УДК 004.056.5(045)

КАЧЕСТВЕННО-КОЛИЧЕСТВЕННЫЙ МЕТОД ОЦЕНИВАНИЯ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Александр Корченко, Светлана Казмирчук

В основу систем менеджмента информационной безопасности положены процессы анализа и оценивания рисков. Для их реализации применяются известные методы анализа и оценивания рисков, основанные на экспертных оценках. Часто в процессе оценивания возникают ситуации, при которых эксперт не всегда четко может оценить ту или иную уязвимость ресурсов информационных систем. В связи с этим целесообразно использовать соответствующие базы данных уязвимостей. Существующие подходы пока не позволяют эффективно решать поставленную задачу. Для этого предлагается качественно-количественный метод оценивания рисков. Он, в отличие от известных методов, путем использования оценок, которые предоставляются в существующих базах данных, позволяет автоматизировать процесс оценивания рисков и не привлекать для этого экспертов соответствующей предметной области.

Ключевые слова: *риск, оценивание рисков, система анализа и оценивания рисков, параметры риска, нечеткая переменная, нечеткие числа, преобразования эталонов нечетких чисел, качественно-количественный метод оценивания рисков, база данных уязвимостей.*

Основной любой системы управления информационной безопасности (ИБ), согласно рекомендациям стандарта ISO/IEC 27001:2013, является менеджмент рисков. Процесс анализа и оценивания рисков (ОР) ИБ – это главная составляющая стандарта [1]. Для реализации такого рода процессов применяются методы ОР [2, 3], которые основываются на экспертных оценках.

Часто при таких оценках не всегда имеется возможность привлечения экспертов, а так же возникают ситуации, при которых эксперт не всегда однозначно может оценить ту или иную уязвимость ресурсов информационных систем (РИС). Для этого предлагается использовать соответствующие базы данных (БД) уязвимостей, в которых представлены их количественные оценки, например, такие как национальная база данных уязвимостей (США) (National Vulnerability Database (NVD)) [5]; банк данных угроз безопасности информации (Российская Федерация) [6]; открытая база данных уязвимостей (США) (Open Sourced Vulnerability Database OSVDB)) [7]; база данных уязвимостей IBM X-Force (США) [8], база данных записей уязвимостей US-CERT VND (США) [9], база данных уязвимостей SecurityFocus (США) [10] и т.д. Базовой составляющей таких БД являются CVSS (Common Vulnerability Scoring System) [11] – показатели, которые можно использовать в качестве альтернативы оценкам экспертов. Поэтому разработка метода ОР с использованием выше представленные БД, является актуальной задачей.

В связи с этим, цель данной работы направлена на разработку метода ОР, который позволит осуществить альтернативное оценивание рисков с использованием известных БД не привлекая экспертов соответствующей предметной области.

В основу такого метода положены исследования проведенные в [2-4]. Рассмотрим детально его работу, которая основывается на 11 шагах.

Шаг 1 (Определение полного множества идентификаторов РИС и уязвимостей). На первом шаге определяется полное множество идентификаторов всех РИС т.е. $\boldsymbol{RIS} = \{\bigcup_{rs=1}^{r} RIS_{rs}\}$, $(rs = \overline{1,r})$, где r – количество всех ресурсов (и соответственно их идентификаторов) и полное множество уязвимостей $\boldsymbol{V} = \{\bigcup_{uz=1}^{n} V_{uz}\}$, $(uz = \overline{1,n})$, где n – количество всех уязвимостей (и соответственно их идентификаторов). На основе $\boldsymbol{RIS}$ и $\boldsymbol{V}$ эксперты могут определять множества РИС и уязвимостей по оцениваемому объекту. Для создания соответствующих множеств в качестве основы, например, может использоваться известная БД уязвимостей NVD [5].

Шаг 2 (Определение множества идентификаторов РИС и уязвимостей для объекта оценивания). Здесь на основе множества $\boldsymbol{RIS}$ для конкретного объекта оценивания экспертами определяется требуемое множество РИС (и соответственно их идентификаторов) $\boldsymbol{RISO}$ $(\boldsymbol{RISO} \subset \boldsymbol{RIS})$, т.е. $\boldsymbol{RISO} = \{\bigcup_{rs=1}^{ro} RISO_{rs}\}$, $(rs = \overline{1,ro})$, где ro – количество оцениваемых РИС на объекте. Далее относительно всех $RISO_{rs}$ определяются множества их уязвимостей $\boldsymbol{V}_{rs}$ (и соответст-

венно их идентификаторов) ($\boldsymbol{V}_{rs} \subset \boldsymbol{V}$), т.е. $\{\bigcup_{rs=1}^{ro} \boldsymbol{V}_{rs}\} = \{\bigcup_{rs=1}^{ro}\{\bigcup_{uz=1}^{n_{rs}} V_{rs,uz}\}\}$, $(rs = \overline{1,ro}, \quad uz = \overline{1,n_{rs}})$, где n_{rs} – возможное количество идентифицированных уязвимостей rs-того оцениваемого РИС ($RISO_{rs}$).

Шаг 3 (Определение множества параметров оценивания риска). Здесь введем множество оценок риска $\boldsymbol{LR}$ для определенного на втором шаге $\boldsymbol{RISO}$, т.е. $\boldsymbol{LR} = \{\bigcup_{rs=1}^{ro} LR_{rs}\} = \{LR_1, ..., LR_{rs}\}$, $(rs = \overline{1,ro})$. Также для ОР по каждой уязвимости, отображенной идентификатором $V_{rs,uz}$ введем множества $\boldsymbol{LRV}_{rs}$ т.е. $\{\bigcup_{rs=1}^{ro} \boldsymbol{LRV}_{rs}\} = \{\bigcup_{rs=1}^{ro}\{\bigcup_{uz=1}^{n_{rs}} LRV_{rs,uz}\}\}$, $(rs = \overline{1,ro}, \ uz = \overline{1,n_{rs}})$, где $LRV_{rs,uz}$ – количественная оценка риска по каждой uz-той уязвимости rs-того РИС на объекте.

Для отображения результата ОР воспользуемся лингвистической переменной (ЛП) «СТЕПЕНЬ РИСКА» ($\boldsymbol{DR}$), представленной в виде кортежа [2] <$\boldsymbol{DR}$, $\underset{\sim}{T}_{DR}$, $\boldsymbol{X}_{DR}$>, где базовые термы-множества определяются m термами $\underset{\sim}{\boldsymbol{T}}_{DR} = \bigcup_{j=1}^{m} \underset{\sim}{T}_{DR_j}$. Для каждого из термов $\underset{\sim}{T}_{DR_1}, ..., \underset{\sim}{T}_{DR_j}, ..., \underset{\sim}{T}_{DR_m}$ соответственно задается свой интервал значений $[dr_1; dr_2[$, …, $[dr_j; dr_{j+1}[$,…, $[dr_m; dr_{m+1}]$.

Далее для обеспечения процесса оценивания берутся за основу показатели CVSS [11] из NVD [5]. Для этого определим необходимые множества параметров $\boldsymbol{EP}_i$, $(i = \overline{1,g})$, используемых для оценивания, т.е. $\boldsymbol{EP} = \{\bigcup_{i=1}^{g} \boldsymbol{EP}_i\}$, $= \{EP_1, EP_2, ..., EP_g\}$, где g – количество множеств таких параметров.

Отметим, например, что *для версии 2 оценок CVSS* (при g=3) [11] могут быть определенны следующие множества значений – $\{\bigcup_{i=1}^{3} \boldsymbol{EP}_i\} = \{\boldsymbol{EP}_1, \boldsymbol{EP}_2, \boldsymbol{EP}_3\} = \{\boldsymbol{B}, \boldsymbol{T}, \boldsymbol{E}\}$, $(i = \overline{1,3})$, где:

$\boldsymbol{B}$ – базовые (Base) метрики, представляемые в виде множества $\boldsymbol{B} = \{\bigcup_{uz=1}^{n_{rs}} B_{uz}\}$, $(uz = \overline{1,n_{rs}})$, члены которого определяются посредством группы множеств параметров $\boldsymbol{AV}_{uz}$, $\boldsymbol{AC}_{uz}$, $\boldsymbol{AU}_{uz}$, $\boldsymbol{C}_{uz}$, $\boldsymbol{I}_{uz}$, $\boldsymbol{A}_{uz}$, $(uz = \overline{1,n_{rs}})$, где: $\boldsymbol{AV}_{uz}$ – вектор доступа, который представляется в виде множества $\boldsymbol{AV}_{uz} = \{\bigcup_{av=1}^{3} AV_{uz,av}\} = \{AV_{uz,1}, AV_{uz,2}, AV_{uz,3}\} = \{L, A, N\}$, $(uz = \overline{1,n_{rs}}, av = \overline{1,3})$ (где: L – «Локальный доступ» = 0,395; A – «Сопряженная сеть» = 0,646; N – «Сеть» = 1); $\boldsymbol{AC}_{uz}$ – сложность доступа, представляемая множеством $\boldsymbol{AC}_{uz} = \{\bigcup_{ac=1}^{3} AC_{uz,ac}\} = \{AC_{uz,1}, AC_{uz,2}, AC_{uz,3}\} = \{H, M, L\}$, $(uz = \overline{1,n_{rs}}, ac = \overline{1,3})$ (где: H – «Высокая» = 0,35; M – «Средняя» = 0,61; L – «Низкая» = 0,71); $\boldsymbol{AU}_{uz}$ – аутентификация, которая представляется множеством $\boldsymbol{AU}_{uz} = \{\bigcup_{u=1}^{3} AU_{uz,u}\} = \{AU_{uz,1}, AU_{uz,2}, AU_{uz,3}\} = \{M, S, N\}$, $(uz = \overline{1,n_{rs}}, u = \overline{1,3})$ (где: M – «Многоразовая» = 0,45; S – «Одноразовая» = 0,56; N – «Отсутствующая» = 0,704); $\boldsymbol{C}_{uz}$ – воздействие на конфиденциальность, определяемое в виде множества $\boldsymbol{C}_{uz} = \{\bigcup_{c=1}^{3} C_{uz,c}\} = \{C_{uz,1}, C_{uz,2}, C_{uz,3}\} = \{N, P, C\}$, $(uz = \overline{1,n_{rs}}, c = \overline{1,3})$, (где: N – «Отсутствующее» = 0; P – «Частичное» = 0,275; C – «Полное» = 0,66); $\boldsymbol{I}_{uz}$ – воздействие на целостность, которое представляется множеством $\boldsymbol{I}_{uz} = \{\bigcup_{in=1}^{3} I_{uz,in}\} = \{I_{uz,1}, I_{uz,2}, I_{uz,3}\} = \{N, P, C\}$, $(uz = \overline{1,n_{rs}}, in = \overline{1,3})$, (где: N – «Отсутствующее» = 0; P – «Частичное» = 0,275; C – «Полное» = 0,66); $\boldsymbol{A}_{uz}$ – воздействие на доступность, которое может представляться множеством $\boldsymbol{A}_{uz} = \{\bigcup_{ai=1}^{3} A_{uz,ai}\} = \{A_{uz,1}, A_{uz,2}, A_{uz,3}\} = \{N, P, C\}$, $(uz = \overline{1,n_{rs}}, ai = \overline{1,3})$, (где: N – «Отсутст-

