УДК 004.056.53:004.492.3 (045)

ОБЧИСЛЮВАЛЬНИЙ КОМПЛЕКС ВИЯВЛЕННЯ ТА ОЦІНЮВАННЯ КРИЗОВИХ СИТУАЦІЙ В ІНФОРМАЦІЙНІЙ СФЕРІ

Андрій Гізун

Для ефективного забезпечення захищеності інформаційних ресурсів на сьогодні необхідно не тільки виявити кризову ситуацію, але і ідентифікувати її та оцінити рівень загрози інформаційній безпеці, спричинений нею. Більшість з відомих систем виявлення, прогнозування та оцінювання кризових ситуацій грунтуються на сигнатурному чи компараторному принципах. Таким чином вони не можуть використовуватися в нечіткому слабоформалізованому середовищі. Це створює перешкоди для їх функціонування в інформаційних системах при реальних умовах. Дану проблему вирішує застосування методів нечіткої логіки та експертних підходів. В даній статті запропонована базова архітектура нового структурного рішення: обчислювального комплексу, що складається з системи виявлення інцидентів/потенційних кризових ситуацій та системи оцінювання критичності ситуації. Архітектура комплексу представлена структурними модулями та блоками, що пов'язані логічно-функціональним зв'язками. Кожна система може використовуватися як окремо та незалежно одна від одної так і разом для задач управління кризовими ситуаціями в інформаційній сфері.

Ключові слова: *управління кризовими ситуаціями, інцидент/потенційна кризова ситуація, система виявлення інцидентів/потенційних кризових ситуацій, система оцінювання критичності ситуації, нечітка логіка, евристичні правила, експертна оцінка.*

Враховуючи стрімкий розвиток інформаційних технологій, що впливає як на захисні механізми так і на засоби для проведення інформаційних атак, набір можливих інцидентів/потенційних кризових ситуацій (ІПКС) значно збільшується. Безперервно зростає кількість загроз інформаційній безпеці, проводяться принципово нові кібератаки на інформаційні ресурси (ІР), що ускладнює реалізацію ефективного захисту. Досягнення максимального ефекту захищеності ІР можливе за умови роботи з відомими можливими ІПКС і вимагає обізнаності щодо рівня спричиненої ними загрози, що створює передумови для підбору та застосування найбільш відповідних заходів та засобів захисту. Дана задача ускладнюється тим, що атаки на ІР здійснюються в реальних умовах, тобто з великим показником випадковості та непередбачуваності. Дану проблему може вирішити застосування методів нечіткої логіки. В роботі [1] показана ефективність застосування математичного апарату нечіткої логіки для вирішення задач, пов'язаних з забезпеченням інформаційної безпеки.

Оскільки лише виявлення інциденту, враховуючи важливість захисту ІС зокрема та ІР загалом в поєднані з стрімким розвитком сучасних засобів та способів порушення інформаційної безпеки, на сьогодні є не достатнім. Виникає необхідність в їх ідентифікації, так як вибір контрзаходів є більш ефективним для конкретного і заздалегідь відомого інциденту. Проте для забезпечення підбору ефективних та дієвих контрзаходів не достатньо лише виявити чи ідентифікувати сам інцидент. На сьогодні є необхідною оцінка критичності інциденту, оскільки знаючи потенційний рівень загроз та ризиків, що можуть спричинятися ІПКС, значно спрощується завдання вибору адекватних заходів з ліквідації ІПКС та їх наслідків. Зрозумілим є той факт, що реагування на ІПКС з високим рівнем критичності, тобто кризові ситуації (КС), потребує великих об'ємів фінансових та матеріальних затрат, що в даному випадку є виправданим.

Тому надзвичайно важливим і актуальним науковим завданням є розробка обчислювального комплексу для виявлення та оцінювання кризових ситуацій, зокрема в інформаційній системі. Він вміщує в собі систему виявлення інцидентів/потенційних кризових ситуацій (СВІПКС), основне призначення якої – прогнозування або раннє виявлення та ідентифікація ІПКС та систему оцінки критичності ситуації (СОКС), яка надає можливість провести оцінку критичності ІПКС і сформувати висновок про можливість його розгляду як КС, а в подальшому підібрати відповідні контрзаходи.

