Список використаної літератури: ***1****. Закон України Про радіочастотний ресурс України N 1770-III від 01.06.2000 http://zakon.nau.ua/doc/?code=1770-14* ***2.*** *Постанова Кабінету Міністрів України від 29.07.2009 N 785 Про затвердження Технічного регламенту з електромагнітної сумісності обладнання.* ***3.*** *Рішення Національної ради України з питань телебачення і радіомовлення від 02.12.2008 № 2151 Про затвердження Порядку розробки висновків щодо електромагнітної сумісності радіоелектронних засобів мовлення, необхідних для створення та розвитку каналів мовлення, мереж мовлення та телемереж.* ***4.*** *Седельников Ю. Е. Электромагнитная совместимость радиоэлектронных средств: учеб. пособие/ Седельников Ю. Е. - Казань: ЗАО «Новое знание», 2006. - 304 с.* ***5.*** *Малков Н. А. Электромагнитная совместимость радиоэлектронных средств: учеб. пособие / Н. А. Малков, А. П Пудовкин. – Тамбов: Изд-во Тамб. гос. техн. ун-та, 2007.- 88 с.* ***6.*** *Быховский М. А. и др. Управление радиочастотным спектром и электромагнитная совместимость радиосистем. учеб. пособие/ Под ред. д. т. н., проф. Быховского М. А. – М.: Эко-Трендз, 2006. – 376 с.* ***7.*** *Технічна колекція Schneider-Electric: вып. 32. ЕМС - Электромагнитная совместимость, 2009, www.schneider-electric.com.ua.* ***8.*** *Рекомендації сектору радіозв'язку МСЕ: - МСЕ-Р ВТ.417 "Мінімальна напруженість поля, захист якої може бути необхідним при плануванні послуг аналогового наземного телевізійного мовлення"; - МСЕ-Р ВТ.470 "Стандартні системи аналогового телебачення";- МСЕ-Р ВТ.500 "Методика суб'єктивної оцінки якості телевізійного зображення".* ***9.*** *ГОСТ 29037-91 (2004) - Порядок проведення сертифікаційних випробувань на відповідність вимогам електромагнітної сумісності.*

Микола Карпінський, Анна Корченко*, Андрій Гізун*
*Університет Бєльсько-Бяла – Техніко-гуманітарна академія (м. Бєльсько-Бяла, Польща), *Національний авіаційний університет*

УДК 004.056.53:004.492.3(045)

ІНТЕГРОВАНА МОДЕЛЬ ПРЕДСТАВЛЕННЯ КРИЗОВИХ СИТУАЦІЙ ТА ФОРМАЛІЗОВАНА ПРОЦЕДУРА ПОБУДОВИ ЕТАЛОНІВ ІДЕНТИФІКУЮЧИХ ПАРАМЕТРІВ

Анотація: **Запропонована інтегрована модель представлення кризових ситуацій, яка шляхом використання нечіткої логіки може бути застосована для опису будь-якої категорії кризових ситуацій в умовах слабоформалізованого нечіткого середовища, а також описана процедура формування еталонів ідентифікуючих параметрів.**
Summary: **The integrated model representation crisis that use fuzzy logic and can be used to describe any category of crisis in weakly-formalized fuzzy environment was proposed. Also was described how to format standards of identifying parameters.**
Ключові слова: **Кризова ситуація, інцидент, рівень критичності, множина критеріїв, теорія нечітких множин, інтегрована модель кризових ситуацій, кортеж, експертні підходи, еталони лінгвістичних змінних.**

І Актуальність

Важливість інформаційних технологій, інформаційно-комунікаційних систем та мереж (ІКСМ) в аспекті забезпечення існування людства як організованої форми суспільства беззаперечна. Так, на сьогодні практично будь-яка діяльність, будь-який бізнес-процес в усіх установах чи організаціях повністю залежать від їх функціонування, при цьому переривання даних процесів залежно від його класу та критичності може завдати значних збитків. Для вирішення такої проблеми була розроблена і сьогодні динамічно розвивається концепція управління безперервністю бізнесу (КУББ). В відомих роботах був проведений аналіз різних трактувань терміна кризова ситуація (КС) та суміжних понять в багатьох сферах людської діяльності, що дозволив відобразити ці поняття у сфері інформаційної безпеки (ІБ) та виявити особливості кожного з визначень, які є загальними для всіх. Саме за цими особливостями проводиться диференціація між КС та інцидентами ІБ (ІІБ). Крім того, встановлено наявність в більшості випадків причинно-наслідкових зв'язків між ними. Так за відсутності контролю існує достатньо висока потенційна можливість того, що ІІБ набуде таких значень параметрів та суттєвих характеристик, які дозволять класифікувати його як КС. Тобто можна говорити, що причиною будь-якої КС може стати ІІБ з високим степенем критичності, що визначається, наприклад, рівнем збитків, числом постраждалих та іншими характеристиками, тобто інцидент-потенційна КС (ІПКС). З метою підвищення рівня захищеності ІКСМ та загалом інформаційних ресурсів необхідним є своєчасне виявлення ІПКС та підбір адекватних засобів та заходів реагування відповідно до критичності

загрози, породженої ними. Тому розробка інтегрованої моделі представлення КС, що має стати базисом для створення методів та засобів їх виявлення та оцінки, є актуальною науковою задачею.

II Аналіз публікацій

В роботах [1, 2] запропонована модель представлення ризиків ІБ, в якій використовуються елементи нечіткої логіки, доцільність чого обґрунтована в [3]. Результати, наведені в цих роботах використані як базис в даному досліджені. Слід зазначити зв'язок роботи з публікаціями, в яких описані системи та методи виявлення порушника ІБ [4, 5] і аномальних станів, породжених комп'ютерними атаками [6], а також відповідні ідентифікуючі параметри їх виявлення та ідентифікації [7 – 9]. Зазначені роботи були використані для формування компонентів моделі представлення КС, зокрема ідентифікатора та підмножини ідентифікуючих параметрів. Крім того, процедура побудови еталонів нечітких ідентифікуючих параметрів заснована на методі, описаному в [10], а також на попередніх роботах, де описані процедури формування евристичних правил [11] та оцінки рівня критичності [12] як елементів кортежу, що відображає ІПКС або КС. Таким чином відмітимо, що в цих роботах не в достатній мірі формалізовані процеси управління КС (УКС), зокрема відсутня модель, яка б давала можливість представити і математично описати процеси виявлення, ідентифікації та оцінки ІПКС.

III Основна мета дослідження

Важливим аспектом КУББ є УКС, що включає в себе низку процесів, а саме: прогнозування, ідентифікація, оцінка КС, реагування та ліквідація наслідків КС. Для ефективного функціонування зазначених етапів УКС необхідною є розробка інтегрованої моделі представлення КС, яка дала б змогу описати різні КС незалежно від їх характеристик, причин походження тощо, що і є метою даної роботи. Використання такої моделі дозволить проводити УКС в умовах невизначеності та неформалізованості контрольованого середовища (зокрема в галузі ІБ) за рахунок застосування експертних методів та математичного апарату нечіткої логіки.

