НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

На правах рукопису

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

Дисертація на здобуття вченого ступеня кандидата технічних наук

Науковий керівник:
кандидат технічних наук, доцент
Корченко Анна Олександрівна

Київ 2015

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АРМ ОПР – автоматизоване робоче місце особи, що приймає рішення

ІБ – інформаційна безпека

ІПКС – інцидент/потенційна кризова ситуація

ІР – інформаційні ресурси

ІС – інформаційна система

КС – кризова ситуація

КУББ – концепція управління безперервністю бізнесу

ЕП – евристичне правило

ЛЗ – лінгвістична змінна

ПЗ – програмне забезпечення

СВІПКС – система виявлення інцидентів/потенційних кризових ситуацій

СОКС – система оцінки критичності ситуації

СРВКС – система ранього виявлення кризових ситуацій

BCP – Business continuity planning (планування безперервності бізнесу)

BCM – Business continuity managment (управління безперервності бізнесу)

BIA – business impact analysis (аналіз впливу на бізнес)

RTO – recovery time objective (час відновлення)

RPO – recovery point objective (точка відновлення)

ВСТУП

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: [29,53] – введені характеристики системи управління КС та розроблена базова архітектура; [9-11,17] – проведене дослідження основних стандартів управління інцидентами ІБ та рекомендованих практик ЗББ, сучасних систем та методів управління КС, виявлення атак, вторгнень, порушника ІБ в ІС; [16,65,115] – запропоновані параметри ідентифікації та виявлення інцидентів ІБ різного характеру (комп'ютерних атак, вторгнень в ІС, особи порушника) та формалізовані процеси

їх описання та вибору; [8,32,42] – запропоновано процес моделювання еталонів ЛЗ для задач управління КС; [14,33,50] – запропоновані підходи до побудови методів виявлення вторгнень, порушників в ІС і розроблено метод виявлення ІПКС; [20] – розроблена формалізована модель побудови множин ЕП для виявлення та ідентифікації ІПКС; [51] – запропонована множина універсальних параметрів оцінки критичності ситуації, що є наслідком впливу КС, та розроблено метод оцінки КС; [32] – запропонована інтегрована модель представлення ІПКС; [17,19] – проведений аналіз поняття «кризова ситуація» та суміжних понять, пов'язаних з процесами управління КС; [91] – 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» ІІРТК-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.

РОЗДІЛ 1. СУЧАСНІ СИСТЕМИ ВИЯВЛЕННЯ ТА ОЦІНКИ КРИЗОВИХ СИТУАЦІЙ

1.1. Поняття кризових ситуацій в аспекті концепції управління безперервністю бізнесу

З розвитком можливостей інформаційних технологій (ІТ) у сучасному світі пріоритетним є автоматизація управлінських, технологічних, виробничих та інших процесів. Інформаційні системи (ІС) займають провідні ролі в системі функціонування бізнесу та держави, причому взаємозв'язок ІТ та бізнес-процесів (БП) стає настільки тісним, що життєздатність підприємств повністю залежить від надійності технологій, що забезпечують підтримку найбільш важливих критичних БП підприємства, організації, установи. Проблема реагування на кризові ситуації (КС) в сфері ІТ є надзвичайно важливою, хоча ще не достатньо вивчена. Адже серйозно нею розпочали займатися лише з кінця 80-х років минулого століття, причому на території країн СНД початок даних досліджень припав на середину першого десятиліття теперішнього століття. З розвитком ІТ та їх можливостей невпинно зростає роль систем реагування на кризові явища в процесі управління та підтримання життєздатності підприємств, установ та організацій усіх форм власності. Недаремно концепція управління безперервністю бізнесу (КУББ) в останні роки є однією з найбільш динамічно розвиваючихся напрямків оперативного та стратегічного менеджменту. Дослідження 114 компаній з списку 1000 найбільших корпорацій показало, що в середньому вони стикаються з кризовими ситуаціями в 10 разів на рік [130]. Так, 10-15 років тому провідні світові компанії, в першу чергу фінансовий сектор ринку, усвідомили ступінь залежності бізнесу від ІТ. Великі корпорації почали цілеспрямовано впроваджувати технології забезпечення безперервності бізнесу (ЗББ) в непередбачених або кризових ситуаціях (КС) [19,79,80,117]. Важливість даної проблеми підтверджена і статистикою появи КС різного характеру в теперішній період розвитку людства. Так наведені в [112] статистичні дані чітко показують, що кількість гідрометеорологічних кризових ситуацій на 2000 рік в порівнянні з 1950 зросла майже в 25 раз, геологічних – в 8 раз, а біологічних – близько в 50. За даними [116] у 2010 році кількість зареєстрованих лих наближається до середнього значення протягом 2000-2009 років (387). Число жертв зросло з 198 700 000 у 2009 році до 217,3 млн. чол. в 2010 році, але залишилася нижче середньорічного числа жертв 227500000 протягом 2000-2009 років.

Економічні збитки від стихійних лих в 2010 році більш ніж в 2,5 рази вищі ніж в 2009 (47,6 млрд. $ США) і збільшились на 25,3% в порівнянні з середньорічним показником (98,9 млрд. $ США). У розвинених країнах ринок технологій і послуг, що забезпечують безперервність бізнесу (ББ), динамічно розвивається. Рівень його зростання становить близько 25% на рік і обумовлений, головним чином, тим, що середні компанії слідом за лідерами індустрії активно впроваджують у своїй діяльності технології управління КС [159]. При цьому все більш актуальним стає забезпечення захисту від не катастрофічних, а, більш ймовірних, надзвичайних ситуацій. Однак залишається досить багато проблем в КУББ. В роботах [80,96,100,101,117,153,159] наведені відомості законодавчого, науково-теоретичного та практичного характеру щодо УББ. Здійснивши аналіз даних та інших відомих джерел визначимо основні поняття та терміни, що використовуються в області технологій УББ. Вони спрямовані на захист активів та ресурсів підприємства чи організації від впливу КС. Тому найперше потрібно дати визначення терміну «кризова ситуація». Нажаль, загальноприйнятого тлумачення цього терміну немає. Розглянемо найбільш вживані варіанти терміну «кризова ситуація» та суміжні з ним поняття і сформуємо коректне та відповідне темі роботи визначення КС.

Поняття криза має багато рівнів і трактувань. Вираз «криза» походить від грецького слова «crisis», яке означає «вирок, рішення по якомусь питанню, чи в сумнівній ситуації» [88]. Найперше дане поняття використовувалось в медицині, а з XVII-XVIII століття – стосовно до процесів, що відбуваються в суспільстві, як то військові, політичні кризи. При цьому використовувалося майже незмінене значення кризи, взяте з медицини. З XIX століття з’являються тлумачення криз в економічній сфері. Класичне економічне поняття кризи, що сформувалося в той час, означає не бажану і драматичну фазу в капіталістичній економічній системі, що характеризується коливаннями і негативними явищами, перешкодами. У цьому розумінні поняття кризи довгий час займало міцне місце в схемі теорій кон'юнктур у розвитку економіки. Так циклічна схема Шпітхоффа містить стадії: спад – перший підйом – другий підйом – пік – брак капіталу – криза [3,89,95]. В медицині, особливо в психіатрії КС стали основою напряму терапевтичних досліджень, названих кризовим втручанням. Виникнення теорії кризових втручань зазвичай повязують з дослідженням Lindemann'ом реакції пацієнтів на горе [126] в якій він визначив симптоматику криз в 101 пацієнта, що нещодавно втратили близьких людей. Подальший розвиток теорії і практики кризових інтервенцій в психіатрії

здійснили Poal [149], Caplan і його коллеги з Гарварда. Caplan запрпоновував визначення кризи [103,104]: він вважає, що кризи з'являються тоді, коли людина опиняється перед проблемою, рішення якої немає і така ситуація не може бути подолана з використання звичайних методів вирішення проблем. Кризова теорія Caplan's заснована на поняті гомеостазу, а кризою вважається порушення гомеостатичного балансу. Проте на думку Taplinj [156] поняття гомеостазу не відділяє адаптивну і не адаптивну нестійкість, не може ефективно характеризувати важливі аспекти людської поведінки: ріст, розвиток, зміни та актуалізація. Відоме визначення в авіаційній галузі: КС – ситуація, яка склалася внаслідок вчинення протиправних і навмисних дій, пов'язаних з посяганням на нормальну, регулярну і безпечну діяльність цивільної авіації, що спричинили нещасні випадки з людьми, майнові збитки, акти незаконного втручання в діяльність цивільної авіації або які створили реальну загрозу настанню таких наслідків [82,86]. В фінансово-страховому секторі КС – це ситуація, яка може мати місце в майбутньому через вплив зовнішніх та/або внутрішніх чинників і яка призводить до суттєвих фінансових втрат страховика [84]. В галузі ядерної безпеки під терміном КС розуміють ситуацію, що склалася або може скластися внаслідок вчинення або загрози вчинення диверсії, крадіжки або будь-якого іншого незаконного вилучення ядерних матеріалів [83].

В даний час розроблено декілька підходів до визначення поняття КС. Так деякі автори визначають кризу як порушення, зміна в гіршу сторону одного або декількох параметрів, характеристик будь-якої системи – людини, групи людей, організації, економіки, екології, суспільства в цілому. Інші сучасні автори характеризують кризу як такий стан організації, при якому вона не здатна жити далі, не зазнаючи деяких внутрішніх змін [7,36]. Відоме ще визначення, наведене в [26], за яким криза – це крайнє загострення внутрішньовиробничих і соціально-економічних відносин, а також відносин організації із зовнішньоекономічним середовищем. Деякі автори визначають кризу через опис її характеристик. Наприклад, Горєлов вказує, що «… виникнення КС супроводжується: наявністю загроз для реалізації найбільш важливих цілей організації; дефіцитом часу для прийняття рішення по врегулюванню кризи; тиском на осіб, котрі приймають рішення» [4]. З точки зору кризового управління (менеджменту) криза – це припинення нормального процесу, непередбачена подія, що ставить під загрозу стабільність підприємства, раптова серйозна подія, яка має потенціал пошкодити або навіть зруйнувати репутацію компанії. Під позаштатними або надзвичайними ситуаціями ро-

зуміються зовнішні впливи, що призводять до неможливості функціонування підприємства в звичайному режимі. Крім прямих втрат організації несуть витрати, пов'язані з порушенням процедур виробничого та фінансового обліку, втратою розташування замовників, погіршенням іміджу і зниженням конкурентоспроможності [55,88,124]. Крім того в даній галузі відомі спроби надати визначення КС багатьма авторами, проте вони не дали загальноприйнятого поняття. Деякі визначення сконцентровані на їх впливі на організації. Наприклад, Coombs в [108] визначив кризу як ситуацію, яка викликає небажані або негативні наслідки для організації. Lerbinger [125], розглядає кризу як випадок, який приносить шкоду репутації компанії, становить небезпеку для її дохідності, зростання і, можливо, існування організації. Miller під кризою розуміє випадок, що вимагає швидкої реакції, створює невпевненість і напругу, загрожує репутації, активам, постійно зростає в аспекті інтенсивності і вимагає змін організації [129]. Інші дослідники вказують на те, що КС впливає не лише на організацію, але й на систему вцілому. Fearn-Banks в [113] визначає кризу як явище з потенційно негативними наслідками, що охоплюють організацію, компанію, промисловість, а також суспільство, продукцію, послуги або імя, в той же час Pauchant і Mitroff в [146] вважали, що криза – це деструктивний чинник, який фізично впливає на систему в цілому і вимагає прийняття відповаідальності на себе, загрожує субєктивному екзистенціальному ядру організації. Деякі дослідники на перший план ставлять такі характеристики КС як непередбачуваність, двозначність тощо. Наприклад, Pearson и Clair [148] під кризою розуміють малоймовірний випадок з високим рівнем впливу, що загрожує життєздатності організації і характеризується двозначністю ситуації, ефекту і засобів вирішення, а також необхідність швидкого прийняття рішень. Один з провідних фахівців в галузі управління кризами Regester визначає [150]: кризу як подію, з вини якої компанія потрапляє в центр «не завжди доброзичливої» уваги засобів масової інформації та інших зовнішніх цільових аудиторій, в тому числі акціонерів, профспілкових організацій, рухів на захист навколишнього середовища, які з тієї чи іншої причини цілком законно цікавляться діями організації.

Виникнення КС зазвичай спричинене певними інцидентами. Інцидент – подія, здатна привести до втрати чи порушення діяльності організації, послуг або функцій підприємства. Причому у випадку відсутності контролю вона може перерости в надзвичайну ситуацію, кризу або стихійне лихо [98,99]. Надзвичайна ситуація (лихо, катастрофа) – це подія, яка має негативний вплив на функціонування

сервісу або системи, вимагає значних зусиль для відновлення початкового рівня продуктивності. Тобто надзвичайна ситуація набагато серйозніша інциденту. Надзвичайна ситуація – це стан на певній території або акваторії, що склалася в результаті аварії, небезпечного природного явища, катастрофи, стихійного чи іншого лиха, які можуть спричинити або спричинили за собою людські жертви, шкоду здоров'ю людей або навколишньому середовищу, значні матеріальні втрати. В КУББ, зокрема в міжнародних стандартах з УББ, найбільш відомих практик дане питання розглядають в такому контексті: криза – ненормальна ситуація, яка загрожує операціям, персоналу, клієнтам і репутації підприємства [120]; надзвичайна ситуація – загальний термін з різними інтерпретаціями в залежності від регіону. У США він означає широкомасштабну катастрофу, що вимагає федеральної підтримки і запуск фінансування Федеральної агенції управління надзвичайними ситуаціями [157]. В інших країнах – вважається еквівалентними за змістом серйозним інцидентам [98,99,120]; громадянська надзвичайна ситуація – подія або ситуація, яка може нанести серйозних збитків людському добробуту, навколишньому середовищу в будь-якому місці чи порушити безпеку цього місця [99]; катастрофа – фізична подія, що перериває бізнес-процеси достатньо, щоб загрожувати життєздатності організації [98,120]. Відповідно до законодавства України надзвичайна ситуація – порушення нормальних умов життя і діяльності людей на об'єкті або території, спричинене аварією, катастрофою, стихійним лихом або іншими чинниками, що призвели (можуть призвести) до загибелі людей, тварин і рослин, значних матеріальних збитків та (або) завдати шкоди довкіллю, а небезпека у надзвичайних ситуаціях – стан, за якого існує наявна або ймовірна загроза виникнення вражаючих чинників і їх впливу (дії) на населення, об'єкти економіки та довкілля [25]. Усі вищеназвані явища та процеси, хоча і мають різний характер та природу, застосовуються в різних галузях економіки та суспільного життя, негативно впливають на життя людей, функціонування бізнес-процесів і бізнесу в цілому, держави, знижують ефективність управління ресурсами. Для уникнення проблем та непорозумінь дамо єдиний загальний термін для їх визначення, що будемо використовувати у досліджені. КС в аспекті безперервності бізнесу – це певна ситуація чи подія, що має місце на деякій території (в фізичному чи організаційному сенсі), потенційно здатна нанести серйозних збитків, призвести до порушення діяльності, загибелі чи поранені персоналу організації чи інших категорій населення, втрати послуг або функцій підприємства в достатньому об’ємі щоб загрожувати життєздатності організації [19].

Кризові ситуаційні центри (КСЦ) як основа систем управління великими (корпоративними) структурами під час КС на сучасному етапі розвитку ІТ знаходять все більше і більше поширення [28,61]. Невід'ємною частиною КСЦ є автоматизовані систему підтримки прийняття рішень (АСППР) і, зокрема, елементи штучного інтелекту – бази знань. В основі їх формування знаходиться модель знань в предметній області, для якої створюється інформаційна система. Для КСЦ – це знання про ситуації, що вимагають оперативного прийняття рішення. Не останнє місце серед таких даних займає класифікація КС. Так, в законодавстві України КС залежно від джерела небезпеки може бути: природна, техногенна, соціально-політична, воєнна; залежно від масштабу: загальнодержавна, регіональна, місцева й об’єктова [24,25].

У літературі зустрічається досить багато моделей окремих вузькоспеціалізованих видів надзвичайних ситуацій [111,154], однак відсутня універсальна модель, що дозволяє описати широкий клас КС. Тож необхідним є виділення базових характеристик, формування універсальної, достатньо повної моделі їх класифікації. Огляд відомих класифікацій був здійснений в [121,127]. З метою вдосконалення процесів антикризового управління багатьма вченими були зроблені спроби класифікувати КС. [107,108,125,128,131]. Наприклад, Mitroff і Killman [131] ідентифікували сім типів КС в менеджменті організацій: фальсифікація продукту, дефект продукції, піратство, хибне звинувачення, обмежене мислення, містифікації та культурна не чуттєвість. Meyers [128] виділив девять типів ділових криз, а саме: зміни суспільних настроїв, різких змінах ринку, дефекти продукції, наслідуваність (спадкоємність) менеджменту, фінансові втрати, відносини між керівництвом і персоналом, корпоративні поглинання бізнесу, негативні міжнародні події, а також впливи повязані з регулюванням або відмовами державного контролю промисловості. Lerbinger [125] пропонував чотири класи криз, названі технологічними кризами, конфронтаційними кризами, кризами недоброзичливості і кризами організаторської відмови. Проте одна з найбільш цікавих і корисних типологій КС булла запропонована Coombs в [108], а згодом вдосконалена в роботі Coombs і Holladay [107]. Ці типології базуються на основі рівня розуміння організацією самої КС і розуміння нею відповідальності [109]. В Coombs [108] КС класифіковані по девяти основним категоріям, до яких віднесені стихійні лиха, недоброзичливість, технічні збої, саботаж, виклики, катастрофічні пошкодження, організаційні злочини, насилля на робочому місці і чутки. Використовуючи поняття організаційної відповідальності вони були сгруповані в п’ять груп: чутки, приро-

дні КС, недоброзичливість, нещасні випадки і злочини [105]. В типології [107] автори запропонували дещо змінену класифікацію і набір з 10 стратегій реагування на КС. Так, було виділено 13 кризових типів, що виділені в 3 групи: КС, в яких організація відчуває себе жертвою; випадкові КС, що виникають внаслідок ненавмисних дій; КС, які можна уникнути, повязані в основному з цілеспрямованим впливом та людським чинником. Крім того в класифікаціях КС виділяють інші показнки і ознаки для класифікації.

Відповідно до причин походження подій, що можуть зумовити виникнення КС (джерел) Державний класифікатор надзвичайних ситуацій виділяє 4 типи КС: техногенного характеру; природного характеру; соціально-політичного характеру, пов'язані з протиправними діями терористичного і антиконституційного спрямування; воєнного характеру, пов'язані з наслідками застосування звичайної зброї або зброї масового ураження [24]. На Заході виділяють п’ять основних типів КС: підприємницькі, соціальні, техногенні, природні та природно-техногенні [112]. Розглянемо інші характеристики, які використовуються в різних джерелах для класифікації КС. За можливістю прогнозування кризи можуть бути передбаченими (закономірними) і несподіваними (випадковими). Різновидом передбачених криз є циклічна криза [3,4,26,91,95]. За ступенем прояву дослідники виділяють кризи явні і латентні (приховані). Перші протікають помітно і легко виявляються. Інші є прихованими, протікають відносно непомітно і тому найбільш небезпечні [91,95]. За глибиною вияву кризових явищ кризи бувають деструктивними, глибокими і легкими. Деструктивні КС часто ведуть до руйнування різних структур соціально-економічної системи. Глибокі КС не ведуть до руйнування різних структур соціально-економічної системи, а лише до їх суттєвих змін. Легкі кризи протікають більш послідовно і безболісно, ними легко управляти. Дана характеристика притаманна в основному для економічних КС, тому в досліджені носить другорядне значення [4,91]. За характером виникнення кризи бувають такими, що виникають за рахунок впливу суб’єктивних – тобто залежних від волі, переконань, помилок, тощо певних суб’єктів-учасників відносин в яких виникла криза – та об’єктивних причин, незалежних від дій та бажань оточуючих [3,91]. За масштабом прояву КС слід розглядати з двох позицій, в географічному та в організаційно-підприємницькому аспекті. Так за даною характеристикою в географічному аспекті КС можуть бути локальними, регіональними, державними та глобальними. А в іншому аспекті доцільно виділити наступні види: КС в межах окремого бізнес-процесу, підприємства, на рівні групи підприємств [26,91]. Яскравим прик-

ладом може служити порушення роботи електронної пошти. Так при відмові поштового клієнта певного відділу, скажімо бухгалтерії – це КС в межах окремого бізнес-процесу, а у випадку відмови поштового сервера провайдера в залежності від масштабів надання послуг провайдерами КС переходить на рівень підприємства чи групи підприємств. За часом дії негативних чинників можна виділити довго, середньо, короткотривалі та миттєві надзвичайні події. Стосовно відображення даної характеристики в числовому значенні існує велика кількість підходів, кожен з яких має свої особливості. Ще більше проблема ускладнюється невизначеністю стосовно того чи дія наслідків КС входить в час дії самої кризи чи обраховуються окремо. Так КС можуть діяти в найрізноманітніших часових інтервалах – від долі секунди (удар блискавки, перепад в мережі електроживлення) до років (війни, кліматичні зміни). За потенційною загрозою людському життю та здоров'ю виділяють два види КС: що несуть потенційну загрозу і що не несуть її. Ті КС, які потенційно можуть нести загрозу людині класифікуються ще за двома характеристиками: за кількістю загиблих та постраждалих осіб, не залежно від категорії. Відносно кількості загиблих можна виділити три категорії КС: катастрофи (понад 500 осіб), КС з великою (понад 100 осіб) та невеликою кількістю жертв. Інколи дану характеристику оцінюють не за абсолютним показником загиблих, а за відношенням їх на 100 000 населення [24,85,91]. Проте однозначної точки зору на числові значення даної шкали немає. Така ж ситуація з шкалою кількості постраждалих, у ній прийнято виділяти аналогічні категорії КС як і з кількістю загиблих. Тому надалі пропонується використовувати лише характеристику кількість жертв, що охоплює в собі загиблих та постраждалих осіб від КС і виділяти наступні категорії: катастрофічні, з великою та невеликою кількістю жертв. За рівнем економічних збитків. Нищівні, з великими, помірними та невеликими збитками, практично не відчутні – основні класи КС, що можна виділити за рівнем завданих економіці збитків. Оцінка кризової ситуації у даному випадку здійснюється за абсолютним показником суми витрачених на ліквідацію її наслідків грошей або за часткою цієї суми в ВВП країни [91,112,116]. В результаті нищівних КС все господарство на території враження зазвичай зруйноване і витрати на її ліквідацію складають порядку 10% ВВП. Натомість невідчутні КС не несуть ніяких руйнацій і витрат на їх ліквідацію.

Визначивши і розглянувши поняття «кризова ситуація», що є одним з центральних об'єктів КУББ, перейдемо до розгляду його фундаментальних основ – процесів стратегічного менеджменту. Багато науковців розглядають кризове уп-

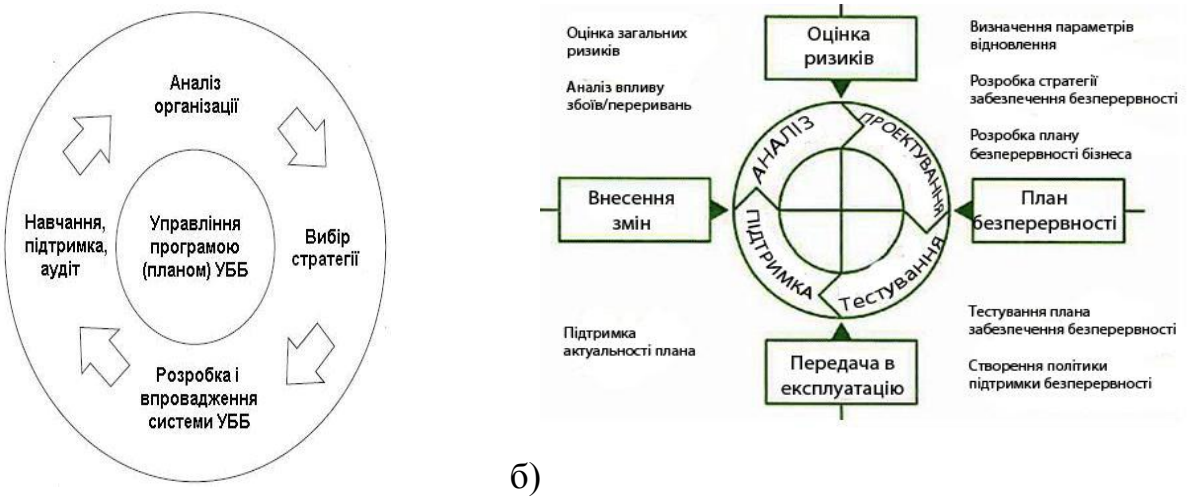
равління як довготривалий процес і пропонують різні моделі його стадій. Всі вони охоплюють часовий проміжок від підготовки перед кризою і до відновлення після неї. Ці моделі представляють різні підходи і відрізняються кількістю етапів. Кризове управління розділяють на три [106,151,152], чотири [122,132], пять [114,147], шість [97] і навіть вісім стадій [118]. Основні етапи названих моделей представлені у вигляді таблиці 1.1.

Таблиця 1.1

Основні етапи моделей процесу кризового управління

Загальні стадії	Smith	Richardson	Coombs	Myers	Jaques	Pearson і Mitroff	Fink	Augustine
Перед кризами	Криза управління	Передкризова стадія	Передкризова стадія	Нормальні операції	Підготовка до кризи	Виявлення сигналу	Кризове зниження	Запобігання криз
						Підготовка	Планування	Підготовка
Під час кризи	Експлуатаційна криза	Кризовий вплив / спасіння	Кризова стадія	Надзвичайна відповідь	Запобігання криз	Стримання	Попередження	Визнання кризи
							Відповідь	Стримання
				Тимчасова обробка	Кризове управління інцидентами			
Після криз	Криза легітимізації	Відновлення / упадку	Посткризова стадія	Відновлення	Посткризове управління	Відновлення	Реагування	Вирішеня
						Вивчення		Оцінка

Міністерство внутрішніх справ Великобританії запропонувало виділити вісім етапів, а саме: керівництво, збір інформації, написання планів, консультація, публікація, учбова ратифікація, підтвердження/перегляд (Harrison ([118]). Слід зазначити, що трьохетапна модель є найбільш відомою і на ній базуються інші моделі, що утворені шляхом деталізації визначених трьох етапів. Деякі дослідники даного питання, серед яких і розробники стандарту BS25999 [100,101], використовують чотирьох етапну модель УББ, яка зображена на рис. 1.1а. На рисунку 1.1б представлений цикл розробки систем ЗББ.



а) б)

Рис. 1.1. Життєвий цикл концепції управління безперервністю бізнесу (а) та розробки систем забезпечення безперервності бізнесу (б)

Існує ще третій підхід, за яким виділяють такі стадії: аналізу, проектування,

тестування та підтримки [159]. Проаналізувавши роботи фахівців та стандарти в цій області, була запропонована модель поділу на етапи процесу застосування методів та технологій ЗББ [19]. Так, основними етапами життєвого циклу систем УББ за даною моделлю є: 1) планування безперервності бізнесу; 2) реалізація (введення в дію, експлуатація, тестування) розробленого плану. На першому етапі повинен бути проведений аналіз загроз, ризиків, визначені активи та критично важливі ресурси, розроблена документація та проведене навчання персоналу. На другому етапі проводиться введення превентивних заходів та встановлення засобів, що забезпечують процедуру відновлення роботи критичних IT-процесів і бізнесу взагалі [19].

Хоча немає чіткого алгоритму створення плану BCP, час від часу з'являються різні практики його проведення. Зокрема, NIST (National Institute of Standards and Technology – Національний інститут стандартів і технологій США) відповідає за відповідає за розробку кращих практик та забезпечення загального доступу до них. NIST передбачив такі кроки в документі SP 800-34 «Керівництво з планування безперервності для IT-систем» (див. рис. 1.2 [117]) [134]:

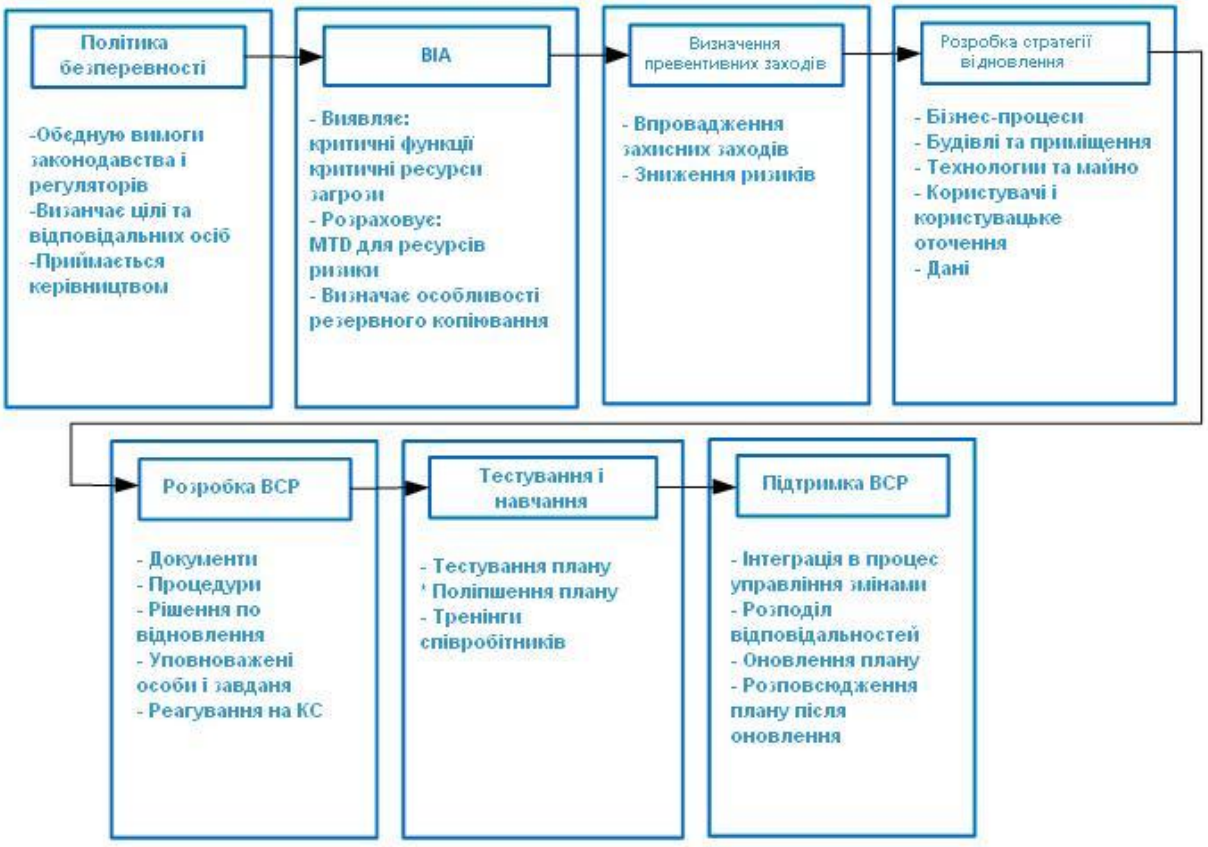


Рис. 1.2. Алгоритм планування безперервності бізнесу

1) Розробити політику планування безперервності бізнесу (continuity planning

policy statement). Написати політику, яка міститиме необхідні керівні принципи для розробки плану BCP і визначить необхідні уповноважених осіб для виконання покладених на них завдань, в тому числі і осіб, що приймають рішення (ОПР).

2) Провести Аналіз впливу на бізнес (BIA – business impact analysis). Ідентифікувати критичні функції і системи, категоризувати (пріоритезувати) їх на основі ступеня їх критичності. Виявити уразливості, розрахувати ризики.

3) Визначити превентивні захисні заходи. Після виявлення загроз, вибрати і впровадити захисні заходи і контролі для зниження рівня ризиків компанії економічно доцільним способом.

4) Розробити стратегії відновлення (recovery strategy). Описати методи, що забезпечують оперативне відновлення працездатності критичних систем, функцій.

5) Розробити план дій на випадок надзвичайних ситуацій (contingency plan). Описати процедури, розробити керівництва, які забезпечать продовження функціонування компанії в аварійному стані.

6) Протестувати план, провести тренінги і навчання. Перевірити план для виявлення недоліків у ньому, провести тренінги та навчання для належної підготовки людей на випадок КС.

7) Підтримувати актуальність плану.

Таким чином, на даний момент в науковій літературі не існує єдиного підходу визначення сутності УББ та його фундаментальних напрямків – планування ББ та планування аварійного відновлення, що є суттєвою проблемою. Шляхом її вирішення може бути детальна систематизація сутності УББ.

1.2. Аналіз систем забезпечення безперервності бізнесу

Серія міжнародних стандартів ISO 27k регламентує і визначає основні процеси управління інформаційною безпекою, в тому числі охоплює питання управління ризиками, інформаційними ресурсами, комунікаціями, інцидентами інформаційної безпеки тощо. Згідно стандартів створення систем менеджменту інформаційної безпеки (СМІБ) здійснюється в чотири етапи: планування та створення ІС; впровадження та використання; моніторинг та аудит; підтримка та вдосконалення ІС, що повністю відповідають циклу Шухарта-Демінга (цикл PDCA). Таким чином захист інформації реалізується завдяки використанню сукупності різноманітних систем проектування, моніторингу, аудиту, керування інформаційної безпеки і інших сфер обслуговування та управління ІС. Серед таких систем доцільно виділити системи антивірусного захисту (САЗ), системи виявлення/попередження

вторгнень (IDS/IPS), системи аналізу та оцінки ризиків (САОР) [47], системи управління інцидентами інформаційної безпеки (СУІІБ, що включають в себе програмне та апаратне забезпечення для команд реагування на комп'ютерні інциденти (CERT) щодо фіксації, ідентифікації, обробки, реагування, ліквідації інцидентів, збирання статистичних даних тощо). Визначені системні засоби функціонують на кожному з етапів циклу PDCA і інтегруються в системах менеджменту (управління) інформаційної безпеки (СМІБ).

Дане дисертаційне дослідження присвячене розробці системи виявлення інцидентів/потенційних кризових ситуацій (СВІПКС) та системи оцінки критичності ситуації, спричиненої виявленим інцидентом (СОКС) (див. пп. 3.2 та 4.2 дисертаційної роботи), які разом з САЗ і IDS/IPS утворюють особливий клас СМІБ – систем управління КС (СУКС). Серед основних функцій СУКС слід виділити виявлення, ідентифікацію КС, проведення їх оцінки, забезпечення прийняття рішень в умовах КС та автоматизація цього процесу, підбір засобів реагування, ліквідації КС і т.п. На сьогодні в світі даний клас реалізований у вигляді вузькоспеціалізованих засобів, які в основному не застосовуються в сфері інформаційної безпеки, а також не можуть бути використані в умовах нечіткості. Детальний аналіз відомих СУКС наведено в розділі 1.3. Місце СУКС в менеджменті інформаційної безпеки та взаємозв'язки даного класу систем з іншими системами захисту інформації представлено на рисунку 1.3.

Як видно з рисунку САОР переважно використовуються на етапі планування і створення ІС, САЗ та IDS/IPS в основному взаємодіють з ІС, що захищається, на стадіях впровадження та моніторингу, а СУІІБ – на етапі підтримка та вдосконалення. Слід зазначити, що СВІПКС і СОКС на етапах впровадження та моніторингу взаємодіють з ІС безпосередньо або через САЗ та IDS/IPS і є основою класу СУКС. В поєднанні з СУІІБ СУКС утворюють клас систем управління безперервності бізнесу (СУББ), який разом з САОР формують загальний клас СМІБ. Розроблені системи СВІПКС та СОКС в якості вхідних даних використовують параметри зняті давачами в контрольованому середовищі (тобто ІС), а також інформацію з САОР, САЗ, IDS/IPS, СУІІБ і крім того мають зворотний зв'язок з САОР та СУІІБ, що забезпечує можливість корегування їх роботи, оновлення даних та формування статистики. Таким чином запропоновані системні засоби є невід'ємною складовою СМІБ і разом з тим утворюють окремий клас систем УКС, що може функціонувати для вирішення задач захисту інформації в поєднані з відомими захисними системами, розширяючи їх функціональні можливості, або автономно,

замінюючи більшість з них.

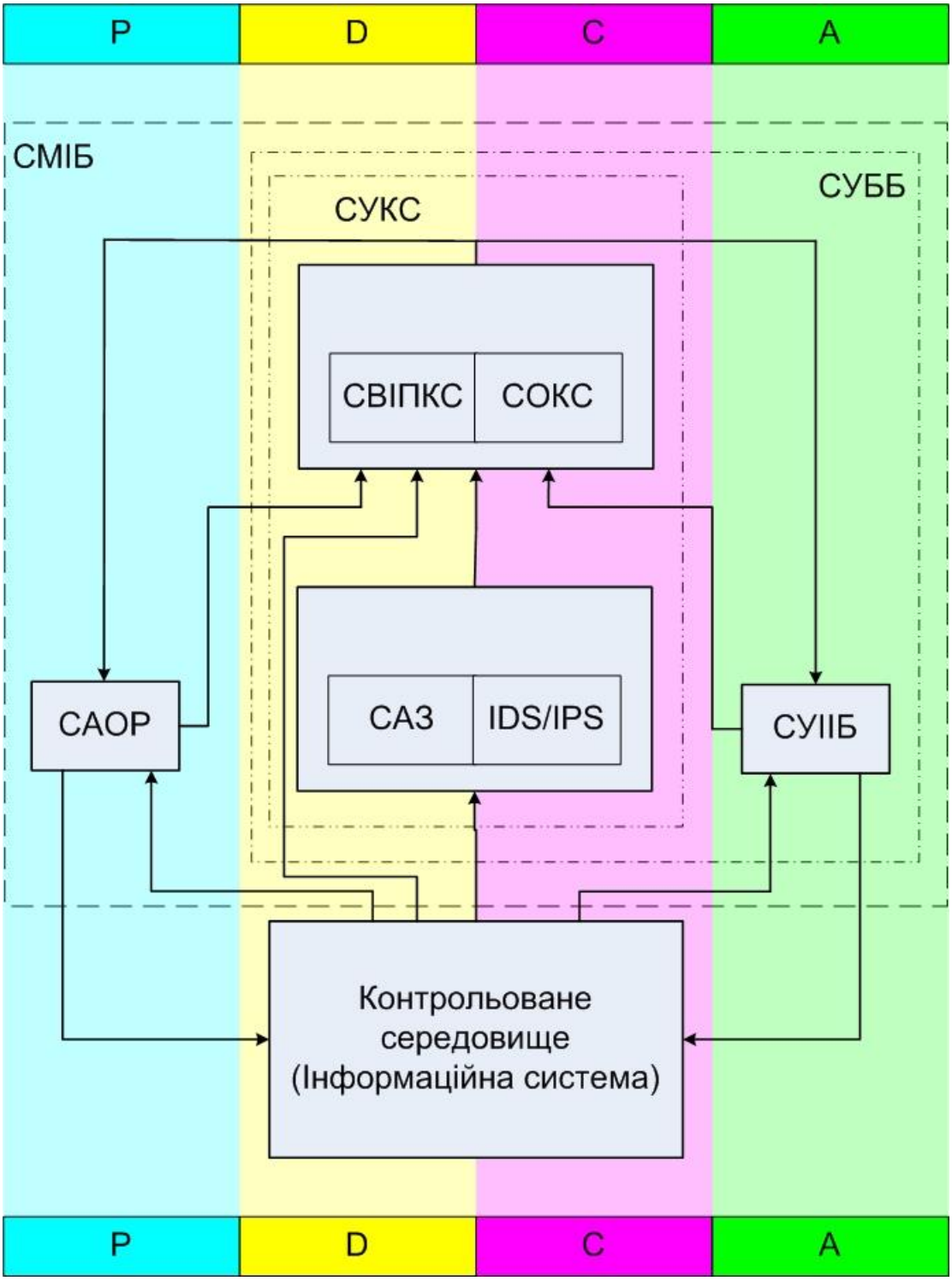


Рисунок 1.3. Взаємозв’язки СУКС з компонентами СМІБ

На сьогоднішній день процеси управління безперервністю бізнесу (УББ) описані в міжнародних стандартах та специфікаціях, серед яких слід відмітити AS/NZ 5050, BS 25999, CAN/CSAZ731-M91, COOP, CSA Z1600-14, HIPAA Gramm-Leach-Bliley, NFPA 1600, NIST ST800-34, SS540:2008 [96,100-102,110, 133,134,143]. Таким чином, зрозуміло, що рівень нормативного, методологічного та організаційного забезпечення КУББ досить високий. Не значною проблемою є

наявність деяких неузгодженостей між різними національними стандартами. Однак значно гіршою є ситуація з технологічною та технічною реалізацією даної концепції. Не дивлячись на те, що існує ряд систем та засобів для документаційного забезпечення BCP, обчислення ризиків, відновлення функціонування систем, практично повністю відсутні системи для прогнозування та оцінки КС, що б реалізовували всі етапи процеси управління КС від їх прогнозування до оцінки та ліквідації наслідків. Розглянемо ці питання в цьому та наступному підрозділах.

До теперішнього часу ринок послуг і рішень в області BCP вже сформований і розвинений. Наприклад, такі компанії, як IBM Business Continuity and Recovery Services і SunGard Availability Services пропонують максимально широкий спектр послуг у цій галузі. Інші компанії, наприклад, Business Protection Systems, LBL Technology Partners і RSM McGladrey, спеціалізуються тільки на розробці програмного забезпечення планування безперервності бізнесу. Для формування уявлення про спектр пропонованих послуг і рішень в області BCP дамо характеристику деяких пропозицій на цьому ринку [62,87]. До них відносяться: Computer Alternate Processing Sites (CAPS) – пропонує консалтингові послуги в області BCP, а також BIA; Hewlett-Packard Business Continuity and Recovery services – пропонує послуги планування і тестування BCP; IBM Business Continuity and Recovery services (бізнес-складова IBM Global services) - пропонує консалтингові послуги, включаючи аналіз і управління ризиками, планування та підтримку BCP, антикризове управління, оцінювання та планування відновлення; служби відновлення, включаючи повністю обладнані резервні компоненти технічної інфраструктури; SunGuard Availability Services пропонує повний спектр забезпечення необхідних безперервності та доступності корпоративних інформаційних систем; Business Protection Systems International (BPSI) пропонує набір засобів Business Protector для створення і підтримки планів безперервності бізнесу; Computer Security Consultants, Inc (CSCI) пропонує програмний продукт відновлення RecoveryPAC; LBL Technology Partners пропонує програму розвитку BCP LBL Contingency Planner, сумісну з Microsoft Office; Recovery Point Sistems пропонує рішення з відновлення критичних функцій бізнесу Integrated Disaster recovery Site (IDRS); RSM McGladrey пропонує програму планування безперервності бізнесу Business Continuity Planning System на основі аналізу та управління бізнес ризиками.

В цілому програмне забезпечення планування та управління безперервністю бізнесу можна умовно розділити на такі категорії [2,62,87]: автономні засоби BIA – введення даних здійснюється вручну менеджерами і потім експортується в підт-

римувані засоби BCP; генератори BCP – експертні системи з певними базами знань, що дозволяють згенерувати актуальний план ББ; бази даних BCP – відображають необхідну інформацію про планування ББ з урахуванням специфіки діяльності компанії; засоби спільного розподіленого планування ББ дозволяють реалізувати деякий корпоративний стандарт ЗББ. Серед виробників програмного забезпечення BCP виділяються компанії Strohl, SunGard, Computer Security Consultants Inc. (CSCI) і RSM McGladrey. Характерні особливості пропонованих програмних продуктів цих компаній наведені в таблиці 1.2. Так, наприклад, RSM McGladrey більше уваги приділяє рішенням BCP в області бухгалтерської діяльності, а SunGard розглядає питання планування та управління безперервністю бізнесу в контексті рішень і послуг обробки фінансової інформації в корпоративних інформаційних системах.

Таблиця 1.2

Характеристика програмного забезпечення BCP

Виробник	Назва програмного продукту	Підтримувана операційне середовище (ОС, бази даних, додатки)
Computer Security Consultants Inc (CSCI). Працює в понад 40 країнах світу і нараховує понад 1,400 інсталяцій свого програмного забезпечення. Основні клієнти знаходяться в Північній Америці і Європі.	RecoveryPAC · Генератор BCP · База даних BCP · Інтеграція з зовнішніми засобами BIA (RiscPac)	Windows 95/98/NT/2000/XP · Windows (NT или 2000) · Linux или Solaris (Unix) · Internet Explorer или Netscape
RSM McGladrey (відокремилася від H&R Block). RSM International має 600 офісів в 75 країнах світу. Пропонує послуги BCP середньому і великому бізнесу з річним доходом від 5 до 250 мільйонів доларів.	Business Continuity Planning System (BCPS), v3 · Аналізатор впливу на бізнес · Генератор BCP · База даних BCP	· Windows 95 / NT / XP · Microsoft Word, Word Pro та інші звичайні текстові редактори
Strohl. Обслуговує клієнтську базу в 60 країнах світу і нараховує понад 1500 клієнтів. Основними клієнтами є компанії з першої сотні Fortune 500.	Living Disaster Recovery Planning System (LDRPS) · Генератор планів безперервності · База даних BCP Інші продукти: BIA Professional Incident Manager	Windows 95/98 / NT / 2000 / NT / XPServer / 2000 / XP server Бази даних: · Sybase · Oracle · SQL Server
SunGard (поглинули Comdisco) SunGard працює більш ніж в 50 країнах світу і нараховує приблизно 20000 клієнтів.	PreCovery · Аналізатор впливу на бізнес · Генератор BCP · База даних BCP Інші продукти: Eplanner Revolution	· Windows 97 / NT / 2000 / XP · База даних SQL · Microsoft Word, Corel, Word Perfect, Lotus, Word Pro

Аналіз стандартів та рекомендацій, практик КУББ показав недостатній рівень обґрунтування застосування тої чи іншої стратегії забезпечення безперервності бізнесу (ЗББ). На сьогоднішній день виділяють такі основні стратегії ЗББ [2,17,80]: проведення превентивних заходів, резервування IT-сервісів на резервному майданчику, аутсорсинг, страхування фінансових ризиків і створення запасу обладнання та устаткування на складі постачальника. Названі стратегії мають свої

переваги та недоліки. Для вибору оптимальної стратегії для певної організації потрібно провести аналіз за такими критеріями: вартість, швидкість реагування на КС, надійність ЗББ, технічна складність реалізації, організаційна складність, можливість внесення змін та модифікацій [17]. Вибір оптимальних організаційних і технічних рішень з допустимим рівнем витрат вимагає розуміння прямих і непрямих витрат, пов'язаних з простоєм бізнес-процесів [2,80].

Основними характеристиками, що визначають вимоги до безперервності IT-сервісів, є наступні параметри [15,80,81,155]. RPO (Recovery point objective – цільова точка відновлення) – узгоджений з бізнесом інтервал часу, передуючий аварії, за який допускається втрата даних. Іншими словами, цей параметр показує, наскільки стан системи і даних може «відкотитися» назад при КС. RTO (Recovery time objective – цільовий час відновлення) – узгоджений з бізнесом інтервал часу після аварії, необхідний для відновлення IT-сервісів. Вони – наріжні камені, що лежать в основі вибору технологій захисту даних і систем (на рівні додатків). Проте ці показники корисно застосовувати в процесі проектування систем ЗББ, а не їх оцінки.

1.3. Аналіз методів та систем управління кризовими ситуаціями

Відповідно до КУББ під поняттям управління КС найбільш часто розуміється сукупність процесів з прогнозування, ідентифікації, оцінки КС, реагування та ліквідація їх наслідків. Розглянемо основні найбільш відомі вітчизняні та світові розробки в галузі управління КС.

Так, серед українських розробок варто відмітити ряд винаходів по забезпеченню безпеки підприємств в гірничодобувній та нафтогазовій промисловості, що ґрунтуються на контролю концентрації небезпечних речовин в свердловинах, видобутках та шахтах, а саме [67-69,73]. Крім того відомі системи збору інформації щодо КС і оповіщення про неї [66,71] та комп’ютеризована систему контролю і визначення місця аварії силових електромереж, на основі складання карти опору і моніторингу її подальшого стану з виявленням відмінностей від еталону [72]. До даної категорії відносяться також так звані системи раннього виявлення КС (СРВКС) [71,75,77,78] та розробки з загальної реалізації антикризового менеджменту [76]. Огляд відомих систем управління КС здійснено в [11].

Розглянемо більш детально СРВКС, запропоновану в [78]. Корисна модель належить до систем виявлення загрози надзвичайних ситуацій техногенного характеру і забезпечення безпеки та життєдіяльності людини. Задачею корисної моде-

лі є розширення функціональних можливостей СРВКС таким чином, щоб вона надавала можливість зберігання та аналізу стану навколишнього середовища і параметрів контрольованих сильно діючих отруйних речовини навколо об'єкта захисту, а також моделювання надзвичайних ситуацій, максимально наближених до реальних. Поставлена задача вирішується системою, що містить метеостанцію, датчики для реєстрації параметрів поточного стану об'єкта захисту та програмно-технічний комплекс зберігання та обробки даних, що в свою чергу складається з програмно-технічного пристрою обробки даних, пристрою накопичення даних, пристрою відображення розрахункових та вимірюваних параметрів, а також додатково програмно-технічний пристрій статистичної обробки даних (надає можливість прогнозування та оцінки розвитку надзвичайної ситуації) та програмно-технічний пристрій симуляції умов надзвичайної ситуації (надає можливість змоделювати умови виникнення надзвичайної ситуації з будь-якими вихідними даними). Прототипом даної системи є винахід, описаний в [75].

Також відома СРВКС [71]. Корисна модель належить до систем, що реагують на небажані або ненормальні умови, наприклад, на злом, пожежу, ненормальну температуру, ненормальну швидкість потоку, ненормальну концентрацію газів, ненормальний рівень рідини тощо, і може бути використана для виявлення загрози КС. В основі корисної моделі поставлено задачу розширення функціональних можливостей СРВКС, яка би цілодобово з максимальною надійністю контролювала параметри технологічних процесів з наступною обробкою інформації диспетчерами за допомогою програмного забезпечення, а також мала би мінімальну вартість обміну даними, за рахунок використання передачі зашифрованої криптографічними методами інформації між системою датчик-концентратор та віддаленим сервером через мережі зв'язку з використанням протоколів пакетної передачі даних TCP/IP наземного або супутникового звязку. Система складається з датчиків, концентраторів, засобів зв’язку та віддаленого сервера, на якому зберігається база даних, що містить реєстр об'єктів та параметрами їх технологічних процесів, гранично допустимі значення цих параметрів, а також їх поточний стан. Датчики (газоаналізатори, рівнеміри, датчики температури, датчики тиску тощо) розміщено у техногенно небезпечних зонах, вони мають три стани – нормальний, небажаний та небезпечний, що сприяє підвищенню надійності системи в порівняння з двозначною градацією. Таким чином в даній системі використовуються частковий випадок нечітких даних, однак значних переваг для впровадження її в слабоформалізованому середовищі це не дає, оскільки градація носить чіткий характер. Да-

тчики підключено до концентраторів – мікропроцесорних пристроїв для збору, зберігання та шифрування одержаних даних. Концентратор періодично відправляє звіт про свій стан. В концентраторі програмується періодичність зв'язку з віддаленим сервером, а також граничне значення параметрів, при досягненні яких зв'язок відбувається позачергово. Описана система дозволяє оперативно збирати інформацію про параметри технологічних процесів з подальшою обробкою для прийняття адекватних управлінських рішень при наявності об'єктивних та оперативних даних.

В правоохоронному документі [76] описана система для всебічного управління КС практично на більшості етапів КУББ. В основу корисної моделі поставлена задача створення інтегрованої інформаційно-аналітичної системи моніторингу зовнішнього і внутрішнього середовища підприємства, здатної за допомогою системного відбору необхідної інформації проводити комплексний аналіз ситуації і на його основі створювати варіанти моделей антикризового розвитку підприємства, що дозволяє особі, що приймає рішення (ОПР), значно полегшити розробку антикризових стратегій.