Отже, метою даної статті є розробка обчислювального комплексу виявлення та оцінювання кризових ситуацій в інформаційній сфері на базі нечіткої логіки, що може бути використаний в нечіткому слабоформалізованому середовищі

На сьогодні аналогічних систем практично немає. Подібні системи для виявлення вторгнень, комп'ютерних атак, системи промислової і виробничої безпеки засновані на теорії ймовірності і ґрунтуються на сигнатурному або компараторному принципах [2]. Такий підхід не дозволяє ви-

являти невідомі атаки чи інциденти, контролювати слабоформалізований простір. Крім того для таких систем необхідний довготривалий підготовчий етап перед введенням їх в експлуатацію. В рамках такої підготовки зазвичай проходить вибірка статистичних даних, навчання системи тощо [1, 3]. Тому при розробці даної системи будемо використовувати підходи засновані на нечіткій логіці та експертні методи, що позбавлені таких недоліків. Слід також згадати подібні системи на базі нечіткої логіки для виявлення аномального стану [4], порушника ІБ [5], а також прототип даної системи [6].

Запропонований в роботі комплекс складається з двох систем СВІПКС і СОКС, основним призначенням яких є виявлення загрозливих для підприємства чи організації інцидентів і оцінка їх рівні критичності відповідно. Базова архітектура обчислювального комплексу представлена на рис. 1.

Призначенням СВІПКС є виявлення та ідентифікація ІПКС. Вхідними даними системи є ідентифікатори ІПКС, контрольовані параметри та їх значення. На виході системи – інформація щодо ІПКС, його ймовірності та ідентифікуючі дані. Функціональні особливості СВІПКС визначаються методом виявлення ІПКС [7, 8], технічною реалізацією якого і є запропонована система.

Архітектура СВІПКС представлена на рисунку 1. Вона включає такі структурні елементи як: система датчиків (СД); модуль первинної обробки вхідних параметрів, що вміщує регістри ідентифікуючих параметрів (РІП), регістри ІПКС (РІПКС), блок формування зв'язки інцидент-параметр (БФЗІП); модуль вторинної обробки ідентифікуючих параметрів, що складається з блоку фазифікації ідентифікуючих параметрів (БФІП) та блоку формування кортежів фазифікованих параметрів (БФКФП); модуль виконання нечітких арифметичних операцій, до якого відносяться блок формування ідентифікатора поточного стану (БФІПС) і блок прийняття рішення (БПР); модуль формування еталонів та евристичних правил, до складу якого входять однойменні відповідні блоки (БФНЕ та БФЕП відповідно); модуль представлення результату, що містить блок логічного висновку (БЛВ) та блок візуалізації (БВ); а також модуль управління режимами (МУР), що переводить систему в режим корекції еталонів (РКЕ) або режим корекції евристичних правил (РКЕП) за рішенням оператора системи чи експерта, якщо така потреба виникає.

В контрольованому середовищі (ІС, внутрішнє середовище будівель та приміщень, зовнішнє середовище певних територій, населених пунктів, держави тощо), що є нечітким та слабоформалізованим, розміщена СД. В залежності від типу середовища датчики можуть бути різного роду – технічні, екологічні, фізичні і т.п. Так в ІС в якості датчиків використовуються програмні та апаратні засоби для фіксації мережевих та хостових параметрів, наприклад tcpdump для контролю трафіку, програмний засіб Everest для визначення завантаженості CPU, оперативної пам'яті тощо чи їх аналоги. В серверній використовуються датчики температури, гігрометри для визначення рівня вологи, датчики наявності пилу, диму і т.д. Склад СД залежить від поставлених цілей і області застосування.

