НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ГІЗУН АНДРІЙ ІВАНОВИЧ

УДК 004.056.53:004.492.3

МЕТОДИ ТА ЗАСОБИ ОЦІНЮВАННЯ ПАРАМЕТРІВ БЕЗПЕКИ ДЛЯ ВИЯВЛЕННЯ КРИЗОВИХ СИТУАЦІЙ В ІНФОРМАЦІЙНІЙ СФЕРІ

Спеціальність 05.13.21 – «Системи захисту інформації»

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ – 2015

Дисертацією є рукопис

Робота виконана на кафедрі безпеки інформаційних технологій Національного авіаційного університету Міністерства освіти і науки України

Науковий керівник: кандидат технічних наук, доцент
Корченко Анна Олександрівна,
доцент кафедри безпеки інформаційних технологій
Національного авіаційного університету.

Офіційні опоненти: доктор технічних наук,
старший науковий співробітник
Кудін Антон Михайлович,
начальник управління Служби безпеки України.

кандидат технічних наук, доцент
Браіловський Микола Миколайович,
доцент кафедри комп'ютерних систем та мереж Державного університету телекомунікацій.

Захист відбудеться 01 жовтня 2015 р. о 13^{00} на засіданні спеціалізованої вченої ради Д 26.062.17 при Національному авіаційному університеті за адресою: 03680, м. Київ, пр. Космонавта Комарова, 1.

З дисертацією можна ознайомитись в науково-технічній бібліотеці Національного авіаційного університету.

Автореферат розісланий 31 серпня 2015 р.

Учений секретар
спеціалізованої вченої ради,
кандидат технічних наук, доцент Гнатюк С.О.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність. На сьогоднішній день інформаційні ресурси (ІР) стають одними з пріоритетних складових інформаційних систем (ІС) і вплив кризових ситуацій (КС) на них може мати вирішальне значення для забезпечення розвитку, функціонування і загалом існування організацій в сучасних умовах. Природа виникнення КС частіше всього носить нечіткий, невизначений характер, але як правило їм передують множини певних інцидентів. Частота і критичність інцидентів можуть породити подію з новою якістю – КС. Вчасне виявлення, стеження та реагування на інциденти дасть можливість створити такі важелі управління, які дозволять запобігти КС або мінімізувати їх наслідки. Таким чином виникає задача виявлення та ідентифікації інцидентів, що можуть спричинити появу КС, тобто інцидентів/потенційних КС (ІПКС). Слід зазначити, що для реалізації процедури управління КС, підбору адекватних і відповідних контрзаходів, застосування ефективних методів і засобів реагування на КС не достатньо лише виявити та ідентифікувати ІПКС. Оскільки, одним з головних принципів інформаційної безпеки (ІБ) є принцип адекватності захисту, що пов'язує витрати на захисні процедури з важливістю ІР та рівнем загрози спричиненої певною КС, то оцінка рівня критичності ситуації, що склалася в результаті появи ІПКС, є важливим етапом управління КС. Слід зазначити, що такі аспекти концепції управління безперервністю бізнесу (КУББ) як документаційне та організаційне забезпечення безперервності бізнесу (ЗББ), технічні рішення резервування ІР і ліквідації наслідків КС достатньо розвинені, однак практично відсутні системи виявлення, прогнозування та оцінки КС. Як зазначалося виникнення КС характеризується тим, що вони відбувається в умовах невизначеності і як правило потребують швидкого прийняття рішень. Тому використання апарату звичайної логіки, сигнатурних і статистичних методів, а також теорії ймовірностей, що застосовуються в більшості з відомих систем управління КС, не дає змогу забезпечити належну ефективність їх функціонування в нечітких умовах в слабоформалізованому середовищі. Також класичні підходи потребують значних часових витрат і виробничих ресурсів та пов'язані з необхідністю формування статистичних даних, процесами навчання систем тощо. Застосування апарату нечіткої логіки та експертних методів дає можливість суттєво усунути зазначені недоліки. Однак, такі системи на сьогодні розроблені для оцінки ризиків, виявлення кібератак, порушників і є вузькоспеціалізованими та не можуть застосовуватися на всіх етапах управління КС.

Значний вклад у розвиток КУББ і підходів, що пов'язані з управлінням КС внесли співробітники інституту BCI і DRII (Б. Альтерман, А. Бєляєв, Л. Бірд, Р. Лукичев, Т. Марш, Я. Мітров, С. Петренко), такі вітчизняні і зарубіжні вчені як Я. Ван Бон, Т. Зирянова, А. Качинський, В. Лифарь, І. Машкіна, М. Угрюмов, С. Харріс та інші. Побудові систем на основі застосування нечіткої логіки в задачах захисту інформації присвячені наукові праці А. Аверкіна, В. Волянської, В. Домрачева, Л. Заде, А. Корченко, О. Корченка, Т. Сааті, Н. Хованова та ін.

Однак, у зазначеній галузі залишається низка завдань, вирішення яких має важливе наукове та практичне значення. З цих позицій, розробка та дослідження моделей, методів і засобів управління КС у нечітких умовах, зокрема в ІС, *є актуальним науковим завданням.*

Зв'язок роботи з науковими програмами, планами, темами. Одержані результати дисертаційної роботи відображені у звітах держбюджетних науково-дослідних робіт Національного авіаційного університету («Нові методи і моделі систем виявлення кібертерористичних атак», № 0108U004007, «Організація систем захисту інформації від кібератак», № 0111U000171).

Мета і задачі дослідження. Метою дисертаційної роботи є розробка моделей, методів та засобів прогнозування, виявлення і ідентифікації ІПКС та оцінювання КС, що за рахунок застосування апарату нечіткої логіки та експертних підходів можуть використовуватися для слабоформалізованих нечітких середовищ.

Для досягнення поставленої мети необхідно розв'язати такі основні задачі:

- проаналізувати поняття і класифікації, що пов'язані з кризовими ситуаціями, сучасний стан розвитку теоретичної та практичної бази, методів і засобів, що застосовуються для вирішення задач КУББ та управління КС;
- розробити узагальнену класифікацію та на її основі інтегровану модель представлення множини ІПКС і визначити множину базових параметрів для виявлення ІПКС, на основі яких запропонувати формалізовані моделі еталонів для відображення і визначення стану параметрів середовища;
- на основі множини параметрів та моделі еталонів лінгвістичних змінних (ЛЗ) вдосконалити модель евристичних правил (ЕП), сформувати множини ЕП для виявлення ІПКС і формалізувати процес їх побудови;
- визначити множину базових параметрів для оцінки рівня критичності ситуації, спричиненої ІПКС та на основі ідентифікуючих і оціночних параметрів, інтегрованої моделі представлення інциденту, моделей еталонів та ЕП розробити методи виявлення ІПКС і оцінки критичності ситуації;
- на основі запропонованих методів розробити структурні рішення для розширення функціональних можливостей сучасних систем управління КС,
- розробити відповідне програмне забезпечення (ПЗ) та провести експериментальне дослідження нових технічних рішень, які дозволяють виявляти ІПКС та оцінити рівень їх критичності в умовах нечіткості.

Об'єктом дослідження є процес виявлення та оцінювання КС.

Предметом дослідження є класифікації, методи та інструментальні засоби оцінювання параметрів безпеки для виявлення КС.

Методи дослідження базуються на теоріях нечіткості, множин, прийняття рішень, моделювання інформаційних процесів та структур, алгоритмів, методах експертного оцінювання та м'яких обчисленнях.

Наукова новизна одержаних результатів полягає у такому:

- *вперше* розроблена узагальнена класифікація кризових ситуацій та на її основі інтегрована модель представлення інцидентів/потенційних кризових ситуацій, в якій за рахунок інтегрування ідентифікаторів інцидентів, підмножин можливих параметрів, нечітких лінгвістичних еталонів, поточних значень параметрів, евристичних правил і показника рівня критичності ситуації в шестикомпонентному кортежі, формуються базові оціночні та ідентифікуючі компоненти, за допомогою яких здійснюється відображення процесу виявлення кризових ситуацій;
- *отримали подальший розвиток* модель евристичних правил, в якій за рахунок логічних зв'язок між введеними множинами ідентифікуючих параметрів,

лінгвістичних ідентифікаторів та унікальних ідентифікаторів поточних станів, формуються множини необхідних евристичних правил для систем управління кризовими ситуаціями;

- *вперше* розроблені метод виявлення інцидентів/потенційних кризових ситуацій та метод оцінки критичності ситуації, що за рахунок обробки нечітких ідентифікуючих та оціночних параметрів, використання інтегрованої моделі представлення інциденту, моделей еталонів та евристичних правил, а також множин формування індикатора рівня критичності, дозволяє виявити інциденти/потенційні кризові ситуації та оцінити критичність ситуації, яка склалася внаслідок впливу зазначених інцидентів;
- *вперше* розроблені структурні рішення систем управління кризовими ситуаціями, які за допомогою блоків фазифікації ідентифікуючих параметрів, формування множин фазифікованих параметрів та ідентифікатора поточного стану, блоків визначення коефіцієнтів важливості, лічильника сенсорів параметрів, фазифікації оціночних параметрів, обрахунку показника рівня критичності і блоку дефазифікації результатів, дозволяють створити системи управління кризовими ситуаціями, які функціонують в нечіткому середовищі.