вующее» = 0; *P* – «Частичное» = 0,275; *C* – «Полное» = 0,66);

$\boldsymbol{T}$ – временные (Temporal) метрики, представленные в виде множества $\boldsymbol{T} = \{\bigcup_{uz=1}^{n_{rs}} T_{uz}\}$, $(uz = \overline{1, n_{rs}})$, члены которого определяются посредством группы множеств параметров: $\boldsymbol{EX}_{uz}$, $\boldsymbol{RL}_{uz}$, $\boldsymbol{RC}_{uz}$, $(uz = \overline{1, n_{rs}})$, где $\boldsymbol{EX}_{uz}$ – возможность использования, которая может представляться как множество $\boldsymbol{EX}_{uz} = \{\bigcup_{ex=1}^{5} EX_{uz,ex}\} = \{EX_{uz,1}, ..., EX_{uz,5}\} = \{U, POC, F, H, X\}$, $(uz = \overline{1, n_{rs}}, \ ex = \overline{1,5})$, (где: *U* – «Теоретическая (нет доказательств)» = 0,85; *POC* – «Экспериментальная» = 0,9; *F* – «Функциональная» = 0,95; *H* – «Высокая» = 1; *X* – «Неопределённая» = 1); $\boldsymbol{RL}_{uz}$ – уровень исправления (показатель степени готовности решения), определяемый в виде множества $\boldsymbol{RL}_{uz} = \{\bigcup_{rl=1}^{5} RL_{uz,rl}\} = \{RL_{uz,1}, ..., RL_{uz,5}\} = \{OF, TF, W, U, X\}$, $(uz = \overline{1, n_{rs}}, \ rl = \overline{1,5})$, (где: *OF* – «Официальный патч» = 0,87; *TF* – «Временное решение» = 0,9; *W* – «Решение на основе советов и рекомендаций» = 0,95; *U* – «Отсутствующий» = 1; *X* – «Неопределенный» = 1); $\boldsymbol{RC}_{uz}$ – достоверность отчета (показатель степени достоверности информации), которая представляется множеством $\boldsymbol{RC}_{uz} = \{\bigcup_{rc=1}^{4} RC_{uz,rc}\} = \{RC_{uz,1}, ..., RC_{uz,4}\} = \{UC, UR, C, X\}$, $(uz = \overline{1, n_{rs}}, \ rc = \overline{1,4})$, (где: *UC* – «Носит предположительный характер» = 0,9; *UR* – «Не работает» = 0,95; *C* – «Подтверждена» = 1; *X* – «Не определена» = 1);

$\boldsymbol{E}$ – метрики среды окружения (Environmental), представляемые в виде множества $\boldsymbol{E} = \{\bigcup_{uz=1}^{n_{rs}} E_{uz}\}$, $(uz = \overline{1, n_{rs}})$, члены которого определяются посредством группы множеств параметров: $\boldsymbol{CDP}_{uz}$, $\boldsymbol{TD}_{uz}$, $\boldsymbol{CR}_{uz}$, $\boldsymbol{IR}_{uz}$, $\boldsymbol{AR}_{uz}$, $(uz = \overline{1, n_{rs}})$, где $\boldsymbol{CDP}_{uz}$ – вероятность косвенного ущерба, имеющая вид множества $\boldsymbol{CDP}_{uz} = \{\bigcup_{cdp=1}^{6} CDP_{uz,cdp}\} = \{CDP_{uz,1}, ..., CDP_{uz,6}\} = \{N, L, LM, MH, H, X\}$, $(uz = \overline{1, n_{rs}}, \ cdp = \overline{1,6})$, (где: *N* – «Отсутствует» = 0; L – «Низкий» = 0,1; *LM* – «Низкий – средний» = 0,3; *MH* – «Средний – Высокий» = 0,4; *H* – «Высокий» = 0,5; *X* – «Не определен» = 0); $\boldsymbol{TD}_{uz}$ – целераспределение, которое представляться множеством $\boldsymbol{TD}_{uz} = \{\bigcup_{td=1}^{5} TD_{uz,td}\} = \{TD_{uz,1}, ..., TD_{uz,5}\} = \{N, L, M, H, X\}$, $(uz = \overline{1, n_{rs}}, \ td = \overline{1,5})$, (где: *N* – «Отсутствует» = 0; *L* – «Низкое» = 0,25; *M* – «Среднее» = 0,75; *H* – «Высокое» = 1; *X* – «Неопределенное» = 1); $\boldsymbol{CR}_{uz}$ – требования к конфиденциальности, определяемые в виде множества $\boldsymbol{CR}_{uz} = \{\bigcup_{cr=1}^{4} CR_{uz,cr}\} = \{CR_{uz,1}, ..., CR_{uz,4}\} = \{L, M, H, X\}$, $(uz = \overline{1, n_{rs}}, \ sr = \overline{1,4})$, (где: *L* – «Низкие» = 0,5; *M* – «Средние» = 1; *H* – «Высокие» = 1,51; *X* – «Неопределенные» = 1); $\boldsymbol{IR}_{uz}$ – требования к целостности, представляемые множеством $\boldsymbol{IR}_{uz} = \{\bigcup_{ir=1}^{4} IR_{uz,ir}\} = \{IR_{uz,1}, ..., IR_{uz,4}\} = \{L, M, H, X\}$, $(uz = \overline{1, n_{rs}}, \ ir = \overline{1,4})$, (где: *L* – «Низкие» = 0,5; *M* – «Средние» = 1; *H* – «Высокие» = 1,51; *X* – «Неопределённые» = 1); $\boldsymbol{AR}_{uz}$ – требования к доступности, которые представляются в виде множества $\boldsymbol{AR}_{uz} = \{\bigcup_{ar=1}^{4} AR_{uz,ar}\} = \{AR_{uz,1}, ..., AR_{uz,4}\} = \{L, M, H, X\}$, $(uz = \overline{1, n_{rs}}, \ ar = \overline{1,4})$, (где: *L* – «Низкие» = 0,5; *M* – «Средние» = 1; *H* – «Высокие» = 1,51; *X* – «Неопределённые» = 1).

Далее введем ЛП «УРОВЕНЬ ОЦЕНОЧНОГО ПАРАМЕТРА $\boldsymbol{EP}_i$» ($\boldsymbol{K}_{EP_i}$), которая определяется кортежем [2, 3] $< \boldsymbol{K}_{EP_i}, \ \underset{\sim}{T}_{K_{EP_i}}, \ \boldsymbol{X}_{EP_i} >$, где базовые терм-множества задаются m термами $\underset{\sim}{\boldsymbol{T}}_{K_{EP_i}} = \bigcup_{j=1}^{m} \underset{\sim}{T}_{K_{EP_i j}}$. Для $\underset{\sim}{T}_{K_{EP_i 1}}$, $\underset{\sim}{T}_{K_{EP_i 2}}$,…, $\underset{\sim}{T}_{K_{EP_i j-1}}$, $\underset{\sim}{T}_{K_{EP_i j}}$, …, $\underset{\sim}{T}_{K_{EP_i m}}$ соответственно определяют свои интервалы значений по каждому $\boldsymbol{EP}_i$, $(i = \overline{1, g})$ – $[k_{EP_i 1}; \ k_{EP_i 2}[$, $[k_{EP_i 2}; \ k_{EP_i 3}[$, …, $[k_{EP_i j-1}; \ k_{EP_i j}[$, $[k_{EP_i j}; \ k_{EP_i j+1}[$, …, $[k_{EP_i m}; \ k_{EP_i m+1}]$. Для удобства отображения

оценочных параметров через интервалы допустимых значений воспользуемся табл. 1.

Далее с помощью соответствующего метода [14], который реализуется посредством четырех этапов осуществим преобразование интервалов в нечеткие числа (НЧ) – $\underset{\sim}{T}_{K_{EP_i j}} = (ai_j; bi_{1j}; bi_{2j}; ci_j)$.

Оценка значимости $\boldsymbol{EP}_i$ выполняется с помощью параметров из множества $\boldsymbol{LS} \in \{LS_i\}$, $(i = \overline{1,g})$, а оценка текущего значения оценочного параметра – с помощью множества $\boldsymbol{ep} \in \{ep_{uz,i}\}$, $(uz = \overline{1,n_{rs}}, i = \overline{1,g})$.

Таблица 1

Определение значений НЧ оценочных параметров

$\boldsymbol{EP}_i$	НЧ $\underset{\sim}{T}_{K_{EP_i j}} = (a_j, b_{1j}, b_{2j}, c_j)_{LR}$ для $\underset{\sim}{T}_{K_{EP_i 1}} - \underset{\sim}{T}_{K_{EP_i m}}$, $(j = \overline{1,m})$				
	$\underset{\sim}{T}_{K_{EP_i 1}}$	…	$\underset{\sim}{T}_{K_{EP_i j}}$	…	$\underset{\sim}{T}_{K_{EP_i m}}$
$\boldsymbol{EP}_1$	$(a1_1; b1_{11}; b1_{21}; c1_1)$	…	$(a1_j; b1_{1j}; b1_{2j}; c1_j)$	…	$(a1_m; b1_{1m}; b1_{2m}; c1_m)$
…	…	…	…	…	…
$\boldsymbol{EP}_i$	$(ai_1; bi_{11}; bi_{21}; ci_1)$	…	$(ai_j; bi_{1j}; bi_{2j}; ci_j)$	…	$(ai_m; bi_{1m}; bi_{2m}; ci_m)$
…	…	…	…	…	…
$\boldsymbol{EP}_g$	$(ag_1; bg_{11}; bg_{21}; cg_1)$	…	$(ag_j; bg_{1j}; bg_{2j}; cg_j)$	…	$(ag_m; bg_{1m}; bg_{2m}; cg_m)$

Шаг 4 (Определение количества терм-множеств). Здесь реализуется определение количества терм-множеств, которые будут использоваться в процессе ОР. При необходимости можно изменить начальное количество терм-множеств. С этой целью для эквивалентного преобразования m-мерных термов НЧ ЛП $\boldsymbol{DR}^{(m)}$ в $\boldsymbol{DR}^{(m-n)}$ [12] или $\boldsymbol{DR}^{(m+n)}$ [13] и $\boldsymbol{K}_{EP_i}^{(m)}$ в $\boldsymbol{K}_{EP_i}^{(m-n)}$ или $\boldsymbol{K}_{EP_i}^{(m+n)}$ предлагается воспользоваться методами реализации функции трансформирования эталонов ЛП [12, 13].