В модулі первинної обробки вхідних параметрів задаються ІПКС, які система прогнозує виявляє та ідентифікує, а також відповідні їм ідентифікуючі параметри. В РІПКС заносяться ідентифікатори основних класів інцидентів $IKS_i, i = \overline{1,n}$ (див. вираз (1) в [9]), а в РІП аналогічно заносяться з певною періодичністю поточні значення ідентифікуючих параметрів $P_{ij}, i = \overline{1,n}, j = \overline{1,m}$, що визначені і описані в (див. вираз (3) в [9]) [9, 10, 11]. В БФЗІП формуються зв'язки $\mathbf{IKS_i \rightarrow P_i}$ конкретного типу ІПКС з параметрами, що необхідні для його виявлення. Так для окремих ІПКС створюються підмножини $\mathbf{P_i}$ [11].

Модуль вторинної обробки ідентифікуючих параметрів призначений для фазифікації ідентифікуючих параметрів та подальшого їх групування відповідно до ІПКС, які вони визначають. В БФІП проводиться процедура фазифікації, яка полягає в перетворені виміряних поточних параметрів за певний період в НЧ, в результаті формуються підмножини $\mathbf{PP_i}$, що в даному випадку складатимуться з таких елементів як $\tilde{Tlog}$, $\tilde{Nlog}$, $\tilde{CPU}$, $\tilde{MU}$, $\tilde{NEr}$, $\tilde{RTPr}$, $\tilde{CNCh}$, $\tilde{NCC}$, $\tilde{DbR}$, $\tilde{STF}$, $\tilde{T}$, $\tilde{H}$, $\tilde{D}$, де $Tlog$ – «Час входу в систему», $Nlog$ – «Частота запитів на вхід у систему», CPU – «Завантаженість процесора», MU – «Завантаженість оперативної пам'яті», NEr – «Кількість збоїв та помилок», $RTPr$ – «Час виконання процесу», $CNCh$ – «Завантаженість мереженого каналу», NCC – «Кількість одночасних підключень», DbR – «Затримка між запитами від одного джерел», STF – «Розмір тимчасових файлів», T – «Температура в серверній кімнаті», H – «Вологість повітря в серверній кімнаті», D – «Концентрація пилу в серверній кімнаті».

