Охрімчук Володимир Васильович, науковий співробітник науково-дослідної лабораторії проблем забезпечення кібернетичної безпеки наукового центру Житомирського військового інституту імені С. П Корольова.
E-mail: Okhrimchuk84@ukr.net

Охримчук Владимир Васильевич, научный сотрудник научно-исследовательской лаборатории проблем кибернетической безопасности научного центра Житомирского военного института имени С. П Королёва.
Vladimir Okhrimchuk, research scientist of scientific research laboratory issues of cybersecurity of scientific center of Zhytomyr military institute after S. P. Korolyov.

УДК 004.056.53:004.492.3 (045)

МЕТОД ОЦІНКИ РІВНЯ КРИТИЧНОСТІ ДЛЯ СИСТЕМ УПРАВЛІННЯ КРИЗОВИМИ СИТУАЦІЯМИ

Анна Корченко, Валерій Козачок, Андрій Гізун

Вплив кризових ситуацій на стан захищеності державних інформаційних ресурсів, різноманітних установ, підприємств, організацій та державу в цілому є досить значним. Так, кризові ситуації здатні не лише загальмувати розвиток системи, що підпадає під її вплив, а й зруйнувати її взагалі. Для запобігання такого впливу необхідним є прийняття адекватних рівню загрози заходів та застосування засобів захисту, що визначає важливість оцінки критичності поточної ситуації. На даний час не існує загальноприйнятих універсальних критеріїв та інтегрованого показника оцінки рівня критичності. Тому визначення рівня критичності інциденту, що може спричиняти КС, є актуальною та важливою науковою задачею. В дослідженні введена множина параметрів оцінки рівня критичності ситуації, запропонований метод визначення рівня критичності з використання експертних підходів та методів нечіткої логіки, які не вимагають збирання та обробку статистичних даних, та описана процедура дефазифікації значення параметрів, на основі якої будується індикатор відображення рівня критичності.

Ключові слова: *кризова ситуація, інцидент, рівень критичності кризової ситуації, індикатор, множина критеріїв, оцінка рівня критичності, збитки, клас критичності, експертні методи, теорія нечітких множин.*

Захист державних інформаційних ресурсів (ДІР) від впливу кризових ситуацій (КС) та їх наслідків на даний час є чи не найбільш актуальною задачею у всій сфері інформаційної безпеки. Будь-які інциденти інформаційної безпеки мають свої причини, тобто дестабілізуючі чинники, що їх спричиняють і завжди створюють негативний вплив на процеси управління інформаційними ресурсами організації чи ДІР. Так, чисельні інциденти за умови відсутності контролю за їх протіканням та відповідної реакції можуть мати критичні наслідки. Відповідно до визначення КС, наведеного в [1], вона характеризується великими збитками, серйозними перериванням бізнес-процесів, що ставлять під сумнів можливість подальшого функціонування організації, руйнуванням структури окремого підприємства чи цілої галузі, потенційними загрозами життю та здоров'ю людей. Таким чином КС не тільки може порушити характеристики безпеки ДІР (конфіденційність, цілісність та доступність), а й порушити процеси управління ними, призвести до їх втрати. При цьому чим більший рівень критичності КС, тим тяжчі наслідки вона може мати і, зрозуміло, більш ефективними мають бути антикризові засоби та заходи. Тому для прийняття ефективних контрзаходів, максимальної ліквідації наслідків необхідним є визначення рівня критичності КС, породженої інцидентом-потенційною кризовою ситуацією (ІПКС), враховуючи динаміку її розвитку.

Процеси захисту інформаційних ресурсів в умовах впливу КС регламентуються концепцією управління безперервністю бізнесу (КУББ). Вона передбачає в собі моніторинг поточної ситуації, прогнозування КС, оцінку рівня критичності ситуації, прийняття контрзаходів та ліквідацію їх наслідків і в цілому відповідає етапам циклу Шухарта-Демінга або PDCA. Кожен з цих процесів має свої особливості і різну ступінь реалізації на практиці.

На даний момент питання визначення поняття КС, їх класифікації були розглянуті в роботах [1, 2], описані та розроблені методи та системи для прогнозування, ідентифікації аномального стану в інформаційно-комунікаційних системах та мережах (ІКСМ) [3, 4], діяльності порушників [5-9], комп'ютерних атак [10]. Питанням іденти-

фікації, прогнозування та моделювання надзвичайних ситуацій екологічної, суспільної, державної безпеки присвячена праця [11], в якій виділені критерії для моделювання КС техногенного, природного та соціального характеру, які однак не є універсальними і не можуть бути застосовані до всієї множини можливих катастроф. А в [12] введені основні індикатори національної безпеки, серед них: коефіцієнт депопуляції, рівень тінізації економіки, рівень витрат на оборону, науку та освіту, рівень злочинності, децильний коефіцієнт, проте ці критерії характеризують стан захищеності держави, а не власне критичність КС. Крім того існує ряд нормативних документів, що регулюють процеси аналізу ризиків, до яких відносяться визначення ймовірності настання КС, ймовірного економічного збитку, людського, індивідуального та колективного ризику [13, 14]. Серед розглянутих методів виділяють різні класи методів аналізу ризиків, а саме: детерміновані, ймовірнісно-статистичні (статистичні, теоретико-ймовірнісні, ймовірнісно-евристичні), в умовах невизначеності нестатистичної природи (нечіткі і нейромережеві), комбіновані. Однак жоден з названих методів не може бути застосований для обробки відповідних критеріїв критичності ситуації різного роду, тобто не є універсальним і не враховує всіх особливостей будь-якої КС. Також слід відмітити роботи, в яких висвітлені особливості управління інформаційною безпекою в умовах невизначеності впливу дестабілізуючих чинників, описані методи оцінки виконання функцій безпеки, оцінки ризику та прийняття рішення в умовах КС [15], а також моделі протидії загрозам порушення інформаційної безпеки з можливістю вибору варіанту залежно від ймовірності атаки та метод оцінки рівня захищеності інформації на базі нечіткої логіки [16]. Останні дві роботи розглядають інформаційну безпеку з точки зору захищеності, а дане дослідження – навпаки з точки зору критичності порушення інформаційної безпеки.

Проблема оцінки рівня критичності КС, як одного з процесів КУББ, визначається тим, що її виникнення та розвиток є важко прогнозованим (а часто і взагалі не прогнозованим), тобто маємо справу з подією в нечітко формалізованому просторі. Крім того не існує загальноприйнятих критеріїв оцінки рівня критичності, більшість з них мають різну природу (в тому числі чіткі та нечіткі) і математичні властивості, що унеможливлює використання більшості з відомих на сьогодні методів оцінок до загального набору цих критеріїв. Тому формування параметрів та розробка методів для оцінки рівня критичності КС та методів його визначення є актуальною задачею. Отже, метою даної статті є визначення множини параметрів оцінки рівня критичності КС, розробка методів оцінки запропонованих параметрів та обчислення загального рівня критичності ситуації.

Розглянемо КС та її вплив на систему, організацію чи державу. Так, КС можуть спричинити в об'єкті впливу зміни структури, функціональних процесів, загрожують їх існуванню і характеризується рівнем критичності (The level of criticality a situation) LCS, при чому з зростанням рівня критичності інциденту зростає ймовірність його переходу в стан КС і значного негативного впливу на системи. Для оцінки КС та визначення рівня критичності пропонується метод, який складається з 6-ти етапів.

Етап 1. Визначення параметрів оцінки рівня критичності. Рівень критичності можна описати врахувавши функціональні залежності між L_e – параметрами оцінки рівня критичності. Параметри L_e можуть мати різну природу, характеризувати вплив КС з різних сторін, тому виникають проблеми в застосуванні їх відомими методами аналізу ризиків, визначення можливих наслідків та збитків. Дані параметри можна представити в якісному (як лінгвістична зміна (ЛЗ) з певним числом термів) або кількісному вигляді. Опишемо можливу множину параметрів для оцінки рівня критичності, виходячи з точки зору максимальної універсалізації цих характеристик та з застосуванням положень щодо класифікації КС, викладених в [2]. Слід відмітити, що при роботі з конкретними типами КС повинна зберігатись можливість поповнення цієї множини додатковими параметрами. Сформуємо множину параметрів $\mathbf{L} = \left\{ \bigcup_{e=1}^{E} L_e \right\}$ і розглянемо детально кожен її елемент, причому в рамках даного дослідження введемо E=15 парметрів. Конкретні параметри були підібрані на основі аналізу основних стандартів КУББ (BS ISO/IEC 17799:2005, BS 25999, NIST ST800-34, NFPA 1600 та інші), кращих методик та практик, таких як DRII, Gartner, BSI, HP, сучасних систем управління КС та вищезгаданих робіт.

Параметр L_1 – тривалість інциденту, TR. Під тривалістю інциденту будемо розуміти час, який пройшов від початку дії чинників, що його спричиняють, до завершення дії останнього з них.