Шаг 5 (Оценка уровня значимости оценочных параметров). На этом шаге каждому компоненту $\boldsymbol{EP} = \{\bigcup_{i=1}^{g} \boldsymbol{EP}_i\}$, $(i = \overline{1,g})$ ставиться в соответствие уровень его значимости – LS_i. Отметим, что если для всех таких уровней справедливо отношение порядка

$$LS_i \geq LS_{i+1}, \quad (1)$$

то значимость i-го параметра определяется по правилу Фишберна [3]:

$$LS_i = \frac{2(g-i+1)}{(g-1)g}. \quad (2)$$

Согласно этому правилу у эксперта отсутствует информация (кроме условия (1)) о значимости параметров. В этом случае выражение (2) отображает максимум энтропии существующей информационной неопределенности об объекте исследования. Если все параметры обладают равной значимостью (равнопредпочтительны т.е. $LS_i = LS_{i+1}$) или системы предпочтений нет, то:

$$LS_i = 1/g. \quad (3)$$

Шаг 6 (Определение эталонных значений степени риска). На этом шаге определяются эталонные значения для ЛП $\boldsymbol{DR}$, т.е. задается количество термов в базовом терм-множестве $\underset{\sim}{\boldsymbol{T}}_{DR}$, где ставиться им в соответствие заданный интервал значений, лежащий в диапазоне от dr_{min} до dr_{max}.

Шаг 7 (Определение эталонных значений оценочных параметров). Здесь экспертами производится определение эталонных значений для ЛП $\boldsymbol{K}_{EP_i}$, т.е. задается количество термов в терм-множестве $\underset{\sim}{\boldsymbol{T}}_{K_{EP_i}}$.

Для преобразования интервалов в НЧ воспользуемся предложенным в [14] методом. Для удобства отображения оценочных параметров через НЧ используем табл. 1.

Например, если $\boldsymbol{EP}_i$ представляются трапециевидными НЧ с функциями принадлежности (ФП) $\mu_1(ep_{uz,i})$, …, $\mu_j(ep_{uz,i})$, …, $\mu_m(ep_{uz,i})$, то они соответственно вычисляются по выражению (4) [4]:

$$\mu_j(ep_{uz,i}) = \begin{cases} L\left(\dfrac{a_{i_j} - ep_{uz,i}}{a_{i_j} - b_{i_{1j}}}\right), & ep_{uz,i} \in [a_{i_j}, b_{i_{1j}}]; \\ 1, & ep_{uz,ii} \in [b_{i_{1j}}, b_{i_{2j}}]; \\ R\left(\dfrac{ep_{uz,i} - c_{i_j}}{b_{i_{2j}} - c_{i_j}}\right), & ep_{uz,i} \in [b_{i_{2j}}, c_{i_j}], \end{cases} \quad (4)$$

где $a_{ij} < b_{i1j} \le b_{i2j} < c_{ij}$, при $j = \overline{1,m}$, а $L(ep_{uz,i})$, $R(ep_{uz,i})$ – функции (невозрастающие на множестве не положительных чисел), которые удовлетворяют свойствам: $L(-ep_{uz,i}) = L(ep_{uz,i})$, $R(-ep_{uz,i}) = R(ep_{uz,i})$, $L(0) = R(0) = 1$. С помощью выражения (4) для интервалов $\boldsymbol{EP}_i$ можно сформировать значения $\mu_j(ep_{uz,i})$.

Шаг 8 (Оценка текущих значений параметров). На этом шаге по каждому оценочному параметру $\{\bigcup_{i=1}^{3} \boldsymbol{EP}_i\} = \{\boldsymbol{EP}_1, \boldsymbol{EP}_2, \boldsymbol{EP}_3\} = \{\boldsymbol{B}, \boldsymbol{T}, \boldsymbol{E}\}$, $(i = \overline{1,3})$ эксперты соответствующей предметной области определяют $ep_{uz,i}$ для всех $V_{rs,uz}$, $(rs = \overline{1,ro}, uz = \overline{1,n_{rs}})$, т.е. $\{ep_{uz,i}\} = \{ep_{uz,\boldsymbol{B}}, ep_{uz,\boldsymbol{T}}, ep_{uz,\boldsymbol{E}}\}$. Значения каждого из параметров, можно взять из известных баз данных [5] или определить по соответствующим формулам [11]:

$$B_{uz} = round(0,6IM_{uz} + 0,4EXb_{uz} - 1,5)\, f(IM_{uz}),$$

где: $round(\ )$ – функция округления до одной десятой; $IM_{uz} = 10,41(1-(1-C_{uz,c})(1-I_{uz,in})(1-A_{uz,ai}))$, значения $C_{uz,c}$, $I_{uz,in}$, $A_{uz,ai}$ берутся из шага 3 метода, $EXb_{uz} = 20AV_{uz,av} \cdot AC_{uz,ac} \cdot AU_{uz,u}$, $f(IM_{uz}) = \begin{cases} 0 \text{ при } IM_{uz} = 0, \\ 1,176 \text{ при } IM_{uz} \ne 0; \end{cases}$

$$T_{uz} = round(B_{uz} \cdot EX_{uz,ex} \cdot RL_{uz,rl} \cdot RC_{uz,rc}),$$ где значения $EX_{uz,ex}$, $RL_{uz,rl}$, $RC_{uz,rc}$ берутся из шага 3 метода;

$$E_{uz} = round((AT_{uz} + (10 - AT_{uz})CDP_{uz,cdp})TD_{uz,td}),$$

где: $AT_{uz} = round(AB_{uz} \cdot EX_{uz,ex} \cdot RL_{uz,rl} \cdot RC_{uz,rc})$ при $AB_{uz} = round((0,6AIM_{uz}) + (0,4EXb_{uz}) - 1,5)\ f(AIM_{uz})$ и $AIM_{uz} = \min(10; 10,41\,(1 - (1 - C_{uz,c} \cdot CR_{uz,cr})\,(1 - I_{uz,in} \cdot IR_{uz,ir})\,(1 - A_{uz,an} \cdot AR_{uz,ar})))$, а $f(AIM_{uz}) = \begin{cases} 0 \text{ при } AIM_{uz} = 0, \\ 1,176 \text{ при } AIM_{uz} \ne 0. \end{cases}$ Здесь E_{uz} является корректирующим оценочным параметром, который переопределяет B_{uz} и T_{uz}.

Шаг 9 (Классификация текущих значений). На этом шаге с помощью эталонных значений, осуществляется определение принадлежности $ep_{uz,i}$ заданному НЧ, по которому с помощью выражения (5) формируются значения $\lambda_{uz,ij}$:

$$\lambda_{uz,i1} = \begin{cases} 1 \text{ при } ep_{uz,i} \in [b_{i_{11}}, b_{i_{12}}[; \\ 0 \text{ при } ep_{uz,i} \notin [b_{i_{11}}, c_{i_1}[; \\ \mu_1(ep_{uz,i}) \text{ при } ep_{uz,i} \in [b_{i_{12}}, c_{i_1}[, \end{cases}$$

$$\dots$$

$$\lambda_{uz,ij} = \begin{cases} \mu_j(ep_{uz,i}) \text{ при } ep_{uz,i} \in [a_{i_j}, b_{i_{1j}}[; \\ 1 \text{ при } ep_{uz,i} \in [b_{i_{1j}}, b_{i_{2j}}[; \\ \mu_j(ep_{uz,i}) \text{ при } ep_{uz,i} \in [b_{i_{2j}}, c_{i_j}[; \\ 0 \text{ при } ep_{uz,i} \notin [a_{i_j}, c_{i_j}[, \end{cases} \quad (5)$$

$$\dots$$

$$\lambda_{uz,im} = \begin{cases} \mu_m(ep_{uz,i}) \text{ при } ep_{uz,i} \in [a_{i_m}, b_{i_{1m}}[; \\ 1 \text{ при } ep_{uz,i} \in [b_{i_{1m}}, b_{i_{2m}}[; \\ 0 \text{ при } ep_{uz,i} \notin [a_{i_m}, b_{i_{2m}}[, \end{cases}$$

а $\mu_j(ep_{uz,i})$, $(uz = \overline{1,n_{rs}}, j = \overline{2,m-1})$ с помощью формулы (4). Для наглядности результаты выполненных вычислений занесены в табл. 2, где $\lambda_{uz,ij}$ – уровень принадлежности носителя $ep_{uz,i}$ нечеткому подмножеству $\underset{\sim}{T}_{K_{EP_ij}}$. Аналогичные преобразования осуществляются для всех $V_{rs,uz}$.

Таблица 2

Классификация текущих значений оценочных параметров

$\boldsymbol{EP}_i$	$\lambda_{uz,ij}$ для $\underset{\sim}{T}_{K_{EP_ij}}$ $(uz = \overline{1,n_{rs}},\ i = \overline{1,g},\ j = \overline{1,m})$				
	$\underset{\sim}{T}_{K_{EP_i1}}$	…	$\underset{\sim}{T}_{K_{EP_ij}}$	…	$\underset{\sim}{T}_{K_{EP_im}}$
$\boldsymbol{EP}_1$	$\lambda_{uz,11}$	…	$\lambda_{uz,1j}$	…	$\lambda_{uz,1m}$
…	…	…	…	…	…
$\boldsymbol{EP}_i$	$\lambda_{uz,i1}$	…	$\lambda_{uz,ij}$	…	$\lambda_{uz,im}$
…	…	…	…	…	…
$\boldsymbol{EP}_g$	$\lambda_{uz,g1}$	…	$\lambda_{uz,gj}$	…	$\lambda_{uz,gm}$

Шаг 10 (Оценка степени риска). На этом шаге производится вычисление показателей степени риска для каждой уязвимости, отображенной идентификатором $V_{rs,uz}$ по формуле:

$$LRV_{rs,uz} = \sum_{j=1}^{m}\left(K_{lr_j} \sum_{i=1}^{g} (ks \cdot LS_i)\lambda_{uz,ij} \right), \quad (6)$$

где $K_{lr_j} = 90 - 20(m - j)$, $ks = \dfrac{1}{(LS_1 + ... + LS_i)}$ – коэффициент нормирования, $\lambda_{uz,ij}$ $(uz = \overline{1, n_{rs}}$, $i = \overline{1, g}$, $j = \overline{1, m},)$ определяется по выражению (5) для каждой $V_{rs,uz}$, $(rs = \overline{1, ro}, uz = \overline{1, n_{rs}})$, а LS_i, $(i = \overline{1, g})$ в зависимости от значимости параметра вычисляется по формуле (2) или (3).