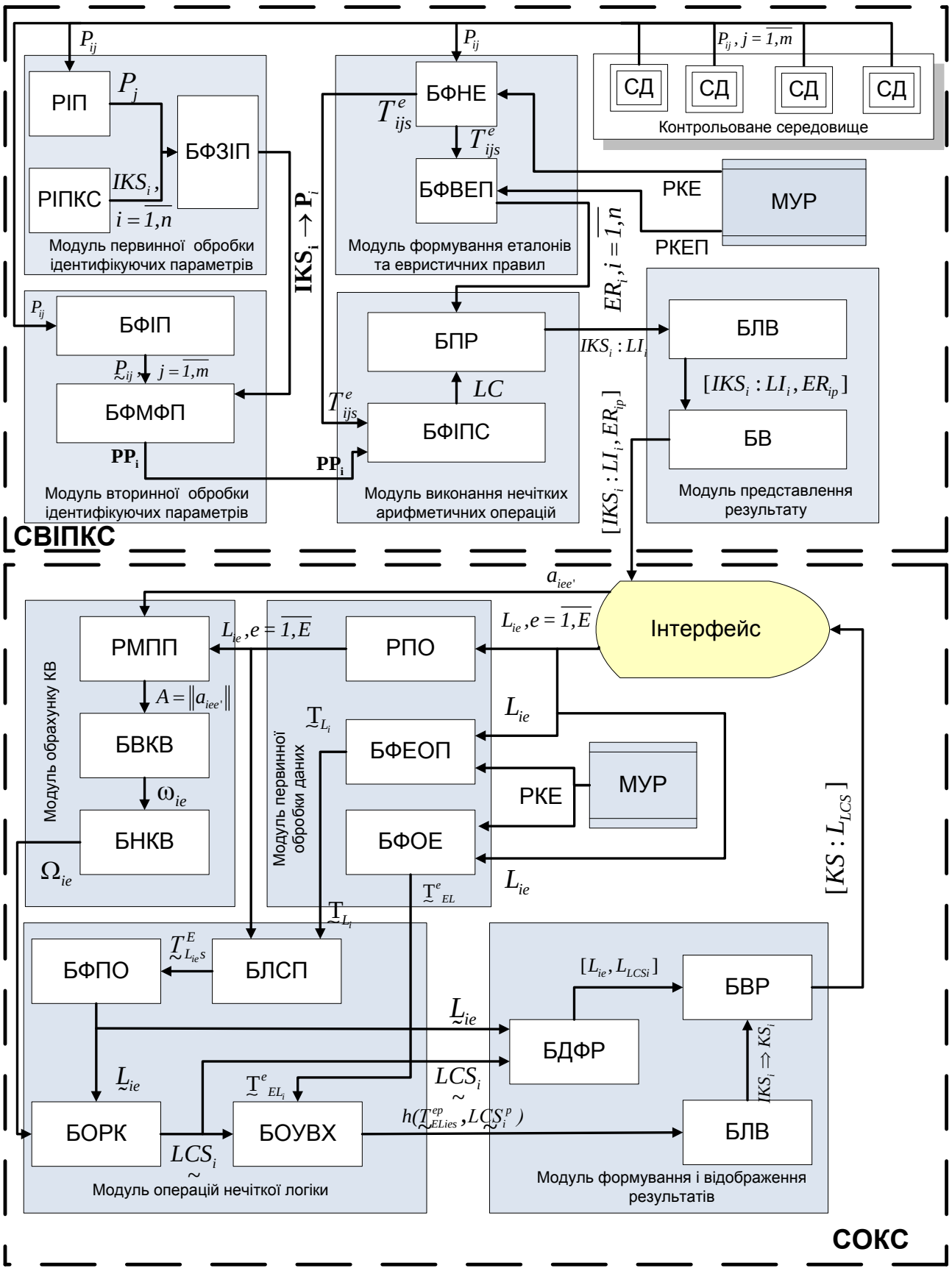

Рис. 1. Обчислювальний комплекс виявлення та оцінювання КС

В БФКФП уже фазифіковані ідентифікуючі параметри групуються в підмножини у відповідністю з сформованими в БФЗІП зв'язками.

В модулі формування еталонів та евристичних правил формуються еталонні величини, необхідні для виміру поточних значень контрольованих параметрів та евристичні правила для прийняття рішення. БФНЕ призначений для створення експертами множини еталонів ідентифікуючих параметрів $\{\bigcup_{i=1}^{n} T_i^e\} = \{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{k_i} T_{ij}^e\}\} = \{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{k_i}\{\bigcup_{s=1}^{r_{ij}} T_{ijs}^e\}\}\}$ [12]. В БФЕП у процесі зіставлення ідентифікаторів поточного стану $LC_i = \{\underset{j=1}{\overset{k_i}{\wedge}} t_j\} = \{\underset{j=1}{\overset{k_i}{\wedge}} (P_{ij} \cong \underset{s=1}{\overset{r_{ij}}{\vee}} T_{ijs}^e)\}$, що визначається комбінацією значень поточних параметрів, та лінгвістичних ідентифікаторів можливості реалізації ІПКС формується набір правил $\mathbf{ER} = \{\bigcup_{i=1}^{n} \mathbf{ER_i}\} = \{\mathbf{ER_1}, ..., \mathbf{ER_n}\}$ для всіх заданих інцидентів, тобто $\mathbf{ER_i} = \{\bigcup_{i=1}^{n}\{\bigcup_{p=1}^{R_i} LC_{ip} \to LI_{ip}\}\}$, де LI_{ip} – лінгвістичний ідентифікатор можливості реалізації ІПКС, а R_i – загальна кількість можливих правил, спрямованих на виявлення *i*-ого ІПКС [13].