Практичне значення одержаних результатів. Отримані в дисертаційній роботі результати можуть бути використані для створення інструментальних засобів у вигляді програмних або програмно-апаратних модулів для виявлення ІПКС, прийняття рішень в умовах КС. *Практична цінність полягає в наступному:*

- використання запропонованих моделей та методів при розробці спеціального ПЗ для виявлення ІПКС та оцінки критичності ситуації, дозволило забезпечити високу ефективність та підвищити рівень автоматизації процесів управління КС і прийняття рішень, що підтверджується актами впровадження у діяльність ТОВ «Сайфер ЛТД» (акт впровадження від 19.11.2014 р.);
- розроблені комп'ютерні програми «Система виявлення ІПКС» та «Система оцінки критичності ситуації» використовується в навчальному процесі підготовки фахівців у галузі знань 1701 «Інформаційна безпека» для ідентифікації і виявлення інцидентів різного характеру в нечітких слабоформалізованих середовищах для підтримки прийняття рішень в умовах дії КС, а також оцінки рівня критичності ситуації, що є наслідком впливу ІПКС. Практичне використання результатів дисертаційного дослідження підтверджується актами впровадження у діяльність ТОВ «Hazon» (акт впровадження від 17.03.2015 р.) та навчальний процес Національного авіаційного університету (акт впровадження від 30.06.2015 р.);
- розроблено методику експерименту, що використовується для дослідження запропонованих засобів виявлення, ідентифікації та оцінки КС і застосована в навчальному процесі підготовки фахівців у галузі знань 1701 «Інформаційна безпека» дисципліни «Методологія та організація наукових досліджень» на кафедрах безпеки інформаційних технологій та засобів захисту інформації Національного авіаційного університету (акт впровадження від 30.06.2015 р.).

Особистий внесок здобувача. Основні положення і результати дисертаційної роботи, що виносяться до захисту, отримані автором самостійно. У роботах, написаних у співавторстві, автору належать: [1,6] – введені характеристики системи управління КС та розроблена базова архітектура; [2,10,13,16] – проведене дослі-

дження основних стандартів управління інцидентами ІБ та рекомендованих практик ЗББ, сучасних систем та методів управління КС, виявлення атак, вторгнень, порушника ІБ в ІС; [3,7,17] – запропоновані параметри ідентифікації та виявлення інцидентів ІБ різного характеру (комп'ютерних атак, вторгнень в ІС, особи порушника) та формалізовані процеси їх описання та вибору; [4,11,19] – запропоновано процес моделювання еталонів ЛЗ для задач управління КС; [5,12,18] – запропоновані підходи до побудови методів виявлення вторгнень, порушників в ІС і розроблено метод виявлення ІПКС; [8] – розроблена формалізована модель побудови множин ЕП для виявлення та ідентифікації ІПКС; [9] – запропонована множина універсальних параметрів оцінки критичності ситуації, що є наслідком впливу КС, та розроблено метод оцінки КС; [11] – запропонована інтегрована модель представлення ІПКС; [13,14] – проведений аналіз поняття «кризова ситуація» та суміжних понять, пов'язаних з процесами управління КС; [15] – запропонована універсальна узагальнена ознакова класифікація КС. З друкованих праць, що опубліковані у співавторстві, у дисертаційній роботі використовуються результати, отримані особисто здобувачем.

Апробація результатів роботи. Основні положення дисертаційної роботи доповідалися та обговорювалися на науково-технічних конференціях та семінарах: Всеукраїнська науково-практична конференція «Інфокомунікації – сучасність та майбутнє» (м. Одеса, 2011 р.); X, XI та XII Міжнародна науково-технічна конференція «АВІА» (м. Київ, 2011 р., 2013 р. та 2015 р.); XI і XV Міжнародна науково-практична конференція «Політ. Сучасні проблеми науки» (м. Київ, 2011 р. та 2015 р.); Міжвідомчий міжрегіональний семінар Наукової Ради НАН України «Технічні засоби захисту інформації» (м. Київ, 2012-2014 р.); II, V та VI Міжнародна науково-технічна конференція «ITSEC: Безпека інформаційних технологій» (м. Київ, 2012 р., 2014 р. та 2015 р.); VI Міжнародна науково-практична конференція «Інтегровані інтелектуальні робототехнічні комплекси» ІПРТК-2013 (м. Київ, 2013 р.); VI Всесвітній конгрес «Авіація у XXI столітті» – «Безпека в авіації та космічні технології» (м. Київ, 2014 р.) та інші.

Публікації. Основні положення дисертації опубліковано у 19 наукових працях, у тому числі 12 статей у фахових наукових виданнях (11 з яких входять до міжнародних наукометричних баз), 1 стаття у збірнику наукових праць та 6 тез доповідей і матеріалів конференцій.

Структура роботи та її обсяг. Дисертація складається зі вступу, чотирьох розділів, загальних висновків, додатків, списку використаних джерел і має 167 сторінки основного тексту, 48 рисунків, 40 таблиць, 49 сторінок додатків. Список літератури містить 160 найменувань і займає 16 сторінок. Загальний обсяг роботи 232 сторінки.

ОСНОВНИЙ ЗМІСТ

У **вступі** представлена загальна характеристика роботи, обгрунтована актуальність наукової теми, сформульовані мета і задачі дослідження, відображено наукову новизну та практичну цінність отриманих результатів і висновків, наведено дані щодо їх апробації та впровадження.

У **першому розділі** проведений аналіз вітчизняної та зарубіжної літератури щодо терміну «кризова ситуація» та суміжних понять. Встановлено, що усі вище-

названі явища та процеси, хоча і мають різний характер та природу, застосовуються в різних галузях, мають спільну множину характеристик і негативний вплив на життя людей, функціонування бізнес-процесів, держави, знижують ефективність управління ІР. На основі цього запропоноване визначення КС в аспекті ЗББ. В відомих класифікаціях КС не враховуються всі необхідні характеристики в межах однієї класифікації, тому для розробки засобів виявлення КС з інтегрованими можливостями необхідна узагальнена класифікація. Досліджено основні стандарти, методи, стратегії та технології ЗББ, проведений аналіз представлених на ринку систем та засобів КУББ. Проведене дослідження дало змогу виявити основні тенденції ринку даного сегменту, недоліки в існуючих засобах, оцінити можливість їх застосування щодо задач різного типу, їх універсальність. Аналіз показав, що значна частина розробок в даній галузі ґрунтується на застосуванні різноманітних сенсорів та порогового механізму за принципом компаратора. Недоліком таких систем є складність їх застосування в умовах невизначеності. Також відомі системи, в основі роботи яких закладені історичні, статистичні та математичні методи (статистичні закони розподілу, теорія ймовірностей, Байєсівські мережі тощо), які є надто ресурсоємними та трудомісткими. Також відсутні універсальні системи, що можуть бути застосовані в будь-якій галузі та на всіх етапах управління КС. Крім того практично повністю відсутні системи, що можуть використовуватися в менеджменті ІБ та функціонувати в умовах невизначеності. Таким чином, забезпечити ефективне управління КС в умовах нечіткості можна за рахунок використання моделей, методів та системних рішень, заснованих на нечіткій логіці.

Другий розділ присвячений розробці узагальненої класифікації КС за базовими характеристиками: причина походження подій (джерело), що може зумовити виникнення КС; можливість прогнозування; ступінь прояву; масштаб прояву КС (в географічному та організаційному аспекті); глибина вияву кризових явищ; характер виникнення; час дії негативних чинників КС; потенційна загроза людському життю та здоров'ю; кількість жертв; рівень економічних збитків, яка стала основою для побудови моделей та методів управління КС. Розроблена інтегрована модель представлення ІПКС, що відображена шестикомпонентним кортежем. Для розробки моделі була введена множина ІПКС, кожен з яких відображається у вигляді узагальненого шестикомпонентного кортежу $\mathbf{IKS_i} = < IKS_i, \mathbf{P_i}, \mathbf{T_i^e}, \mathbf{PP_i}, \mathbf{ER_i}, L\underset{\sim}{C}S_i >$, 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 $\mathbf{P_i}$; $\mathbf{PP_i}$ – підмножина поточних значень параметрів за певний проміжок часу; $\mathbf{ER_i}$ – підмножина ЕП, побудованих на основі нечітких параметрів, які використовуються для виявлення/ідентифікації i-го ІПКС; $L\underset{\sim}{C}S_i$ – показник рівня критичності ситуації, спричиненої i-м ІПКС. Ситуація відноситься до класу кризової лише якщо рівень її критичності достатній для цього, тобто $L\underset{\sim}{C}S_i \gtrsim B\underset{\sim}{C}^e$. В іншому разі інцидент взагалі залишається поза увагою

або проводиться реагування на нього з метою контролю і усунення як для звичайного інциденту.