Шаг 11 (Формирование структурированного параметра риска). На основании вычисленного значения $LRV_{rs,uz}$ и построенных эталонов формируем структурированный параметр степени риска *SP* по выражению (7):

$$SP_{uz} = \begin{cases} (LRV_{rs,uz}; \underset{\sim}{T}_{DR_j}) \; при \; \mu_j(LRV_{rs,uz}) = 1; \\ (LRV_{rs,uz}; \underset{\sim}{T}_{DR_j}(\mu_j(LRV_{rs,uz})); \underset{\sim}{T}_{DR_{j+1}}(\mu_{j+1}(LRV_{rs,uz}))) \; при \; \mu_j(LRV_{rs,uz}) \neq 1 \wedge \mu_{j+1}(LRV_{rs,uz}) \neq 1, \end{cases} \quad (7)$$

где $(LRV_{rs,uz}; \underset{\sim}{T}_{DR_j})$ словесно интерпретируется как – «Степень риска $\underset{\sim}{T}_{DR_j}$ с числовым эквивалентом $LRV_{rs,uz}$», а $(LRV_{rs,uz}; \underset{\sim}{T}_{DR_j}(\mu_j(LRV_{rs,uz})); \underset{\sim}{T}_{DR_{j+1}}(\mu_{j+1}(LRV_{rs,uz})))$, как – «Степень риска с числовым эквивалентом $LRV_{rs,uz}$ граничит между $\underset{\sim}{T}_{DR_j}$ и $\underset{\sim}{T}_{DR_{j+1}}$ по границе $\underset{\sim}{T}_{DR_j} - \mu_j(LRV_{rs,uz})$ и $\underset{\sim}{T}_{DR_{j+1}} - \mu_{j+1}(LRV_{rs,uz})$».

С помощью *SP* можно получить как числовое значение степени риска, так и его лингвистическую интерпретацию.

Также по выражению (8) можно вычислить среднее значение LR_{rs} по оцениваемому ресурсу:

$$LR_{rs} = (\sum_{uz=1}^{n_{rs}} LRV_{rs,uz}) / n_{rs}. \quad (8)$$

Рассмотрим работу предложенного метода на конкретном примере.

Пример 1

Шаг 1. На первом шаге определяется полные множества всех РИС и уязвимостей, при $r = r_{BD}$ и $n = n_{NVD}$, т.е. $\boldsymbol{RIS} = \{\bigcup_{rs=1}^{r} RIS_{rs}\}$, $(rs = \overline{1, r})$ и $\boldsymbol{V} = \{\bigcup_{uz=1}^{n} V_{uz}\}$, $(uz = \overline{1, n})$, где r_{BD} и n_{NVD} – количество РИС, например, в государственных или частных БД и количество уязвимостей в NVD [5] соответственно.

Шаг 2. На этом шаге посредством множества $\boldsymbol{RIS}$ эксперты определяют содержимое $\boldsymbol{RISO}$ для конкретного объекта оценивания при ro = 5, т.е. – $\boldsymbol{RISO} = \{\bigcup_{rs=1}^{5} RISO_{rs}\} = \{RISO_1, ..., RISO_5\}$, $(rs = \overline{1, 5})$, где, например, $RISO_1$ = «Файловый сервер», $RISO_2$ = «Банк данных», $RISO_3$ = «Архив данных», $RISO_4$ = «Маршрутизатор», $RISO_5$ = «Web-сервер». Далее относительно $\boldsymbol{RISO}$ например, при $n_1 = 5$, $n_2 = 3$, $n_3 = 7$, $n_5 = 4$, $n_6 = 2$, эксперты с помощью NVD [5] идентифицировали следующие уязвимости – $\{\bigcup_{rs=1}^{5} \boldsymbol{V}_{rs}\} = \{\bigcup_{rs=1}^{5} \{\bigcup_{uz=1}^{n_{rs}} V_{rs,uz}\} = \{\{V_{1,1}, V_{1,2}, V_{1,3}, V_{1,4}, V_{1,5}\}, \{V_{2,1}, V_{2,2}, V_{2,3}\}, \{V_{3,1}, V_{3,2}, V_{3,3}, V_{3,4}, V_{3,5}, V_{3,6}, V_{3,7}\}, \{V_{4,1}, V_{4,2}, V_{4,3}, V_{4,4}\}, \{V_{5,1}, V_{5,2}\}\}$.

Далее, например, при $rs = 1$ реализуем ОР для $RISO_1$, по которому экспертами идентифицировано следующие уязвимости:

$V_{1,1}$ = «CVE-2013-1324» – на основе стека переполнения буфера в Microsoft Office 2003 SP3, 2007 SP3, 2010 SP1 и SP2, 2013 и 2013 RT уязвимость позволяет удаленному злоумышленнику выполнить произвольный код с помощью файла созданного WordPerfect документ (.wpd), также известный как «Word Stack Buffer Overwrite Vulnerability». Оценка CVSS Severity (v2) = 9,3 (HIGH);

$V_{1,2}$ = «CVE-2015-2516» – уязвимость в журналах Windows в Microsoft Windows Vista SP2, Windows Server 2008 SP2 и R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server

2012 Gold и R2, Windows RT Gold и 8.1, и Windows 10 позволяет удаленному злоумышленнику вызвать отказ в сервисе (потеря данных) с помощью созданного JNT-файла, также известный как «Windows Journal DoS уязвимости». Оценка CVSS Severity (v2) = 4,3 (MEDIUM);

$V_{1,3}$ = «CVE-2016-2386» – уязвимость SQL инъекций сервера UDDI в SAP NetWeaver J2EE Engine 7.40 позволяет удаленному злоумышленнику выполнить произвольные команды SQL с помощью неопределенных векторов (SAP Security Note 2101079). Оценка CVSS Severity (v2) = 7,5 (HIGH);

$V_{1,4}$ = «CVE-2015-1830» – каталог обхода уязвимости в загрузке файла сервера/загрузки функциональности для Blob сообщений в Apache ActiveMQ 5.x до 5.11.2 для Windows, позволяет удаленным злоумышленникам создавать JSP-файлы в произвольных каталогах посредством неопределённого вектора. Оценка CVSS Severity (v2) = 5,0 (MEDIUM);

$V_{1,5}$ = «CVE-2016-0497» – неуказанная уязвимость в компоненте Oracle Agile Engineering – управление данными в Oracle Supply Chain Products Suite, 6.1.2.2, 6.1.3.0 и 6.2.0.0 позволяет удаленному злоумышленнику повлиять на целостность с помощью неизвестных векторов, связанных с веб-клиентом. Оценка CVSS Severity (v2) = 4,3 (MEDIUM).

Шаг 3. Здесь, например, определим множество параметров ОР при ro = 1 (т.е. для LR_1) и при $n_1 = 5$ (т.е. для $\{\bigcup_{uz=1}^{5} LRV_{1,uz}\} = \{LRV_{1,1}, LRV_{1,2}, LRV_{1,3}, LRV_{1,4}, LRV_{1,5}\}$). Отображение результатов ОР для LR_1 и $LRV_{1,uz}$, $(uz = \overline{1,5})$ при $m = 5$ выполним посредством термов $\bigcup_{j=1}^{5} \underset{\sim}{T}_{DR_j} = \{$«Незначительный риск нарушения ИБ» (НР), «Степень риска нарушения ИБ низкая» (РН), «Степень риска нарушения ИБ средняя» (РС), «Степень риска нарушения ИБ высокая» (РВ), «Предельный риск нарушения ИБ» (ПР)$\}$, которые могут быть отображены на универсальное множество $\boldsymbol{X}_{DR} \in \{0, max_{DR}\}$. В последствии для каждого $\underset{\sim}{T}_{DR_1}$, $\underset{\sim}{T}_{DR_2}$, $\underset{\sim}{T}_{DR_3}$, $\underset{\sim}{T}_{DR_4}$, $\underset{\sim}{T}_{DR_5}$ определяются интервалы с использованием модифицированной шкалы Харрингтона [2, 3] т.е. $[dr_1; dr_2[$, $[dr_2; dr_3[$, $[dr_3; dr_4[$, $[dr_4; dr_5[$ и $[dr_5; dr_6]$ будут соответственно принимать значения [0; 20[, [20; 40[, [40; 60[, [60; 80[и [80; 100].

Далее воспользуемся множеством оценочных параметров $\boldsymbol{EP} = \{\boldsymbol{B}, \boldsymbol{T}, \boldsymbol{E}\}$. Зададим для ЛП $\boldsymbol{K}_{EP_i}$ при $m = 5$ следующие термы – $\bigcup_{j=1}^{5} \underset{\sim}{T}_{K_{EP_i j}} =$ {«Отсутствует» (N), «Низкий» (L), «Средний» (M), «Высокий» (H), «Критический» (C)}, которые в лингвистической форме характеризуют уровень оценочного параметра и могут быть отображены на универсальное множество $\boldsymbol{X}_{EP_i} \in \{0, \max_{K_{EP_i}}\}$. Далее для каждого терма $\underset{\sim}{T}_{K_{EP_i 1}}$, $\underset{\sim}{T}_{K_{EP_i 2}}$, $\underset{\sim}{T}_{K_{EP_i 3}}$, $\underset{\sim}{T}_{K_{EP_i 4}}$, $\underset{\sim}{T}_{K_{EP_i 5}}$ оценочных параметров [2, 3] определим интервалы $[k_{EP_i 1}; k_{EP_i 2}[$, $[k_{EP_i 2}; k_{EP_i 3}[$, $[k_{EP_i 3}; k_{EP_i 4}[$, $[k_{EP_i 4}; k_{EP_i 5}[$, $[k_{EP_i 5}; k_{EP_i 6}]$, которым будут соответствовать значения [2, 11] – [0; 0,1[, [0,1; 4[, [4; 7[, [7; 9[, [9; 10].

Шаг 4. Определим количество необходимых терм-множеств для ОР ЛП $\boldsymbol{DR}^{(m)}$ и $\boldsymbol{K}_{EP_i}^{(m)}$, при m = 5 (см. табл. 3 и 4 соответственно). В случае необходимости можем с помощью методов [12, 13] реализовать инкрементирование или декрементирование соответствующих терм-множеств.

Таблица 3

Определение эталонных значений НЧ степени риска (пример)

ЛП	НЧ $\underset{\sim}{X}_{DR_j} = (a_j, b_{1j}, b_{2j}, c_j)_{LR}$ для $\underset{\sim}{T}_{DR_1} \div \underset{\sim}{T}_{DR_5}$, $(j = \overline{1,5})$				
	$\underset{\sim}{T}_{DR_1}$	$\underset{\sim}{T}_{DR_2}$	$\underset{\sim}{T}_{DR_3}$	$\underset{\sim}{T}_{DR_4}$	$\underset{\sim}{T}_{DR_5}$
	$(a_1; b_{11}; b_{21}; c_1)$	$(a_2; b_{12}; b_{22}; c_2)$	$(a_3; b_{13}; b_{23}; c_3)$	$(a_4; b_{14}; b_{24}; c_4)$	$(a_5; b_{15}; b_{25}; c_5)$
DR	(0;0; 11,11; 22,22)	(11,11; 22,22; 33,33; 44,44)	(33,33; 44,44; 55,55; 66,66)	(55,55; 66,66; 77,77; 88,88)	(77,77; 88,88; 100; 100)

Шаг 5. На этом шаге произведем оценку значимости оценочных параметров. Так как для всех оценочных параметров, по мнению экспертов, справедливо отношение порядка $LS_1 \geq LS_2 \geq LS_3$ (1), тогда оценку LS осуществим по формуле (2) т.е.