Утворені еталони та евристичні правила є основними експертними даними, що забезпечують роботу СВІПКС. Вони задаються перед початком роботи системи з виявлення ІПКС. Існує можливість їх корекції. Для цього МУР переводить в систему в РКЕ або РКЕП, під час яких еталони та ЕП можуть бути змінені експертом чи оператором системи.

Призначення модуля виконання нечітких арифметичних операцій полягає в порівнянні поточних значень параметрів з еталонними і визначені ЕП, що узгоджує поточну ситуацію, тобто прийняті рішення щодо факту існування чи можливості появи ІПКС. В БФІПС виміряні і фазиковані ідентифікуючі параметри з використанням методу узагальненої відстані Хемінга порівнюються з еталонами, визначаючи відповідні (найбільш близькі) поточній ситуації терми, і на основі цього формується ідентифікатор поточного стану. В БПР LC порівнюється з наборами ЕП, в процесі чого шукається правило, що погоджує поточний ідентифікатор. Ймовірність появи ІПКС прирівнюється значенню лінгвістичного ідентифікатора можливості реалізації ІПКС LI_{ip} правила, що спрацювало.

Призначення модуля представлення результату полягає в відображені отриманих результатів в зрозумілій для оператори системи вигляді. Отриманий результат може бути відображений в лінгвістичній формі. В БЛВ конкретній поточній ситуації присвоюється відповідний їй ідентифікатор ІПКС і ймовірність його реалізації, що відповідає лінгвістичному ідентифікатору правила, що його ідентифікував, тобто $IKS_i : LI_i$ [7]. Крім того здійснюється прив'язка до правила, за яким ІПКС був ідентифікований. В БВ формується остаточний результат і виводиться на екран оператора системи. На екрані відображені наступні дані: конкретний тип ІПКС, лінгвістичний ідентифікатор імовірності його реалізації та використовуване правило: $[IKS_i : LI_i, ER_{ip}]$ [7].

Після виявлення інциденту його необхідно оцінити. Для цього використовується СОКС, яка, крім того, може використовуватися окремо від СВІПКС для оцінювання критичності заданого інциденту або поточної ситуації. Робота системи заснована на методі оцінки рівня критичності для систем управління КС, що описаний в [14]. Основним її призначення є оцінка рівня критичності ІПКС і прийняття рішення чи є цей інцидент КС. Вхідними даними у системі є інформація щодо ідентифікованого ІПКС, параметри оцінки рівня критичності та їх значення. Вихідні дані – рівень критичності ситуації і, у випадку якщо цей рівень перевищує допустимі значення, ідентифікуючі дані КС.

До складу СОКС входять: модуль первинної обробки даних, що складається з регістри параметрів оцінки рівня критичності (РПО), блоку формування еталонів параметрів оцінки (БФЕПО) та блоку формування оціночних еталонів (БФОЕ); модуль обрахунку коефіцієнтів важливості (КВ), який містить у собі регістри матриці попарного порівняння (РМПП), блок визначення КВ (БВКВ) і блок нормування КВ (БНКВ); модуль операцій нечіткої логіки, до якого входять блок лічильника се-

нсорів параметрів (БЛСП), блок фазифікації оціночних параметрів (БФОП), блок обрахунку рівня критичності (БОРК) і блок обчислення відстані Хеммінга (БОВХ); модуль формування і відображення результатів, до складу якого входять блок дефазифікації результатів (БДФР), блок логічного висновку (БЛВ), блок візуалізації результатів (БВР), а також як і в СВІПКС модуль управління режимом роботи системи (МУР), що забезпечує функціонування режиму корекції еталонів (РКЕ) та інтерфейс користувача (експерта або оператора).