Інколи в тривалість включають і час на усунення наслідків КС, проте в такому випадку оцінка інциденту можлива лише постфактум, тобто по його завершенню, що суперечить поставленим цілям. Зрозуміло, що чим більша тривалість ІПКС, тим більша його критичність і, відповідно, можливість переростання його в статус КС. Однак даний показник не можна використовувати в абсолютному масштабі, оскільки час тривалості надзвичайних подій дуже різний. Так, тривалість спалаху блискавки становить долі секунди, а військовий конфлікт може тривати роками. Тому, оцінюючи критичність інциденту за цим параметром слід враховувати не лише показник його тривалості, а й клас інциденту (КС) за часом дії негативних чинників.

Параметр L_2 – Ступінь порушення функціоналу критичних ресурсів/процесів, *DVF*. Даний критерій визначається з точки зору двох аспектів: критичність ресурсів/процесів та порушення функціоналу. В першу чергу необхідно визначити наявні інформаційні ресурси, а також комунікаційні та життєзабезпечуючі системи, здійснити їх ранжування за критичністю. Ці питання розглянуті в таких практиках КУББ як BCI, DRII, SANS, рекомендаціях Gartner. Так в методиці Gartner, основуючись на показниках RTO та RPO, виділяють чотири класи бізнес-процесів і IT-сервісів, які наведені в таблиці 1 [17].

Таблиця 1

Класифікація БП та IT-сервісів згідно рекомендацій Gartner

Клас	Послуги бізнес-сервісу	Рівень послуг
1-ий клас	Основні бізнес-процеси і сервіси, орієнтовані на роботу з клієнтами та партнерами	RTO– 2 год., RPO– 0 год.
2-ий клас	Допоміжні бізнес-процеси і сервіси (логістика, маркетинг, PR і ін.)	RTO– 8-24 год., RPO– 4 год.
3-ій клас	Процеси і сервіси, що забезпечують власні потреби компанії	RTO– 3 дня., RPO–1 день
4-ий клас	Процеси і сервіси, що забезпечують потреби окремих бізнес-підрозділів	RTO– 5 дня., RPO–1 день

Дану класифікацію можна застосувати як для окремих ІКСМ, підприємств та компаній, так і для держави в цілому. В аспекті порушення функціоналу можна виділити повне припинення надання послуг, часткове припинення зі зниженням якості надання послуг, часткове зниження якості надання послуг, відсутність порушення функціоналу тощо. Загальна оцінка визначається поєднанням цих двох аспектів і визначається таким чином, що чим критичніший ресурс і більша ступінь порушення функціоналу, тим вища оцінка.

Параметр L_3 – Географічний масштаб інциденту, *GS*. Зв'язок між критичністю інциденту і зоною його розповсюдження є очевидним. Так, чим більшу територію охоплює інцидент, деструктивно впливаючи на неї, тим більш імовірним є перехід ІПКС в ранг КС. При цьому до території, яку охоплює інцидент, доцільно включати і області на які поширюється не лише негативні чинники інциденту, а й наслідки. Проводячи ранжування в питаннях географічного масштабу виділяють наступні групи інцидентів, починаючи з найменшого: мікролокальні (окремий об'єкт, споруда чи їх комплекс), макролокальні (охоплює територію селища чи міста), регіональні (декілька міст чи інших адміністративно-територіальних одиниць), державні та глобальні [2, 12]. При цьому чим вище ранг інциденту, тим вища оцінка експерта в балах.

Параметр L_4 – Масштаб інциденту в організаційному аспекті, *OS*. Так само як інцидент може охоплювати різні географічні зони, він може й впливати на об'єкт з різних організаційних сторін. Тут доцільно виділити наступні види: інциденти в межах окремого бізнес-процесу, підприємства, на рівні групи підприємств, на рівні галузі економіки та загальноекономічні, при яких в кризовому стані знаходиться вся економічна структура держави чи групи держав [2, 12]. Наприклад, вихід з ладу сервера електронної пошти в відділі бухгалтерії на певному підприємстві можна оцінити як інцидент в межах окремого бізнес процесу, натомість значне підтоплення гірничодобувного регіону може паралізувати залежно від географічних масштабів та характеристик економіки як мінімум окреме підприємство, а як максимум цілу гірничу галузь. Звісно чим більший масштаб інциденту в організаційному аспекті, тим вища експертна оцінка.

Параметр L_5 – Загальний рівень економічних збитків, *OLED*. В поняття економічних збитків включаються всі фінансові та матеріальні витрати, спричинені наслідками інциденту, в тому числі і руйнуваннями, затрати щодо реагування на інцидент, його ліквідацію, інколи збитки від втрати репутації, які можна оцінити в грошовому еквіваленті тощо. Сума збитків обраховується за час з початку дії чинників інциденту до поточного моменту. Нищівні, з великими, помірними та невеликими збитками, практично не відчутні – основні класи КС, що можна виділити за рівнем завданих економіці збитків [2]. Оцінка у даному випадку здійснюється за абсолютним показником суми витрачених на ліквідацію наслідків грошей

або за часткою цієї суми в ВВП країни чи прибутку підприємства. Так, якщо збитки від КС знаходяться в інтервалі [N1; N2] мінімальних зарплат, то вона має статус надзвичайної ситуації місцевого рівня, [N2; N3] – регіонального та [N3; >N3] – державного. Згідно постанови КМУ №368 від 24.03.2004 р. N1=500 мінімальних зарплат, N2=5000 та N3=25000 [12, 18]. Зазвичай в разі збитків в розмірі понад 10% ВВП або 50% чистого прибутку рекомендується інцидент назвати катастрофічним і експертом надається максимальна оцінка. Залежність між рівнем збитків та оцінкою експерта є пропорційною.

Параметр L_6 – Відношення рівня економічних збитків за поточний період до відповідного рівня за попередній період, RD. Даний критерій дає змогу оцінити динаміку інциденту в економічному плані і показує як змінюється величина збитків від інциденту з часом. Якщо збитки за поточний період зростають в порівняні з попереднім, то динаміка є негативною, в іншому випадку – позитивною. Якщо $RD=0$, то можна зробити висновок, що деструктивний вплив на даному етапі відсутній і при умові збереження тенденцій КС вважається закінченою.

Параметр L_7 – Рівень загрози життю та здоров'ю людей, $RTLH$. Даний критерій може бути обрахований суто математично або визначений експертним методом. В першому разі використовуються наступна математична база. Величину потенційного ризику $R_{пот}(x,y)$, рік$^{-1}$, в певній точці (x, y) на території об'єкта і поблизу нього рекомендується визначати за формулою з [19] $R_{пот}(x,y)=\sum_{i=1}^{J} Q_i \cdot \max_j\left(P_{гиб}^{\ ij}(x;y)\cdot \nu_{уяз}^{\ ij}(x;y)\right)$, де J – число сценаріїв розвитку аварій; Q_i – частота реалізації протягом року j-го сценарію розвитку аварії, рік$^{-1}$; $\nu_{уяз}^{\ ij}(x;y)$ – коефіцієнт уразливості людини, що знаходиться в точці території з координатами (x, y) від j-го уражаючого чинника, який може реалізуватися в ході i-го сценарію аварії і залежний від захисних властивостей приміщення, укриття, в якому може знаходитися людина в момент аварії, і змінюється від 0 (людина невразлива) до 1 (людина не захищена через незначні захисні властивості укриття); $P_{гиб}^{\ ij}(x;y)$ – умовна ймовірність загибелі незахищеної людини на відкритому просторі в точці території з координатами (x;y) від j-го уражаючого чинника при реалізації i-го сценарію аварії. Індивідуальний ризик рекомендується оцінювати частотою ураження певної людини (групи людей) в результаті аварії протягом року. Величину індивідуального ризику $R_{ iно}^{\ i}$, рік$^{-1}$, для i-го індивіда рекомендується визначати за формулою

$R_{ино}^{\ i}=\sum_{k=1}^{G} q_{ki}\cdot R_{пот}(x,y)$, де q_{ki} – ймовірність присутності в k_i-й області території; G – число областей, на які умовно можна розбити територію, за умови, що величину потенційного ризику на всій площі кожної з таких областей можна вважати однаковою; Ймовірність рекомендується визначати, виходячи з частки часу знаходження людини на певній території [14].

При визначені експертом, виходячи зі своїх суб'єктивних суджень чи використовуючи вище описаний математичний апарат залежно від своєї кваліфікації, він оцінює критерій $RTLH$ за лінгвістичною або бальною шкалою. Можлива оцінка КС виходячи з кількості загиблих чи постраждалих. Оскільки під час КС можуть бути як загиблі так і поранені, то в [2] пропонується користуватися характеристикою кількість жертв, що охоплює в собі обидві категорії і виділяти наступні категорії КС: катастрофічні, з великою та невеликою кількістю жертв. Крім того. зазначена наступна залежність рівня надзвичайної ситуації від кількості жертв: місцевий рівень – загинуло [0; Z1[, постраждало [P0, P1] осіб, регіональний – загинуло [Z2; Z3], постраждало [P2, P3] осіб, державний – загинуло [Z4; >Z4], постраждало [P4, >P4] осіб. В постанові КМУ №368 від 24.03.2004 р. встановлено Z1=2, Z2=3, Z3=5, Z4=6, P0=20, P1=50, P2=51, P3=100, P4=101 особа(и) [12, 18]. Чим вищою є загрозу життю і здоров'ю людини, тим вища експертна оцінка.