$LS_1 = 2(g-i+1)/(g-1)g = 2(3-1+1)/(3-1)3 = 1;$

$LS_2 = 2(3-2+1)/(3-1)3 = 0{,}67;$

$LS_3 = 2(3-3+1)/(3-1)3 = 0{,}33,\ (i=\overline{1,3})$.

Шаг 6. Здесь определим эталонные значения для ЛП ***DR***. С помощью выражений (1)–(5) из [14] представим для $\underset{\sim}{T}_{DR_j} = (a_j;\ b_{1j};\ b_{2j};\ c_j)$ числовые значения, которые заносятся в таблицу 3. Их графическая интерпретация отображена на рис. 1.

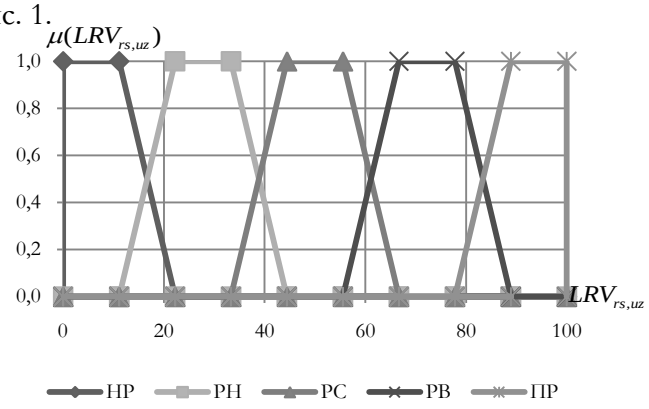

Рис. 1. Пример эталонных НЧ для ЛП ***DR***

Шаг 7. Далее определим эталонные значения для ЛП $\boldsymbol{K}_{EP_i}$. Преобразование интервалов в НЧ $\underset{\sim}{T}_{K_{EP_i j}} = (ai_j;\ bi_{1j};\ bi_{2j};\ ci_j)$ реализуем с помощью четырех этапов предложенного в [14] метода.

Этап 1. Посредством выражения (1) из [14] получим значения корректирующих параметров:
$h_{i_1} = (k_{EP_i 2} - k_{EP_i 1})/4$ = (0,1 – 0) / 4 = 0,025;
$h_{i_2} = (k_{EP_i 3} - k_{EP_i 2})/4$ = (4 – 0,1) / 4 = 0,975;
$h_{i_3} = (k_{EP_i 4} - k_{EP_i 3})/4$ = (7 – 4) / 4 = 0,75;
$h_{i_4} = (k_{EP_i 5} - k_{EP_i 4})/4$ = (9 – 7) / 4 = 0,5;
$h_{i_5} = (k_{EP_i 6} - k_{EP_i 5})/4$ = (10 – 9) / 4 = 0,25.

Этап 2. Вычислим значения абсцисс НЧ по формуле (2) в [14]: $a'_{i_1} = k_{EP_i 1} - h_{i_1}$ = 0 – 0,025 = –0,025; $a'_{i_2} = k_{EP_i 2} - h_{i_2}$ = –0,875; $a'_{i_3} = k_{EP_i 3} - h_{i_3}$ = 3,25; a'_{i_4} = 6,5; a'_{i_5} = 8,75; $c'_{i_1} = k_{EP_i 2} + h_{i_1}$ = 0,125; $c'_{i_2} = k_{EP_i 3} + h_{i_2}$ = 4,975; c'_{i_3} = 7,75; c'_{i_4} = 9,5; c'_{i_5} = 10,25, $b'_{i_{11}} = k_{EP_i 1} + h_{i_1}$ = 0,025; $b'_{i_{21}} = k_{EP_i 2} - h_{i_1}$ = 0,075; $b'_{i_{12}}$ = 1,075; $b'_{i_{22}}$ = 3,025; $b'_{i_{13}}$ = 4,75; $b'_{i_{23}}$ = 6,25; $b'_{i_{14}}$ = 7,5; $b'_{i_{24}}$ = 8,5; $b'_{i_{15}}$ = 9,25; $b'_{i_{25}}$ = 9,75.

Этап 3. Здесь по выражению (3) (см. [14]) определим базовое значение сдвига $sf_i = b'_{i_{11}} - k_{EP_i 1}$ = 0,03 – 0 = 0,03 и далее реализуем поправку термов по формуле (4) (см. [14]): $a''_{i_1} = a'_{i_1} - sf_i$ = –0,025 – 0,025 = –0,05; a''_{i_2} = –0,9; a''_{i_3} = 3,225; a''_{i_4} = 6,475; a''_{i_5} = 8,725; $c''_{i_1} = c'_{i_1} - sf_i$ = 0,1; c''_{i_2} = 4,95; c''_{i_3} = 7,725; c''_{i_4} = 9,475; c''_{i_5} = 10,225; $b''_{i_{11}} = b'_{i_{11}} - sf_i$ = 0; $b''_{i_{21}}$ = 0,05; $b''_{i_{12}}$ = 1,05; $b''_{i_{22}}$ = 3; $b''_{i_{13}}$ = 4,725; $b''_{i_{23}}$ = 6,225; $b''_{i_{14}}$ = 7,475; $b''_{i_{24}}$ = 8,475; $b''_{i_{15}}$ = 9,225; $b''_{i_{25}}$ = 9,725.

Этап 4. На этом этапе реализуем нормирование результатов по выражению (5) из [14]: $a_{i_1} = (a''_{i_1} \cdot k_{EP_i 6})/b''_{i_{25}}$ = –0,051; a_{i_2} = –0,925; a_{i_3} = 3,316; a_{i_4} = 6,658; a_{i_5} = 8,972; $c_{i_1} = (c''_{i_1} \cdot k_{EP_i 6})/b''_{i_{25}}$ = 0,103; c_{i_2} = 5,09; c_{i_3} = 7,943; c_{i_4} = 9,743; c_{i_5} = 10,514; $b_{i_{11}} = (b''_{i_{11}} \cdot k_{EP_i 6})/b''_{i_{25}} = 0$;

$b_{i_{21}} = (b''_{i_{21}} \cdot k_{EP_i 6})/b''_{i_{25}}$ = 0,051 и т.д. Далее по условию (из той же формулы (5)) $a_{i_1} = a_{i_2}$ = 0, а c_{i_5} = 10. Все полученные в результате вычисления значения занесены в таблицу 4, а их графическая интерпретация отображена на рис. 2.

Таблица 4

Определение эталонных значений НЧ оценочных параметров (пример)

$\boldsymbol{EP_i}$	НЧ $\underset{\sim}{T}_{K_{EP_i j}} = (a_j, b_{1j}, b_{2j}, c_j)_{LR}$ для $\underset{\sim}{T}_{K_{EP_i 1}} \div \underset{\sim}{T}_{K_{EP_i 5}}$, $(j=\overline{1,5},\ i=\overline{1,g})$				
	$\underset{\sim}{T}_{K_{EP_i 1}}$ $(ai_1;\ bi_{11};\ bi_{21};\ ci_1)$	$\underset{\sim}{T}_{K_{EP_i 2}}$ $(ai_2;\ bi_{12};\ bi_{22};\ ci_2)$	$\underset{\sim}{T}_{K_{EP_i 3}}$ $(ai_3;\ bi_{13};\ bi_{23};\ ci_3)$	$\underset{\sim}{T}_{K_{EP_i 4}}$ $(ai_4;\ bi_{14};\ bi_{24};\ ci_4)$	$\underset{\sim}{T}_{K_{EP_i 5}}$ $(ai_5;\ bi_{15};\ bi_{25};\ ci_5)$
B, T, E	(0;0;0,051;0,103)	(0;1,08;3, 085;5,09)	(3,316;4,859;6,401;7,943)	(6,658;7,686;8,715;9,743)	(8,972;9,486;10;10)

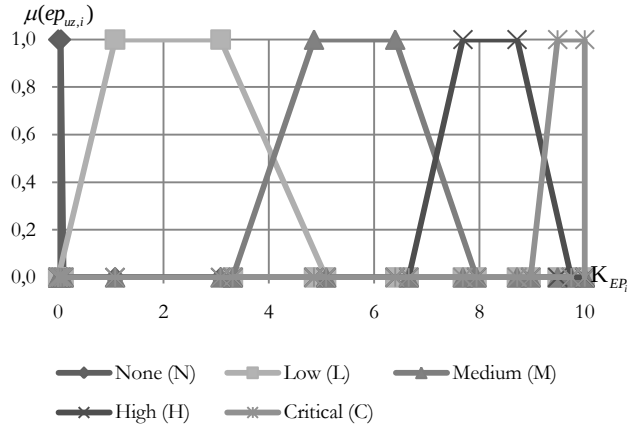

Рис. 2. Пример эталонных НЧ для оценочных параметров B_{uz}, T_{uz}, E_{uz}, $(uz=\overline{1,5})$

Шаг 8. Текущее состояние $RISO_1$ характеризуется значениями оценочных параметров $ep_{uz,i}$ по каждому $V_{rs,uz}$, которые определяются с помощью оценок CVSS представленных на сайте NVD [5]. Поскольку не всегда все значения оценочных параметров по уязвимостям присутствуют в базе NVD, то для получения недостающих воспользуемся формулами из шага 7.