В модулі первинної обробки даних ініціалізуються параметри для оцінки рівня критичності: $L_1 = TR,\quad L_2 = DVF,\quad L_3 = GS,\quad L_4 = OS,$ $L_5 = OLED,\quad L_6 = RD,\quad L_7 = RTLH,\quad L_8 = RM,$ $L_9 = F,\quad L_{10} = DDI,\quad L_{11} = CRT,\quad L_{12} = CRP,$ $L_{13} = LM,\quad L_{14} = DIEPF,\quad L_{15} = DVChS$ – відповідно «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)», «Степінь руйнування інфраструктури», «Співвідношення орієнтовного часу відновлення і показника RTO», «Відношення рівня втрат ресурсів і показника RPO», «Рівень панічних, протестних та антидержавних настроїв персоналу/населення», «Степінь впливу зовнішніх дестабілізуючих та психологічних чинників», «Степінь порушення характеристик безпеки ІР з обмеженим доступом» [14]. А також формуються еталони параметрів та оціночні еталони. Значення параметрів оцінки рівня критичності та їх ідентифікатори з множини $\mathbf{L_e}$ заносяться до РПО. В БФЕПО за участю експерта параметричним методом формування НЧ будуються еталони, які відображаються відповідними термами. В БФОЕ будується оціночний еталон з аналогічними термами для визначення рівня критичності шляхом його порівняння з обрахованим значення рівня критичності ситуації.

Модуль обрахунку КВ функціонує з метою формування вагових коефіцієнтів, що визначають важливість (пріоритетність) параметрів в порівнянні один з одним. Оцінка важливості проводиться експертом з урахуванням умов функціонування ІС чи інших об'єктів, на які впливає ІПКС, галузі застосування, набору потенційних загроз тощо. В РМПП заносяться елементи матриці попарного порівняння $A=\|a_{iee'}\|$, що визначають думку експерта щодо пріоритетності того чи іншого параметра стосовно впливу ІПКС на контрольований об'єкт. В БОКВ розраховуються КВ для кожного параметра за формулою $\omega_e = \sqrt[n]{\prod_{e'=1}^{E} a_{iee'}}, e' = \overline{1,E}$, а в БНКВ проходить процедура їх нормування.

Модуль операцій нечіткої арифметики призначений для обробки значень параметрів оцінки рівня критичності та визначення рівня критичності з застосуванням методів нечіткої логіки та експертних підходів. В БЛСП реалізований механізм сенсорів, що покладений в основу процедури фазифікації [14,15]. Виміряні поточні значення параметрів оцінки рівня критичності визначають покази лічильника сенсорів кожного параметра в відповідності з заданими інтервалами термів еталонів параметрів. На виході БЛСП формуються так звані поправочні еталони $\underset{\sim}{T}^{E}_{ELis}$. На їх основі в БФОП проводиться фазифікація поточних значень параметрів, під час якої формується НЧ, що відображає рівень параметрів за певний період часу отриманий шляхом проведення Т вимірювань. Оскільки задані експертами еталони параметрів оцінки рівня критичності задані параметричним способом і мають трикутну форму, то сформоване НЧ, наприклад, для параметра $\underset{\sim}{L}_{14}$ «Ступінь впливу зовнішніх дестабілізуючих та психологічних чинників» може мати такий вигляд:

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

$$(5*\underset{\sim}{НС}^{e} + 2*\underset{\sim}{ВС}^{e})/10 = \{0/0{,}25;\ 1/0{,}5;\ 0/0{,}75\}.$$

В БОРК проводиться обрахунок рівня критичності за виразом $\underset{\sim}{LCS}_i = \sum_{e=1}^{E} (\Omega_e * \underset{\sim}{L}_{ie})$ з використ-

танням ЛАЛМ при додаванні нечітких значень параметрів. В БОВХ з використанням методу, описаного в [16], обчислюється узагальнена відстань Хемінга (УВХ) між отриманим значенням рівня критичності ситуації та термами оціночного еталону.