IV Основна частина дослідження

Для формалізації процесів УКС введемо множину ІПКС:

$$\mathbf{ІКS} = \{\bigcup_{i=1}^{n} \mathbf{ІКS_i}\} = \{\mathbf{ІКS_1}, \ldots, \mathbf{ІКS_n}\}, \ (i = \overline{1,n}), \tag{1}$$

де n визначає кількість потенційних ІПКС, тобто інцидентів, що можуть спричинити кризовий стан, кожен з яких відображається у вигляді узагальненого шестикомпонентного кортежу за аналогією з [13]:

$$\mathbf{ІКS_i} = < IKS_i, \ \mathbf{P_i}, \mathbf{T_i^e}, \ \underset{\sim}{\mathbf{P}}_\mathbf{i}, \ \mathbf{ER_i}, \ LCS_i >, \tag{2}$$

в якому: IKS_i – ідентифікатор i-го ІПКС, що є (або може стати) причиною виникнення КС; $\mathbf{P_i}$ – підмножина можливих параметрів, що використовуються для прогнозування чи ідентифікації i-го інциденту; $\mathbf{T_i^e}$ – підмножина всіх можливих нечітких (лінгвістичних) еталонів, що відображають еталонні стани відповідних параметрів з підмножини $\mathbf{P_i}$; $\underset{\sim}{\mathbf{P}}_\mathbf{i}$ – підмножина поточних значень параметрів за певний проміжок часу; $\mathbf{ER_i}$ – підмножина евристичних правил, побудованих на основі нечітких параметрів, які використовуються для виявлення/ідентифікації i-го ІПКС; LCS_i – рівень критичності ситуації, спричиненої i-м ІПКС.

Ситуація відноситься до кризової лише якщо рівень її критичності вищий середнього або більший, тобто $LCS_i \gtrsim BC^e$. В іншому разі інцидент взагалі залишається поза увагою (при достатньо низькому рівні критичності) або проводиться реагування на нього з метою контролю і усунення як для звичайного ІІБ. Розглянемо кожен з компонентів кортежу.

Ідентифікатор IKS_i зв'язує елемент множини $\mathbf{ІКS}$ з певним інцидентом, який визначається через відповідне йому ім'я. Наприклад, при $n = 5$ отримаємо $\mathbf{ІКS} = \{\bigcup_{i=1}^{5} \mathbf{ІКS_i}\} = \{\mathbf{ІКS_1}, \ \mathbf{ІКS_2}, \ \mathbf{ІКS_3}, \ \mathbf{ІКS_4}, \ \mathbf{ІКS_5}\} = \{\mathbf{A}, \ \mathbf{B}, \ \mathbf{C}, \ \mathbf{D}, \ \mathbf{E}\}$ де **A**, **B**, **C**, **D**, **E** – назви інцидентів. В роботах [4, 5] запропонована і описана

система та метод для прогнозування та ідентифікації фактів діяльності порушника, в якій виділені такі категорії як порушник-людина (дезінформатор, спамер, хакер та крекер) та порушник-бот (бот-зломщик та спам-бом). Крім того, в роботі [6] розглянута система та метод виявлення аномальних станів та атак в ІКС, зокрема, спуфінг, атаки відмови в обслуговувані і сканування портів. В [7] розглянуто комп'ютерні інциденти, що можуть стати причинами виникнення КС. Узагальнивши дані робіт та проаналізувавши статистику КС та комп'ютерних атак виділимо такі ІПКС як: «Проникнення порушника в ІКСМ (злом)» – ZL, «Спам» – SP, «Мережева атака відмова в обслуговувані (Dos/DDos)» – DD, «Вірусна атака» – VA, «Вихід з ладу (збій) ІКСМ через вплив мікрокліматичних умов» – ZK.

Отже, множину ідентифікаторів для кількості досліджуваних ІПКС при $n = 5$ згідно з (1) задамо так:

$$\mathbf{IKS} = \{\bigcup_{i=1}^{5} \mathbf{IKS_i}\} = \{\mathbf{IKS_1}, \mathbf{IKS_2}, \mathbf{IKS_3}, \mathbf{IKS_4}, \mathbf{IKS_5}\} = \{\mathbf{ZL}, \mathbf{SP}, \mathbf{DD}, \mathbf{VA}, \mathbf{ZK}\},$$

де $\mathbf{IKS_1} = \mathbf{ZL}$, $\mathbf{IKS_2} = \mathbf{SP}$, $\mathbf{IKS_3} = \mathbf{DD}$, $\mathbf{IKS_4} = \mathbf{VA}$, $\mathbf{IKS_5} = \mathbf{ZK}$ відображають стани контрольованого середовища при відповідних ІПКС, яким будуть присвоєні ідентифікатори $IKS_1 = ZL$, $IKS_2 = SP$, $IKS_3 = DD$, $IKS_4 = VA$, $IKS_5 = ZK$.

Підмножина можливих параметрів $\mathbf{P_i}$, що використовуються для прогнозування чи ідентифікації i-го інциденту формується на основі множини можливих параметрів $\mathbf{P}$, яка включає в себе всі параметри, що контролюються в середовищі, без прив'язки до конкретного типу ІПКС, $\mathbf{P_i} \subseteq \mathbf{P}$. Виходячи з аналізу параметрів, описаних в [7 – 9] та провівши їх узагальнення сформуємо множину можливих параметрів, що характеризують стан контрольованого середовища і дають можливість спрогнозувати та ідентифікувати ІПКС, а за умов високого рівня критичності і КС, $\mathbf{P} = \{\bigcup_{j=1}^{m} P_j\} = \{P_1, \ldots, P_m\}$, $(j = \overline{1,m})$, де m визначає загальну кількість заданих параметрів.

Наприклад, за умови дослідження при $m = 13$ сформована множина матиме такий вигляд:

$$\mathbf{P} = \{\bigcup_{j=1}^{13} P_j\} = \{P_1, \ldots, P_{13}\} = \{Tlog, Nlog, CPU, MU, NEr, RTPr, CNCh, NCC, DbR, STF, T, H, D\},$$

де $P_1 = Tlog$, $P_2 = Nlog$, $P_3 = CPU$, $P_4 = MU$, $P_5 = NEr$, $P_6 = RTPr$, $P_7 = CNCh$, $P_8 = NCC$, $P_9 = DbR$, $P_{10} = STF$, $P_{11} = T$, $P_{12} = H$, $P_{13} = D$ – відповідно є ідентифікаторами таких параметрів як: «Час входу в систему (Tlog)» (при *j=1*), «Частота запитів на вхід у систему (Nlog)» (при *j=2*), «Завантаженість процесора (CPU)» (при *j=3*), «Завантаженість оперативної пам'яті (MU)» (при *j=4*), «Кількість збоїв та помилок (NEr)» (при *j=5*), «Час виконання процесу (RTPr)» (при *j=6*), «Завантаженість мереженого каналу (CNCh)» (при *j=7*), «Кількість одночасних підключень (NCC)» (при *j=8*), «Затримка між запитами від одного джерела (DbR)» (при *j=9*), «Розмір тимчасових файлів (STF)» (при *j=10*), «Температура в серверній кімнаті (T)» (при *j=11*), «Вологість повітря в серверній кімнаті (H)» (при *j=12*), «Концентрація пилу в серверній кімнаті (D)» (при *j=13*).

Слід зазначити, що в роботах [7, 8] використані не лише нечіткі параметри, як в даному досліджені, а й чіткі. Це збільшує кількість параметрів і теоретично підвищує достовірність результатів, однак не може бути застосовано в реальних умовах, оскільки розраховано на використанні в honeypot-системах. В реальних умовах застосування чітких параметрів навпаки призведе до зростання кількості помилок 1-го та 2-го роду за рахунок збільшення обмежень чіткої логіки та появи колізій між ними.