Расчет для $V_{1,1}$ = «CVE-2013-1324»:

– для B_1, исходя из того, что величинам $AV_{1,3}$, $AC_{1,2}$, $AU_{1,3}$, $C_{1,3}$, $I_{1,3}$ и $A_{1,3}$ соответствуют определенные значения «*N*», «*M*», «*N*», «*C*», «*C*» и «*C*», то $AV_{1,3}$ = 1, $AC_{1,2}$ = 0,61, $AU_{1,3}$ = 0,704, $C_{1,3}$ = 0,66, $I_{1,3}$ = 0,66 и $A_{1,3}$ = 0,66. На основе этого вычисляем $EXb_1 = 20 AV_{1,3} \cdot AC_{1,2} \cdot AU_{1,3}$ = 20·1·0,61·0,704 = 8,6, $IM_1 = 10,41\,(1-(1-C_{1,3})\,(1-I_{1,3})(1-A_{1,3}))$ = 10,41(1 – (1 – 0,66)(1 – 0,66)(1 – 0,66)) = 10 и тогда $f(IM_1)$ = 1,176, а $B_1 = round(0,6IM_1 + 0,4EXb_1 - 1,5)\ f(IM_1)$ = *round*(0,6·10 + 0,4·8,6 – 1,5) 1,176 = 9,3;

– для T_1 в базе NVD отсутствуют определенные значения, поэтому, например, на основе суждений экспертов определим значения для $EX_{1,3}$ = «*F*», $RL_{1,1}$ = «*OF*», $RC_{1,3}$ = «*C*» и тогда $EX_{1,3}$ = 0,95, $RL_{1,1}$ = 0,87, $RC_{1,3}$ = 1, $T_1 = round(B_1 \cdot EX_{1,3} \cdot RL_{1,1} \cdot RC_{1,3})$ = *round* (9,3· 0,95·0,87·1)=7,7;

– для E_1, по аналогии с T_1, значения также определяются с помощью экспертов. Если $CDP_{1,4}$ = «MH», $TD_{1,2}$ = «L», $CR_{1,2}$ = «M», $IR_{1,2}$ = «M» и $AR_{1,2}$ = «M» то $CDP_{1,4}$ = 0,4, $TD_{1,2}$ = 0,25, $CR_{1,2}$ = 1, $IR_{1,2}$ = 1 и $AR_{1,2}$ = 1. На основе этого находим $AIM_1 = \min(10; 10,41\,(1-(1-C_{1,3}\cdot CR_{1,2})\,(1-I_{1,3}\cdot IR_{1,2})\,(1-A_{1,3}\cdot AR_{1,2})))$ = min(10; 10,41 (1 – (1 – 0,66·1) (1 – 0,66·1) (1 – 0,66·1)) = 10, AB_1 = $round((0,6AIM_1) + (0,4EXb_1) - 1,5)\,f(AIM_1)$ = *round*((0,6·10)+ (0,4·10) – 1,5) 1,176 = 10, AT_1 = $round(AB_1 \cdot EX_{1,3} \cdot RL_{1,1} \cdot RC_{1,3})$ = *round*(10·0,95· 0,87·1) = 8,3, E_1 = $round((AT_1 + (10 - AT_1)\,CDP_{1,4})\,TD_{1,2})$ = *round*((8,3 + (10 – 8,3) 0,4)) 0,25) = 2,2. Полученное значение E_1 скорректировало параметры B_1 и T_1.

Расчет для $V_{1,2}$ = «CVE-2015-2516»:

– для B_2 определены следующие значения $AV_{2,3}$ = «*N*», $AC_{2,2}$ = «*M*», $AU_{2,3}$ = «*N*», $C_{2,1}$ = «*N*», $I_{2,1}$ = «*N*», $A_{2,2}$ = «*P*», тогда $AV_{2,3}$ = 1, $AC_{2,2}$ = 0,61, $AU_{2,3}$ = 0,704, $C_{2,1}$ = $I_{2,1}$ = 0, $A_{2,2}$ = 0,275. Вычисляем EXb_2 = 20·1·0,61· 0,704 = 8,6, IM_2 = 10,41 (1 – (1 – 0) (1 – 0) (1 – 0,275)) = 2,9 и тогда $f(IM)$ = 1,176, B_2 = *round*(0,6·2,9 + 0,4·8,6 – 1,5) 1,176 = 4,3;

– для T_2 в базе NVD отсутствуют определенные значения, поэтому с помощью суждений экспертов, например, определим значения для $EX_{2,1}$ = «*U*», $RL_{2,2}$ = «*TF*», $RC_{2,1}$ = «UC» и тогда $EX_{2,1}$ = 0,85, $RL_{2,2}$ = 0,9, $RC_{2,1}$ = 0,9, T_2 = *round*(4,3·0,85·0,9·0,9) = 3;

– для E_2, по аналогии с T_2, значения определяются также с помощью экспертов, если $CDP_{2,4}$ = «MH», $TD_{2,3}$ = «M», $CR_{2,2}$ = «M», $IR_{2,2}$ = «M», $AR_{2,3}$ = «H», то $CDP_{2,4}$ = 0,4, $TD_{2,3}$ = 0,75, $CR_{2,2}$ = 1, $IR_{2,2}$ = 1, $AR_{2,3}$ = 1,51. На основе этого вычисляем AIM_2 = min(10; 10,41 (1 – (1 – 0·1) (1 – 0·1) (1 – 0,275·1,51)) = 4,3, AB_2 = *round*((0,6·4,3) + (0,4·8,6) – 1,5) 1,176 = 5,3, AT_2 = *round*(5,3·0,85·0,9·0,9) = 3,7, E_2 = *round*((3,7 + (10 – 3,7) 0,4)) 0,75) = 4,6. Полученное значение E_2 скорректировало параметры B_2 и T_2.

По аналогии с предыдущими уязвимостями для $V_{1,3}$ = «CVE-2016-2386», $V_{1,4}$ = «CVE-2015-

1830», $V_{1,5}$ = «CVE-2016-0497» также были сформированы оценочные параметры. Их значения занесены в таблицу 5.

Таблица 5

Определение текущих значений оценочных параметров (пример)

$\boldsymbol{EP}_i$	$ep_{1,i}$	$ep_{2,i}$	$ep_{3,i}$	$ep_{4,i}$	$ep_{5,i}$
$\boldsymbol{B}$, (i=1)	9,3	4,3	7,5	5	4,3
$\boldsymbol{T}$, (i=2)	7,7	3	6,8	3,8	3,5
$\boldsymbol{E}$, (i=3)	2,2	4,6	8,8	1,7	1,2

Шаг 9. Далее осуществим классификацию текущих значений $ep_{uz,i}$ по формуле (4) и (5) при $m = 5$, результаты которых заносятся в табл. 6:

$$\mu_1(ep_{uz,i}) = \begin{cases} L\left(\dfrac{a_{i_1} - ep_{uz,i}}{a_{i_1} - b_{i_{11}}}\right), & ep_{uz,i} \in [a_{i_1}, b_{i_{11}}]; \\ 1, & ep_{uz,i} \in [b_{i_{11}}, b_{i_{21}}]; \\ R\left(\dfrac{ep_{uz,i} - c_{i_1}}{b_{i_{21}} - c_{i_1}}\right), & ep_{uz,i} \in [b_{i_{21}}, c_{i_1}], \end{cases}$$

$$\mu_2(ep_{uz,i}) = \begin{cases} L\left(\dfrac{a_{i_2} - ep_{uz,i}}{a_{i_2} - b_{i_{12}}}\right), & ep_{uz,i} \in [a_{i_2}, b_{i_{12}}]; \\ 1, & ep_{uz,i} \in [b_{i_{12}}, b_{i_{22}}]; \\ R\left(\dfrac{ep_{uz,i} - c_{i_2}}{b_{i_{22}} - c_{i_2}}\right), & ep_{uz,i} \in [b_{i_{22}}, c_{i_2}], \end{cases}$$

$$\mu_3(ep_{uz,i}) = \begin{cases} L\left(\dfrac{a_{i_3} - ep_{uz,i}}{a_{i_3} - b_{i_{13}}}\right), & ep_{uz,i} \in [a_{i_3}, b_{i_{13}}]; \\ 1, & ep_{uz,i} \in [b_{i_{13}}, b_{i_{23}}]; \\ R\left(\dfrac{ep_{uz,i} - c_{i_3}}{b_{i_{23}} - c_{i_3}}\right), & ep_{uz,i} \in [b_{i_{23}}, c_{i_3}], \end{cases}$$

$$\mu_4(ep_{uz,i}) = \begin{cases} L\left(\dfrac{a_{i_4} - ep_{uz,i}}{a_{i_4} - b_{i_{14}}}\right), & ep_{uz,i} \in [a_{i_4}, b_{i_{14}}]; \\ 1, & ep_{uz,i} \in [b_{i_{14}}, b_{i_{24}}]; \\ R\left(\dfrac{ep_{uz,i} - c_{i_4}}{b_{i_{24}} - c_{i_4}}\right), & ep_{uz,i} \in [b_{i_{24}}, c_{i_4}], \end{cases}$$

$$\mu_5(ep_{uz,i}) = \begin{cases} L\left(\dfrac{a_{i_5} - ep_{uz,i}}{a_{i_5} - b_{i_{15}}}\right), & ep_{uz,i} \in [a_{i_5}, b_{i_{15}}]; \\ 1, & ep_{uz,i} \in [b_{i_{15}}, b_{i_{25}}]; \\ R\left(\dfrac{ep_{uz,i} - c_{i_5}}{b_{i_{25}} - c_{i_5}}\right), & ep_{uz,i} \in [b_{i_{25}}, c_{i_5}]. \end{cases}$$

Шаг 10. Произведем вычисление показателя степени риска нарушения ИБ по формуле (6), где $m = 5$, $j = \overline{1,5}$, $i = \overline{1,3}$, $n_1 = \overline{1,5}$, $K_{lr_1} = 10$, $K_{lr_2} = 30$, $K_{lr_3} = 50$, $K_{lr_4} = 70$, $K_{lr_5} = 90$, $ks = 0{,}5$ и тогда $LRV_{1,1} = 71{,}95$, $LRV_{1,2} = 39{,}94$, $LRV_{1,3} = 62{,}25$, $LRV_{1,4} = 41{,}57$, $LRV_{1,5} = 36{,}75$.

Таблица 6

Классификация текущих значений оценочных параметров (пример)

$\boldsymbol{EP}_i$	Значение $\lambda_{uz,ij}$ для $\{\bigcup_{uz=1}^{5} \boldsymbol{V}_{1,uz}\}$, $(uz = \overline{1,5})$																									
	$\lambda_{1,ij}$ для $\underset{\sim}{T}_{K_{EP_i 1}}$ $(i = \overline{1,3},\ j = \overline{1,5})$					$\lambda_{2,ij}$ для $\underset{\sim}{T}_{K_{EP_i 2}}$ $(i = \overline{1,3},\ j = \overline{1,5})$					$\lambda_{3,ij}$ для $\underset{\sim}{T}_{K_{EP_i 3}}$ $(i = \overline{1,3},\ j = \overline{1,5})$					$\lambda_{4,ij}$ для $\underset{\sim}{T}_{K_{EP_i 4}}$ $(i = \overline{1,3},\ j = \overline{1,5})$					$\lambda_{5,ij}$ для $\underset{\sim}{T}_{K_{EP_i 5}}$ $(i = \overline{1,3},\ j = \overline{1,5})$				
$\boldsymbol{B}$	0	0	0	0,43	0,64	0	0,39	0,64	0	0	0	0	0,29	0,82	0	0	0	1	0	0	0	0,39	0,64	0	0
$\boldsymbol{T}$	0	0	0	1	0	0	1	0	0	0	0	0	0,74	0,14	0	0	0,64	0,31	0	0	0	0,79	0,12	0	0
$\boldsymbol{E}$	0	1	0	0	0	0	0,24	0,83	0	0	0	0	0	0,92	0	0	1	0	0	0	0	1	0	0	0