Модуль формування і відображення результатів реалізує формування кінцевого результату системи і відображення його в формі зрозумілій оператору. В БЛВ за отриманим рівнем критичності система приймає рішення чи оцінюваний ІПКС є КС Для цього обраховані УВХ порівнюються між собою і знаходиться мінімальна, а отриманий в результаті терм і буде відповідати рівню критичності. У випадку якщо $L\tilde{C}S_i \gtrsim BC_{EL}^e$ ІПКС переходить у ранг КС. В БДФР отримані значення параметрів оцінки та загального рівня критичності обробляються одним з відомих методів [1] таким чином, щоб приставити їх у вигляді чітких чисел. БВР відображає одержані дані в зручній користувачу форму. Так, тут формується індикатор рівня критичності, в якому відображаються значення параметрів та рівня критичності, а також ідентифікатор ІПКС, що спричинив дану КС. За необхідності можливе відображення інформації щодо ІПКС, отриманої в процесі роботи СВІПКС, а також загального рівня критичності ситуацій в формі ЛЗ або графічно.

Для переведення СОКС в режим корекції еталонів по аналогії з СВІПКС застосовується МУР. Інтерфейс реалізує процеси вводу/виводу інформації експертом чи оператором системи.

Висновки

В статті запропоноване нове структурне рішення обчислювального комплексу виявлення та оцінки критичних інцидентів 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. На їх основі можна розробляти алгоритмічне, програмне і програмно-апаратне забезпечення в даній сфері.

За рахунок застосування методів виявлення ІПКС та оцінки критичності ситуації, розроблених на базі нечіткої логіки та експертних підходів, обчислювальний комплекс може бути використаний в нечіткому слабоформалізованому середовищі, якому відповідають реальні умови, а також не потребують великих затрат часових і виробничих ресурсів для збирання та опрацювання статистичних даних, обробки складних математичних моделей теорії імовірності. Запропоновані системи можуть використовуватись автономно одна від одної, як окремий обчислювальний комплекс або як складова комплексної системи захисту інформації.

ЛІТЕРАТУРА

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

[2]. 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. 87-101.

[3]. Корт С.С. Структура систем обнаружения нарушителя (СОН) [Електронній ресурс]: стаття / С.С. Корт. – Режим доступу: World Wide Web. – http://www.ssl.stu.neva.ru/sam/.

[4]. Корченко А.А. Система выявления аномального состояния в компьютерных сетях / А.А. Корченко // Безпека інформації. – 2012. – № 2 (18). – С. 80-84.

[5]. Корченко А.О. Система виявлення та ідентифікації порушника в інформаційно–комунікаційних мережах // А.О. Корченко, В.В. Волянська, А.І. Гізун / Безпека інформації. – 2013. – Т.19. – №3. – С. 158-162.

[6]. 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.

[7]. 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.

[8]. Gizun A. Approaches to Improve the Activity of Computer Incident Response Teams / A. Gizun, V. Gnatyuk, N. Balyk, P. Falat // Proceedings of the

2015 IEEE 8th International Conference on "Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications" (IDAACS'2015), Warsaw, Poland, September 24-26, 2015: Vol. 1. – Pp. 442-447.

[9]. 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.

[10]. 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.

[11]. 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.

[12]. 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. – №1 (19). – 2013. – С. 13-21.

[13]. 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.

[14]. 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.

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

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

REFERENCES

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

[2]. Gizun A.I., Korchenko A.O., Skvortsov S.O. Analysis of modern crisis management system, Ukrainian Scientific Journal of Information Security, 2015, T.21, №1, P. 87-101.

[3]. Kort S.S. The structure of intruder detection systems [Electronic resource]: abstract / S.S. Kort. – Mode of access: http://www.ssl.stu.neva.ru/sam/

[4]. Korchenko A.A. System of detection of abnormal state in computer networks, Ukrainian Scientific Journal of Information Security, №1 (19), 2013, P. 158-162.

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

[6]. Ivanchenko Ye.V., Gavrylenko O.V., Gizun A.I. Basic architecture of an expert system of prediction and prevention crisis situation. Ukrainian Information Security Research Journal, 2012, №3, P. 94-104.

[7]. Karpinkiy M.P., Korchenko A.O., Gizun A.I. Detection of incidents / potential crisis situations method. Ukrainian Information Security Research Journal, 2015, T.17, №2, P. 124-130.