Підмножини $\mathbf{P_i}$, що використовуються для прогнозування чи ідентифікації i-го інциденту формуються на основі множини можливих параметрів $\mathbf{P}$ так, що $\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{P_i}\} = \{\mathbf{P_1}, \ldots, \mathbf{P_n}\}$, $\mathbf{P_i} \subseteq \mathbf{P}$, а $\mathbf{P_i} = \{\bigcup_{j=1}^{k_i} P_{ij}\} = \{P_{i1}, \ldots, P_{ik_i}\}$, де n – загальна кількість ІПКС, k_i – кількість параметрів, що пов'язані з i-м інцидентом. Таким чином $\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{P_i}\} = \{\bigcup_{i=1}^{n} \{\bigcup_{j=1}^{k_i} P_{ij}\}\} = \{\{P_{11}, \ldots, P_{1k_1}\}, \ldots, \{P_{n1}, \ldots, P_{nk_n}\}\}$ [13]. Наприклад, за умовами

дослідження при $n = 5$, $k_1 = k_3 = 6$, $k_2 = k_4 = 5$, $k_5 = 3$ визначимо необхідні параметри для виявлення відповідних ІПКС: $P_{11} = P_1$, $P_{12} = P_2$, $P_{13} = P_3$, $P_{14} = P_4$, $P_{15} = P_5$, $P_{16} = P_6$, $P_{21} = P_3$, $P_{22} = P_4$, $P_{23} = P_5$, $P_{24} = P_6$, $P_{25} = P_7$, $P_{31} = P_3$, $P_{32} = P_4$, $P_{33} = P_5$, $P_{34} = P_7$, $P_{35} = P_8$, $P_{36} = P_9$, $P_{41} = P_3$, $P_{42} = P_4$, $P_{43} = P_5$, $P_{44} = P_7$, $P_{45} = P_{10}$ і $P_{51} = P_{11}$, $P_{52} = P_{12}$, $P_{53} = P_{13}$. Тоді отримаємо:

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{3}} \mathbf{P_i}\} = \{\bigcup_{i=1}^{5}\{\bigcup_{j=1}^{k_i} P_{ij}\}\} = \{\{P_{11}, P_{12}, P_{13}, P_{14}, P_{15}, P_{16}\}, \{P_{21}, P_{22}, P_{23}, P_{24}, P_{25}\},$$

$$\{P_{31}, P_{32}, P_{33}, P_{34}, P_{35}, P_{36}\}, \{P_{41}, P_{42}, P_{43}, P_{44}, P_{45}\}, \{P_{51}, P_{52}, P_{53}\}\} =$$

$$\{\{Tlog, Nlog, CPU, MU, NEr, RTPr\}, \{CPU, MU, NEr, RTPr, CNCh\}, \{CPU,$$

$$MU, NEr, CNCh, NCC, DbR\}, \{CPU, MU, NEr, CNCh, STF\}, \{T, H, D\}\}, \quad (3)$$

де: $P_{11} = Tlog$, $P_{12} = Nlog$, $P_{13} = CPU$, $P_{14} = MU$, $P_{15} = NEr$, $P_{16} = RTPr$ – ідентифікуючі параметри для виявлення ІПКС з ідентифікатором ZL; $P_{21} = CPU$, $P_{22} = MU$, $P_{23} = NEr$, $P_{24} = RTPr$, $P_{25} = CNCh$ – відповідні параметри для виявлення ІПКС з ідентифікатором SP; $P_{31} = CPU$, $P_{32} = MU$, $P_{33} = NEr$, $P_{34} = CNCh$, $P_{35} = NCC$, $P_{36} = DbR$ – ідентифікуючі параметри для виявлення ІПКС з ідентифікатором DD; $P_{41} = CPU$, $P_{42} = MU$, $P_{43} = NEr$, $P_{44} = CNCh$, $P_{45} = STF$ – відповідні параметри для виявлення ІПКС з ідентифікатором VA; $P_{51} = T$, $P_{52} = H$, $P_{53} = D$ – ідентифікуючі параметри для виявлення ІПКС з ідентифікатором ZK.

Підмножини нечітких еталонів $\mathbf{T_i^e}$ і евристичних правил $\mathbf{ER_i}$, а також показник рівня критичності LCS_i формується за допомогою експертних методів та нечіткої логіки.

Компонент кортежу (2) $\mathbf{T_i^e}$ визначає множину еталонів $\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{T_i^e}\} = \{\mathbf{T_1^e}, \ldots, \mathbf{T_n^e}\}, (i = \overline{1,n})$, з загальної множини еталонів $\mathbf{T^e}$, $\mathbf{T_i^e} \subseteq \mathbf{T^e}$. Аналогічно до підмножини параметрів для ідентифікації конкретного ІПКС виділимо підмножину еталонів, пов'язаних з ними $\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{T_i^e}\} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\{\bigcup_{\mathbf{j=1}}^{\mathbf{k_i}} \mathbf{T_{ij}^e}\}\} = \{\{\mathbf{T_{11}^e}, \ldots, \mathbf{T_{1k_1}^e}\}, \ldots,$ $\{\mathbf{T_{n1}^e}, \ldots, \mathbf{T_{nk_n}^e}\}\}$. Підмножину $\mathbf{T_{ij}^e} \subseteq \mathbf{T_i^e}$ визначимо як: $\mathbf{T_{ij}^e} = \{\bigcup_{s=1}^{r_{ij}} \underset{\sim}{T}_{ijs}^e\} = \{\underset{\sim}{T}_{ij1}^e, \ldots, \underset{\sim}{T}_{ijr_{ij}}^e\}$, де $\underset{\sim}{T}_{ijs}^e$ $(s = \overline{1,r_{ij}})$ – еталонні нечіткі числа, а r_{ij} – кількість елементів (термів) в $\mathbf{T_{ij}^e}$. Тоді множина пов'язаних з ІПКС еталонів матиме наступний вигляд:

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{T_i^e}\} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\{\bigcup_{\mathbf{j=1}}^{\mathbf{k_i}} \mathbf{T_{ij}^e}\}\} = \{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{k_i}\{\bigcup_{s=1}^{r_{ij}} \underset{\sim}{T}_{ijs}^e\}\}\} =$$

$$\{\{\{\underset{\sim}{T}_{111}^e, \ldots, \underset{\sim}{T}_{11r_{11}}^e\}, \ldots, \{\underset{\sim}{T}_{1k_11}^e, \ldots, \underset{\sim}{T}_{1k_1r_{1k_1}}^e\}\}, \ldots, \{\{\underset{\sim}{T}_{n11}^e, \ldots, \underset{\sim}{T}_{n1r_{n1}}^e\}, \ldots, \{\underset{\sim}{T}_{nk_n1}^e, \ldots, \underset{\sim}{T}_{nk_nr_{nk_n}}^e\}\}\}. \quad (4)$$

Формалізація процедури побудови еталонів T_{ijs}^e реалізується за допомогою методу, описаного в [10], яка здійснюється в кілька кроків: 1) формування множини всіх можливих ідентифікаторів лінгвістичних оцінок (суджень) експертів $\mathbf{LE}$ та підмножини таких ідентифікаторів $\mathbf{LE_{ij}} \subseteq \mathbf{LE}$ для характеристики поточного стану j-го параметра в певному середовищі $\mathbf{LE_{ij}} = \{\bigcup_{s=1}^{r_{ij}} LE_{ijs}\} = \{LE_{ij1}, \ldots, LE_{ijr}\}$, (див. (1)