Параметр L_8 – Питомий показник смертності на поточний момент, RM. За своєю суттю критерій аналогічний з RD. Він також дає змогу оцінити динаміку розвитку інциденту чи КС в аспекті людських втрат. Динаміка буде негативною, якщо кількість загиблих зростає в часі і навпаки при зменшені числа людських втрат в порівняні з попереднім періодом – динаміка буде позитивною. Критерій $RM=0$ свідчить про зникнення чинника, що спричиняє людські втрати.

Параметр L_9 – Частота проявів інцидентів (інтенсивність), F. Під частотою інцидентів будемо розуміти величину, що показує скільки разів в одиницю часу виникають або повторюються певні дестабілізуючі чинники, що негативно впливають на об'єкт та хід інциденту. Наприклад, при масштабних аваріях на газопроводах може виникати серія вибухів з деякими інтервалами між вибухами. Величина загальної кількість цих вибу-

хів поділена на проміжок часу між першим і останнім і є частотою прояву інциденту. Можливі ситуації коли не можливо точно встановити часові інтервали чи кількість інцидентів, особливо під час КС що тривають на момент оцінки, тому пропонується дану величину оцінювати експертними методами. Чим вища інтенсивність інциденту, тим вищою є експертна оцінка. Неодмінним є врахування типу КС при її оцінці, так $F=10$ для кількості вибухів в газопроводі за годину є досить великою, а для кількості вистрілів при військових діях навпаки низькою, тому і експертні оцінки будуть відрізнятися відповідно.

Параметр L_{10} – Ступінь руйнування інфраструктури, *DDI*. Даний критерій характеризує вплив інциденту на інфраструктуру, приміщення, обладнання тощо. Інциденти з високим степенем руйнувань можна з певною ймовірністю охарактеризувати як кризову ситуацію і чим більші руйнування, тим вища така ймовірність. Доцільно у відповідності існуючим ДБН, нормативно-правовим актам та стандартам в галузі техніки безпеки, промислового виробництва та менеджменту виділити такі ступені руйнування: повне, сильне, середнє та слабке руйнування. Даний критерій тісно пов'язаний з рівнем економічних збитків та рівнем загрози життю та здоров'ю людей [14].

Параметр L_{11} – Співвідношення реального часу відновлення і показника RTO, *CRT*. Однією з особливостей будь-якої КС є вихід з ладу обладнання, приладів та систем, переривання процесів тощо. Чим довшим є переривання в їх роботі, тим більші збитки отримує суб'єкт господарювання чи держава. В концепції УББ виділяють допустимий час переривання RTO, який не призводить до значних проблем. У випадку коли час, затрачений на відновлення більший за RTO виникає суттєва небезпека, що зростає з ростом різниці між цими величинами. Слід зазначити, що для різних систем залежно від їх критичності вводять різні показники RTO (див. табл. 1), тому при відновленні системи, наприклад, за 48 годин оцінка критерію *CRT* для систем класу критичності 1 буде більшою ніж для систем інших класів. Крім того при оцінці впливу на комплекс систем вона здійснюється виходячи з позицій системи, клас критичності якої є найвищим.

Параметр L_{12} – Відношення рівня втрат ресурсів і показника RPO, *CRP*. Цей критерій як і попередній відноситься до одних з основних в аспекті КУББ. Так при будь-якій КС має місце певна втрата інформації чи інформаційних ресурсів, при чому введені спеціальні показники допустимої величини цих втрат. Параметр RPO характеризує цю величину в часовому вимірі, тобто RPO=1 год. означає, що допустимі втрати інформаційних ресурсів в такому об'ємі, щоб після відновлення величина наявних ресурсів була не меншою ніж за 1 годину до початку КС. Іншими словами резервні копії повинні робитися, зберігатися і оновлюватись кожну годину. За суттю критерій аналогічний з попереднім.

Параметр L_{13} – Рівень панічних, протестних та антидержавних настроїв персоналу/населення, *LM*. Цей критерій складається з двох складових. При будь-яких серйозних ІПКС чи КС незалежно від причин їх походження (джерел виникнення) присутні панічні настрої, що зазвичай ще більше ускладнює перебіг ситуації, вносячи додаткові дестабілізуючі чинники. А от протестні та антидержавні настрої характерні переважно лише для КС соціального характеру, причинами яких і є соціальний людський чинник. До протестних та антидержавних настроїв можна віднести соціальну невдоволеність, підтримку радикальних сил, сепаратизм тощо. Наявність таких настроїв сама по собі може стати причиною КС або значно ускладнити інші чинники, в тому числі перешкоджаючи їх усуненню та ліквідації. Оцінка настроїв людей не може бути проведена в жодній існуючій системі координат вимірювання, тому апріорі здійснюється експертними методами на базі теорії нечітких множин.

Параметр L_{14} – Ступінь впливу зовнішніх дестабілізуючих та психологічних чинників, *DIEPF*. Цей критерій характеризує зовнішній вплив на ситуацію ззовні ворожими чи конкуруючими сторонами, що включає в собі також вплив на свідомість та психіку населення/персоналу. До таких характеристик можна віднести такі явища та процеси як ворожа пропаганда, навмисне введення в оману з приводу ситуації на економічних ринках, вплив на політичну ситуацію, контроль ЗМІ та дії шпигунської мережі, застосування методів недобросовісної конкуренції, інсайдерська діяльність тощо. Даний параметр найбільш тісно пов'язаний з поняттям інформаційних воєн та інформаційної боротьби як на державному так і приватному (підприємницькому чи корпоративному) рівнях.

Параметр L_{15} – Ступінь порушення характеристик безпеки ДІР з ОД, *DVChS*. Найбільш важливий критерій з точки зору інформаційної безпеки. Основними характеристиками інформаційної безпеки є: конфіденційність – характеристика безпеки інформації, що відображає її влас-

тивість невиявленості й недоступності без відповідних повноважень; цілісність – характеристика безпеки інформації (даних), що відображає її властивість протистояти несанкціонованій модифікації, наприклад, користувач, що накопичує інформацію, має право очікувати, що вміст його файлів залишиться незмінним, незважаючи на цілеспрямовані впливи, а також відмови програмних або апаратних засобів; доступність – характеристика безпеки інформації, що відображає її властивість, яка полягає в можливості її використання у заданий момент часу відповідно до пред'явлених повноважень [20]. Порушення інформаційної безпеки визначається як порушення однієї чи декількох з цих характеристик. Ступінь порушення характеристик може градуюватися від незначної (наприклад, тимчасові проблеми з доступністю, зміна або втрата незначної частини файлу чи документу, її розголошення) до повної (тривала втрата доступності, знищення чи спотворення всього документу та його розголос). В залежності від цього експерт здійснює свою оцінку.

Запропоновані параметри є нечіткими, оскільки оцінка експерта характеризується функцією належності (ФН) до певного терму нечіткого числа (НЧ) (наприклад, для параметра степінь порушення функціоналу критичних ресурсів/процесів – повна, незначна, значна тощо) відповідно до його суб'єктивного рішення, а не об'єктивних причин, відсутні критичні значення показників цих параметрів, універсальні для них шкали вимірювання та еталонні значення і оцінка експерта не дає однозначної відповіді щодо критичності ІПКС. Саме тому при обробці даних параметрів необхідно (і можливо) використовувати методи експертного оцінювання та апарату нечіткої логіки.

Для оцінки рівня критичності КС використаємо нечітку модель з лінгвістичною шкалою (НМЛШ) [21], коли на основі даних експертів будуються еталоні значення, а в результаті вимірювання поточного рівня кожного з параметрів приймається рішення щодо загального рівня критичності ІПКС.

Отже, сформована множина

$\mathbf{L} = \left\{ \bigcup_{e=1}^{E} L_e \right\} = \{L_1, L_2, ..., L_E\}, e = \overline{1, E}$, де E – кількість параметрів.

Наприклад, за умов дослідження при E=15,

$\mathbf{L} = \left\{ \bigcup_{e=1}^{15} L_e \right\} = \{L_1, L_2, ..., L_{15}\} = \{$*TR, DVF, GS, OS, OLED, RD, RTLH, RM, F, DDI, CRT, CRP, LM, DIEPF, DVChS*$\}$.