Ідентифікатор IKS_i зв'язує елемент множини **ІКS** з певним інцидентом, який ідентифікується через відповідне йому ім'я, $\mathbf{IKS} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{IKS_i}\} = \mathbf{\{IKS_1, ..., IKS_n\}}$. Наприклад, при $n=5$: $\mathbf{IKS} = \{\mathbf{IKS_1}, ..., \mathbf{IKS_5}\} = \{\mathbf{ZL}, \mathbf{SP}, \mathbf{DD}, \mathbf{VA}, \mathbf{ZK}\}$, де $\mathbf{IKS_1 = ZL}$, $\mathbf{IKS_2 = SP}$, $\mathbf{IKS_3 = DD}$, $\mathbf{IKS_4 = VA}$, $\mathbf{IKS_5 = ZK}$ – відображають стани контрольованого середовища при відповідних ІПКС з ідентифікаторами «Злом ІС», «Спам», «Відмова в обслуговувані», «Вірусна атака» та «Вихід з ладу ІС через вплив кліматичних умов» відповідно.

Введена множина можливих параметрів **P** без прив'язки до конкретного типу ІПКС, $\mathbf{P} = \{\bigcup_{j=1}^{m} P_j\} = \{P_1,...,P_m\}, (j = \overline{1,m})$, де m – загальна кількість параметрів, та сформовані підмножини параметрів $\mathbf{P_i}$, що використовуються для ідентифікації i-го інциденту, $\mathbf{\{\bigcup_{i=1}^{n} P_i\}} = \{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{k_i} P_{ij}\}\} = \{\{P_{11},...,P_{1k_1}\}, ..., \{P_{n1},...,P_{nk_n}\}\}$, де n – загальна кількість ІПКС, k_i – кількість параметрів, що пов'язані з i-м інцидентом. Так при $m=13$: $\mathbf{P} = \{\bigcup_{j=1}^{13} P_j\} = \{P_1,...,P_{13}\} = \{Tlog, Nlog, CPU, MU, NEr, RTPr, CNCh, NCC, DbR, STF, T, H, D\}$ – відповідно «Час входу в систему», «Частота запитів на вхід у систему», «Завантаженість процесора», «Завантаженість оперативної пам'яті», «Кількість збоїв та помилок», «Час виконання процесу», «Завантаженість мереженого каналу», «Кількість одночасних підключень», «Затримка між запитами від одного джерела», «Розмір тимчасових файлів», «Температура в серверній кімнаті», «Вологість повітря в серверній кімнаті», та «Концентрація пилу в серверній кімнаті». Наприклад, при $n=5$, $k_1 = k_3 = 6$, $k_2 = k_4 = 5$, $k_5 = 3$ сформована підмножина $\mathbf{P_i}$, матиме вигляд: $\mathbf{\{\bigcup_{i=1}^{5} P_i\}} = \{\bigcup_{i=1}^{5}\{\bigcup_{j=1}^{k_i} P_{ij}\}\} = \{\{P_{11}, P_{12}, P_{13}, P_{14}, P_{15}, P_{16}\}, \{P_{21}, P_{22}, P_{23}, P_{24}, P_{25}\}, \{P_{31}, P_{32}, P_{33}, P_{34}, P_{35}, P_{36}\}, \{P_{41}, P_{42}, P_{43}, P_{44}, P_{45}\}, \{P_{51}, P_{52}, P_{53}\}\} = \{\{Tlog, Nlog, CPU, MU, NEr, RTPr\}, \{CPU, MU, NEr, RTPr, CNCh\}, \{CPU, MU, NEr, CNCh, NCC, DbR\}, \{CPU, MU, NEr, CNCh, STF\}, \{T, H, D\}\}$.

Компонент кортежу $\mathbf{T_i^e}$ визначає множину еталонів $\mathbf{\{\bigcup_{i=1}^{n} T_i^e\} = \{T_1^e, ..., T_n^e\}}$, $(i = \overline{1,n})$. Аналогічно до $\mathbf{P_i}$ сформуємо підмножину еталонів пов'язану з певним ІПКС $\mathbf{\{\bigcup_{i=1}^{n} T_i^e\} = \{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{k_i} T_{ij}^e\}\} = \{\{T_{11}^e,..., T_{1k_1}^e\}, ..., \{T_{n1}^e, ..., T_{nk_n}^e\}\}}$. Тоді $\mathbf{T_{ij}^e \subseteq T_i^e}$ ви-

значимо як: $\mathbf{T_{ij}^e} = \{\bigcup_{s=1}^{r_{ij}} \underset{\sim}{T}_{ijs}^e\} = \{\underset{\sim}{T}_{ij1}^e, \ldots, \underset{\sim}{T}_{ijr_{ij}}^e\}$, $(s = \overline{1,r_{ij}})$, де $\underset{\sim}{T}_{ijs}^e$ – еталоні нечіткі числа, а r_{ij} – кількість елементів (термів) в $\mathbf{T_{ij}^e}$. Тоді множина пов'язаних з ІПКС еталонів матиме такий вигляд: $\{\bigcup_{i=1}^{n} \mathbf{T_i^e}\} = \{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{k_i} \mathbf{T_{ij}^e}\}\} = \{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{k_i}\{\bigcup_{s=1}^{r_{ij}} \underset{\sim}{T}_{ijs}^e\}\}\} = \{\{\{\underset{\sim}{T}_{i11}^e, \ldots, \underset{\sim}{T}_{i1r_{11}}^e\}, \ldots, \{\underset{\sim}{T}_{ik_i1}^e, \ldots, \underset{\sim}{T}_{ik_ir_{ik_i}}^e\}\}, \ldots, \{\{\underset{\sim}{T}_{n11}^e, \ldots, \underset{\sim}{T}_{n1r_{n1}}^e\}, \ldots, \{\underset{\sim}{T}_{nk_n1}^e, \ldots, \underset{\sim}{T}_{nk_nr_{nk_n}}^e\}\}\}$. В роботі запропонована процедура побудови еталонів T_{ijs}^e, що здійснюється за кілька кроків: 1) формування множини **LE** та підмножини ідентифікаторів лінгвістичних оцінок (суджень) експертів $\mathbf{LE_{ij}} \subseteq \mathbf{LE}$ для характеристики поточного стану j-го параметра в певному середовищі $\mathbf{LE_{ij}} = \{\bigcup_{s=1}^{r_{ij}} LE_{ijs}\} = \{LE_{ij1}, \ldots, LE_{ijr}\}$, $(s = \overline{1,r_{ij}})$, де LE_{ijs} – ідентифікатор s-ї лінгвістичної оцінки j-го параметра; 2) формування множини ідентифікаторів інтервалів **N** і підмножини таких ідентифікаторів $\mathbf{N_{ij}} \subseteq \mathbf{N}$ відносно конкретного контрольованого параметра, де $\mathbf{N_{ij}} = \{\bigcup_{q=1}^{r_{ij}} N_{ijq}\} = \{N_{ij1}, \ldots, N_{ijr_{ij}}\}$, $(q = \overline{1,r_{ij}})$, а N_{ijq} – ідентифікатор q-го інтервалу, що використовується для формування на ньому частот зустрічання оцінок експерта по j-му параметру; 3) формування узагальненої таблиці оцінок, в якій фіксуються поточні твердження експертів відносно j-го параметра. Також сформовано таблиці з елементів емпіричних даних f_{ijsq}, які відображають 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 $F_{ij} = \|f_{ijsq}\|$; 4) формування похідної матриці частот $F_{ij}^{'} = \|f_{ijsq}^{'}\| = (vsm_{ij} / vs_{ijq})\|f_{ijsq}\|$, де $VS_{ij} = \left\|\sum_{s=1}^{r_{ij}} f_{ijs1}, \ldots, \sum_{s=1}^{r_{ij}} f_{ijsr_{ij}}\right\|$ – 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; 5) розрахунок матриці функцій належності $M_{ij} = \|\mu_{ijsq}\|$, що складається з елементів обчислюваних як $m_{ijsq} = f_{ijsq}^{'} / fm_{ijs}$, $(s,q = \overline{1,r_{ij}})$, де $FM_{ij} = \left\|\bigvee_{s=1}^{r_{ij}} f_{ijs1}^{'}, \ldots, \bigvee_{s=1}^{r_{ij}} f_{ijsr_{ij}}^{'}\right\|$ – вектор максимумів елементів кожного стовпця (ін-

тервалу). Результати обчислень дають змогу сформувати нечіткі терми $\underset{\sim}{T}_{ijs} = \{\bigcup_{q=1}^{r_{ij}} \mu_{ijsq} / x_{ijsq}\} = \{ \mu_{ijs1} / x_{ijs1},\ ...,\ \mu_{ijsr_{ij}} / x_{ijsr_{ij}}\}$, де $x_{ijsq} = N_{ijq}^{\max} / N_{ijr_{ij}}^{\max}$.