в [10]) де LE_{ijs}, $(s=\overline{1,r_{ij}})$ – ідентифікатор s-ї лінгвістичної оцінки j-го параметра; 2) формування множини ідентифікаторів інтервалів $\mathbf{N}$ і підмножини таких ідентифікаторів $\mathbf{N_{ij}} \subseteq \mathbf{N}$ відносно конкретного контрольованого параметра, що відображаються як $\mathbf{N_{ij}} = \{\bigcup_{q=1}^{r_{ij}} N_{ijq}\} = \{N_{ij1},\ \ldots,\ N_{ijr_{ij}}\}$, $(q=\overline{1,r_{ij}})$, де N_{ijq} – ідентифікатор q-го інтервалу, що використовується для формування на ньому частот зустрічання оцінок експерта по даному j-му параметру; 3) формування узагальненої таблиці оцінок, в якій фіксуються поточні твердження експертів відносно j-го параметра. В таблиці 1 сформовано f_{ijsq} – елемент емпіричних даних, який відображає частоту вживання однакових суджень експерта LE_{js} щодо стану параметра P_{ij} на інтервалі $N_{ijq} \cong [N_{ijq}^{\min}; N_{ijq}^{\max}]$, де $N_{ijq}^{\min}$ і $N_{ijq}^{\max}$ відповідно нижня і верхня межа q-го інтервалу. На її основі формується базова матриця частот $F_{ij} = \left\| f_{ijsq} \right\|$; 4) формування похідної матриці частот $F_{ij}^{'} = \left\| f_{ijsq}^{'} \right\| = (vsm_{ij} / vs_{ijq}) \left\| f_{ijsq} \right\|$, $(q,s=\overline{1,r_{ij}})$, де $VS_{ij} = \left\| vs_{ijq} \right\| = \left\| vs_{ij1},\ldots,vs_{ijr_{ij}} \right\| = \left\| \sum_{s=1}^{r_{ij}} f_{ijs1},\ldots,\sum_{s=1}^{r_{ij}} f_{ijsr_{ij}} \right\|$ – вектор суми елементів f_{ijsq} відповідних стовпців матриці частот F_{ij}, а $vsm_{ij} = \bigvee_{q=1}^{r_{ij}} vs_{ijq}$ – максимальне значення цього вектору;

Таблиця 1 – Узагальнена таблиця оцінок експертом значень параметра P_{ij}

$\mathbf{LE_{ij}}$	$\mathbf{N_{ij}}$		
	N_{ij1}	…	$N_{ijr_{ij}}$
LE_{j1}	f_{ij11}	...	$f_{ij1r_{ij}}$
...	...	...	...
$LE_{jr_{ij}}$	$f_{jr_{ij}1}$	...	$f_{ijr_jr_{ij}}$

5) розрахунок матриці функцій належності $M_{ij} = \left\| \mu_{ijsq} \right\|$, що складається з елементів обчислюваних як $m_{ijsq} = f_{ijsq}^{'} / fm_{ijs}$, $(s,q=\overline{1,r_{ij}})$, де $FM_{ij} = \left\| fm_{ijq} \right\| = \left\| fm_{ij1},\ldots,fm_{ijr_{ij}} \right\| = \left\| \bigvee_{s=1}^{r_{ij}} f_{ijs1}^{'},\ldots,\bigvee_{s=1}^{r_{ij}} f_{ijsr_{ij}}^{'} \right\|$ – вектор максимумів елементів кожного стовпця (інтервалу).

Результати обчислень дають змогу сформувати нечіткі терми еталонів $\underset{\sim}{T}_{ijs}$ використовуючи вираз $\underset{\sim}{T}_{ijs} = \{\bigcup_{q=1}^{r_{ij}} \mu_{ijsq} / x_{ijsq}\} = \{\mu_{ijs1} / x_{ijs1},\ \ldots,\ \mu_{ijsr_{ij}} / x_{ijsr_{ij}}\}$, $(q=\overline{1,r_{ij}})$, де $x_{ijsq} = N_{ijq}^{\max} / N_{ijr_{ij}}^{\max}$ (див. (9) в [10]).

Наприклад, при $i=1$ для ІПКС $\mathbf{IKS_1} = \mathbf{ZL}$, з ідентифікаторами $IKS_1 = ZL$ («проникнення порушника в ІКСМ (злом)») $j=4$ та $r_{14}=3$ для параметра $P_{14} = MU$ «Завантаженість оперативної пам'яті» введемо підмножину ідентифікаторів лінгвістичних оцінок $\mathbf{LE_{14}} = \{\bigcup_{s=1}^{3} LE_{14s}\} = \{LE_{141},\ LE_{142},\ LE_{143}\} = \{LE_{1MU1},\ LE_{1MU2},\ LE_{1MU3}\} = \{H,\ C,\ B\}$, де Н – низька, С – середня, В – висока. Враховуючи, що в нормальних

умовах середньої експлуатації потужностей персональних комп'ютерів і при відсутності впливу шкідливого програмного забезпечення середній показник завантаженості оперативної пам'яті становить 10-20% в стані спокою та 20-40% під час активного виконання операцій на робочій станції, а більші показники свідчать про не нормальну роботу, що дуже ймовірно може бути спричинено вірусною, спам- та DDOs-атаками чи діяльністю зломщика. Звичайно норма може дещо варіюватися, залежно від операційної системи, встановленого програмного забезпечення і виробничих завдань організації. Виходячи з цього задамо підмножину інтервалів $\mathbf{N_{14}} = \{\bigcup_{q=1}^{3} N_{14q}\} = \{N_{141},\ N_{142},\ N_{143}\} = \{N_{1MU1},\ N_{1MU2},\ N_{1MU3}\} = \{[0;20[,\ [20;50[,\ [50;100]\}$. На основі отриманих значень сформуємо узагальнену таблицю експертних оцінок (див. табл. 2).

Таблиця 2 – Узагальнена таблиця експертних оцінок параметра P_{14}

$\mathbf{LE_{14}}$	$\mathbf{N_{14}}$		
	[0;20[	[20;50[	[50;100[
Низька	8	1	0
Середня	3	9	1
Висока	0	2	9

На основі даних таблиці побудуємо базову матрицю:

$$F_{14} = \left\| f_{i4sq} \right\| = \left\| \begin{matrix} 8 & 1 & 0 \\ 3 & 9 & 1 \\ 0 & 2 & 9 \end{matrix} \right\|, \quad (s,q = \overline{1,3})$$

а також, відповідно, вектор сум та максимальний елемент будуть: $VS_{14} = \left\| vs_{141}, vs_{142}, vs_{143} \right\| = \left\| vs_{1MU1}, vs_{1MU2}, vs_{1MU3} \right\| = \left\| 11;\ \ 12;\ \ 10 \right\|$ і $vsm_{14} = \bigvee_{q=1}^{3} vs_{14q} = 12$. Обрахуємо похідну матрицю частот:

$$F_{14}^{'} = (vsm_{14} / vs_{14q}) F_{14} = \left\| \begin{matrix} 8{,}72 & 1 & 0 \\ 3{,}27 & 9 & 1{,}2 \\ 0 & 2 & 10{,}8 \end{matrix} \right\|$$

та вектор максимумів $FM_{14} = \left\| fm_{141}, fm_{142}, fm_{143} \right\| = \left\| 8{,}72;\ \ 9;\ \ 10{,}8 \right\|$.