Шаг 11. По аналогии с шагом 8 по формуле (4) вычислим $\mu_j(LRV_{1,uz})$, $(uz = \overline{1,5})$,

$$\mu_j(LRV_{1,uz}) = \begin{cases} L\left(\dfrac{a_j - LRV_{1,uz}}{a_j - b_{1j}}\right), & LRV_{1,uz} \in [a_j, b_{1j}]; \\ 1, & LRV_{1,uz} \in [b_{1j}, b_{2j}]; \\ R\left(\dfrac{LRV_{1,uz} - c_j}{b_{2j} - c_j}\right), & LRV_{1,uz} \in [b_{2j}, c_j]. \end{cases}$$

Далее с помощью (7) формируются SP_{uz}: $SP_1 = (LRV_{1,1}; T_{DR_4}(\mu_4(LRV_{1,1})))$ = (71,95; PB), SP_2 = $(LRV_{1,2};\ T_{DR_2}(\mu_2(LRV_{1,2}));\ T_{DR_3}(\mu_3(LRV_{1,2})))$ = (39,94; PH(0,41); PC(0,59)), $SP_3 = (LRV_{1,3};\ T_{DR_3}(\mu_3(LRV_{1,3}));$ $T_{DR_4}(\mu_4(LRV_{1,3})))$ = (62,25; PC(0,4); PB(0,6)), SP_4 = $(LRV_{1,4};\ T_{DR_2}(\mu_2(LRV_{1,4}));\ T_{DR_3}(\mu_3(LRV_{1,4})))$ = (41,57; PH(0,26); PC(0,74)), $SP_5 = (LRV_{1,5};\ T_{DR_2}(\mu_2(LRV_{1,5}));$

$T_{DR_3}(\mu_3(DRV_{1,5}))$ = (36,75; РН(0,69); РС(0,31)), где, например, (62,25; РС(0,4); РВ(0,6)) словесно интерпретируется, как «Степень риска с числовым эквивалентом 62,25 граничит между средним риском и высоки риском по границе РС – 0,4 и РВ – 0,6».

Также для данного $RISO_1$ на основе выражения (8), можно вычислить среднее значение степени риска: LR_1=(71,95 + 39,94 + 62,25 + 41,57 + 36,75) / 5 = 50,5 и сформировать для него SP = (50,5; РС).

Для верификации представленного метода осуществим моделирование нескольких состояний среды оценивания: 1-е состояние – уменьшим относительно текущего состояния значения всех оценочных параметров (см. табл. 7 и 8); 2-е состояние – увеличим относительно текущего состояния значения всех оценочных параметров (см. табл. 9 и 10).

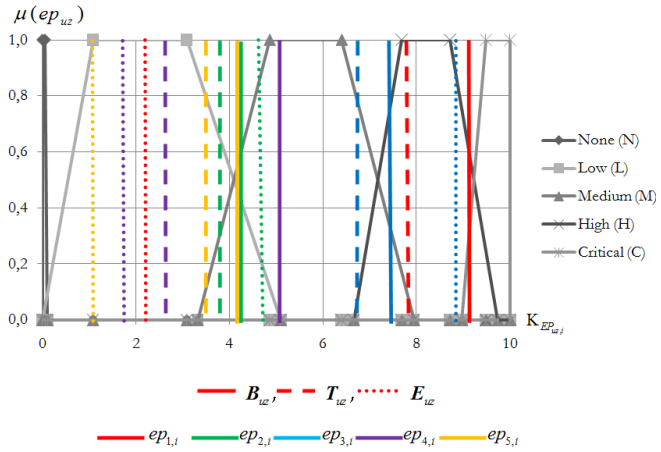

Рис. 3. Результаты вычисления числовых значений для оценочных параметров

Пример 2 (1-е состояние)

Согласно 1-го состояния при m = 5 оценочные параметры принимают значения, которые отражены в табл. 7.

Реализуем классификацию значений $ep_{uz,i}$ по формуле (9) и (10), результаты которой занесены в табл. 8.

Таблица 7

1-е состояние значений оценочных параметров

EP_i	$ep_{1,i}$	$ep_{2,i}$	$ep_{3,i}$	$ep_{4,i}$	$ep_{5,i}$
B, (i=1)	8,3	3,3	6,5	4	3,3
T, (i=2)	6,7	2	5,8	2,8	2,5
E, (i=3)	1,2	3,6	7,8	0,7	0,2

Произведем вычисление показателя степени риска нарушения ИБ по формуле (6), где m = 5, $j=\overline{1,5}$, $i=\overline{1,3}$, $n_1=\overline{1,5}$, K_{lr_1} = 10, K_{lr_2} = 30, K_{lr_3} = 50, K_{lr_4} = 70, K_{lr_5} = 90, ks = 0,5 и тогда $LRV_{1,1}$ = 54,46, $LRV_{1,2}$ = 30,2, $LRV_{1,3}$ = 51,98, $LRV_{1,4}$ = 32,37, $LRV_{1,5}$ = 24,34. По формуле (4) вычислим $\mu_j(LRV_{1,uz})$, $(uz=\overline{1,5})$. С помощью (7) формируются SP_{uz}: $SP_1=(LRV_{1,1};\ T_{DR_3}(\mu_3(LRV_{1,1})))$ = (54,46; РС), $SP_2=(LRV_{1,2};\ T_{DR_2}(\mu_2(LRV_{1,2})))$ = (30,2; РН), $SP_3=(LRV_{1,3};\ T_{DR_3}(\mu_3(LRV_{1,3})))$ = (51,8; РС), $SP_4=(LRV_{1,4};\ T_{DR_2}(\mu_2(LRV_{1,4})))$ = (32,37; РН), $SP_5=(LRV_{1,5};\ T_{DR_2}(\mu_2(LRV_{1,5})))$ = (24,34; РН).

Далее на основе выражения (8) для $RISO_1$, можно вычислить среднее значение степени риска, т.е. LR_1 = 38,64 и сформировать для него SP = (38,64; РН(0,52); РС(0,48)).

Таблица 8

Классификация 1-го состояния значений оценочных параметров

EP_i	Значение $\lambda_{uz,ij}$ для $\{\bigcup_{uz=1}^{5} V_{1,uz}\}$, $(uz=\overline{1,5})$																									
	$\lambda_{1,ij}$ для $T_{K_{EP_i1}}$ $(i=\overline{1,3},\ j=\overline{1,5})$					$\lambda_{2,ij}$ для $T_{K_{EP_i2}}$ $(i=\overline{1,3},\ j=\overline{1,5})$					$\lambda_{3,ij}$ для $T_{K_{EP_i3}}$ $(i=\overline{1,3},\ j=\overline{1,5})$					$\lambda_{4,ij}$ для $T_{K_{EP_i4}}$ $(i=\overline{1,3},\ j=\overline{1,5})$					$\lambda_{5,ij}$ для $T_{K_{EP_i5}}$ $(i=\overline{1,3},\ j=\overline{1,5})$				
B	0	0	0	1	0	0	1	0	0	0	0	0	0,94	0	0	0	0,54	0,44	0	0	0	0,89	0	0	0
T	0	0	0,81	0,04	0	0	1	0	0	0	0	0	1	0	0	0	1	0	0	0	0	1	0	0	0
E	0	1	0	0	0	0	0,74	0,18	0	0	0	0	0	1	0	0	0,65	0	0	0	0	0,19	0	0	0

Пример 3 (2-е состояние)

Согласно 2-го состояния при m = 5 оценочные параметры принимают значения, которые отражены в табл. 9.

Произведем классификацию значений $ep_{uz,i}$ по формуле (4) и (5), результаты которой занесены в табл. 10.

Таблица 9

2-е состояние значений оценочных параметров

EP_i	$ep_{1,i}$	$ep_{2,i}$	$ep_{3,i}$	$ep_{4,i}$	$ep_{5,i}$
B, (i=1)	10	5,3	8,5	6	5,3
T, (i=2)	8,7	4	7,8	4,8	4,5
E, (i=3)	3,2	5,6	9,8	2,7	2,2

Далее, аналогично первому состоянию, вычислим показатель степени риска нарушения ИБ по формуле (6), т.е. $LRV_{1,1}$ = 73,1, $LRV_{1,2}$ = 46,05, $LRV_{1,3}$ = 73,3, $LRV_{1,4}$ = 47,44, $LRV_{1,5}$ = 45,76.

Посредством (4) вычислим $\mu_j(LRV_{1,uz})$, $(uz=\overline{1,5})$, а по выражению (7) формируются SP_{uz}:

$SP_1 = (LRV_{1,1};\ T_{DR_4}(\mu_4(LRV_{1,1}))) = (73{,}1;\ \text{РВ})$,

$SP_2 = (LRV_{1,2};\ T_{DR_3}(\mu_3(LRV_{1,2}))) = (46{,}05;\ \text{РС})$,

$SP_3 = (LRV_{1,3};\ T_{DR_4}(\mu_4(LRV_{1,3}))) = (73{,}3;\ \text{РВ})$,

$SP_4 = (LRV_{1,4};\ T_{DR_3}(\mu_3(LRV_{1,4}))) = (47{,}44;\ \text{РС})$,

$SP_5 = (LRV_{1,5};\ T_{DR_3}(\mu_3(LRV_{1,5}))) = (45{,}76;\ \text{РС})$.

Таблица 10

Классификация 2-го состояния значений оценочных параметров

EP_i	Значение $\lambda_{uz,ij}$ для $\{\bigcup_{uz=1}^{5} V_{1,uz}\}$, $(uz=\overline{1,5})$																									
	$\lambda_{1,ij}$ для $\underset{\sim}{T}_{K_{EP_i1}}$ $(i=\overline{1,3},\ j=\overline{1,5})$					$\lambda_{2,ij}$ для $\underset{\sim}{T}_{K_{EP_i2}}$ $(i=\overline{1,3},\ j=\overline{1,5})$					$\lambda_{3,ij}$ для $\underset{\sim}{T}_{K_{EP_i3}}$ $(i=\overline{1,3},\ j=\overline{1,5})$					$\lambda_{4,ij}$ для $\underset{\sim}{T}_{K_{EP_i4}}$ $(i=\overline{1,3},\ j=\overline{1,5})$					$\lambda_{5,ij}$ для $\underset{\sim}{T}_{K_{EP_i5}}$ $(i=\overline{1,3},\ j=\overline{1,5})$				
B	0	0	0	0	1	0	0	1	0	0	0	0	0	1	0	0	0	1	0	0	0	0	1	0	0
T	0	0	0	1	0	0	0,54	0,44	0	0	0	0	0	1	0	0	0,14	0,96	0	0	0	0,29	0,77	0	0
E	0	0,94	0	0	0	0	0	1	0	0	0	0	0	0	1	0	1	0	0	0	0	1	0	0	0

На основе выражения (8), вычислим среднее значение степени риска LR_1 = 57,13 и сформируем для него SP = (57,13; РС(0,86); РВ(0,14)).

Графическое представление полученных результатов отображено на рис. 4. и рис. 5.