Кожен з параметрів і результуючий рівень критичності КС можна описати використовуючи ЛЗ, що складається з певної кількості термів:

$$\mathbf{T_L} = \bigcup_{e=1}^{E} \left\{ \bigcup_{s=1}^{r} \mathrm{T}_{L_e s} \right\} = \bigcup_{e=1}^{E} \left\{ \mathrm{T}_{L_e 1}, \mathrm{T}_{L_e 2}, ..., \mathrm{T}_{L_e r} \right\} =$$

$$\left\{ \mathrm{T}_{L_1 1}, \mathrm{T}_{L_1 2}, ..., \mathrm{T}_{L_1 r} \right\}, \left\{ \mathrm{T}_{L_2 1}, \mathrm{T}_{L_2 2}, ..., \mathrm{T}_{L_2 r} \right\}, ..., \left\{ \mathrm{T}_{L_{15} 1}, \mathrm{T}_{L_{15} 2}, ..., \mathrm{T}_{L_{15} r} \right\},$$

$$\mathbf{T_{LCS}} = \left\{ \bigcup_{s=1}^{r} \mathrm{T}_{LCPs} \right\} = \left\{ \mathrm{T}_{LCP1}, \mathrm{T}_{LCP2}, ..., \mathrm{T}_{LCPr} \right\}, \; s = \overline{1, r},$$

де r – кількість термів, що визначають ЛЗ. Наприклад, при $r=5$ і $E=15$

$$\mathbf{T_L} = \bigcup_{e=1}^{15} \left\{ \bigcup_{s=1}^{5} \mathrm{T}_{L_e s} \right\} = \bigcup_{e=1}^{15} \left\{ \mathrm{T}_{L_e 1}, \mathrm{T}_{L_e 2}, \mathrm{T}_{L_e 3}, \mathrm{T}_{L_e 4}, \mathrm{T}_{L_e 5} \right\} =$$

$$\bigcup_{e=1}^{15} \left\{ \mathrm{МН}_{L_e}, \mathrm{НС}_{L_e}, \mathrm{С}_{L_e}, \mathrm{ВС}_{L_e}, \mathrm{МК}_{L_e} \right\},$$

$$\mathbf{T_{LCS}} = \{\mathrm{МН}, \mathrm{НС}, \mathrm{С}, \mathrm{ВС}, \mathrm{МК}\},$$

при цьому терми приймають значення МН – мінімальне, НС – нижче середнього, С – середнє, ВС – вище середнього, МК - максимальне.

Етап 2. Формування оціночних еталонів. Під час другого етапу формується оціночні еталони, що використовуватиметься для порівняння з НЧ сформованим під час визначення рівня всіх параметрів та загального рівня критичності (фазифікації). Для кожного параметру формується окремий еталон, проте цілком можливо використовувати один оціночний еталон $\mathbf{T^e_{EL}}$

$$= \left\{ \bigcup_{s=1}^{r} \mathrm{T}^{\mathrm{e}}_{ELs} \right\} = \left\{ \mathrm{T}^{\mathrm{e}}_{EL1}, \mathrm{T}^{\mathrm{e}}_{EL2}, ..., \mathrm{T}^{\mathrm{e}}_{ELr} \right\} = \{ \bigcup_{q=1}^{r_s} \mu^{\mathrm{e}}_{\mathrm{ELsq}} / x^{e}_{\mathrm{ELsq}} \} =$$

$$= \{ \mu^{e}_{\mathrm{ijs}1} / x^{e}_{ijs1}, \mu^{\mathrm{e}}_{\mathrm{ijs}2} / x^{e}_{ijs2}, ..., \mu^{\mathrm{e}}_{\mathrm{ijsr_s}-1} / x^{e}_{ijsr_s-1}, \mu^{\mathrm{e}}_{\mathrm{ijsr_s}} / x^{\mathrm{e}}_{ijsr_s} \},$$

$(q = \overline{1, r_s})$, де r_s $(s = \overline{1, r})$ – кількість компонент в T^{e}_{EL} з аналогічними термами, що і в T_{L_e} та T_{LCS}. Побудуємо даний еталон використавши метод побудови параметричних НЧ, описаний в [22]. Функція, що задає значення ФН оціночних еталонів буде мати вигляд:

$$\mu_{\underset{\sim}{A}}(x) = \begin{cases} 0, & \text{якщо } x < a; \\ (x-a)/(b-a), & \text{якщо } a \le x < b; \\ (c-x)/(c-b), & \text{якщо } b \le x < c; \\ 0, & \text{якщо } x > c. \end{cases}$$

Діапазон зміни носіїв НЧ з $r=5$ термів та $r_s=3$ компонент відобразимо на універсальній множині U=[0, 1]. Отримані еталоні НЧ представлені на рис. 1, а їх математичний опис виразом:

$$\mathrm{T}^{e}_{EL} = \begin{cases} MH^{e} = \{0/0 \quad 1/0 \quad 0/0,25\}; \\ HC^{e} = \{0/0 \quad 1/0,25 \quad 0/0,5\}; \\ C^{e} = \{0/0,25 \quad 1/0,5 \quad 0/0,75\}; \\ BC^{e} = \{0/0,5 \quad 1/0,75 \quad 0/1\}; \\ MK^{e} = \{0/0,75 \quad 1/1 \quad 0/1\} \end{cases}.$$

Етап 3. Обчислення коефіцієнтів важливості (КВ). Етап застосовується для обчислення (КВ) та відповідно ранжування параметрів оцінки рівня критичності. Застосовуємо для цього метод кількісного парного порівняння з визначенням квадратного кореня, що є різновидом методу кількісного парного порівняння [22]. В основі лежить формування матриці парного порівняння $A=\|a_{ee'}\|$, де a_{ij} вибирається виходячи з суджень експерта відповідно шкалі відносної важливості: 1 – альтернативні варіанти мають рівне значення (пріоритет, важливість), 3 – досвід і судження дають легку перевагу однієї альтернативи над іншою, 5 – досвід і судження дають сильну перевагу однієї альтернативи над іншою (наявні переконані свідчення на користь одного з альтернативних варіантів), 7 – одна з альтернатив значно переважає іншу, що є очевидним, 9 – перевага однієї альтернативи над іншою є беззаперечною та абсолютною; 2, 4, 6, 8 – компромісні випадки. Якщо при порівнянні першої альтернативи з другою отримане вищезгадане число (наприклад, 5), то при порівнянні другої альтернативи з першою – зворотна величина (1/5). Вагові коефіцієнти обчислюються згідно виразу $\omega_e=\sqrt[n]{\prod_{e'=1}^{E}a_{ee'}}, e'=\overline{1,E},$ де E – кількість параметрів оцінки. Після цього проводиться нормування отриманих коефіцієнтів за виразом $\Omega_e=\omega_e/(\sum_{e=1}^{E}\omega_e)$ таким чином щоб $\sum_{e=1}^{E}\Omega_e=1.$

Етап 4. Вимірювання та фазифікація параметрів. На даному етапі здійснюється обчислення НЧ, що представляють поточні значення параметрів, виміряних системою та фазифікованих. Система оцінює параметри L_e відповідно до еталонних значень. На основі Т поточних вимірювань, що здійснюються протягом певного періоду часу, формується НЧ, що відображає поточне значення параметру. Воно визначається як

$$\underset{\sim}{L}_e=(\sum_{s=1}^{r}\underset{\sim}{T}_{ELs}^{E})/T=(\underset{\sim}{T}_{EL1}^{E}\,\tilde{+}\,\underset{\sim}{T}_{EL2}^{E}\,\tilde{+}\ldots\tilde{+}\,\underset{\sim}{T}_{ELs}^{E}\,\tilde{+}\ldots\tilde{+}\,\underset{\sim}{T}_{ELr}^{E})/T \quad (1)$$

де Т – загальна кількість вимірювань, $\underset{\sim}{T}_{ELs}^{E}$ - поправочний еталон. $\underset{\sim}{T}_{ELs}^{E}$ визначається за допомогою сенсорів і механізму лічильника. За своєю суттю процедура аналогічна з методом фазифікації параметрів, описаному в [23].

Етап 5. Обчислення рівня критичності КС. На четвертому етапі здійснюються обчислення загальної оцінки рівня критичності ситуації. Спочатку з врахуванням визначених КВ формується НЧ

$$\underset{\sim}{LCS}=\sum_{e=1}^{E}(\Omega_e*\underset{\sim}{L}_e). \quad (2)$$

Сформоване НЧ порівнюється з оціночним еталоном за одним з відомих методів порівняння НЧ. Для даних цілей використаємо метод формування α-рівневої номіналізації НЧ [24] і метод визначення ідентифікуючих термів [25]. Процедура полягає в обрахунку номіналізованих (перетворених) еталонів та рівня критичності (попередньо проводиться розбиття на α-рівні AL_{ELg} і AL_{LCSg}) $\mathbf{T}_{\mathbf{EL}}^{\mathbf{ep}}=\{\bigcup_{s=1}^{r}\underset{\sim}{T}_{ELs}^{ep}\}=\{\underset{\sim}{T}_{EL1}^{ep},\ \underset{\sim}{T}_{EL2}^{ep},\ \ldots,\ \underset{\sim}{T}_{ELs}^{ep},\ \ldots,\ \underset{\sim}{T}_{ELr}^{ep}\}$, де $\underset{\sim}{T}_{ELs}^{ep}=\{\bigcup_{g=1}^{z}\mu_{ELsg}^{ep}/x_{ELsg}^{ep}\}=\{\mu_{ELs1}^{ep}/x_{ELs1}^{ep},\ \mu_{ELs2}^{ep}/x_{ELs2}^{ep},\ldots,\ \mu_{ELsz}^{ep}/x_{ELsz}^{ep}\}$, $(g=\overline{1,z})$, $(s=\overline{1,r})$, а $\mu_{ELsg}^{ep}=\mu_{ELs(z-g+1)}^{ep}=AL_{ELg}$ і $x_{ELg}^{p}=x_{ELq}+\frac{(\mu_{ELg}^{p}-\mu_{ELq})(x_{ELq+1}-x_{ELq})}{\mu_{ELq+1}-\mu_{ELq}}$, $(g=\overline{2,z})$, z – кількість компонент $\underset{\sim}{T}_{ELs}^{ep}$. Аналогічна процедура здійснюється з поточними значеннями рівня критичності. Далі проводиться визначення узагальненої відстані Хемінга

$$h(\underset{\sim}{T}_{ELs}^{ep},\ \underset{\sim}{LCS}^{p})=\sum_{g=1}^{z}\left|x_{ELsg}^{ep}-x_{LCSg}^{p}\right|=|\,x_{ELs1}^{ep}-x_{LCS1}^{p}\,|+|\,x_{ELs2}^{ep}-x_{LCS2}^{p}\,|+\ldots+|\,x_{ELsg}^{ep}-x_{LCSg}^{p}\,|+\ldots+|\,x_{ELsz}^{ep}-x_{LCSz}^{p}\,|, \quad (3)$$

де $(g=\overline{1,z})$, $(z=2\pi\text{-}1)$, $(s=\overline{1,r})$.