Провівши необхідні обчислення знайдемо супорти $x_{1411} = x_{1421} = x_{1431} = 20/100 = 0{,}2$, $x_{1412} = x_{1422} = x_{1432} = 50/100 = 0{,}5$, $x_{1413} = x_{1423} = x_{1433} = 100/100 = 1$ та матрицю функцій належності

$$M_{ij} = \left\| \mu_{ijsq} \right\| = \left\| \begin{matrix} 1 & 0{,}11 & 0 \\ 0{,}38 & 1 & 0{,}11 \\ 0 & 0{,}22 & 1 \end{matrix} \right\|.$$

Таким чином, на основі нечітких термів $\underset{\sim}{T}_{ijs}$ еталон параметра $P_{14} = MU$ матиме вигляд $\underset{\sim}{T}^{e}_{14s} = \{\bigcup_{s=1}^{3} \underset{\sim}{T}^{e}_{14s}\} = \{\underset{\sim}{T}^{e}_{141},\ \underset{\sim}{T}^{e}_{142},\ \underset{\sim}{T}^{e}_{143}\} = \{\underset{\sim}{H},\ \underset{\sim}{C},\ \underset{\sim}{B}\}$ і терми лінгвістичних змін (ЛЗ) для цього параметра: $\underset{\sim}{T}^{e}_{141} = \underset{\sim}{T}^{e}_{1MU1} = \underset{\sim}{H}_{14} = \{\bigcup_{q=1}^{3} \mu^{e}_{141q} / x^{e}_{141q}\} = \{0/0{,}2;\ 1/0{,}2;\ 0{,}11/0{,}5;\ 0/1\}$, $\underset{\sim}{T}^{e}_{142} = \underset{\sim}{T}^{e}_{1MU2} = \underset{\sim}{C}_{14} = \{\bigcup_{q=1}^{3} \mu^{e}_{142q} / x^{e}_{142q}\} = \{0/0{,}2;\ 0{,}38/0{,}2;\ 1/0{,}5;\ 0{,}11/1;\ 0/1\}$, $\underset{\sim}{T}^{e}_{143} = \underset{\sim}{T}^{e}_{1MU3} = \underset{\sim}{B}_{14} = \{\bigcup_{q=1}^{3} \mu^{e}_{143q} / x^{e}_{143q}\} = \{0/0{,}2;$

$0,22/0,5;\ 1/1;\ 0/1\}$, де $\underset{\sim}{H}_{14}$ – низька, $\underset{\sim}{C}_{14}$ – середня, $\underset{\sim}{B}_{14}$ – висока. Графік функції належності термів ЛЗ «Завантаженість оперативної пам'яті» показаний на рис. 1.

Виходячи з цього, наприклад, при $n=5$ для ІПКС ($\mathbf{ІКS_1 = ZL}$, $\mathbf{ІКS_2 = SP}$, $\mathbf{ІКS_3 = DD}$, $\mathbf{ІКS_4 = VA}$, $\mathbf{ІКS_5 = ZK}$) з ідентифікаторами $IKS_1 = ZL$, $IKS_2 = SP$, $IKS_3 = DD$, $IKS_4 = VA$, $IKS_5 = ZK$ та $k_1 = k_3 = 6$, $k_2 = k_4 = 5$, $k_5 = 3$, $r_{1j} = r_{2j} = r_{3j} = r_{4j} = 3$ і $r_{5j} = 5$ вираз (4) описуватиме множину еталонів наступним чином:

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{5}} \mathbf{T_i^e}\} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{5}} \{\bigcup_{\mathbf{j=1}}^{\mathbf{k_i}} \mathbf{T_{ij}^e}\}\} = \{\bigcup_{i=1}^{5} \{\bigcup_{j=1}^{k_i} \{\bigcup_{s=1}^{r_{ij}} \underset{\sim}{T}_{ijs}^e\}\}\} = \{\{\{\underset{\sim}{T}_{111}^e, ..., \underset{\sim}{T}_{11r_{11}}^e\}, ..., \{\underset{\sim}{T}_{1k_11}^e, ..., \underset{\sim}{T}_{1k_1r_{16}}^e\}\}, \{\{\underset{\sim}{T}_{211}^e, ..., \underset{\sim}{T}_{21r_{21}}^e\}, ..., \{\underset{\sim}{T}_{2k_21}^e, ..., \underset{\sim}{T}_{2k_2r_{25}}^e\}\}, \{\{\underset{\sim}{T}_{311}^e, ..., \underset{\sim}{T}_{31r_{31}}^e\}, ..., \{\underset{\sim}{T}_{3k_31}^e, ..., \underset{\sim}{T}_{3k_3r_{36}}^e\}\}, \{\{\underset{\sim}{T}_{411}^e, ..., \underset{\sim}{T}_{41r_{41}}^e\}, ..., \{\underset{\sim}{T}_{4k_41}^e, ..., \underset{\sim}{T}_{4k_4r_{45}}^e\}\}, \{\{\underset{\sim}{T}_{511}^e, ..., \underset{\sim}{T}_{51r_{51}}^e\}, ..., \{\underset{\sim}{T}_{5k_51}^e, ..., \underset{\sim}{T}_{5k_5r_{53}}^e\}\}\} =$$

$$= \{\{\{\underset{\sim}{T}_{111}^e, \underset{\sim}{T}_{112}^e, \underset{\sim}{T}_{113}^e\}, ..., \{\underset{\sim}{T}_{161}^e, \underset{\sim}{T}_{162}^e, \underset{\sim}{T}_{163}^e\}\}, \{\{\underset{\sim}{T}_{211}^e, \underset{\sim}{T}_{212}^e, \underset{\sim}{T}_{213}^e\}, ..., \{\underset{\sim}{T}_{251}^e, \underset{\sim}{T}_{252}^e, \underset{\sim}{T}_{253}^e\}\}, \{\{\underset{\sim}{T}_{311}^e, \underset{\sim}{T}_{312}^e, \underset{\sim}{T}_{313}^e\}, ..., \{\underset{\sim}{T}_{361}^e, \underset{\sim}{T}_{362}^e, \underset{\sim}{T}_{363}^e\}\}, \{\{\underset{\sim}{T}_{411}^e, \underset{\sim}{T}_{412}^e, \underset{\sim}{T}_{413}^e\}, ..., \{\underset{\sim}{T}_{461}^e, \underset{\sim}{T}_{462}^e, \underset{\sim}{T}_{463}^e\}\}, \{\{\underset{\sim}{T}_{511}^e, \underset{\sim}{T}_{512}^e, \underset{\sim}{T}_{513}^e, \underset{\sim}{T}_{514}^e, \underset{\sim}{T}_{515}^e\}, ..., \{\underset{\sim}{T}_{531}^e, \underset{\sim}{T}_{532}^e, \underset{\sim}{T}_{533}^e, \underset{\sim}{T}_{534}^e, \underset{\sim}{T}_{535}^e\}\}\} =$$

$$= \{\{\{\underset{\sim}{H}_{11}, \underset{\sim}{C}_{11}, \underset{\sim}{B}_{11}\}, ..., \{\underset{\sim}{H}_{16}, \underset{\sim}{C}_{16}, \underset{\sim}{B}_{16}\}\}, \{\{\underset{\sim}{H}_{21}, \underset{\sim}{C}_{21}, \underset{\sim}{B}_{21}\}, ..., \{\underset{\sim}{H}_{25}, \underset{\sim}{C}_{25}, \underset{\sim}{B}_{25}\}\}, \{\{\underset{\sim}{H}_{31}, \underset{\sim}{C}_{31}, \underset{\sim}{B}_{31}\}, ..., \{\underset{\sim}{H}_{36}, \underset{\sim}{C}_{36}, \underset{\sim}{B}_{36}\}\}, \{\{\underset{\sim}{H}_{41}, \underset{\sim}{C}_{41}, \underset{\sim}{B}_{41}\}, ..., \{\underset{\sim}{H}_{45}, \underset{\sim}{C}_{45}, \underset{\sim}{B}_{45}\}\}, \{\{\underset{\sim}{H}_{51}, \underset{\sim}{HC}_{51}, \underset{\sim}{C}_{51}, \underset{\sim}{BC}_{51}, \underset{\sim}{B}_{51}\}, ..., \{\underset{\sim}{H}_{53}, \underset{\sim}{HC}_{53}, \underset{\sim}{C}_{53}, \underset{\sim}{BC}_{55}, \underset{\sim}{B}_{53}\}\}\} =$$