Інтегрована інформаційно-аналітична система моніторингу та моделювання антикризового розвитку підприємства містить автоматизоване робоче місце (АРМ) ОПР, підсистему управління наповненням інформації та централізовану базу даних, підсистему консолідованої інформації для ОПР, управляючу підсистему, що включає АРМ осіб, які готують стислий огляд ситуації і оцінюють перспективи її розвитку у сферах стратегічного менеджменту, маркетингу, виробничого, кадрового та фінансового менеджменту, підсистему інфраструктури менеджменту, яка включає АРМ осіб, які здійснюють цілеспрямований пошук та збір інформації в сферах інформаційного, інноваційного, інвестиційного, проектного менеджменту, управління безпекою бізнесу та консалтингу, її структуризацію та зберігання, попередню обробку і моніторинг інформації, яка необхідна фахівцям управляючої підсистеми. Ця система має централізовану базу даних, яка є спеціалізованою антикризовою базою даних, що містить актуальну і архівну інформацію з стратегічного менеджменту, маркетингу, виробничого, кадрового та фінансового менеджменту, інформаційного, інноваційного, інвестиційного, проектного менеджменту, управління безпекою бізнесу і консалтингу, що сформована фахівцями відповідних підрозділів і відповідає критеріям антикризового розвитку. Вона має також підсистему консолідованої інформації для ОПР, яка представляє блок інтегрованої інформації, що містить агреговані дані та прогнози розвитку

ситуації у зовнішньому і внутрішньому середовищі, пропозиції відносно подальших дій, що дає можливість розробляти моделі антикризового розвитку. загальну структурну схему наповнення підсистеми консолідованої антикризової інформації, яка спрямовується на АРМ ОПР, зображено на рисунку 1.4 [76].

Рис. 1.4. Структурна схема наповнення підсистеми консолідованої антикризової інформації.

Відомий спосіб прогнозування викидонебезпечності масиву гірських порід, який включає аналіз змін сили тяжіння в конкретній зоні масиву, облік геологічних порушень, розрахунок несприятливих часових інтервалів [74]. Однак даний спосіб не забезпечує можливість прогнозування конкретного місця і часу будь-якої аварії в шахті. Автори роботи [93] стверджують, що всі матеріальні об'єкти мають свою тривимірну полярність. Гірничі машини, транспортні засоби, різні механізми, електрообладнання та інші об'єкти при безаварійному стані мають нормальну полярність. Зміна енерго-інформаційного стану технічного об'єкта може привести до зміни полярності і аварій. Ретроспективний аналіз фантомів технічних систем, які опинилися в аваріях, показав, що всі вони мали зворотну полярність [23].

На основі квантового підходу ними розроблений спосіб прогнозування аварійних ситуацій в шахтах [73]. Спосіб здійснюється шляхом дистанційного визначення і контролю інтегральних параметрів полярності і напрямку обертання локального торсіонного поля системи гірський масив-видобуток. Для аналізу стану безпеки окремих виробок, ділянок або шахт в цілому використовують їх моделі, план гірничих робіт, технологічні схеми, що їх характеризують. Виявлено, що поєднання нормального розподілу знаків полярності з правостороннім торсіонним полем означає безаварійне стан об'єкта. А зворотна полярність в поєднанні з лівостороннім торсійним полем означає, що аварійна ситуація виникла. Між нормаль-

ним і аварійним станом об'єкта існує перехідний стан, коли полярність об'єкта змінена на зворотну при збереженні правостороннього торсіонного поля. Момент виникнення аварійної ситуації визначають відповідно до виразу $m_a = m_c + Аг_c \pm Аг_в$, де m_a – момент виникнення аварійної ситуації в часі; m_c – момент появи сигналів про можливу аварійної ситуації; $Аг_c$ – тривалість загрозливого стану об'єкта; $Аг_в$ – середньостатистичне відхилення від значення $Аг_c$. Момент появи сигналу про можливу аварійної ситуації визначають з виразу $m_c = m_m - Am_p$, де m_m – момент поточного часу, коли був виявлений сигнал про можливу аварійної ситуації; Am_p – затримка прийому оператором аварійного сигналу. Контроль за станом гірських масивів і виробок з даного способу здійснюється шляхом періодичного тестування їх методом біолокації. Періодичність тестування визначають з таким розрахунком, щоб залишався час для виконання превентивних заходів проти можливої аварійної ситуації або аварії. Спочатку тестують систему в цілому, наприклад шахту. Потім тестують окремі ділянки і виробки. Аналіз аварій, що сталися на шахтах Донбасу, показав, що сигнал про можливу аварійну ситуацію з'являється не тільки на аварійній ділянці, а й по шахті в цілому, тобто система за допомогою торсіонних полів і випромінювань відгукується на зміни в її підсистемах і елементах. Перевагою квантового способу прогнозування аварійних ситуацій в підземних виробках є можливість дистанційного та оперативного отримання інформації про можливу аварійну ситуацію до її виникнення. Спосіб дозволяє визначити місце і час аварії, в тому числі: раптові викиди вугілля, породи і газу; спалахи і вибухи газу; пожежі; обвалення породи; аварії на гірничодобувному, гірничотранспортного і електротехнічному устаткуванні; травмування гірників; теплові удари та інше [94]. Даний метод є повністю універсальним і може використовуватися не лише в гірничій галузі. Однак для використання даного методу на сьогоднішній день не сформована відповідна теоретико-доказова база.

Дослідження російського сегменту ринку програмних продуктів забезпечення безперервності бізнесу показало, що виявлені в публічному доступі продукти призначені для моделювання розвитку та наслідків надзвичайних ситуацій конкретного типу (Автоматизована система підтримки прийняття рішень з ліквідації надзвичайних ситуацій на хімічно небезпечних об'єктах, Програма «АХОВ», Програма «ТОКСІ», Програма «АМІАК», Програма «ЕКСПРЕС-ОЦІНКА», Програмний комплекс ТОКСІ + (Версія 4.1) («ТОКСІ + RISK»), Програмний комплекс з розрахунку наслідків аварій ТОКСІ +, Модуль «Ризик НС (оператор)», ArcMap, ArcScene, «РизЕкс - 2», Дослідницький програмний комплекс моделювання аварій

і оцінки ризику. Модуль «Розсіювання НХР. РД52»), що може бути використано в колекції сценаріїв ліквідації критичних ситуацій, але не для комплексної підтримки управління критичними ситуаціями [92].

З метою оптимізації процесів інформаційної підтримки управління кризовими ситуаціями в [92] розроблена стратифікована модель управління промисловою безпекою організації / підприємства. Нормативний страт моделі насичений відомостями про технології, підходи, методики ліквідації критичних, у тому числі надзвичайних, ситуацій, сконцентрованими в нормативних документах федерального і галузевого рівнів. У структурі програмного комплексу програмного страта моделі управління кризовими ситуаціями ключовими об'єктами є підприємство / організація, небезпечний виробничий об'єкт, технологічний процес, речовина / небезпечна речовина, проблема / збій / аварійна ситуація. Надзвичайна ситуація характеризується наступною інформацією: можливі причини аварії; система протиаварійного захисту; відомості про заходи щодо локалізації та ліквідації наслідків аварій на декларованому небезпечному виробничому об'єкті і т.д. Для забезпечення можливості прогнозування виникнення аварійної ситуації експерт задає для кожної неполадки два вектора ймовірностей. Перший вектор вказується за допомогою значень в діапазоні від 0 до 1 і визначає ймовірність того, що відбудеться надзвичайна ситуація з певної групи сценаріїв аварій. Другий вектор містить значення ймовірностей того, що станеться конкретна аварія з групи сценаріїв надзвичайної ситуації. Висновок про найбільш вірогідну групу сценаріїв аварії робиться за формулою Байеса. Спочатку ймовірність кожної альтернативи задається як результат ділення 1 на кількість груп сценаріїв надзвичайних ситуацій або аварій відповідно. Перемноживши, по Байесу, вектора ймовірностей всіх вказаних користувачем неполадок (проблем), отримується вектор, що характеризує найбільш ймовірні групу сценаріїв і аварію, її значення ймовірності буде максимальним [92] Запропонована система відповідає вимогам універсальності і за умов спеціального налаштування може бути використана в ІБ. Подібна експертна система запропонована в [31,123,160].

Доступні для аналізу сучасні методи та технології підтримки дій диспетчера в основному спрямовані на створення апаратної підтримки ранньої стадії виявлення аварій [37] і систем оповіщення [45]. Наприклад, комплекс автоматизованих систем раннього виявлення надзвичайних ситуацій та оповіщення, що розробляється підприємствами ТОВ ВНФ «Елон-ТТ» (м. Харків), ТОВ НВП «Озон-С» (м. Дніпропетровськ) та ТОВ «Оптіма-Комплекс» (м. Запоріжжя), призначений

для реалізації наступних операцій: раннього виявлення загрози виникнення надзвичайних ситуацій (контроль до критичних параметрів); виявлення надзвичайних ситуацій (контроль критичних параметрів); оповіщення працюючого персоналу та інших осіб, які перебувають на території ВАТ «Запоріжкокс», керівного складу, відповідальних посадових осіб територіальних органів МНС та цивільного захисту населення, органів виконавчої влади про загрозу або виникнення КС. Даний комплекс задовольняє вимогам наказу МНС України № 288 і може бути базовим для підтримки дій диспетчера підприємства, але цей комплекс не вирішує завдання прогнозування наслідків аварії з урахуванням поточних реальних умов. До локальних систем оповіщення, керованим диспетчером, відносяться такі системи, як комплекс централізованого оповіщення «Співак» або комплекс централізованого оповіщення «Зоря» [45]. Дані системи виконують тільки частину функцій, покладених на диспетчера і пов'язаних з автоматичним сповіщенням. Основним недоліком цих систем є неможливість динамічного формування таблиць оповіщення і повна відсутність підтримки дій диспетчера в прогнозуванні та координації служб при ліквідації наслідків аварії. У Росії останнім часом створюється загальноросійська комплексна система інформування та оповіщення населення в місцях масового перебування людей (ОКСІОН) – комплекс сучасних систем спостереження, інформування та оповіщення, що розробляється в рамках Федеральної цільової програми «Зниження ризиків і пом'якшення наслідків надзвичайних ситуацій природного і техногенного характеру в Російської Федерації до 2010 року». До середини 2010 року збудовано та введено в експлуатацію всього 520 термінальних комплексів ОКСІОН. Весь комплекс знаходиться в управлінні ГУ ІЦ «ОКСІОН» – (Державна установа: «Інформаційний центр Загальноросійської комплексної системи інформування та оповіщення населення в місцях масового перебування») [1]. Цей комплекс має структуру і функції загальнодержавного рівня із застосуванням в регіональному масштабі. Незважаючи на складне і множинне функціональне і програмно-апаратне забезпечення, вхідні дані такої системи не можуть бути суміщені з даними конкретного підприємства, що дозволяють встановити масштаб аварії і провести достовірний прогноз. У всякому разі в такому комплексі немає підтримки дій диспетчера та формування динамічних таблиць оповіщення.

Метод прогнозування наслідків та модель автоматизованої системи підтримки дій диспетчера небезпечного виробництва при виникненні аварійних ситуацій, запропонований в [59], базуються на розгляді складної фізичної системи (СФС),

що включає в себе небезпечне виробництво, диспетчерську службу, апаратну систему контролю технічного стану виробництва як єдину інформаційну структуру. Математична модель процесу прийняття рішень ОПР при виникненні і розвитку аварій на небезпечному виробництві заснована на послідовності перетворень. Ця модель представлена кортежем виду $D=\langle \vec{T},\vec{P},\vec{M},\vec{E},\vec{R} \rangle$, де $\vec{T}$ – вектор параметрів стану засобів технічного забезпечення оповіщення та визначення погодних умов; $\vec{P}$ – вектор параметрів, що визначають розташування джерел небезпеки в метричному просторі; $\vec{M}$ – вектор параметрів, що характеризують масштаби і величини параметрів аварійного процесу; $\vec{E}$ – вектор текстових семантичних параметрів, що визначають тип аварійної події; $\vec{R}=[R_d,R_s]^T$ – вектор величин параметрів, що характеризують дії диспетчера R_d в різних ситуаціях і список оповіщення R_s, сформований динамічно на основі даних прогнозу. Таким чином, необхідно в заданий час провести: введення початкової інформації; виконати математичне моделювання несприятливих фізичних процесів; провести аналіз отриманих даних і виділити об'єкти, для яких прогнозовані наслідки перевищують прийнятний рівень $\vec{M}_к > \vec{M}_{приєм}$, де $\vec{M}_{приєм}$ – вектор значень прийнятних наслідків; визначити значення вектора параметрів $\vec{R}$, що характеризують реакцію СФС на вплив; виконати операції інформаційного забезпечення засобів автосповіщення. Передбачається, що в процесі роботи виробництва в аварійній ситуації за допомогою програмних засобів ведеться моніторинг стану СФС в реальному часі [59]. Автоматизований програмно-апаратний комплекс (АПАК), розроблений на основі даної моделі, складається з наступних складових: 1. Програмний модуль, що містить засоби моделювання несприятливих фізичних процесів і дозволяє проводити попередній аналіз і прогнозування розмірів областей і значень параметрів вражаючих факторів для зазначених видів загроз; 2. Програмний модуль, що дозволяє формувати, доповнювати і редагувати базу даних, що містить інформацію про джерела небезпеки, види загроз, обслуговуючий персонал, служби і об'єкти відповідальності; 3. Апаратна група, що включає в себе: комплекс датчиків, локальну мережу комп'ютерів, програмне забезпечення для збору, обробки і відображення інформації, автоматичну цифрову метеостанцію, локальну систему оповіщення та АТС, керовані цифровими комутованими засобами [59]. На підставі проведеного аналізу засобами програмного забезпечення формується база даних (БД). У таблицях БД вказуються місця розташування джерел небезпеки. Далі здійснюється прив'язка аварійної ділянки до об'єктних карт, виконаних у реальному масштабі; задаються ра-

строві і векторні карти для відображення; визначаються види загроз, реалізація яких можлива при даному джерелі небезпеки; вводяться дані, необхідні для виконання математичного моделювання та визначення параметрів для прогнозу наслідків аварії. У підсумку формуються таблиці, що містять вимоги щодо обов'язкового оприлюднення і дій диспетчера в умовах КС. Важливою частиною АПАК підтримки прийняття рішень диспетчерської служби при виникненні і розвитку аварій є достовірність та інформаційна повнота прогнозу. Прогноз заснований на використанні даних про реальний стан навколишнього середовища в момент виникнення аварії та наявних у розпорядженні математичних моделей несприятливих фізичних процесів.

Відома система для зменшення збитків та руйнувань в результаті стихійних лих [135]. Основною метою розглянутої системи є зменшення пошкоджень будівлі після землетрусу. Так система призначена для управління зовнішніми комунікаціями надання комунальних послуг, такими як водо-, газо- та електропостачання до окремої будівлі, що знаходиться в зоні ураження. До складу системи входять набори датчиків 3-ьох типів: сенсор виявлення землетрусу, датчики контролю стану приміщень в будівлі (наявність/відсутність затоплень, пожежі, розривів трубопроводів тощо) та датчики контролю постачання комунальних послуг. При отримані сигналу щодо можливості чи факту землетрусу система перевіряє датчики контролю приміщень на наявність пошкоджень і передає сигнал щодо прийняття рішення про відключення або залишення в працюючому стані комунікацій. Наприклад, якщо в результаті руйнувань, спричинених землетрусом, в будівлі виникає пожежа, система приймає рішення про відключення газопостачання або при наявності розривів в газопроводах система терміново відключає електроживлення в будинку з метою унеможливлення появи пожежі. Більш того, система цілеспрямовано не відключає комунікації, які можуть посприяти усуненню негативних чинників під час КС, наприклад, при пожежі система водопостачання залишається працювати в повному об’ємі. Перевірки системою стану будівлі періодично повторюються до усунення всіх негативних факторів. При кожній перевірці стан комунікацій перевіряється і може бути змінений. Рішення системи здійснюються в відповідності до набору правил, зображених на рисунку 1.5, в базі даних, які можуть коректуватися в подальшому.

В правоохоронному документі США [136] описані апарат та метод прогнозування стихійних лих. В основу апарату прогнозування стихійних лих входять комп’ютер, мінімальна конфігурація якого складає наявність процесора і пам’яті,

що містить програму функціонування апарату прогнозування, а також базу даних, в якій записані різноманітні сценарії КС. Крім того апарат отримує дані з метеорологічної станції, дані прогнозу погоди, землетрусів тощо, звіти щодо надзвичайних ситуацій та КС, а також має зв'язок з супутниковим сателітом, що передає картографічну інформацію та географічні координати КС через мережу Інтернет, і різними адміністративними органами, такими як міністерства.

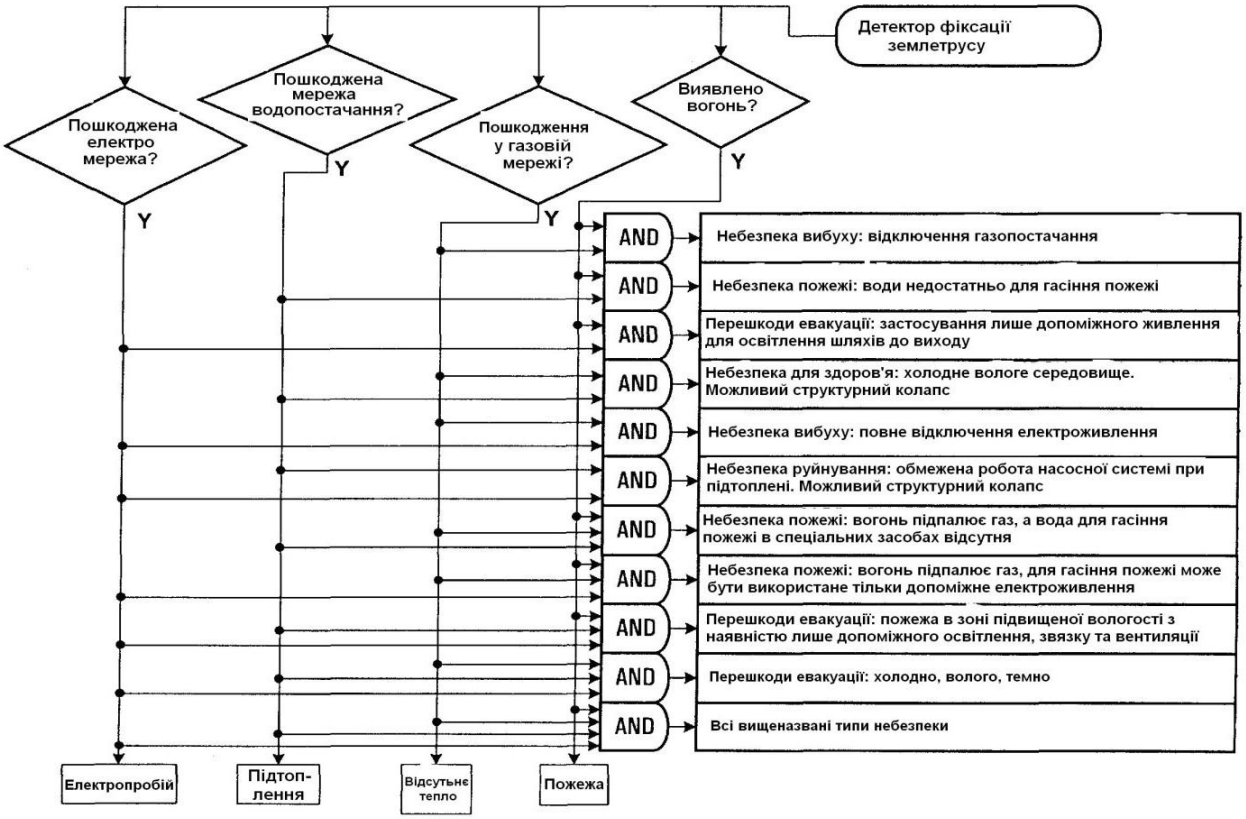


Рис. 1.5. Схематичне зображення набору правил контролю комунікацій.

Типова структура описаного апарату наведена на рисунку 1.6. Виконуючи свої функції комп’ютер посилає запит щодо надання супутникових знімків території, визначає географічні координати місця можливого стихійного лиха, вираховує індекс ризику лиха. Для здійснення прогнозів метеорологічні дані передаються через мережу від метеорологічних центрів або приватних метеорологічних компаній, таких як автоматизована метеорологічна система отримання і накопичування даних (AMeDAS). До них відносяться інформація щодо цунамі, землетрусів, вулканічної діяльності, штормових попереджень, довгострокові прогнози, матеріали спостережень, спеціальна погодна інформація, авіаційні погодні матеріали і т.п. Крім того, також через мережу передаються дані прогнозу погоди та відомості з сейсмічних станцій.

Метод прогнозування стихійних лих полягає в наступних кроках: 1) отри-

мання та аналіз метеоданих, 2) у випадку якщо вони перевищують встановлені порогові значення робиться запит до супутника на отримання картографічної інформації, 3) отримані супутникові дані порівнюються з стандартними і пікселі, в яких поточні значення менші або рівні пороговим видаляються, тобто визначається область ураження, 4) відправляється аварійне повідомлення, в якому вказано тип та місце можливого стихійного лиха, 5) реєструється факт відправлення аварійної почти та її вміст.

Рис. 1.6. Типова структура апарату прогнозування стихійних лих.

Подібна система, описана в [140], для прогнозування землетрусів з використанням сейсмічних вимірювань вираховує координати його епіцентру, силу землетрусу та зону враження. Отримані дані передаються на термінали системи.

Описаний в [139] статистично-детермінований підхід щодо прогнозування стихійного лиха, використовуючи історичні та статистичні дані щодо фіксації в регіоні ураганів, шквальних вітрів, смерчів, а також математичний апарат теорії імовірності та математичні розподіли (Гауса, Пуассона), здійснює прогнозування та оцінку ймовірності появи урагану на певній території.

В [137] розглянуті метод і апарат для попередження КС, що за своєю суттю може бути названий «Евакуаційним гідом». На певній території різних масштабів (будинок, готель, торговельно-розважальний центр) встановлюються датчики, що фіксують появу тої чи іншої КС, переважно орієнтовані на пожежу. В якості датчиків можуть використовуватися температурні датчики, датчики емісії диму, вологи тощо. У випадку появи кризового чинника, тобто виникнення КС, датчики передають на сервер відомості щодо їх місцезнаходження. Опрацювавши отримані дані сервер формує оптимальні маршрути евакуації в онлайн-режимі, враховуючи всі можливі зміни в розвитку ситуації, що включають напрями руху, відстані, розміщення перешкод. Сформований план евакуації передається на мобільні тер-

мінали жителів/персоналу, в тому числі в якості терміналів можуть використовуватися особисті мобільні телефони, комунікатори, цифрові асистенти PDA, приймачі чи інші гаджети. Крім того система здатна управляти електронними засобами, наприклад, блокувати/відкривати електроні замки, двері. Зв'язок між датчиками, сервером та мобільними терміналами здійснюється через радіоканал.

Аналогічним є пристрій, права на якого підтверджені документом [145]. Він визначений автором як динамічний план дій на випадок КС сімейного типу. Користувач, оператор чи урядові агенції можуть генерувати повідомлення про КС, їх масштаб та вказівки необхідних дій, що відсилаються особам в ареалі враження. До того ж можуть бути використані шаблони типових КС і дій при них, що передаються мешканцям районів історично схильним до них. Система дозволяє підтримувати зв'язок членам сім'ї між собою та з оператором до, під час і після КС.

Схожим за призначенням та принципом дії є спосіб управління та апарат контролю за системою протидії лиху [141]. У випадку виникнення КС система підпорядковує собі контроль за радіоканалом в зоні враження і використовує його для передачі інформації щодо ситуації та її статусу. Повідомлення передаються через мережі мобільної комунікації та стаціонарні мережі на користувацькі термінали в зоні розповсюдження КС. Є можливість відправляти швидкі повідомлення, задавати їх пріоритет в радіоканалі, блокувати непідтверджені повідомлення, Користувач може підписатися на оновлення щодо ситуації в реальному часі, створювати, передавати і отримувати повідомлень 5-ти видів: дані статусу КС, текстові коментарі, зображення місця КС, відео з місця локалізації КС, голосові повідомлення.

Відомі метод та апарат [138] для визначення ймовірності КС в сфері комунікацій, а саме в мережі чи її частині, та збитків, принесених ними. Тобто він напряму використовується в питаннях менеджменту ІБ, але сфера його використання досить обмежена. Апарат та метод можуть бути використані як для окремих елементів мережі, множини елементів мережі, всієї мережі та множини мереж.

Визначення очікуваного впливу різних КС на систему комунікацій і її різні частини здійснюється з використанням моделі аналізу КС, що є комбінацією моделі мережі і моделі КС. Модель КС охоплює різні типи ситуацій згідно їх структури (представлення специфічних категорій моделлю Пуассона) і параметрів. Серед специфічних категорій виділені стихійні лиха, технічні аварії або ситуації, пов'язані з людським фактором. До стихійних лих розробники відносять землетруси, торнадо, паводки, до технічних – відмови електроживлення, витоки газу, а

до людських – тероризм, вандалізм тощо. Взаємозв'язок параметрів цих моделей описується у вигляді матриці. Так, одне з основних місць займає матриця ймовірності впливу КС D на елемент системи E: $\begin{bmatrix} Parametr(Pd) & E1 & ... & EN \\ D1 & Pd(E1,D1) & ... & Pd(EN,D1) \\ ... & ... & ... & ... \\ DE & Pd(E1,DE) & ... & Pd(EN,DE) \end{bmatrix}$.

Модель аналізу КС включає в себе параметри для визначення кількісної імовірності того чи іншого пошкодження в різних сегментах мережі. Так, імовірність виникнення КС D дану кількість раз (a) протягом періоду часу T в елементі мережі E визначається як $Pd_{(E_i,D_j)}(a,T) = e^{-(Rd_{(E_i,D_j)} * Ph_{(E_i,D_j)} * T)} \left[\frac{(Rd_{(E_i,D_j)} * Ph_{(E_i,D_j)} * T)^a}{a!} \right]$, де Rd – норма виникнення Кс, Ph – імовірність, що КС вплине на елемент E. Також модель аналізу КС використовується для визначення її впливу на мережу. Наприклад, до параметрів впливу відносять вартість заміни пошкоджених елементів мережі, вартість переривання надання послуг, втрату доходів, штрафи SLA і інші. В методі пропонується вираховувати вартість заміни пошкодженого обладнання елементу мережі E внаслідок впливу КС D за виразом $Gbm_{(Ei,Dj)} = Pg_{(Ei,Dj)} * Pk_{(Ei,Dj)} * Ce_{(Ei,Dj)}$, де Pg – параметр пошкодження основного обладнання, Pk – імовірність пошкодження елементу мережі, Ce – вартість відновлення елементів мережі. А вартість переривання обслуговування елемента мережі як $Sbm_{(Ei,Dj)} = Sl_{(Ei,Dj)} * Pk_{(Ei,Dj)} * Si_{(Ei,Dj)} * MTTR_{(Ei,Dj)}$, де Sl – вартість переривання обслуговування, Si – індикатор переривання обслуговування мережевого елемента, $MTTR$ – середній час відновлення елементу мережі. Таким чином вартість впливу КС на мережу становить $Cbm_{(Ei,Dj)} = Gbm_{(Ei,Dj)} + Sbm_{(Ei,Dj)}$.

Розробка [142] включає в себе систему, метод та комп'ютерну програму для оцінки ризику КС в IT-інфраструктурі. Запропонований метод і система ґрунтуються на теорії небезпек. Вхідними даними в даному випадку є інформація про час і серйозність попередніх інцидентів. На основі залежності між попередніми інцидентами (відповідним часом виникнення та силою негативного впливу), використовуючи статистичні залежності між ними, що описуються поліномом Чебишева $P_n(x) = \sum_{i=1}^{n} (y_i \prod_{j=1}^{n} \frac{(x - x_j)}{(x_i - x_j)})$, здійснюється оцінка ризику майбутніх інцидентів та їх величини, тобто можливий час виникнення і серйозність наслідків майбутньої КС. Метод оцінки ризику майбутньої КС в IT-інфраструктурі включає наступні кроки: 1) ідентифікація часу попередніх КС, 2) визначення рівня серйозності

(величини впливу) попередніх КС, 3) побудова функції полінома Чебишева на основі співвідношення отриманих на етапах 1-2 даних щодо попередніх КС і 4) оцінка ризику майбутніх КС в ІТ-інфраструктурі. Реалізована система вміщує в собі відповідні засоби для реалізації кроків вищеописаного методу.

Відома система прогнозування катастроф або КС [143] грунтується на методах, що оперують поняттями нормальності та ненормальності на основі порівняння поточних значень з пороговими значеннями. Система прогнозування КС складається власне з апарату прогнозування, що збирає, обробляє, зберігає, приймає та передає сигнали ненормальності, та множини мобільних радіоапаратів комунікації (термінали), які збирають та передають інформацію щодо ситуації до центрального апарату через мережу радіозв'язку. Мобільні радіоапарати вміщують в собі модуль визначення місцезнаходження, модуль виявлення ненормального сигналу (тут отримавши електромагнітний сигнал з навколишнього середовища датчик визначає ненормальний сигнал і формує сигнал виявлення ненормальності), 1-ий модуль комунікацій, що передає актуальне місцезнаходження на апарат управління місцезнаходженням, а сигнал виявлення ненормальності – до апарату прогнозування, а також здійснює зворотний зв'язок. Апарат управління місцезнаходженням фіксує і контролює положення і географічні координати кожного мобільного терміналу. Центральний апарат прогнозування складається з 2-ого модуля комунікацій (отримує сигнали ненормальності та інформацію щодо місцезнаходження від множини мобільних терміналів і у відповідь передає сформовану інформацію щодо КС назад) та модуля прогнозування КС, який збирає та аналізує сигнали ненормальності і прогнозує виникнення стихійного лиха, визначає області ураження та формує аварійні повідомлення. До складу модуля прогнозування входять блок зберігання порогового значення, з яким порівнюється електромагнітний сигнал (визначається середнє та максимальне значення рівня сигналу), і, власне, блок порівняння, що продукує сигнал виявлення КС у випадку якщо рівень електромагнітного сигналу перевищує рівень порогу. Тут приймається рішення щодо прогнозу КС. Крім того, до складу системи прогнозування КС входить модуль приведення в стан готовності, в якому формуються звукові, вібраційні, світлові, графічні та відеосигнали, пов'язані з КС та її перебігом. Система є достатньо універсальної з точки зору її використання щодо різних КС, але не підтримує всі етапи КУББ.

Метод і система формування планів реагування на КС (по суті планів ЗББ) та оцінки впливів на бізнес, описана в [144] поєднують в собі функції прогнозування

динаміки КС і планування бізнесу, полегшуючи обчислення фізичних і інших ефектів від КС в грошовому виразі. А також дозволяють користувачу оцінити витрати на реалізацію різних окремих планів ЗББ чи їх комбінацій, вибрати оптимальний набір заходів. Це досягається через системний аналіз багатьох сценаріїв КС, за рахунок аналізу потенційного впливу КС на ділові операції, фізичну і IT-інфраструктуру, персонал та клієнтів, ділових партнерів, витрати на сервісне обслуговування. Система може бути використана користувачем як локально так і через мережу, в тому числі Інтернет. Система складається з таких складових (рисунок 1.7): калькулятор динаміки КС, калькулятор інфраструктурних чинників, калькулятор економічних чинників, калькулятор поведінкових чинників і калькулятор ефективності бізнесу та блок введення вхідних параметрів та корегування планів реагування. Таким чином система і метод з використанням комп'ютерних потужностей проводить інструктаж щодо BIA і ризиків, пов'язаних з КС. До вихідних функцій системи відносяться: 1) обчислення матеріальної або глобальної динаміки КС, 2) обчислення психологічних, економічних і/або фізичних впливів КС, включаючи, але не обмежуючись потенційними взаємозалежностями між цими чинниками і динамікою КС, 3) обчислення фінансових і експлуатаційних впливів КС, 4) оцінка ефектів різних планів реагування і витрат на їх виконання, 5) оптимізація планів відносно однієї чи декількох бізнес-цілей. В процесі роботи системи використовуються методи моделювання для того, щоб вирахувати глобальну динаміку КС, виміряти психологічні, фізичні та економічні впливи на підприємстві і ефекти від впровадження різних планів ЗББ, наприклад зберігання резервного інвентарю та обладнання, розподіл вакцин, навчання та інструктажі персоналу, договори з постачальниками, закриття окремих ланок підприємства та евакуація працівників. Для характеристики планів реагування на КС використовують ряд параметрів, а саме рівень запасів інвентарю в резерві, ефективність евакуації, ефективність вакцин, часові характеристики виконання плану УББ (період старту і закінчення) тощо. Оптимізації планів реагування може здійснюватися шляхом: 1) модифікації структури залежностей між постачальниками, партнерами та клієнтами підприємства, фізичною і IT-інфраструктурою, 2) модифікації детальних параметрів планів, 3) модифікації тривалості планів. Сутність цих змін може бути визначена через проект одного чи декількох експериментів, який систематично досліджує вказані параметри і ідентифікую їх комбінацію оптимальну для роботи підприємства відносно тієї чи іншої бізнес-цілі. Плани реагування на КС, якими підприємство не керує (наприклад, державні, міністерські плани) мо-

жуть задаватися як незмінні. При введені відповідних параметрів така система може бути використана в менеджменті ІБ.

Рис. 1.7. Структура системи формування планів ЗББ та оцінки впливів КС.

Детально розглянувши описані засоби, визначимо основні параметри їх функціонування, вхідні і вихідні дані, принципи роботи та основні галузі застосування. Отримані результати наведемо в вигляді таблиці 1.3 та таблиці 1.4.

В таблиці використані такі позначення: + – так, +/- – частково, скоріше так, -/+ – скоріше ні, - – ні. Під універсальністю розуміється характеристика, що визначає здатність системи бути використаною для управління КС різного роду та походження в різних галузях без необхідності їх пере налаштування з підтримкою більшості ключових етапів КУББ.

Таблиця 1.3

Порівняльний аналіз сучасних систем управління кризовими ситуаціями

Засіб	Вхідні дані	Принцип функціонування	Вихідні дані	Галузь застосування/ Використання в ІТ
Система раннього виявлення надзвичайних ситуацій [78] (Україна)	Статистичні дані метеоумов, параметри контрольованих отруйних речовин (концентрація і т.п.)	Оперативний режим: компараторний принцип. Імітаційний режим: моделювання на основі статистичних даних	Сигналізація щодо КС, прогноз розвитку та динаміки	Промислова безпека / не використовується
Система раннього виявлення надзвичайних ситуацій [71] (Україна)	Параметри датчиків в техногенно небезпечних зонах	Компараторний принцип, теорія прийняття рішень	Контроль технологічних процесів, підтримка прийняття рішень в умовах КС	Промислова безпека / не використовується
Інтегрована інформаційно-аналітична система моніторингу та моделювання антикризового розвитку підприємства [76] (Україна)	Актуальна і архівна інформація щодо управління підприємством (менеджмент, маркетинг, фінансові показники, безпеки тощо).	Аналітична та консолідована обробка інформації, теорія прийняття рішень, експертні підходи	Прогноз розвитку ситуації, розробка рекомендацій, моделювання варіантів антикризового розвитку	Менеджменет / частково використовується
Спосіб прогнозування викидонебезпечності масиву гірських порід [74] (Україна)	Геологічні дані, вимірювання сили тяжіння	Аналіз зміни сили тяжіння, геологічних порушень Статистичні характеристики	Прогноз викидів в гірських масивах	Гірничодобувна галузь / не використовується
Спосіб прогнозування аварійних ситуацій в підземних гірничих виробках [73, 93] (Україна)	Інтегральні параметри полярності і напрямку обертання локального торсіонного поля	Теорія торсіоних полів, квантові методи вимірювання	Прогнозування КС в шахтах	Гірничодобувна галузь / не використовується

Продовження табл.1.3.

Програмний страт моделі управління кризовими ситуаціями [92] (РФ)	Параметри технологічних процесів, вектор ймовірностей реалізації сценаріїв, вектор ймовірностей реалізації аварій	Байесівські мережі, теорія ймовірностей	Прогноз загальної ймовірності реалізації КС, моделі ліквідації наслідків	Менеджменет, промислова безпека / не використовується
Автоматизована система підтримки дій диспетчера небезпечного виробництва при виникненні аварійних ситуацій [59] (РФ)	Місця розташування джерел небезпеки, прив'язка аварійної ділянки до об'єктних карт, види загроз, дані про ландшафтні, погодні умови	Математична модель прийняття рішень в складній фізичній системі	Відомості про небезпечні зони, ступені загрози в прилеглому просторі; кількість і місця знаходження людей, що потрапляють в зону ураження, заздалегідь підготовлені дані про можливі шляхи евакуації	Менеджменет, промислова безпека, безпека населення / не використовується
System for reducing disaster damage – Система для зменшення збитків та руйнувань в результаті стихійних лих [135] (США)	Дані сенсорів виявлення землетрусу, датчиків контролю стану приміщень в будівлі та датчиків контролю постачання комунальних послуг	Системний аналіз стану контрольованого об'єкта, теорія прийняття рішень, компараторний принцип	Контроль комунікацій в приміщені під час КС	Цивільний захист населення під час землетрусів / не використовується
Disaster predicting method, disaster predicting apparatus, disaster predicting program – Апарат прогнозування стихійних лих [136] (США)	Сценарії КС, метеодані, звіти щодо КС, картографічні дані з супутника	Обробка статистичних даних, компараторний принцип, обробка растрового зображення	Обчислення рівня ризику стихійних лих, визначення географічних координат. Сигналізація	Цивільний захист населення від природних стихійних лих / не використовується
Statistical-deterministic approach to natural disaster prediction – Статистично-детермінований підхід щодо прогнозування стихійного лиха [139] (США)	Статистичні та історичні дані метеорологічних спостережень	Математичний апарат теорії імовірності та статистичних розподілів (Гауса, Пуассона)	Прогнозування стихійних лих, сигналізація	
Method and apparatus for disaster prevention – «Евакуаційний гід» [137] (США)	Параметри датчиків контролю стану приміщень (температурні датчики, датчики емісії диму, вологи)	Компараторний принцип, використання наборів сценаріїв поведінки	Виявлення КС. Сигналізація, рекомендації та контроль за евакуацією	Цивільний захист населення в громадських та розважальних місцях, місцях проживання / не використовується
Dynamic emergency disaster plan – Динамічний план дій на випадок КС [145] (США)	Сигнал про КС	Статистичні та історичні дані, використання наборів сценаріїв поведінки, моделювання	Сигналізація, рекомендації та контроль за евакуацією, рекомендовані плани дій в умовах КС	
Method and apparatus for quantifying an impact of a disaster on a network – Метод та апарат для визначення впливу КС на комп'ютерні мережі [138] (США)	Вартість обладнання та відновлюваних робіт, вартість переривання обслуговування (встановлюється експертом), $MTTR$ – середній час відновлення	Теорія ймовірності, теорія небезпек, статистичні розподіли Пуасона, системний аналіз об'єктів, методики аналізу впливу на бізнес	Вартість впливу КС на комп'ютерну мережу, зокрема ІТ інфраструктуру	ІТ-інфраструктура, відновлення бізнес-процесів після КС в КУББ / використовується
System, method and program for estimating risk of disaster in infrastructure – Система, метод та комп'ютерна програма для оцінки ризику КС в ІТ-інфраструктурі [142] (США)	Інформація про час і серйозність попередніх інцидентів	Теорія небезпек, статистичні залежності між попередніми і майбутніми інцидентами (задаються поліномом Чебишева)	Оцінка ризику майбутніх інцидентів та їх величини (серйозності наслідків)	ІТ-інфраструктура, прогнозування та оцінка ризиків, КУББ / використовується
Disaster prediction system – Система прогнозування КС (катастроф) [143] (США)	Парметри датчиків контролю навколишнього середовища у вигляді електромагнітних сигналів	Теорія небезпек, апарат еталоних значень (нормальності / ненормальності), компараторний принцип	Прогноз виникнення стихійного лиха, визначення області ураження. Сигналізація (аварійні повідомлення)	Менеджменет, промислова та цивільна безпека / не використовується
Method and system for disaster mitigation planning and business impact assessment – Метод і система формування планів реагування на КС (та оцінки впливів на бізнес [144] (США)	Сценарії КС, параметри технічного, фінансового характеру щодо управління підприємством та планів УББ	Моделювання ситуацій, режиму функціонування ІС чи підприємства в цілому. Експертні підходи	Обчислення фізичних і інших ефектів від КС в грошовому виразі, підбір оптимального набору заходів реагування на КС	Аналіз впливу на бізнес (BIA), менеджмент / частково використовується

Таблиця 1.4.

Основні ознаки систем управління кризовими ситуаціями

Засіб	Функціонування в нечіткому слабоформалізованому середовищі	Застосування в менеджменті ІБ	Підтримка прогнозування КС	Підтримка ідентифікації КС	Підтримка оцінки КС	Підтримка реагування на КС та ліквідації їх наслідків	Універсальність	Використання параметрів, характерних для КС в ІБ
Система раннього виявлення надзвичайних ситуацій [78] (Україна)	-	-	+	+	+/-	+/-	-	-
Система раннього виявлення надзвичайних ситуацій [71] (Україна)	-/+	-	+	+	-	-	-	-
Інтегрована інформаційно-аналітична система моніторингу та моделювання антикризового розвитку підприємства [76] (Україна)	-	+/-	-/+	-/+	+	+	+	-
Спосіб прогнозування викидонебезпечності масиву гірських порід [74] (Україна)	-	-	+	+	-	-	-	-
Спосіб прогнозування аварійних ситуацій в підземних гірничих виробках [73, 93] (Україна)	-	-	+	-	-	-	-	-
Програмний страт моделі управління кризовими ситуаціями [92] (РФ)	-	-/+	+	-/+	-/+	-	-/+	-
Автоматизована система підтримки дій диспетчера небезпечного виробництва при виникненні аварійних ситуацій [59] (РФ)	-	-	+/-	+/-	+	+	-/+	-
Система для зменшення збитків та руйнувань в результаті стихійних лих [135] (США)	-	-	+	-	-	+	-	-
System for reducing disaster damage [136] (США)	-	-	+	+/-	+/-	-	-	-
Statistical-deterministic approach to natural disaster prediction [139] (США)	-	-	+	+	-	-	-	-
Method and apparatus for disaster prevention [137], Dynamic emergency disaster plan [145] (США)	-	-	-	+	-	+	-	-
Method and apparatus for quantifying an impact of a disaster on a network [138] (США)	-	+	+/-	-/+	+	-/+	+/-	-/+
System, method and program for estimating risk of disaster in infrastructure [142] (США)	-	+	+	-	+	-	-	-
Disaster prediction system [143] (США)	-	-	+	+	-	-	-/+	-
Method and system for disaster mitigation planning and business impact assessment [144] (США)	-	+/-	-	-	+	+	-/+	-

1.4. Висновки до першого розділу

1. Проаналізовано базові поняття КУББ, зокрема поняття кризової ситуації, їх класифікації. Проведений аналіз показав, що в різних трактуваннях даний термін завжди включає такі характеристики як збитки, загрози функціонування, наявність жертв, непередбачуваність та раптовість. Крім того на сьогодні відсутня універсальна класифікація КС, що відображала б усі аспекти пов’язані з безперервністю бізнесу (роботи ІС) та необхідні для формування інтегрованої моделі представлення ІПКС, розробки методів та засобів управління КС.

2. Визначено місце та взаїмозвяки СУКС з компонентами СМІБ. Досліджено

основні стандарти, методи і стратегії ЗББ та технології, що їх реалізують, проведений аналіз представлених на ринку систем та засобів УББ. В результаті встановлено, що ринок таких засобів достатньо структурований та розвинений, за винятком засобів безпосереднього прогнозування та оцінки КС.

3. Проведений аналіз відомих систем та засобів управління КС, що включає в себе прогнозування, ідентифікацію, оцінку КС та реагування на неї з метою виділення основних принципів їх побудови, переваг та недоліків. Аналіз показав, що значна частина розробок в даній галузі ґрунтується на застосування різноманітних датчиків та порогового механізму за принципом компаратора. Недоліком таких систем є складність їх застосування в умовах невизначеності та виникненні невідомих типів КС. Також відомі системи, що під час своєї роботи застосовують історичні, статистичні та математичні методи (статистичні закони розподілу, теорія ймовірностей, Байєсівські мережі тощо), які є надто ресурсоємні та трудомісткі. Також відсутні універсальні системи, що можуть бути застосовані в будь-якій галузі та на всіх етапах управління КС.

РОЗДІЛ 2. МОДЕЛІ ВИЯВЛЕННЯ ТА ОЦІНКИ КРИЗОВИХ СИТУАЦІЙ

2.1. Узагальнена класифікація та інтегрована модель представлення інцидентів/потенційних кризових ситуацій

Важливим аспектом КУББ є управління КС, що включає в себе ряд процесів, а саме: прогнозування КС, ідентифікація КС, оцінка КС, реагування на КС та ліквідація наслідків, спричинених КС. Для ефективного функціонування кожного з названих етапів управління КС необхідним є розробка інтегрованої моделі КС, що дала б змогу описати будь-яку КС незалежно від її характеристик, причин походження, галузі, яку вона охоплює, тощо. На основі цієї моделі і повинно проводитися прогнозування, ідентифікація та оцінка КС, причому, враховуючи що більшість рішень з приводу управління КС приймається в умовах невизначеності, нечіткості та неформалізованості простору (зокрема щодо галузі ІБ в ІС), на основі експертних методів та на базі нечіткої логіки.

Аналіз поняття і класифікацій КС показав, що на сьогодні відсутня єдина класифікація, що охоплювала б усі аспекти і характеристики КС в аспекті КУББ. Так, в багатьох відомих класифікаціях враховані типології КС щодо їх походження, масштабів, але не враховані показники охоплення організаційних структур, тривалості, прояву КС тощо. Оскільки відображення КС, їх виявлення та оцінка потребують різносторонньої і всеохоплючої характеристики, то наявність узагальненої класифікації є обов’язковою вимогою для формування інтегрованої моделі представлення ІПКС, розробки методів виявлення ІПКС та оцінки критичності ситуації, спричиненої інцидентами.

В процесі дослідження були виділені наступні базові характеристики КС: причина походження подій (джерело), що можуть зумовити виникнення КС, можливість прогнозування, ступінь прояву, глибина вияву кризових явищ, характер виникнення, масштаб прояву КС (в географічному та організаційному аспекті), час дії негативних чинників КС, потенційна загроза людському життю та здоров’ю, кількість жертв, рівень економічних збитків. На основі даних характеристик розроблено класифікацію КС. Узагальнені результати проведеного дослі-

дження зображені на рис. 2.1.

Рис. 2.1. Узагальнена класифікація КС

Пропонується виділити наступні типи КС: природного, техногенного, соціального, економічного та екологічного характеру. В свою чергу природні КС доцільно розділити на біологічні, геологічні (або геофізичні) та гідрометеорологічні, до яких відносять гідро-, метео- та кліматологічні. Техногенні в залежності від необхідності їх деталізації можна розділити за галузями економіки, в яких вони відбулися, або на наступні підкласи: аварії на транспорті, пожежі та вибухи, аварії з викидами небезпечних хімічних речовин, з викидами радіаційних речовин, раптове руйнування будівель та споруд, аварії в електроенергетичних системах, в системах життєзабезпечення, в системах зв'язку та телекомунікацій, у системах нафтогазового промислового комплексу, аварії на очисних спорудах, гідродинамічні

аварії. Соціальні КС доцільно розділити на власне соціальні (шантаж, крадіжка), соціально-психологічні (стрес, паніка, погрози працівнику), соціально-політичні (страйки, трудові конфлікти) та соціально-військові (терористичні акти, повстання, війни). Економічні КС вміщують в собі банкрутства, невиплачені кредитні закупівлі, від'ємний торговий баланс, тощо і не є об'єктом даного дослідження. Серед екологічних КС за способом впливу на біосферу слід виокремити інгредієнтні (надходження в біосферу кількісно і якісно чужих їй речовин), енергетичні (шум, радіація, електромагнітні поля, теплове і світлове забруднення), деструкційні (вирубка лісів, порушення водотоків, зміна ландшафтів) та біоценотичні (вплив шкідливих і небезпечних факторів на склад, структуру і вид популяції) КС [24,85, 91].

Розроблена модель класифікації крім теоретичного носить і практичний характер. Так за нею вихід з ладу почтового серверу в одному з підрозділів організації можна класифікувати наступним чином: аварія у системах зв'язку та телекомунікацій техногенного характеру, несподівана, явна, легка, як суб'єктивна так і об'єктивна, локальна, в межах окремого бізнес-процесу, зазвичай короткотривала, не загрожує людському життю та здоров'ю, зазвичай з невеликими збитками КС. Чилійський землетрус 2010 року класифікується так: геологічна природного характеру, несподівана, явна, глибока, суб'єктивна, регіональна, на рівні групи підприємств, короткотривала, загрозлива для життя і здоров'я людей, катастрофічна за кількістю жертв та з великим економічними збитками.

В розділі 1.1 був проведений аналіз різних трактувань терміна КС та суміжних понять в багатьох сферах людської діяльності, що дозволив відобразити ці поняття в сфері ІБ та виявити особливості кожного з визначень, які є загальними для всіх. Саме за цими особливостями проводиться диференціація між КС та інцидентами інформаційної безпеки (ІІБ). Крім того, встановлено наявність в більшості випадків причинно-наслідкових зв'язків між ними. Так при відсутності контролю існує ймовірність, що ІІБ набуде таких параметрів, які дозволять класифікувати їх як КС. Тобто можна стверджувати, що причиною будь-якої КС є ІІБ з найвищим степенем критичності, що визначається рівнем збитків, числом постраждалих та іншими характеристиками, тобто інцидент/потенційна КС (ІПКС). Питання оцінки критичності інциденту буде розглянуто далі в досліджені.

Для формалізації процесів УКС [32] введемо множину ІПКС:

$$\mathbf{IKS} = \{\bigcup_{i=1}^{n} \mathbf{IKS_i}\} = \{\mathbf{IKS_1}, \ldots, \mathbf{IKS_n}\},\ (i = \overline{1,n}), \qquad (2.1)$$

де n визначає кількість потенційних ІПКС, тобто інцидентів, що можуть спричинити кризовий стан, кожен з яких відображається у вигляді узагальненого шестикомпонентного кортежу за аналогією з [45,48]:

$$\mathbf{IKS_i} = < IKS_i,\ \mathbf{P_i},\ \mathbf{T_i^e},\ \mathbf{PP_i},\ \mathbf{ER_i},\ L\underset{\sim}{C}S_i >, \qquad (2.2)$$

в якому:

IKS_i – ідентифікатор i-го ІПКС, що є (може бути) 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 еталоні стани відповідних параметрів з підмножини $\mathbf{P_i}$;

$\mathbf{PP_i}$ – підмножина поточних значень параметрів за певний проміжок часу;

$\mathbf{ER_i}$ – підмножина евристичних правил, побудованих на основі нечітких параметрів, які використовуються для виявлення/ідентифікації i-го ІПКС;

$L\underset{\sim}{C}S_i$ – рівень критичності ситуації, спричиненої i-м ІПКС.

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

Ідентифікатор IKS_i зв'язує елемент множини **IKS** з певним інцидентом, який визначається через відповідне йому ім'я. Наприклад, при $n = 5$ отримаємо $\mathbf{IKS} = \{\bigcup_{i=1}^{5} \mathbf{IKS_i}\} = \{\mathbf{IKS_1}, \mathbf{IKS_2}, \mathbf{IKS_3}, \mathbf{IKS_4}, \mathbf{IKS_5}\} = \{\mathbf{A}, \mathbf{B}, \mathbf{C}, \mathbf{D}, \mathbf{E}\}$, де **A**, **B**, **C**, **D**, **E** – назви інцидентів. В роботах [50,53] запропонована і описана система та метод для прогнозування та ідентифікації фактів діяльності порушника, в якій виділені такі категорії як порушник-людина (дезінформатор, спамер, хакер та крекер) та порушник-бот (бот-зломщик та спам-бом). Крім того, в роботі [44] розглянута система

та метод виявлення аномальних станів та атак в ІС, зокрема, спуфінг, атаки відмови в обслуговувані і сканування портів. В [65] розглянуті комп'ютерні інциденти, що можуть стати причинами виникнення КС. Узагальнивши дані робіт та проаналізувавши статистику КС та комп'ютерних атак виділимо такі ІПКС як:

- «Проникнення порушника в ІС (злом)» – ZL,
- «Спам» – SP,
- «Мережева атака відмова в обслуговувані (Dos/DDos)» – DD,
- «Вірусна атака» – VA,
- «Вихід з ладу (збій) ІС через вплив мікрокліматичних умов» – ZK.

