обоих случаях является минимальными. Таким образом, $DO_{(1)}$ получит первый УГК, а $DO_{(2)}$ – второй. Как видим, улучшение определяющих показателей ведет к увеличению УГК.

Теперь проанализируем как ведет себя система при изменении показателей в пределах одного УГК.

Пример 4. Рассмотрим данные из примера 1, в котором две оцениваемых АТС одного класса получили одинаковый УГК ДО – $\Gamma(\text{УКД}i-1)$.

Изменим для $DO_{(2)}$ показатель требования к полноте, которому будет соответствовать эталон $\tilde{C}_{T2.1.4}$. В результате получим следующие нечеткие оценки: для $DO_{(1)}$ ($k_{ij\max}=100$) $\tilde{B}_{T2.1.2} = \{0/30, 0.2/40, 0.8/50, 1/60\}$ и

$\underline{C}_{T2.2.3} = \{0.2/50, 0.6/60, 1/70, 0.4/80\}$, а для $DO_{(2)}$ ($k_{ijmax}=60$) $\underline{C}_{T2.1.4}=\{0.2/42, 0.4/48, 1/54, 0.6/60\}$ и $\underline{M}_{T2.2.2}=\{1/18, 0.6/24, 0.2/30, 0/36\}$.

Пусть требования T2.3 и T2.4 для $DO_{(1)}$ и $DO_{(2)}$ выполнены и соответствуют второму УГК ДО. Изменение данных показателей не влияет на УГК ДО, т. к. они не являются минимальными из всех показателей, определяющих этот уровень.

Рассмотрим интегрированную оценку ДО. Согласно описанной выше методике вначале определим суммарные нечеткие показатели полученных оценок каждой из АТС. Для выполнения этой нечеткой операции, учитывая вид полученных НЧ [8] и исходя из проведенных исследований [11], выберем метод ЛАЛИМ при $\Omega_2=1$ [12]. Получим: $\underline{S}_1 = \underline{B}_{T2.1.2} \tilde{+} \underline{C}_{T2.2.3} = \{0/80, 0.2/90, 0.2/100, 0.6/110, 0.8/120, 1/130, 0.4/140\}$, $\underline{S}_2 = \underline{C}_{T2.1.4} \tilde{+} \underline{M}_{T2.2.2} = \{0.2/60, 0.4/66, 1/72, 0.6/78, 0.6/84, 0.2/90, 0/96\}$.

Поскольку значения k_{ijmax} различны для каждого из объектов, то для сравнения полученных величин используем переход к универсальным шкалам и получим следующие НЧ (рис. 6): $\underline{S}_{1u} = \{0/0.55, 0.2/0.65, 0.2/0.7, 0.6/0.8, 0.8/0.85, 1/0.9, 0.4/1\}$, $\underline{S}_{2u} = \{0.2/0.6, 0.4/0.7, 1/0.75, 0.6/0.8, 0.6/0.85, 0.2/0.95, 0/1\}$.

Применяя метод ЦТ [9] для определения ОК, получим следующие результаты: $OK(\underline{S}_{1u})=0.856$ и $OK(\underline{S}_{2u})=0.717$. По-прежнему $\underline{S}_{1u} > \underline{S}_{2u}$, т.к. $0.856 > 0.717$. Однако, заметим, что с улучшением показателей \underline{S}_{1u} и \underline{S}_{2u} сближаются.

Данный эксперимент доказывает, что при изменении отдельных показателей, которые не являются определяющими для определения УГК ДО, система адекватно реагирует на подобные изменения. Так, в нашем примере, УГК ДО остался прежним, а ОК, как и сами НЧ, наглядно продемонстрировали изменение в лучшую сторону состояния системы.

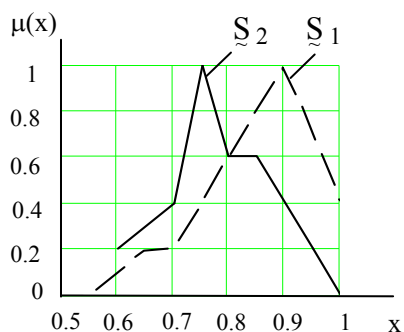


Рисунок 6 – НЧ \underline{S}_{1u} и \underline{S}_{2u} из примера 4

IV Выводы

В итоге можно сделать вывод, что построенная модель оценки качества защищенности информационных ресурсов АТС адекватно отображает реальный процесс, проходящий при осуществлении экспертных оценок.

Предложенная методология оценки качества может использоваться для решения соответствующих задач в различных областях техники при экспертных оценках, а также при создании новых, более гибких стандартов, особенно в случаях, когда присутствуют не полностью определенные параметры и существенную роль играет человеческий фактор.

По мнению авторов, эта методология может быть рекомендована, в частности, для оценки качества ДО в стандарте “Критерии оценки защищенности информации в КС от НСД”.

Литература: 1. Стенг Д., Мун С. Секреты безопасности сетей. - К.: Диалектика, 1995. – 544 с. 2. НД ТЗИ 2.5-004-99. Критерии оценки защищенности информации в компьютерных системах от несанкционированного доступа. - Введ.01.07.99. – К.: ДСТСЗИ СБ Украины, 1999.- 38 с. 3. НД ТЗИ 2.3-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова). - Введ.01.07.99. – К.: ДСТСЗИ СБ Украины, 1999.- 62 с. 4. НД ТЗИ 2.5-002-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту.-Введ.01.07.99.–К.:ДСТСЗИ СБ Украины, 1999.-25 с. 5. НД ТЗИ 2.5-003-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту. - Введ. 01.07.99. – К.: ДСТСЗИ СБ Украины, 1999.- 117 с. 6. Корченко А. Г., Рындюк В. А. Исследование статистических методов формирования функций принадлежности // Сб. науч. тр. – К.: НАУ, 2002. – № 2 (9). – С. 54 – 60. 7. Кофман А. Введение в теорию нечетких множеств.- М.: Радио и связь, 1982.- 432 с. 8. Корченко А. Г., Рындюк В. А., Пацира Е. В. Классификация нечетких чисел для рационального применения в методах и моделях систем защиты информации // Матеріали V Міжнародн.