Рис. 4. Результаты вычисления значений для $LRV_{1,uz}$ при разных состояниях: 1-е состояние – уменьшенные, относительно текущего состояния, значения всех оценочных параметров; текущие состояние – значения оценочных параметров определенных с помощью базы NVD; 2-е состояние – увеличенные, относительно текущего состояния, значения всех оценочных параметров

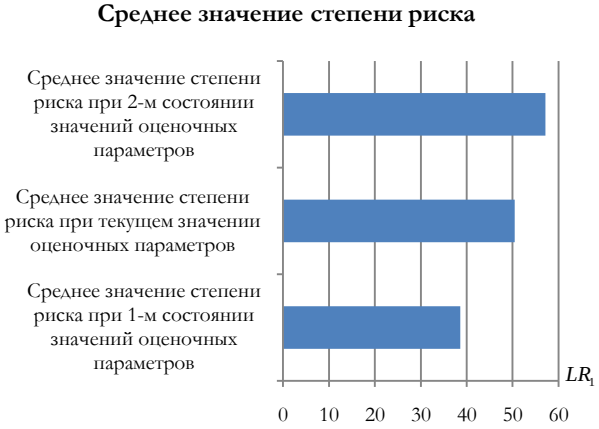

Рис. 5. Результаты вычисления значений для LR_1 при разных состояниях

Как видно из полученных результатов, предлагаемый метод адекватно реагирует на изменения выходных значений оценочных параметров, т.е. при их уменьшении показатели степени риска уменьшаются, а при увеличении – увеличиваются.

Выводы. Таким образом, представленный качественно-количественный метод анализа и оценивания рисков информационной безопасности за счет модификации процедур определения множества параметров оценивания риска и оценки текущих значений параметров с возможностью интеграции (в качестве альтернативы

оценок экспертов) значений CVSS показателей, которые представлены в соответствующих базах данных, позволяет автоматизировать процесс оценивания уязвимостей без привлечения экспертов необходимой предметной области.

ЛИТЕРАТУРА

[1] Information technology. Security techniques. Information security management systems. Requirements: ISO/IEC 27001:2013, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2013, 34 p.

[2] Казмирчук С.В. Интегрированный метод анализа и оценивания рисков информационной безопасности / С.В. Казмирчук, А.Ю. Гололобов // Защита информации – 2014. – №3. – С. 252-261.

[3] Корченко А.Г. Анализ и оценивание рисков информационной безопасности / А.Г. Корченко, А.Е. Архипов, С.В. Казмирчук // Монография. – К.: ООО «Лазурит-Полиграф», 2013. – 275 с.

[4] Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / А.Г. Корченко – К. : «МК-Пресс», 2006. – 320с.

[5] National Vulnerability Database [Electronic resource] / National Institute of Standards and Technology – Gaithersburg, 2016 – Access mode: World Wide Web. – URL: https:// nvd.nist.gov / home.cfm.

[6] Банк данных угроз безопасности информации [Электронный ресурс] / Федеральной службой по техническому и экспортному контролю России – Москва, 2016 – Режим доступа: World Wide Web. – URL: http://bdu.fstec.ru/.

[7] Open Sourced Vulnerability Database [Electronic resource] / Open Security Foundation – Lafayette, 2016 – Access mode: World Wide Web. – URL: https:// http://osvdb.org/.

[8] IBM X-Force Exchange [Electronic resource] / IBM Corporation – New York, 2016 – Access mode: World Wide Web. – URL: https:// exchange.xforce.ibmcloud.com/vulnerabilities/109429.

[9] Vulnerability Notes Database [Electronic resource] / United States Computer Emergency Readiness Team Murray Lane, 2016 Access mode: World Wide Web. – URL: https:// www. kb.cert.org /vuls/#.

[10] Vulnerabilities [Electronic resource] / SecurityFocus - Mountain View, 2016 - Access mode: World Wide Web. – URL: http:// www. securityfocus.com /.

[11] A Complete Guide to the Common Vulnerability Scoring System. Version 2.0 [Electronic resource] / Forum of Incident Response and Security Teams – Morrisville, 2016 – Access mode: World Wide Web. – URL: http:// www.first.org /cvss/ v2/guide.

[12] Корченко А.Г. Метод n-кратного понижения числа термов лингвистических переменных в задачах анализа и оценивания рисков / А.Г. Корченко, Б.С. Ахметов, С.В. Казмирчук, А.Ю. Гололобов, Н. А. Сейлова // Защита информации – 2014. – Том 16 №4 (65), жовтень-грудень. – С. 284-291.

[13] Корченко А.Г. Метод n-кратного инкрементирования числа термов лингвистических переменных в задачах анализа и оценивания рисков / А.Г. Корченко, Б.С. Ахметов, С.В. Казмирчук, М.Н. Жекамбаева // Безпека інформації. – 2015. – Т.21. –№2. – С. 191-200.

[14] Корченко А.Г. Метод преобразования интервалов в нечеткие числа для систем анализа и оценивания рисков / А.Г. Корченко, С.В. Казмирчук // Правовое, нормативное и метрологическое обеспечение системы защиты информации в Украине – 2016. - № 1(31). - С. 57-64.

REFERENCES

[1] Information technology. Security techniques. Information security management systems. Requirements: ISO/IEC 27001:2013, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2013, 34 p.

[2] Kazmirchuk S.V., Gololobov A. Ur., The integrated risk analysis and risk assessment method of information security, Zahist ìnformacìï, 2014, VOL. 16 №3, pp. 252-261.

[3] Korchenko A.G., Arkhipov A.E., Kazmirchuk S.V. Analysis and assessment of information security risks, Monograph., K : LLC «Lazurit-Polygraph», 2013., 275 p.

[4] Korchenko A.G. The construction of security systems on the fuzzy sets. Theory and practical solutions, 2006, 320 p.

[5] National Vulnerability Database [Electronic resource] / National Institute of Standards and Technology – Gaithersburg, 2016 – Access mode: World Wide Web. – URL: https://nvd.nist.gov/ home.cfm.

[6] Data Bank information security threats [electronic resource] / by the Federal Service for Technical and Export Control of Russia - Moscow, 2016 – Access mode: World Wide Web. – URL: http://bdu.fstec.ru/.

[7] Open Sourced Vulnerability Database [Electronic resource] / Open Security Foundation – Lafayette, 2016 – Access mode: World Wide Web. – URL: https:// http://osvdb.org/.

[8] IBM X-Force Exchange [Electronic resource] / IBM Corporation – New York, 2016 – Access mode: World Wide Web. – URL: https:// exchange.xforce.ibmcloud.com/vulnerabilities/109429.

[9] Vulnerability Notes Database [Electronic resource] / United States Computer Emergency Readiness Team Murray Lane, 2016 Access mode: World Wide Web. – URL: https:// www. kb.cert.org/ vuls/#.

[10] Vulnerabilities [Electronic resource] / SecurityFocus - Mountain View, 2016 - Access mode: World Wide Web. – URL: http:// www. securityfocus.com/.

[11] A Complete Guide to the Common Vulnerability Scoring System. Version 2.0 [Electronic resource] / Forum of Incident Response and Security Teams – Morrisville, 2016 – Access mode: World Wide Web. – URL: http://www.first.org/ cvss/v2/guide.

[12] Korchenko A.G., Akhmetov B.S., Kazmirchuk S.V., Gololobov A. Ur., Seilova N.A., The n-fold decrease method of terms number of linguistic variables in risk assessment and task analysis, Zahist ìnformacïi, 2014, VOL. 16 №4, pp. 284-291.

[13] Korchenko A.G., Akhmetov B.S., Kazmirchuk S.V., Zhekambaeva M.N. Method of n-fold incrementation the number of terms the linguistic variables in the tasks of analysis and risk assessment, Bezpeka Informácie, 2015, VOL. 21 №2, pp. 191-200.

[14] Korchenko A.G., Kazmirchuk S.V., Method of intervals transformation in fuzzy numbers for information security risk analysis and assessment systems, Pravovoye, normativnoye i metrologicheskoye obespecheniye sistemy zashchity informatsii v Ukraine, 2016, № 1(31), pp. 57-64.

ЯКІСНО-КІЛЬКІСНИЙ МЕТОД ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В основу систем менеджменту інформаційної безпеки покладені процеси аналізу і оцінювання ризиків. Для їх реалізації застосовуються відомі методи аналізу та оцінювання ризиків, засновані на експертних оцінках. Часто в процесі оцінювання виникають ситуації, при яких експерт не завжди чітко може оцінити ту чи іншу уразливість ресурсів інформаційних систем. У зв'язку з цим доцільно використовувати відповідні бази даних уразливостей. Існуючі підходи поки не дозволяють ефективно вирішувати поставлену задачу. Для цього пропонується якісно-кількісний метод оцінювання ризиків. Він, на відміну від відомих методів, шляхом використання оцінок, які надаються в існуючих базах даних, дозволяє автоматизувати процес оцінювання ризиків і не привертати для цього експертів відповідної предметної області.

Ключові слова: ризик, оцінювання ризиків, система аналізу і оцінювання ризиків, параметри ризику, нечітка змінна, нечіткі числа, перетворення еталонів нечітких чисел, якісно-кількісний метод оцінювання ризиків, база даних уразливостей.

THE QUALITATIVE AND QUANTITATIVE METHOD OF INFORMATION SECURITY RISK ASSESSMENT

The basis of information security management system (ISMS) is the processes of analysis and risk assessment. The known methods of analysis and risk assessment based on expert assessments are applied for their implementation. Often in the process of assessment there are situations when the expert cannot always clearly determine a particular vulnerability of Information Systems Resources (ISR). Therefore, it is advisable to use the corresponding database vulnerabilities. The existing approaches do not solve the task effectively. For this purpose, the qualitative and quantitative method of risk assessment is offered. It, in contrast to the known methods, through the use of assessments that are available in existing databases, automates the process of risk assessment not involving the experts for this related subject area.

Index terms: risk, risk assessment, system analysis and risk assessment, risk parameters, fuzzy variable, fuzzy numbers, conversion of fuzzy numbers standards, qualitative-quantitative method of risk assessment, database vulnerabilities.

Корченко Александр Григорьевич, доктор технических наук, профессор, лауреат Государственной премии Украины в области науки и техники, заведующий кафедрой безопасности информационных технологий Национального авиационного университета.
E-mail: icaocentre@nau.edu.ua

Корченко Олександр Григорович, доктор технічних наук, професор, лауреат Державної премії України в галузі науки і техніки, завідувач кафедрою безпеки інформаційних технологій Національного авіаційного університету.

Korchenko Oleksandr, Dr Eng (Information security), professor, laureate of the State Prize of Ukraine in Science and Technology, Head of IT-Security Academic Department, National Aviation University (Kyiv, Ukraine).

Казмирчук Светлана Владимировна, кандидат технических наук, доцент, доцент кафедры безопасности информационных технологий Национального авиационного университета.
E-mail: sv.kazmirchuk@gmail.com

Казмірчук Світлана Володимирівна, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.

Kazmirchuk Svitlana, PhD in Eng., Associate Professor of IT-Security Academic Department, National Aviation University.