Отже, множину ідентифікаторів для кількості досліджуваних ІПКС при $n=5$ згідно (1) задамо так: $\mathbf{IKS} = \{\bigcup_{i=1}^{5} \mathbf{IKS_i}\} = \{\mathbf{IKS_1}, \mathbf{IKS_2}, \mathbf{IKS_3}, \mathbf{IKS_4}, \mathbf{IKS_5}\} = \{\mathbf{ZL}, \mathbf{SP}, \mathbf{DD}, \mathbf{VA}, \mathbf{ZK}\}$, де $\mathbf{IKS_1} = \mathbf{ZL}$, $\mathbf{IKS_2} = \mathbf{SP}$, $\mathbf{IKS_3} = \mathbf{DD}$, $\mathbf{IKS_4} = \mathbf{VA}$, $\mathbf{IKS_5} = \mathbf{ZK}$ відображають стани контрольованого середовища при відповідних ІПКС, яким будуть присвоєні ідентифікатори $IKS_1 = ZL$, $IKS_2 = SP$, $IKS_3 = DD$, $IKS_4 = VA$, $IKS_5 = ZK$.

Підмножина можливих параметрів $\mathbf{P_i}$, що використовуються для прогнозування чи ідентифікації i-го інциденту формується на основі множини можливих параметрів $\mathbf{P}$, яка включає в себе всі параметри, що контролюються в середовищі, без прив'язки до конкретного типу ІПКС, $\mathbf{P_i} \subseteq \mathbf{P}$. Виходячи з аналізу параметрів, описаних в [16,65,90] та провівши їх узагальнення сформуємо множину можливих параметрів, що характеризують стан контрольованого середовища і дають можливість спрогнозувати та ідентифікувати ІПКС, а за умов високого рівня критичності і КС, $\mathbf{P} = \{\bigcup_{j=1}^{m} P_j\} = \{P_1, \ldots, P_m\}, (j = \overline{1,m})$, де m визначає загальну кількість заданих параметрів.

Наприклад, за умови дослідження при $m=13$ сформована множина матиме такий вигляд: $\mathbf{P} = \{\bigcup_{j=1}^{13} P_j\} = \{P_1, \ldots, P_{13}\} = \{Tlog, Nlog, CPU, MU, NEr, RTPr, CNCh, NCC, DbR, STF, T, H, D\}$, де $P_1 = Tlog$, $P_2 = Nlog$, $P_3 = CPU$, $P_4 = MU$, $P_5 = NEr$, $P_6 = RTPr$, $P_7 = CNCh$, $P_8 = NCC$, $P_9 = DbR$, $P_{10} = STF$, $P_{11} = T$, $P_{12} = H$, $P_{13} = D$ – відповідно є іденти-

фікаторами таких параметрів як:

– «Час входу в систему (*Tlog*)» (при *j=1*),

– «Частота запитів на вхід у систему (*Nlog*)» (при *j=2*),

– «Завантаженість процесора (*CPU*)» (при *j=3*),

– «Завантаженість оперативної пам'яті (*MU*)» (при *j=4*),

– «Кількість збоїв та помилок (*NEr*)» (при *j=5*),

– «Час виконання процесу (*RTPr*)» (при *j=6*),

– «Завантаженість мереженого каналу (*CNCh*)» (при *j=7*),

– «Кількість одночасних підключень (*NCC*)» (при *j=8*),

– «Затримка між запитами від одного джерела (*DbR*)» (при *j=9*),

– «Розмір тимчасових файлів (*STF*)» (при *j=10*),

– «Температура в серверній кімнаті (*T*)» (при *j=11*),

– «Вологість повітря в серверній кімнаті (*H*)» (при *j=12*),

– «Концентрація пилу в серверній кімнаті (*D*)» (при *j=13*).

Опишемо ці параметри [65].

Час входу в систему, *Tlog* . Використовується виключно для виявлення злому ІС, спричиненого діяльністю порушника ІБ. Параметр заснований на тому, що активність ІС і користувачів цих систем залежить від часу доби. Зазвичай більша активність користувачів щодо входу в систему виявляється в денний час, менша – в нічний, але можлива інша статистика, яка визначається режимом роботи організації, до яких належать ІС. Природа цього параметра нечітка, адже неможливо однозначно зробити висновок про нелегальну активність порушника. Так, наприклад, в організаціях з часом роботи з 08:00 до 16:00 імовірність того, що користувач, який авторизувався – це зловмисник, найнижча в 08:00 і з часом зростає, досягаючи максимуму в години після 16:00.

Частота запитів на вхід у систему, *Nlog* . Також використовується для прогнозування наслідків діяльності порушників. Основу обгрунтування застосування даного параметра складає той факт, що найвища частота запитів на вхід буде відмічатися при атаках системи порушниками-ботами, проте порушники-люди теж від-

значається підвищеною частотою запитів внаслідок намагання обійти захист і теоретичного припущення що він не володіє легітимним логіном та паролем, тому буде змушений робити як мінімум декілька спроб. Причому чим більше число спроб, тим більша ймовірність що в ІС дійсно намагається ввійти порушник. Зрозуміло, що цей параметр теж є нечітким.

Завантаженість процесора, *CPU*. Використовується для прогнозування багатьох категорій ІПКС. Основні причини завантаження процесора програмні. Це або велика кількість запущених одночасно програм, або вірус. Також завантаженість процесора може бути не програмна, а апаратна. Велике завантаження процесора вказує на те, що в комп'ютері виконується будь-яка дія, а за рівнем завантаженості можна визначити наскільки сильно комп'ютер схильний до шкідливих впливів. Виходячи з того, що кількість активних процесів на honeypot-системах мусить бути мінімальною, то будь-яке збільшення навантаження є ознакою діяльності в системі порушників. У реальних ІС імовірність того, що активність спричинена саме зловмисними діями дещо нижча, а, зрозуміло, нормальна величина процесорного часу вища. Проте цей параметр все одно можна ефективно використовувати для ідентифікації факту порушення в системах виявлення вторгнень і системах виявлення порушника, а отже і КС. Параметр є нечітким, так як завантаження центрального процесора змінюється кожну секунду, її оптимальне (нормальне) значення різному для різних систем і, до того ж, не дає чіткої відповіді про наявність факту атаки.

Завантаженість оперативної пам’яті, *MU*. Це показник кількості зайнятих структурних одиниць оперативної пам'яті. В оперативній пам'яті інформація зберігається тимчасово і при відключенні живлення видаляється. У ній зберігається інформація наступного роду: системна інформація, необхідна для роботи операційної системи; інформація від пристроїв підключених до комп'ютера і їх драйвера; антивіруси, віруси, резидентні програми; програми та файли, які в даний момент відкриті і знаходяться в обробці. Параметр є нечітким, оскільки завантаженість оперативної пам'яті змінюється кожну секунду, її оптимальне (нормальне) значення різному для різних систем і до того ж не дає чіткої відповіді про наяв-

ність атак в ІС. Є дуже близьким до попереднього параметра.

Кількість збоїв та помилок, NEr. Помилка в ІС – це ненормальна ситуація, яка може призвести до зниження або втрати здатності функціонального вузла по виконанню визначеної функції, тобто до відмови. Цей параметр відноситься до нечітких, оскільки помилки дуже часто є елементом нормальної роботи системи в ІС через технічні характеристик апаратного та програмного забезпечення. Аналогічно збої та помилки можуть відбуватися під час роботи як авторизованого користувача так і порушника. Проте при частому повторені збоїв чи помилок можна зробити висновок з певною долею імовірності що система атакована. У цю групу входить широкий спектр подій від помилок при авторизації до збоїв при виконанні певних процесів або файлів. При атаці в ІС, незалежно від її виду, частота появи несправностей буде дещо вищою. Так велика інтенсивність виникнення помилок і збоїв свідчить із певною ймовірністю про можливість реалізації того чи іншого ІПКС.

Час виконання процесу, $RTPr$. Використовується виключно для виявлення злому ІС. Досліджуючи статистику роботи ІС різних підприємств та організацій легко помітити, що залежно від специфіки роботи час, затрачений на виконання певної операції є приблизно однаковий для однотипних ІС та їх задач. Таким чином, при ідентифікації невластивих процесів для системи по часовій характеристиці (час запуску, припинення процесу, його тривалість) можна зробити висновок про атаку системи. Оскільки, такий стан речей може бути спричинений халатністю працівника, то висновок є неоднозначний і відповідно параметр носить нечіткий характер.

Завантаженість мереженого каналу, $CNCh$. Параметр пов'язаний з поняттям трафіку – це обсяг інформації, який проходить через сервер за певний період часу. Трафік буває вхідним – дані, одержувані комп'ютером; вихідний – дані, що відправляються комп'ютером; внутрішній – в межах певної мережі, найчастіше локальної, зовнішній – за межами певної мережі, найчастіше Інтернет-трафік. Моніторинг трафіку дозволяє фіксувати дані, які передаються по інтернет-каналу. Значне зростання трафіку свідчить про можливу DDos-атаку або інший тип атаки ІС. А

оскільки величину нормальної завантаженості мережевого каналу визначити практично неможливо, то параметр є нечітким.

Кількість одночасних підключень, *NCC*. Як показує практика для ефективного проведення DDoS необхідне залучення великої кількості джерел, які беруть участь у нападі на систему-«жертву». Отже, параметр NCC при збільшенні кількості підключень до сервера може використовуватися в якості однієї з ознак початку атаки. Максимальне число підключень, яке може підтримувати сервер, залежить від його апаратних і програмних особливостей і характеризується параметром maxNCC, значення якого буде відрізнятися для різних серверів [60]. Параметр є нечітким, оскільки при невеликих значеннях характерний і для стану нормального функціонування і його точний показник, який може свідчити про атаку, визначити практично неможливо.

Затримка між запитами від одного джерела, *DbR*. Параметр характеризує час між послідовними запитами від одного підключеного до сервера клієнта. На деяких серверах, для запобігання атак, цей параметр встановлюється вручну (наприклад, 1 запит за 1 секунду від користувача). Зменшення затримки між запитами може свідчити про початок DDoS-атаки, метою якої є відправка якомога більшої кількості запитів, які виведуть сервер з працездатного стану. Значення параметра визначається величиною maxDbR, яка залежить від програмного забезпечення та призначення сервера [60]. Цей параметр також є нечітким.

Розмір тимчасових файлів, *STF*. Це величина, що демонструє скільки місця тимчасовий файл займає на диску. Тимчасовий файл – файл, що створюється певною програмою або операційною системою для збереження проміжних результатів у процесі функціонування або передачі даних в іншу програму. Зазвичай такі файли видаляються автоматично процесом, що їх створив. У ньому може зберігатися копія вірусу, або резервне тіло вірусу для автоматичного запуску. Параметр є нечітким через те що занадто багато різних тимчасових файлів створюється і видаляється під час роботи комп'ютера і розмір їх при нормальному функціонуванні може бути різним.

Параметри мікроклімату приміщення серверної: Температура в серверній кі-

мнаті T; Вологість повітря в серверній кімнаті H; Концентрація пилу в серверній кімнаті D. Серверна кімната являє собою приміщення, спеціально призначене для забезпечення оптимального, безпечного і стабільного режиму роботи комплексу обладнання, що виконує ряд процесів в організації. Виділення спеціальної кімнати для серверів дозволяє з найменшими витратами забезпечити дорогому обладнанню оптимальний режим роботи. Якщо створити для апаратури відповідні умови, підвищиться надійність її роботи і збільшиться термін служби. Серед основних чиників, що впливають на роботу файлового серверу є особливості мікроклімату в приміщені. Оскільки немає чіткої і однозначної градації для будь-якого виду обладнання які показники цих параметрів можуть призвести до КС, то параметр є нечітким.

Слід зазначити, що в роботах [16,65] використані не лише нечіткі параметри, як в даному досліджені, а й чіткі. Це збільшує кількість параметрів і теоретично підвищує достовірність результатів, однак не може бути застосовано в реальних умовах, оскільки розраховано на використанні в honeypot-системах. В реальних умовах застосування чітких параметрів навпаки призведе до зростання кількості помилок 1-го та 2-го роду за рахунок збільшення обмежень чіткої логіки та появи колізій між ними.

Підмножини $\mathbf{P_i}$, що використовуються для прогнозування чи ідентифікації i-го інциденту формується на основі множини можливих параметрів $\mathbf{P}$ так, що $\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{P_i}\} = \{\mathbf{P_1}, ..., \mathbf{P_n}\}$, $\mathbf{P_i} \subseteq \mathbf{P}$, а $\mathbf{P_i} = \{\bigcup_{j=1}^{k_i} P_{ij}\} = \{P_{i1}, ..., P_{ik_i}\}$, де n – загальна кількість ІПКС, k_i – кількість параметрів, що пов’язані з i-м інцидентом. Таким чином $\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{P_i}\} = \{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{k_i} P_{ij}\}\} = \{\{P_{11},...,P_{1k_1}\}, ..., \{P_{n1},...,P_{nk_n}\}\}$ [48]. Наприклад, за умовами дослідження при $n=5$, $k_1 = k_3 = 6$, $k_2 = k_4 = 5$, $k_5 = 3$ визначимо необхідні параметри для виявлення відповідних ІПКС: $P_{11} = P_1$, $P_{12} = P_2$, $P_{13} = P_3$, $P_{14} = P_4$, $P_{15} = P_5$, $P_{16} = P_6$, $P_{21} = P_3$, $P_{22} = P_4$, $P_{23} = P_5$, $P_{24} = P_6$, $P_{25} = P_7$, $P_{31} = P_3$, $P_{32} = P_4$, $P_{33} = P_5$, $P_{34} = P_7$, $P_{35} = P_8$, $P_{36} = P_9$, $P_{41} = P_3$, $P_{42} = P_4$, $P_{43} = P_5$, $P_{44} = P_7$, $P_{45} = P_{10}$ і $P_{51} = P_{11}$, $P_{52} = P_{12}$, $P_{53} = P_{13}$. Тоді отримаємо:

$$\{\bigcup_{\mathbf{i=1}}^{5}\mathbf{P_i}\}=\{\bigcup_{i=1}^{5}\{\bigcup_{j=1}^{k_i}P_{ij}\}\}=\{\{P_{11},\,P_{12},\,P_{13},\,P_{14},\,P_{15},\,P_{16}\},\,\{P_{21},\,P_{22},\,P_{23},\,P_{24},\,P_{25}\},$$
$$\{P_{31},\,P_{32},\,P_{33},\,P_{34},\,P_{35},\,P_{36}\},\,\{P_{41},\,P_{42},\,P_{43},\,P_{44},\,P_{45}\},\,\{P_{51},\,P_{52},\,P_{53}\}\}=$$
$$\{\{Tlog,\,Nlog,\,CPU,\,MU,\,NEr\;RTPr\},\{CPU,\,MU,\,NEr,\,RTPr,\,CNCh\},\tag{2.3}$$
$$\{CPU,\,MU,\,NEr,\,CNCh,\,NCC\;DbR\},\{CPU,\,MU,\,NEr,\,CNCh,\,STF\},\{T,\,H,\,D\}\},$$

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

Таким чином, щоб спрогнозувати можливість реалізації КС або виявити її та ідентифікувати необхідно розробити систему, яка буде проводити моніторинг мережевих характеристик (параметрів трафіку) і локальних характеристик (параметрів комп'ютерної системи або хоста), а також фізичних параметрів, наведених в табл. 2.1, характерних для стану можливої реалізації ІПКС.

Таблиця 2.1
Параметри для виявлення та ідентифікації ІПКС

№ по порядку, j	Параметр	Проникнення порушника в ІС (злом)	Спам	Мережева атака відмова в обслуговувані (Dos/DDos)	Вірусна атака	Вихід з ладу (збій) ІС через вплив мікрокліматичних умов
1	Tlog	X				
2	Nlog	X				
3	CPU	X	X	X	X	
4	MU	X	X	X	X	
5	NEr	X	X	X	X	
6	RTPr	X	X			
7	CNCh		X	X	X	
8	NCC			X		
9	DbR			X		
10	STF				X	
11	T					X
12	H					X
13	D					X

Так, кожному інциденту відповідає той чи інший набір параметрів, що визначається підмножиною $\mathbf{P_i}$. Враховуючи те, що реалізація КС може мати як зумовлений так і випадковий характер, а ІС є за своєю суттю слабоформалізованних середовищем, то система повинна бути заснована на спеціальних методах теорії нечітких множин [46], а отже деякі з використовуваних параметрів можуть бути нечіткими за своєю природою.

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

Компонент кортежу (2.2) $\mathbf{T_i^e}$ визначає множину еталонів $\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{T_i^e}\} = \{\mathbf{T_1^e}, \ldots, \mathbf{T_n^e}\}$, $(i = \overline{1,n})$, з загальної множини еталонів $\mathbf{T^e}$, $\mathbf{T_i^e} \subseteq \mathbf{T^e}$. Аналогічно до підмножини параметрів для ідентифікації конкретного ІПКС виділимо підмножину еталонів пов'язаних з ними $\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{T_i^e}\} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \{\bigcup_{\mathbf{j=1}}^{\mathbf{k_i}} \mathbf{T_{ij}^e}\}\} = \{\{\tilde{T}_{11}^e, \ldots, \tilde{T}_{1k_1}^e\}, \ldots, \{\tilde{T}_{n1}^e, \ldots, \tilde{T}_{nk_n}^e\}\}$. Підмножину $\mathbf{T_{ij}^e} \subseteq \mathbf{T_i^e}$ визначимо як: $\mathbf{T_{ij}^e} = \{\bigcup_{s=1}^{r_{ij}} \tilde{T}_{ijs}^e\} = \{\tilde{T}_{ij1}^e, \ldots, \tilde{T}_{ijr_{ij}}^e\}$, де $\tilde{T}_{ijs}^e$ $(s = \overline{1,r_{ij}})$ – еталоні нечіткі числа, а r_{ij} – кількість елементів (термів) в $\mathbf{T_{ij}^e}$. Тоді множина пов'язаних з ІПКС еталонів матиме наступний вигляд:

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{T_i^e}\} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \{\bigcup_{\mathbf{j=1}}^{\mathbf{k_i}} \mathbf{T_{ij}^e}\}\} = \{\bigcup_{i=1}^{n} \{\bigcup_{j=1}^{k_i} \{\bigcup_{s=1}^{r_{ij}} \tilde{T}_{ijs}^e\}\}\} = \{\{\{\tilde{T}_{111}^e, \ldots, \tilde{T}_{11r_{11}}^e\}, \ldots, \{\tilde{T}_{1k_11}^e, \ldots, \tilde{T}_{1k_1r_{1k_1}}^e\}\}, \ldots, \{\{\tilde{T}_{n11}^e, \ldots, \tilde{T}_{n1r_{n1}}^e\}, \ldots, \{\tilde{T}_{nk_n1}^e, \ldots, \tilde{T}_{nk_nr_{nk_n}}^e\}\}\}. \quad (2.4)$$

Виходячи з цього, наприклад, при $n = 5$ для ІПКС ($\mathbf{IKS_1 = ZL}$, $\mathbf{IKS_2 = SP}$, $\mathbf{IKS_3 = DD}$, $\mathbf{IKS_4 = VA}$, $\mathbf{IKS_5 = ZK}$) з ідентифікаторами $IKS_1 = ZL$, $IKS_2 = SP$, $IKS_3 = DD$, $IKS_4 = VA$, $IKS_5 = ZK$ та $k_1 = k_3 = 6$, $k_2 = k_4 = 5$, $k_5 = 3$, $r_{1j} = r_{2j} = r_{3j} = r_{4j} = 3$ і $r_{5j} = 5$ вираз (2.4) описуватиме множину еталонів наступним чином:

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{5}} \mathbf{T_i^e}\} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{5}} \{\bigcup_{\mathbf{j=1}}^{\mathbf{k_i}} \mathbf{T_{ij}^e}\}\} = \{\bigcup_{i=1}^{5} \{\bigcup_{j=1}^{k_i} \{\bigcup_{s=1}^{r_{ij}} \tilde{T}_{ijs}^e\}\}\} = \{\{\{\tilde{T}_{111}^e, \ldots, \tilde{T}_{11r_{11}}^e\}, \ldots, \{\tilde{T}_{1k_11}^e, \ldots, \tilde{T}_{1k_1r_{16}}^e\}\}, \{\{\tilde{T}_{211}^e, \ldots, \tilde{T}_{21r_{21}}^e\}, \ldots, \{\tilde{T}_{2k_21}^e, \ldots, \tilde{T}_{2k_2r_{25}}^e\}\}, \{\{\tilde{T}_{311}^e, \ldots, \tilde{T}_{31r_{31}}^e\}, \ldots, \{\tilde{T}_{3k_31}^e, \ldots, \tilde{T}_{3k_3r_{36}}^e\}\}, \{\{\tilde{T}_{411}^e, \ldots, \tilde{T}_{41r_{41}}^e\}, \ldots, \{\tilde{T}_{4k_41}^e, \ldots, \tilde{T}_{4k_4r_{45}}^e\}\}, \{\{\tilde{T}_{511}^e, \ldots, \tilde{T}_{51r_{51}}^e\}, \ldots, \{\tilde{T}_{5k_51}^e, \ldots, \tilde{T}_{5k_5r_{53}}^e\}\}\} = \{\{\{\tilde{T}_{111}^e, \tilde{T}_{112}^e, \tilde{T}_{113}^e\}, \ldots, \{\tilde{T}_{161}^e, \tilde{T}_{162}^e, \tilde{T}_{163}^e\}\}, \{\{\tilde{T}_{211}^e, \tilde{T}_{212}^e, \tilde{T}_{213}^e\}, \ldots, \{\tilde{T}_{251}^e, \tilde{T}_{252}^e, \tilde{T}_{253}^e\}\}, \{\{\tilde{T}_{311}^e, \tilde{T}_{312}^e, \tilde{T}_{313}^e\}, \ldots, \{\tilde{T}_{361}^e, \tilde{T}_{362}^e, \tilde{T}_{363}^e\}\}, \{\{\tilde{T}_{411}^e, \tilde{T}_{412}^e, \tilde{T}_{413}^e\}, \ldots, \{\tilde{T}_{461}^e, \tilde{T}_{462}^e, \tilde{T}_{463}^e\}\}, \{\{\tilde{T}_{511}^e, \tilde{T}_{512}^e, \tilde{T}_{513}^e, \tilde{T}_{514}^e, \tilde{T}_{515}^e\}, \ldots, \{\tilde{T}_{531}^e, \tilde{T}_{532}^e, \tilde{T}_{533}^e, \tilde{T}_{534}^e, \tilde{T}_{535}^e\}\}\} = \{\{\{\tilde{H}_{11}, \tilde{C}_{11}, \tilde{B}_{11}\}, \ldots, \{\tilde{H}_{16}, \tilde{C}_{16}, \tilde{B}_{16}\}\}, \{\{\tilde{H}_{21}, \tilde{C}_{21}, \tilde{B}_{21}\}, \ldots, \{\tilde{H}_{25}, \tilde{C}_{25}, \tilde{B}_{25}\}\}, \{\{\tilde{H}_{31}, \tilde{C}_{31}, \tilde{B}_{31}\}, \ldots, \{\tilde{H}_{36}, \tilde{C}_{36}, \tilde{B}_{36}\}\}, \{\{\tilde{H}_{41}, \tilde{C}_{41}, \tilde{B}_{41}\}, \ldots, \{\tilde{H}_{45}, \tilde{C}_{45}, \tilde{B}_{45}\}\},$$

$\{\{\underset{\sim}{H}_{51}, \underset{\sim}{HC}_{51}, \underset{\sim}{C}_{51}, \underset{\sim}{BC}_{51}, \underset{\sim}{B}_{51}\}, \ldots, \{\underset{\sim}{H}_{53}, \underset{\sim}{HC}_{53}, \underset{\sim}{C}_{53}, \underset{\sim}{BC}_{55}, \underset{\sim}{B}_{53}\}\} = \{\{\{\underset{\sim}{T}^e_{ZLTlog1}, \underset{\sim}{T}^e_{ZLTlog2}, \underset{\sim}{T}^e_{ZLTlog3}\}, \ldots, \{\underset{\sim}{T}^e_{ZLRTPr1}, \underset{\sim}{T}^e_{ZLRTPr2}, \underset{\sim}{T}^e_{ZLRTPr3}\}\}, \{\{\underset{\sim}{T}^e_{SPCPU1}, \underset{\sim}{T}^e_{SPCPU2}, \underset{\sim}{T}^e_{SPCPU3}\}, \ldots, \{\underset{\sim}{T}^e_{SPCNCh1}, \underset{\sim}{T}^e_{SPCNCh2}, \underset{\sim}{T}^e_{SPCNCh3}\}\}, \{\{\underset{\sim}{T}^e_{DDCPU1}, \underset{\sim}{T}^e_{DDCPU2}, \underset{\sim}{T}^e_{DDCPU3}\}, \ldots, \{\underset{\sim}{T}^e_{DDDbR1}, \underset{\sim}{T}^e_{DDDbR2}, \underset{\sim}{T}^e_{DDDbR3}\}\}, \{\{\underset{\sim}{T}^e_{VACPU1}, \underset{\sim}{T}^e_{VACPU2}, \underset{\sim}{T}^e_{VACPU3}\}, \ldots, \{\underset{\sim}{T}^e_{VASTF1}, \underset{\sim}{T}^e_{VASTF2}, \underset{\sim}{T}^e_{VASTF3}\}\}, \{\{\underset{\sim}{T}^e_{ZKT1}, \underset{\sim}{T}^e_{ZKT2}, \underset{\sim}{T}^e_{ZKT3}, \underset{\sim}{T}^e_{ZKT4}, \underset{\sim}{T}^e_{ZKT5}\}, \ldots, \{\underset{\sim}{T}^e_{ZKD1}, \underset{\sim}{T}^e_{ZKD2}, \underset{\sim}{T}^e_{ZKD3}, \underset{\sim}{T}^e_{ZKD4}, \underset{\sim}{T}^e_{ZKD5}\}\}\} = \{\{\{\underset{\sim}{H}_{ZLTlog}, \underset{\sim}{C}_{ZLTlog}, \underset{\sim}{B}_{ZLTlog}\}, \ldots, \{\underset{\sim}{H}_{ZLRTPr}, \underset{\sim}{C}_{ZLRTPr}, \underset{\sim}{B}_{ZLRTPr}\}\}, \{\{\underset{\sim}{H}_{SPCPU}, \underset{\sim}{C}_{SPCPU}, \underset{\sim}{B}_{SPCPU}\}, \ldots, \{\underset{\sim}{H}_{SPCNCh}, \underset{\sim}{C}_{SPCNCh}, \underset{\sim}{B}_{SPCNCh}\}\}, \{\{\underset{\sim}{H}_{DDCPU}, \underset{\sim}{C}_{DDCPU}, \underset{\sim}{B}_{DDCPU}\}, \ldots, \{\underset{\sim}{H}_{DDDbR}, \underset{\sim}{C}_{DDDbR}, \underset{\sim}{B}_{DDDbR}\}\}, \{\{\underset{\sim}{H}_{VACPU}, \underset{\sim}{C}_{VACPU}, \underset{\sim}{B}_{VACPU}\}, \ldots, \{\underset{\sim}{H}_{VASTF}, \underset{\sim}{C}_{VASTF}, \underset{\sim}{B}_{VASTF}\}\}, \{\{\underset{\sim}{H}_{ZKT}, \underset{\sim}{HC}_{ZKT}, \underset{\sim}{C}_{ZKT}, \underset{\sim}{BC}_{ZKT}, \underset{\sim}{B}_{ZKT}\}, \ldots, \{\underset{\sim}{H}_{ZKD}, \underset{\sim}{HC}_{ZKD}, \underset{\sim}{C}_{ZKD}, \underset{\sim}{BC}_{ZKD}, \underset{\sim}{B}_{ZKD}\}\}\},$

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

Підмножина $\mathbf{PP_i}$ формується на основі даних, що зняті з датчиків контролю відповідних кожному інциденту параметрів середовища за певний період часу з заданим інтервалом, тобто $\mathbf{PP_i} = \{\bigcup_{j=1}^{k_i} \underset{\sim}{P}_{ij}\} = \{\underset{\sim}{P}_{11}, \ldots, \underset{\sim}{P}_{nk_n}\}$, де $\mathbf{PP_i} \subseteq \mathbf{PP}$, $(i = \overline{1,n},\ j = \overline{1,k_i})$.

Наприклад, при $n = 5$, $i = \overline{1,5}$ для ІПКС ($\mathbf{ІКS_1} = \mathbf{ZL}$, $\mathbf{ІКS_2} = \mathbf{SP}$, $\mathbf{ІКS_3} = \mathbf{DD}$, $\mathbf{ІКS_4} = \mathbf{VA}$, $\mathbf{ІКS_5} = \mathbf{ZK}$), $k_1 = k_3 = 6$, $k_2 = k_4 = 5$, $k_5 = 3$ ця підмножина може бути визначена як: $\mathbf{PP_1} = \{\bigcup_{j=1}^{6} \underset{\sim}{P}_{1j}\} = \{\underset{\sim}{P}_{11}, \underset{\sim}{P}_{12}, \underset{\sim}{P}_{13}, \underset{\sim}{P}_{14}, \underset{\sim}{P}_{15}, \underset{\sim}{P}_{16}\} = \{\underset{\sim}{Tlog}, \underset{\sim}{Nlog}, \underset{\sim}{CPU}, \underset{\sim}{MU}, \underset{\sim}{NEr}, \underset{\sim}{RTPr}\}$, при $i = 1\ \ k_1 = 6$; $\mathbf{PP_2} = \{\bigcup_{j=1}^{5} P_{2j}\} = \{\underset{\sim}{P}_{21}, \underset{\sim}{P}_{22}, \underset{\sim}{P}_{23}, \underset{\sim}{P}_{24}, \underset{\sim}{P}_{25}\} = \{\underset{\sim}{CPU}, \underset{\sim}{MU}, \underset{\sim}{NEr}, \underset{\sim}{RTPr}, \underset{\sim}{CNCh}\}$, при $i = 2\ \ k_2 = 5$; $\mathbf{PP_3} = \{\bigcup_{j=1}^{6} P_{3j}\} = \{\underset{\sim}{P}_{31}, \underset{\sim}{P}_{32}, \underset{\sim}{P}_{33}, \underset{\sim}{P}_{34}, \underset{\sim}{P}_{35}, \underset{\sim}{P}_{36}\} = \{\underset{\sim}{CPU}, \underset{\sim}{MU}, \underset{\sim}{NEr}, \underset{\sim}{CNCh}, \underset{\sim}{NCC}, \underset{\sim}{DbR}\}$, при $i = 3\ \ k_3 = 6$; $\mathbf{PP_4} = \{\bigcup_{j=1}^{5} P_{4j}\} = \{\underset{\sim}{P}_{41}, \underset{\sim}{P}_{42}, \underset{\sim}{P}_{43}, \underset{\sim}{P}_{44}, \underset{\sim}{P}_{46}\} = \{\underset{\sim}{CPU}, \underset{\sim}{MU}, \underset{\sim}{NEr}, \underset{\sim}{CNCh}, \underset{\sim}{STF}\}$, при $i = 4\ \ k_4 = 5$; $\mathbf{PP_5} = \{\bigcup_{j=1}^{3} P_{5j}\} = \{\underset{\sim}{P}_{51}, \underset{\sim}{P}_{52}, \underset{\sim}{P}_{56}\} = \{\underset{\sim}{T}, \underset{\sim}{H}, \underset{\sim}{D}\}$, при $i = 5\ \ k_5 = 3$.

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-о ІПКС. Таким чином $LC_i = \{ \underset{j=1}{\overset{k_i}{\wedge}} t_j \} = \{ \underset{j=1}{\overset{k_i}{\wedge}} (\underset{\sim}{P}_{ij} \cong \underset{s=1}{\overset{r_{ij}}{\vee}} T^e_{ijs}) \}$, де k_i – кількість параметрів, що ідентифікують i-й інцидент, а r_{ij} – кількість термів у відповідних еталонах. Для кожного ІПКС і правила формується унікальний ідентифікатор стану LC. Зазначимо, що кожному ER_{ip} відповідає евристичний вираз (правило), тобто: $\mathbf{ER} = \bigcup_{i=1}^{n} \{ \bigcup_{p=1}^{R_i} ER_{ip} \} = \{ \bigcup_{i=1}^{n} \{ \bigcup_{p=1}^{R_i} LC_{ip} \rightarrow LI_{ip} \} \} = \{ \bigcup_{i=1}^{n} \{ \bigcup_{p=1}^{R_i} ER_{ip} = (LC_{ip} \rightarrow LI_{ip}) \} \}$, де ER_{ip} – p-те правило для виявлення та ідентифікації i-о ІПКС, яке буквально інтерпретується як: «Якщо LC_{ip} істинно, то імовірність настання ІПКС буде LI_{ip}», а LI_{ip} – один з елементів множини лінгвістичних ідентифікаторів ймовірності реалізації ІПКС, необхідних для відображення судження експерта в лінгвістичній формі, $\mathbf{LI} = \bigcup_{d=1}^{D} LI_d = \{LI_1, ..., LI_D\}$.

Побудова правил зазвичай здійснюється на основі експертного підходу, особливо це важливо в тих випадках, коли необхідно дати перевагу одній з альтернатив, наприклад, при якому LC_{ip} результат, пов'язаний з LI_{ip} буде найбільш об'єктивно відображати стан системи. Виходячи з цих позицій формуються набори правил. Так, правило ER_{41} [20] буде мати вигляд: $ER_{41} = \{ (\underset{\sim}{P}_{VACPU} \cong H, \ \underset{\sim}{P}_{VAMU} \cong H, \ \underset{\sim}{P}_{VANEr} \cong M, \ \underset{\sim}{P}_{VACNCh} \cong H, \ \underset{\sim}{P}_{VASTF} \cong M) \rightarrow H \}$, що словесно можна інтерпретувати таким чином: «Якщо поточні значення $\underset{\sim}{P}_{VACPU}$, $\underset{\sim}{P}_{VAMU}$, $\underset{\sim}{P}_{VANEr}$, $\underset{\sim}{P}_{VACNCh}$, $\underset{\sim}{P}_{VASTF}$ найбільш близько розташовані до значень $\underset{\sim}{H}_{VACPU}$, $\underset{\sim}{H}_{VAMU}$, $\underset{\sim}{M}_{VANEr}$, $\underset{\sim}{H}_{VACNCh}$, $\underset{\sim}{M}_{VASTF}$ відповідно, що входять до $\underset{\sim}{T}^{e}_{VACPU}$, $\underset{\sim}{T}^{e}_{VACNCh}$, $\underset{\sim}{T}^{e}_{VASTF}$, $\underset{\sim}{T}^{e}_{VAMU}$, $\underset{\sim}{T}^{e}_{VANEr}$, то рівень можливості виникнення ІПКС в даний момент буде НИЗЬКИЙ».

Кожен інцидент характеризується рівнем критичності, що задається множиною $\mathbf{LCS} = \{ \bigcup_{i=1}^{n} \underset{\sim}{LCS}_i \} = \{ \underset{\sim}{LCS}_1, ..., \underset{\sim}{LCS}_n \}, \ (i = \overline{1,n})$. Рівень критичності визначається через параметри оцінки критичності ситуації з врахуванням їх вагових коефіцієнтів, тобто $\underset{\sim}{LCS}_i = \sum_{e=1}^{E} (\Omega_e * \underset{\sim}{L}_e)$. Встановлено, що рівень критичності можна описати вра-

хувавши функціональні залежності між $\underset{\sim}{L}_e$ – параметрами оцінки рівня критичності. Детально метод оцінювання рівня критичності та множина оціночних параметрів описані в роботі [51] та в пп 2.3 і 3.1 даної дисертаційної роботи.

Сформувавши всі компоненти кортежу (2) наведемо модель представлення ІПКС «Вірусна атака». Отже, при $i = 4$ для ІПКС ($\mathbf{IKS_4} = \mathbf{VA}$) з ідентифікатором $IKS_4 = VA$ та $k_4 = 5$, $r_{4j} = 3$ і $R_4 = 243$ інтегрована модель матиме такий вигляд:

$$\begin{aligned}\mathbf{IKS_4} = &< IKS_4, \mathbf{P_4}, \mathbf{T_4^e}, \mathbf{PP_4}, \mathbf{ER_4}, LCS_4 > = < VA, \{P_{41}, P_{42}, P_{43}, P_{44}, P_{45}\}, \\ &\{\{\underset{\sim}{T}^e_{411}, \underset{\sim}{T}^e_{412}, \underset{\sim}{T}^e_{413}\}, \{\underset{\sim}{T}^e_{421}, \underset{\sim}{T}^e_{422}, \underset{\sim}{T}^e_{423}\}, \{\underset{\sim}{T}^e_{431}, \underset{\sim}{T}^e_{432}, \underset{\sim}{T}^e_{433}\}, \{\underset{\sim}{T}^e_{441}, \underset{\sim}{T}^e_{442}, \underset{\sim}{T}^e_{443}\}, \{\underset{\sim}{T}^e_{451}, \underset{\sim}{T}^e_{452}, \\ &\underset{\sim}{T}^e_{453}\}\}, \{\underset{\sim}{P}_{41}, \underset{\sim}{P}_{42}, \underset{\sim}{P}_{43}, \underset{\sim}{P}_{44}, \underset{\sim}{P}_{45}\}, \{ER_{41}, ..., ER_{4243}\}, \underset{\sim}{LCS}_4 > = < VA, \{CPU, MU, NEr, \\ &CNCh, STF\}, \{\{\underset{\sim}{T}^e_{VACPU1}, \underset{\sim}{T}^e_{VACPU2}, \underset{\sim}{T}^e_{VACPU3}\}, \{\underset{\sim}{T}^e_{VAMU1}, \underset{\sim}{T}^e_{VAMU2}, \underset{\sim}{T}^e_{VAMU3}\}, \\ &\{\underset{\sim}{T}^e_{VANEr1}, \underset{\sim}{T}^e_{VANEr2}, \underset{\sim}{T}^e_{VANEr3}\}, \{\underset{\sim}{T}^e_{VACNCh1}, \underset{\sim}{T}^e_{VACNCh2}, \underset{\sim}{T}^e_{VACNCh3}\}, \{\underset{\sim}{T}^e_{VASTF1}, \underset{\sim}{T}^e_{VASTF2}, \\ &\underset{\sim}{T}^e_{VASTF3}\}\}, \{\underset{\sim}{CPU}, \underset{\sim}{MU}, \underset{\sim}{NEr}, \underset{\sim}{CNCh}, \underset{\sim}{STF}\}, \{ER_{41}, ..., ER_{4243}\}, \underset{\sim}{LCS}_{VA} >\end{aligned} \tag{2.5}$$

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

2.2. Моделі еталонів лінгвістичних змінних та вирішальних правил для системи виявлення та оцінки кризових ситуацій

Для того, щоб спрогнозувати КС і ідентифікувати її необхідно заздалегідь виявити КА чи інцидент, що її породжує. Тому розробка комплексу систем виявлення та оцінки кризових ситуацій загалом та системи виявлення ІПКС (СВІПКС) як його складової є актуальними і важливими науковими і науково-практичними задачами. При цьому основними функціями даного комплексу мають бути: 1) моніторинг середовища ІС за певними параметрами, 2) виявлення та ідентифікація ІПКС, 3) оцінка рівня критичності ситуації, спричиненої виявленим інцидентом, 4) оголошення КС і, можливо, надання рекомендації щодо її припинення та ліквідації наслідків.

Слід зазначити, що питання, які стосуються застосування моделей еталонів лінгвістичних змінних та інших метолів і аспектів теорії нечітких множин є не новим. Так, питання особливостей застосування нечіткої логіки і експертних ме-

тодів для вирішення проблем захисту інформації підняті в роботах О.Г. Корченка [46]. Крім того використання моделей еталонів лінгвістичних зміних розглянуті в [41] – для виявлення аномальних станів в ІС, в [8] – для виявлення порушника інформаційної безпеки.

Оскільки процес виявлення і ідентифікації порушника відбувається в умовах невизначеності, а ряд наведених параметрів СВІПКС носять нечіткий характер, то функціонування такої системи має грунтуватись на нечіткій логіці. Для ідентифікації комп'ютерних атак можна використовувати логіко-лінгвістичний підхід і базову модель параметрів, частково описану в [32,65], які й будуть основою побудови розроблюваної системи.

Досягнення мети роботи СВОКС здійснюється шляхом виявлення та ідентифікації атак на ІС в СВІІПКС та оцінки їх рівня критичності. В зв'язку з цим основною метою даної роботи є побудова моделей еталонів параметрів, необхідних для функціонування СВІПКС в нечітко визначеному, слабоформалізованому середовищі.

Побудова підмножини нечітких (лінгвістичних) еталонів $\underset{\sim}{T}^{e}_{ijs}$ здійснюється на базі методу МЛТС [46] та методу формування лінгвістичних еталонів (МФЛЕ) для системи виявлення атак [41].

Формалізована процедура побудови еталонів здійснюється в кілька кроків:

1) Формування множини всіх можливих ідентифікаторів лінгвістичних оцінок (суджень) експертів $\mathbf{LE}$ та підмножини таких ідентифікаторів $\mathbf{LE_{ij}} \subseteq \mathbf{LE}$ для характеристики поточного стану j-го параметра в певному середовищі $\mathbf{LE_{ij}} = \{\bigcup_{s=1}^{r_{ij}} LE_{ijs}\} = \{LE_{ij1}, \ldots, LE_{ijr}\}$, (див. (1) в [41]) де LE_{ijs}, $(s = \overline{1,r_{ij}})$ – ідентифікатор s-ї лінгвістичної оцінки j-го параметра;

2) Формування множини ідентифікаторів інтервалів $\mathbf{N}$ і підмножини таких ідентифікаторів $\mathbf{N_{ij}} \subseteq \mathbf{N}$ відносно конкретного контрольованого параметра, що відображаються як $\mathbf{N_{ij}} = \{\bigcup_{q=1}^{r_{ij}} N_{ijq}\} = \{N_{ij1}, \ldots, N_{ijr_{ij}}\}$, $(q = \overline{1,r_{ij}})$, де N_{ijq} – ідентифікатор q-го інтервалу, що використовується для формування на ньому частот зустрічання оці-

нок експерта по даному j-му параметру;

3) Формування узагальненої таблиці оцінок, в якій фіксуються поточні твердження експертів відносно j-го параметра. В таблиці 2.2 сформовано f_{ijsq} – елемент емпіричних даних, який відображає частоту вживання однакових суджень експерта LE_{js} щодо стану параметра P_{ij} на інтервалі $N_{ijq} \cong [N_{ijq}^{\min}; N_{ijq}^{\max}]$, де $N_{ijq}^{\min}$ і $N_{ijq}^{\max}$ відповідно нижня і верхня межа q-го інтервалу. На її основі формується базова матриця частот $F_{ij} = \| f_{ijsq} \|$;

4) Формування похідної матриці частот

$$F_{ij}^{'} = \| f_{ijsq}^{'} \| = (vsm_{ij} / vs_{ijq}) \| f_{ijsq} \|, (q,s = \overline{1,r_{ij}}), \tag{2.6}$$

де

$$VS_{ij} = \| vs_{ijq} \| = \| vs_{ij1},...,vs_{ijr_{ij}} \| = \left\| \sum_{s=1}^{r_{ij}} f_{ijs1},...,\sum_{s=1}^{r_{ij}} f_{ijsr_{ij}} \right\|, \tag{2.7}$$

– вектор суми елементів f_{ijsq} відповідних стовпців матриці частот F_{ij}, а $vsm_{ij} = \bigvee_{q=1}^{r_{ij}} vs_{ijq}$ – максимальне значення цього вектору;

Таблиця 2.2

Узагальнена таблиця оцінок експертом значень параметра P_{ij}

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

5) Розрахунок матриці функцій належності $M_{ij} = \| \mu_{ijsq} \|$, що складається з елементів обчислюваних як

$$\mu_{ijsq} = f_{ijsq}^{'} / fm_{ijs}, \ (s,q = \overline{1,r_{ij}}), \tag{2.8}$$

де

$$FM_{ij} = \| fm_{ijq} \| = \| fm_{ij1},..., fm_{ijr_{ij}} \| = \left\| \bigvee_{s=1}^{r_{ij}} f_{ijs1}^{'},..., \bigvee_{s=1}^{r_{ij}} f_{ijsr_{ij}}^{'} \right\| \tag{2.9}$$

– вектор максимумів елементів кожного стовпця (інтервалу).

Результати обчислень дають змогу сформувати нечіткі терми еталонів $\underset{\sim}{T}_{ijs}$ використовуючи вираз $\underset{\sim}{T}_{ijs} = \{\bigcup_{q=1}^{r_{ij}} \mu_{ijsq} / x_{ijsq}\} = \{\mu_{ijs1} / x_{ijs1}, ..., \mu_{ijsr_{ij}} / x_{ijsr_{ij}}\}, (q = \overline{1,r_{ij}})$, де $x_{ijsq} = N_{ijq}^{\max} / N_{ijr_{ij}}^{\max}$ (див. (9) в [41]) – супорти НЧ.

Для того, щоб отримати підмножини лінгвістичнх еталони базових станів *j*-го параметру, що входять до множини всіх можливих еталонів, $\underset{\sim}{T}^{e}_{ij} \subseteq \mathbf{T^e}$ необхідно привести НЧ $\underset{\sim}{T}_{ijs}$ до канонічної форми запису. Даний процес складається з трьох кроків, при цьому виходячи з практичних міркувань в даному досліджені 3-ій крок відрізняється від відповідного в методі-прототипі.

Крок 1. Упорядкувати компоненти НЧ $\underset{\sim}{T}_{ijs}$ в порядку зростання, тобто $\forall x_{ijsq} : x_{ijsq} < x_{ijsq+1}\ \ (q = \overline{1,r-1})$.

Крок 2. В кожному $\underset{\sim}{T}_{ijs}$ здійсниться поглинання ряду компонентів відповідними компонентами $0 / x_{ijs}^{min}$ і $0 / x_{ijs}^{max}$ відповідно згідно виразам $x_{ijs}^{min} = \bigvee_{\substack{q=1 \\ при\ U1}}^{M-1} x_{ijsq}$ і $x_{ijs}^{max} = \bigwedge_{\substack{q=M \\ при\ U2}}^{r} x_{ijsq}$, де $U_1 \cong \forall x_{ijsq} < x_{ijsM} : \mu_{ijsq} = 0$, $U_2 \cong \forall x_{ijsq} > x_{ijsM} : \mu_{ijsq} = 0$, а x_{ijsM} і M – відповідно мода $\underset{\sim}{T}_{ijs}$ і її порядковий номер. Отже, формується підмножина еталонів

$$\underset{\sim}{T}^{e}_{ijs} = \{\bigcup_{q=1}^{r_s} \mu^{e}_{ijsq} / x^{e}_{ijsq}\} = \{\mu^{e}_{ijs1} / x^{e}_{ijs1}, \mu^{e}_{ijs2} / x^{e}_{ijs2}, ..., \mu^{e}_{ijsr_s-1} / x^{e}_{ijsr_s-1}, \mu^{e}_{ijsr_s} / x^{e}_{ijsr_s}\}\ \ (q = \overline{1,r_s}),$$

де $\mu^{e}_{ijs1} / x^{e}_{ijs1} = 0 / x_{ijsb} = 0 / x_{ijs}^{min}$, $\mu^{e}_{ijs2} / x^{e}_{ijs2} = \mu_{ijs\beta+1} / x_{ijs\beta+1}$, …, $\mu^{e}_{ijsr_s-1} / x^{e}_{ijsr_s-1} = \mu_{ijsr-\gamma} / x_{ijsr-\gamma}$, $\mu^{e}_{ijsr_s} / x^{e}_{ijsr_s} = 0 / x_{ijsr-\gamma+1} = 0 / x_{ijs}^{max}$, $r_s\ \ (s = \overline{1,r})$ – кількість компонентів в $\underset{\sim}{T}^{e}_{ijs}$, а β і γ – число поглинутих відповідно мінімальних і максимальних компонент.

Крок 3. Якщо при реалізацій 2-ого кроку $\exists\, \underset{\sim}{T}^{e}_{ijs} : \{0 / x_{ijs}^{min}\} \in \varnothing$ або $\exists\, \underset{\sim}{T}^{e}_{ijs} : \{0 / x_{ijs}^{max}\} \in \varnothing$ (тобто $\mu_{ijs\beta} \neq 0$, $\mu_{ijsr-\gamma+1} \neq 0$), то для таких термів проводиться розширення $\underset{\sim}{T}^{'}_{js}$ через введення додаткових $\mu_{js\beta-1} / x_{js\beta-1}$ і $\mu_{jsr-\gamma+2} / x_{jsr-\gamma+2}$, а потім компоненти НЧ заново індексуються з $q = 1$.

Отримавши всі підмножини еталонних значень параметрів з множини всіх можливих еталонів відбувається їх візуалізація, тобто побудова геометричних об-

разів кожного з еталонів, що вміщує відповідну кількість термів. Геометричне місце точок на площині визначається через ламану, що з'єднує точки, які відображають компоненти НЧ $\underset{\sim}{T}^{e}_{ijs}$ в порядку зростання їх супортів (носіїв) x^{e}_{ijsq}.

В описаному методі використовуються дані статистичних досліджень. Їх обробка досить трудомістка, оскільки для побудови функції належності (ФН) одного терму потрібно проводити статистичні дослідження всіх термів ЛЗ [46].

Побудуємо модель еталонів ЛЗ для параметрів виявлення та ідентифікації ІПКС в ІС з множини параметрів **P**, визначених в роботах [65]. При цьому введемо наступне допущення: еталони однойменних параметрів будуть однаковими для виявлення кожного виду ІПКС, тобто, наприклад, параметр $P_4 = MU$ характеризується еталоном $\underset{\sim}{T}^{e}_{14s} = \underset{\sim}{T}^{e}_{22s} = \underset{\sim}{T}^{e}_{32s} = \underset{\sim}{T}^{e}_{42s} = \underset{\sim}{T}^{e}_{ZKMUs} = \underset{\sim}{T}^{e}_{SPMUs} = \underset{\sim}{T}^{e}_{DDMUs} = \underset{\sim}{T}^{e}_{VAMUs} = \underset{\sim}{T}^{e}_{MUs}$. Аналогічно $LE_{14} = LE_{22} = LE_{32} = LE_{42} = LE_{ZKMU} = LE_{SPMU} = LE_{DDMU} = LE_{VAMU} = LE_{MU}$ і $N_{14} = N_{22} = N_{32} = N_{42} = N_{ZKMU} = N_{SPMU} = N_{DDMU} = N_{VAMU} = N_{MU}$.

Час входу в систему, $P_1 = Tlog$. Як вже було відмічено від часу тої чи іншої події в ІС певної організації чи підприємства залежить імовірність класифікації цих дій як дозволених чи не дозволених, тобто здійснених авторизованою або не авторизованою стороною.

Введемо підмножину ідентифікаторів лінгвістичних оцінок $\mathbf{LE_{Tlog}} = \{\bigcup_{s=1}^{3} LE_{Tlogs}\} = \{легітимний(Л), підозрілий(П), нелегітимний(Н)\}$ та ідентифікатори оціночних інтервалів, врахуємо що в даному випадку використовуються часові інтервали $\mathbf{N_{Tlog}} = \{\bigcup_{q=1}^{3} N_{Tlogq}\} = \{[00:00;08:00[,[08:00;16:00[,[16:00;24:00]\}$. Тепер сформуємо узагальнену таблицю оцінок (табл. 2.3) і базову матрицю частот для параметру Час входу в систему. Сформована на основі даних таблиці базова матриця матиме такий вигляд.

$$F_{Tlog} = \begin{vmatrix} 2 & 8 & 2 \\ 4 & 2 & 5 \\ 6 & 1 & 4 \end{vmatrix}.$$

Таблиця 2.3.

Узагальнена таблиця оцінок експертом значень параметра P_1

LE*1*	**N*1***		
	$[00:00;08:00[$	$[08:00;16:00[$	$[16:00;24:00]$
Легітимний	2	8	2
Підозрілий	4	2	5
Нелегітимний	6	1	4

Розрахуємо вектор сум $VS_{Tlog} = \|12 \quad 11 \quad 11\|$ і знайдемо максимальне значення цього вектору $vsm_{Tlog} = 12$.