Критерієм відповідності $\underset{\sim}{LCS}$ одному з термів оціночного еталону є найменша відстань Хемінга. Таким чином відповідному терму відповідає і рівень критичності ситуації або ІПКС:

$$h\min_s=\bigwedge_{s=1}^{r}h(\underset{\sim}{T}_{ELs}^{ep},\underset{\sim}{LCS}^{p}). \quad (4)$$

Етап 6. Візуалізація результатів. Отримані результати в нечіткій формі відображені на рис.1. Крім того для кращого відображення рівня критичності ІПКС пропонується відобразити параметри критичності за допомогою індикатора критичності. Для цього відповідні параметри $\underset{\sim}{L}_e$ слід попередньо дефазифікувати. Найбільш доцільним в даному випадку є застосування методу центру ваги [22], за яким НЧ перетворюють в чітке за формулою

$$L_e = \frac{\sum_{i=1}^{z} y_{L_e i} * \mu(y_{L_e i})}{\sum_{i=1}^{z} \mu(y_{L_e i})}, \qquad (5)$$

де z - кількість супортів НЧ.

Можливий випадок, коли значення окремих параметрів обчислюються напряму без використання експертних методів. В такому випадку вони на індикаторі відображаються гістограмою.

Розглянемо роботу методу на конкретному прикладі згідно умов дослідження, оцінивши загальний рівень критичності ситуації на основі раніше введених параметрів. Тобто при r =5 і E=15. Оскільки параметри L_6 та L_8 носять чіткий характер, то на даному етапі вони залишаються без змін. В результаті ранжування параметрів отримана множина значень КВ, що відображені в табл. 2.

Таблиця 2

Результат попарного порівняння параметрів рівня критичності ІПКС L_e

e\e'	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ω_e	Ω_e
1	1	1/7	1/6	1/5	1/7	—	1/9	—	1	1/8	1/7	1/7	1/6	1/6	1/8	0,244	0,014
2	7	1	3	8	9	—	1/3	—	7	2	3	2	5	4	2	2,602	0,144
3	6	1/3	1	8	8	—	1/6	—	6	5	6	6	8	7	8	2,934	0,162
4	5	1/8	1/8	1	7	—	1/5	—	5	4	5	5	8	6	8	1,942	0,107
5	7	1/8	1/8	1/7	1	—	1/4	—	7	6	6	7	8	8	4	1,806	0,1
6	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
7	9	3	6	5	4	—	1	—	9	3	4	5	5	5	3	3,477	0,192
8	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
9	1	1/7	1/6	1/5	1/7	—	1/9	—	1	1/8	1/7	1/7	1/6	1/6	1/9	0,243	0,013
10	8	1/2	1/5	1/4	1/6	—	1/3	—	8	1	3	3	4	5	3	1,294	0,072
11	7	1/3	1/6	1/5	1/6	—	1/4	—	7	1/3	1	2	3	5	2	0,949	0,052
12	7	1/2	1/6	1/5	1/7	—	1/5	—	7	1/3	1/2	1	3	4	2	0,854	0,047
13	6	1/5	1/8	1/8	1/8	—	1/5	—	6	1/4	1/3	1/3	1	3	3	0,616	0,035
14	6	1/4	1/7	1/6	1/8	—	1/5	—	6	1/5	1/5	1/4	1/3	1	2	0,505	0,028
15	8	1/2	1/8	1/8	1/4	—	1/3	—	9	1/3	1/2	1/2	1/3	1/2	1	0,613	0,034
																18,079	1

Проведемо фазифікацію заданих параметрів за допомогою фіксації їх поточних значень, використовуючи механізм сенсорів. Результати даних з сенсорів наведені в табл. 3.

Таблиця 3

Показники лічильника сенсорів параметрів L_e

e	Виміряне значення параметра L_e відповідно до оціночних еталонів				
	МН	НС	С	ВС	МК
1	10	0	0	0	0
2	0	10	0	0	0
3	0	0	10	0	0
4	0	0	0	10	0
5	0	0	0	0	10
6	—	—	—	—	—
7	8	2	0	0	0
8	—	—	—	—	—
9	0	8	2	0	0
10	0	0	8	2	0
11	0	0	0	8	2
12	0	5	5	0	0
13	0	0	5	5	0
14	0	5	0	5	0
15	0	0	0	5	5

Обрахуємо значення параметрів за виразом (1) та рівень критичності за виразом (2):

$\underset{\sim}{L}_1 = (10*\mathrm{T}^e_{EL1})/10 = (10*\underset{\sim}{\mathrm{МН}}^e)/10$ = (10* {0/0; 1/0; 0/0,25})/10 = {0/0; 1/0; 0/0,25}. Аналогічно:

$\underset{\sim}{L}_2 = (10*\mathrm{T}^e_{EL2})/10 = (10*\underset{\sim}{\mathrm{НС}}^e)/10 =$ {0/0; 1/0,25; 0/0,5},

$\underset{\sim}{L}_3 = (10*\mathrm{T}^e_{EL3})/10 = (10*\underset{\sim}{\mathrm{С}}^e)/10 =$ {0/0,25; 1/0,5; 0/0,75},

$\underset{\sim}{L}_4 = (10*\mathrm{T}^e_{EL4})/10 = (10*\underset{\sim}{\mathrm{ВС}}^e)/10 =$ {0/0,5; 1/0,75; 0/1},

$\underset{\sim}{L}_5 = (10*\mathrm{T}^e_{EL5})/10 = (10*\underset{\sim}{\mathrm{МК}}^e)/10 =$ {0/0,75; 1/1; 0/1},

$\underset{\sim}{L}_7 = (8*\mathrm{T}^e_{EL1} + 2*\mathrm{T}^e_{EL2})/10 = (8*\underset{\sim}{\mathrm{МН}}^e + 2*\underset{\sim}{\mathrm{НС}}^e)/10$

= (8 * {0/0; 1/0; 0/0,25} + 2 * {0/0; 1/0,25; 0/0,5}) / 10 = ({0/0; 1/0; 0/2} + {0/0; 1/0,5; 0/1}) / 10 = ({0/0; 0/0,5; 0/1; 0/1; 1/0,5; 0/1; 0/2; 0/2,5; 0/3}) / 10 = ({0/0; 1/0,5; 0/1; 0/2; 0/2,5; 0/3}) / 10 = ({0/0; 1/0,5; 0/3}) / 10 = {0/0; 1/0,05; 0/0,3},

$\underset{\sim}{L}_9 = (8*\mathrm{T}^e_{EL2} + 2*\mathrm{T}^e_{EL3})/10 = (8*\underset{\sim}{\mathrm{НС}}^e + 2*\underset{\sim}{\mathrm{С}}^e)/10$

= {0/0,05; 1/0,3; 0/0,55},

$\underset{\sim}{L}_{10} = (8*\mathrm{T}^e_{EL3} + 2*\mathrm{T}^e_{EL4})/10 = (8*\underset{\sim}{\mathrm{С}}^e + 2*\underset{\sim}{\mathrm{ВС}}^e)/10$

= {0/0,3; 1/0,55; 0/0,8},

$\underset{\sim}{L}_{11} = (8*\mathrm{T}^e_{EL4} + 2*\mathrm{T}^e_{EL5})/10 = (8*\underset{\sim}{\mathrm{ВС}}^e + 2*\underset{\sim}{\mathrm{МК}}^e)/10$

= {0/0,55; 1/0,8; 0/1},

$\underset{\sim}{L}_{12} = (5*\mathrm{T}^{e}_{EL2} + 5*\mathrm{T}^{e}_{EL3})/10 = (5*\underset{\sim}{\mathrm{HC}}^{e} + 5*\underset{\sim}{\mathrm{C}}^{e})/10$

$= \{0/0{,}125;\ 1/0{,}375;\ 0/0{,}625\}$,

$\underset{\sim}{L}_{13} = (5*\mathrm{T}^{e}_{EL3} + 5*\mathrm{T}^{e}_{EL4})/10 = (5*\underset{\sim}{\mathrm{C}}^{e} + 5*\underset{\sim}{\mathrm{BC}}^{e})/10$