Підмножина $\mathbf{PP_i}$ формується на основі даних, що зняті з давачів контролю відповідних кожному інциденту параметрів середовища за певний період часу з заданим інтервалом, тобто $\mathbf{PP_i} = \{\bigcup_{j=1}^{k_i} \underset{\sim}{P}_{ij}\} = \{\underset{\sim}{P}_{i1}, ... , \underset{\sim}{P}_{ik_i}\}$, $j = \overline{1,k_i}$, де $\mathbf{PP_i} \subseteq \mathbf{PP}$. Встановлено, що поточні значення j-х параметрів з кожного набору $\mathbf{PP_i}$ 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 $LC_i = \{ \underset{j=1}{\overset{k_i}{\wedge}} t_j \} = \{ \underset{j=1}{\overset{k_i}{\wedge}} (\underset{\sim}{P}_{ij} \cong \underset{s=1}{\overset{r_{ij}}{\vee}} T_{ijs}^{e}) \}$, 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: $\mathbf{ER_i} = \{\bigcup_{i=1}^{n} \{ \bigcup_{p=1}^{R_i} ER_{ip} \}\} = \{\bigcup_{i=1}^{n} \{ \bigcup_{p=1}^{R_i} LC_{ip} \to LI_{ip} \}\} = \{\bigcup_{i=1}^{n} \{ \bigcup_{p=1}^{R_i} ER_{ip} = (LC_{ip} \to LI_{ip}) \}\}$, де ER_{ip} – p-те правило для виявлення та ідентифікації i-го ІПКС, яке буквально інтерпретується як: «Якщо LC_{ip} істинно, то можливість настання ІПКС буде LI_{ip}», а LI_{ip} – один з елементів множини лінгвістичних ідентифікаторів можливості реалізації ІПКС, необхідних для відображення судження експерта.

В роботі запропонований процес побудови множин ЕП, який представимо на прикладі створення правил при $i = 2$ для виявлення ІПКС «Спам», що пов'язаний з такими параметрами як $IKS_2 = SP \to P_2 = \{P_{21}, P_{22}, P_{23}, P_{24}, P_{25}\} = \{CPU, MU, NEr, RTPr, CNCh\}$, а LI_d може мати значення: «низька» (Н), «середня» (С), «підвищена» (П), «висока» (В), «критична» (К). Сформуємо набір ЕП $\mathbf{ER_2}$ для виявлення та ідентифікації даного ІПКС і представимо його фрагмент в вигляді таблиці 1, позначивши рівні параметрів: низький – Н, середній – С, високий – В, малий – М. Враховуючи всі можливі комбінації станів контрольованих параметрів можна сформувати 243 відповідних ЕП ER_{2p}, $p = \overline{1,243}$.

Таблиця 1

Набір правил ER_2 для виявлення спаму

p	$\underset{\sim}{P}_{CPU}$	$\underset{\sim}{P}_{MU}$	$\underset{\sim}{P}_{NEt}$	$\underset{\sim}{P}_{RTPr}$	$\underset{\sim}{P}_{CNCh}$	Рівень можливості реалізації ІПКС
1	Н	Н	М	М	Н	Н
2	Н	Н	М	М	С	Н
.....						
242	В	В	В	В	С	П
243	В	В	В	В	В	В

Використовуючи побудовані еталони, шляхом їх порівняння з поточними значеннями ідентифікуючих параметрів, і застосовуючи ЕП, ви-

значається оцінка експертом можливості реалізації ІПКС. Далі необхідною є оцінка критичності ситуації, що сформована під впливом даного інциденту. Встановлено, що рівень критичності можна описати, врахувавши функціональні залежності між L_e – параметрами оцінки рівня критичності. Наприклад, при $E = 15$ множина $\mathbf{L} = \{\bigcup_{e=1}^{E} L_e\} = \{L_1,...,L_E\}$ для оцінки критичності ситуації містить наступні параметри: «Тривалість інциденту», «Ступінь порушення функціоналу критичних ресурсів/процесів», «Географічний масштаб інциденту», «Масштаб інциденту в організаційному аспекті», «Загальний рівень економічних збитків», «Відношення рівня економічних збитків за поточний період до відповідного рівня за попередній період», «Рівень загрози життю та здоров'ю людей», «Питомий показник смертності на поточний момент», «Частота проявів інцидентів (інтенсивність)», «Ступінь руйнування інфраструктури», «Співвідношення орієнтовного часу відновлення і показника RTO», «Відношення рівня втрат ресурсів і показника RPO», «Рівень панічних, протестних та антидержавних настроїв персоналу/населення», «Ступінь впливу зовнішніх дестабілізуючих та психологічних чинників», «Ступінь порушення характеристик безпеки IP з обмеженим доступом».

Кожен з параметрів і результуючий рівень критичності КС можна описати використовуючи ЛЗ, що складається з певної кількості термів: $\mathbf{T_L} = \{\bigcup_{e=1}^{E}\{\bigcup_{s=1}^{r_e} \underset{\sim}{T}_{L_e s}\}\} =$

$\{\{\underset{\sim}{T}_{L_1 1},...,\underset{\sim}{T}_{L_1 r_1}\}, ..., \{\underset{\sim}{T}_{L_E 1},...,\underset{\sim}{T}_{L_E r_E}\}\}$, $\mathbf{T_{LCS}} = \{\bigcup_{s=1}^{r_{LCS}} \underset{\sim}{T}_{LCS}\} = \{\underset{\sim}{T}_{LCS1},..., \underset{\sim}{T}_{LCS_{r_{LCS}}}\} = \{\underset{\sim}{MH}, \underset{\sim}{HC}, \underset{\sim}{C}, \underset{\sim}{BC}, \underset{\sim}{MK}\}$, де МН – мінімальний, НС – нижче середнього, С – середній, ВС – вище середнього, МК – максимальний, $s = \overline{1,r}$, а r – кількість термів в ЛЗ.

Кожен інцидент характеризується рівнем критичності, що задається множиною $\mathbf{LCS} = \{\bigcup_{i=1}^{n} \underset{\sim}{LCS}_i\} = \{\underset{\sim}{LCS}_1,...,\underset{\sim}{LCS}_n\}$, $(i = \overline{1,n})$. Він визначається через параметри оцінки критичності ситуації з врахуванням їх вагових коефіцієнтів, тобто $\underset{\sim}{LCS}_i = \sum_{e=1}^{E} (\Omega_e * \underset{\sim}{L}_e)$. Сформувавши компоненти кортежу представимо ІПКС «Вірусна атака». Отже, для $\mathbf{IKS_4 = VA}$ та $k_4 = 5$, $r_{4j} = 3$ і $R_4 = 243$ інтегрована модель матиме такий вигляд: $\mathbf{IKS_4} = < IKS_4, \mathbf{P_4}, \mathbf{T_4^e}, \mathbf{PP_4}, \mathbf{ER_4}, \underset{\sim}{LCS}_4 > = < VA, \{P_{41}, P_{42}, P_{43}, P_{44}, P_{45}\}, \{\{\underset{\sim}{T}^e_{411}, \underset{\sim}{T}^e_{412}, \underset{\sim}{T}^e_{413}\}, \{\underset{\sim}{T}^e_{421}, \underset{\sim}{T}^e_{422}, \underset{\sim}{T}^e_{423}\}, \{\underset{\sim}{T}^e_{431}, \underset{\sim}{T}^e_{432}, \underset{\sim}{T}^e_{433}\}, \{\underset{\sim}{T}^e_{441}, \underset{\sim}{T}^e_{442}, \underset{\sim}{T}^e_{443}\}, \{\underset{\sim}{T}^e_{451}, \underset{\sim}{T}^e_{452}, \underset{\sim}{T}^e_{453}\}\}, \{\underset{\sim}{P}_{41}, \underset{\sim}{P}_{42}, \underset{\sim}{P}_{43}, \underset{\sim}{P}_{44}, \underset{\sim}{P}_{45}\}, \{ER_{41},...,ER_{4243}\}, \underset{\sim}{LCS}_4 > = < VA, \{CPU, MU, NEr, CNCh, STF\}, \{\{\underset{\sim}{T}^e_{VACPU1}, \underset{\sim}{T}^e_{VACPU2}, \underset{\sim}{T}^e_{VACPU3}\}, \{\underset{\sim}{T}^e_{VAMU1}, \underset{\sim}{T}^e_{VAMU2}, \underset{\sim}{T}^e_{VAMU3}\}, \{\underset{\sim}{T}^e_{VANEr1}, \underset{\sim}{T}^e_{VANEr2}, \underset{\sim}{T}^e_{VANEr3}\}, \{\underset{\sim}{T}^e_{VACNCh1}, \underset{\sim}{T}^e_{VACNCh2}, \underset{\sim}{T}^e_{VACNCh3}\}, \{\underset{\sim}{T}^e_{VASTF1}, \underset{\sim}{T}^e_{VASTF2}, \underset{\sim}{T}^e_{VASTF3}\}\}, \{\underset{\sim}{CPU}, \underset{\sim}{MU}, \underset{\sim}{NEr}, \underset{\sim}{CNCh}, \underset{\sim}{STF}\}, \{ER_{41},...,ER_{4243}\}, \underset{\sim}{LCS}_{VA} >$.