Використавши вираз (2.6) отримаємо похідну матрицю частот

$$F'_{Tlog} = \begin{vmatrix} 2 & 8,72 & 2,18 \\ 4 & 2,18 & 5,45 \\ 6 & 1,09 & 4,36 \end{vmatrix}$$

та вектор максимумів $FM_{Tlog} = \|6 \quad 8,72 \quad 5,45\|$.

Використавши формулу (2.8) обрахуємо матрицю належностей та супорти НЧ еталону для параметра P_1

$$M_{T\log} = \begin{vmatrix} 0,33 & 1 & 0,4 \\ 0,66 & 0,25 & 1 \\ 1 & 0,13 & 0,8 \end{vmatrix}.$$

Супорти: $x_{Tlog11} = x_{Tlog21} = x_{Tlog31} = 8/24 = 0,33$, $x_{Tlog12} = x_{Tlog22} = x_{Tlog32} = 16/24 = 0,66$, $x_{Tlog13} = x_{Tlog23} = x_{Tlog33} = 24/24 = 1$. Здійснивши перетворення отримаємо набір еталонів параметра $P_1 = Tlog$ $\underset{\sim}{T}^e_{Tlog} = \{\bigcup_{s=1}^{3} \underset{\sim}{T}^e_{Tlog\,s}\} = \{$*легітимний(Л), підозрілий(П), нелегітимний(Н)*$\}$ і терми ЛЗ для цього параметра

$$\underset{\sim}{Л} = \underset{\sim}{T}^e_{Tlog1} = \{0/0,33; \quad 0,14/0,33; \quad 1/0,66; \quad 0,33/1; \quad 0/1\},$$

$$\underset{\sim}{П} = \underset{\sim}{T}^e_{Tlog2} = \{0/0,33; \quad 0,71/0,33; \quad 0,29/0,66; \quad 1/1; \quad 0/1\},$$

$$\underset{\sim}{Н} = \underset{\sim}{T}^e_{Tlog3} = \{0/0,33; \quad 1/0,33; \quad 0,14/0,66; \quad 0,67/1; \quad 0/1\}.$$

Графік ФН термів ЛЗ Час входу в систему показаний на рис. 2.2.

Частота запитів на вхід у систему, $P_2 = Nlog$. Аналогічно до попереднього використовується для виявлення факту порушення безпеки ІС, тобто їх злому. За-

снований на тому, що при намаганні підібрати логін при вході слід здійснити неодноразові спроби.

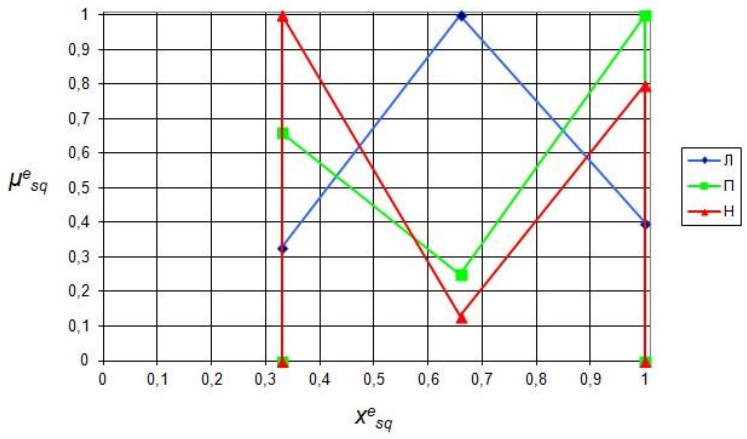


Рис. 2.2. ФН лінгвістичних термів еталонів нечітких чисел для *Tlog*

Введемо підмножину ідентифікаторів лінгвістичних оцінок $\mathbf{LE_{Nlog}} = \{\bigcup_{s=1}^{3} LE_{Nlogs}\} = \{низька(H), середня(C), висока(B)\}$ та ідентифікатори оціночних інтервалів. Врахуємо що в даному випадку частота запитів на вхід у систему звичайного користувача зазвичай мінімальна (найчастіше легітимний користувач вводить логін і пароль один раз), а сучасні програми для підбору паролів здатні перебрати 5310986 паролів/с [21]. Проте для визначення термів даної ЛЗ буде достатньо обмежитись значенням 15 запитів/с, адже людина не здатна пройти процедуру аутентифікації більше 10-15 раз за хвилину. Отже $\mathbf{N_{Nlog}} = \{\bigcup_{q=1}^{3} N_{Nlogq}\} = \{[0;3[,[3;6[,[6;15]\}$.

Сформуємо узагальнену таблицю оцінок і базову матрицю частот, що представлена у вигляді таблиці 2.4.

Таблиця 2.4.

Узагальнена таблиця оцінок експертом значень параметра P_2

LE2	**N2**		
	[0;3[	[3;6[	[6;15]
Низька	6	1	0
Середня	2	7	0
Висока	0	1	6

Сформована на основі даних таблиці базова матриця матиме такий вигляд.

$$F_{Nlog} = \begin{vmatrix} 6 & 1 & 0 \\ 2 & 7 & 0 \\ 0 & 1 & 6 \end{vmatrix}.$$

Згідно (2.7) $VS_{Nlog} = \|8 \quad 9 \quad 6\|$ і $vsm_{Nlog} = 9$.

Обрахуємо похідну матрицю частот, використавши вираз (2.6):

$$F'_{Nlog} = \begin{vmatrix} 6,75 & 1 & 0 \\ 2,25 & 7 & 0 \\ 0 & 1 & 9 \end{vmatrix}$$

та вектор максимумів $FM_{Nlog} = \|6,75 \quad 7 \quad 9\|$.

Використавши формули (2.8) обрахуємо матрицю належностей та суппорти НЧ еталону для параметра P_2

$$M_{Nlog} = \begin{vmatrix} 1 & 0,14 & 0 \\ 0,33 & 1 & 0 \\ 0 & 0,14 & 1 \end{vmatrix}.$$

Супорти: $x_{Nlog11} = x_{Nlog21} = x_{Nlog31} = 3/15 = 0,2$, $x_{Nlog12} = x_{Nlog22} = x_{Nlog32} = 6/15 = 0,4$, $x_{Nlog13} = x_{Nlog23} = x_{Nlog33} = 15/15 = 1$. Здійснивши перетворення отримаємо набір еталонів параметра $P_2 = Nlog$ $\underset{\sim}{T}^e_{Nlog} = \{\bigcup_{s=1}^{3} \underset{\sim}{T}^e_{Nlog\,s}\} = \{низька(H), середня(C), висока(B)\}$ і терми ЛЗ для цього параметра:

$$\underset{\sim}{H} = \underset{\sim}{T}^e_{Nlog1} = \{0/0,2; \quad 1/0,2; \quad 0,14/0,4; \quad 0/1\},$$

$$\underset{\sim}{C} = \underset{\sim}{T}^e_{Nlog2} = \{0/0,2; \quad 0,33/0,2; \quad 1/0,4; \quad 0/1\},$$

$$\underset{\sim}{B} = \underset{\sim}{T}^e_{Nlog3} = \{0/0,2; \quad 0,14/0,4; \quad 1/1; \quad 0/1\}.$$

Графік ФН термів ЛЗ Частота запитів на вхід в систему показаний на рис. 2.3.

Завантаженість процесора, $P_3 = CPU$. В реальних ІС на хостах виконуються певні процеси, що завантажують процесори на певну величину. При нормальних умовах і відсутності атаки на ІС цей показник залежатиме від виконуваних функцій на робочій станції і буде знаходитись в певних допустимих межах, а його зростання свідчитиме про проведення ккібератак, а саме DDos-атаки або зараження комп'ютерним вірусом (мережевий черв'як і троянська програма). Таким чином цей параметр можна ефективно використовувати для ідентифікації факту комп'ютерної атаки в СВІІПКС. Оскільки завантаження центрального процесора змінюється кожну секунду, її оптимальне (нормальне) значення відрізняється для різних

систем і, до того ж, не дає чіткої відповіді про наявність факту атаки, так як це може свідчити про апаратну несправність (що в принципі є також ІПКС), діяльність порушника чи зміну режиму роботи системи, то CPU – нечіткий параметр [8, 16,65].

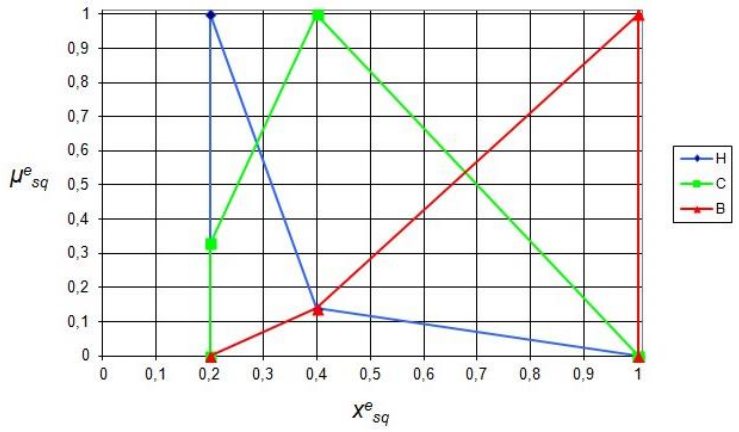


Рис. 2.3. ФН лінгвістичних термів еталонів нечітких чисел для *Nlog*

Введемо підмножину ідентифікаторів лінгвістичних оцінок $\mathbf{LE_{CPU}} = \{\bigcup_{s=1}^{3} LE_{CPUs}\} = \{низька(H), середня(C), висока(B)\}$ та ідентифікатори оціночних інтервалів. Врахуємо що в нормальних умовах середньої експлуатації потужностей ПК і при відсутності впливу порушників чи шкідливого ПЗ середній показник завантаженості процесора становить 15-35%. Звичайно норма може дещо варіюватися залежно від ОС, встановленого ПЗ і виробничих завдань організації. Максимально можливий відсоток завантаженості CPU=100%. Доцільно виділити такі ідентифікатори інтервалів: $\mathbf{N_{CPU}} = \{\bigcup_{q=1}^{3} N_{CPUq}\} =$ *{[0;5[,[5;50[,[50;100]}*. Таблиця оцінок (табл. 2.5) і базова матриця частот сформовані на основі експертних суджень відносно заданих підмножин будуть такими:

$$F_{CPU} = \begin{vmatrix} 8 & 2 & 0 \\ 3 & 10 & 0 \\ 0 & 3 & 8 \end{vmatrix}.$$

Використаємо (2.7) щоб знайти вектор сум і максимальний елемент відповідно:

$VS_{CPU} = \|11 \quad 15 \quad 8\|$ і $vsm_{CPU} = 15$.

Таблиця 2.5.

Узагальнена таблиця оцінок експертом значень параметра P_3

LE_3	N_3		
	$[0;5[$	$[5;50[$	$[50;100]$
Низька	8	2	0
Середня	3	10	0
Висока	0	3	8

Обрахуємо похідну матрицю частот, використавши вираз (2.6):

$$F'_{CPU} = \begin{vmatrix} 10,91 & 2 & 0 \\ 4,09 & 10 & 0 \\ 0 & 3 & 15 \end{vmatrix}.$$

та вектор максимумів $FM_{CPU} = \|10,91 \quad 10 \quad 15\|$.

Використавши формулу (2.8) обрахуємо матрицю належностей та супорти НЧ еталону для параметра P_3

$$M_{CPU} = \begin{vmatrix} 1 & 0,2 & 0 \\ 0,37 & 1 & 0 \\ 0 & 0,3 & 1 \end{vmatrix}$$

Супорти: $x_{CPU11} = x_{CPU21} = x_{CPU31} = 5/100 = 0,05$, $x_{CPU12} = x_{CPU22} = x_{CPU32} = 50/100 = 0,5$, $x_{CPU13} = x_{CPU23} = x_{CPU33} = 100/100 = 1$. Здійснивши перетворення отримаємо набір еталонів параметра $P_3 = CPU$ $\underset{\sim}{T}^e_{CPU} = \{\bigcup_{s=1}^{3} \underset{\sim}{T}^e_{CPU\,s}\} = \{низька(H), середня(C), висока(B)\}$ і терми ЛЗ для цього параметра:

$$\underset{\sim}{H} = \underset{\sim}{T}^e_{CPU1} = \{0/0,05;\quad 1/0,05;\quad 0,2/0,5;\quad 0/1\},$$

$$\underset{\sim}{C} = \underset{\sim}{T}^e_{CPU2} = \{0/0,05;\quad 0,37/0,05;\quad 1/0,5;\quad 0/1\},$$

$$\underset{\sim}{B} = \underset{\sim}{T}^e_{CPU3} = \{0/0,05;\quad 0,3/0,5;\quad 1/1;\quad 0/1\}.$$

Графік ФН термів ЛЗ «Завантаженість процесора» показаний на рис. 2.4.

Завантаженість оперативної пам'яті, $P_4 = MU$. Аналогічний за суттю з ЛЗ «Завантаженість процесора», тому ФН для них є практично ідентичними.

Введемо підмножину ідентифікаторів лінгвістичних оцінок $\mathbf{LE_{MU}} = \{\bigcup_{s=1}^{3} LE_{MUs}\} = \{низька(H), середня(C), висока(B)\}$ та ідентифікатори оціночних інтервалів. Враховуючи, що в нормальних умовах середньої експлуатації потужностей ПК і

при відсутності впливу шкідливого ПЗ середній показник завантаженості оперативної пам'яті становить 10-20%. в стані спокою та 20-40% під час активного виконання операцій на робочій станції. Більші показники свідчать про не нормальну роботу, що дуже ймовірно може бути спричинено вірусною, спам- та DDOs-атакоми чи діяльністю зломщика. Звичайно норма може дещо варіюватися залежно від ОС, встановленого ПЗ і виробничих завдань організації. Виходячи з цього $\mathbf{N_{MU}} = \{\bigcup_{q=1}^{3} N_{MUq}\} = \{[0;20[,[20;50[,[50;100]\}$. Всі дані відображені в табл. 2.6.

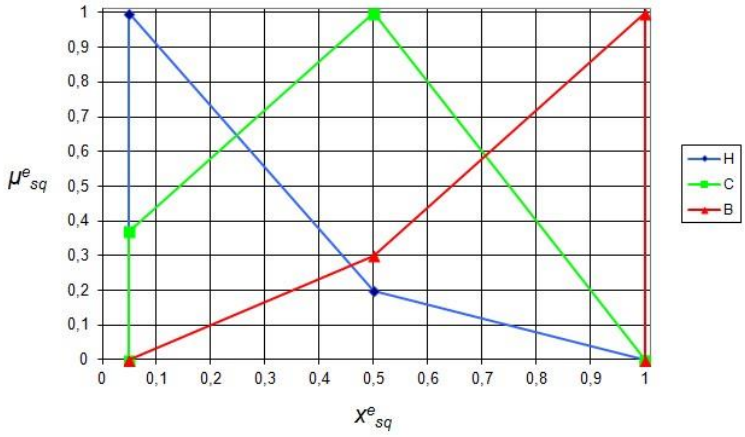


Рис. 2.4. ФН лінгвістичних термів еталонів нечітких чисел для *CPU*

Таблиця 2.6.

Узагальнена таблиця оцінок експертом значень параметра P_4

LE4	**N4**		
	$[0;20[$	$[20;50[$	$[50;100]$
Низька	8	1	0
Середня	3	9	1
Висока	0	2	9

Сформована на основі даних таблиці базова матриця матиме такий вигляд, а також згідно (2.7) вектор сум та максимальний елемент будуть:.

$$F_{MU} = \begin{vmatrix} 8 & 1 & 0 \\ 3 & 9 & 1 \\ 0 & 2 & 9 \end{vmatrix}.$$

$VS_{MU} = \|11 \quad 12 \quad 10\|$ і $vsm_{MU} = 12$. Обрахуємо похідну матрицю частот, використавши вираз (2.6):

$$F'_{MU} = \begin{vmatrix} 8,72 & 1 & 0 \\ 3,27 & 9 & 1,2 \\ 0 & 2 & 10,8 \end{vmatrix}$$

та вектор максимумів $FM_{MU} = \|8,72 \quad 9 \quad 10,8\|$.

Використавши формулу (2.8) обрахуємо матрицю належностей та супорти НЧ еталону для параметра P_4

$$M_{MU} = \begin{vmatrix} 1 & 0,11 & 0 \\ 0,38 & 1 & 0,11 \\ 0 & 0,22 & 1 \end{vmatrix}.$$

Супорти: $x_{MU11} = x_{MU21} = x_{MU31} = 20/100 = 0,2$, $x_{MU12} = x_{MU22} = x_{MU32} = 50/100 = 0,5$, $x_{MU13} = x_{MU23} = x_{MU33} = 100/100 = 1$. Здійснивши перетворення отримаємо набір еталонів параметра $P_4 = MU$ $T^e_{MU} = \{\bigcup_{s=1}^{3} T^e_{MU\,s}\} = \{низька(H), середня(C), висока(B)\}$ і терми ЛЗ для цього параметра:

$$\underset{\sim}{H} = T^e_{MU1} = \{0/0,2;\quad 1/0,2;\quad 0,11/0,5;\quad 0/1\},$$

$$\underset{\sim}{C} = T^e_{MU2} = \{0/0,2;\quad 0,38/0,2;\quad 1/0,5;\quad 0,11/1;\quad 0/1\},$$

$$\underset{\sim}{B} = T^e_{MU3} = \{0/0,2;\quad 0,22/0,5;\quad 1/1;\quad 0/1\}.$$

Графік ФН термів ЛЗ «Завантаженість оперативної пам'яті» показаний на рис. 2.5.

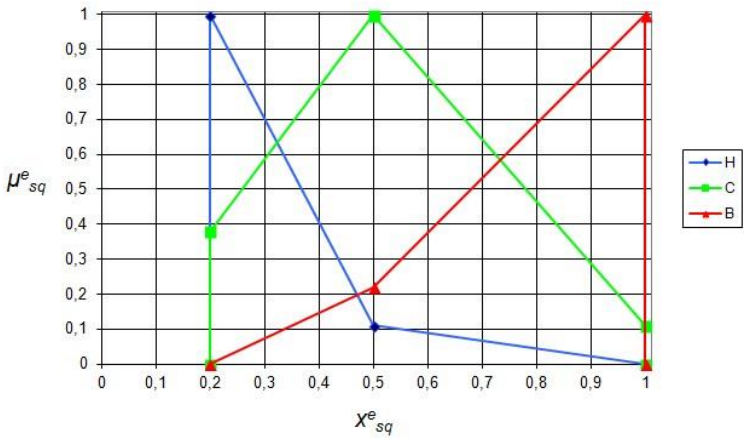


Рис. 2.5. ФН лінгвістичних термів еталонів нечітких чисел для *MU*

Кількість збоїв та помилок, $P_5 = NEr$. Функціональність ІС вважається нормальною, якщо в її роботі відсутні помилки та збої взагалі. Проте поява невеликої кількості збоїв все ж можлива, в основному через недостатню кваліфікацію кори-

стувача, його халатність або застосування неякісного апаратного / програмного забезпечення. Офіційної статистики з даного питання немає, тому складно визначити нормальну величину цього параметру. В рамках дослідження встановимо максимальну кількість помилок та збоїв за добу в 10 збоїв.

Введемо підмножину ідентифікаторів лінгвістичних оцінок $\mathbf{LE_{NEr}} = \{\bigcup_{s=1}^{3} LE_{NErs}\} = \{мала(M), середня(C), велика(B)\}$ та ідентифікатори оціночних інтервалів $\mathbf{N_{NEr}} = \{\bigcup_{q=1}^{3} N_{NErq}\} = \{[0;2[,[2;7[,[7;10]\}$. Таблиця оцінок і базова матриця частот сформовані на основі експертних суджень відносно заданих підмножин будуть такими:

Таблиця 2.7.

Узагальнена таблиця оцінок експертом значень параметра P_5

LE5	**N5**		
	$[0;2[$	$[2;7[$	$[7;10]$
Мала	7	1	0
Середня	1	8	1
Велика	0	1	8

Сформована на основі даних таблиці базова матриця матиме такий вигляд.

$$F_{NEr} = \begin{vmatrix} 7 & 1 & 0 \\ 1 & 8 & 1 \\ 0 & 1 & 8 \end{vmatrix}.$$

Використаємо (2.7) щоб знайти вектор сум і максимальний елемент відповідно $VS_{NEr} = \|8 \quad 10 \quad 9\|$ і $vsm_{NEr} = 10$. Обрахуємо похідну матрицю частот за виразом (2.6):

$$F'_{NEr} = \begin{vmatrix} 8,75 & 1 & 0 \\ 1,25 & 8 & 1,11 \\ 0 & 1 & 8,88 \end{vmatrix}$$

та вектор максимумів $FM_{NEr} = \|8,75 \quad 8 \quad 8,88\|$.

Використавши (2.8) обрахуємо матрицю належностей та супорти НЧ еталону для параметра P_5

$$M_{NEr} = \begin{vmatrix} 1 & 0,13 & 0 \\ 0,14 & 1 & 0,13 \\ 0 & 0,13 & 1 \end{vmatrix}.$$

Супорти: $x_{NEr11} = x_{NEr21} = x_{NEr31} = 2/10 = 0{,}2$, $x_{NEr12} = x_{NEr22} = x_{NEr32} = 7/10 = 0{,}7$, $x_{NEr13} = x_{NEr23} = x_{NEr33} = 10/10 = 1$. Здійснивши перетворення отримаємо набір еталонів параметра $P_5 = NEr$ $\underset{\sim}{T}^e_{NEr} = \{\bigcup_{s=1}^{3} \underset{\sim}{T}^e_{NErs}\} = \{мала(M), середня(C), велика(B)\}$ і терми ЛЗ для цього параметра

$$\underset{\sim}{M} = \underset{\sim}{T}^e_{NEr1} = \{0/0,2;\quad 1/0,2;\quad 0,13/0,7;\quad 0/1\},$$

$$\underset{\sim}{C} = \underset{\sim}{T}^e_{NEr2} = \{0/0,2;\quad 0,14/0,2;\quad 1/0,7;\quad 0,13/1;\quad 0/1\},$$

$$\underset{\sim}{B} = \underset{\sim}{T}^e_{NEr3} = \{0/0,2;\quad 0,13/0,7;\quad 1/1;\quad 0/1\}.$$

Графік ФН термів ЛЗ «Кількість збоїв та помилок» показаний на рис. 2.6.

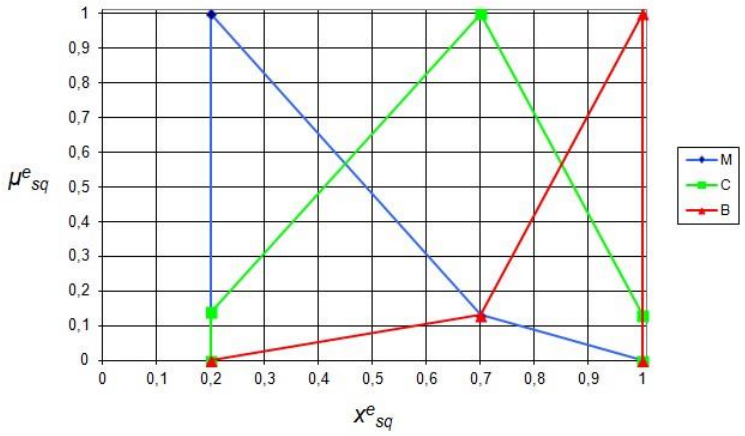


Рис.2.6. ФН лінгвістичних термів еталонів нечітких чисел для NEr

Час виконання процесу, $P_6 = RTPr$. Використовуються лише в випадках виявлення злому ІС. Залежить від виду організації, виробничих процесів, функцій, прав та обов'язків персоналу. Легітимний користувач у ІС в процесі виконання своїх посадових обов'язків працює з певним файлом чи процесом протягом певного часу. Так середньостатистичний працівник працює з одним файлом чи процесом період часу від 30 хвилин до 3 годин. Якщо цей показник значно менший чи більший, то це може свідчити про підозрілу активність. Оскільки зазвичай робоча зміна триває близько 8 годин, то встановимо верхню межу в 12 годин, що визначає ідентифікатори інтервалів.

Введемо підмножину ідентифікаторів лінгвістичних оцінок $\mathbf{LE_{RTPr}} = \{\bigcup_{s=1}^{3} LE_{RTPrs}\} = \{малий(M), середній(C), великий(B)\}$ та ідентифікатори оціночних

інтервалів $\mathbf{N_{RTPr}} = \{\bigcup_{q=1}^{3} N_{RTPrq}\} = \{[0;3[,[3;6[,[6;12]\}$ і наведемо узагальнено оцінку експертних оцінок (див. табл. 2.7).

Таблиця 2.8.

Узагальнена таблиця оцінок експертом значень параметра P_6

LE6	**N6**		
	[0;3[	[3;6[	[6;12]
Малий	9	0	0
Середній	2	9	1
Великий	0	4	8

Сформована на основі даних таблиці базова матриця матиме такий вигляд, а також згідно (2.7) вектор сум та максимальний елемент будуть:.

$$F_{RTPr} = \begin{vmatrix} 9 & 0 & 0 \\ 2 & 9 & 1 \\ 0 & 4 & 8 \end{vmatrix},$$

$VS_{RTPr} = \|11 \quad 13 \quad 9\|$ і $vsm_{RTPr} = 13$. Обрахуємо похідну матрицю частот, використавши вираз (2.6):

$$F'_{RTPr} = \begin{vmatrix} 10,63 & 0 & 0 \\ 2,36 & 9 & 1,44 \\ 0 & 4 & 11,56 \end{vmatrix}$$

та вектор максимумів $FM_{RTPr} = \|10,63 \quad 9 \quad 11,56\|$.

Використавши формулу (2.8) обрахуємо матрицю належностей та супорти НЧ еталону для параметра P_6

$$M_{RTPr} = \begin{vmatrix} 1 & 0 & 0 \\ 0,22 & 1 & 0,12 \\ 0 & 0,44 & 1 \end{vmatrix}.$$

Супорти: $x_{RTPr11} = x_{RTPr21} = x_{RTPr31} = 3/12 = 0,25$, $x_{RTPr12} = x_{RTPr22} = x_{RTPr32} = 6/12 = 0,5$, $x_{RTPr13} = x_{RTPr23} = x_{RTPr33} = 12/12 = 1$. Здійснивши перетворення отримаємо набір еталонів параметра $P_6 = RT\,\mathrm{Pr}$ $\underset{\sim}{T}^e_{RTPr} = \{\bigcup_{s=1} \underset{\sim}{T}^e_{RTPrs}\} = \{малий(M), середній(C), великий(B)\}$ і терми ЛЗ для цього параметра

$$\underset{\sim}{M} = \underset{\sim}{T}^e_{RTPr1} = \{0/0,25; \quad 1/0,25; \quad 0/0,5; \quad 0/1\},$$

$$\underset{\sim}{C} = \underset{\sim}{T}^e_{RTPr2} = \{0/0,25; \quad 0,22/0,25; \quad 1/0,5; \quad 0,12/1; \quad 0/1\},$$

$$\underset{\sim}{B} = \underset{\sim}{T}^{e}_{RTPr3} = \{0/0,25;\quad 0,44/0,5;\quad 1/1;\quad 0/1\}.$$

Графік ФН термів ЛЗ «Час виконання процесу» показаний на рис. 2.7.

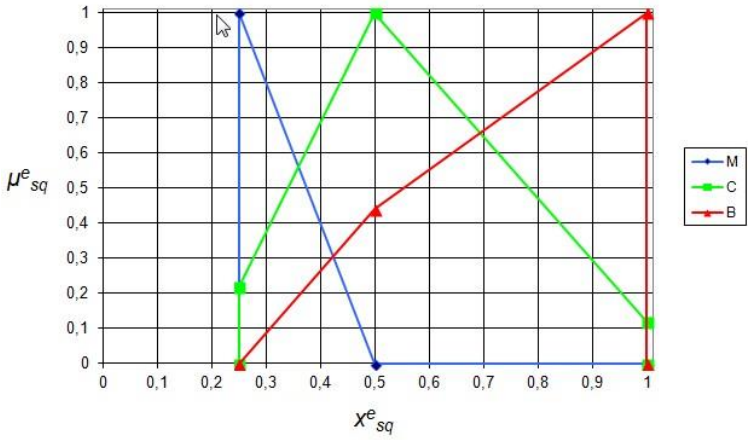


Рис. 2.7. ФН лінгвістичних термів еталонів нечітких чисел для *RTPr*

Завантаженість мереженого каналу, $P_7 = CNCh$. Моніторинг трафіку дозволяє фіксувати дані, які передаються по інтернет-каналу. Значне зростання трафіку свідчить про можливу DDos-атаку або іншу атаку.

Введемо підмножину ідентифікаторів лінгвістичних оцінок $\mathbf{LE_{CNCh}} = \{\bigcup_{s=1}^{3} LE_{CNChs}\} = \{низька(H), середня(C), висока(B)\}$ та ідентифікатори оціночних інтервалів. Врахуємо що для того, щоб використовувати даний параметр необхідно дослідити пропускну здатність каналу і середнє значення об'єму трафіку, що проходить по цьому каналу за певний період часу. В звичайних умовах величина переданої і отриманої інформації за умов звичайного використання хоста в ІС були близьке до середнього значення, тобто відрізнятиметься на відносно невелику величину. Так, якщо виразити ці величини у відсотки, прийнявши $CNCh_{aver}$=100%, то нормальні показники з врахуванням режиму роботи коливатимуться в межах 50-120%. Для дослідження візьмемо верхню межу B=200%, хоча на практиці цей показник може бути і більший. Доцільно виділити такі ідентифікатори інтервалів: $\mathbf{N_{CNCh}} = \{\bigcup_{q=1}^{3} N_{CNChq}\} = \{[0;60[, [60;140[, [140;200]\}$. Результати відображенві в табл. 2.9.

Сформована на основі даних таблиці базова матриця матиме такий вигляд.

$$F_{CNCh} = \begin{vmatrix} 9 & 1 & 0 \\ 1 & 9 & 1 \\ 0 & 2 & 8 \end{vmatrix}.$$

Використаємо (2.7) щоб знайти вектор сум і максимальний елемент відповідно $VS_{CNCh} = \|10 \quad 12 \quad 9\|$ і $vsm_{CNCh} = 12$. Обрахуємо похідну матрицю частот, використавши вираз (2.6):

$$F'_{CNCh} = \begin{vmatrix} 10,8 & 1 & 0 \\ 1,2 & 9 & 1,33 \\ 0 & 2 & 10,67 \end{vmatrix}$$

та вектор максимумів $FM_{CNCh} = \|10,8 \quad 9 \quad 10,67\|$.

Таблиця 2.9.

Узагальнена таблиця оцінок експертом значень параметра P_7

LE7	**N7**		
	$[0;60[$	$[60;140[$	$[140;200]$
Низька	9	1	0
Середня	1	9	1
Висока	0	2	8

Використавши (2.8) обрахуємо матрицю належностей та суппорти НЧ еталону для параметра P_7

$$M_{CNCh} = \begin{vmatrix} 1 & 0,11 & 0 \\ 0,11 & 1 & 0,12 \\ 0 & 0,22 & 1 \end{vmatrix}.$$

Супорти: $x_{CNCh11} = x_{CNCh21} = x_{CNCh31} = 60 / 200 = 0,3$, $x_{CNCh12} = x_{CNCh22} = x_{CNCh32} = 140 / 200 = 0,7$, $x_{CNCh13} = x_{CNCh23} = x_{CNCh33} = 200 / 200 = 1$. Здійснивши перетворення отримаємо набір еталонів параметра $P_7 = CNCh$ $\underset{\sim}{T}^e_{CNCh} = \{\bigcup_{s=1}^{3} \underset{\sim}{T}^e_{CNChs}\} = \{низька(H), \ середня(C), висока(B)\}$ і терми ЛЗ для цього параметра

$$\underset{\sim}{H} = \underset{\sim}{T}^e_{CNCh1} = \{0/0,3; \quad 1/0,3; \quad 0,11/0,7; \quad 0/1\},$$

$$\underset{\sim}{C} = \underset{\sim}{T}^e_{CNCh2} = \{0/0,3; \quad 0,11/0,3; \quad 1/0,7; \quad 0,12/1; \quad 0/1\},$$

$$\underset{\sim}{B} = \underset{\sim}{T}^e_{CNCh3} = \{0/0,3; \quad 0,22/0,7; \quad 1/1; \quad 0/1\}.$$

Графік ФН ЛЗ «Завантаженість мережевого каналу» показаний на рис. 2.8.

Кількість одночасних підключень, $P_8 = NCC$. Використовувані на сьогодні сервери мають різну конфігурацію. Проте практика показує, що найбільш часто максимально можлива кількість підключень встановлюється на рівні 1024

підключення. В нормальних умовах функціонування серверів крупних організацій зазвичай коливається в межах 100-200 одночасних підключень. Ці параметри обумовлюють розміри заданих інтервалів.

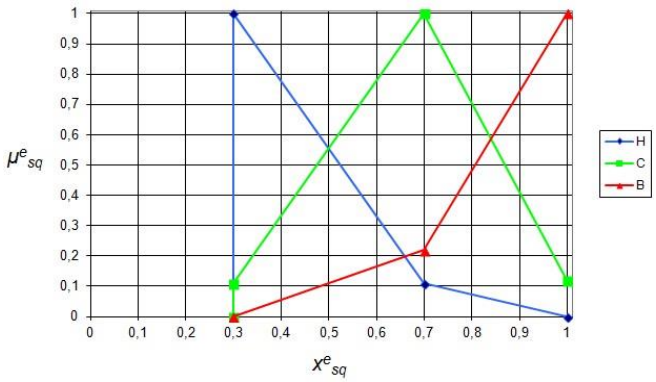


Рис. 2.8. ФН лінгвістичних термів еталонів нечітких чисел для *CNCh*

Введемо підмножину ідентифікаторів лінгвістичних оцінок $\mathbf{LE_{NCC}} = \{\bigcup_{s=1}^{3} LE_{NCCs}\} = \{мала(M), середня(C), велика(B)\}$ та ідентифікатори оціночних інтервалів $\mathbf{N_{NCC}} = \{\bigcup_{q=1}^{3} N_{NCCq}\} = \{[0;64[, [64;512[, [512;1024]\}$. Тепер сформуємо узагальнену таблицю оцінок і базову матрицю частот (див. табл. 2.10).

Таблиця 2.10.

Узагальнена таблиця оцінок експертом значень параметра P_8

LE8	**N8**		
	[0;64[	[64;512[	[512;1024]
Мала	11	1	0
Середня	2	12	1
Велика	0	3	11

Сформована на основі даних таблиці базова матриця матиме такий вигляд.

$$F_{NCC} = \begin{vmatrix} 11 & 1 & 0 \\ 2 & 12 & 1 \\ 0 & 3 & 11 \end{vmatrix}$$

Розрахуємо вектор сум $VS_{NCC} = \|13 \quad 16 \quad 14\|$ і знайдемо максимальне значення цього вектору $vsm_{NCC} = 16$. Використавши вираз (2.6) отримаємо похідну матрицю частот

$$F'_{NCC} = \begin{vmatrix} 13{,}54 & 1 & 0 \\ 2{,}46 & 12 & 1{,}14 \\ 0 & 3 & 12{,}57 \end{vmatrix}$$

та вектор максимумів $FM_{NCC} = \|13,54 \quad 12 \quad 12,57\|$.

Використавши формулу (2.8) обрахуємо матрицю належностей та супорти НЧ еталону для параметра P_8

$$M_{NCC} = \begin{vmatrix} 1 & 0,08 & 0 \\ 0,18 & 1 & 0,09 \\ 0 & 0,25 & 1 \end{vmatrix}$$

Супорти: $x_{NCC11} = x_{NCC21} = x_{NCC31} = 64/1024 = 0,0625$, $x_{NCC12} = x_{NCC22} = x_{NCC32} = 512/1024$ $0,5$, $x_{NCC13} = x_{NCC23} = x_{NCC33} = 1024/1024 = 1$. Здійснивши перетворення отримаємо набір еталонів параметра $P_8 = NCC$ $\underset{\sim}{T}^e_{NCC} = \{\bigcup_{s=1}^{3} \underset{\sim}{T}^e_{NCCs}\} = \{мала(M), середня(C), велика(B)\}$ і терми ЛЗ для цього параметра

$$\underset{\sim}{M} = \underset{\sim}{T}^e_{NCC1} = \{0/0,0625; \quad 1/0,0625; \quad 0,08/0,5; \quad 0/1\},$$

$$\underset{\sim}{C} = \underset{\sim}{T}^e_{NCC2} = \{0/0,0625; \quad 0,18/0,0625; \quad 1/0,5; \quad 0,09/1; \quad 0/1\},$$

$$\underset{\sim}{B} = \underset{\sim}{T}^e_{NCC3} = \{0/0,0625; \quad 0,25/0,5; \quad 1/1; \quad 0/1\}.$$

Графік ФН термів ЛЗ Час входу в систему показаний на рис. 2.9.

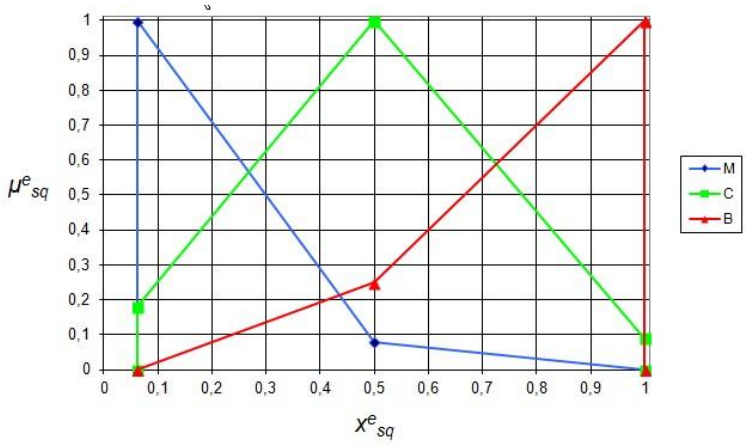


Рис.2.9. ФН лінгвістичних термів еталонів нечітких чисел для NCC

Затримка між запитами від одного джерела, $P_9 = DbR$. Параметр характеризує час між послідовними запитами від одного підключеного до сервера клієнта. Велика частота запитів, тобто зменшення часу між окремими відправками пакетів, може свідчити про початок DDoS-атаки.

Введемо підмножину ідентифікаторів лінгвістичних оцінок $\mathbf{LE_{DbR}} = \{\bigcup_{s=1}^{3} LE_{DbRs}\} = \{мала(M), середня(C), велика(B)\}$ та ідентифікатори оціночних інтервалів,

вводячи які врахуємо наступні положення. Значення затримки вимірюється в мілісекундах. Так, при мережевій взаємодії при відправлені / прийманні пакетів даних або запитів на з'єднання відзначається певна часова затримка. В звичайних умовах зазвичай ця затримка становить від декількох мілісекунд до десятків секунд. При цьому при надзвичайно великій частоті запитів ймовірність того, що система атакується значно зростає. Величини інтервалів і максимальне значення приймемо відштовхуючись від статистики запитів GET і POST. В нашому дослідженні обмежимось величиною запитів в 1000 мс. Доцільно виділити такі інтервали: $\mathbf{N_{DbR}} = \{\bigcup_{q=1}^{3} N_{DbRq}\} = \{[0;30[,[30;300[,[300;1000]\}$. В табл. 2.11 наведемо узагальнені оцінки експерта.

Таблиця 2.11.

Узагальнена таблиця оцінок експертом значень параметра P_9

LE9	**N9**		
	$[0;30[$	$[30;300[$	$[300;1000]$
Мала	9	2	0
Середня	1	8	3
Велика	0	1	10

Сформована на основі даних таблиці базова матриця матиме такий вигляд

$$F_{DbR} = \begin{vmatrix} 9 & 2 & 0 \\ 1 & 8 & 3 \\ 0 & 1 & 10 \end{vmatrix}.$$

Використаємо (2.7) щоб знайти вектор сум і максимальний елемент відповідно $VS_{DbR} = \|10 \quad 11 \quad 13\|$ і $vsm_{DbR} = 13$, а також похідну матрицю частот, використавши (2.6):

$$F'_{DbR} = \begin{vmatrix} 11,7 & 2,36 & 0 \\ 1,3 & 9,45 & 3 \\ 0 & 1,18 & 10 \end{vmatrix}$$

та вектор максимумів $FM_{DbR} = \|11,7 \quad 9,45 \quad 10\|$.

Використавши формули (2.8) обрахуємо матрицю належностей та супорти НЧ еталону для параметра P_9

$$M_{DbR} = \begin{vmatrix} 1 & 0,25 & 0 \\ 0,11 & 1 & 0,3 \\ 0 & 0,12 & 1 \end{vmatrix}.$$

Супорти: $x_{DbR11} = x_{DbR21} = x_{DbR31} = 30/1000 = 0{,}03$, $x_{DbR12} = x_{DbR22} = x_{DbR32} = 300/1000 = 0{,}3$, $x_{DbR13} = x_{DbR23} = x_{DbR33} = 1000/1000 = 1$. Здійснивши перетворення отримаємо набір еталонів параметра $P_9 = DbR$ $\underset{\sim}{T}^e_{DbRs} = \{\bigcup_{s=1}^{3} \underset{\sim}{T}^e_{DbRs}\} = \{мала(M), середня(C), велика(B)\}$ і терми ЛЗ для цього параметра:

$$\underset{\sim}{M} = \underset{\sim}{T}^e_{DbR1} = \{0/0{,}03;\quad 1/0{,}03;\quad 0{,}25/0{,}3;\quad 0/1\},$$

$$\underset{\sim}{C} = \underset{\sim}{T}^e_{DbR2} = \{0/0{,}03;\quad 0{,}11/0{,}03;\quad 1/0{,}3;\quad 0{,}3/1;\quad 0/1\},$$

$$\underset{\sim}{B} = \underset{\sim}{T}^e_{DbR3} = \{0/0{,}03;\quad 0{,}12/0{,}3;\quad 1/1;\quad 0/1\}.$$

Графік ФН термів ЛЗ «Затримка» показаний на рис. 2.10.

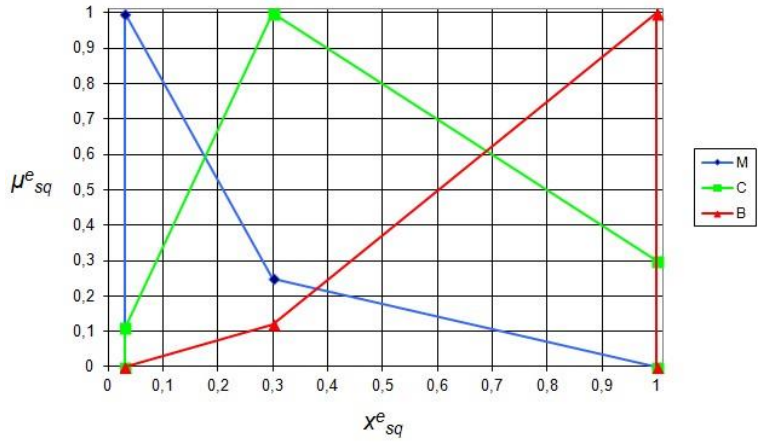


Рис.2.10. ФН лінгвістичних термів еталонів нечітких чисел для DbR

Розмір тимчасових файлів, $P_{10} = STF$. Це величина, що демонструє, скільки місця тимчасовий файл чи каталог з ними займають на жорсткому диску. Візьмемо, наприклад, операційну систему Windows 7. В ній знаходиться декілька тимчасових каталогів: C:\Windows\Temp, C:\Users\ Імя користувача\ AppData\ Local\ Temp, C:\Users\All Users\TEMP, C:\Users\Default\AppData\Local\Temp. Проведені експерименти в [64] показали, що каталог C: \ Windows \ Temp, за день роботи на комп'ютері накопичив всього 33,7 Мб, хоча за тиждень це значення може становити кілька гігабайт. Каталог C: \ Users \ Ім'я користувача \ AppData \ Local \ Temp, за день роботи накопичив 149 Мб. Таким чином приріст тимчасових файлів за добу склав близько 200 Мб. Проте це число може значно варіюватись залежно від режиму роботи, виконуваних операцій, тощо. Так тимчасовий файл MS Word має розмір менше 1 Кб. Тому візьмемо максимальне значення, що

визначає особливості створення інтервалів, для дослідження 1000 Мб (хоча це значення на практиці може бути більшим при створені так званих форк-бомб).

Введемо підмножину ідентифікаторів лінгвістичних оцінок $\mathbf{LE_{STF}} = \{\bigcup_{s=1}^{3} LE_{STFs}\} = \{малий(M), середній(C), великий(B)\}$ та ідентифікатори оціночних інтервалів $\mathbf{N_{STF}} = \{\bigcup_{q=1}^{3} N_{STFq}\} = \{[0;100[, [100;500[, [500;1000]\}$. Сформуємо узагальнену таблицю оцінок (див. табл.. 2.12) і базову матрицю частот.

Таблиця 2.12.

Узагальнена таблиця оцінок експертом значень параметра P_{10}

$\mathbf{LE_{10}}$	$\mathbf{N_{10}}$		
	$[0;100[$	$[100;500[$	$[500;1000]$
Малий	7	2	0
Середній	1	8	2
Великий	0	1	8

Сформована на основі даних таблиці базова матриця матиме такий вигляд.

$$F_{STF} = \begin{vmatrix} 7 & 2 & 0 \\ 1 & 8 & 2 \\ 0 & 1 & 8 \end{vmatrix}.$$

Згідно (2.7) $VS_{STF} = \|8 \quad 11 \quad 10\|$ і $vsm_{STF} = 11$. Обрахуємо похідну матрицю частот, використавши вираз (2.6):

$$F'_{STF} = \begin{vmatrix} 9,63 & 2 & 0 \\ 1,38 & 8 & 2,2 \\ 0 & 1 & 8,8 \end{vmatrix}$$

та вектор максимумів $FM_{STF} = \|9,63 \quad 8 \quad 8,8\|$.

Використавши формулу (2.8) обрахуємо матрицю належностей та суппорти НЧ еталону для параметра P_{10}

$$M_{STF} = \begin{vmatrix} 1 & 0,25 & 0 \\ 0,14 & 1 & 0,25 \\ 0 & 0,13 & 1 \end{vmatrix}.$$

Супорти: $x_{STF11} = x_{STF21} = x_{STF31} = 100/1000 = 0,1$, $x_{STF12} = x_{STF22} = x_{STF32} = 500/1000 = 0,5$, $x_{STF13} = x_{STF23} = x_{STF33} = 1000/1000 = 1$. Здійснивши перетворення отримаємо набір ета-

лонів параметра $P_{10} = STF$ $\underset{\sim}{T}^e_{STF} = \{\bigcup_{s=1}^{3} \underset{\sim}{T}^e_{STFs}\} = \{малий(M), середній(C), великий(B)\}$ і терми ЛЗ для цього параметра

$$\underset{\sim}{M} = \underset{\sim}{T}^e_{STF1} = \{0/0{,}1;\quad 1/0{,}1;\quad 0{,}25/0{,}5;\quad 0/1\},$$

$$\underset{\sim}{C} = \underset{\sim}{T}^e_{STF2} = \{0/0{,}1;\quad 0{,}14/0{,}1;\quad 1/0{,}5;\quad 0{,}25/1;\quad 0/1\},$$

$$\underset{\sim}{B} = \underset{\sim}{T}^e_{STF3} = \{0/0{,}1;\quad 0{,}13/0{,}5;\quad 1/1;\quad 0/1\}.$$

Графік ФН термів ЛЗ параметра Частота запитів на вхід в систему показаний на рис. 2.11.

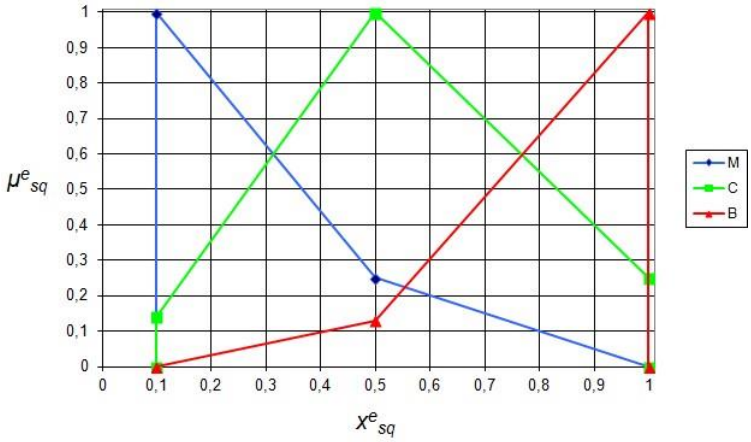


Рис. 2.11. ФН лінгвістичних термів еталонів нечітких чисел для STF

Параметри $P_{11} = T$, $P_{12} = H$, $P_{13} = D$ мають фізичну природу, досить вузький діапазон можливих значень і відповідно ІПКС, що виникають через їх вплив, надто чутливі до їх змін, тому при побудові еталонів опишемо для них 5 термів, а не 3 як у попередніх випадках.

Температура в серверній кімнаті, $P_{11} = T$. Оптимальна температура для правильної роботи сервера становить 15-30 ° С. Висока температура влітку може привести до його тимчасового або повної відмови. Це призведе до простою співробітників і, можливо, зриву наміченого плану або втрати замовлень. Для забезпечення оптимальної температури в приміщенні необхідно використовувати кондиціонери і відповідне опалення. Крім того, самі сервери виділяють багато тепла. Тому в приміщенні важливо забезпечити хорошу циркуляцію повітря.

Введемо підмножину ідентифікаторів лінгвістичних оцінок $\mathbf{LE_T} = \{\bigcup_{s=1}^{5} LE_{Ts}\} =$ $\{\textit{дуже мала}(ДМ), \textit{мала}(М), \textit{середня}(С), \textit{велика}(В), \textit{дуже велика}(ДВ)\}$ та ідентифікатори оціночних інтервалів, обмеживши верхню межу в 40°С, $\mathbf{N_T} = \{\bigcup_{q=1}^{5} N_{Tq}\} =$ $\{[0;10[, [10;15[, [15;30[, [30;37[, [37;40]\}$. Тепер сформуємо узагальнену таблицю оцінок (див. табл. 2.13) і базову матрицю частот.

Таблиця 2.13.

Узагальнена таблиця оцінок експертом значень параметра P_{11}

LE11	**N11**				
	[0;10[	[10;15[	[15;30[	[30;37[	[37;40[
Дуже мала	9	3	0	0	0
Мала	5	10	1	0	0
Середня	1	5	7	1	0
Велика	0	1	2	9	2
Дуже велика	0	0	0	6	10

Сформована на основі даних таблиці базова матриця матиме такий вигляд:

$$F_T = \begin{vmatrix} 9 & 3 & 0 & 0 & 0 \\ 5 & 10 & 1 & 0 & 0 \\ 1 & 5 & 7 & 1 & 0 \\ 0 & 1 & 2 & 9 & 2 \\ 0 & 0 & 0 & 6 & 10 \end{vmatrix}.$$

Розрахуємо вектор сум $VS_T = \|15 \quad 19 \quad 10 \quad 16 \quad 12\|$ і знайдемо максимальне значення цього вектору $\text{vsm}_T = 19$.

Використавши вираз (2.6) отримаємо похідну матрицю частот

$$F_T^{'} = \begin{vmatrix} 11,4 & 3 & 0 & 0 & 0 \\ 6,33 & 10 & 1,9 & 0 & 0 \\ 1,27 & 5 & 13,3 & 1,19 & 0 \\ 0 & 1 & 3,8 & 10,69 & 3,17 \\ 0 & 0 & 0 & 7,13 & 15,83 \end{vmatrix}.$$

та вектор максимумів $FM_T = \|11,4 \quad 10 \quad 13,3 \quad 10,69 \quad 15,83\|$.