$$= \{\{\{\underset{\sim}{T}_{ZLTlog1}^e, \underset{\sim}{T}_{ZLTlog2}^e, \underset{\sim}{T}_{ZLTlog3}^e\}, ..., \{\underset{\sim}{T}_{ZLRTPr1}^e, \underset{\sim}{T}_{ZLRTPr2}^e, \underset{\sim}{T}_{ZLRTPr3}^e\}\}, \{\{\underset{\sim}{T}_{SPCPU1}^e, \underset{\sim}{T}_{SPCPU2}^e, \underset{\sim}{T}_{SPCPU3}^e\}, ..., \{\underset{\sim}{T}_{SPCNCh1}^e, \underset{\sim}{T}_{SPCNCh2}^e, \underset{\sim}{T}_{SPCNCh3}^e\}\}, \{\{\underset{\sim}{T}_{DDCPU1}^e, \underset{\sim}{T}_{DDCPU2}^e, \underset{\sim}{T}_{DDCPU3}^e\}, ..., \{\underset{\sim}{T}_{DDDbR1}^e, \underset{\sim}{T}_{DDDbR2}^e, \underset{\sim}{T}_{DDDbR3}^e\}\}, \{\{\underset{\sim}{T}_{VACPU1}^e, \underset{\sim}{T}_{VACPU2}^e, \underset{\sim}{T}_{VACPU3}^e\}, ..., \{\underset{\sim}{T}_{VASTF1}^e, \underset{\sim}{T}_{VASTF2}^e, \underset{\sim}{T}_{VASTF3}^e\}\}, \{\{\underset{\sim}{T}_{ZKT1}^e, \underset{\sim}{T}_{ZKT2}^e, \underset{\sim}{T}_{ZKT3}^e, \underset{\sim}{T}_{ZKT4}^e, \underset{\sim}{T}_{ZKT5}^e\}, ..., \{\underset{\sim}{T}_{ZKD1}^e, \underset{\sim}{T}_{ZKD2}^e, \underset{\sim}{T}_{ZKD3}^e, \underset{\sim}{T}_{ZKD4}^e, \underset{\sim}{T}_{ZKD5}^e\}\}\} =$$

$$\{\{\{\underset{\sim}{H}_{ZLTlog}, \underset{\sim}{C}_{ZLTlog}, \underset{\sim}{B}_{ZLTlog}\}, ..., \{\underset{\sim}{H}_{ZLRTPr}, \underset{\sim}{C}_{ZLRTPr}, \underset{\sim}{B}_{ZLRTPr}\}\}, \{\{\underset{\sim}{H}_{SPCPU}, \underset{\sim}{C}_{SPCPU}, \underset{\sim}{B}_{SPCPU}\}, ..., \{\underset{\sim}{H}_{SPCNCh}, \underset{\sim}{C}_{SPCNCh}, \underset{\sim}{B}_{SPCNCh}\}\}, \{\{\underset{\sim}{H}_{DDCPU}, \underset{\sim}{C}_{DDCPU}, \underset{\sim}{B}_{DDCPU}\}, ..., \{\underset{\sim}{H}_{DDDbR}, \underset{\sim}{C}_{DDDbR}, \underset{\sim}{B}_{DDDbR}\}\}, \{\{\underset{\sim}{H}_{VACPU}, \underset{\sim}{C}_{VACPU}, \underset{\sim}{B}_{VACPU}\}, ..., \{\underset{\sim}{H}_{VASTF}, \underset{\sim}{C}_{VASTF}, \underset{\sim}{B}_{VASTF}\}\}, \{\{\underset{\sim}{H}_{ZKT}, \underset{\sim}{HC}_{ZKT}, \underset{\sim}{C}_{ZKT}, \underset{\sim}{BC}_{ZKT}, \underset{\sim}{B}_{ZKT}\}, ..., \{\underset{\sim}{H}_{ZKD}, \underset{\sim}{HC}_{ZKD}, \underset{\sim}{C}_{ZKD}, \underset{\sim}{BC}_{ZKD}, \underset{\sim}{B}_{ZKD}\}\}\},$$

де, наприклад, $\underset{\sim}{T}_{111}^e = \underset{\sim}{H}_{11} = \underset{\sim}{T}_{Tlog1}^e = \underset{\sim}{H}_{Tlog}$ – компоненти еталонів (терми), що описують відповідні ідентифікуючі параметри і дають змогу ідентифікувати задані ІПКС.

Підмножина $\underset{\sim}{\mathbf{P}}_\mathbf{i}$ формується на основі даних, що зняті з датчиків контролю відповідних кожному інциденту параметрів середовища за певний період часу з заданим інтервалом, тобто $\underset{\sim}{\mathbf{P}}_\mathbf{i} = \{\bigcup_{j=1}^{k_i} P_{ij}\} = \{\underset{\sim}{P}_{11}, ..., \underset{\sim}{P}_{nk_n}\}$, де $\underset{\sim}{\mathbf{P}}_\mathbf{i} \subseteq \underset{\sim}{\mathbf{P}}$, $(i = \overline{1,n},\ j = \overline{1,k_i})$. Наприклад, при $n=5$, $i = \overline{1,5}$ для ІПКС ($\mathbf{ІКS_1 = ZL}$, $\mathbf{ІКS_2 = SP}$, $\mathbf{ІКS_3 = DD}$, $\mathbf{ІКS_4 = VA}$, $\mathbf{ІКS_5 = ZK}$), $k_1 = k_3 = 6$, $k_2 = k_4 = 5$, $k_5 = 3$ ця підмножина може бути визначена як: $\underset{\sim}{\mathbf{P}}_\mathbf{1} = \{\bigcup_{j=1}^{6} P_{1j}\} = \{\underset{\sim}{P}_{11}, \underset{\sim}{P}_{12}, \underset{\sim}{P}_{13}, \underset{\sim}{P}_{14}, \underset{\sim}{P}_{15}, \underset{\sim}{P}_{16}\} = \{\underset{\sim}{Tlog}, \underset{\sim}{Nlog}, \underset{\sim}{CPU}, \underset{\sim}{MU}, \underset{\sim}{NEr}, \underset{\sim}{RTPr}\}$, при $i=1$, $k_1 = 6$; $\underset{\sim}{\mathbf{P}}_\mathbf{2} = \{\bigcup_{j=1}^{5} P_{2j}\} = \{\underset{\sim}{P}_{21}, \underset{\sim}{P}_{22}, \underset{\sim}{P}_{23}, \underset{\sim}{P}_{24}, \underset{\sim}{P}_{25}\} = \{\underset{\sim}{CPU}, \underset{\sim}{MU}, \underset{\sim}{NEr}, \underset{\sim}{RTPr}, \underset{\sim}{CNCh}\}$, при $i=2$, $k_2 = 5$; $\underset{\sim}{\mathbf{P}}_\mathbf{3} = \{\bigcup_{j=1}^{6} P_{3j}\} = \{\underset{\sim}{P}_{31}, \underset{\sim}{P}_{32}, \underset{\sim}{P}_{33}, \underset{\sim}{P}_{34}, \underset{\sim}{P}_{35}, \underset{\sim}{P}_{36}\} =$

$\{\underset{\sim}{CPU},\ \underset{\sim}{MU},\ \underset{\sim}{NEr},\ \underset{\sim}{CNCh},\ \underset{\sim}{NCC},\ \underset{\sim}{DbR}\}$, при $i=3,\ k_3=6$; $\underset{\sim}{\mathbf{P_4}}=\{\bigcup_{j=1}^{5}P_{4j}\}=\{\underset{\sim}{P_{41}},\ \underset{\sim}{P_{42}},\ \underset{\sim}{P_{43}},\ \underset{\sim}{P_{44}},\ \underset{\sim}{P_{45}}\}=\{\underset{\sim}{CPU},\ \underset{\sim}{MU},\ \underset{\sim}{NEr},\ \underset{\sim}{CNCh},\ \underset{\sim}{STF}\}$, при $i=4,\ k_4=5$; $\underset{\sim}{\mathbf{P_5}}=\{\bigcup_{j=1}^{3}P_{5j}\}=\{\underset{\sim}{P_{51}},\ \underset{\sim}{P_{52}},\ \underset{\sim}{P_{53}}\}=\{\underset{\sim}{T},\ \underset{\sim}{H},\ \underset{\sim}{D}\}$, при $i=5,\ k_6=3$.