Третій розділ присвячений розробці методів управління КС та на їх основі системи виявлення ІПКС (СВІПКС) і системи оцінки критичності ситуації (СОКС).

Запропоновані методи розв'язання задач виявлення та оцінки КС, а саме: метод виявлення ІПКС; метод оцінки критичності ситуації. Вони базуються на методах: лінгвістичних термів з використанням статистичних даних (МЛТС) – для побудови еталонних значень параметрів та оціночних еталонів; лінійної апроксимації по локальним максимумам (ЛАЛМ) – для виконання нечітких математичних операцій; узагальненої відстані Хемінга (УВХ) – для порівняння поточних і еталонних значень параметрів. Також використовуються експертні методи оцінювання і ранжування: середніх рангів (СР) та попарного порівняння з визначенням квадратного кореня (ППВКК). Метод виявлення ІПКС (рис. 1) орієнтований на вирішення задачі виявлення інцидентів, в якому використовується теорія нечітких множин для прийняття рішення щодо факту наявності ІПКС, що реалізовано за 6 етапів: етап 1.1 – формування множин ІПКС та ідентифікуючих параметрів; етап 1.2 – формування зв'язки ІПКС з параметрами; етап 1.3 – формування еталонів нечітких параметрів; етап 1.4 – формування множини евристичних правил; етап 1.5 – фазифікація параметрів, що моніторяться з метою виявлення ІПКС; етап 1.6 – обробка поточних значень ідентифікуючих параметрів і формування результату.

Для розробки методу оцінювання критичності ситуації (рис. 2) скористаємось даними, що отримані за допомогою методу виявлення ІПКС. Метод засновується на шести етапах: **Етап 2.1 – формування множини оціночних параметрів.** На даному етапі задається множини оціночних параметрів **L** для визначення показника рівня критичності. **Етап 2.2 – формування ЛЗ для оцінки заданих параметрів та оціночних еталонів.** Етап орієнтований на створення ЛЗ $\underset{\sim}{T}_{L_e}$, які б дали змогу визначити оціночні параметри. Крім того задається оціночний еталон $\underset{\sim}{T}^{e}_{EL} = \{\underset{\sim}{MH}^{e},\ \underset{\sim}{HC}^{e},\ \underset{\sim}{C}^{e},\ \underset{\sim}{BC}^{e},\ \underset{\sim}{MK}^{e}\}$, що використовуються на наступних етапах для обчислення НЧ, які характеризують рівень критичності LCS. **Етап 2.3 – обчислення коефіцієнтів важливості (КВ) і ранжування оціночних параметрів.** Результатом етапу є формування вагових коефіцієнтів та проведення відповідно до них ранжування параметрів оцінки рівня критичності ІПКС. Для цього застосовується метод ППВКК, в якому експерт задає матрицю попарного порівняння $A = \|a_{ee'}\|$, елементи якої визначають його думку щодо пріоритетності того чи іншого параметра, а на основі неї обчислюються вагові коефіцієнти $\omega_e = \sqrt[n]{\prod_{e'=1}^{E} a_{ee'}}$ і отримані результати нормуються. **Етап 2.4 – фазифікація параметрів оцінки рівня критичності.** Етап орієнтований на створення НЧ, які відображають поточні значення оціночних параметрів, що визначаються за формулою $\underset{\sim}{L}_e = (\sum_{s=1}^{r} \underset{\sim}{T}^{E}_{L_e s}) / T$, де Т – загальна кількість вимірювань, $\underset{\sim}{T}^{E}_{L_e s}$ – поправочний еталон. Поправочні еталони формується з використанням механізму сенсорів. Сформоване НЧ порівнюється з відповідними еталонами $\underset{\sim}{T}_{Le}$ за методом УВХ. **Етап 2.5 – обчислення**