Супорти даного НЧ: $x_{T11} = x_{T21} = x_{T31} = x_{T41} = x_{T51} = 10 / 40 = 0,25$, $x_{T12} = x_{T22} = x_{T32} = x_{T42} = x_{T52} = 15 / 40 = 0,375$, $x_{T13} = x_{T23} = x_{T33} = x_{T43} = x_{T53} = 30 / 40 = 0,75$, $x_{T14} = x_{T24} = x_{T34} = x_{T44} =$

$x_{T54} = 37/40 = 0{,}925$, $x_{T15} = x_{T25} = x_{T35} = x_{T45} = x_{T55} = 40/40 = 1$. Використавши формулу (2.8) обрахуємо матрицю належностей та суппорти НЧ еталону для параметра P_{11}

$$M_T = \begin{vmatrix} 1 & 0{,}3 & 0 & 0 & 0 \\ 0{,}56 & 1 & 0{,}14 & 0 & 0 \\ 0{,}11 & 0{,}5 & 1 & 0{,}11 & 0 \\ 0 & 0{,}1 & 0{,}29 & 1 & 0{,}23 \\ 0 & 0 & 0 & 0{,}67 & 1 \end{vmatrix}.$$

Здійснивши перетворення отримаємо набір еталонів параметра $P_{11} = T$ $\underset{\sim}{T}^e_T = \{\bigcup_{s=1}^{5} \underset{\sim}{T}^e_{Ts}\} = \{дуже\ мала(ДМ), мала(М), середня(С), велика(В), дуже\ велика(ДВ)\}$ і терми ЛЗ для цього параметра:

$$ДМ = \underset{\sim}{T}^e_{T1} = \{0/0{,}25;\quad 1/0{,}25;\quad 0{,}3/0{,}375;\quad 0/0{,}75\},$$

$$М = \underset{\sim}{T}^e_{T2} = \{0/0{,}25;\quad 0{,}56/0{,}25;\quad 1/0{,}375;\quad 0{,}14/0{,}75;\quad 0/0{,}925\},$$

$$С = \underset{\sim}{T}^e_{T3} = \{0/0{,}25;\quad 0{,}11/0{,}25;\quad 0{,}5/0{,}375;\quad 1/0{,}75;\quad 0{,}11/0{,}925;\quad 0/1\},$$

$$В = \underset{\sim}{T}^e_{T4} = \{0/0{,}25;\quad 0{,}1/0{,}375;\quad 0{,}29/0{,}75;\quad 1/0{,}925;\quad 0{,}23/1;\quad 0/1\},$$

$$ДВ = \underset{\sim}{T}^e_{T5} = \{0/0{,}75;\quad 0{,}67/0{,}925;\quad 1/1;\quad 0/1\}.$$

Графік ФН термів ЛЗ «Температура в серверній» показаний на рис. 2.12.

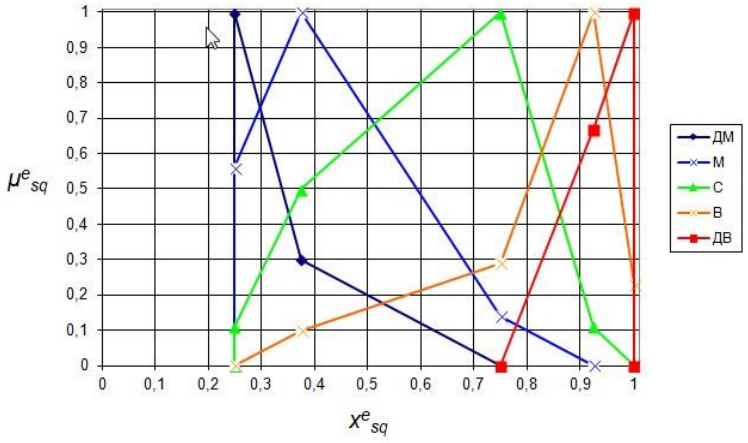


Рис. 2.12. ФН лінгвістичних термів еталонів нечітких чисел для Т

Вологість повітря в серверній кімнаті, $P_{12} = H$. Серверне обладнання чутливо до рівня вологи. Важливо щоб в приміщенні, в якому розташовується сервер, рівень вологості підтримувався в межах 40-55% або хоча б 40-60%. При більш високій вологості вода, що знаходиться в повітрі, конденсується на платах обладнання. Конденсат призводить до окислення контактів і замикань. Цього

можна уникнути, якщо використовувати кондиціонери з функцією осушення повітря. Якщо вологість у приміщенні, в якому розташовується сервер навпаки занадто низька, можуть виникнути проблеми з електростатичними розрядами, які виводять складне і дороге устаткування з ладу. Щоб підвищити рівень вологості в приміщенні, застосовуються зволожувачі повітря.

Введемо підмножину ідентифікаторів лінгвістичних оцінок $\mathbf{LE_H} = \{\bigcup_{s=1}^{5} LE_{Hs}\} =$ $\{\text{дуже низька}(ДН), \text{низька}(Н), \text{середня}(С), \text{висока}(В), \text{дуже висока}(ДВ)\}$ та ідентифікатори оціночних інтервалів $\mathbf{N_{12}} = \{\bigcup_{q=1}^{5} N_{12q}\} = \{[0;20[, [20;45[, [45;55[, [55;80[, [80;100]\}$. Таблиця оцінок (див. табл.. 2.14) і базова матриця частот сформовані на основі експертних суджень відносно заданих підмножин будуть такими:

Таблиця 2.14.

Узагальнена таблиця оцінок експертом значень параметра P_{12}

$\mathbf{LE_{12}}$	$\mathbf{N_{12}}$				
	$[0;20[$	$[20;45[$	$[45;55[$	$[55;80[$	$[80;100[$
Дуже низька	8	5	1	0	0
Низька	4	7	1	0	0
Середня	1	4	9	3	1
Висока	0	0	1	7	3
Дуже висока	0	0	0	5	10

Сформована на основі даних таблиці базова матриця матиме такий вигляд.

$$F_H = \begin{vmatrix} 8 & 5 & 1 & 0 & 0 \\ 4 & 7 & 1 & 0 & 0 \\ 1 & 4 & 9 & 3 & 1 \\ 0 & 0 & 1 & 7 & 3 \\ 0 & 0 & 0 & 5 & 10 \end{vmatrix}.$$

Використаємо (2.7) щоб знайти вектор сум і максимальний елемент $VS_H = \|13 \quad 16 \quad 12 \quad 15 \quad 14\|$ і $vsm_H = 16$. Обрахуємо похідну матрицю частот, використавши вираз (2.6):

$$F_H^{'} = \begin{vmatrix} 9{,}85 & 5 & 1{,}33 & 0 & 0 \\ 4{,}92 & 7 & 1{,}33 & 0 & 0 \\ 1{,}23 & 4 & 12 & 3{,}2 & 1{,}14 \\ 0 & 0 & 1{,}33 & 7{,}47 & 3{,}43 \\ 0 & 0 & 0 & 5{,}33 & 11{,}43 \end{vmatrix}.$$

та вектор максимумів $FM_H = \|9{,}85 \quad 7 \quad 12 \quad 7{,}47 \quad 11{,}43\|$.

Використавши формулу (2.8) обрахуємо матрицю належностей та суппорти НЧ еталону для параметра P_{12}

$$M_H = \begin{vmatrix} 1 & 0{,}71 & 0{,}11 & 0 & 0 \\ 0{,}5 & 1 & 0{,}11 & 0 & 0 \\ 0{,}12 & 0{,}57 & 1 & 0{,}43 & 0{,}1 \\ 0 & 0 & 0{,}11 & 1 & 0{,}3 \\ 0 & 0 & 0 & 0{,}71 & 1 \end{vmatrix}.$$

Супорти: $x_{H11} = x_{H21} = x_{H31} = x_{H41} = x_{H51} = 20/100 = 0{,}2$, $x_{H12} = x_{H22} = x_{H32} = x_{H42} = x_{H52} = 45/100 = 0{,}45$, $x_{H13} = x_{H23} = x_{H33} = x_{H43} = x_{H53} = 55/100 = 0{,}55$, $x_{H14} = x_{H24} = x_{H34} = x_{H44} = x_{H54} = 80/100 = 0{,}8$, $x_{H15} = x_{H25} = x_{H35} = x_{H45} = x_{H55} = 100/100 = 1$. Здійснивши перетворення отримаємо набір еталонів параметра $P_{12} = H$ $\underset{\sim}{T}^e_H = \{\bigcup_{s=1}^{5} \underset{\sim}{T}^e_{Hs}\} = \{$*дуже низька*$(ДН)$, *низька*$(Н)$, *середня*$(С)$, *висока*$(В)$, *дуже висока*$(ДВ)\}$ і терми ЛЗ для цього параметра:

$$\underset{\sim}{ДН} = \underset{\sim}{T}^e_{H1} = \{0/0{,}2; \quad 1/0{,}2; \quad 0{,}71/0{,}45; \quad 0{,}11/0{,}55; \quad 0/0{,}8\},$$

$$\underset{\sim}{Н} = \underset{\sim}{T}^e_{H2} = \{0/0{,}2; \quad 0{,}5/0{,}2; \quad 1/0{,}45; \quad 0{,}11/0{,}55; \quad 0/0{,}8\},$$

$$\underset{\sim}{С} = \underset{\sim}{T}^e_{H3} = \{0/0{,}2; \quad 0{,}12/0{,}2; \quad 0{,}57/0{,}45; \quad 1/0{,}55; \quad 0{,}43/0{,}8; \quad 0{,}1/1; \quad 0/1\},$$

$$\underset{\sim}{В} = \underset{\sim}{T}^e_{H4} = \{0/0{,}45; \quad 0{,}11/0{,}55; \quad 1/0{,}8; \quad 0{,}3/1; \quad 0/1\},$$

$$\underset{\sim}{ДВ} = \underset{\sim}{T}^e_{H5} = \{0/0{,}55; \quad 0{,}71/0{,}8; \quad 1/1; \quad 0/1\}.$$

Графік ФН термів ЛЗ «Вологість повітря в серверній» показаний на рис. 2.13.

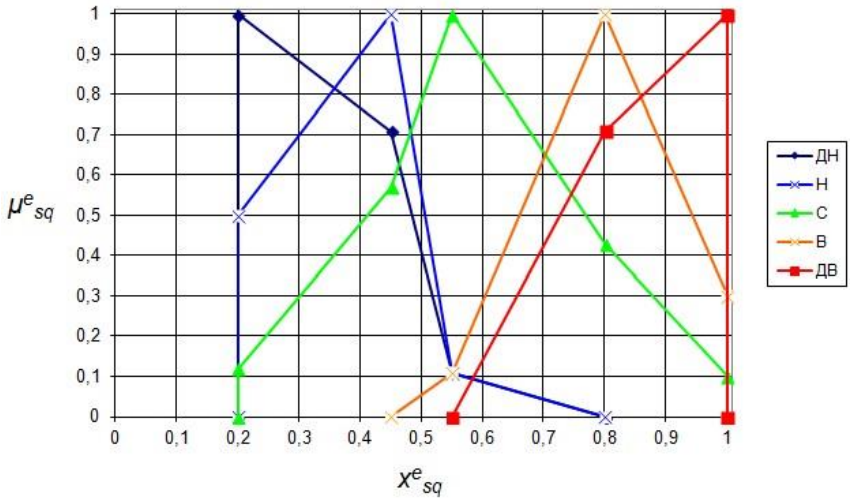


Рис.2.13. ФН лінгвістичних термів еталонів нечітких чисел для Н

Концентрація пилу в серверній кімнаті, $P_{13} = D$. Також як і волога, коротке замикання в платах сервера може викликати пил. Він проводить електрику, її велика кількість небезпечно для апаратури. Пил, що накопився і бруд ізолюють пристрої і заважають нормальному теплообміну. Якщо тепло не виділяється від пристрою, температура усередині елементів підніметься вище норми, що приведе до більш швидкого зносу. Пил – це головна причина збоїв у чіпах пам'яті. Тому для надійної роботи серверів повітря в приміщенні має бути чистим. Очищення проводиться за допомогою кондиціонерів, оснащених відповідними фільтрами. Тому наявність пилу в кімнаті за певної його концентрації може бути як причиною так і ознакою можливого інциденту, пов'язаного з виходом з ладу ІС внаслідок перегріву, зупинки технічних систем тощо. Введемо підмножину ідентифікаторів лінгвістичних оцінок $\mathbf{LE_D} = \{\bigcup_{s=1}^{5} LE_{Ds}\} = \{$*дуже мала*$(ДМ)$, *мала*$(М)$, *середня*$(С)$, *велика*$(В)$, *дуже велика*$(ДВ)\}$ та ідентифікатори оціночних інтервалів.

Врахуємо при цьому, що згідно стандартів, будівельних та санітарних норм, рекомендацій TIA [158] концентрація пилу в повітрі не повинна перевищувати 0,0001 г/м^3 = 100 мкг/м^3, тому $\mathbf{N_D} = \{\bigcup_{q=1}^{5} N_{Dq}\} = \{[0;10[, [10;35[, [35;65[, [65;90[, [90;100]\}$.

Сформуємо узагальнену таблицю оцінок (табл. 2.15) і базову матрицю частот.

Таблиця 2.15.

Узагальнена таблиця оцінок експертом значень параметра P_{13}

LE13	**N13**				
	[0;10[	[10;35[	[35;65[	[65;90[	[90;100[
Дуже мала	7	4	1	0	0
Мала	3	8	2	0	0
Середня	0	5	9	2	0
Велика	0	0	1	7	3
Дуже велика	0	0	0	4	11

Сформована на основі даних таблиці базова матриця матиме такий вигляд.

$$F_D = \begin{vmatrix} 7 & 4 & 1 & 0 & 0 \\ 3 & 8 & 2 & 0 & 0 \\ 0 & 5 & 9 & 2 & 0 \\ 0 & 0 & 1 & 7 & 3 \\ 0 & 0 & 0 & 4 & 11 \end{vmatrix}.$$

Згідно (2.7) $VS_D = \|10 \quad 17 \quad 13 \quad 13 \quad 14\|$ і $vsm_D = 17$. Обрахуємо похідну матрицю частот, використавши вираз (2.6):

$$F_D^{'} = \begin{vmatrix} 11,9 & 4 & 1,31 & 0 & 0 \\ 5,1 & 8 & 2,62 & 0 & 0 \\ 0 & 5 & 11,77 & 2,62 & 0 \\ 0 & 0 & 1,31 & 9,15 & 3,64 \\ 0 & 0 & 0 & 5,23 & 13,36 \end{vmatrix}.$$

та вектор максимумів $FM_D = \|11,9 \quad 8 \quad 11,77 \quad 9,15 \quad 13,36\|$.

Використавши формулу (2.8) обрахуємо матрицю належностей та суппорти НЧ еталону для параметра P_{13}

$$M_D = \begin{vmatrix} 1 & 0,5 & 0,11 & 0 & 0 \\ 0,43 & 1 & 0,22 & 0 & 0 \\ 0 & 0,63 & 1 & 0,29 & 0 \\ 0 & 0 & 0,11 & 1 & 0,27 \\ 0 & 0 & 0 & 0,57 & 1 \end{vmatrix}.$$

Супорти: $x_{1311} = x_{1321} = x_{1331} = x_{1341} = x_{1351} = 10/100 = 0,1$, $x_{1312} = x_{1322} = x_{1332} = x_{1342} = x_{1352} = 35/100 = 0,35$, $x_{1313} = x_{1323} = x_{1333} = x_{1343} = x_{1353} = 65/100 = 0,65$, $x_{1314} = x_{1324} = x_{1334} = x_{1344} = x_{1354} = 90/100 = 0,9$, $x_{1315} = x_{1325} = x_{1335} = x_{1345} = x_{1355} = 100/100 = 1$. Здійснивши перетворення отримаємо набір еталонів параметра $P_{13} = D$ $\underset{\sim}{T}_D^e = \{\bigcup_{s=1}^{5} \underset{\sim}{T}_{Ds}^e\} = \{$*дуже мала*$(ДМ)$, *мала*$(M)$, *середня*$(C)$, *велика*$(B)$, *дуже велика*$(ДВ)\}$ і терми ЛЗ для цього параметра:

$$\underset{\sim}{ДМ} = \underset{\sim}{T}_{D1}^e = \{0/0,1; \quad 1/0,1; \quad 0,5/0,35; \quad 0,11/0,65; \quad 0/0,9\},$$

$$\underset{\sim}{M} = \underset{\sim}{T}_{D2}^e = \{0/0,1; \quad 0,43/0,1; \quad 1/0,35; \quad 0,22/0,65; \quad 0/0,9\},$$

$$\underset{\sim}{C} = \underset{\sim}{T}_{D3}^e = \{0/0,1; \quad 0,63/0,35; \quad 1/0,65; \quad 0,29/0,9; \quad 0/1\},$$

$$\underset{\sim}{B} = \underset{\sim}{T}_{D4}^e = \{0/0,35; \quad 0,11/0,65; \quad 1/0,9; \quad 0,27/1; \quad 0/1\},$$

$$\underset{\sim}{ДВ} = \underset{\sim}{T}_{D5}^e = \{0/0,65; \quad 0,57/0,9; \quad 1/1; \quad 0/1\}.$$

Графік ФН термів ЛЗ Концентрація пилу в серверній показаний на рис. 2.14.

Таким чином з використанням МЛТС та МФЛЕ були введені ЛЗ та побудовані моделі еталонів параметрів $P_1 = T\log$, $P_2 = N\log$, $P_3 = CPU$, $P_4 = MU$, $P_5 = NEr$, $P_6 = RT\,\mathrm{Pr}$, $P_7 = CNCh$, $P_8 = NCC$, $P_9 = DbR$, $P_{10} = STF$, $P_{11} = T$, $P_{12} = H$, $P_{13} = D$. Також для кожної ЛЗ були розраховані ФН та побудовані графіки їх термів. Сформовані ета-

лони необхідні для формування логічних правил. Модель еталонів ЛЗ розширена та оптимізовано їх застосування за рахунок формалізації процесу побудови еталонів, введення специфічних параметрів для прогнозування ІКПС, що дозволить розробити ПВІІПКС і СВОКС в цілому. В подальшому необхідно передбачити можливість переведення в режим підвищеної точності в разі високої критичності функціонування ІС та вимог щодо захищеності інформаційних ресурсів через формування моделей еталонів з використання 5-ти значень ЛЗ, а не 3-х, як розраховано в даному дослідженні для більшості параметрів.

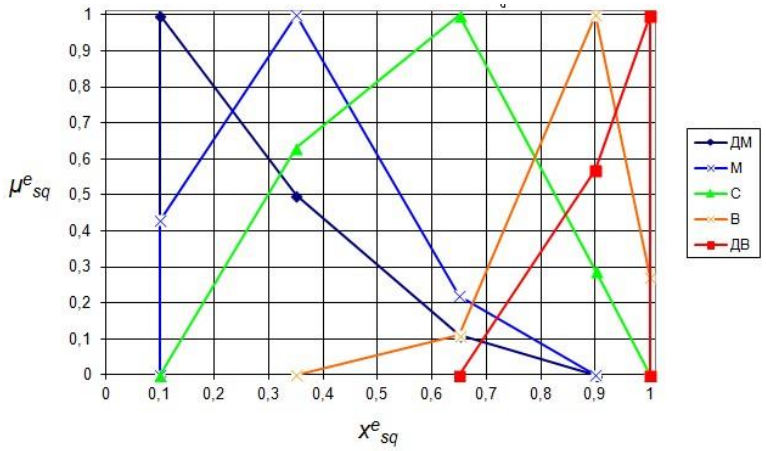


Рис. 2.14. ФН лінгвістичних термів еталонів нечітких чисел для D

Існуючі захисні системи евристичного принципу в основному орієнтовані на використання складних математичних моделей, що вимагають великих часових затрат на формування статистичних даних. Проте, як показано в [46], експертні підходи не мають такої вимоги, що значно спрощує використання даного метода в області побудови СВІПКС. Застосування даних моделей при побудові систем евристичного типу пов'язане з необхідністю формування правил направлених на виявлення ІПКС та їх ідентифікацію. Для вирішення поставленої задачі необхідно побудувати набори евристичних правил, що представляють собою деякі твердження, які засновані на результаті узагальнення певних теоретичних і експериментальних знань і відображають інтуїтивні судження експертів для забезпечення пошуку раціонального смислового рішення слабоформалізованих задач.

Побудову евристичних правил можна здійснити за допомогою відповідної моделі [13,43], для створення якої введемо множину лінгвістичних ідентифікаторів

ймовірності реалізації ІПКС $\mathbf{LI} = \bigcup_{d=1}^{D} LI_d = \{LI_1, LI_2, ..., LI_d, ..., LI_D\}$, де d – кількість елементів множини, необхідних для відображення судження (рішення, твердження) експерта, а LI_d $(d = \overline{1,D})$ - елементи LI, кожен з яких приймає одне з текстових значень, що характеризують в лінгвістичній формі це судження. Наприклад, при $d=5$

$\mathrm{LI} = \bigcup_{d=1}^{5} LI_d = \{LI_1, ..., LI_5\} = \{$*низька, середня, підвищена, висока, критична*$\}$.

Далі на основі множин ідентифікаторів **LI** і набору логіко-лінгвістичних зв'язок **LC** побудуємо множину евристичних правил $\mathbf{ER} = \{\bigcup_{i=1}^{n} ER_i\} = \{ER_1, ER_2, ..., ER_n\}$, де ER_i $(i = \overline{1,n})$ – підмножина можливих правил для виявлення i-го ІПКС, при цьому $\bigcup_{i=1}^{n} ER_i = \bigcup_{i=1}^{n} \bigcup_{p=1}^{R_i} ER_{ip} = \{ER_{11}, ..., ER_{1R_1}\}, ..., \{ER_{n1}, ..., ER_{nR_n}\}$ де ER_{ip} $(i = \overline{1,n}, p = \overline{1,R_i})$ – p-е правило i-ої підмножини можливих правил, а R_i – загальна кількість можливих правил, спрямованих на виявлення i-о ІПКС.

Поточні значення j-тих параметрів з кожного набору $\mathbf{PP_i}$ (аналогічні з підмножинами $\mathbf{P_i}$ за складом) характеризують ситуацію контрольованого середовища в певний момент часу і формують ідентифікатор поточного стану LC через їх співвідношення з еталонними значеннями відповідних параметрів відносно i-ого ІПКС [32].

$$LC_i = \{\bigwedge_{j=1}^{k_i} t_j\} = \{\bigwedge_{j=1}^{k_i} (P_{ij} \cong \bigvee_{s=1}^{r_{ij}} T_{ijs}^{e})\} \qquad (2.10)$$

де k_i – кількість параметрів, що ідентифікують i-ий інцидент, а r – кількість термів у відповідних еталонах. Для кожного ІПКС і кожного правила формується унікальний ідентифікатор стану LC. Зазначимо, що кожному ER_{ip} відповідає евристичний вираз (правило), тобто:

$$\mathbf{ER_i} = \{\bigcup_{i=1}^{n}\{\bigcup_{p=1}^{R_i} ER_{ip}\}\} = \{\bigcup_{i=1}^{n}\{\bigcup_{p=1}^{R_i} LC_{ip} \to LI_{ip}\}\} = \{\bigcup_{i=1}^{n}\{\bigcup_{p=1}^{R_i} ER_{ip} = (LC_{ip} \to LI_{ip})\}\}, \qquad (2.11)$$

де ER_{ip} є p-е правило виявлення аномалії породженої i-ою атакою, яке буквально інтерпретується як: «Якщо LC_{ip} істинно, то можливість настання ІПКС (або імовірність що поточна ситуація є ІПКС), буде LI_{ip}».

Побудова правил зазвичай здійснюється на основі експертного підходу, особливо це важливо в тих випадках, коли необхідно дати перевагу одній з альтернатив, наприклад, при якому LC_{ip} результат, пов'язаний з LI_{ip} буде найбільш об'єктивно відображати стан системи. Для вибору одного рішення з множини альтернативних скористаємося методами визначення коефіцієнтів важливості (КВ) [22,43]. Скористаємося методом рангових перетворень (РП), оскільки він дозволяє залучити кількох експертів, в якості вхідних даних застосовуються табличні форми, вихідна функція лінійна, а трудомісткість низька (див. в роботі [22]).

Згідно цього методу, як приклад, скористаємося судженнями 4-х експертів щодо $D=5$ можливих результатів першого правила ідентифікації VA ER^d_{41} $(d=\overline{1,D})$:

$$\bigcup_{d=1}^{5} ER^d_{41} = \{ER^1_{41}, ER^2_{41}, ER^3_{41}, ER^4_{41}, ER^5_{41}\} = \{(P_{VACPU} \cong H, P_{VACNCh} \cong H, P_{VASTF} \cong M, P_{VAMU} \cong H, P_{VANEr} \cong M) \rightarrow$$
$$H,\ (P_{VACPU} \cong H, P_{VACNCh} \cong H, P_{VASTF} \cong M, P_{VAMU} \cong H, P_{VANEr} \cong M) \rightarrow БНВ, (P_{VACPU} \cong H, P_{VACNCh} \cong H,$$
$$P_{VASTF} \cong M, P_{VAMU} \cong H, P_{VANEr} \cong M) \rightarrow БВН, (P_{VACPU} \cong H, P_{VACNCh} \cong H, P_{VASTF} \cong M, P_{VAMU} \cong H, P_{VANEr} \cong M) \rightarrow$$
$$В, (P_{VACPU} \cong H, P_{VACNCh} \cong H, P_{VASTF} \cong M, P_{VAMU} \cong H, P_{VANEr} \cong M) \rightarrow К\}.$$

Далі на основі РП визначимо КВ, які відображаються параметром λ. Його мінімальне значення свідчить про більшу перевагу альтернативи, тобто її КВ більш високий. Для правила ER_{11} зробимо розрахунки значень x^d_{41} і λ^d_{41} по кожному з можливих результатів ER^d_{41} $(d=\overline{1,5})$: x^1_{41}=(1+3+1+2)/4=1,75; x^2_{41}=(2+1+3+ +2)/4=2; x^3_{41}=(3+2+2+2)/4=2,25; x^4_{41}=(2+4+3+ +3)/4=3; x^5_{41}=(4+4+3+4)/4=3,75. Значення КВ визначається як $\lambda^d_{41} = x^d_{41} / N$, де N – сума всіх рангів (N=10). За результатами, занесеним в табл. 2.16 видно, що кращий результат має ER^1_{41}, оскільки $\bigwedge_{d=1}^{5} \lambda^d_{41} = \lambda^d_{41} = 0{,}18$. Аналогічно здійснюється визначення найбільш відповідних альтернатив для всіх наступних правил. Отримані дані можна використовувати в якості конкретних значень при побудові реальних правил у практичних СВІПКС, СВІП, IDS/IPS тощо.

Застосуємо апарат логіко-лінгвістичних зв'язок «ІПКС-параметр» і взаємозалежність між показниками параметрів, що контролюються системою, та можливістю реалізації ІПКС, сформуємо евристичні правила для їх виявлення та ідентифікації [20]. Евристичні правила дають змогу оцінити можливість (степінь) реалізації

тої чи іншої атаки в залежності від набору значень параметрів в певний момент часу. Як було описано ІПКС «Злом ІС» пов'язаний з такими параметрами як $IKS_1 = ZL \to P_1 = \{T\log, N\log, CPU, MU, NEr, RTPr\}$, а LI_d може мати значення: «низька» (Н), «середня» (С), «підвищена» (П), «висока» (В), «критична» (К). Сформуємо множину евристичних правил ER_1 для виявлення та ідентифікації «Злому ІС» і представимо його в вигляді таблиці 2.17, позначивши значення параметрів Н – низький, С – середній, В – високий (великий), М – малий. Враховуючи всі можливі комбінації станів контрольованих параметрів можна сформувати 729 відповідних ЕП $ER_{1j}, j = \overline{1,729}$. Наведемо деякі з них.

Таблиця 2.16

Ранги ER^k_{1j} і їх коефіцієнти важливості

$ER^d{}_{41}$	d	Експерти				$x^d{}_{41}$	$\lambda^d{}_{41}$
		1	2	3	4		
$ER^1{}_{41}$	1	1	3	1	2	1,75	0,18
$ER^2{}_{41}$	2	2	1	3	2	2	0,2
$ER^3{}_{41}$	3	3	2	2	2	2,25	0,23
$ER^4{}_{41}$	4	2	4	3	3	3	0,3
$ER^5{}_{41}$	5	4	4	3	4	3,75	0,38

Таблиця 2.17

Множина правил ER_1 для виявлення злому ІС

p	P_{Tlog}	P_{Nlog}	P_{CPU}	P_{MU}	P_{NEr}	P_{RTPr}	Результат
1	Л	Н	Н	Н	М	М	С
2	Л	Н	Н	Н	М	С	Н
3	Л	Н	Н	Н	М	В	Н
4	Л	Н	Н	Н	С	М	С
5	Л	Н	Н	Н	С	С	С
.....							
390	П	С	В	С	М	В	П
391	П	С	В	С	С	М	В
392	П	С	В	С	С	С	П
393	П	С	В	С	С	В	П
.....							
725	Н	В	В	В	С	С	В
726	Н	В	В	В	С	В	В
727	Н	В	В	В	В	М	К
728	Н	В	В	В	В	С	К
729	Н	В	В	В	В	В	В

Аналогічно ІПКС «Спам» пов'язаний з такими параметрами як $IKS_2 = SP \to P_2 = \{CPU, MU, NEr, RTPr, CNCh\}$, а LI_d може мати значення: «низька» (Н), «середня» (С), «підвищена» (П), «висока» (В), «критична» (К). Сформуємо мно-

жину евристичних правил ER_2 для виявлення та ідентифікації даного ІПКС і представимо його фрагмент в вигляді таблиці 2.18 (повний набір наведений в додатках), позначивши значення параметрів Н – низький, С – середній, В – високий (великий), М – малий. Враховуючи всі можливі комбінації станів контрольованих параметрів можна сформувати 243 відповідних ЕП $ER_{2j}, j=\overline{1,243}$.

Таблиця 2.18

Множина правил ER_2 для виявлення спаму

p	P_{CPU}	P_{MU}	P_{NEr}	P_{RTPr}	P_{CNCh}	Результат
1	Н	Н	М	М	Н	С
2	Н	Н	М	М	С	С
3	Н	Н	М	М	В	П
…….						
241	В	В	В	В	Н	П
242	В	В	В	В	С	В
243	В	В	В	В	В	В

Ідентифікуючими параметрами для ІПКС «Відмова в обслуговувані» формують зв'язку $IKS_3 = DD \rightarrow P_3 = \{CPU, MU, NEr, CNCh, NCC, DbR\}$, а LI_d може мати значення: «низька» (Н), «середня» (С), «підвищена» (П), «висока» (В), «критична» (К). Сформуємо набір евристичних правил ER_3 для виявлення та ідентифікації «DDOS» і представимо фрагмент набору в вигляді таблиці 2.19, позначивши значення параметрів Н – низький, С – середній, В – високий (великий), М – малий. Враховуючи всі можливі комбінації станів контрольованих параметрів можна сформувати 729 відповідних ЕП $ER_{3j}, j=\overline{1,729}$.

Таблиця 2.19

Множина правил ER_3 для виявлення атаки типу відмова в обслуговувані

p	P_{CPU}	P_{MU}	P_{NEr}	P_{CNCh}	P_{NCC}	P_{DbR}	Результат
1	Н	Н	М	Н	М	М	С
2	Н	Н	М	Н	М	С	Н
3	Н	Н	М	Н	М	В	Н
…….							
727	В	В	В	В	В	М	К
728	В	В	В	В	В	С	К
729	В	В	В	В	В	В	В

Як було описано ІПКС «Вірусна атака» пов'язаний з такими параметрами як $IKS_4 = VA \rightarrow P_4 = \{CPU, MU, NEr, CNCh, STF\}$, а LI_d може мати значення: «низька» (Н), «середня» (С), «підвищена» (П), «висока» (В), «критична» (К). Сформуємо множину евристичних правил ER_4 для його виявлення та ідентифікації і представимо в

вигляді таблиці 2.20 фрагмент набору, позначивши значення параметрів Н – низький, С – середній, В – високий (великий), М – малий. Враховуючи всі можливі комбінації станів контрольованих параметрів можна сформувати 729 відповідних ЕП $ER_{4j}, j=\overline{1,243}$.

Таблиця 2.20

Множина правил ER_4 для виявлення вірусної атаки

p	P_{CPU}	P_{MU}	P_{NEr}	P_{CNCh}	P_{STF}	Результат
1	Н	Н	М	Н	М	Н
2	Н	Н	М	Н	С	Н
3	Н	Н	М	Н	В	С
…….						
241	В	В	В	В	М	В
242	В	В	В	В	С	К
243	В	В	В	В	В	К

Дещо відрізняються правила для виявлення та ідентифікації «Збоїв внаслідок мікрокліматичних умов в серверній», для якого справедлива залежність «ІПКС-параметр» $IKS_5 = ZK \rightarrow P_5 = \{T,H,D\}$. Введемо наступні LI_d: «низька» (Н), «середня» (С), «підвищена» (П), «висока» (В), «критична» (К). Сформуємо набір евристичних правил ER_5 для виявлення та ідентифікації даного ІПКС і представимо його в вигляді таблиці 2.21, позначивши значення параметрів ДН – дуже низький, Н – низький, С – середній, В – високий (великий), ДВ – дуже високий (великий), ДМ – дуже малий, М – малий. Враховуючи всі можливі комбінації станів контрольованих параметрів можна сформувати 729 відповідних ЕП $ER_{5j}, j=\overline{1,125}$.

Таблиця 2.21

Множина правил ER_5 для виявлення збоїв внаслідок мікрокліматичних умов в серверній

p	P_T	P_H	P_D	Результат
1	ДМ	ДН	ДМ	П
2	ДМ	ДН	М	В
3	ДМ	ДН	С	В
4	ДМ	ДН	В	В
5	ДМ	ДН	ДВ	К
…….				
80	В	ДН	ДВ	В
81	В	Н	ДМ	С
…….				
124	ДВ	ДВ	В	В
125	ДВ	ДВ	ДВ	К

Слід зазначити, що можливі випадки коли одну і ту ж ситуацію погоджують декілька евристичних правил з різних груп. В такому випадку виникає колізія. Тому необхідно ввести систему пріоритетів. Так пріоритетним є правило з більшим ступенем критичності, а в випадку рівності ступеню – з більшим числом параметрів.

Запропонована в роботі модель евристичних правил з застосуванням нечіткої логіки дозволяє за рахунок використання множини «ІПКС-параметр», та «ІПКС-ідентифікатор поточного стану», а також універсальної моделі еталонів параметрів відобразити наявність ІПКС чи передумов до їх появи. На основі цієї моделі були розроблені приклади правил для виявлення і ідентифікації злому ІС, DDOS-атаки, спам-атаки, вірусної атаки та збої через вплив мікрокліматичних умов серверної, які можуть бути використані для удосконалення існуючих чи розробки нового комплексу СВОКС в цілому або окремо СВІПКС.

2.3. Базові параметри та підходи до оцінки кризових ситуацій

Захист ІР від впливу 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 ІР. Так, чисельні інциденти за умови відсутності контролю за їх протіканням та відповідної реакції можуть мати критичні наслідки. Відповідно до визначення КС, наведеного в [19], вона характеризується великими збитками, серйозними переривання 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 ІР (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 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 [19,91], описані та розроблені методи та системи для прогнозування, ідентифікації аномального стану в ІС [43,60], діяльності порушників [5,13,16,50,53], комп'ютерних атак [65]. Питанням ідентифікації, прогнозування та моделювання надзвичайних ситуацій екологічної, суспільної, державної безпеки присвячена праця [34], 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 [35] 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 [30,56,57]. 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 невизначе-

ності впливу дестабілізуючих чинників, описані методи оцінки виконання функцій безпеки, оцінки ризику та прийняття рішення в умовах КС [27], 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 [58]. 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 розробка параметрів 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 може 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. Оцінити вплив КС можна використовуючи параметри оцінки рівня критичності поточної ситуації L_e. 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 [91]. Слід відмітити, що при роботі з конкретними типами КС повинна зберігатись можливість поповнення цієї множини додатковими параметрами. Сформуємо множину параметрів $\mathrm{L} = \{\bigcup_{e=1}^{E} L_e\}$ 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 тривалістю 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 [6], 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 2.22 [80].

Дану класифікацію можна застосувати як для окремих ІС, 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 степінь 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 [35,91]. При цьому чим вище ранг інциденту, тим вища оцінка експерта в балах.

Таблиця 2.22

Класифікація БП та ІТ-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

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: інциден-

ти 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 [35,91]. 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 [91]. 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 [35,85]. 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 (х, у) на території об'єкта і поблизу нього рекомендується визначати за формулою [56,57] $R_{пот}(x,y) = \sum_{i=1}^{J} Q_i \cdot \max_j \left(P_{гиб}{}^{ij}(x;y) \cdot \nu_{уяз}{}^{ij}(x;y) \right)$, 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 (х,у) 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 (х;у) 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 $R_{інд}{}^{i}$, рік$^{-1}$, для *i*-го індивіда рекомендується визначати за формулою $R_{инд}{}^{i} = \sum_{k=1}^{G} q_{ki} \cdot R_{пот}(x,y)$, де q_{ki} – ймовірність присутності в *k*-ій 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 розглянутого людини в певній галузі території [57].

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 оцін-

ка КС виходячи з кількості загиблих чи постраждалих. Оскільки під час КС можуть бути як загиблі так і поранені, то в [91] 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) [35,85]. Чим вищою є загрозу життю і здоров'ю людини, тим вища експертна оцінка.

Параметр L_8 – Питомий показник смертності на поточний момент, RM. По своїй суті 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 вибухів 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 [57].

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. Слід зазначити, що 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 віз 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 властивість 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 [5]. 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) [46], 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 $L = \left\{ \bigcup_{e=1}^{E} L_e \right\} = \{L_1, ..., L_E\}, e = \overline{1, E}$, де E – кількість параметрів. Наприклад, за умов дослідження при E=15, $L = \{\bigcup_{e=1}^{15} L_e\} = \{L_1, ..., L_{15}\} = \{TR,$ $DVF, GS, OS, OLED, RD, RTLH, RM, F, DDI, CRT, CRP, LM, DIEPF, DVChS\}$.

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

$$\mathbf{T_L} = \{\bigcup_{e=1}^{E}\{\bigcup_{s=1}^{r_e}\underset{\sim}{T}_{L_e s}\}\} = \{\{\underset{\sim}{T}_{L_1 1},...,\underset{\sim}{T}_{L_1 r_1}\}, ..., \{\underset{\sim}{T}_{L_E 1},...,\underset{\sim}{T}_{L_E r_E}\}\},$$

$$\mathbf{T_{LCS}} = \{\bigcup_{s=1}^{r_{LCS}}\underset{\sim}{T}_{LCS}\} = \{\underset{\sim}{T}_{LCS1},..., \underset{\sim}{T}_{LCS_{r_{LCS}}}\}, \; s = \overline{1,r}$$

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

$$\mathbf{T_L} = \bigcup_{e=1}^{15}\{\bigcup_{s=1}^{5}\underset{\sim}{T}_{L_e s}\} = \bigcup_{e=1}^{15}\{\underset{\sim}{T}_{L_e 1},\underset{\sim}{T}_{L_e 2},\underset{\sim}{T}_{L_e 3},\underset{\sim}{T}_{L_e 4},\underset{\sim}{T}_{L_e 5}\} = \bigcup_{e=1}^{15}\{\underset{\sim}{MH}_{L_e},\underset{\sim}{HC}_{L_e},\underset{\sim}{C}_{L_e},\underset{\sim}{BC}_{L_e},\underset{\sim}{MK}_{L_e}\},$$

$$\mathbf{T_{LCP}} = \{\underset{\sim}{MH}, \underset{\sim}{HC}, \underset{\sim}{C}, \underset{\sim}{BC}, \underset{\sim}{MK}\},$$

де МН – мінімальний, НС – нижче середнього, С – середній, ВС – вище середнього, МК – максимальний.

2.4. Висновки до другого розділу

1. Побудовані інтегровані моделі представлення множини ІПКС та КС, та описані кортежі, що їх визначають. Основними елементами кортежів є ідентифікатор ІПКС, набори параметрів для виявлення ІПКС, набори НЧ еталонних та поточних значень контрольованих параметрів та рівень критичності ситуації, спричиненої ІПКС. Крім того проведена побудови зв'язків ІПКС→параметр. Отримані результати є базисом для побудови СВОКС.

2. Проведена формалізація методів побудови моделі еталонів параметрів та ЕП, що дає змогу застосовувати їх в умовах невизначеності і слабоформалізованого середовища для виявлення ІПКС різного роду, тобто забезпечення універсальності, та їх оцінки. На базі методу МЛТС запропонований метод формування еталонів ЛЗ параметрів $P_1 = T\log$, $P_2 = N\log$, $P_3 = CPU$, $P_4 = MU$, $P_5 = NEr$, $P_6 = RT\,\mathrm{Pr}$, $P_7 = CNCh$, $P_8 = NCC$, $P_9 = DbR$, $P_{10} = STF$, $P_{11} = T$, $P_{12} = H$, $P_{13} = D$. Також для кожної ЛЗ були розраховані ФН та побудовані графіки їх термів. Сформовані еталони необхідні для формування логічних правил, що дозволяють забезпечити функціонування СВОКС. Розроблені набори правил для виявлення ІПКС.

3. Запропонована в роботі множина критеріїв $\mathbf{L} = \{\bigcup_{e=1}^{E} L_e\} = \{T, DVF, GS, OS, OLED,$ $RTLH, F, DDI, CRT, CRP, LM, DIEPF, DVChS\}$ є універсальною і може застосовуватися

для оцінки будь-яких ІПКС (КС) незалежно від природи їх походження. На базі цієї множини введено поняття рівня критичності ситуації $L\tilde{C}S_i = \sum_{e=1}^{E}(\Omega_e * \tilde{L}_e)$, що визначається функціональними залежностями між критеріями оцінки рівня критичності. 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.

РОЗДІЛ 3. МЕТОДИ ТА СИСТЕМИ УПРАВЛІННЯ КРИЗОВИМИ СИТУАЦІЯМИ

3.1. Методи виявлення та оцінки критичності кризових ситуацій

Враховуючи стрімкий розвиток інформаційних технологій, що впливає як на захисні механізми так і на засоби для проведення інформаційних атак, набір можливих ІПКС значно збільшується. Безперервно зростає кількість загроз інформаційній безпеці, проводяться принципово нові кібератаки на інформаційні ресурси, що ускладнює реалізацію ефективного захисту. Досягнення максимального ефекту захищеності ІР можливе за умови того, що відомі можливі ІПКС, що створює передумови для підбору та застосування найбільш відповідних заходів та засобів захисту. Дана задача ускладнюється тим, що атаки на ДІР здійснюються в реальних умовах, тобто з великим показником випадковості та непередбачуваності. Таким чином ІС), в яких циркулюють ІР, є слабоформалізованим середовищем. Дану проблему може вирішити застосування методів нечіткої логіки. Тому розробка методу виявлення та оцінки критичності КС є актуальною задачею. В роботі [46] показана ефективність застосування математичного апарату нечіткої логіки для вирішення задач, пов’язаних з забезпеченням інформаційної безпеки.

Запропонований метод розв’язує задачу виявлення ІПКС. В методі використовуються елементи нечіткої логіки для попереднього прийняття рішення щодо факту наявності ІПКС, оцінки параметрів критичності та визначення загального рівня критичності. Метод вміщує в собі два методи: 1) метод виявлення ІПКС та 2) метод оцінки рівня критичності КС, що можуть використовуватися як разом так і поодинці.

Розглянемо запропонований метод детально. Схематичне зображення запропонованого методу наведене на рисунку 3.1.

В методі використовуються такі методи нечіткої логіки як метод лінгвістичних термів з використанням статистичних даних (МЛТС) – для побудови еталонних значень параметрів та оціночних еталонів, лінійної

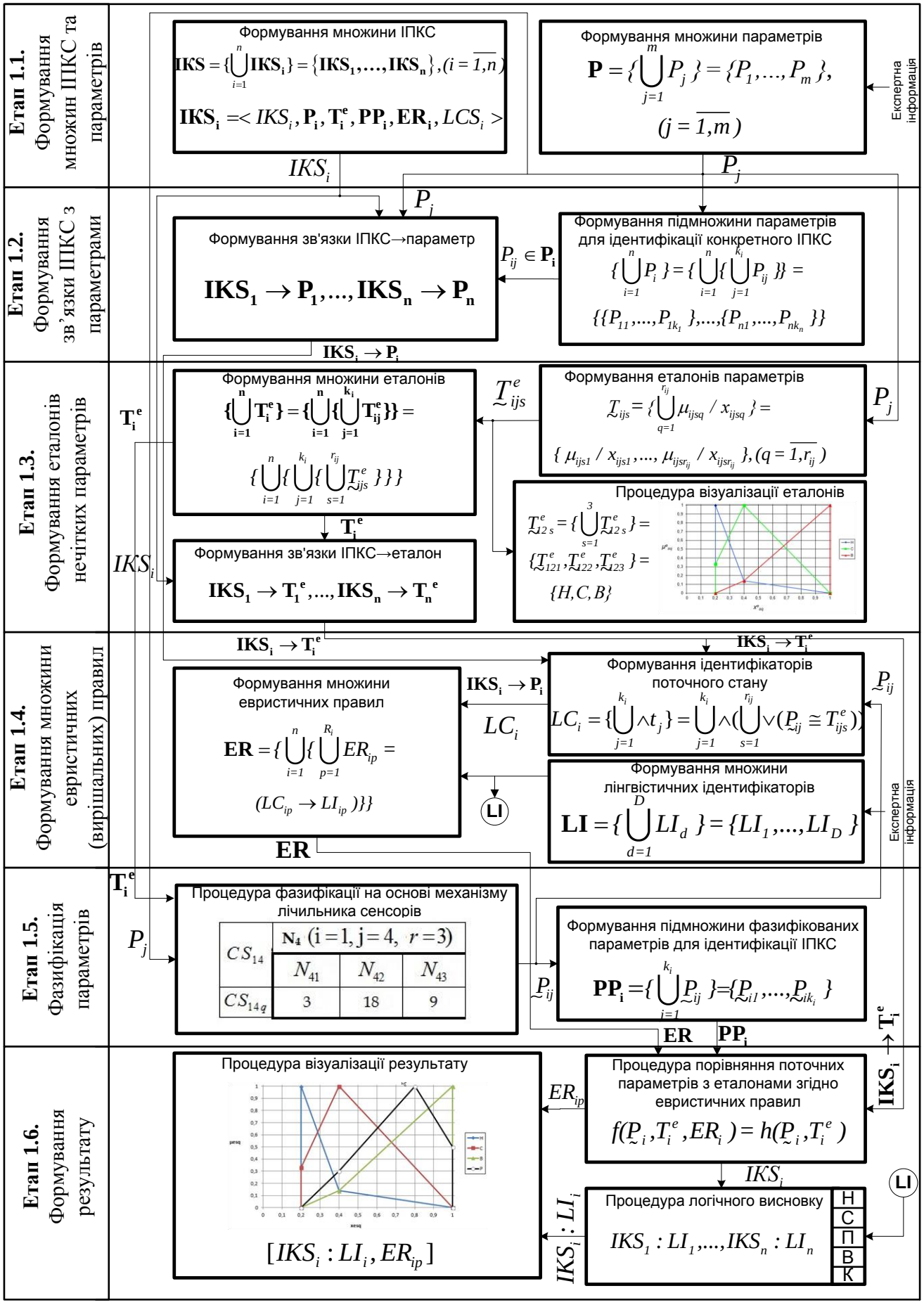


Рисунок 3.1. Схема відображення методу виявлення ІПКС

апроксимації по локальним максимумам (ЛАЛМ), відстань Хемінга (ВХ) і α-рівнева відстань (АРВ) – для обробки нечітких даних та проведення операцій нечіткої логіки Крім того використовується також експертні методи оцінювання та ранжування: метод середніх рангів (СР) та парного порівняння з визначенням квадратного кореня (ППВКК).

В першому методі реалізовані етапи 1.1-1.6.

Етап 1.1 – формування множин ІПКС та ідентифікуючих параметрів. Етап орієнтований на визначення множин ІПКС та параметрів їх ідентифікації. На основі аналізу середовища ІС формуються ідентифікатор ІПКС з множини $\mathbf{IKS} = \{\bigcup_{i=1}^{n} \mathbf{IKS}_i\}$, $(i = \overline{1,n})$, де n – загальна кількість ІПКС, а також множини контрольованих нечітких параметрів $\mathbf{P} = \{\bigcup_{j=1}^{m} P_j\}$, $(j = \overline{1,m})$ [32] і з певною, заздалегідь встановленою, періодичністю їх поточні значення заносяться в регістри системи виявлення ІПКС. Відповідно фіксуються IKS_i та P_j [32,48], які дозволяють виявити ознаки ІПКС на основі значень параметрів. Наприклад, при $n = 5$ та $m = 13$ система здатна виявити такі потенційні КС з ідентифікаторами $IKS_1 = ZL$, $IKS_2 = SP$, $IKS_3 = DD$, $IKS_4 = VA$, $IKS_5 = ZK$ з іменами «Злом ІС», «Спам», «Відмова в обслуговуванні», «Вірусна атака» та «Вихід з ладу ІС через вплив кліматичних умов» відповідно) на основі 13 нечітких параметрів P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8, P_9, P_{10}, P_{11}, P_{12}, P_{13} (де $P_1 = Tlog$, $P_2 = Nlog$, $P_3 = CPU$, $P_4 = MU$, $P_5 = NEr$, $P_6 = RTPr$, $P_7 = CNCh$, $P_8 = NCC$, $P_9 = DbR$, $P_{10} = STF$, $P_{11} = T$, $P_{12} = H$, $P_{13} = D$ – відповідно ідентифікатори таких параметрів як «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», «Концентрація пилу в серверній кімнаті») [65].

Етап 1.2 – формування зв'язки ІПКС з параметрами. На цьому етапі формуються зв'язки конкретного типу ІПКС з параметрами, що необхідні для його виявлення. Вхідними даними на даному етапі є ідентифікатори інцидентів і нечіткі параметри, занесені в регістри системи виявлення ІПКС на попередньому етапі. Формується n підмножин параметрів $\mathbf{P_i} \subseteq \mathbf{P}$, кожна з яких містить k_i елементів , а на їх основі створюються зв'язки «ІПКС» → «ідентифікуючий параметр», $\mathbf{IKS_i} \to \mathbf{P_i}$. Наприклад, при $n=5$ та $k_1 = k_3 = 6$, $k_2 = k_4 = 5$, $k_5 = 3$ будуть сформовані такі зв'язки: $IKS_1 = ZL \to \{Tlog, Nlog, CPU, MU, NEr, RTPr\}$, $IKS_2 = SP \to \{CPU, MU, NEr, RTPr, CNCh\}$, $IKS_3 = DD \to \{CPU, MU, NEr, CNCh, NCC, DbR\}$, $IKS_4 = VA \to \{CPU, MU, NEr, CNCh, STF\}$, $IKS_5 = ZK \to \{T, H, D\}$.

Етап 1.3 – формування еталонів нечітких параметрів. Цей етап направлений на отримання еталонних величин, необхідних для виміру поточних значень контрольованих параметрів. Еталони кожного параметру визначають множиною еталонів $\{\bigcup_{i=1}^{n} \mathbf{T_i^e}\} = \{\underset{\sim}{T}_1^e, \ldots, \underset{\sim}{T}_n^e\}$, $(i = \overline{1,n})$ необхідних для виявлення конкретного ІПКС з загальної множини еталонів $\mathbf{T^e}$, $\mathbf{T_i^e} \subseteq \mathbf{T^e}$. На основі вхідних даних, отриманих на етапі 1 та статистичних даних шляхом використання експертних методів формуємо відповідні значення еталонів лінгвістичних змінних для всіх $\underset{\sim}{T}_{ij}^e = \bigcup_{s=1}^{r_{ij}} \underset{\sim}{T}_{ijs}^e$ з використанням вибраного методу формування функцій приналежності, наприклад, $\mathbf{T_i^e} = \{\underset{\sim}{T}_{ZLTlog}^e, \ldots, \underset{\sim}{T}_{ZLRTPr}^e\}$. Так, для CPU [32,65] отримаємо еталоні значення $\underset{\sim}{T}_{CPU}^e = \bigcup_{s=1}^{3} \underset{\sim}{T}_{CPUs}^e$, які можна представити у вигляді лінгвістичних термів – $\{\underset{\sim}{T}_{CPU1}^e, \underset{\sim}{T}_{CPU2}^e, \underset{\sim}{T}_{CPU3}^e\} = \{\underset{\sim}{H}^e, \underset{\sim}{C}^e, \underset{\sim}{B}^e\}$ за допомогою процедури візуалізації. Процедура формування еталонів здійснюється за допомогою МЛТС, формалізованого за аналогією з [41] відповідно до виразів (2.6-2.9). Крім того, аналогічно до етапу 2 створюються зв'язки «ІПКС» → «еталон ідентифікуючого параметра», $\mathbf{IKS_i} \to \mathbf{T_i^e}$.