$= \{0/0{,}375;\ 1/0{,}625;\ 0/0{,}875\}$,

$\underset{\sim}{L}_{14} = (5*\mathrm{T}^{e}_{EL2} + 5*\mathrm{T}^{e}_{EL4})/10 =$

$(5*\underset{\sim}{\mathrm{HC}}^{e} + 5*\underset{\sim}{\mathrm{BC}}^{e})/10 = \{0/0{,}25;\ 1/0{,}5;\ 0/0{,}75\}$,

$\underset{\sim}{L}_{15} = (5*\mathrm{T}^{e}_{EL4} + 5*\mathrm{T}^{e}_{EL5})/10 = (5*\underset{\sim}{\mathrm{BC}}^{e} + 5*\underset{\sim}{\mathrm{MK}}^{e})/10$

$= \{0/0{,}625;\ 1/0{,}875;\ 0/1\}$,

$\underset{\sim}{LCS} = \sum_{e=1}^{E}(\Omega_e * \underset{\sim}{\mathrm{L}}_e)$ = 0,014*{0/0; 1/0; 0/0,25} + 0,144 * {0/0; 1/0,25; 0/0,5} + 0,162 * {0/0,25; 1/0,5; 0/0,75} + 0,107 * {0/0,5; 1/0,75; 0/1} + 0,1 * {0/0,75; 1/1; 0/1} + 0,192 * {0/0; 1/0,05; 0/0,3} + 0,013 * {0/0,05; 1/0,3; 0/0,55} + 0,072 * {0/0,3; 1/0,55; 0/0,8} + 0,052 * {0/0,55; 1/0,8; 0/1} + 0,047 * {0/0,125; 1/0,375; 0/0,625} + 0,035 * {0/0,375; 1/0,625; 0/0,875} + 0,028 * {0/0,25; 1/0,5; 0/0,75} + 0,034 * {0/0,625; 1/0,875; 0/1} = {0/0,2671; 1/0,4752; 0/0,69335}.

Використовуючи вираз (3) порівняємо результуючий рівень критичності з оціночними еталонами. Оскільки в даному випадку оціночні еталони і НЧ, що відображає рівнеь критичності ситуації мають трикутну форму, тоді згідно [24] кількість α-рівнів буде два: α = 0 і α = 1. Результати обрахунку номіналізованих еталонів та поточних значень параметрів представимо у вигляді таблиці 4.

Таблиця 4

Значення носіїв номіналізованих $\underset{\sim}{T}^{ep}_{ELs}$, $(\mathrm{s} = \overline{1,5})$ – $\underset{\sim}{MH}^{ep}$, $\underset{\sim}{HC}^{ep}$, $\underset{\sim}{C}^{ep}$, $\underset{\sim}{BC}^{ep}$, $\underset{\sim}{MK}^{ep}$ та $\underset{\sim}{LCS}^{p}$

$\underset{\sim}{T}^{ep}_{ELs}$ / $\underset{\sim}{LCS}^{p}$	μ^{ep}_{sg} / μ^{p}_{g} $(\mathrm{g} = \overline{1,9})$		
	μ^{ep}_{ELs1} / μ^{p}_{LCS1}	μ^{ep}_{ELs5} / μ^{p}_{LCS5}	μ^{ep}_{ELs9} / μ^{p}_{LCS9}
	0	1	0
$\underset{\sim}{T}^{ep}_{EL1} = \underset{\sim}{MH}^{ep}$	0	0	0,25
$\underset{\sim}{T}^{ep}_{EL2} = \underset{\sim}{HC}^{ep}$	0	0,25	0,5
$\underset{\sim}{T}^{ep}_{EL3} = \underset{\sim}{C}^{ep}$	0,25	0,5	0,75
$\underset{\sim}{T}^{ep}_{EL4} = \underset{\sim}{BC}^{ep}$	0,5	0,75	1
$\underset{\sim}{T}^{ep}_{EL5} = \underset{\sim}{MK}^{ep}$	0,75	1	1
$\underset{\sim}{LCS}^{p}$	0,2671	0,4752	0,69335

Обрахуємо відстані Хемінга:

$h\ (\underset{\sim}{T}^{ep}_{EL1},\ \underset{\sim}{\mathrm{LCS}}^{p}) = \sum_{g=1}^{z}\left|x^{\mathrm{ep}}_{\mathrm{EL1g}} - x^{\mathrm{p}}_{\mathrm{LCSg}}\right| = |0\text{-}0{,}2671| + |0\text{-}0{,}4752| + |0{,}25\text{-}0{,}69335| = 1{,}1857;$

$h\ (\underset{\sim}{T}^{ep}_{EL2},\ \underset{\sim}{\mathrm{LCS}}^{p}) = \sum_{g=1}^{z}\left|x^{\mathrm{ep}}_{\mathrm{EL2g}} - x^{\mathrm{p}}_{\mathrm{LCSg}}\right| = |0\text{-}0{,}2671| + |0{,}25\text{-}0{,}4752| + |0{,}5\text{-}0{,}69335| = 0{,}6857;$

$h\ (\underset{\sim}{T}^{ep}_{EL3},\ \underset{\sim}{\mathrm{LCS}}^{p}) = \sum_{g=1}^{z}\left|x^{\mathrm{ep}}_{\mathrm{EL3g}} - x^{\mathrm{p}}_{\mathrm{LCSg}}\right| = |0{,}25\text{-}0{,}2671| + |0{,}5\text{-}0{,}4752| + |0{,}75\text{-}0{,}69335| = 0{,}0986;$

$h\ (\underset{\sim}{T}^{ep}_{EL4},\ \underset{\sim}{\mathrm{LCS}}^{p}) = \sum_{g=1}^{z}\left|x^{\mathrm{ep}}_{\mathrm{EL4g}} - x^{\mathrm{p}}_{\mathrm{LCSg}}\right| = |0{,}5\text{-}0{,}2671| + |0{,}75\text{-}0{,}4752| + |1\text{-}0{,}69335| = 0{,}8144;$

$h\ (\underset{\sim}{T}^{ep}_{EL5},\ \underset{\sim}{\mathrm{LCS}}^{p}) = \sum_{g=1}^{z}\left|x^{\mathrm{ep}}_{\mathrm{EL5g}} - x^{\mathrm{p}}_{\mathrm{LCSg}}\right| = |0{,}75\text{-}0{,}2671| + |1\text{-}0{,}4752| + |1\text{-}0{,}69335| = 1{,}3144.$

Отже, згідно (4) $h\min_s = \bigwedge_{s=1}^{r} h(\underset{\sim}{T}^{ep}_{ELs}, \underset{\sim}{\mathrm{LCS}}^{p})$, тобто рівень критичності КС - середній. Даний результат можна відобразити графічно (рис. 1).

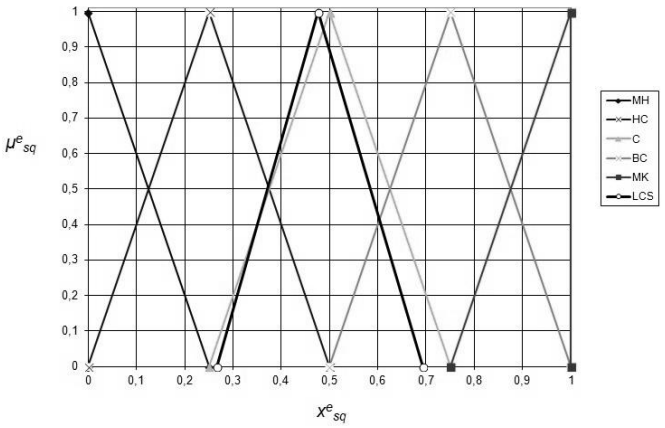

Рис. 1. Графічне представлення еталонних НЧ та рівня критичності ІПКС

Для відображення отриманих результатів за 100-бальною шкалою проведемо дефазифікацію кожного з запропонованих оціночних параметрів та обрахованого загального рівня критичності оцінки, використавши (5) і одночасно представимо їх 100-бальною шкалою, тобто:

$L_1 = 100 * \dfrac{\sum_{i=1}^{n} y_{L_1 i} * \mu(y_{L_1 i})}{\sum_{i=1}^{n} \mu(y_{L_1 i})}$ = 100 * (0 * 0 + 1 * 0 + 0 * 0,25) / (0 + 1 + 0) = 100 * 0 / 1 = 0; $L_2 = 25$; $L_3 = 50$; $L_4 = 75$; $L_5 = 100$; $L_7 = 5$; $L_9 = 30$; $L_{10} = 55$; $L_{11} = 80$; $L_{12} = 37{,}5$; $L_{13} = 62{,}5$; $L_{14} = 50$; $L_{15} = 87{,}5$ та $LCS = 47{,}52$.

Крім того параметри L_8 – Відношення рівня економічних збитків за поточний період до відповідного рівня за попередній період, *RD* та L_{10} – Питомий показник смертності на поточний момент, *RM* можна безпосередньо обрахувати за формулами (6) і (7) відповідно:

$$RD = \frac{LED(t)}{LED(t-1)}, \quad (6)$$

де $LED(t)$ – величина економічних збитків за поточний період, $LED(t-1)$ – величина економічних збитків за попередній період і

$$RM = \frac{SMR(t)}{SMR(t-1)}, \quad (7)$$

де $SMR(t)$ – смертність за поточний період, $SMR(t-1)$ – смертність за попередній період.