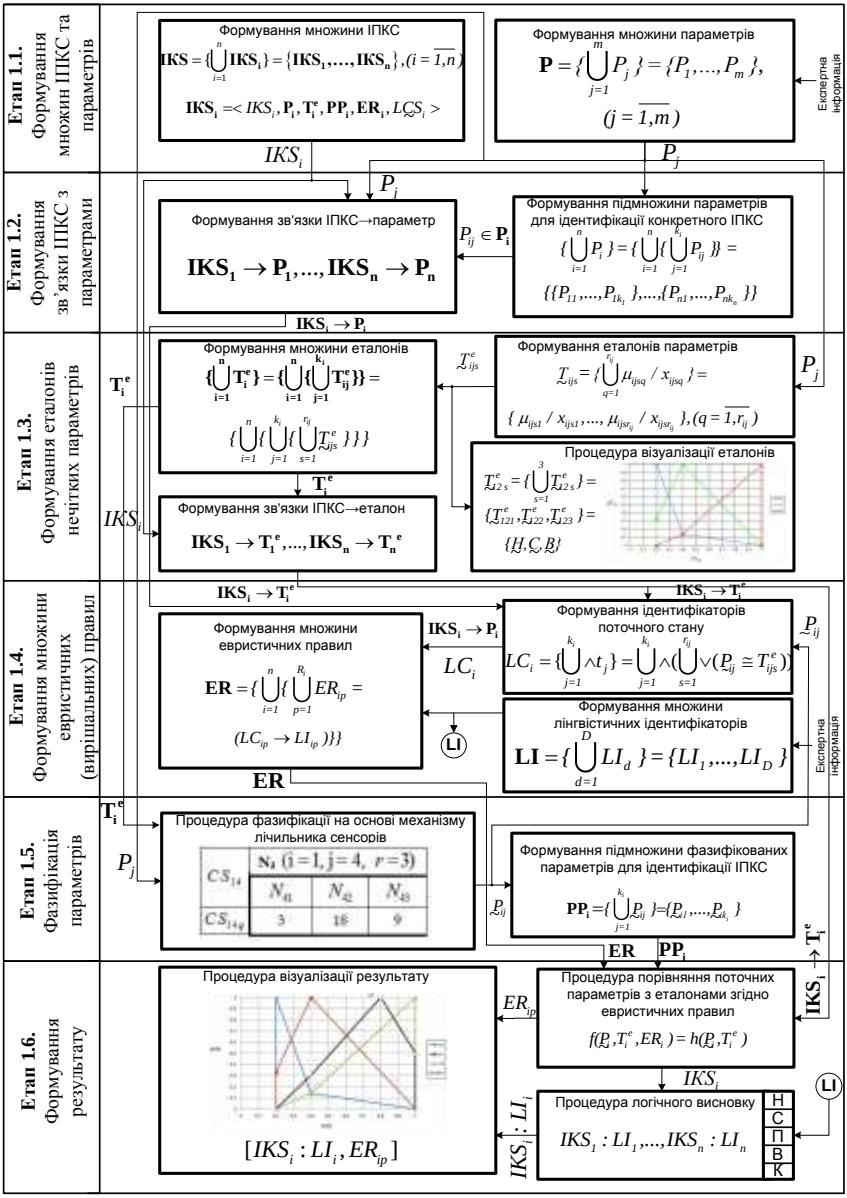

Рис.1. Схема відображення методу виявлення ІПКС

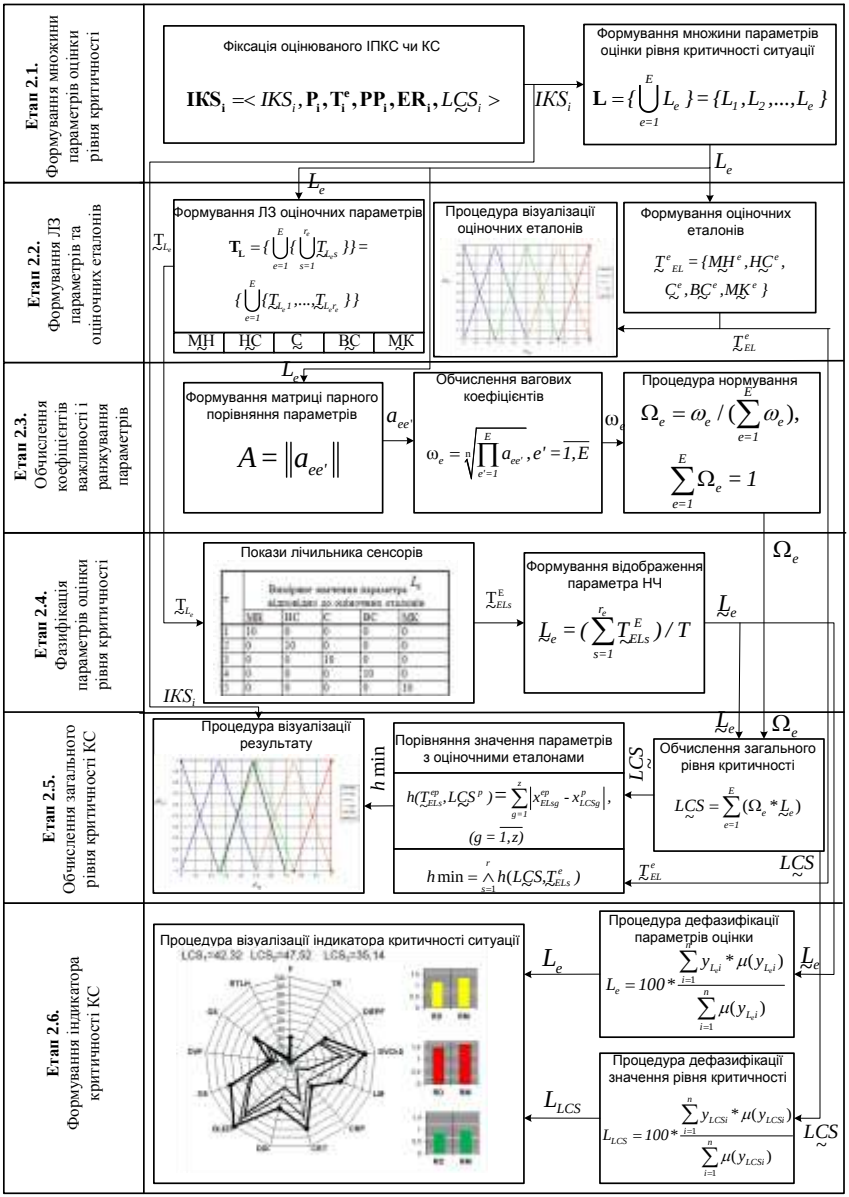

Рис. 2. Схема відображення методу оцінки критичності ситуації

загального рівня критичності. Результатом даного етапу є НЧ, що відображає загальний результуючий рівень критичності ІПКС. З врахуванням вагових коефіцієнтів кожного параметру рівень критичності можна задати як $\underset{\sim}{LCS} = \sum_{e=1}^{E} (\Omega_e * \underset{\sim}{L}_e)$, при цьому обчислення здійснюються за методом ЛАЛМ. Отримане НЧ $\underset{\sim}{LCS}$ та оціночні еталони $\underset{\sim}{T}^{e}_{EL}$ оброблюються за процедурою, в основі якої лежать метод α-рівневої номіналізації НЧ і метод визначення ідентифікуючих термів. Так, проводиться визначення УВХ $h\ (\underset{\sim}{T}^{ep}_{ELs}, \underset{\sim}{LCS}^{P}) = \sum_{g=1}^{z} \left| x^{ep}_{ELsg} - x^{p}_{LCSg} \right|$, де $(g = \overline{1,z})$ – кількість заданих α-рівнів. Критерієм відповідності $\underset{\sim}{LCS}$ одному з термів оціночного еталону є найменша УВХ $hmin_s = \bigwedge_{s=1}^{r_e} h\ (\underset{\sim}{LCS}, \underset{\sim}{T}^{e}_{ELs})$, де $s = \overline{1,r_e}$ – кількість термів в оціночному еталоні. Отриманий результат відображається в вигляді НЧ або графічно. Якщо поточний рівень критичності $\underset{\sim}{LCS}$ визначається термом $\underset{\sim}{ВС}$ (вище середнього) або $\underset{\sim}{МК}$ (максимальний) з еталону $\underset{\sim}{T}_{LCS}$, то приймається рішення, що ІПКС набуває характеристик КС. **Етап 2.6 – формування індикатора критичності КС.** На даному етапі проводиться процедура дефазифікації параметрів оцінки критичності та рівня критичності за методом центра ваги для відображення на 100 бальній шкалі за виразом $L = 100 * (\sum_{i=1}^{q} x_{L_q} * \mu(x_{L_q}) / \sum_{i=1}^{q} \mu(x_{L_q}))$. На основі значень вказаних оціночних параметрів формується індикатор рівня критичності ІПКС. Представлення результатів можливе в лінгвістичній та графічній формі.

На базі запропонованих методів розроблені структури нових системних рішень, що розширяють функціональні можливості сучасних систем управління КС в аспекті їх виявлення і оцінювання в умовах нечіткості: СВІПКС (рис. 3) та СОКС (рис. 4). Основне призначення СВІПКС є виявлення та ідентифікація ІПКС. Вхідними даними системи є ідентифікатори ІПКС, контрольовані нечіткі параметри та їх значення, а вихідними – ідентифікуючі дані та можливість реалізації ІПКС. Архітектура СВІПКС включає наступні структурні елементи як: система давачів (СД); модуль первинної обробки вхідних параметрів, що вміщує регістри ідентифікуючих параметрів (РІП) та ІПКС (РІПКС), блок формування зв'язки інцидент-параметр (БФЗІП); модуль вторинної обробки ідентифікуючих параметрів, що складається з блоків фазифікації ідентифікуючих параметрів (БФІП) та формування множин фазифікованих параметрів (БФКФП); модуль виконання нечітких арифметичних операцій, до якого відносяться блоки формування ідентифікатора поточного стану (БФІПС) і прийняття рішення (БПР); модуль формування еталонів та ЕП; модуль представлення результату, що містить блоки логічного висновку (БЛВ) та візуалізації (БВ); а також модуль управління режимами (МУР), що переводить систему в режим корекції еталонів (РКЕ) або режим корекції ЕП (РКЕП).

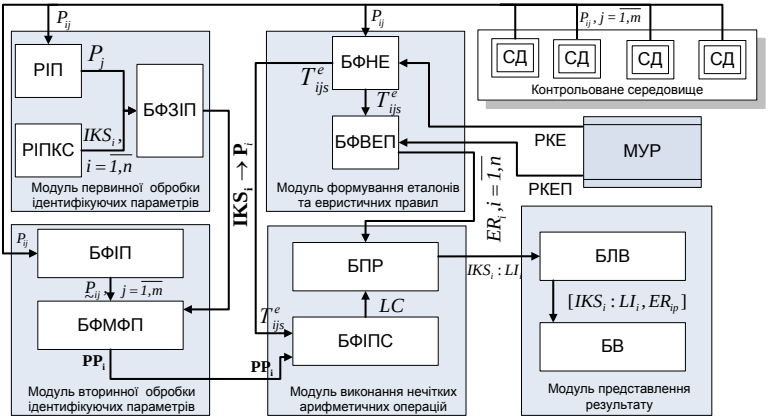

Рис. 3. Структура розробленої СВІПКС

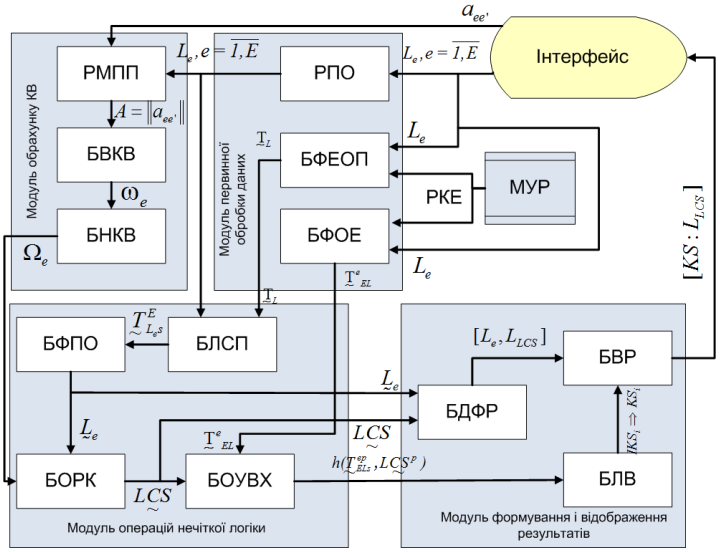

Рис. 4. Структура розробленої СОКС

В роботі описана процедура фазифікації контрольованих ідентифікуючих параметрів та параметрів оцінки рівня критичності, що є одним з ключових етапів роботи запропонованих СВ ІПКС і СОКС. Процедура заснована на використані сенсорів параметрів та побудові з їх використанням частот зустрічання значень відповідних параметрів. Застосування даної процедури дозволяє приймати рішення та використовувати СВОКС в слабоформалізованому нечіткому середовищі.