Етап 1.4 – формування множини евристичних (вирішальних) правил (ЕП). Створення наборів ЕП, що використовуються для виявлення ІПКС на основі

зіставлення еталонних $\underset{\sim}{T}^{e}_{ijs}$ та поточних значень параметрів з множини $\mathbf{PP_i}$ $(i=\overline{1,n})$ за допомогою набору ідентифікаторів поточного стану LC, що є унікальним для кожного ІПКС. На основі цього формується набір правил $\mathbf{ER}=\{\bigcup_{i=1}^{n} ER_i\}$, що містить правила для виявлення та ідентифікації всіх ІПКС. Для формування правил використовуються лінгвістичні ідентифікатори ймовірності реалізації ІПКС LI_i, необхідні для відображення судження експерта в лінгвістичній формі. Формується множина альтернатив ER^{d}_{ip} $(i=\overline{1,n};\ d=\overline{1,D};\ p=\overline{1,R_n}$, де n – кількість категорій ІПКС, R_n – кількість правил для виявлення *i*-ї категорії порушника, а D – кількість альтернативних варіантів для формування одного правила). Наприклад, для першої категорії порушника і першого правила отримаємо $\mathbf{ER_{11}}=\{\bigcup_{d=1}^{D} ER^{d}_{11}\}=\{ER^{1}_{11}$, ..., $ER^{D}_{11}\}$. Формування правил здійснюється на основі множини альтернатив за допомогою процедури їх вибору, яка базується на методі СР. Так, 1-е правило для виявлення $\mathbf{IKS_4 = VA}$ (вірусна атака) матиме вигляд: $ER_{41}=\{(\underset{\sim}{P}_{CPU}\cong\underset{\sim}{H},\ \underset{\sim}{P}_{CNCh}\cong\underset{\sim}{H},\ \underset{\sim}{P}_{STF}\cong\underset{\sim}{M},\ \underset{\sim}{P}_{MU}\cong\underset{\sim}{H},\ \underset{\sim}{P}_{NEr}\cong\underset{\sim}{M})\rightarrow H\}$ Детально процедура формування правил та приклади наборів наведені в роботі [20].

Етап 1.5 – фазифікація параметрів, що моніторяться з метою виявлення ІПКС. На даному етапі відбувається перетворення множини поточних значень параметрів, що фіксуються кожні t проміжки часу протягом певного періоду часу T в одне нечітке число і таким чином отримаємо нечіткі числа, характеризуючі поточні значення ідентифікуючих параметрів (за виразом). З врахування процедури формування зв'язок $\mathbf{IKS_i}\rightarrow\mathbf{P_i}$ для окремого ІПКС надалі застосовується відповідні йому параметри з підмножин $\mathbf{PP_i}$, де $\mathbf{PP_i}\subseteq\mathbf{PP}$ – множина всіх фазифікованих параметрів. Фазифікація здійснюється на основі механізму лічильника сенсорів [40], при чому вхідними параметрами є їх показники і нечіткі еталони лінгвістичних змінних. Сформовані нечіткі значення параметрів групуються в підмножини з k_i елементів, тобто $\mathbf{PP_i}=\{\bigcup_{j=1}^{k_i}\underset{\sim}{P}_{ij}\}=$, $(i=\overline{1,n})$для кожного типу ІПКС.

Етап 1.6 – обробка поточних значень ідентифікуючих параметрів і формування результату. Етап спрямований на прийняття рішення щодо наявності ІПКС, що можуть загрожувати інформаційній безпеці. Сформовані на попередньому етапі нечіткі числа, які відображають поточні значення контрольованих параметрів, групуються відповідно до ІПКС, а функції належності їх елементів порівнюються з еталонними значеннями за допомогою визначення УВХ. На основі цього виконується зіставлення ідентифікатора поточної ситуації з ЕП з заданого набору. Погодження певним правилом ідентифікатора ситуації дає змогу зробити висновок щодо наявності передумов реалізації ІПКС і поточній ситуації присвоюється відповідний правилу лінгвістичний ідентифікатор можливості реалізації ІПКС $IKS_i : LI_i$. Тобто фіксується факт появи ІПКС (його виявлення). Отриманий результат може відображатися в лінгвістичній формі, у вигляді нечіткого числа або лінгвістичної змінної з зазначенням правила, яке ідентифікувало (погодило) поточну ситуацію. Наприклад, при $i = 4$ та якщо на етапі 5 були виміряні такі значення контрольованих параметрів, з яких сформовано ідентифікатор поточної ситуації у вигляді $LC_4 = (\underset{\sim}{P}_{CPU} \cong \underset{\sim}{B},\ \underset{\sim}{P}_{CNCh} \cong \underset{\sim}{B},\ \underset{\sim}{P}_{STF} \cong \underset{\sim}{B},\ \underset{\sim}{P}_{MU} \cong \underset{\sim}{B},\ \underset{\sim}{P}_{NEr} \cong \underset{\sim}{B})$, то дана ситуація буде ідентифікована правилом ER_{4243} з набору $\mathbf{ER_4}$. Лінгвістичний ідентифікатор можливості реалізації ІПКС. Згідно даного правила «критична» Таким чином на виході методу отримаємо фіксацію факту виявлення ІПКС «вірусна атака» з критичною можливістю реалізації. Після виявлення ІПКС його необхідно оцінити за встановленою процедурою, використовуючи метод оцінки критичності ситуації, описаного в [51].

Після виявлення ІПКС його необхідно оцінити. Опишемо метод оцінювання критичності ситуації, що є наслідком впливу певного інциденту. Він складається також з 6 етапів, схематичне зображення якого наведено на рис. 3.2.

Етап 2.1. 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

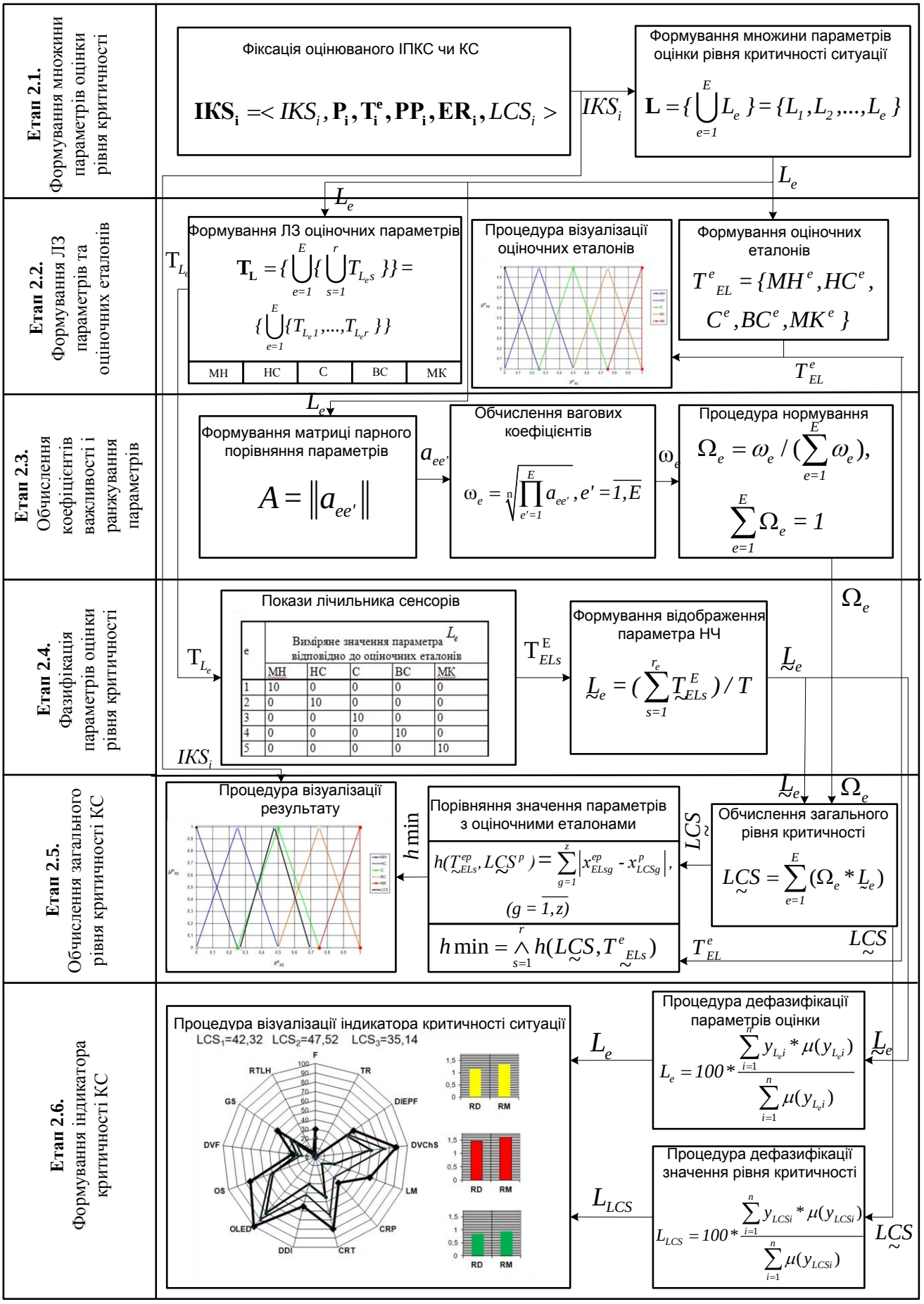


Рис. 3.2. Схема відображення методу оцінки критичності ситуації

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. Провівши аналіз сучасних методик оцінки ризику, кращих практик КУББ була сформована наступна множина: $\mathbf{L} = \{\bigcup_{e=1}^{E} L_e\} = \{L_1,...,L_E\}$, наприклад, за умов дослідження при E=15 $\mathbf{L} = \{\bigcup_{e=1}^{15} L_e\} = \{L_1,,...,L_{15}\}$ де $L_1 = TR$, $L_2 = DVF$, $L_3 = GS$, $L_4 = OS$, $L_5 = OLED$, $L_6 = RD$, $L_7 = RTLH$, $L_8 = RM$, $L_9 = F$, $L_{10} = DDI$, $L_{11} = CRT$, $L_{12} = CRP$, $L_{13} = LM$, $L_{14} = DIEPF$, $L_{15} = DVChS$ ідентифікують такі параметри як «Тривалість інциденту», «Степінь 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 ДІР з ОД» відповідно.

Етап 2.2. 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

$$\mathbf{T^e_{EL}} = \{\bigcup_{s=1}^{r} \underset{\sim}{T}^e_{ELs}\} = \{\underset{\sim}{T}^e_{EL1},...,\underset{\sim}{T}^e_{ELr}\} = \bigcup_{s=1}^{r}\{\bigcup_{q=1}^{r_s} \mu^e_{ELsq} / x^e_{ELsq}\} =$$
$$= \bigcup_{s=1}^{r}\{\mu^e_{ijs1} / x^e_{ijs1}, \mu^e_{ijs2} / x^e_{ijs2},..., \mu^e_{ijsr_s\text{-}1} / x^e_{ijsr_s\text{-}1}, \mu^e_{ijsr_s} / x^e_{ijsr_s}\} \ ,(q = \overline{1,r_s}), \quad (3.1)$$

де r_s $(s=\overline{1,r})$ – кількість компонент в $\underset{\sim}{T}^e_{ELs}$ з аналогічними термами, що і в $\underset{\sim}{T}_{L_e s}$ та $\underset{\sim}{T}_{LCSs}$. Побудуємо даний еталон використавши метод побудови параметричних НЧ, описаний в [46]. Функція, що задає значення ФН оціночних еталонів буде мати вигляд: $\mu_{\underset{\sim}{A}}(x)=\begin{cases}0, & якщо\ x<a;\\ (x-a)/(b-a), & якщо\ a\le x<b;\\ (c-x)/(c-b), & якщо\ b\le x<c;\\ 0, & якщо\ x>c.\end{cases}$. Діапазон зміни носіїв НЧ з $r=5$ термів та $r_s=5$ компонент відобразимо на універсальній множині U=[0, 1]. Отримані еталоні НЧ представлені на рис.3.3, а їх математичний опис виразом:

$$\underset{\sim}{T}^e_{EL}=\begin{Bmatrix}\underset{\sim}{МН}^e=\{0/0 \quad 1/0 \quad 0/0,25\};\\ \underset{\sim}{НС}^e=\{0/0 \quad 1/0,25 \quad 0/0,5\};\\ \underset{\sim}{С}^e=\{0/0,25 \quad 1/0,5 \quad 0/0,75\};\\ \underset{\sim}{ВС}^e=\{0/0,5 \quad 1/0,75 \quad 0/1\};\\ \underset{\sim}{МК}^e=\{0/0,75 \quad 1/1 \quad 0/1\}\end{Bmatrix}.$$

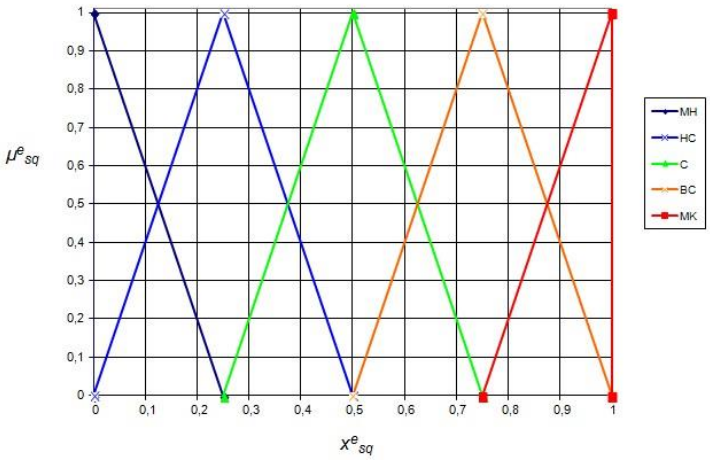


Рис. 3.3. Графічне представлення еталонних НЧ

Етап 2.3. 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 [46]. 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 су-

дження 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 2.4. 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 T поточних вимірювань, що робляться протягом певного періоду часу, формується НЧ, що відображає поточне значення параметру. Воно визначається як

$$\tilde{L}_e = (\sum_{s=1}^{r} \tilde{T}_{ELs}^{E}) / T = (\tilde{T}_{EL1}^{E} \tilde{+} \tilde{T}_{EL2}^{E} \tilde{+} \ldots \tilde{+} \tilde{T}_{ELs}^{E} \tilde{+} \ldots \tilde{+} \tilde{T}_{ELr}^{E}) / T \qquad (3.2)$$

де Т – загальна кількість вимірювань, $\tilde{T}_{ELs}^{E}$ – поправочний еталон. $\tilde{T}_{ELs}^{E}$ визначається за допомогою сенсорів і механізму лічильника. За своєю суттю процедура аналогічна з методом фазифікації параметрів, описаному в [40].

Етап 2.5. Обчислення рівня критичності КС. На четвертому етапі здійснюються обчислення загальної оцінки рівня критичності ситуації. Спочатку з врахуванням визначених КВ формується НЧ

$$\tilde{LCS}_i = \sum_{e=1}^{E} (\Omega_e * \tilde{L}_e) \qquad (3.3)$$

Сформоване НЧ порівнюється з оціночним еталоном за одним з відомих методів порівняння НЧ. Для даних цілей використаємо метод формування α-рівневої номіналізації НЧ [49] і метод визначення ідентифікуючих термів [39]. Процедура полягає в обрахунку номіналізованих (перетворених) еталонів та рівня

критичності (попередньо проводиться розбиття на α-рівні AL_{ELg} і AL_{LCSg}) $\mathbf{T}^{ep}_{EL} = \{\bigcup_{s=1}^{r} \underset{\sim}{T}^{ep}_{ELs}\} = \{\underset{\sim}{T}^{ep}_{EL1}, \ldots, \underset{\sim}{T}^{ep}_{ELr}\}$, де $\underset{\sim}{T}^{ep}_{ELs} = \{\bigcup_{g=1}^{z} \mu^{ep}_{ELsg} / x^{ep}_{ELsg}\} = \{\mu^{ep}_{ELs1} / x^{ep}_{ELs1}, ..., \mu^{ep}_{ELsz} / x^{ep}_{ELsz}\}$, $(g = \overline{1,z})$, $(s = \overline{1,r})$, а $\mu^{ep}_{ELsg} = \mu^{ep}_{ELs(z-g+1)} = AL_{ELg}$ і $x^{p}_{ELg} = x_{ELq} + \frac{(\mu^{p}_{ELg} - \mu_{ELq})(x_{ELq+1} - x_{ELq})}{\mu_{ELq+1} - \mu_{ELq}}$, $(g = \overline{2,z})$, z – кількість компонент $\underset{\sim}{T}^{ep}_{ELs}$. Аналогічна процедура здійснюється з поточними значеннями рівня критичності. Далі проводиться визначення узагальненої відстані Хемінга

$$h(\underset{\sim}{T}^{ep}_{ELs}, \underset{\sim}{LCS}^{p}) = \sum_{g=1}^{z} \left| x^{ep}_{ELsg} - x^{p}_{LCSg} \right| = |x^{ep}_{ELs1} - x^{p}_{LCS1}| + |x^{ep}_{ELs2} - x^{p}_{LCS2}| + \ldots + |x^{ep}_{ELsg} - x^{p}_{LCSg}| + \ldots + |x^{ep}_{ELsz} - x^{p}_{LCSz}|, \quad (3.4)$$

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

$$h\min_s = \bigwedge_{s=1}^{r} h(\underset{\sim}{T}^{ep}_{ELs}, \underset{\sim}{LCS}^{P}) \quad (3.5)$$

Етап 2.6. 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 [46], за яким НЧ перетворюють в чітке за формулою

$$L = 100 * (\sum_{i=1}^{q} x_{Lq} * \mu(x_{Lq}) / \sum_{i=1}^{q} \mu(x_{Lq})) \quad (3.6)$$

де q – 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. 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. 3.1.

Таблиця 3.1

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. 3.2.

Таблиця 3.2

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 (3.2) та рівень критичності за виразом (3.3).

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

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

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

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

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

$\underset{\sim}{L}_7 = (8*\underset{\sim}{T}^e_{EL1} + 2*\underset{\sim}{T}^e_{EL2})/10 = (8*\underset{\sim}{MH}^e + 2*\underset{\sim}{HC}^e)/10 =$ *(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}.*

$\underset{\sim}{L}_9 = (8*\underset{\sim}{T}^e_{EL2} + 2*\underset{\sim}{T}^e_{EL3})/10 = (8*\underset{\sim}{HC}^e + 2*\underset{\sim}{C}^e)/10$ *= (8*{0/0; 1/0,25; 0/0,5}+2*{0/0,25; 1/0,5; 0/0,75})/10 = ({0/0; 1/2; 0/4}+{0/0,5; 1/1; 0/1,5})/10 = ({0/0,5; 0/1; 0/1,5; 0/2,5; 1/3; 0/3,5; 0/4,5; 0/5; 0/5,5})/10 = ({0/0,5; 1/3; 0/5,5})/10 = {0/0,05; 1/0,3; 0/0,55}.*

$\underset{\sim}{L}_{10} = (8*\underset{\sim}{T}^e_{EL3} + 2*\underset{\sim}{T}^e_{EL4})/10 = (8*\underset{\sim}{C}^e + 2*\underset{\sim}{BC}^e)/10$ *= (8*{0/0,25; 1/0,5; 0/0,75}+2*{0/0,5; 1/0,75; 0/1})/10 = ({0/2; 1/4; 0/6}+{0/1; 1/1,5; 0/2})/10 = ({0/3; 0/3,5; 0/4; 0/5; 1/5,5; 0/6; 0/7; 0/7,5; 0/8})10 = ({0/3; 1/5,5; 0/8})10 = {0/0,3; 1/0,55; 0/0,8}.*

$\underset{\sim}{L}_{11} = (8*\underset{\sim}{T}^e_{EL4} + 2*\underset{\sim}{T}^e_{EL5})/10 = (8*\underset{\sim}{BC}^e + 2*\underset{\sim}{MK}^e)/10$ *= (8*{0/0,5; 1/0,75; 0/1}+2*{0/0,75; 1/1; 0/1})/10 = ({0/4; 1/6; 0/8}+{0/1,5; 1/2; 0/2})/10 = ({0/5,5; 0/6; 0,6; 0/7,5; 1/8; 0/8; 0/9,5; 0/10; 0/10})/10 = ({0/5,5; 0/6; 0/7,5; 1/8; 0/9,5; 0/10})/10 = ({0/5,5; 1/8; 0/10})/10 = {0/0,55; 1/0,8; 0/1}.*

$\underset{\sim}{L}_{12} = (5*\underset{\sim}{T}^e_{EL2} + 5*\underset{\sim}{T}^e_{EL3})/10 = (5*\underset{\sim}{HC}^e + 8*\underset{\sim}{C}^e)/10$ *= (5*{0/0; 1/0,25; 0/0,5}+5*{0/0,25; 1/0,5; 0/0,75})/10 = ({0/0; 1/1,25; 0/2,5}+{0/1,25; 1/2,5; 0/3,75})/10 = ({0/1,25; 0/2,5; 0/3,75; 0/2,5; 1/3,75; 0/5; 0/3,75; 0/5; 0/6,25})/10 = ({0/1,25; 0/2,5; 1/3,75; 0/5; 0/6,25})/10 = ({0/1,25; 1/3,75; 0/6,25})/10 = {0/0,125; 1/0,375; 0/0,625}.*

$\underset{\sim}{L}_{13} = (5*\underset{\sim}{T}^e_{EL3} + 5*\underset{\sim}{T}^e_{EL4})/10 = (5*\underset{\sim}{C}^e + 5*\underset{\sim}{BC}^e)/10$ *= (5*{0/0,25; 1/0,5; 0/0,75}+5*{0/0,5; 1/0,75; 0/1})/10 = ({0/1,25; 1/2,5; 0/3,75}+{0/2,5; 1/3,75; 0/5})/10 = ({0/3,75; 0/5; 0/6,25; 0/5; 1/6,25; 0/7,5; 0/6,25; 0/7,5; 0/8,75})/10 = ({0/3,75; 0/5; 1/6,25; 0/7,5; 0/8,75})/10 = ({0/3,75; 1/6,25; 0/8,75})/10 = {0/0,375; 1/0,625; 0/0,875}.*

$\underset{\sim}{L}_{14} = (5*\underset{\sim}{T}^{e}_{EL2} + 5*\underset{\sim}{T}^{e}_{EL4})/10 = (5*\underset{\sim}{НС}^{e} + 2*\underset{\sim}{ВС}^{e})/10$ = *(5*{0/0; 1/0,25; 0/0,5}+5*{0/0,5; 1/0,75; 0/1})/10 = ({0/0; 1/1,25; 0/2,5}+{0/2,5; 1/3,75; 0/5})/10 = ({0/2,5; 0/0,375; 0/5; 0/3,75; 1/5; 0/6,25; 0/5; 0/6,25; 0/7,5})/10 = ({0/2,5; 0/0,375; 1/5; 0/6,25; 0/7,5})/10 = ({0/2,5; 1/5; 0/7,5})/10 = {0/0,25; 1/0,5; 0/0,75}.*

$\underset{\sim}{L}_{15} = (5*\underset{\sim}{T}^{e}_{EL4} + 5*\underset{\sim}{T}^{e}_{EL5})/10 = (5*\underset{\sim}{ВС}^{e} + 5*\underset{\sim}{МК}^{e})/10$ = *(5*{0/0,5; 1/0,75; 0/1}+5*{0/0,75; 1/1; 0/1})/10 = ({0/2,5; 1/3,75; 0/5}+{0/3,75; 1/5; 0/5})/10 = ({0/6,25; 0/7,5; 0/7,5; 0/7,5; 1/8,75; 0/8,75; 0/8,75; 0/10; 0/10})/10 = ({0/6,25; 0/7,5; 1/8,75; 0/10})/10 = ({0/6,25; 1/8,75; 0/10})/10 = {0/0,625; 1/0,875; 0/1}.*

$\underset{\sim}{LCS}_i = \sum_{e=1}^{E}(\Omega_e * \underset{\sim}{L}_e)$ = *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; 1/0; 0/0,0035}+{0/0; 1/0,036; 0/0,072}+{0/0,0405; 1/0,081; 0/0,1215}+{0/0,0535; 1/0,08025; 0/0,107}+{0/0,075; 1/0,1; 0/0,1}+{0/0; 1/0,0096; 0/0,0576}+{0/0,00065; 1/0,0039; 0/0,00715}+{0/0,0216; 1/0,0396; 0/0,0576}+{0/0,0286; 1/0,0416; 0/0,052}+{0/0,005875 1/0,017625; 0/0,029375}+{0/0,013125; 1/0,021875; 0/0,030625}+{0/0,007; 1/0,014; 0/0,021}+{0/0,02125; 1/0,02975; 0/0,034}={0/0; 1/0,036; 0/0,0755}+{0/0,094; 1/0,16125; 0/0,2285}+{0/0,075; 1/0,1096; 0/0,1576}+{0/0,02225; 1/0,0435; 0/0,06475}+{0/0,034475; 1/0,059225; 0/0,081375}+{0/0,020125; 1/0,035875; 0/0,051625}+{0/0,02125; 1/0,02975; 0/0,034}={0/0,094; 1/0,19725; 0/0,304}+{0/0,09725; 1/0,1531; 0/0,22235}+{0/0,0546; 1/0,0951; 0/0,133}+{0/0,02125; 1/0,02975; 0/0,034}={0/0,19125; 1/0,35035; 0/0,52635}+{0/0,07585; 1/0,12485; 0/0,167}={0/0,2671; 1/0,4752; 0/0,69335}.*

Використовуючи вираз (3.4) 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 [49] кількість α-рівнів буде два: α = 0 і α = 1. Результати обрахунку номіналізованих еталонів та поточних значень параметрів представимо у вигляді таблиці 3.3.

Таблиця 3.3

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

$\underset{\sim}{T}^{ep}_{ELs} / \underset{\sim}{LCS}^{p}$	$\mu^{ep}_{sg} / \mu^{p}_{g}$ $(g=\overline{1,3})$		
	$\mu^{ep}_{ELs1} / \mu^{p}_{LCS1}$	$\mu^{ep}_{ELs2} / \mu^{p}_{LCS2}$	$\mu^{ep}_{ELs3} / \mu^{p}_{LCS3}$
	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:

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

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

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

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

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

Отже, згідно (3.5) рівень критичності КС - середній. Даний результат можна відобразити графічно (рис. 3.4).

Для відображення отриманих результатів за 100-бальною шкалою проведемо дефазифікацію кожного з запропонованих оціночних параметрів та обрахованого загального рівня критичності оцінки методом визначення центру ваги, використавши (3.6) і одночасно здійснимо перетворення, представивши їх 100-бальною шкалою.

$$L_1 = 100 * (\sum_{i=1}^{n} x_{L_1 i} * \mu(x_{L_1 i}) / \sum_{i=1}^{n} \mu(x_{L_1 i})) = 100*(0*0+1*0+0*0{,}25)/(0+1+0) = 100*0/1 = 0.$$

Аналогічно $L_2 = 25$, $L_3 = 50$, $L_4 = 75$, $L_5 = 100$, $L_7 = 5$, $L_9 = 30$, $L_{10} = 55$, $L_{11} = 80$, $L_{12} = 37{,}5$, $L_{13} = 62{,}5$, $L_{14} = 50$, $L_{15} = 87{,}5$ та $LCS = 47{,}52$.

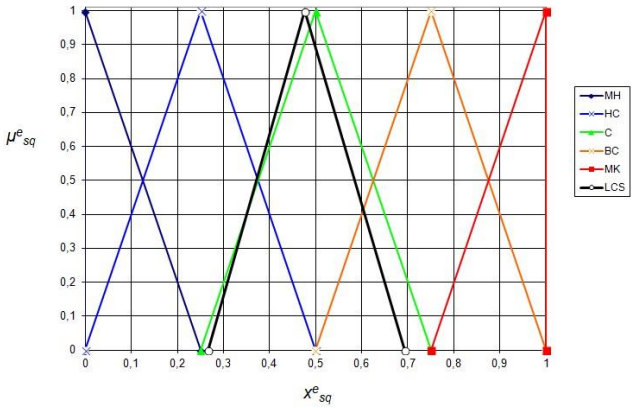


Рис. 3.4. Графічне представлення еталонних НЧ та рівня критичності ІПКС

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 $RD = \frac{LED(t)}{LED(t-1)}$, де $LED(t)$ – величина економічних збитків за поточний період, $LED(t-1)$ – величина економічних збитків за попередній період і $RM = \frac{SMR(t)}{SMR(t-1)}$, де $SMR(t)$ – смертність за поточний період, $SMR(t-1)$ – смертність за попередній період.

При цьому тривалості часових проміжків, що 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. 3.5. На ньому відображені рівня оціночних параметрів та обрахований загальний рівень критичності.

Запропонований метод, заснований на методах нечіткої логіки та експертних підходах дає змогу проводити оцінки критичності поточної ситуації. Застосування експертних методів пояснюється необхідністю зменшення часових та виробничих ресурсів, оскільки математичний апарат даних методів не потребує збору та обро-

бки 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.

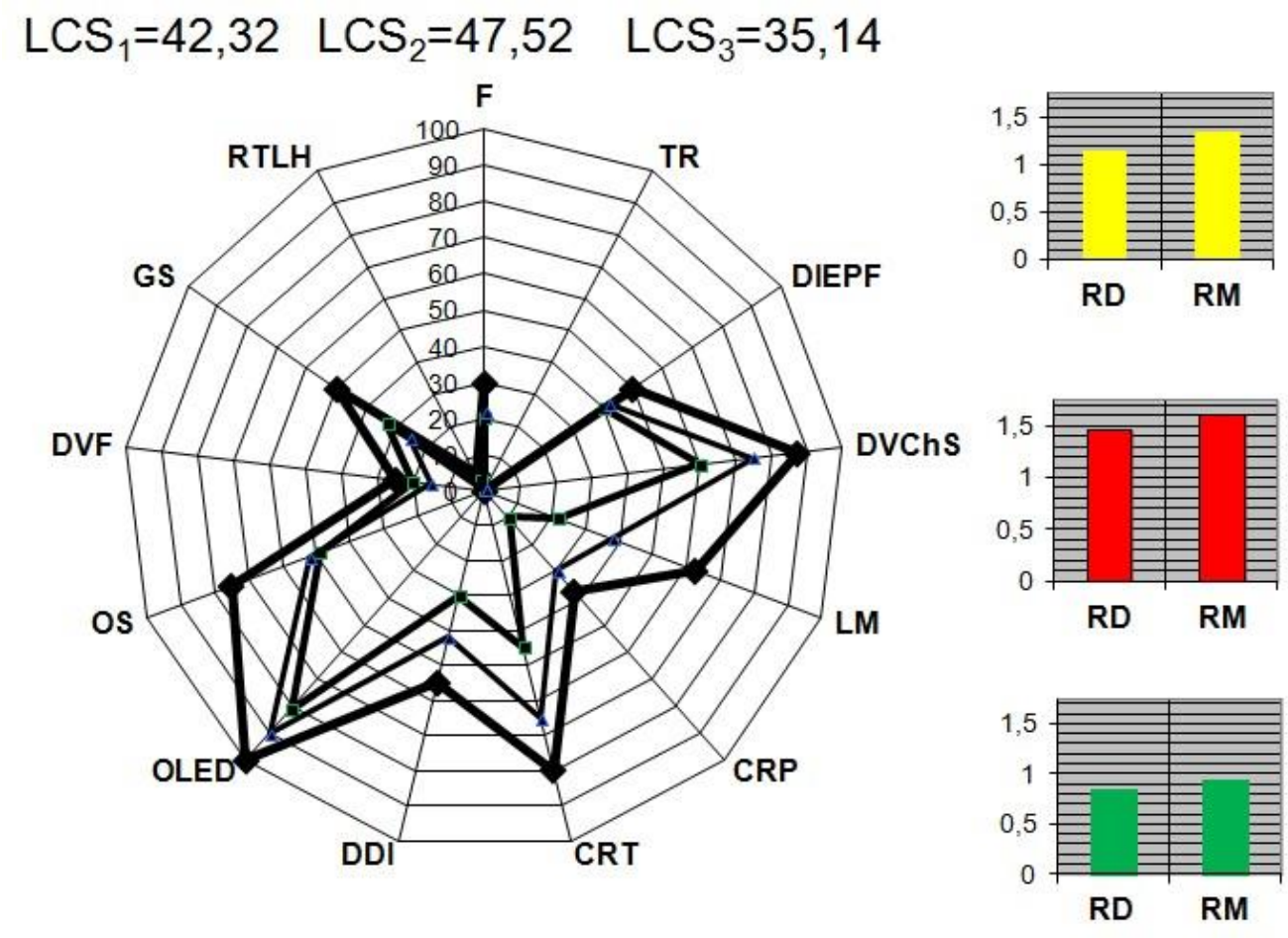


Рис. 3.5. Зображення індикатор рівня критичності ІПКС

3.2. Побудова системи виявлення інцидентів / кризових ситуацій

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. Тому основне призначення даної системи – прогнозування або виявлення та ідентифікація ІПКС.

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 [11]. Такий підхід не дозволяє виявляти 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 [38,46]. 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 [44,52], порушника ІБ [53], а також прототип даної системи [12,18,29].

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.

Архітектура СВІПКС представлена на рисунку 3.6. Вона включає такі структурні елементи як: система датчиків (СД); модуль первинної обробки вхідних парметрів, що вміщує регістри ідентифікуючих параметрів (РІП), регістри ІПКС (РІПКС), блок формування зв'язки інцидент-параметр (БФЗІП); модуль вториної 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 і блок прийняття рішення; модуль формування еталонів та евристичних правил, до складу якого входять одноймені відповідні блоки; модуль представлення результату, що міс-

тить блок логічного висновку та блок візуалізації; а також модуль управління режимами (МУР), що переводить систему в режим корекції еталонів (РКЕ) або режим корекції евристичних правил (РКЕП).

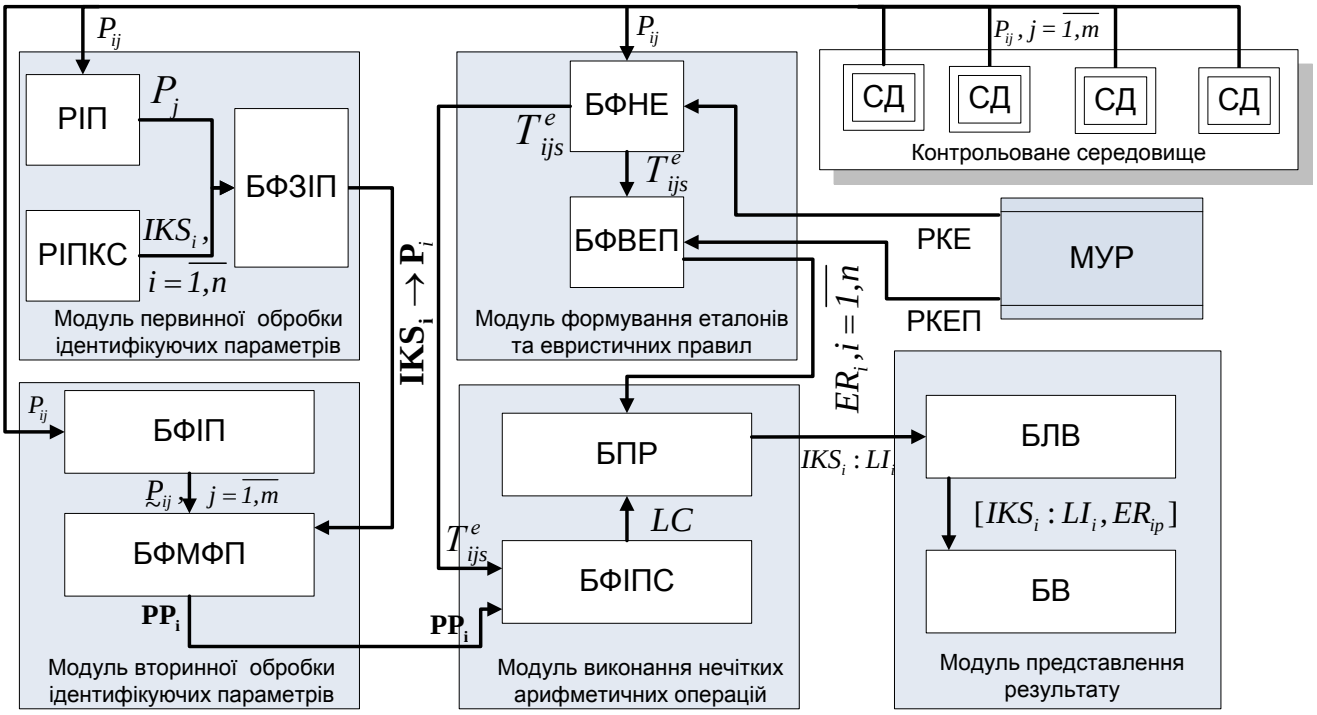


Рис. 3.6. Структура розробленої СВІПКС

СД розміщена в контрольованому середовищі (ІС, внутрішнє середовище будівель та приміщень, зовнішнє середовище певних територій, населених пунктів, держави тощо), що є нечітким та слабоформалізованим. 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 памяті тощо чи їх аналоги. В серверній використовуються датчики температури, гігрометри для визначеня 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 $IKS_i, i=\overline{1,n}$, а в РІП аналогічно заносяться з певною періодичністю поточні значення ідентифіку-

ючтх параметрів $P_{ij}, i = \overline{1,n}, j = \overline{1,m}$, що визначені і описані в попередніх розділах (див. пп. 2.1 та 3.1). В БФЗІП формуються зв'язки $\mathbf{IKS_i} \to \mathbf{P_i}$ конкретного типу ІПКС з параметрами, що необхідні для його виявлення. Так для окремих ІПКС створюються підмножини $\mathbf{P_i}$ [32].

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 складатимються з таких елементів як $\tilde{Tlog}$, $\tilde{Nlog}$, $\tilde{CPU}$, $\tilde{MU}$, $\tilde{NEr}$, $\tilde{RTPr}$, $\tilde{CNCh}$, $\tilde{NCC}$, $\tilde{DbR}$, $\tilde{STF}$, $\tilde{T}$, $\tilde{H}$, $\tilde{D}$ 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 (див. (2.10)). Еталони описуються за допомогою термів як ЛЗ. В БФЕП у процесі зіставлення ідентифікаторів поточного стану LC, що визначається комбінацією значень поточних параметрів, та лінгвістичних ідентифікаторів можливості реалізації ІПКС формується набір правил $\mathbf{ER} = \{\bigcup_{i=1}^{n} ER_i\} = \{\mathrm{ER}_1, ..., \mathrm{ER}_n\}$ для всіх заданих інцидентів [20].

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 еталоними 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 (див. формула 2.10). 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 $IKS_i : LI_i$. 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: $[IKS_i : LI_i, ER_{ip}]$.

3.3. Розробка система оцінки критичності ситуації

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 – за своєю суттю КС – потребує великих об'ємів фінансових та матеріальних затрат, що в даному випадку є виправданим. Запропонована система дозволяє провести оцінку критичності ІПКС і сформувати висновок про можливість його розгляду як КС.

Робота системи заснована на методі оцінки рівня критичності для систем управління КС [51], що описаний в розділі 3.1. Основним її призначення є оцінка рівня критичності ІПКС і прийняття рішення чи є цей інцидент КС. Вхідними да-

ними 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 Архітектура СОКС представлена на рис. 3.7.

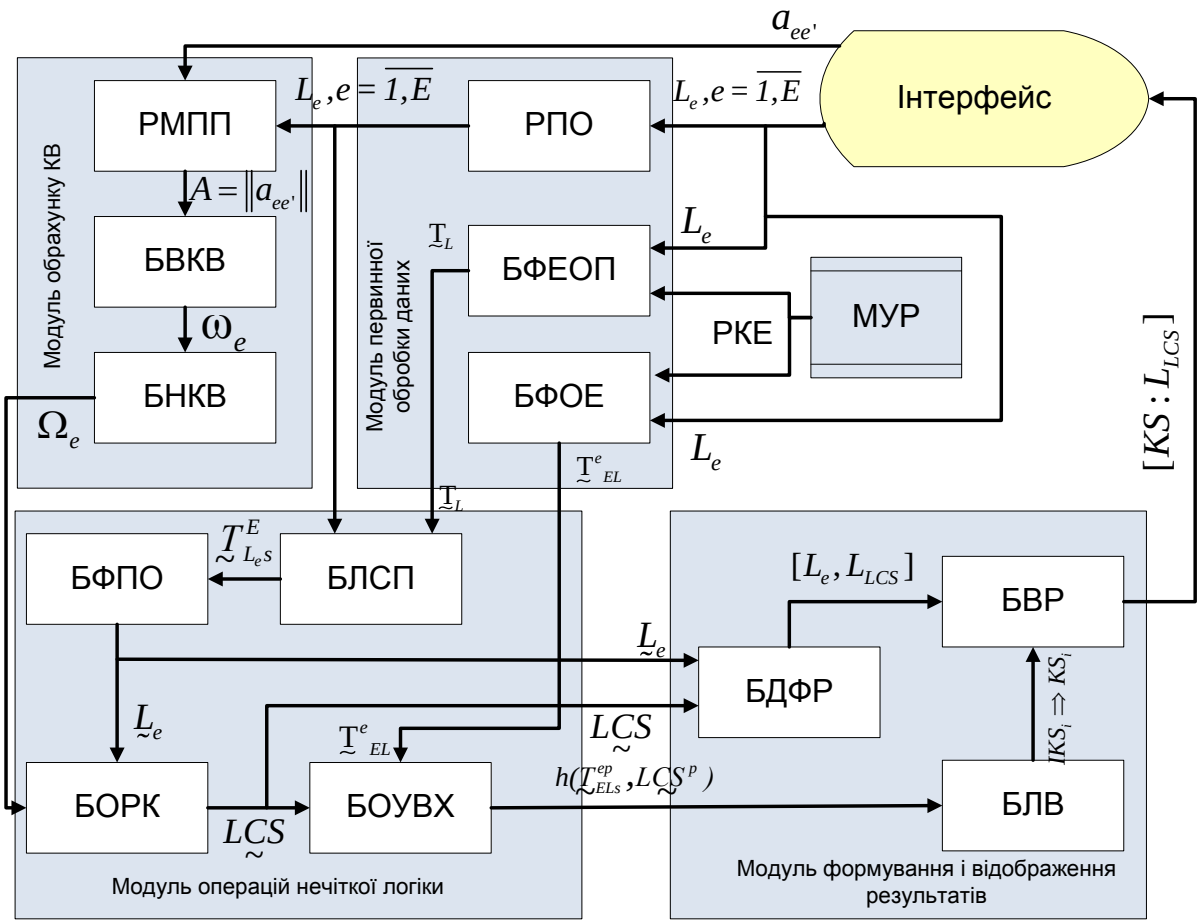


Рис. 3.7. Структура розробленої СОКС

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 КВ, який містить у собі ругістри матриці попарного порівняння (РМПП), блок визначення КВ (БВКВ) і блок нормування КВ (БНКВ); модуль операцій нечіткої логіки, до якого входять блок лічильника сенсорів параметрів (БЛСП), блок фазифікації оціночних параметрів (БФОП), блок обрахунку рівня критичності (БОРК), блок обчислення відстані Хемінга (БОВХ); модуль формування і відображення результатів, до складу якого входять блок дефазифікації результатів (БДФР), блок логічного висновку (БЛВ), блок візуалізації результатів

(БВР) 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, 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 $A=\|a_{ee'}\|$, 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 $\omega_e=\sqrt[n]{\prod_{e'=1}^{E} a_{ee'}}, e'=\overline{1,E}$, 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. 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 $T^{E}_{\sim ELs}$. 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: $\underset{\sim}{L}_{14} = (5*\underset{\sim}{T}^{e}_{EL2} + 5*\underset{\sim}{T}^{e}_{EL4})/10 = (5*\underset{\sim}{НС}^{e} + 2*\underset{\sim}{ВС}^{e})/10 = \{0/0{,}25;\ 1/0{,}5;\ 0/0{,}75\}$. Детально процедура фазифікації описана в розділах 3.4 дисертаційного дослідження. В БОРК проводиться обрахунок рівня критичності за виразом (3.3) з використанням ЛАЛМ при додаванні нечітких значень параметрів. В БОВХ з використанням методу, описаного в [39], обчислюється узагальнена ВХ 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 $\underset{\sim}{LCS}_i \gtrsim BC^{e}_{EL}$ ІПКС переходить у ранг КС. В БДФР отримані значення параметрів оцінки та загального рівня критичності обробляються таким чином, щоб приставити їх у вигляді чітких чисел, при цьому використовуються вирази (3.6). БВР відображає одержані дані в зручній користувачу форму. Так, тут формується індикатор рівня критичності, в якому відображаються значенні параметрів та рівня критичності, а також ідентифікатор ІПКС, що спричинив дану КС. За необхідності можливе відображення інформації щодо ІПКС, отриманої в прцесі роботи СВІПКС, а також загального рівня критичності ситуацій в формі ЛЗ або графічно.

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

3.4. Процедура визначення поточних параметрів середовища

Суть фазифікації полягає в обробці поточних значень контрольованих парметрів, знятих за певний період часу, і представлені їх у вигляді одного НЧ. Процедура фазифікації проводиться на основі методу, описаного в [40,46]. Фазифікуються лише нечіткі параметри, а саме на етапі виявлення та ідентифікації ІПКС – $P_1 = Tlog$, $P_2 = Nlog$, $P_3 = CPU$, $P_4 = MU$, $P_5 = NEr$, $P_6 = RTPr$, $P_7 = CNCh$, $P_8 = NCC$, $P_9 = DbR$, $P_{10} = STF$, $P_{11} = T$, $P_{12} = H$, $P_{13} = D$, а на етапі оцінки рівня критичності – $L_1 = TR$, $L_2 = DVF$, $L_3 = GS$, $L_4 = OS$, $L_5 = OLED$, $L_7 = RTLH$, $L_9 = F$, $L_{10} = DDI$, $L_{11} = CRT$, $L_{12} = CRP$, $L_{13} = LM$, $L_{14} = DIEPF$, $L_{15} = DVChS$.

Для проведення процедури фазифікації вимірюваних параметрів необхідно внести поняття сенсорів параметрів [40], що використовуються для контролю поточного стану параметрів. Введемо множину всіх сенсорів **S** і підмножину сенсорів, що визначаються для кожного заданого інтервалу значень всіх представлених параметрів $\mathbf{S_{ij}} \subseteq \mathbf{S}$:

$$\mathbf{S_{ij}} = \{\bigcup_{q=1}^{r_{ij}} S_{ijq}(t_T)\} = \{S_{ij1}(t_T), ..., S_{ijr_{ij}}(t_T)\}, \qquad (3.7)$$

де $S_{ijq}(t_T)$, $(i = \overline{1,n},\ j = \overline{1,m},\ q = \overline{1,r_{ij}})$ є сенсором N_{ijq}-го інтервала (див. процедуру формування еталонів у розділі 2.2), який відображає значення параметра $P_{ij}(t_T)$ на відповідному інтервалі в момент часу t_T, а r_{ij} – кількість сенсорів, що дорівнює кількості інтервалів. Сенсор $S_{ijq}(t_T)$ реалізований як бінарна функція, яка еквівалентна одиниці тільки в випадку, якшо значення $P_{ij}(t_T)$ в момент часу t_T буде знаходитись в інтервалі N_{ijq} тобто:

$$S_{ijq}(t_T) = \begin{cases} 1, при\ P_{ij}(t_T) \in N_{ijq} \\ 0, при\ P_{ij}(t_T) \notin N_{ijq} \end{cases} \quad (q = \overline{1,r_{ij}}), \qquad (3.8)$$

Щоб визначити частоти зустрічаємості значень $P_{ij}(t_T)$ на кожному з інтервалів N_{ijq} $(q = \overline{1,r_{ij}})$ введемо множину всіх лічильників сенсорів **CS** і підмножину таких лічильників $\mathbf{CS_{ij}} \subseteq \mathbf{CS}$ для кожного параметра, які і визначають необхідні частоти за виразом:

$$\mathbf{CS_{ij}} = \{\bigcup_{q=1}^{r_{ij}} CS_{ijq}\} = \{\bigcup_{q=1}^{r_{ij}} \sum_{T=1}^{T_{\max}} S_{ijq}(t_T)\} = , \qquad (3.9)$$

де CS_{ijq} – лічильник сенсора $S_{ijq}(t_T)$, а T_{max} відповідає загальній кількості можливих t_T, тобто кількості вимірювань. Отримані частоти відображаються лічильниками.

Наступним кроком в процедурі фазифікації [40] є побудова поправочних еталонів на основі показів лічильника сенсорів та еталоних НЧ параметрів. З метою реалізації цього кроку вводиться множина всіх можливих поправочних еталонів $\mathbf{T^E}$ і підмножина відповідних параметрам поправочних еталонів $\mathbf{T_{ij}^E} \subseteq \mathbf{T^E}$, що будуються на основі $\mathbf{T_{ij}^E}$ і визначаються як

$$\mathbf{T_{ij}^E} = \{\bigcup_{s=1}^{r_{ij}} \underset{\sim}{T}_{ijq}^{E}\} = = \{\underset{\sim}{T}_{ij1}^{E}, \ \ldots, \ \underset{\sim}{T}_{ijr_{ij}}^{E}\} = \{\underset{\sim}{T}_{ij1}^{e} \cdot CS_{ij1}, \ \ldots, \ \underset{\sim}{T}_{ijr_{ij}}^{e} \, CS_{ijr_{ij}}\}, \qquad (3.10)$$

де $\underset{\sim}{T}_{ijs}^{E}$ $(s = \overline{1,r_{ij}})$ – поправочні еталоні НЧ з r_{ij} термів. Вони формуються за виразом:

$$\{\bigcup_{s=1}^{r_{ij}} \underset{\sim}{T}_{ijs}^{E}\} = \{\bigcup_{\substack{s=1 \\ q=1}}^{r_{ij}} \underset{\sim}{T}_{ijs}^{e} \cdot \underset{\sim}{CS}_{ijq}\} = \{\underset{\sim}{T}_{ij1}^{e} \cdot CS_{ij1}, \ \ldots, \ \underset{\sim}{T}_{ijr_{ij}}^{e} \cdot CS_{ijr_{ij}}\}, \qquad (3.11)$$

при $(s = q = \overline{1,r_{ij}})$.

Отримані дані дають можливість розрахувати нечіткі значення параметрів за певний час. Так результат процедури фазифікації формується за виразом:

$$\underset{\sim}{P}_{ij} = (\sum_{s=1}^{r_{ij}} \underset{\sim}{T}_{ijs}^{E}) / T_{max} = (\underset{\sim}{T}_{ij1}^{E} \tilde{+} \underset{\sim}{T}_{ij2}^{E} \tilde{+} \ldots \tilde{+} \underset{\sim}{T}_{ijr_{ij}}^{E}) / T_{max}, \qquad (3.12)$$

де $\underset{\sim}{P}_{ij} = \{\bigcup_{q=1}^{r_{ij}} \mu_{ijq} / x_{ijq}\} = \{\mu_{ij1} / x_{ij1}, ..., \mu_{ijsr_{ij}} / x_{ijr_{ij}}\}, (q = \overline{1,r_{ij}})$, r_{ij} – кількість компонент в поточному НЧ $\underset{\sim}{P}_{ij}$.

Розглянемо описану процедуру на прикладі фазифікації параметра «Завантаженість оперативної пам'яті» для виявлення ІПКС «Злом ІС», $P_{14} = MU$. При формувані еталону параметра була введена множина ідентифікаторів інтервалів його значень $\mathbf{N_{14}} = \{\bigcup_{q=1}^{3} N_{14q}\} = \{N_{141}, N_{142}, N_{143}\} = \{N_{ZLMU1}, N_{ZLMU2}, N_{ZLMU3}\} = \{[0;20[, [20;50[, [50;$

100]}. Введемо для даного параметра відповідні його інтервалам сенсори $\mathbf{S_{14}} = \{\bigcup_{q=1}^{3} S_{14q}(t_T)\} = \{S_{141}(t_T), S_{142}(t_T), S_{143}(t_T)\}$.