Важливо те, що тривалості часових проміжків, які використовуються при обчислені даних параметрів мають бути однаковими.

На основі значень вказаних параметрів з врахуванням процедури ранжування формується індикатор критичності ІПКС, який представлений на рис. 2. На ньому відображені рівня оціночних параметрів та обрахований загальний рівень критичності.

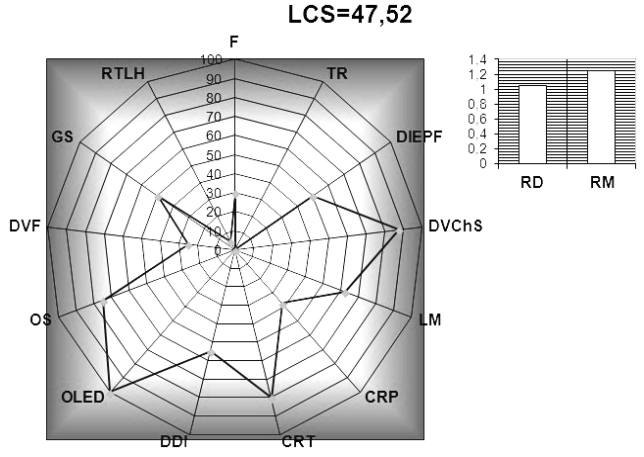

Рис. 2. Зображення індикатора рівня критичності ІПКС

Висновки. Запрпонований метод, заснований на методах нечіткої логіки та експертних підходах дає змогу проводити оцінку критичності поточної ситуації. Застосування експертних методів пояснюється необхідністю зменшення витрат часових та виробничих ресурсів, оскільки математичний апарат даних методів не потребує збору та обробки статистичних даних. Метод складається з 6 етапів: визначення параметрів оцінки рівня критичності, формування оціночних еталонів, обчислення КВ, вимірювання та фазифікація параметрів, обчислення рівня критичності КС, візуалізація результатів. Візуалізація результатів здійснюється через індикатор, який представляє собою інтерфейс з двома панелями для виводу значень критеріїв. У вигляді пелюсткової діаграми виводяться значення нечітких параметрів, а окремі параметри, оцінити які можливо оперуючи чіткими даними, – у вигляді гістограми. Крім того розроблений індикатор рівня критичності дає змогу оцінити динаміку розвитку ситуації, підібрати ефективні засоби та заходи реагування, полегшити процес прийняття рішень в умовах невизначеності та впливу КС.

Також наведено приклад використання методу, так в рамках дослідження запропонована множина критеріїв $\mathbf{L} = \{T, DVF, GS, OS, OLED, RTLH, F, DDI, CRT, CRP, LM, DIEPF, DVChS\}$, що є універсальною і може застосовуватися для оцінки будь-яких ІПКС (КС) незалежно від природи їх походження. Множина критеріїв може бути змінена шляхом додавання чи зміни специфічних критеріїв, характерних окремим ІПКС та КС залежно від потреб застосування. На базі цієї множини введено поняття рівня критичності ситуації $\underset{\sim}{LCS} = \sum_{e=1}^{E} (\Omega_e * \underset{\sim}{L}_e)$, що визначається функціональними залежностями між параметрами оцінки рівня критичності.

ЛІТЕРАТУРА

[1]. Гізун А.І. Сучасні підходи до захисту інформаційних ресурсів для забезпечення безперервності бізнесу / А.І. Гізун, В.О. Гнатюк, О.П. Дуксенко, А.О. Корченко // Матеріали X Міжнародної науково-технічної конференції «АВІА-2011». - К.: НАУ, 2011. - Т1 - с. 2.5-2.9.

[2]. Стасюк О.І. Базові характеристики та класифікація кризових ситуацій в ІТ-сфері / О.І. Стасюк, А.І. Гізун // Інфокомунікації – сучасність та майбутнє: Всеукр. наук.-практ. конф. 6-7 жовтня 2011 р. : тези доп. - Одеса: ОНАЗ, 2011. - С. 62-65.

[3]. Модели эталонов лингвистических переменных для систем выявления атак / М.Г. Луцкий, А.А. Корченко, А.В. Гавриленко, А.А Охрименко // Захист інформації. - 2012. - №2 (55). - С. 71- 78.

[4]. Корченко А.А. Модель эвристических правил на логико-лингвистических связках для обнаружения аномалий в компьютерных системах /А.А. Корченко // Захист інформації'. - 2012. - №4 (57). - С. 109-115.

[5]. 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. - Т.15. - №1. - С. 66-75.

[6]. Волянська В.В. Моделі еталонів лінгвістичних змінних для систем виявлення та ідентифікації порушника інформаційної безпеки // В.В. Волянська, А.І. Гізун, В.О. Гнатюк / Безпека інформації. - 2013. - Т.19. - №1. - С. 13-20.

[7]. Гізун А.І. Евристичні правила на основі логіколінвистичних зв'язок для виявлення та ідентифікації порушника інформаційної безпеки / А.І. Гізун, В.В. Волянська, О.В. Гавриленко, А.О. Корченко // Захист інформації. - 2013. - Т.15. - №3. – с. 251-257.

[8]. Корченко А.О. Метод виявлення та ідентифікації порушника в інформаційно-комунікаційних системах // А.О. Корченко, А.І. Гізун, В.В. Волянська, С.О. Гнатюк // Захист інформації. - 2013. - Т.15. - №4. - С. 387-393.

[9]. 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.

[10]. Параметры прогнозирования и идентификации атак в информационно-комуникационных системах / В. М. Азарсков, А.И. Гизун, А.М. Грехов, С.О. Скворцов // Захист інформації. - 2014. - Том 16. - №1. - С. 89-95.

[11]. Качинський, А. Б. Безпека, загрози і ризик: наукові концепції та математичні методи [Текст] : [монографія] / А. Б. Качинський. - К. : Нац. акад. служби безпеки України, 2004. – 471 с. - ISBN 966-8440-34-X.

[12]. Качинський, А. Б. Індикатори національної безпеки: визначення та застосування їх граничних значень [Текст] : монографія / А. Б. Качинський ; Нац. ін-т стратег. дослідж. - Київ : НІСД, 2013. - 102 с. - Бібліогр. в кінці розд. - ISBN 978-966-554-209-4.

[13]. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. : ГОСТ Р ИСО/МЭК 27001. - М.: Стандартинформ, 2008. - 32 с.

[14]. Методические указания по проведению анализа риска опасных производственных объектов. : РД 03-418-01. - М.: Государственное унитарное предприятие «Научно-технический центр по безопасности в промышленности Госгортехнадзора России», 2002. - 18 с.

[15]. Зырянова Т.Ю. Модель системы управления информационной безопасностью в условиях неопределенности воздействия дестабилизирующих факторов : автореф. дис. ... канд. техн. наук : 05.13.19 / Т. Ю. Зырянова - М, 2008. . - 26 с.

[16]. Машкина И.В. Управление защитой информации в сегменте корпоративной информационной системы на основе интеллектуальных технологий : автореф. дис. ... докт. техн. наук : 05.13.19 / И. В. Машкина - М, 2009. - 34 с.

[17]. Петренко С.А., Беляев А.В. Управление непрерывностью бизнеса. Ваш бизнес будет продолжаться / С.А. Петренко, А.В. Беляев. - М.: ДМК Пресс, Компания АйТи, 2011. - 400 с.

[18]. Про затвердження Порядку класифікації надзвичайних ситуацій за їх рівнями : Постанова Кабінету Міністрів України від 24.03.2004 № 368 // Офіційний вісник України. - 2004. - № 12. - Ст. 740.

[19]. Методические основы по проведению анализа опасностей и оценки риска аварий на опасных производственных объектах: Руководство по безопасности [Електроний ресурс]. – Режим доступу: www.gosnadzor.ru/ public/ discussion/ acts/Приложение%20001.doc.

[20]. Бабак В.П. Інформаційна безпека та сучасні мережеві технології: Англо-українсько-російський словник термінів / В.П. Бабак, О.Г. Корченко. - К.: НАУ, 2003. - 670 с.

[21]. Корченко А.О. Метод формирования лингвистических эталонов для систем выявления вторжений / А.О. Корченко // Захист інформації. - 2014. - Т.16. - №1. - С. 5-12.

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

[23]. Корченко А.А. Метод фаззификации параметров на лингвистических эталонах для систем выявления кибератак / А.А. Корченко // Безпека інформації. – 2014. – № 1 (20). – С. 21-28.

[24]. Корченко А.О. Метод а-рівневої номіналізації нечітких чисел для систем виявлення вторгнень / А.О. Корченко // Захист інформації. - 2014. - Т.16. - №4. - С. 304-311.

[25]. Корченко А.А. Метод определения идентифицирующих термов для систем обнаружения вторжений / А.А. Корченко // Безпека інформації. – 2014. – № 3 (20). – С. 217-223.