Встановлено, що поточні значення j-х параметрів з кожного набору $\underset{\sim}{\mathbf{P_i}}$ характеризують ситуацію контрольованого середовища в певний момент часу і формують ідентифікатор поточного стану LC через їх співвідношення з еталонними значеннями відповідних параметрів відносно i-го ІПКС. Таким чином $LC=\underset{j=1}{\overset{k_i}{\wedge}}t_j=\underset{j=1}{\overset{k_i}{\wedge}}(\underset{\sim}{P_{ij}}\cong\underset{s=1}{\overset{r_{ij}}{\vee}}T_{js}^{e})$, де k_i – кількість параметрів, що ідентифікують i-й інцидент, а r_{ij} – кількість термів у відповідних еталонах. Для кожного ІПКС і правила формується унікальний ідентифікатор стану LC. Зазначимо, що кожному ER_{ip} відповідає евристичний вираз (правило), тобто: $\mathbf{ER}=\{\bigcup_{i=1}^{n}\{\bigcup_{p=1}^{P_i}ER_{ip}\}\}=\{\bigcup_{i=1}^{n}\{\bigcup_{p=1}^{P_i}(LC_{ip}\rightarrow LI_{ip})\}\}=\{\bigcup_{i=1}^{n}\{\bigcup_{p=1}^{P_i}ER_{ip}=(LC_{ip}\rightarrow LI_{ip})\}\}$, де ER_{ip} – p-те правило для виявлення та ідентифікації i-го ІПКС, яке буквально інтерпретується як: «Якщо LC_{ip} істинно, то імовірність настання ІПКС буде LI_{ip}», а LI_{ip} – один з елементів множини лінгвістичних ідентифікаторів ймовірності реалізації ІПКС, необхідних для відображення судження експерта в лінгвістичній формі, $\mathbf{LI}=\{\bigcup_{d=1}^{D}LI_d\}=\{LI_1,...,LI_D\}$.

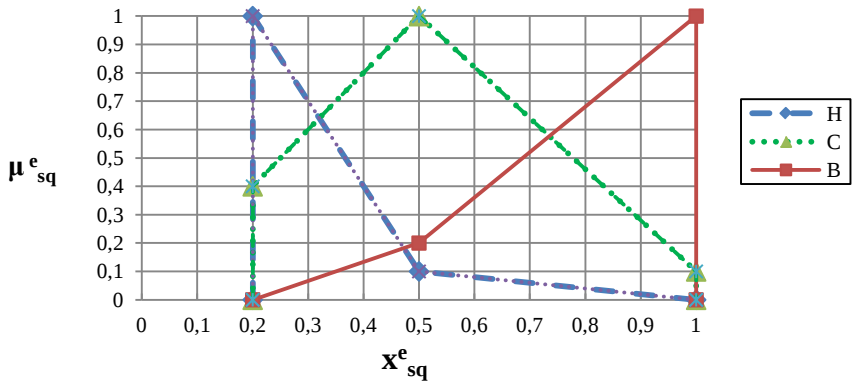

Рисунок 1 – Лінгвістичні терми еталонів нечітких чисел для MU

Побудова правил зазвичай здійснюється на основі експертного підходу, особливо це важливо в тих випадках, коли необхідно дати перевагу одній з альтернатив, наприклад, при якому LC_{ip} результат, пов'язаний з LI_{ip} буде найбільш об'єктивно відображати стан системи. Виходячи з цих позицій формуються набори правил. Так, правило ER_{41} [11] буде мати вигляд: $ER_{41}=\{(\underset{\sim}{P_{VACPU}}\cong H,\ \underset{\sim}{P_{VAMU}}\cong H,\ \underset{\sim}{P_{VANEr}}\cong M,\ \underset{\sim}{P_{VACNCh}}\cong H,\ \underset{\sim}{P_{VASTF}}\cong M)\rightarrow H\}$, що словесно можна інтерпретувати таким чином: «Якщо поточні значення $\underset{\sim}{P_{VACPU}}$, $\underset{\sim}{P_{VAMU}}$, $\underset{\sim}{P_{VANEr}}$, $\underset{\sim}{P_{VACNCh}}$, $\underset{\sim}{P_{VASTF}}$ найбільш близько розташовані до значень $\underset{\sim}{H_{VACPU}}$, $\underset{\sim}{H_{VAMU}}$, $\underset{\sim}{M_{VANEr}}$, $\underset{\sim}{H_{VACNCh}}$, $\underset{\sim}{M_{VASTF}}$ відповідно, що входять до $\underset{\sim}{T}^{e}_{VACPU}$, $\underset{\sim}{T}^{e}_{VACNCh}$, $\underset{\sim}{T}^{e}_{VASTF}$, $\underset{\sim}{T}^{e}_{VAMU}$, $\underset{\sim}{T}^{e}_{VANEr}$, то рівень можливості виникнення ІПКС в даний момент буде НИЗЬКИЙ».

ISSN 2074-9481
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 1 (29), 2015 р.

Кожен інцидент характеризується рівнем критичності, що задається множиною $\mathbf{LCS} = \{\bigcup_{i=1}^{n} LCS_i\} = \{LCS_1,..,LCS_n\}$, $(i = \overline{1,n})$. Рівень критичності визначається через параметри оцінки критичності ситуації з врахуванням їх вагових коефіцієнтів, тобто $\underset{\sim}{LCS}_i = \sum_{e=1}^{E} (\Omega_e * \underset{\sim}{L}_e)$. Встановлено, що рівень критичності можна описати врахувавши функціональні залежності між $\underset{\sim}{L}_e$ – параметрами оцінки рівня критичності. Детально метод оцінювання рівня критичності та множина оціночних параметрів описані в роботі [12].

Сформувавши всі компоненти кортежу (2) наведемо модель представлення ІПКС «Вірусна атака». Отже, при $i = 4$ для ІПКС ($\mathbf{IKS_4 = VA}$) з ідентифікатором $IKS_4 = VA$ та $k_4 = 5$, $r_{4j} = 3$ і $P_4 = 243$ інтегрована модель матиме такий вигляд:

$$\mathbf{IKS_4} = < IKS_4, \mathbf{P_4}, \mathbf{T_4^e}, \underset{\sim}{\mathbf{P}}_{\mathbf{4}}, \mathbf{ER_4}, LCS_4 > =$$

$$< VA, \{P_{41}, P_{42}, P_{43}, P_{44}, P_{45}\}, \{\underset{\sim}{T}^e_{41}, \underset{\sim}{T}^e_{42}, \underset{\sim}{T}^e_{43}, \underset{\sim}{T}^e_{44}, \underset{\sim}{T}^e_{45}\},$$

$$\{\underset{\sim}{P}_{41}, \underset{\sim}{P}_{42}, \underset{\sim}{P}_{43}, \underset{\sim}{P}_{44}, \underset{\sim}{P}_{45}\}, \{ER_{41},...,ER_{4243}\}, LCS_4 > =$$

$$< VA, \{CPU, MU, NEr, RTPr, CNCh, STF\}, \{\underset{\sim}{T}^e_{VACPU}, \underset{\sim}{T}^e_{VACNCh}, \underset{\sim}{T}^e_{VASTF}, \underset{\sim}{T}^e_{VAMU}, \underset{\sim}{T}^e_{VANEr}\},$$

$$\{\underset{\sim}{CPU}, \underset{\sim}{MU}, \underset{\sim}{NEr}, \underset{\sim}{RTPr}, \underset{\sim}{CNCh}, \underset{\sim}{STF}\}, \{ER_{41},...,ER_{4243}\}, LCS_{VA} > . \quad (5)$$

Дана модель дозволяє відобразити ІПКС, оперуючи ідентифікуючими параметрами та характерними ознаками з використанням елементів нечіткої логіки та експертних підходів. Слід відмітити універсальність даної моделі.