Проведемо вимірювання значень параметрів протягом періоду в 5 хв з їх фіксацією кожні 10 с, тобто здійснивши 30 замірів. А також зафіксуємо показники сенсорів в момент вимірювання. Результати представлені в таблиці .

Таблиця 3. 4

Значення параметра $P_{14}(t_T) = P_{ZLMU}(t_T)$ і їх сенсорів при t_T $(T = \overline{1,30})$

t_T $(T = \overline{1,30})$	$P_{14}(t_T) = P_{ZLMU}(t_T)$	S_{41}	S_{42}	S_{43}
1	39	0	1	0
2	41	0	1	0
3	35	0	1	0
4	56	0	0	1
5	64	0	0	1
6	62	0	0	1
7	50	0	0	1
8	43	0	1	0
9	38	0	1	0
10	35	0	1	0

t_T $(T = \overline{1,30})$	$P_{14}(t_T) = P_{ZLMU}(t_T)$	S_{41}	S_{42}	S_{43}
11	37	0	1	0
12	39	0	1	0
13	41	0	1	0
14	50	0	0	1
15	42	0	1	0
16	54	0	0	1
17	61	0	0	1
18	66	0	0	1
19	51	0	0	1
20	40	0	1	0

t_T $(T = \overline{1,30})$	$P_{14}(t_T) = P_{ZLMU}(t_T)$	S_{41}	S_{42}	S_{43}
21	37	0	1	0
22	25	0	1	0
23	18	1	0	0
24	23	0	1	0
25	19	1	0	0
26	22	0	1	0
27	31	0	1	0
28	35	0	1	0
29	24	0	1	0
30	19	1	0	0

Згідно виразу (3.8) сенсор $S_{141}(t_T)$ визначається як $S_{141}(t_T) = \begin{cases} 1, при\ P_{14}(t_T) \in N_{141} \\ 0, при\ P_{14}(t_T) \notin N_{141} \end{cases}$, $T = \overline{1,30}$ і очевидно, що в моменти часу t_{23}, t_{25}, t_{30} значення $S_{141}(t_{23}) = S_{141}(t_{25}) = S_{141}(t_{30}) = 1$, а в інші моменти відповідно прийматиме значення 0. Далі визначимо лічильники сенсорів $\mathbf{CS_{14}}$ згідно виразу (3.9) і відобразимо їх в табл. 3.5.

Таблиця 3.5

Частоти зустрічає мості поточного стану параметра $P_{14}(t_T) = MU(t_T)$ (значення лічильників сенсорів)

$\mathbf{CS_{14}}$	$\mathbf{N_4}$ $(i = 1, j = 4, q = 3)$		
	N_{41}	N_{42}	N_{43}
CS_{14q}	3	18	9

Отримавши значення лічильників, обрахуємо поправочні еталони НЧ за виразом (3.11). Так, будемо мати:

$$\underset{\sim}{T}^{E}_{141} = CS_{141} \cdot \underset{\sim}{T}^{e}_{141} = \{0/0{,}6;\quad 1/0{,}6;\quad 0{,}11/1{,}5;\quad 0/3\},$$

$$\underset{\sim}{T}^{E}_{142} = CS_{142} \cdot \underset{\sim}{T}^{e}_{142} = \{0/3{,}6;\quad 0{,}38/3{,}6;\quad 1/9;\quad 0{,}11/18\},$$

$\underset{\sim}{T}^{E}_{143} = CS_{143} \cdot \underset{\sim}{T}^{e}_{143} = \{0 / 1{,}8;\quad 0{,}22 / 4{,}5;\quad 1 / 9;\quad 0 / 9\},$

Таким чином за виразом (3.12) $\underset{\sim}{P}_{14} = (\sum_{s=1}^{3} \underset{\sim}{T}^{E}_{14s}) / T_{max} =$ *({0/0,6; 1/0,6; 0,11/1,5; 0/3}+{0/3,6; 0,38/3,6; 1/9; 0,11/18; 0/18}+{0/1,8; 0,22/4,5; 1/9; 0/9})/30=({0/4,2; 0/4,2; 0/9,6; 0/18,6; 0/18,6; 0/4,2; 0,38/4,2; 1/9,6; 0,11/18,6; 0/18,6; 0/5,1; 0,11/5,1; 0,11/10,5; 0,11/19,5; 0/19,5; 0/6,6; 0/6,6; 0/12; 0/21; 0/21}+{0/1,8; 0,22/4,5; 1/9; 0/9})/30=({0/4,2; 0,38/4,2; 1/9,6; 0,11/19,5; 0/21}+{0/1,8; 0,22/4,5; 1/9; 0/9})/30={0/6; 0/8,7; 0/13,2; 0/13,2; 0/6; 0,22/8,7; 0,38/13,2; 0/13,2; 0/11,4; 0,22/14,1; 1/18,6; 0/18,6; 0/21,3; 0,11/24; 0,11/28,5; 0/28,5; 0/22,8; 0/25,5; 0/30; 0/30}/30={0/6; 0,22/8,7; 0,38/13,2; 1/18,6; 0,11/28,5; 0/30}/30={0/0,2; 0,22/0,29; 0,38/0,44; 1/0,62; 0,11/0,95; 0/1}.*

Таким чином, в результаті процедури фазифікації сформоване НЧ $\underset{\sim}{P}_{14} =$ *{0/0,2; 0,22/0,29; 0,38/0,44; 1/0,62; 0,11/0,95; 0/1}*, яке відображає значення параметра «Завантаженість оперативної памяті» в контрольований період часу. Після цього відбувається порівняння сформованого НЧ з еталоними значеннями за виразом (3.4), при цьому попередньо проводиться процедура розбиття на α-рівні, з метою визначення ЛЗ, що характеризує рівень контрольованого параметру [39,49]. Результати розбиття на α-рівні і обрахунку номіналізованих еталонів та поточних значень параметрів представимо у вигляді таблиці 3.6.

Таблиця 3.6

Значення носіїв номіналізованих $\underset{\sim}{T}^{ep}_{14s}$**,** $(s = \overline{1,3})$ **–** $\underset{\sim}{H}^{ep}$**,** $\underset{\sim}{C}^{ep}$**,** $\underset{\sim}{B}^{ep}$ **та** $\underset{\sim}{P}^{p}_{14}$

$\underset{\sim}{T}^{ep}_{14s} / \underset{\sim}{P}^{p}_{14}$	$\mu^{ep}_{sg} / \mu^{p}_{g}$ $(g = \overline{1,9})$								
	$\mu^{ep}_{14s1} / \mu^{p}_{141}$	$\mu^{ep}_{14s2} / \mu^{p}_{142}$	$\mu^{ep}_{14s3} / \mu^{p}_{143}$	$\mu^{ep}_{14s4} / \mu^{p}_{144}$	$\mu^{ep}_{14s5} / \mu^{p}_{145}$	$\mu^{ep}_{14s6} / \mu^{p}_{146}$	$\mu^{ep}_{14s7} / \mu^{p}_{147}$	$\mu^{ep}_{14s8} / \mu^{p}_{148}$	$\mu^{ep}_{14s9} / \mu^{p}_{149}$
	0	0,11	0,22	0,38	1	0,38	0,22	0,11	0
$\underset{\sim}{T}^{ep}_{141} = \underset{\sim}{H}^{ep}$	0	0	0	0	0	0,409	0,463	0,5	1
$\underset{\sim}{T}^{ep}_{142} = \underset{\sim}{C}^{ep}$	0	0	0	0	0,5	0,848	0,938	1	1
$\underset{\sim}{T}^{ep}_{143} = \underset{\sim}{B}^{ep}$	0	0,35	0,5	0,603	1	1	1	1	1
$\underset{\sim}{P}^{p}_{14}$	0,2	0,245	0,29	0,44	0,62	0,85	0,909	0,95	1

Обрахуємо відстані Хемінга згідно даних наведених в таблиці:

$$h\left(\underset{\sim}{T}^{ep}_{141}, \underset{\sim}{P}^{p}_{14}\right) = \sum_{g=1}^{9} \left| x^{ep}_{141g} - x^{p}_{14g} \right| = |0\text{-}0{,}2| + |0\text{-}0{,}245| + |0\text{-}0{,}29| + |0\text{-}0{,}44| + |0\text{-}0{,}62| + |0{,}409\text{-}$$

$0{,}85| + |0{,}463\text{-}0{,}909| + |0{,}5\text{-}0{,}95| + |1\text{-}1| = 3{,}132.$

$$h\left(\underset{\sim}{T}^{ep}_{142}, \underset{\sim}{P}^{p}_{14}\right) = \sum_{g=1}^{9} \left| x^{ep}_{142g} - x^{p}_{14g} \right| = |0\text{-}0{,}2| + |0\text{-}0{,}245| + |0\text{-}0{,}29| + |0\text{-}0{,}44| + |0{,}5\text{-}0{,}62| + |0{,}848\text{-}$$

$0{,}85| + |0{,}938\text{-}0{,}909| + |1\text{-}0{,}95| + |1\text{-}1| = 1{,}376.$

$$h\left(\underset{\sim}{T}^{ep}_{143}, \underset{\sim}{P}^{p}_{14}\right) = \sum_{g=1}^{9} \left| x^{ep}_{143g} - x^{p}_{14g} \right| = |0\text{-}0{,}2| + |0{,}35\text{-}0{,}245| + |0{,}5\text{-}0{,}29| + |0{,}603\text{-}0{,}44| + |1\text{-}$$

$0{,}62| + |1\text{-}0{,}85| + |1\text{-}0{,}909| + |1\text{-}0{,}95| + |1\text{-}1| = 1{,}349.$

Отже, $h\min_s = \bigwedge_{s=1}^{r_{ij}} h(\underset{\sim}{T}^{ep}_{14s}, \underset{\sim}{P}^{p}_{14}) = h(\underset{\sim}{T}^{ep}_{143}, \underset{\sim}{P}^{p}_{14})$, тобто поточне значення контрольованого параметра $P_{14}(t_T) = P_{ZLMU}(t_T)$ найбільш близьке до $\underset{\sim}{T}^{ep}_{14} = \underset{\sim}{B}^{ep}$ і описується ЛЗ «Висока», що може бути зображено графічно на рисунку 3.8.

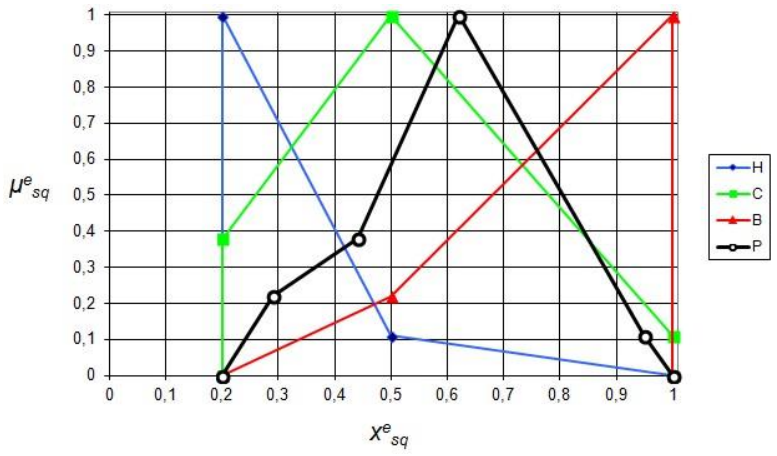


Рис. 3.8. Графічне представлення еталонних НЧ та рівня критичності ІПКС.

Аналогічно проходить процедура фазифікації інших параметрів і визначення їх поточного значення. Процедура обробки параметрів оцінки рівня критичності ситуації проводиться таким же чином, що детально описано в розділі 2.3.

3.5. Висновки до третього розділу

1. Вперше розроблено методи виявлення та оцінки КС, що за рахунок використання методів нечіткої логіки та експертних підходів дає можливість виявити ІПКС в слабоформалізованому середовищі і оцінити рівень критичності поточної ситуації, спричиненої даним інцидентом чи КС. Ці методи, що можуть застосовуватись як разом так і поодинці. Обидва методи включають в себе 6 етапів. Вхід-

ними даними методу виявлення ІПКС є параметри середовища, які підлягають моніторингу і, власне, ідентифікатори ІПКС, на виході формується повідомлення про фіксацію факту настання інциденту з уточненням ймовірності його настання. Вхідними даними методу оцінки рівня критичності КС є судження експертів щодо значень параметрів оцінки рівня критичності та щодо їх важливості (пріоритетності), на виході – результуючий показник загального рівня критичності поточної ситуації.

2. В роботі запропоноване нове структурне рішення, на основі якого можна розробляти алгоритмічне, програмне і програмно-апаратне забезпечення, що застосовується для виявлення та ідентифікації ІПКС в різних середовищах, зокрема в ІС. Робота описаної СВІПКС заснована на методі виявлення ІПКС, що описаний в розділі 2.3 дисертаційного дослідження. Система працює з заданими нечіткими параметрами, за якими здійснюється ідентифікація ІПКС. За рахунок використання методів нечіткої логіки та експертних підходів система може бути використана в нечіткому слабоформалізованому просторі, а також не потребує великих затрат часових і виробничих ресурсів для збирання та опрацювання статистичних даних, обробки складних математичних моделей теорії імовірності. Запропонована СВІПКС може використовуватись автономна, як складова СВОКС або як складова комплексної системи захисту інформації.

3. Запропоноване нове структурне рішення, на основі якого можна розробляти алгоритмічне, програмне і програмно-апаратне забезпечення, що застосовується для оцінки рівня критичності ситуації, що спричинена ІПКС. Робота описаної СОКС заснована на методі оцінки рівня критичності, що описаний в розділі 2.3 дисертаційного дослідження. Система працює з заданими нечіткими параметрами, за якими здійснюється оцінка рівня критичності. За рахунок використання методів нечіткої логіки та експертних підходів система може бути використана в нечіткому слабоформалізованому просторі, якому відповідають реальні умови. Запропонована СОКС може використовуватись автономна, як складова СВОКС або як складова комплексної системи захисту інформації.

4. Описана процедура фазифікації контрольованих параметрів та параметрів оцінки рівня критичності, що є одним з ключових етапів роботи запропонованих систем виявлення та ідентифікації ІПКС і оцінки рівня критичності ситуації. Про-

цедура заснована на технологій сенсорів параметрів та побудові з їх використанням частот зустрічання значень відповідних парметрів. Застосування даної процедури дозволяє використовувати СВОКС в слабоформалізованому нечіткому середовищі, приймати рішення в умовах нечіткості.

РОЗДІЛ 4. ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ СИСТЕМ ВИЯВЛЕННЯ ТА ОЦІНКИ КРИЗОВИХ СИТУАЦІЙ

4.1. Методика проведення експериментального дослідження

Метою будь-якого експериментального дослідження є виявлення якостей досліджуваних об’єктів, перевірка достовірності гіпотез, а також широке та глибоке вивчення досліджуваної наукової тематики. Існує багато різних класифікацій експериментів в залежності від галузі науки, мети дослідження, структури об’єктів та явищ, організаційних заходів, характеру взаємодії об’єкту та засобів дослідження тощо. Особливе значення в ході проведення експерименту займає правильна розробка методики експерименту – визначена послідовність процесів, у результаті якої досягається мета дослідження. Саме правильність розробки методики експериментального дослідження і визначає його цінність [94].

На початку проведення експериментального дослідження складається план-програми дослідження, де визначається: гіпотеза; мета та задачі; вхідні і вихідні параметри, область їх визначення та крок дискредитації; порядок проведення власне експерименту; зазначаються необхідні засоби проведення дослідження, моделювання, обробки результатів; порядок і вимоги щодо оформлення результатів. Наступним етапом є визначення об’єму експериментальних досліджень та необхідних програмних та апаратних засобів тощо. Далі безпосередньо проводиться експеримент з регламентацією всіх кроків, а на заключному етапі здійснюється обробка та систематизація експериментальних і усіх числових даних, перевірка зведення до єдиної системи одиниць, побудова графіків залежностей, таблиць, діаграм тощо.

Гіпотеза

Експеримент базується на припущені, що запропоновані системи управління КС адекватно реагують на зміну ідентифікуючих та оціночних параметрів при різних умов контрольованого середовища.

Мета та задачі експерименту

Метою експерименту є перевірка адекватності запропонованих моделей (пп. 2.2, 2.3), методів (п 3.1) і структурних рішень (пп. 3.2, 3.3) за допомогою розробленого програмного забезпечення управління КС, а саме:

– дослідження запропонованої СВІПКС на основі експертних методів та нечіткої логіки стосовно ефективності її роботи, а саме коректності виявлення різного роду ІПКС в ІС;

– дослідження запропонованої СОКС на основі експертних методів та нечіткої логіки стосовно ефективності її роботи, а саме коректності оцінювання критичності ситуації, що склалася під впливом ІПКС, та встановлені факту переходу небажаних подій з класу «інциденти інформаційної безпеки» до класу «кризова ситуація» .

Для досягнення поставленої мети необхідно вирішити наступні задачі:

– дослідження розробленого програмного забезпечення управління КС;

– обробка і верифікація отриманих результатів;

– проведення виявлення ІПКС та оцінки критичності ситуацій в контрольованому середовищі при зміні ідентифікуючих та оціночних параметрів

– визначення можливості використання СВІПКС та СОКС для забезпечення процесів КУББ.

Вибір вхідних та вихідних параметрів

Для СВІПКС вхідні параметри – нечіткі $Tlog, Nlog, CPU, MU, NEr, RTPr, CNCh, NCC, DbR, STF, T, H, D$; вихідні параметри – степінь впевненості експерта в рішенні щодо виявлення факту реалізації ІПКС ($H, C, П, B, K$) та категорія інциденту ZL, SP, DD, VA, ZK. Для СОКС вхідні параметри – нечіткі $T, DVF, GS, OS, OLED, RTLH, F, DDI, CRT, CRP, LM, DIEPF, DVChS$ та чіткі RD і RM, а також порівняльні судження експертів $a_{ee'}$ щодо важливості оціночних e-го та e'-го параметрів між собою відповідно до методу кількісного парного порівняння з визначенням квадратного кореня; вихідні параметри – показник рівня критичності ситуації (MH, HC, C, BC, MK), спричиненої впливом ІПКС, відображений індикатором критичності.

Вибір кроку зміни вхідних параметрів. Значення параметрів $Tlog, Nlog, CPU, MU, NEr, RTPr, CNCh, NCC, DbR, STF, T, H, D$ для обробки в СВІПКС приймаються значення в нормованому вигляді від 0 до 1, причому їх максимальні значення задані як $Tlog_{max} = 24год,\ Nlog_{max} = 15\ запити / с,\ CPU_{max} = 100\%,\ MU_{max} = 100\%,\ NEr_{max} = 10\ збоїв / добу,\ RTPr_{max} = 12\ год,\ CNCh_{max} = 200\%,\ NCC_{max} = 1024\ підключення,\ DbR_{max} = 1000\ мс,\ STF_{max} = 1000\ Мб,\ T_{max} = 40^0 C,\ H_{max} = 100\%,\ D_{max} = 100мкг / м^3$. Для обробки в СОКС параметри $T, DVF, GS, OS, OLED, RTLH, F, DDI, CRT, CRP, LM, DIEPF, DVChS$ приймають значення від 0 до 1, попередньо нормуючись. Максимальні значення параметрів встановлюються експертом в залежності від галузі застосування, контрольованого середовища і виду інциденту, що є причиною поточної ситуації.

Крім того ідентифікуючі та оціночні параметри можуть бути описані в вигляді лінгвістичних змінних, наприклад, «низький» (Н), «середній» (С), «великий» (В) тощо.

Послідовність дій в експериментальному досліджені

Для дослідження СВІПКС виконуються в повній відповідності до етапів методу виявлення ІПКС та режиму роботи системи (див. п.3.1 і 3.2) – задається множина ідентифікуючих параметрів; вимірюються і фазифікуються їх поточні значення, які потім порівнюються з еталонами; перевіряються ідентифікатори поточної ситуації на відповідність заданим правилам з набору ЕП, формується результат (приймається рішення щодо можливості реалізації ІПКС).

Для дослідження СОКС виконуються в повній відповідності до етапів методу оцінки критичності ситуації та режиму роботи системи (див. п.3.1 і 3.3) – задається множина оціночних параметрів; визначаються КВ важливості кожного параметра; проводиться фазифікація їх поточних значень; обчислюється показник рівня критичності ситуації; отриманий показник порівнюється з оціночним еталоном, на основі чого приймається рішення щодо критичності ситуації; проводиться дефазифікації значень оціночних параметрів та рівня критичності і на основі отриманих даних створюється індикатор критичності.

Засоби проведення експерименту

Для дослідження, створення необхідного програмного забезпечення, імітаційного модулювання, обробки результатів та представлення їх в табличному та графічному вигляді використовувалося середовище 1С:Підприємство 8.3. Для відображення індикатора рівня критичності поточної ситуації Microsoft Excel 2007.

Аналіз результатів

Аналіз результатів імітаційного моделювання буде представлено у підрозділі 4.4 даної роботи. Результати представлені в табличній формі та у вигляді графіків і діаграм.

4.2. Програмна система виявлення інцидентів/потенційних кризових ситуацій

У якості середовища розробки програмних засобів обрано технологічну платформу 1С: Підприємство 8.3. Технологічна платформа надає об'єкти (даних і метаданих) і механізми управління об'єктами [63]. Об'єкти (дані та метадані) описуються у вигляді конфігурацій. При автоматизації будь-якої діяльності (розробці програмних засобів) складається своя конфігурація об'єктів, яка і являє собою закінчене прикладне рішення. Конфігурація створюється в спеціальному режимі роботи програмного продукту під назвою «Конфігуратор», потім запускається режим роботи під назвою «1С: Підприємство», в якому користувач отримує доступ до основних функцій, реалізованим в даному прикладному рішенні (конфігурації). Сама платформа не є програмним продуктом для використання кінцевими користувачами, а слугує фундаментом для розробки та роботи прикладних рішень.

Основні ключові можливості технологічної платформи 1С: Підприємства 8.3, які вплинули на вибір даного середовища [63]:

1. Можливість використання трьох клієнтських програм: Товстий клієнт, Тонкий клієнт, Веб-клієнт.

2. Багатоплатформеність. У версії 1С: Підприємство 8.3, завдяки появі веб-клієнта, всі компоненти системи можуть працювати на комп'ютерах як під управлінням Windows, так і під управлінням Linux.

3. Відмовостійкий масштабований кластер з динамічним розподілом навантаження. В 1С: Підприємстві 8.3 розвиток кластера серверів виконано відразу по декількох напрямках: масштабованість, відмовостійкість, динамічний розподіл навантаження. Масштабованість. Можна управляти розподілом навантаження, яке раніше виконувалось єдиним менеджер кластеру. Відмовостійкість кластера в цілому досягається за рахунок того, що в 1С: Підприємство 8.3 кілька кластерів можуть бути об'єднані в групу резервування. Кластери, що знаходяться в одній групі резервування синхронізуються автоматично. Відмовостійкість робочих процесів досягається за рахунок їх резервування. Динамічний розподіл навантаження. Завантаженість робочих процесів аналізується динамічно і при необхідності клієнт автоматично перемикається на більш продуктивний робочий процес.

4. Новий інтерфейс. 1С: Підприємство 8.3 повністю змінює весь шар роботи з інтерфейсом, до якого відноситься командний інтерфейс, форми, віконна система.

5. Нова модель клієнт-серверної взаємодії. Архітектура керованого додатку орієнтована на максимальний перенос виконання всієї функціональності на сервер і максимальне «полегшення» клієнта. Функціональність форм і командного інтерфейсу також реалізована на сервері. На клієнті відображається вже підготовлена на сервері форма, виконується введення даних і виклики сервера для запису введених даних та інших необхідних дій. Аналогічно командний інтерфейс і звіти формується на сервері і відображається на клієнті.

Усі вище перечисленні можливості використання 1С: Підприємства 8.3 свідчать про те, що дана технологічна платформа може слугувати зручним засобом не тільки для автоматизації бухгалтерського та управлінського обліків підприємств, але й може знаходить своє застосування в областях, далеких від власне бухгалтерських завдань, наприклад для проведення наукових досліджень. Саме, тому дану платформу обрано для проведення експериментальних досліджень розроблених рішень.

Виконуваний програмний модуль може бути використаний на будь-якому комп’ютері, характеристики яких відповідають мінімальним вимогам для роботи

із 1С Підприємством (1С Підприємство має бути встановлено на комп'ютері):

- Процесор Intel Pentium IV/Xeon 2,4 ГГц і більше
- Оперативна память 1024 Мб і більше
- Жорсткий диск 40 Гб і більше
- ОС – Microsoft Windows.

Програмне забезпечення «СВІПКС v.1.0»

Структура розробленого програмного засобу (прикладного рішення) у режимі роботи «Конфігуратор» наведена на рис. 4.1.

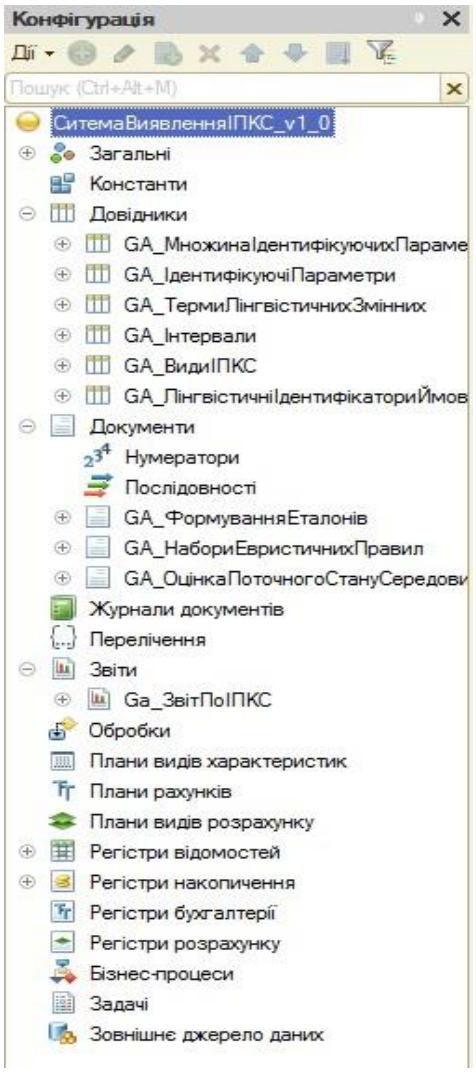


Рис. 4.1. Структура ПЗ «*СВІПКС v.1.0*» у режимі роботи «Конфігуратор»

Для проведення експерименту, на основі методу виявлення ІПКС (див. п.3.1), було розроблено програмне забезпечення «*СВІПКС v.1.0*». Дане програмне забезпечення реалізує виявлення ІПКС різного характеру в умовах слабоформалізованого нечіткого середовища. В ньому реалізовані процеси побудови еталонів

ідентифікуючих параметрів, наборів ЕП, фазифікації значень поточних параметрів та їх порівняння з еталонними за рахунок розрахунку УВХ. В регістри системи заносяться ідентифікуючі параметри та ідентифікатори ІПКС, склад і кількість яких може коригуватися.

Інтерфейс програми представлений на рисунку 4.2.

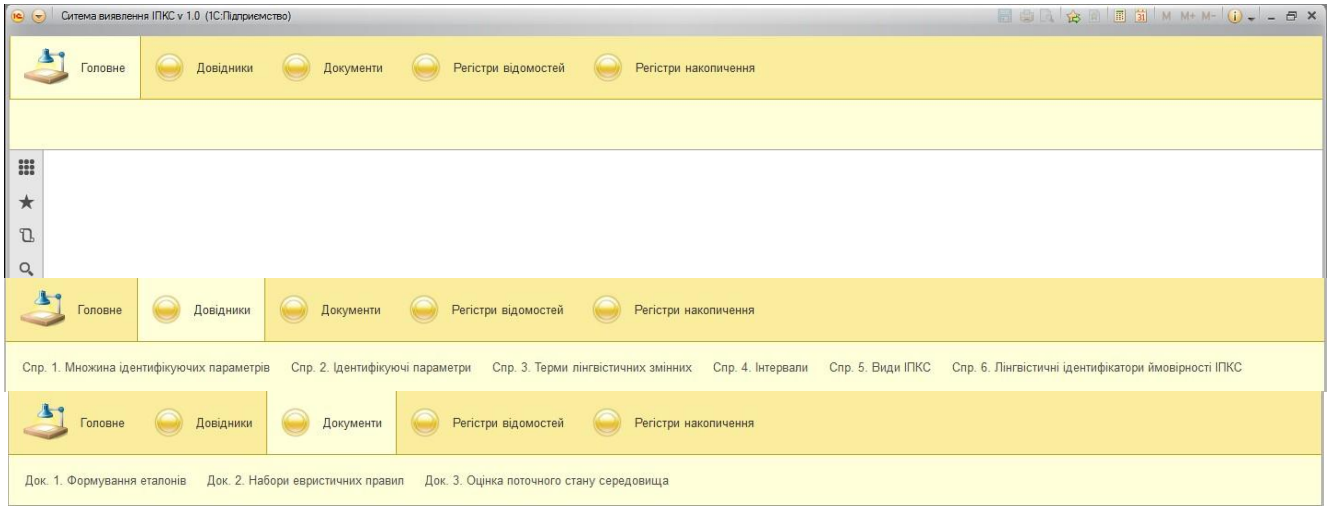


Рис. 4.2. Інтерфейс користувача ПЗ «*СВІПКС v.1.0*»

Як видно з рис. 4.1 − 4.2 розроблене ПЗ вміщує шість довідників і трьох документів. У середовищі 1С для роботи з постійною і умовно постійною інформацією з деякою множиною значень в системі використовуються об'єкти типу "Довідники". Для реалізації запропонованих математичних моделей були створені наступні об'єкти типу «Довідники»: «Множина ідентифікуючих параметрів», «Ідентифікуючі параметри», «Терми лінгвістичних зміних», «Інтервали», «Види ІПКС», «Лінгвістичні ідентифікатори можливості реалізації ІПКС». Через меню «Довідники» в інтерфейсі можна отримати доступ до цих довідників. Розглянемо названі довідники більш детально:

У довіднику «Множина ідентифікуючих параметрів» зберігаються множини (набори) ідентифікуючих параметрів, що використовується під час роботи системи для виявлення та ідентифікації ІПКС, та задається їх список. На рис. 4.3 наведено вікна форми елемента вказаного довідника.

Довідник «Ідентифікуючі параметри» використовується для зберігання всіх параметри, що задіяні в роботі системи. Також у кожному параметрі вказуються його інтервали та терми ЛЗ, що його характерихують. На рис. 4.4 наведено вікна

форми списку та форми елементу довідника «Ідентифікуючі параметри».

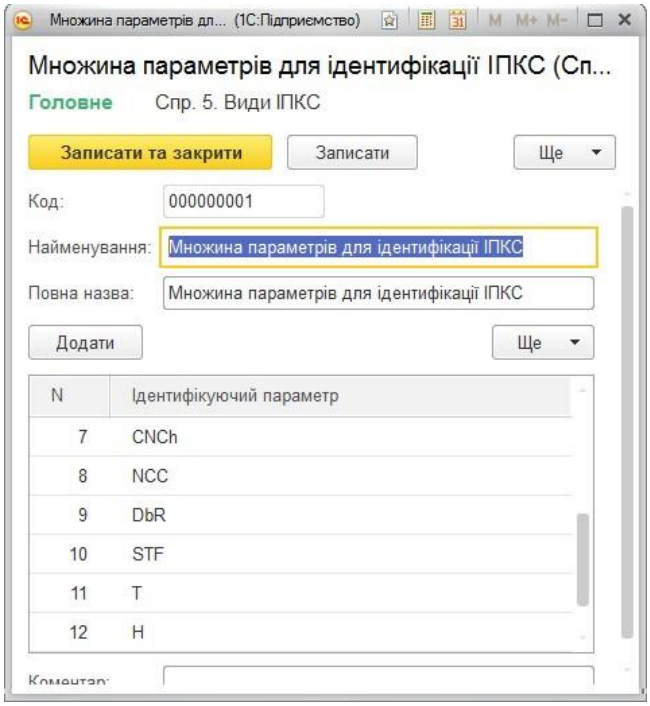


Рис. 4.3. Вікно форми елемента «Множина ідентифікуючих параметрів»

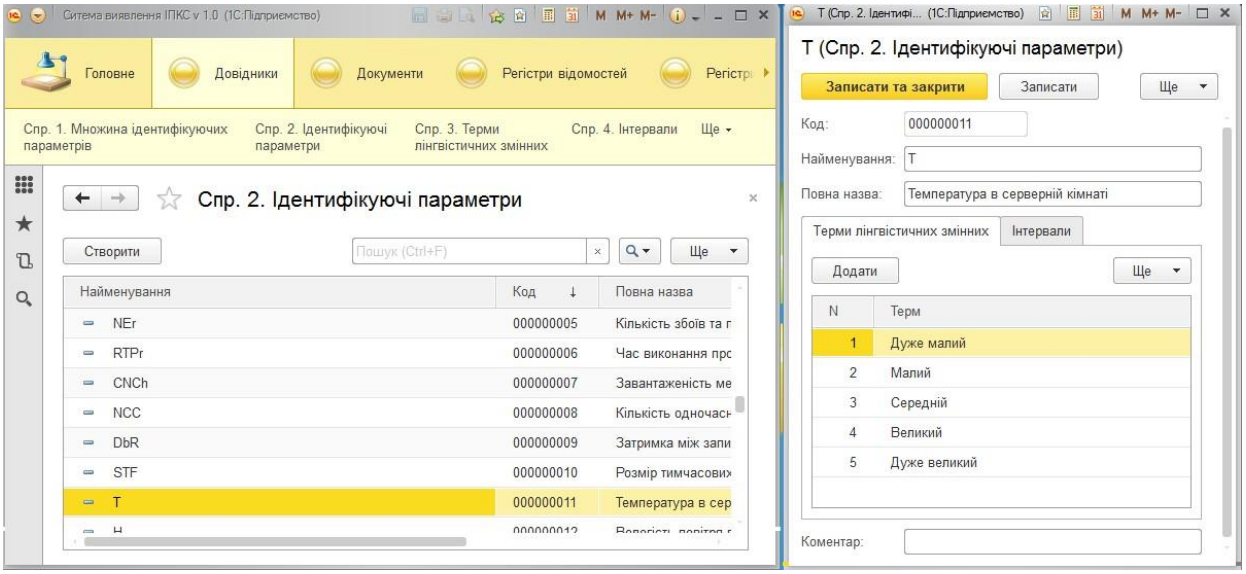


Рис. 4.4. Вікна форми списку та елемента довідника «Ідентифікуючі параметри»

Довідники «Терми лінгвістичних зміних» та «Інтервали» слугуються для зберігання інформації про вищевказані ЛЗ та інтервали. Довідник «Лінгвістичні ідентифікатори можливості реалізації ІПКС» слугує для зберігається інформація по всім лінгвістичним ідентифікаторам, що використовуються в дослідженні (приклад форми списку представлено на рис. 4.5).

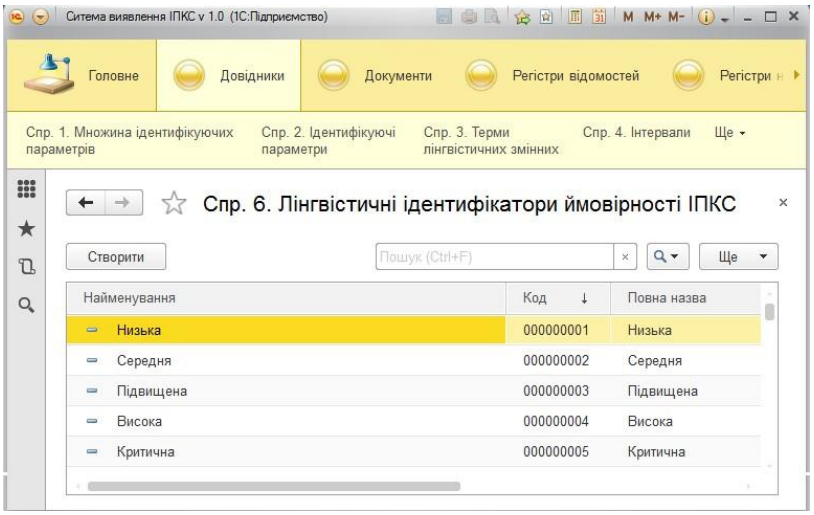


Рис. 4.5. Вікно форми списку довідника «Лінгвістичні ідентифікатори»

Довідник «Види ІПКС» необхідний для зберігання переліку інцидентів, що виявлялися при експерементальному дослідженні, та відповідні їм ідентифікуючі параметри. На рис. 4.6 наведено вікно форми списку даного довідника.

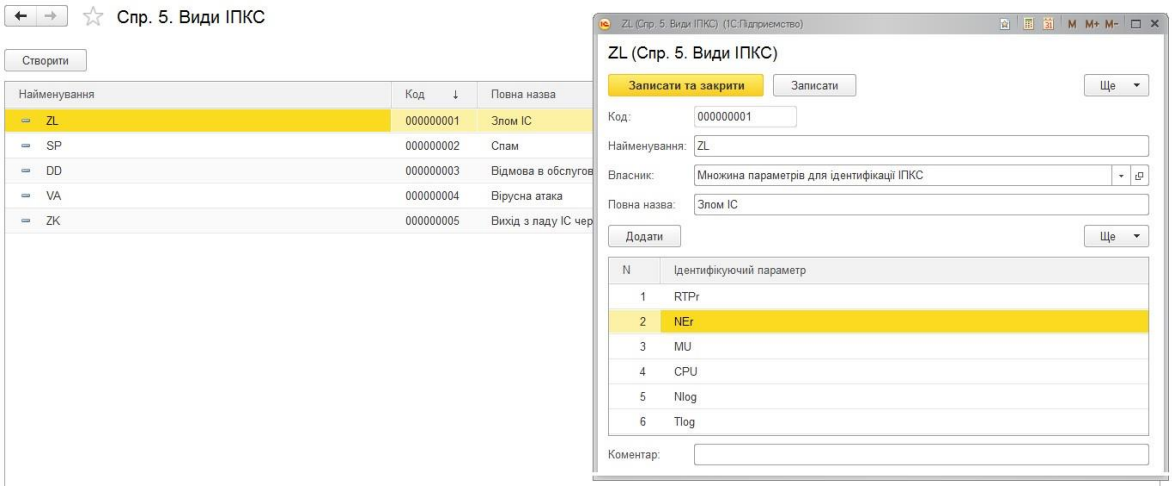


Рис. 4.6. Вікна форми списку та форми елемента довідника «Види ІПКС»

В 1С за допомогою об'єктів типу «Документы» організовується введення в систему інформації про здійснення будь-яких операцій, а також їх перегляд і корегування. В розробленій конфігурації були створені наступні об'єкти типу «Документы»: «Формування еталонів», «Набори евристичних правил», «Оцінка поточного стану середовища». Через меню «Документы» в інтерфейсі можна отримати доступдо них.

Еталони параметрів задаються експертом у документі «Формування еталонів» (приклад див на рис. 4.7). На вкладці «Аналітичні дані параметра» заносяться експертні дані для формування еталонів за методом МЛТС. Програмний

засіб автоматично будує графік функції належності еталонів лінгвістичної зміної.

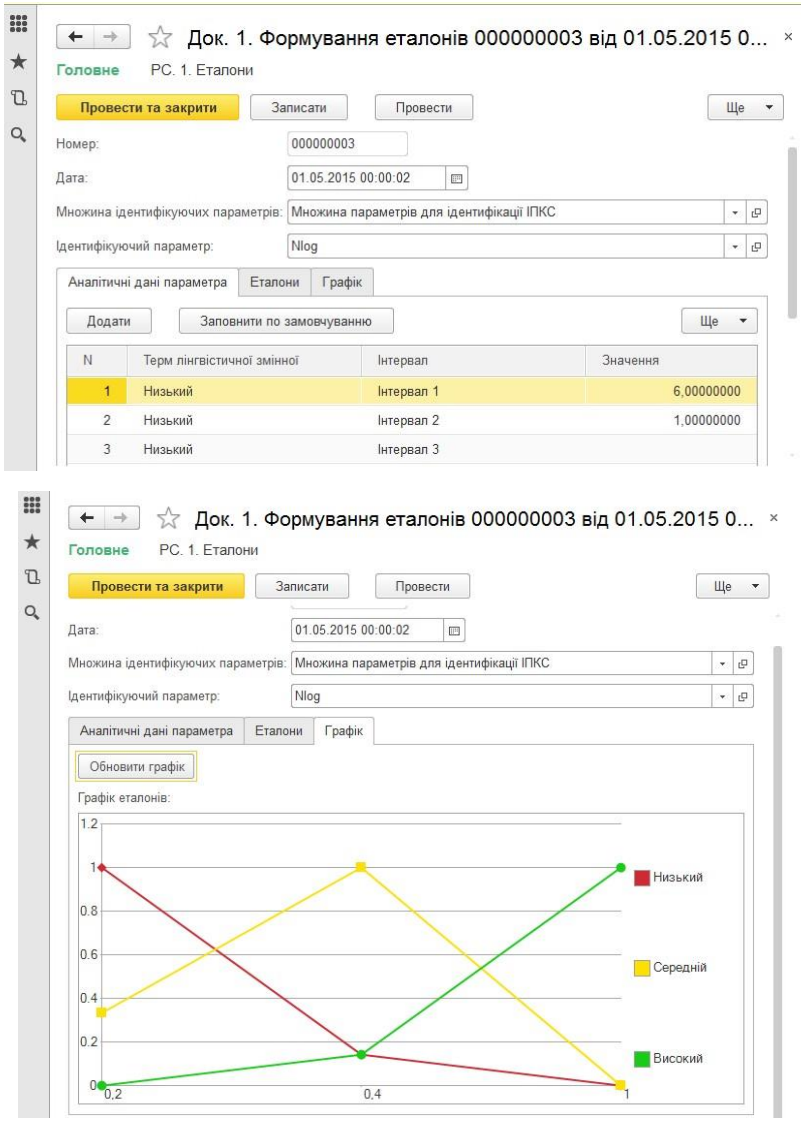


Рис. 4.7. Вікно форми елемента документа «Установка эталонов»

У документі «Набори евристичних правил» на вкладці «Список параметрів» задаються параметри, що входять в відповідні правила щодо виявлення певного ІПКС, на вкладці «Лінгвістичні ідентифікатори» задаються лінгвістичні значення, які характеризують судження експерта щодо можливості реалізації ІПКС, на вкладці «Правила» формуються набори ЕП з зазначенням відповідного лінгвістичного ідентифікатора.

Документ «Оцінка поточного стану» безпосередньо реалізує експеримент. У формі елемента документа «Оцінка поточного стану» задається кількість серій експерименту в графі «Кількість записів стаститики», а також інші параметри (дата, множина параметрів, номер експеремента, кількість даних для

групування під час фазифікації). На вкладці «Таблиця даних статистики» відображаються зібрані дані, а на вкладці «Таблиця сгрупованих даних» відображені вже фазифіковані значеня і результуючий рівень можливості реалізації ІПКС з вказанням його виду. Вікно форми елемента документа «Оцінка поточного стану» зображено на рис. 4.9.

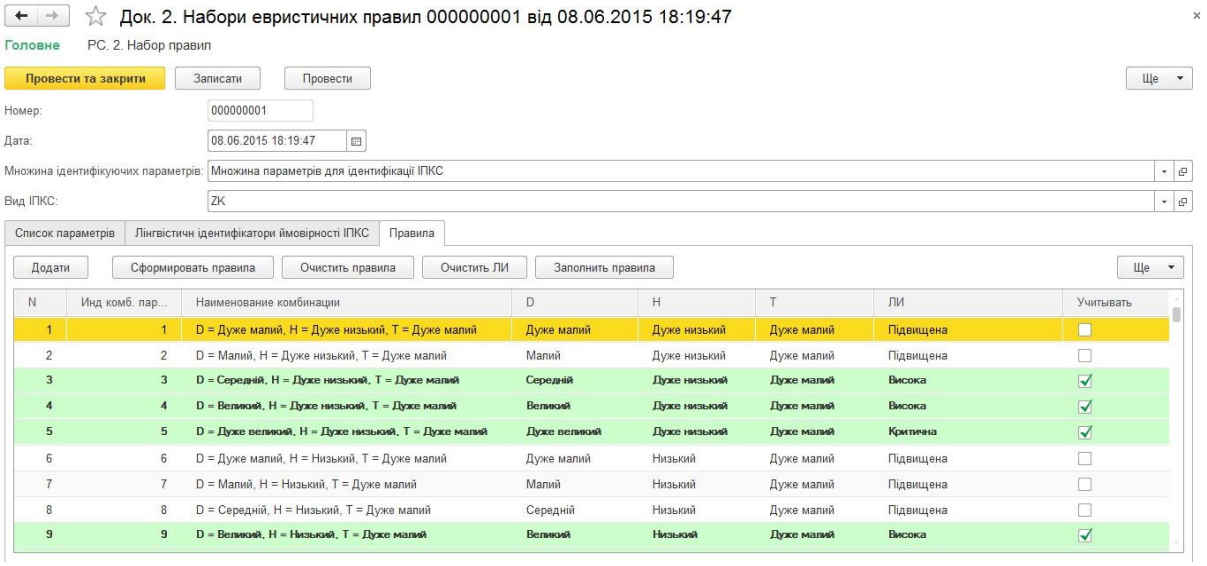


Рис. 4.8. Вікно форми елемента документа «Набори евристичних правил»

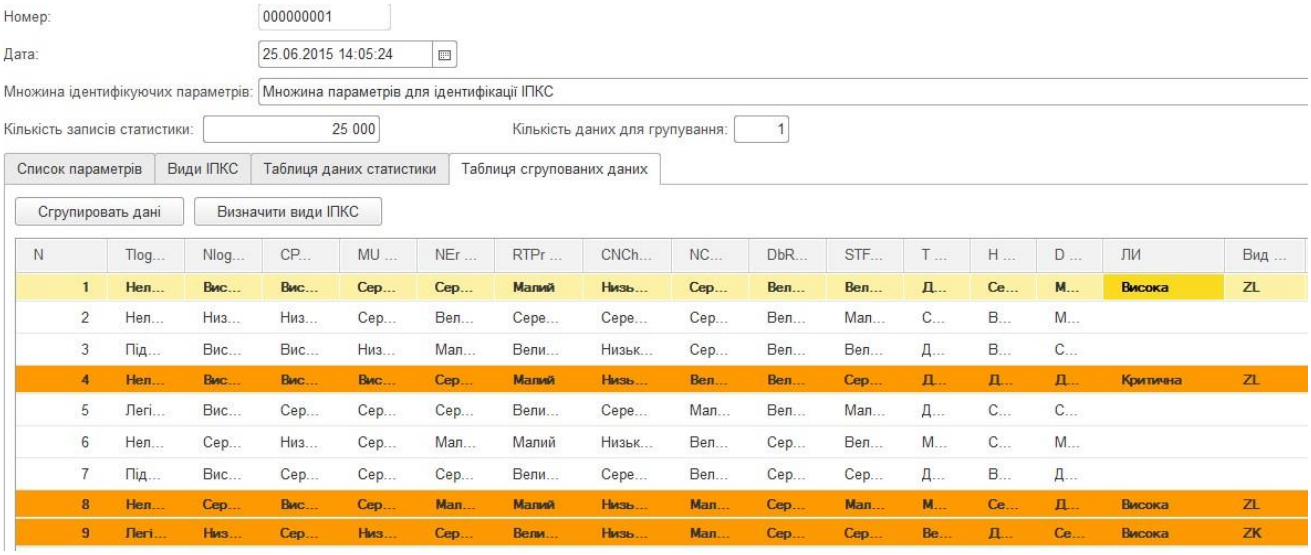


Рис. 4.9. Вікно форми елемента документа «Оцінка поточного стану»

У 1С звіти використовуються для отримання зведеної інформації на підставі даних, введених в системі. В розробленій конфігурації був створений один об'єкт типу «Звіти» − «Звіт по ІПКС». За допомгою даного звіту можна отримати доступ до детального звіту за результатами проведення імітаційного моделювання, що здійснюється програмним засобом.

4.3. Програмна система оцінки критичності ситуації

Виконуваний програмний модуль як і попередній може бути використаний на будь-якому комп'ютері, характеристики яких відповідають мінімальним вимогам для роботи із 1С Підприємством.

Програмне забезпечення «СОКС v.1.0»

Структура розробленого програмного засобу (прикладного рішення) у режимі роботи «Конфігуратор» наведена на рис. 4.10.

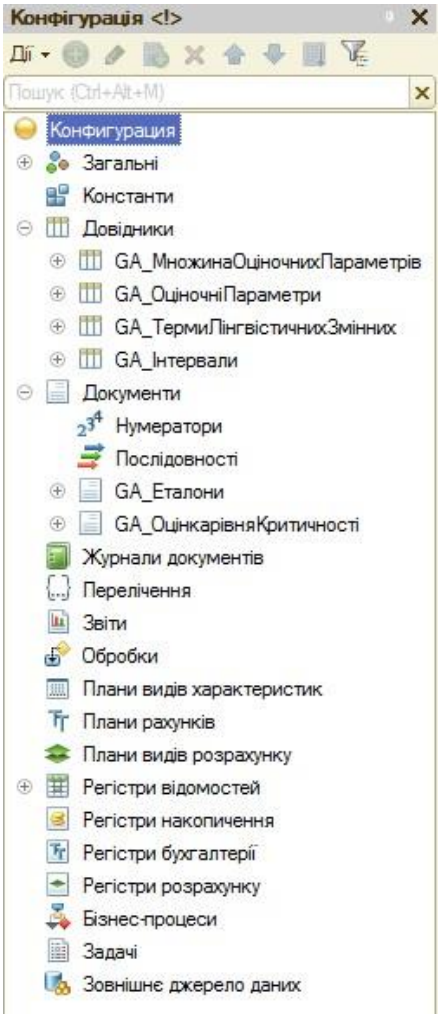


Рис. 4.10. Структура ПЗ «*СОКС v.1.0*» у режимі роботи «Конфігуратор»

Для проведення експерименту, на основі методу оцінки критичності ситуації (див. п.3.1), було розроблено програмне забезпечення «*СОКС v.1.0*». Дане програмне забезпечення реалізує процес оцінювання рівня критичності ситуації, що сталася внаслідок впливу ІПКС різного характеру в умовах слабоформалізованого нечіткого середовища. В ньому реалізовані процеси побудови еталонів оціночних параметрів, визначення коефіцієнтів важливості і ранжування параметрів, фазифі-

кації значень поточних параметрів, обрахунку показника рівня критичності, що представлений в формі НЧ, та їх дефазифікація для відображення в вигляді індикатора рівня критичності. В регістри системи заносяться оціночні параметри та експертні дані. Оціночні параметри в подальшому можуть бути скореговані.

Інтерфейс програми представлений на рисунку 4.11.