REFERENCES

[1]. Gizun A. I. Current approaches to protecting information resources for business continuity, A. I. Gizun, V. O. Gnatuk, O. P. Duksenko, A. O. Korchenko, Materials of the 10thscience – technical conferention «AVIA-2011», K.: NAU, 2011, T1, P. 2.5-2.9.

[2]. Stasyuk O. I. The baseline characteristics and classification of crises in the IT field, O. I. Stasyuk, A.I. Gizun, Infocommunications - Presentand Future: International Ukraine Conference. October, 6 – 7, 2011 p. :report thesis, Odesa: ONAZ, 2011, P. 62-65.

[3]. Lutskiy M.G. Model standards of linguistic variables for systems detect attacks, M.G. Lutskiy, A.V. Gavrelenko, A.A. Korchenko, A.A. Okhrimenko, Information security, 2012, №2 (55), P. 5-13.

[4]. Korchenko A.A. The model of heuristic rules on the logical-linguistic bundles to detect anomalies in computer systems, A.A. Korchenko, Information Security Research Journal, 2012, №4 (57), P. 109-115.

[5]. Gizun A.I. The main parameters to identify the intruder of information security, A.I. Gizun, V.V. Volyanska, V.O. Ryndyuk, S.O. Gnatyuk, Ukrainian Information Security Research Journal, 2013, T.15, №1, P.66-75.

[6]. Volyanska V.V. Models of standards of linguistic variables for detection and identification the intruder of information security, V.V. Volyanska, A.I. Gizun, V.O. Gnatyuk, Ukrainian Scientific Journal of Information Security, №1 (19), 2013, P. 13-21.

[7]. Gizun A.I. Heuristic rules based on logic-linguistic connection for information security intruder`s detection and identification, A.I. Gizun, V.V. Volyanska, O.V. Gavrylenko, A.O. Korchenko, Ukrainian Information Security Research Journal, 2013, T. 15, №3, P.251-257.

[8]. Korchenko A.A. Method of intruder detection and identification in information & communication systems. A.A. Korchenko, A.I. Gizun, V.V. Volyanska, S.O. Gnatyuk. Ukrainian Information Security Research Journal, 2013, T. 15, №4, P.387-393.

[9]. Korchenko A.A. System of intruder detection and identification in information & communication networks. A.A. Korchenko, A.I. Gizun, V.V. Volyanska. Ukrainian Scientific Journal of Information Security, №1 (19), 2013, P. 158-162.

[10]. Parameters identification and prediction of attacks in the information and communication system, V. Azarskov, A. Gizun, A. Grekhov, S. Skvortsov. Ukrainian Information Security Research Journal, 2014, T. 16, №1, P. 89-95.

[11]. Kaczynski, A.B. Security Threat and Risk: concepts and mathematical methods [text]: [monograph]. A.B. Kaczynski. K: Nat. Acad. Security Service of Ukraine, 2004, 471 p. ISBN 966-8440-34-X.

[12]. Kaczynski, A.B. Indicators of national security: the definition and application of limit values [Text]: monograph. A.B. Kaczynski; Nat. Inst strategist. resear. Kyiv: NISS, 2013, 102 p. Ref. at the end of Sec. - ISBN 978-966-554-209-4.

[13]. Information technology. Methods and means ofsecurityprovision.InformationalSystem Management security.Requirements. : GOST R ISO / IEC 27001. M .: Standartinform, 2008, 32 p.

[14]. Methodical specified in conducting analysis of risk manufacture hazard objects. : RD 03-418-01. M .: State Unitary Enterprise "Scientific and Technical Center for Russia Industrial Safety ", 2002, 18 p.

[15]. Zyryanova T.Y. Information security model management system in the face of uncertainty impact of destabilizing factors: Author. dis. ... Cand. tehn. Sciences: 05.13.19. T.Y. Zyryanova. M, 2008, 26p.

[16]. Mashkina I.V. Information security management of the corporate information system based on intelligent technologies: Author. dis. ... Doctor.tehn. Sciences: 05.13.19. I.V. Mashkina. M, 2009, 34 p.

[17]. Petrenko S.A., Belyaev A.V. Business management continuity. Your business will be continuing, S.A. Petrenko, A.V. Belyaev, M.: DMKPress, IT Company, 2011, 400 p.

[18]. On classification approval of the emergencies on their levels: Cabinet of Ministers of Ukraine of 24.03.2004 № 368. Official Journal of the Ukraine. – 2004, № 12., Art. 740.

[19]. Methodical bases for the hazard analysis and risk assessment of accidents on dangerous production objects : Security Guide [Electron resource]. Access of mode: www.gosnadzor.ru/ public/ discussion/ acts/Приложение%20001.doc.

[20]. Babak V.P. Information security and advanced network technologies: English-Ukrainian-Russian dictionary of terms. V.P. Babak, O.G. Korchenko., K: NAU, 2003, 670 p.

[21]. Korchenko A.O. Method of forming linguistic standards for intrusion detection systems. A.O. Korchenko. Ukrainian Information Security Research Journal, 2014, T. 16, №1, P.5-12.

[22]. Korchenko A.G. Development of the security systems on fuzzy sets. Theory and practical solutions, A.G. Korchenko, K.: "MK-Press", 2006, 320 P.

[23]. Korchenko A.A. The method of parameter fuzzification based on linguistic standards for cyber attacks detection. A.A. Korchenko. Ukrainian Scientific Journal of Information Security, №1 (20), 2014, P. 21-28.

[24]. Korchenko A.O. The method of α-level of nominalization for intrusion detection systems. A.O. Korchenko. Ukrainian Information Security Research Journal, 2014, T. 16, №4, P.304-311.

[25]. Korchenko A.A. The detection method of identification terms for intrusion detection system. A.A. Korchenko. Ukrainian Scientific Journal of Information Security, №3 (20), 2014, P. 217-223.

МЕТОД ОЦЕНКИ УРОВНЯ КРИТИЧНОСТИ ДЛЯ СИСТЕМ УПРАВЛЕНИЯ КРИЗИСНЫМИ СИТУАЦИЯМИ

Влияние кризисных ситуаций на состояние защищённости государственных информационных ресурсов, различных предприятий, организаций и государства в целом является очень существенным. Так, кризисные ситуации могут не только приостановить развитие системы, которая подвержена их влиянию, но и уничтожить ее вообще. Для противодействия такому влиянию необходимым есть принятие адекватных уровню угрозы мер и средств защиты, что определяет важность оценки критичности текущей ситуации. Сейчас не существует общепринятых универсальных критериев и интегрированного показателя оценки уровня критичности. Поэтому определение уровня критичности инцидента, который может провоцирует кризисные ситуации, является актуальной и важной научной задачей. В исследовании введено множество параметров оценки уровня критичности ситуации, предложен метод определения уровня критичности ситуации с использованием экспертных подходов и методов нечеткой логики, которые не требуют сбора и обработки статистических данных, а также описана процедура дефазификации значений параметров, на основе которых формируется индикатор отображения уровня критичности.

Ключевые слова: кризисная ситуация, инцидент, уровень критичности кризисной ситуации, индикатор, множество критериев, оценка уровня критичности, ущерб, класс критичности, экспертные методы, теория нечетких множеств.

METHOD OF CRITICALITY LEVEL ASSESSMENT FOR CRISIS MANAGEMENT SYSTEMS

Crisis influence on the security level of state information resources, different organizations and whole state is very serious. Crisis can stop system development that comes under its influence and also it can crush the system in the bud. To prevent this influence the adequate (to threats level) measures and security means must be taken and it defines the importance of current situation criticality assessment. There is no generally accepted universal criteria and integrated parameter for criticality level assessment of crisis. That's why defining of criticality level assessment for incident is actual and important scientific task. In the paper the set of parameters for criticality level assessment of crisis was introduced and also method for defining the criticality level of crisis with expert approach and fuzzy sets theory was proposed. These don't require the statistical data gathering and processing. Besides the defazification procedure for parameters was described and on its base indicator of criticality level was built.

Index terms: crisis, incident, criticality level of crisis, indicator, criteria set, criticality level assessment, loss, criticality class, expert methods, fuzzy sets theory.

Корченко Анна Олександрівна, кандидат технічних наук, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: annakor@ukr.net

Корченко Анна Александровна, кандидат технических наук, доцент кафедры безопасности информационных технологий Национального авиационного университета.
Anna Korchenko, PhD in Eng., Associate Professor of Academic Department of IT-Security, National Aviation University (Kyiv, Ukraine).

Козачок Валерій Анатолійович, кандидат технічних наук, доцент кафедри Інформаційної та кібернетичної безпеки Державного університету телекомунікацій.
E-mail: andriy.gizun@gmail.com
Козачок Валерий Анатолиевич, кандидат технических наук, доцент кафедры Информационной икибернетической безопасности Государственного университета телекоммуникаций.
Valerii Kozachok, PhD, Associate Professor of the Academic Department of Information and cyber security, State University of Telecommunications.

Гізун Андрій Іванович, асистент кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: andriy.gizun@gmail.com
Гизун Андрей Иванович, асистент кафедры безопасности информационных технологий Национального авиационного университета.
Andrii Gizun, Assistant of Academic Department of IT-security, National Aviation University.