[8]. Gizun A., Gnatyuk V., Balyk N., Falat P. Approaches to Improve the Activity of Computer Incident Response Teams. Proceedings of the 2015 IEEE 8th International Conference on "Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications" (IDAACS'2015), Warsaw, Poland, September 24-26, 2015: Vol. 1, Pp. 442-447.

[9]. Karpinkiy M.P., Korchenko A.O., Gizun A.I. Integrated model for crises presentation and formalized procedures for identifying parameters building. Legal, Normative and metrological support of information security in Ukraine, 2015, V.2 (28), P. 76-85.

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

[11]. Gizun A.I., Topcheev S.I., Ryabyy M.O. Base parameters of forecasting and identification of computer attacks in information and communication systems. 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.

[12]. Volyanska V.V., Gizun A.I., Gnatyuk V.O. Models of standards of linguistic variables for detection and identification the intruder of information security,

Ukrainian Scientific Journal of Information Security, №1 (19), 2013, P. 13-21.

[13]. Gizun A.I., Gnatiuk V.O., Suprun O.M. Formalized model of heuristic rules for incident detection, Journal of Engineering Academy of Ukraine, 2015, №1, P. 110-115.

[14]. Korchenko A.O., Kozachok V.A., Gizun A.I. Method of criticality level assessment for crisis management systems. Ukrainian Information Security Research Journal, 2015, T. 17, №1, P.86-98.

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

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

ВЫЧИСТЛИТЕЛЬНЫЙ КОМПЛЕКС ВЫЯВЛЕНИЯ И ОЦЕНИВАНИЯ КРИЗИСНЫХ СИТУАЦИЙ В ИНФОРМАЦИОННОЙ СФЕРЕ

Для эффективного обеспечения защищенности информационных ресурсов на сегодня необходимо не только выявить кризисную ситуацию, но и идентифицировать ее и оценить уровень угрозы информационной безопасности, вызванный ею. Большинство из известных систем обнаружения, прогнозирования и оценки кризисных ситуаций основываются на сигнатурном или компараторном принципах. Таким образом они не могут использоваться в нечеткой слабоформализованому среде. Это создает препятствия для их функционирования в информационных системах при реальных условиях. Данную проблему решает применение методов нечеткой логики и экспертных подходов. В данной статье предложена базовая архитектура нового структурного решения: вычислительного комплекса, который состоит из системы обнаружения инцидентов / потенциальных кризисных ситуаций и системы оценивания критичности ситуации. Архитектура систем представлена структурными модулями и блоками, которые связаны логически-функциональным связями. Каждая система может использоваться как отдельно и независимо друг от друга так и вместе для задач управления кризисными ситуациями в информационной сфере.

Ключевые слова: управление кризисными ситуациями, инцидент / потенциальная кризисная ситуация, система обнаружения инцидентов / потенциальных кризисных ситуаций, система оценивания критичности ситуации, нечеткая логика, эвристические правила, экспертная оценка.

COMPUTER COMPLEX FOR DETECTION AND EVALUATION OF CRISIS SITUATIONS IN INFORMATION SPHERE

Today to ensure the effective information resources security it is needed not only to identify the crisis satiation, but also to identify and evaluate the level of information security threats, which were caused by it. Most of the known detection and prediction evaluation systems for crisis situations are based on the signature or comparator principles. Thus they can not be used in the fuzzy weakly-formalized environment. This creates obstacles for their functioning in real information systems. This problem is solved by using fuzzy logic application and expert approach. In this paper represented the basic architecture of a new structural solution: computer complex which consist of incidents / potential crises detection and situation criticality evaluation system. Complex architecture is represented as structural modules and blocks, which is associated by logically functional connections. Each system can be used separately and independently or together for the crisis situation management tasks in the information scope.

Keywords: crisis management, incident/potential crisis situation, detection of incidents / potential crisis situations and evaluation critical situations system, basic architecture, module, structural block, fuzzy logic, heuristic rules, expert evaluation, fuzzification.

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.

Gizun Andriy, Assistant of Academic Department of IT-security, National Aviation University.