Четвертий розділ присвячено практичним реалізаціям та експериментальним дослідженням засобів виявлення ІПКС і оцінки КС. Розроблено базові алгоритми реалізації запропонованих систем, методику проведення експериментального дослідження, у якій визначено мету та задачі експерименту, вхідні та вихідні параметри, гіпотезу і критерії дослідження, а також послідовність необхідних дій. Для проведення експерименту було розроблено ПЗ «Система виявлення та ідентифікація ІПКС» (рис. 5) та «Система оцінки критичності ситуації» (рис. 6).

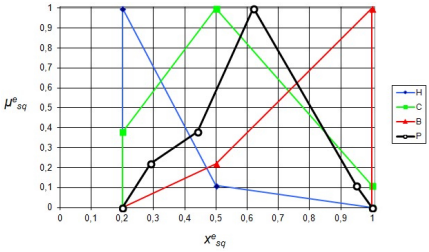

Рис. 5. Результат фазифікації поточного значення параметра MU і його порівняння з еталонними в СВІПКС

У процесі проведення експерименту за допомогою розробленої СВІПКС, відповідно до зазначених ідентифікуючих параметрів, було здійснене моделювання поточного стану середовища. Серед змодельованих 110000 ситуацій були задані 31411 таких, які можна характеризувати як відповідні для реалізації окремих ІПКС. Контроль усіх поточних станів середовища здійснювався за допомогою 2069 ЕП. Система успішно ідентифікувала всі змодельовані інциденти з зазначенням задіяних ЕП, за яким відбулось виявлення, причому 1397 ІПКС виявлено за правилом з лінгвістичним ідентифікатором «Критична» та 30014 – «Висока». Проведено дослідження впливу значень параметрів на отримані результати щодо виявлення ІПКС і підтверджена адекватність реагування системи на їх зміну.

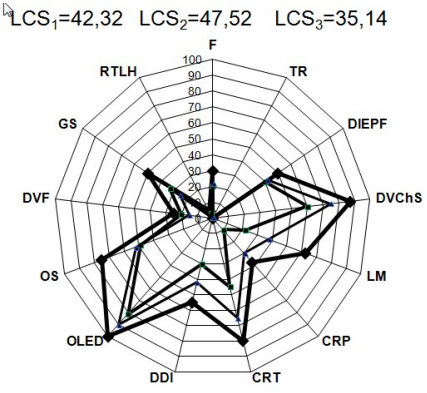

Рис. 6. Індикатор критичності ситуації, спричиненої ІПКС $IKS_3 = DD$ в СОКС

За допомогою СОКС була проведена оцінка критичності ситуацій, спричинених впливом ІПКС. На основі розроблених еталонів оціночних параметрів з врахування їх КВ та фазифікації поточних значень отримана оцінка критичності ситуації і сформований індикатор критичності. Так, було оцінено критичність збоїв роботи почтового сервера внаслідок проведення DDOS-атаки і ситуація в зоні землетрусу в моменти виникнення ситуації, в процесі розвитку та після застосування контрзаходів (при цьому змінювалися оціночні характеристики). Отриманий результат підтвердив адекватність розроблених еталонів і коректність вибору множини оціночних параметрів.

Отже, проведене експериментальне дослідження підтвердило адекватність запропонованих моделей, підбору множин оціночних та ідентифікуючих параметрів,

а також здатність побудованих на їх основі інструментальних засобів ефективно функціонувати в умовах слабоформалізованого нечіткого середовища. Використання теорії нечітких множин та експертних підходів дозволяє зменшити вимоги систем управління КС до ресурсів, розширити їхфункціональні можливості та область застосування, а також автоматизувати та прискорити процеси прийняття рішень в умовах впливу КС з врахуванням доцільності їх застосування.

У **додатках** вміщено акти впровадження результатів дисертаційної роботи та фрагменти кодів програм, що відображають практичну частину досліджень.

ВИСНОВКИ

Результатом виконаної роботи є розв'язання наукової задачі побудови і дослідження моделей, методів та інструментальних засобів, призначених для автоматизації, забезпечення ефективного функціонування та інформаційно-аналітичної підтримки процесів прийняття рішень в умовах кризової ситуації щодо захисту інформаційних ресурсів і реалізації концепції управління безперервністю бізнесу в аспекті управління кризовими ситуаціями. Запропоновані моделі, методи та інструментальні засоби можуть використовуватися як самостійно так і разом з іншими засобами захисту інформаційних ресурсів.

У процесі виконання дисертаційної роботи отримані такі вагомі результати:

1. В результаті аналізу поняття та класифікацій кризових ситуацій встановлено їх недоліки, зокрема неможливість відображення всіх необхідних характеристик в межах однієї класифікації. Дослідження сучасної теоретичної та практичної бази, систем та методів управління кризовими ситуаціями показали суттєві недоліки щодо їх використання в умовах нечіткості. Показано, що застосування методів і моделей нечіткої логіки та експертних підходів дасть змогу будувати ефективні системи управління кризовими ситуаціями для функціонування в нечіткому слабоформалізованому середовищі.
2. Вперше розроблена узагальнена класифікація та інтегрована модель представлення інцидентів/потенційних кризових ситуацій, які за рахунок інтегрування ідентифікаторів інцидентів, підмножин можливих параметрів, нечітких лінгвістичних еталонів, поточних значень параметрів, евристичних правил і показника рівня критичності ситуації в шестикомпонентному кортежі, дозволяють визначити базові оціночні та ідентифікуючі компоненти та можуть бути використаними для відображення процесу виявлення кризових ситуацій.
3. Отримала подальший розвиток модель евристичних правил, яка за рахунок використання логічних зв'язків між введеними множинами ідентифікуючих параметрів, лінгвістичних ідентифікаторів та унікальних ідентифікаторів поточних станів, пов'язаних зі значеннями ідентифікуючих параметрів, дозволяє сформувати множини необхідних евристичних правил для систем управління кризовими ситуаціями.
4. Вперше розроблено метод виявлення інцидентів/потенційних кризових ситуацій та метод оцінки критичності ситуації, що за рахунок обробки нечітких ідентифікуючих та оціночних параметрів, використання інтегрованої моделі представлення інциденту, моделей еталонів і евристичних правил та індикатора рівня

критичності, дозволяють виявляти інциденти/потенційні кризові ситуації і оцінити критичність ситуації, яка склалася внаслідок їх впливу в нечітких умовах.

5. На основі методів розроблені структурні рішення для розширення функціональних можливостей сучасних систем управління кризовими ситуаціями, які за рахунок використання блоків фазифікації ідентифікуючих параметрів, формування множин фазифікованих параметрів, формування ідентифікатора поточного стану, блоків визначення коефіцієнтів важливості, лічильника сенсорів параметрів, фазифікації оціночних параметрів, обрахунку показника рівня критичності і блоку дефазифікації результатів, дозволяють їх застосовувати в умовах нечіткості для задач виявлення та оцінки кризових ситуацій.

6. На основі запропонованих моделей, методів та нових структурних рішень розроблено відповідне програмне забезпечення для управління кризовими ситуаціями і проведені експериментальні дослідження запропонованих систем, які підтвердили адекватність побудованих моделей та достовірність теоретичних і практичних результатів дисертаційної роботи щодо можливості виявляти та оцінювати кризові ситуації. Зазначені результати впроваджені у діяльність ТОВ «Сайфер ЛТД», ТОВ «Hazon», Національного авіаційного університету, що підтверджено відповідними актами впровадження, які містяться у додатках до дисертаційної роботи.

ПУБЛІКАЦІЇ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Іванченко Є.В. Базова архітектура експертної системи прогнозування та попередження кризових ситуацій / Є.В. Іванченко, О.В. Гавриленко, А.І. Гізун // Захист інформації. – 2012. – № 3. – С. 94-104.

2. Волянська В.В. Огляд систем виявлення вторгнень на основі honeypot-технологій / В.В. Волянська, А.І. Гізун, В.О. Гнатюк // Безпека інформації. – 2012. – №2 (18). – С. 75-79.

3. 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.

4. 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.

5. 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.

6. 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.