V Висновки

Побудована інтегрована модель представлення ІПКС та описаний кортеж, який її визначає. Основними компонентами кортежу є ідентифікатор ІПКС, набори параметрів для виявлення ІПКС, набори нечітких еталонних чисел та поточних значень контрольованих параметрів, набори правил та рівень критичності ситуації, спричиненої ІПКС. Отримані результати є базисом для побудови методу і системи виявлення та оцінки КС. Розроблена інтегрована модель представлення ІПКС, що за рахунок узагальнення оціночних та ідентифікуючих параметрів, відображених шестикомпонентним кортежем, в поєднанні з елементами нечіткої логіки та експертних підходів дозволяє будувати більш гнучкі та ефективні методи виявлення та оцінки КС, враховуючих можливість формування необхідних множин наборів параметрів та використання в умовах слабоформалізованого середовища. Проведена формалізація процедури побудови еталонів параметрів, що дає змогу застосовувати їх в умовах невизначеності і слабоформалізованого середовища для виявлення ІПКС різного роду, тобто забезпечення універсальності, та їх оцінки. Сформовані еталони необхідні для формування логічних правил, що дозволяють забезпечити належне функціонування системи виявлення і оцінки кризових ситуацій.

Список використаної літератури: ***1.*** *Корченко А. Г. Интегрированное представление параметров риска / Корченко А. Г., Иванченко Е. В., Казмирчук С. В. // Защита информации – 2011. – №1 (50). – С. 96-101.* ***2.*** *Корченко А. Г. Системы анализа и оценивания рисков информационной безопасности / А. Г. Корченко, А. Е. Архипов, С. В. Казмирчук. – К. : Palmarium Academic Publishing, 2013. – 316 с.* ***3.*** *Корченко О.Г. Построение систем защиты информации на нечетких множествах [Текст]: Теория и практические решения / О. Г. Корченко. – К. : МК-Пресс, 2006. – 320 с.* ***4.*** *Корченко А. Метод виявлення та ідентифікації порушника в інформаційно-комунікаційних системах / А. Корченко, А. Гізун, В. Волянська, С. Гнатюк // Захист інформації. – 2013. – Т.15. – №4. – С. 387-393.* ***5.*** *Корченко А. О. Система виявлення та ідентифікації порушника в інформаційно-комунікаційних мережах / А. О. Корченко, В. В. Волянська, А. І. Гізун // Безпека інформації. – 2013. – Т.19. – №3. – С. 158-162.* ***6.*** *Корченко А. А. Система выявления аномального*

состояния в компьютерных сетях / А. А. Корченко // Безпека інформації. – 2012. – № 2 (18). – С. 80-84. ***7.*** *Параметры прогнозирования и идентификации атак в информационно-комуникационных системах / В. Азарсков, А. Гизун, А. Грехов, С. Скворцов // Захист інформації. – 2014. – Том 16. – №1. – С. 89-95.* ***8.*** *Гізун А. І. Основні параметри для ідентифікації порушника інформаційної безпеки / А.І. Гізун, В. В. Волянська, В. О. Риндюк, С. О. Гнатюк // Захист інформації. – 2013. – №1 (58). – С.66-75.* ***9.*** *Стасюк А. И. Базовая модель параметров для построения систем выявления атак / А. И. Стасюк, А. А. Корченко // Захист інформації. – 2012. – № 2 (55). – С. 47-51.* ***10.*** *Корченко А. А. Метод формирования лингвистических эталонов для систем выявления вторжений / А. А. Корченко // Захист інформації. – Т.16, №1. – 2014. – С. 5-12.* ***11.*** *Гізун А. І. Формалізована модель побудови евристичних правил для виявлення інцидентів // А. І. Гізун, В. О. Гнатюк, О. М. Супрун / Вісник Інженерної академії України. – 2015. – №1. – С. 110-115.* ***12.*** *Корченко А.О. Метод оцінки рівня критичності для систем управління кризовими ситуаціями // А. О. Корченко, В. А. Козачок, А. І. Гізун // Захист інформації. – 2015.– Т.17. – №1. – С. 86-98.* ***13.*** *Корченко А. О. Кортежная модель формирования набора базовых компонент для выявления кибератак / А. А. Корченко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2014. – В.2 (28). – С. 29-36.*

Сергій Гончар, Геннадій Леоненко, Олексій Юдін
ДержНДІ Спецзв'язку

УДК 004.056.5

ЗАГАЛЬНА МОДЕЛЬ ЗАГРОЗ БЕЗПЕЦІ ІНФОРМАЦІЇ АСУ ТП

Анотація: **Запропонована загальна модель загроз безпеці інформації в автоматизованих системах управління технологічними процесами об'єктів критичної інфраструктури, яка враховує технічний та соціокультурний компоненти системи захисту інформації.**
Summary: **Offered general model of information security threats in industrial control systems of critical information objects, which takes into account technical and sociocultural components of information protection system.**
Ключові слова: **АСУ ТП, критична інфраструктура, захист інформації, соціокультурний компонент, модель загроз.**

І Вступ

Сьогодні практично всі держави світу залежать від автоматизації виробничих процесів, а саме, від безперебійної роботи автоматизованих систем управління технологічними процесами (АСУ ТП). Найбільш значущими АСУ ТП є ті, що забезпечують роботу об'єктів критичної інфраструктури (ОКІ). Під ОКІ будемо розуміти атомні і гідроелектростанції, нафто- і газопроводи, національні мережі розподілу електроенергії, транспортні системи національного і світового рівня, загальнодержавні системи зв'язку, галузеутворюючі підприємства тощо [1]. Таким чином, від ступеню захищеності АСУ ТП ОКІ залежить не тільки прибуток крупних компаній (корпорацій), але й національна або регіональна безпека [2]. Викладене вище робить актуальною задачею розробку та впровадження систем захисту ОКІ, в тому числі і АСУ ТП. Термін «система захисту інформації ОКІ» визначимо як взаємопов'язану сукупність організаційних, нормативно-правових, науково-методичних та технічних заходів, засобів і методів захисту інформації, спрямованих на унеможливлення витоку, знищення, блокування, порушення цілісності та режиму доступу до інформації [3].

У класичній інфраструктурі інформаційних технологій вже давно існує множина способів і методів забезпечення захисту інформації. Натомість організаційно-технічні рішення щодо захисту АСУ ТП ОКІ повинні бути суттєво змінені з урахуванням специфіки виробничих процесів підприємств. Внаслідок цього, для ряду завдань, наприклад, таких, які потребують прийняття рішення у режимі реального часу, часто необхідно не просто доопрацювання засобів захисту, а їх розробка з нуля з урахуванням додаткових вимог.

З урахуванням викладеного здійснимо декомпозицію системи захисту АСУ ТП ОКІ на складові частини. Так, на нашу думку, система захисту складається з:

- нормативно-правової бази;
- науково-методичної бази;
- організаційно-технічних і режимних заходів;
- персоналу забезпечення.

При цьому персонал забезпечення, який виділений в окрему складову системи захисту, може бути і джерелом загроз [4]. Так, результати аналізу джерел порушень безпеки в інформаційних системах [5] свідчать, що близько 70 відсотків порушень відбуваються через персонал забезпечення, рис. 1.