7. Параметры прогнозирования и идентификации атак в информационно-коммуникационных системах / В. Азарсков, А. Гизун, А. Грехов, С. Скворцов // Захист інформації. – 2014. – 16, № 1. – С. 89-95.

8. 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.

9. 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.

10. Гізун А.І. Аналіз сучасних систем управління кризовими ситуаціями / А.І. Гізун, А.О. Корченко, С.О. Скворцов // Безпека інформації. – 2015. – Т.21. – №1. – С. 86-99 .

11. Карпінський М.П. Інтегрована модель представлення кризових ситуацій та формалізована процедура побудови еталонів ідентифікуючих параметрів / М.П. Карпінський, А.О. Корченко, А.І. Гізун // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2015. – В.1 (29). – С. 76-85.

12. Карпінський М.П. Метод виявлення інцидентів/потенційних кризових ситуацій / М.П. Карпінський, А.О. Корченко, А.І. Гізун // Захист інформації. – 2015. – Т.17. – №2. – С. 124-130.

13. Гізун А.І. Основні стратегії захисту інформаційних систем для забезпечення безперервності бізнесу / А.І. Гізун, О.І. Стасюк, В.О. Гнатюк // Защита информации: сборник научных трудов. – К. : НАУ, 2011. – Выпуск 18. – С. 65-75.

14. 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.

15. 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.

16. Волянська В.В. Нормативне та технічне забезпечення систем управління інцидентами інформаційної безпеки / А.І. Гізун, В.В. Волянська, В.О. Гнатюк // АВІА-2013 : XI міжнар. наук.-техн. конф., 21-23 травня 2013 р. : тези доп. – К. : НАУ, 2013. – С. 2.13-2.17.

17. Gizun A.I. Base parameters of forecasting and identification of computer attacks in information and communication systems / A.I. Gizun, S.I. Topcheev, M.O. Ryabyy // Proceedings the sixth world congress «Aviation in the XXI-st century». «Safety in Aviation and Space Technologies». – Vol. 1. – K. : NAU, 2014. – P. 1.11.40-1.11.44.

18. Гізун А.І. Метод виявлення та ідентифікації інцидентів-потенційних кризових ситуацій / А.І. Гізун, А.О. Корченко // АВІА-2015 : XII міжнар. наук.-техн. конф., 28-29 квітня 2015 р. : тези доп. – К. : НАУ, 2015. – С. 2.26-2.29.

19. Корченко А.А. Моделирование эталонов параметров для систем выявления кибератак / А.А. Корченко, А.И. Гизун // АВІА-2015 : XII міжнар. наук.-техн. конф., 28-29 квітня 2015 р. : тези доп. – К. : НАУ, 2015. – С. 2.34-2.37 .

АНОТАЦІЯ

Гізун А.І. Методи та засоби оцінювання параметрів безпеки для виявлення кризових ситуацій в інформаційній сфері. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації». – Національний авіаційний університет, Київ, 2015.

У роботі досліджено сучасний стан розвитку теоретичної та практичної бази, що використовується для реалізації завдань концепції управління безперервністю бізнесу, зокрема процесів управління кризовими ситуаціями, тобто їх виявлення, ідентифікацію та оцінку. Виявлено, що основним недоліком сучасних засобів в даній галузі є неможливість їх застосування в слабоформалізованому середовищі та значні вимоги до часових та виробничих ресурсів. З огляду на це, розроблено інтегровану модель представлення інцидентів/потенційних кризових ситуацій, визначено мно-

жини ідентифікуючих параметрів, характерних для визначених категорії інциденту, та оціночних параметрів щодо критичності ситуації, спричиненої інцидентом, формалізовано моделі параметрів та еталонів, а також сформовано модель евристичних правил виявлення та ідентифікації інцидентів/потенційних кризових ситуацій. Крім того, розроблено метод виявлення інцидентів/потенційних кризових ситуацій, метод оцінки критичності ситуації та нові структурні рішення системи виявлення інцидентів/потенційних кризових ситуацій і системи оцінки критичності ситуації, які дають можливість розширити функціональні можливості сучасних систем управління кризовими ситуаціями, а саме прогнозування, виявлення та ідентифікації інцидентів/потенційних кризових ситуацій і оцінки кризових ситуацій. Розроблено програмне забезпечення та проведено експериментальне дослідження, які підтвердили адекватність розроблених моделей, методів та систем.

Ключові слова: інформаційна безпека, інцидент/потенційна кризова ситуація, кризова ситуація, інформаційні системи, нечітка логіка, коефіцієнти важливості, евристичні правила, моделі еталонів лінгвістичних змінних, фазифікація, ідентифікуючі та оціночні параметри.

ABSTRACT

Gizun A.I. Methods and tools for evaluating the security settings to detect crisis in information sphere. – Manuscript.

Thesis for a Candidate of Technical Science degree in specialty 05.13.21 – «information security systems». – National Aviation University, Kyiv, 2015.

The thesis considers research of current state of development theoretical and practical base that is used to achieve the objectives concept of business continuity management, including crisis management processes, in other words their detection, identification and assessment. The main disadvantage of modern means in this field is the impossibility of their use in weakly-formalized environment and large demands to time and production resources. Considering this, developed integrated model for presenting incidents/potential crisis, defined identifying parameters set, specific to the defined incident categories, and evaluation parameters regarding the critical situation caused by the incident, formalized model of parameters and etalons, and also formed the model of heuristic detection rules and incidents/potential crisis identification. Among other things, developed method of incidents/potential crisis detection, method for evaluation criticality of the situation and new structural solution for detection incidents/potential crisis system, which enable to expand functionality of modern crisis management, namely forecasting, detection and identification of incidents/potential crisis and evaluation crisis. Software is developed and conducted experimental studies that confirmed the adequacy of the developed models, methods and systems.

Keywords: information security, incident/potential crisis, crisis, information system, fuzzy logic, importance factors, heuristic rules, models of linguistic variables etalons, fazzification, identifying and evaluation parameters.

АННОТАЦИЯ

Гизун А.И. Методы и средства оценивания параметров безопасности для выявления кризисных ситуаций. – Рукопись.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.21 – «Системы защиты информации». – Национальный авиационный университет, Киев, 2015.

В работе исследовано современное состояние развития теоретической и практической базы, используемой для реализации задач концепции управления непрерывностью бизнеса, включая процессы управления кризисными ситуациями, то есть их обнаружение, идентификацию и оценку. Выявлено, что основным недостатком современных средств в данной области является невозможность их применения в слабоформализированной среде и значительные требования к временным и производственным ресурсам, в частности потребность сбора статистических данных, подготовительного и обучающего этапов и прочее. Учитывая это, разработана интегрированная модель представления инцидентов/потенциальных кризисных ситуаций в виде шестикомпонентного кортежа, элементами которого являются: идентификатор инцидентов/потенциальных кризисных ситуаций; подмножество возможных идентифицирующих параметров; подмножество всех возможных эталонов; подмножество текущих значений параметров за определенный промежуток времени; подмножество эвристических правил, которые используются для выявления/идентификации инцидентов/потенциальных кризисных ситуаций; уровень критичности ситуации, вызванной инцидентом/потенциальной кризисной ситуацией. Определены множества идентифицирующих параметров, характерных для определенных категории инцидентов, и оценочных параметров относительно критичности ситуации, вызванной инцидентом. Формализированы модели параметров и эталонов, а также сформирована модель эвристических правил обнаружения и идентификации инцидентов/потенциальных кризисных ситуаций. Кроме того, разработан метод обнаружения инцидентов/потенциальных кризисных ситуаций, что за счет обработки нечетких идентифицирующих параметров дает принципиальную возможность выявить и идентифицировать инцидент/потенциальную кризисную ситуацию в определенной среде в нечетких условиях; метод оценки критичности ситуации, что за счет обработки нечетких оценочных параметров дает принципиальную возможность оценить критичность ситуации, сложившейся в результате воздействия инцидента или КС в определенной среде в нечетких условиях и структуру системы выявления инцидентов/потенциальных кризисных ситуаций и системы оценки критичности ситуации, которые дают возможность расширить функциональные возможности современных систем управления кризисными ситуациями, а именно прогнозирования, обнаружения и идентификации инцидентов/потенциальных кризисных ситуаций и оценки кризисных ситуаций. Разработано соответствующее программное обеспечение и проведено экспериментальное исследование, что заключалось в моделировании поточных состояний информационных систем, некоторые из которых соответствовали той или иной категории инцидентов информационной безопасности. Полученные результаты подтвердили адекватность разработанных моделей, методов и систем.

Ключевые слова: информационная безопасность, инцидент/потенциальная кризисная ситуация, кризисная ситуация, информационные системы, нечеткая логика, коэффициенты важности, эвристические правила, модели эталонов лингвистических переменных, фазификация, идентифицирующие и оценочные параметры.