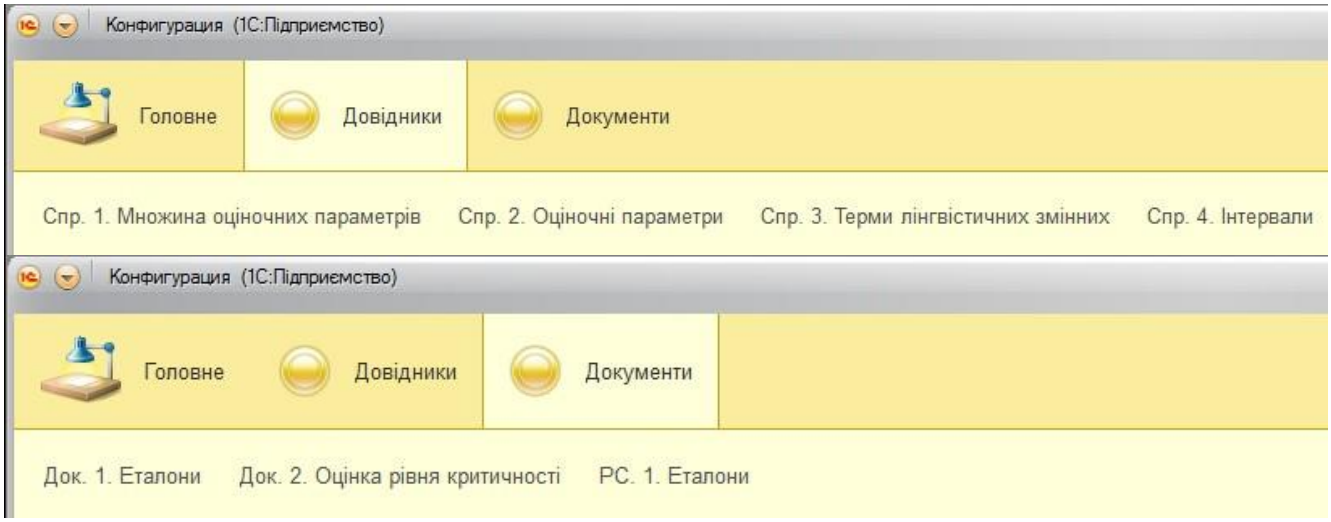


Рис. 4.11. Інтерфейс користувача ПЗ *«СОКС v.1.0»*

Як видно з рис. 4.10-4.11 розроблене ПЗ *«СОКС v.1.0»* вміщує чотири довідника і два документи. Для реалізації запропонованих математичних моделей були створені наступні об'єкти типу «Довідники»: «Множина оціночних параметрів», «Оціночні параметри», «Терми лінгвістичних зміних» та «Інтервали». Через меню «Довідники» в інтерфейсі можна отримати доступ до цих довідників. В розробленій конфігурації були створені наступні об'єкти типу «Документи»: «Еталони», «Оцінка рівня критичності». Через меню «Документы» в інтерфейсі можна отримати доступдо них.

У довіднику «Множина оціночних параметрів» визначаються параметри для оцінки рівня критичності, задається їх список та обраховуються коефіцієнти важливості в відповідних вкладках вікна форми елемента. На рис. 4.12 наведено вікна форми елемента вказаного довідника.

Довідник «Оціночні параметри» використовується для зберігання всіх параметри, що задіяні в роботі системи. Також у кожному параметрі вказуються його інтервали та терми ЛЗ, що його характерихують. На рис. 4.13 наведено вікна форми списку та форми елементу довідника «Оціночні параметри».

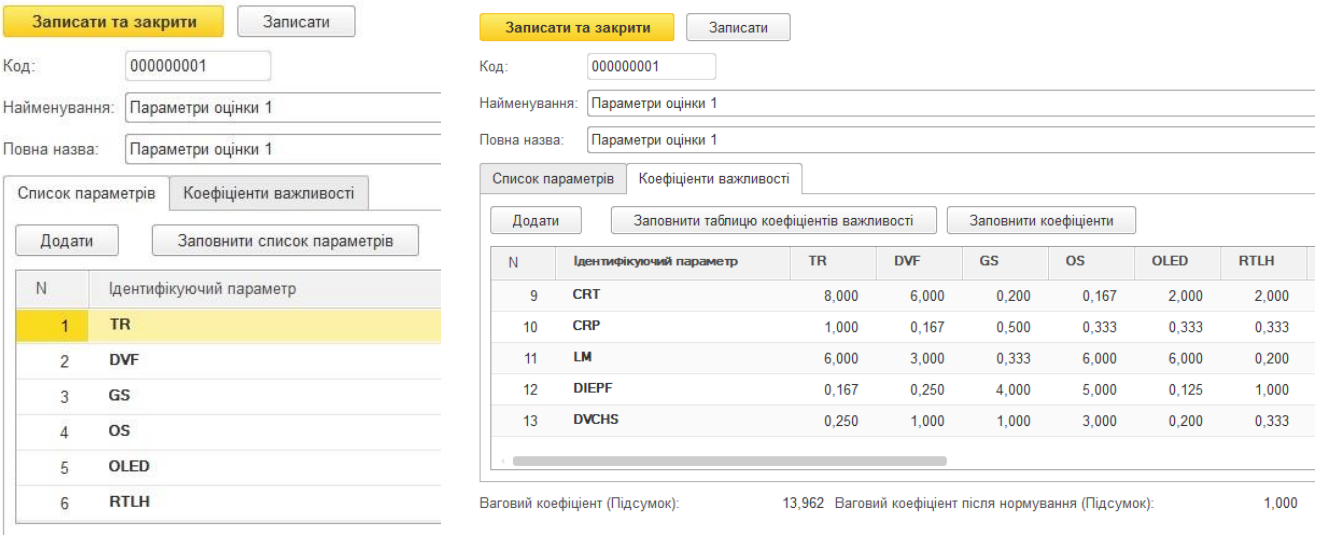


Рис. 4.12. Вікно форми елемента «Множина оціночних параметрів»

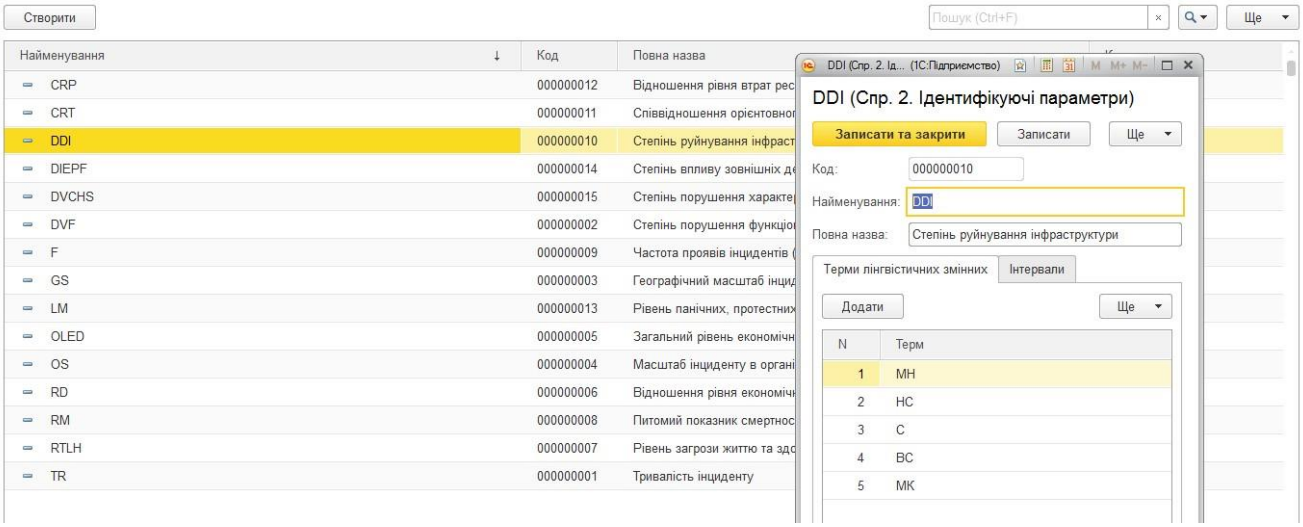


Рис. 4.13. Вікна форми списку та елемента довідника «Ідентифікуючі параметри»

Довідники «Терми лінгвістичних зміних» та «Інтервали» слугуються для зберігання інформації про вищевказані ЛЗ та інтервали, на основі яких будуються еталони.

Еталони параметрів задаються експертом у документі «Еталони» (приклад див на рис. 4.14). На вкладці «Еталони» заносяться експертні дані для формування еталонів за параметричним методом. Програмний засіб автоматично будує графік функції належності еталонів лінгвістичної зміної, що відображується на вкладці «Графік».

Документ «Оцінка рівня критичності» безпосередньо реалізує експеримент і в ньому обчислюється поточний рівень критичності. У формі елемента документа «Оцінка рівня критичності» задається кількість вимірювань показника сенсорів в

графі «Кількість даних для групування», а також інші параметри (дата, множина параметрів, номер експеремента). На вкладці «Список параметрів» вибираються параметри, по яким здійснюється оцінка рівня критичності. На вкладках «Таблиця даних статистики» і Таблиця сгрупованих даних» відображаються зібрані дані, та їх фазифіковані значення. Вкладка «Таблиця даних ЛЦС» відображає обрахований рівень критичності поточної ситуації в нечіткому вигляді, а вкладки «Таблиця розгрупованих даних» та «Таблиця розгрупованих даних ЛЦС» – значення оціночних параметрів та рівня критичності в чіткому вигляді після проведення процедури дефазифікації. На вкладці «Порівняння рівнів критичності» визначається відповідний поточному рівню критичності терм оціночного еталона через обрахунок УВХ. Вікно форми елемента документа «Оцінка поточного стану» зображено на рис. 4.15.

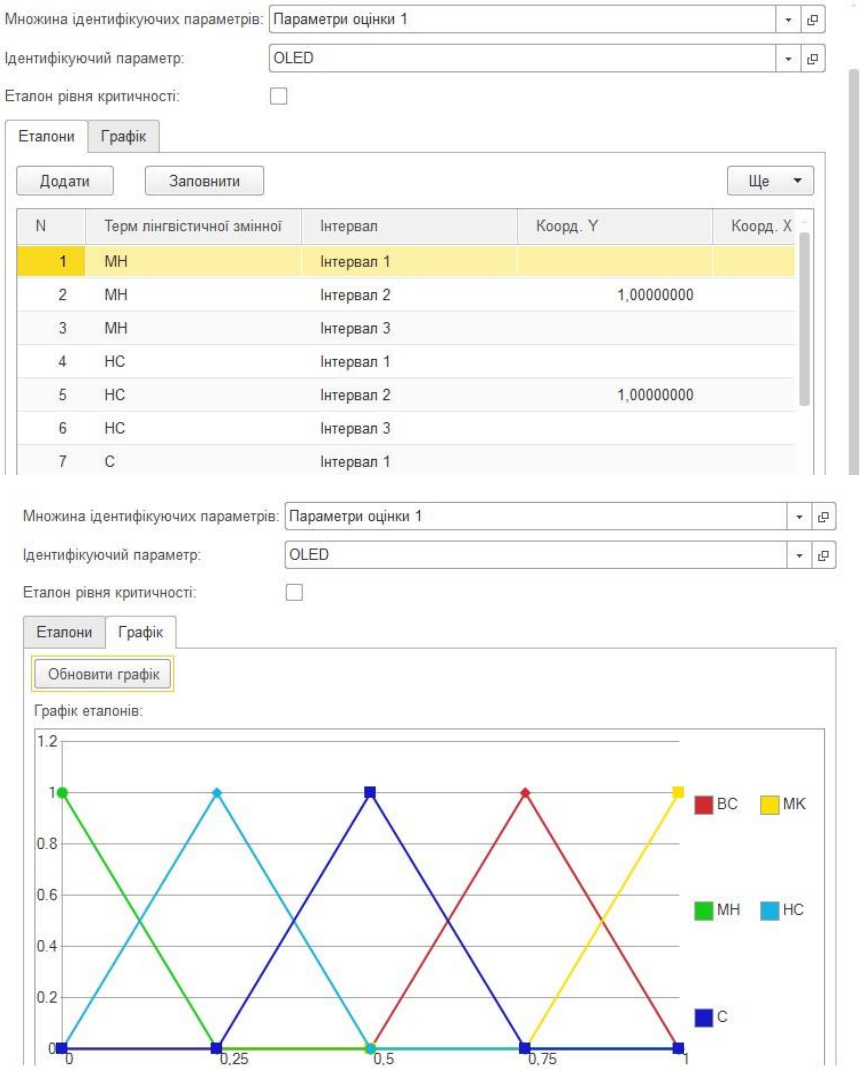


Рис. 4.14. Вікно форми елемента документа «Еталони»

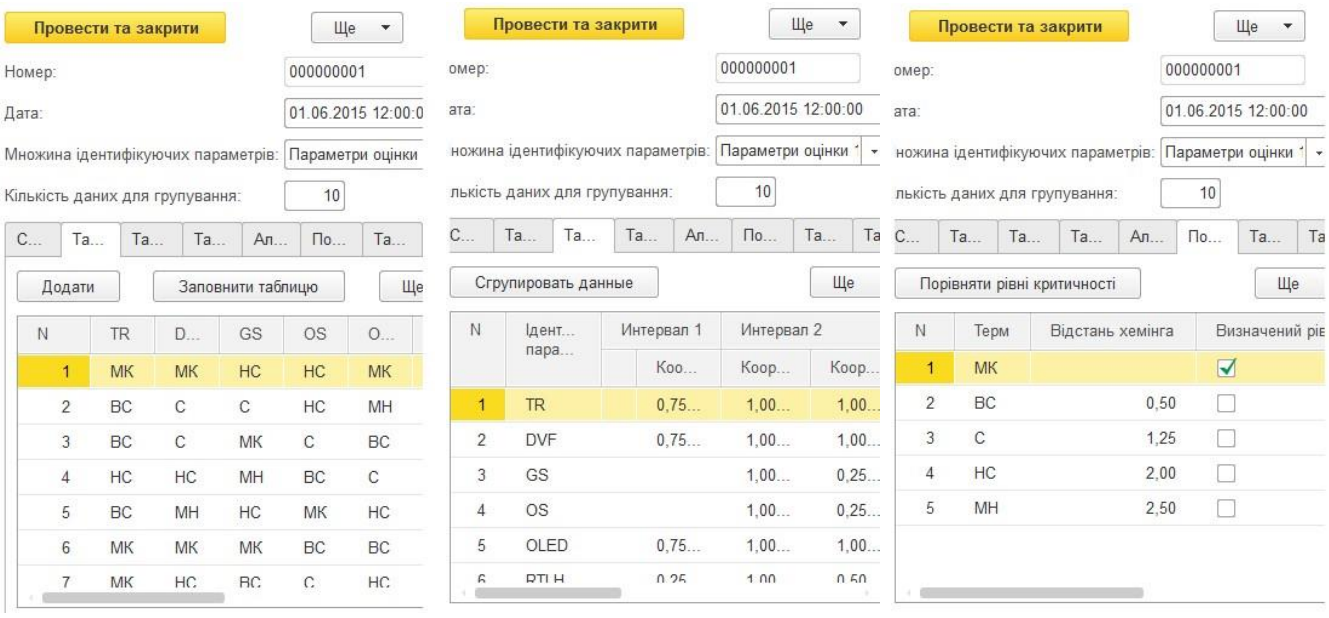


Рис. 4.15. Вікно форми елемента документа «Оцінка рівня критичності»

Таким чином, можна побачити, що структура ПЗ *«СОКС v.1.0»* дуже подібна до попередньої програмної розробки, а інтерфейс практично ідентичний.

4.4. Експериментальне дослідження програмної реалізації систем виявлення інцидентів/потенційних кризових ситуацій та оцінки критичності ситуації

Відповідно до розробленої методики було проведено експериментальні дослідження СВІПКС і СОКС. Далі опишемо хід проведення експерименту, а також обробку та аналіз його результатів. Експериментальне дослідження проводилось на окремому сервері, який піддавався мережевим атакам різного роду. Параметри сервера:

- CPU: Intel Core i7-2600 3.4GHz
- Memory: 4Gb DDR3
- OS: CentOS 6.3 x86_64 з останнім пакетом оновлень
- Kernel Version: 2.6.23-279
- Network: 100 Mbit/s

Виявлення ІПКС в процесі імітаційного моделювання контрольованого середовища ІС. Перевірка адекватності розроблених моделей еталонів та ЕП і коректності виявлення ІПКС. Згідно визначеним ідентифікуючим параметрам та категоріями ІПКС було промодельовані 110 000 станів контрольованого середовища

з різними поточними значеннями заданих параметрів. Серед них 31 411 моделюють стани, характерні для певних ІПКС з заданої множини. Для контролю середовища було задіяно 2063 правила. Кожен змодельований стан визначається 30 поточними значеннями параметрів, що знімаються кожні 10 с протягом 5 хв. Представимо деякі змодельовані стани середовища ІС та дані, отримані в процесі роботи СВІПКС в вигляді таблиць 4.1-4.3.

Таблиця 4.1

Стан характеристик змодельованого середовища №1 (злом інформаційної системи) і результати роботи СВІПКС

Параметр	Значення										Відповідна ЛЗ	Активоване ЕП	Інцидент: можливість
Tlog	01:18	01:18	01:18	01:18	01:18	01:19	01:19	01:19	01:19	01:19	Н		
	01:20	01:20	01:20	01:20	01:20	01:21	01:21	01:21	01:21	01:21			
	01:22	01:22	01:22	01:22	01:22	01:23	01:23	01:23	01:23	01:23			
Nlog	5	5	6	6	7	8	11	12	11	10	В		
	12	12	11	15	15	12	12	11	10	9			
	8	5	4	12	14	11	10	12	11	12			
CPU	1	2	1	5	1	3	28	35	60	62	В		
	62	68	81	75	77	75	76	77	80	82			
	87	82	82	80	76	81	84	82	82	83			
MU	22	25	30	21	29	25	44	41	56	95	В		
	88	92	91	90	91	95	91	92	96	91			
	75	85	88	91	93	94	91	87	92	91			
NEr	0	0	0	1	6	5	5	4	8	9	С		
	5	4	6	6	7	5	4	1	2	5			
	6	7	7	5	5	4	3	3	5	4			
RTPr	0,005	0,003	0,001	0.021	0,025	0,001	0,005	0,01	0,003	0,025	М		
	0,005	0,003	0,001	0.021	0,025	0,001	0,005	0,01	0,003	0,025		ER_{1724}	ZL:К
	0,005	0,003	0,001	0.021	0,025	0,001	0,005	0,01	0,003	0,025		ER_{2226}	SP:В
CNCh	35	38	37	40	22	54	60	51	20	69	Н	ER_{3596}	DD:П
	35	31	25	64	81	25	22	64	21	18		ER_{4227}	VA:П
	20	29	28	27	41	45	50	47	41	38		ER_{557}	ZK:С
NCC	5	5	17	12	10	8	8	10	5	7	М		
	12	25	31	41	35	31	25	17	18	21			
	12	11	8	60	24	26	28	32	18	40			
DbR	35	39	42	55	71	32	35	69	64	62	С		
	29	35	34	45	41	23	80	89	26	24			
	91	92	94	93	105	110	152	35	108	77			
STF	204	204	204	207	207	207	207	207	207	208	С		
	208	208	208	209	211	211	211	211	211	211			
	211	211	211	211	211	211	211	211	212	212			
T	25	25	25	25	25	25	25	25	25	26	С		
	26	26	26	26	26	26	26	26	26	26			
	25	26	26	25	26	26	26	26	26	27			
H	41	41	39	39	39	39	39	39	40	41	Н		
	40	40	40	40	39	40	40	40	41	40			
	40	39	39	39	39	40	40	40	40	39			
D	15	15	15	12	15	18	15	15	19	18	М		
	21	20	21	21	18	18	18	20	21	22			
	17	18	17	17	18	19	20	21	22	20			

Таблиця 4.2

Стан характеристик змодельованого середовища №2 (вірусна атака) і результати роботи СВІПКС

Параметр	Значення										Відповідна ЛЗ	Активоване ЕП	Інцидент: можливість
Tlog	15:34	15:34	15:34	15:34	15:34	15:35	15:35	15:35	15:35	15:35	Л	ER_{178} ER_{2234} ER_{3696} ER_{4234} ER_{557}	ZL:П SP:В DD:П VA:К ZK:С
	15:36	15:36	15:36	15:36	15:36	15:37	15:37	15:37	15:37	15:37			
	15:38	15:38	15:38	15:38	15:38	15:38	15:38	15:38	15:38	15:38			
Nlog	0	1	1	0	0	1	0	0	2	1	Н		
	1	1	0	0	2	1	2	1	1	1			
	0	0	0	1	1	2	0	1	0	0			
CPU	1	2	1	5	1	3	28	35	60	62	В		
	62	68	81	75	77	75	76	77	80	82			
	87	82	82	80	76	81	84	82	82	83			
MU	22	25	30	21	29	25	44	41	56	95	В		
	88	92	91	90	91	95	91	92	96	91			
	75	85	88	91	93	94	91	87	92	91			
NEr	0	0	0	1	6	5	5	4	8	9	С		
	5	4	6	6	7	5	4	1	2	5			
	6	7	7	5	5	4	3	3	5	4			
RTPr	7	8	11	5	6	5	7	8	4	8	В		
	6	8	8	10	7	9	5	6	6	4			
	4	4	8	9	10	10	7	8	4	7			
CNCh	178	178	154	165	140	158	181	175	172	189	В		
	199	200	200	200	200	184	193	184	195	200			
	200	199	171	185	154	175	162	180	188	189			
NCC	5	5	17	12	10	8	8	10	5	7	М		
	12	25	31	41	35	31	25	17	18	21			
	12	11	8	60	24	26	28	32	18	40			
DbR	400	420	410	400	410	380	450	200	250	400	В		
	500	480	520	350	370	480	520	550	560	510			
	570	600	520	480	490	500	510	520	510	470			
STF	514	520	521	522	578	580	580	595	600	625	В		
	687	691	721	726	727	750	781	784	785	799			
	801	805	811	812	812	812	812	812	812	813			
T	25	25	25	25	25	25	25	25	25	26	С		
	26	26	26	26	26	26	26	26	26	26			
	25	26	26	25	26	26	26	26	26	27			
H	41	41	39	39	39	39	39	39	40	41	Н		
	40	40	40	40	39	40	40	40	41	40			
	40	39	39	39	39	40	40	40	40	39			
D	15	15	15	12	15	18	15	15	19	18	М		
	21	20	21	21	18	18	18	20	21	22			
	17	18	17	17	18	19	20	21	22	20			

Таблиця 4.3

Стан характеристик змодельованого середовища №3 (Вихід з ладу ІС через мікрокліматичні умови)і результати роботи СВІПКС

Параметр	Значення										Відповідна ЛЗ	Активоване ЕП	Інцидент: можливість
Tlog	15:34	15:34	15:34	15:34	15:34	15:35	15:35	15:35	15:35	15:35	Л		
	15:36	15:36	15:36	15:36	15:36	15:37	15:37	15:37	15:37	15:37			
	15:38	15:38	15:38	15:38	15:38	15:38	15:38	15:38	15:38	15:38			

Продовження табл. 4.3

Nlog	0	1	1	0	0	1	0	0	2	1	Н	ER_{178} ER_{2232} ER_{3677} ER_{4227} ER_{5120}	ZL:П SP:П DD:П VA:П ZK:К
	1	1	0	0	2	1	2	1	1	1			
	0	0	0	1	1	2	0	1	0	0			
CPU	1	2	1	5	1	3	28	35	60	62	В		
	62	68	81	75	77	75	76	77	80	82			
	87	82	82	80	76	81	84	82	82	83			
MU	22	25	30	21	29	25	44	41	56	95	В		
	88	92	91	90	91	95	91	92	96	91			
	75	85	88	91	93	94	91	87	92	91			
NEr	0	0	0	1	6	5	5	4	8	9	С		
	5	4	6	6	7	5	4	1	2	5			
	6	7	7	5	5	4	3	3	5	4			
RTPr	7	8	11	5	6	5	7	8	4	8	В		
	6	8	8	10	7	9	5	6	6	4			
	4	4	8	9	10	10	7	8	4	7			
CNCh	35	38	37	40	22	54	60	51	20	69	Н		
	35	31	25	64	81	25	22	64	21	18			
	20	29	28	27	41	45	50	47	41	38			
NCC	5	5	17	12	10	8	8	10	5	7	М		
	12	25	31	41	35	31	25	17	18	21			
	12	11	8	60	24	26	28	32	18	40			
DbR	35	39	42	55	71	32	35	69	64	62	С		
	29	35	34	45	41	23	80	89	26	24			
	91	92	94	93	105	110	152	35	108	77			
STF	204	204	204	207	207	207	207	207	207	208	С		
	208	208	208	209	211	211	211	211	211	211			
	211	211	211	211	211	211	211	211	212	212			
T	36	38	38	37	38	39	40	38	39	38	ДВ		
	38	36	35	38	37	39	38	39	40	38			
	40	39	37	36	38	38	39	37	40	38			
H	65	65	65	70	70	72	72	71	70	68	В		
	65	68	70	72	71	72	75	77	69	71			
	71	75	74	69	71	71	72	70	68	71			
D	81	85	84	85	81	89	92	94	94	95	ДВ		
	96	98	99	94	92	95	94	93	98	97			
	92	93	97	91	90	92	94	89	91	94			

При налаштуванні правил була вибрана опція задіювати лише правила з лінгвістичними ідентифікаторами «висока» і «критична», тобто фіксувалися лише ІПКС можливість реалізації яких була високою. Під час проведення експериментального дослідження в змодельованому середовищі СВІПКС було виявлено 31 411 станів, характерних для певних ІПКС, причому рівень можливості реалізації виявлених станів мав значення «критична» у 1397 випадках, а «висока» – 30014. Загальна статистика відповідно до типу фіксованого ІПКС наведена в вигляді таблиці 4.4, а звіт представлений на рис. 4.16.

Оцінювання критичності ситуації під впливом ІПКС. За допомогою СОКС була проведена оцінка критичності різних ситуацій, спричинених впливом ІПКС. В процесі дослідження на основі розроблених еталонів множини оціночних

параметрів з врахування їх КВ та проведення фазифікації поточних значень отримана оцінка критичності ситуації за виразом (3.3) та 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. Отриманий результат підтвердив адекватність розроблених еталонів і коректність вибору множини оціночних параметрів.

Таблиця 4.4

Результати роботи СВІПКС

Кількість змодельованих ситуацій (станів ІС)	ІПКС	Кількість станів, характеристики яких відповідають реалізації ІПКС	Кількість виявлених ІПКС	
			з впевненістю щодо можливості реалізації «Критична»	з впевненістю щодо можливості реалізації «Висока»
110 000	Разом	31 411	1 397	30 014
	ZL	10 504	275	10 229
	SP	4 753	151	4 602
	DD	4 070	7	4 063
	VA	3 797	176	3 621
	ZK	8 287	788	7 499

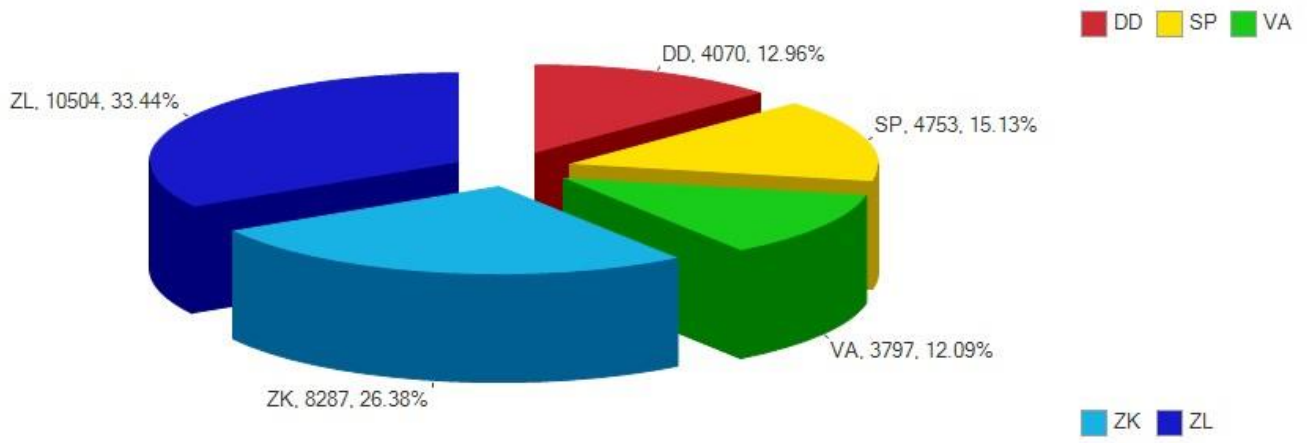


Рис. 4.16. Вікно звіту «Виявлення ІПКС»

Шляхом експертного порівняння з використання методу ППВКК були встановлені КВ для оціночних параметрів землетрусу і DDOS-атаки. Так були отримані наступні КВ нечітких оціночних параметрів: $\Omega_1 = 0{,}014$, $\Omega_2 = 0{,}144$, $\Omega_3 = 0{,}162$, $\Omega_4 = 0{,}107$, $\Omega_5 = 0{,}1$, $\Omega_6 = 0{,}192$, $\Omega_7 = 0{,}013$, $\Omega_8 = 0{,}072$, $\Omega_9 = 0{,}052$, $\Omega_{10} = 0{,}047$, $\Omega_{11} = 0{,}035$, $\Omega_{12} = 0{,}028$, $\Omega_{13} = 0{,}034$ – для землетрусу; $\Omega_1 = 0{,}088$, $\Omega_2 = 0{,}072$, $\Omega_3 = 0{,}05$, $\Omega_4 = 0{,}059$, $\Omega_5 = 0{,}035$, $\Omega_6 = 0{,}093$, $\Omega_7 = 0{,}034$, $\Omega_8 = 0{,}055$, $\Omega_9 = 0{,}148$,

$\Omega_{10} = 0{,}064$, $\Omega_{11} = 0{,}078$, $\Omega_{12} = 0{,}024$, $\Omega_{13} = 0{,}2$ – для DDOS. Наприклад, вікно розрахунку КВ DDOS зображено на рис. 4.17

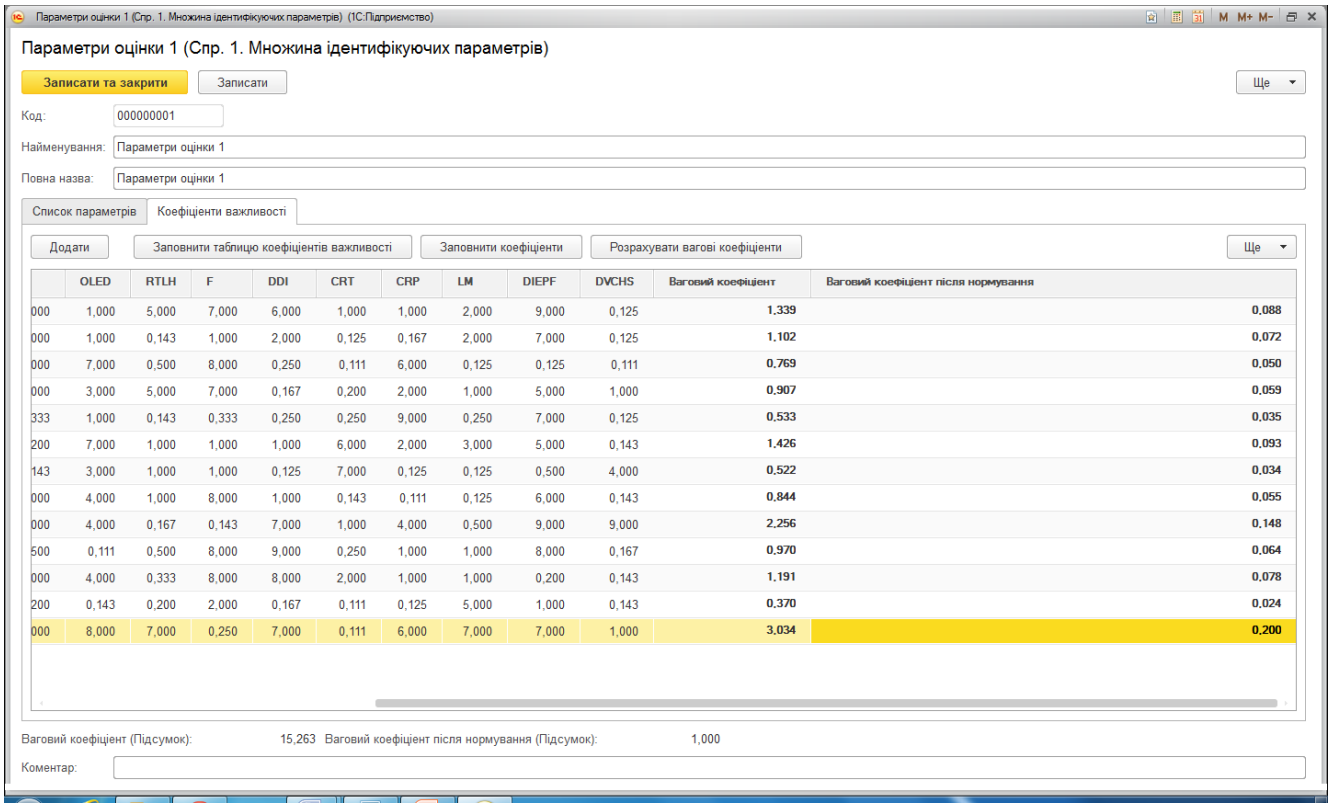


Рис. 4.17. Вікно розрахунку КВ для DDOS

Виміряні та аналітичні дані (наприклад, експертна інформація з звітів щодо КС, їх розвитку різноманітних служб і організацій) заносяться до таблиці і після процесу фазифікації визначаються значення оціночних параметрів та обраховується показник рівня критичності в нечіткій формі за виразом (3.3), що далі після дефазифікації переводяться в чітку форму (див. (3.6)), а результати відображаються на індикаторі критичності ситуації. В табл.. 4.5. наведені результати оцінки критичності ситуації в зоні землетрусу на момент виникнення КС.

Таблиця 4.5

Результати оцінювання СОКС критичності ситуації в зоні землетрусу

Параметр	КВ	НЧ, що характеризує значення параметра	Дефазифіковане значення
TR	0,014	{0/0; 1/0; 0/0,25}	0
DVF	0,144	{0/0; 1/0,25; 0/0,5}	25
GS	0,162	{0/0,25; 1/0,5; 0/0,75}	50
OS	0,107	{0/0,5; 1/0,75; 0/1}	75
OLED	0,1	{0/0,75; 1/1; 0/1}	100

Продовження табл. 4.5

RTLH	0,192	{0/0; 1/0,05; 0/0,3}	5
F	0,013	{0/0,05; 1/0,3; 0/0,55}	30
DDI	0,072	{0/0,3; 1/0,55; 0/0,8}	55
CRT	0,052	{0/0,55; 1/0,8; 0/1}	80
CRP	0,047	{0/0,125; 1/0,375; 0/0,625}	37,5
LM	0,035	{0/0,375; 1/0,625; 0/0,875}	62,5
DIEPF	0,028	{0/0,25; 1/0,5; 0/0,75}	50
DVChS	0,034	{0/0,625; 1/0,875; 0/1}	87,5
RD	-	-	1,05
RM	-	-	1,25
LCS	-	{0/0,2671; 1/0,4752; 0/0,69335}	47,52

Для відображення показника рівня критичності ситуації в лінгвістичній формі здійснюється процедура визначення УВХ між термами оціночного еталону та рівнем LCS. Провівши необхідні обчислення УВХ, використавши (3.5 і 3.6) за допомогою СОКС отримали, шо поточний рівень критичності ситуація «Середній»

Крім того, оцінка проводилась на різних стадіях КС, що дало змогу показати динаміку розвитку ситуації і оцінити адекватність задіяних контрзаходів. Результати відображені в таблиці 4.6, в якій параметр розташовані в порядку зростання рівня критичності. На рисунку 4.17 наведений індикатор критичності ситуації в процесі розвитку ІПКС (КС) для землетрусу.

Таблиця 4.6

Оцінка критичності ситуації на різних стадіях розвитку КС

Параметр	Значення в момент виникнення інциденту	Значення при безконтрольному розвитку ситуації	Значення після застосування контрзаходів
F	22	30	20
TR	0	0	0
DIEPF	42	50	40
DVChS	75	87,5	60
LM	38	62,5	22
CRP	30	37,5	10
CRT	65	80	45
DDI	42	55	30
OLED	90	100	81
OS	52	75	49
DVF	15	25	20
GS	25	50	33
RTLH	0	5	3
RD	1,15	1,45	0,85
RM	1,35	1,6	0,95
LCS	42,32	47,52	35,14

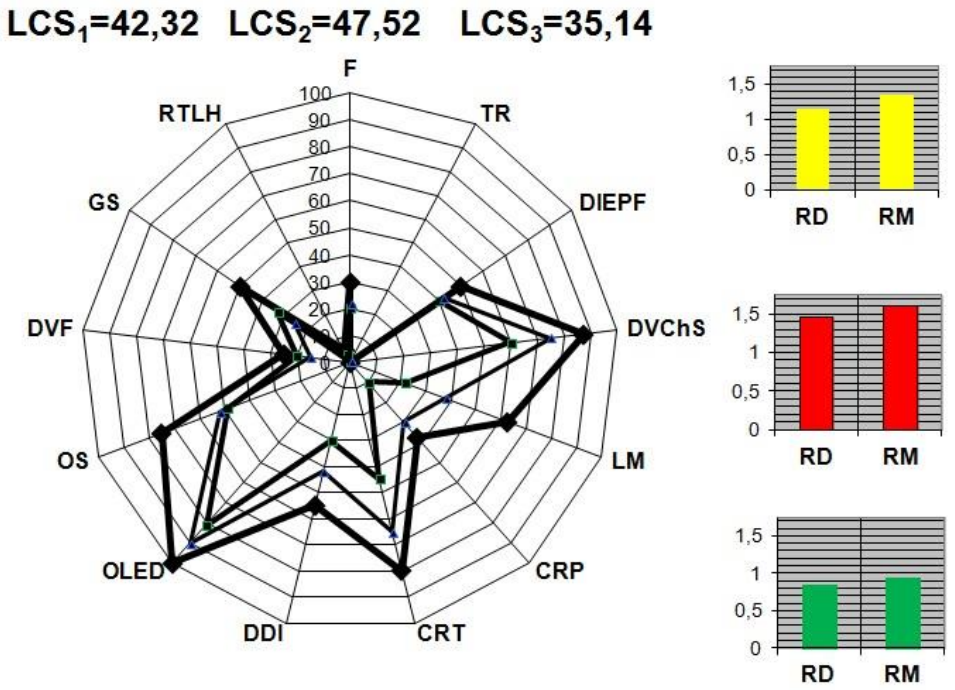


Рис. 4.17. Індикатор рівня критичності ситуації в зоні землетрусу на стадіях виникнення, розвитку та ліквідації КС після застосування контрзаходів

Аналогічно проводилась оцінка DDOS-атаки. Отримані результати показані в вигляді таблиці 4.7 та рисунка 4.18, на якому зображений результат порівняння поточного рівня критичності ситуація з оціночним еталоном за методом УВХ.

Таблиця 4.7

Результати оцінювання СОКС критичності ситуації внаслідок відмови почтового серверу через DDOS-атаку

Параметр	КВ	НЧ, що характеризує значення параметра	Дефазифіковане значення
TR	0,088	{0/0,75; 1/1; 0/1}	100
DVF	0,072	{0/0,5; 1/0,75; 0/1}	75
GS	0,05	{0/0; 1/0; 0/0,25}	0
OS	0,059	{0/0,75; 1/1; 0/1}	100
OLED	0,035	{0/0,5; 1/0,75; 0/1}	75
RTLH	0,093	{0/0; 1/0; 0/0,25}	0
F	0,034	{0/0; 1/0; 0/0,25}	0
DDI	0,055	{0/0,75; 1/1; 0/1}	100
CRT	0,148	{0/0,25; 1/0,5; 0/0,75}	50
CRP	0,064	{0/0; 1/0; 0/0,25}	0
LM	0,078	{0/0,5; 1/0,75; 0/1}	75
DIEPF	0,024	{0/0,25; 1/0,5; 0/0,75}	50
DVChS	0,2	{0/0,5; 1/0,75; 0/1}	75
RD	-	-	1,75
RM	-	-	0
LCS	-	{0/0,64; 1/0,82; 0/1}	82

Для відображення показника рівня критичності ситуації в лінгвістичній формі здійснюється процедура визначення УВХ між термами оціночного еталону та рівнем LCS. Результат процедури УВХ зображений на рисунку 4.8

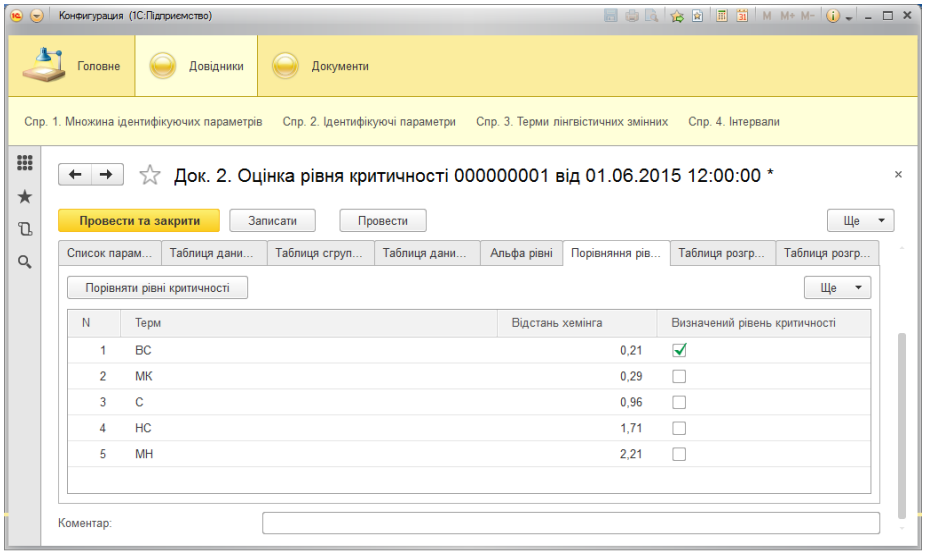


Рис. 4.18. Визначення лінгвістичної змінної, що відповідає поточному рівню критичності в СОКС

Таким чином результат показаний в лінгвістичній формі, тобто визначений рівень «Максимальний» для ситуації, спричиненої відмовою обслуговування на почтовому сервері.

Аналогічно проводилась оцінка на різних стадіях розвитку КС. Результати відображені в таблиці 4.8, в якій параметр розташовані в порядку зростання рівня критичності. На рисунку 4.19 наведений індикатор критичності ситуації в процесі розвитку ІПКС (КС) для відмови серверу внаслідок DDOS-атаки.

Таблиця 4.8

Оцінка критичності ситуації на різних стадіях розвитку КС

Параметр	Значення в момент виникнення інциденту	Значення при безконтрольному розвитку ситуації	Значення після застосування контрзаходів
DVChS	66	75	35
DIEPF	30	50	22
F	0	0	0
OLED	60	75	45
GS	0	0	0
DDI	82	100	61
OS	65	100	35
CRP	0	0	0
DVF	60	75	50
LM	50	75	40

Продовження табл. 4.8

TR	80	100	50
RTLH	0	0	0
CRT	30	50	15
RD	1,25	1,75	0,75
RM	0	0	0
LCS	67	82	51

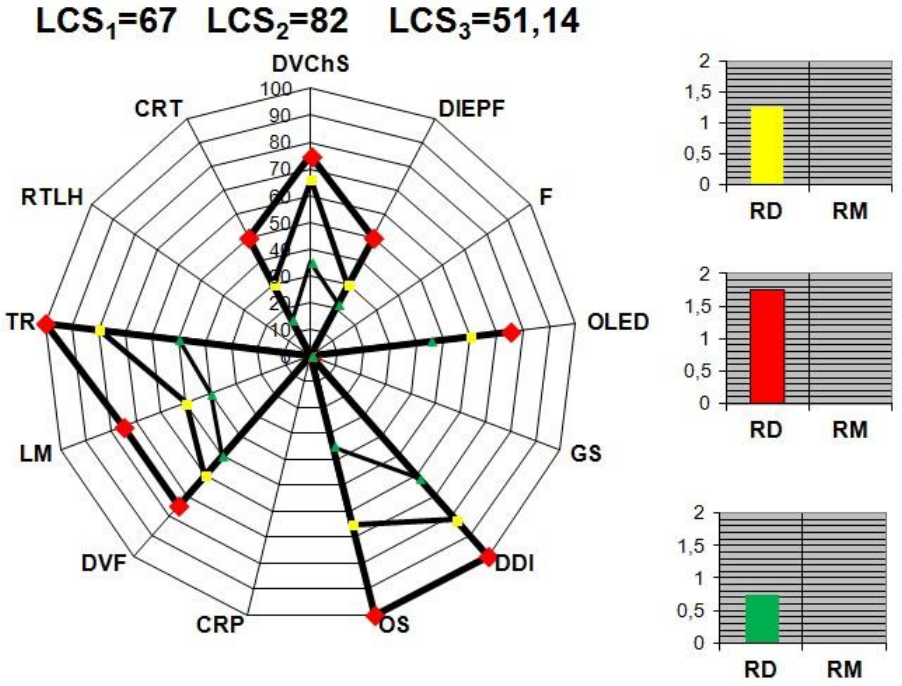


Рис. 4.19. Індикатор рівня критичності ситуації, спричиненої DDOS-атакою сервера на стадіях виникнення, розвитку КС та її ліквідації після застосування контрзаходів

4.5. Висновки до четвертого розділу

1. Розроблено методику проведення експериментального дослідження, у якій обґрунтовано доцільність вибору бази експерименту, визначено гіпотезу, мету та задачі експерименту, вхідні, вихідні параметри та крок їх дискретизації, сформовані критерії дослідження, визначені основні засоби, які використовуються для проведення експерименту, а також послідовність необхідних дій.

2. На основі методу виявлення інцидентів/потенційних кризових ситуацій та структури системи виявлення інцидентів/потенційних кризових ситуацій розроблений програмний засіб «*СВІПКС v.1.0*» в розробницькому середовищі 1С Підприємство 8.3. До складу програмного забезпечення входять об’єкти типу «Довід-

ники» («Множина ідентифікуючих параметрів», «Ідентифікуючі параметри», «Терми лінгвістичних зміних», «Інтервали», «Види ІПКС», «Лінгвістичні ідентифікатори можливості реалізації ІПКС») та «Документи» («Формування еталонів», «Набори евристичних правил», «Оцінка поточного стану середовища»). В ньому реалізується процеси виявлення інцидентів, що потенційно здатні спровокувати кризові ситуації в інформаційній сфері.

3. На основі методу оцінки критичності ситуацій та структури системи оцінки критичності ситуації розроблений програмний засіб «*СВОКС v.1.0*» в розробницькому середовищі 1С Підприємство 8.3. До складу програмного забезпечення входять об'єкти типу «Довідники» («Множина оціночних параметрів», «Оціночні параметри», «Терми лінгвістичних зміних» та «Інтервали») та «Документи» («Еталони», «Оцінка рівня критичності»). В ньому реалізується процеси обрахунку показника рівня критичності поточної ситуації та створення індикатора рівня критичності, що відображає динаміку розвитку кризової ситуацій, що виникла в інформаційній системі.

4. Були проведені експериментальні дослідження, що полягали в: 1) перевіркі точності та достовірності роботи «*СВІПКС v.1.0*», моделей та методів, на яких вона заснована, шляхом виявлення промодельованих поточних станів інформаційної системи, що можна характеризувати як відповідні для реалізації окремих інцидентів; 2) перевірці достовірності та адекватності роботи «*СВОКС v.1.0*», моделей та методів, на яких вона заснована, шляхом оцінювання показника рівня критичності ситуації, спричиненої різними інцидентами на різних етапах їх розвитку. Так було виявлено всі 31411 інцидентів/потенційних кризових ситуацій, причому 1397 інцидентів виявлено за правилом з лінгвістичним ідентифікатором «Критична» та 30014 – «Висока». Також була здійснена оцінка критичності ситуації в різні моменти часу, що підтвердило адекватність реакції системи на зміну 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 рескрсів, розширити їх функціональні можливості та область застосування, а також автоматизувати та прискорити процеси прийняття рішень в умовах впливу КС з врахуванням доцільності їх застосування.

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 сфор-

мувати 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.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Актуальные проблемы гражданской защиты. Материалы одиннадцатой Международной научно–практической конференции по проблемам защиты населения и территорий от чрезвычайных ситуаций. 18-20 апреля 2009 г. / МЧС России. – Н. Новгород: Вектор-ТиС, 2009. – 386 с.

2. Альтерман Б.Д. Обеспечение непрерывности деятельности организации в нештатных ситуаціях / Б.Д. Альтерман, В.И. Дрожжинов, Г.Е. Моисеенко // Jet Info. – №5(120). – 2003. – 28 с.

3. Антикризисное управление: [учеб. для вузов по экон. спец.] / [Э.М. Коротков, А.А. Беляев, Д.В. Валовой и др.]; Под ред. Э.М. Короткова. – М.: Инфра-М, 2002. – 431с.

4. Антикризисное управление человеческими ресурсами / под ред. Н.А. Горелова. – СПб.: Питер, 2010. – 429 с.

5. 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.

6. Брежнев Е.В. Метод диверсификации оценок безопасности критических инфраструктур в условиях неопределенности [Електронний ресурс] / Е.В. Брежнев // Системи озброєння і військова техніка. – 2012. – № 3. – С. 116-120. – Режим доступу: World Wide Web. – URL: http://nbuv.gov.ua/j–pdf/soivt_2012_3_31.pdf.

7. Василенко В. О. Антикризове управління підприємствам [текст] / В.О. Василенко – Київ: ЦУЛ, 2003. – 504с.

8. 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.

9. 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.

10. 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.

11. 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.

12. Гізун А.І., Базова архітектура експертної системи прогнозування та попередження кризових ситуацій / А. І. Гізун, Ю. Б. Іванчук // Безпека інформаційних технологій = Information Technology Security (ITSEC–2012) : II науково–технічна конференція : Збірник тез. – К.: НАУ, 2012. – С. 3-5.

13. Гізун А.І. Евристичні правила на основі логіко–лінвистичних зв'язок для виявлення та ідентифікації порушника інформаційної безпеки / А.І. Гізун, В.В. Волянська, О.В. Гавриленко, А.О. Корченко // Захист інформації. – 2013. – №3 (60). – С.251-257.

14. 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.

15. Гізун А.І. Огляд технологій захисту інформаційних систем для забезпечення безперервності бізнесу / А.І. Гізун, Р.М. Гамрецький, Б.С. Дорошенко // Безпекотворення: питання теорії, практики та правові аспекти. Механізми управління безпекою підприємств в сучасних умовах господарювання: збірник тез. – К.: Видавництво Європейського університету, 2013. – С. 49-52.

16. Гізун А.І. Основні параметри для ідентифікації порушника інформаційної безпеки / А.І. Гізун, В.В. Волянська, В.О. Риндюк, С.О. Гнатюк // Захист інформації. – 2013. –№1 (58). – С.66-75.

17. 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.

18. Гізун А.І., Основні характеристики експертної системи прогнозування та попередження кризових ситуацій / А.І. Гізун, К.П. Ануфрієнко // Захист інформації з обмеженим доступом та автоматизація її обробки = Protection jf Information with Restricted Access and Automation of its Treatment (PIRAT–2012) : IV науково–технічна конференція студентів та аспірантів 9–10 лютого 2012 р. : Збірник тез. – К.: НАУ, 2012. – С. 3-5.

19. 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.

20. 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.

21. Голуб В. Парольная защита [Електронний ресурс]: стаття / В. Голуб // Relga. – 01.12.2009. – №17 (197). – Режим доступу: http://www.relga.ru/ Environ/WebObjects/tgu–www.woa/wa/Main?textid=2516&level1=main&level2= artic les.

22. Горніцька Д.А. Визначення коефщенпв важливості для експертного оцінювання у галузі інформаційної безпеки / Д.А. Горніцька, В.В. Волянська, А.О. Корченко // Захист інформації. – 2012. – №1 (54) . – С. 108-121.

23. Гуляев Э.А. Влияние обратных полярностей в нашей жизни / Э.А. Гуляев, Ф.И. Гуляева. – Одесса: Optimum, 2008. – 7 с.

24. ДК 019:2010 Класифікатор надзвичайних ситуацій. – К.: Держспоживстандарт України, 2010. – 19 с.

25. ДСТУ 3891:2013 Безпека у надзвичайних ситуаціях. Терміни та визначення основних понять [Текст]. – На заміну ДСТУ 3891–99 ; Чинний від 2014–01–01. – Київ : Мінекономрозвитку України, 2014. – IV, 17 с. – (Національний стандарт України).

26. Жарковская Е. П. Антикризисное управление : учебник / Е. П. Жарковская, Б. Е. Бродский, И.Б. Бродский. – 7–е изд., испр. и доп. – М. : Омега-Л, 2011. – 467 с.

27. 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.

28. Еременко Т.К. Онтологическая модель ситуаций для баз знаний систем поддержки принятия решений / Т.К. Еременко, Ю.Г. Пилипенко // Математичні машини і системи. – 2010. – № 3. – С. 69 – 75.

29. 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.

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

31. Использование байесовской сети при разработке экспертных систем с нечеткими знаниями [Электронный ресурс] / А.П. Частиков, И.Ю. Леднева – Электрон. дан. – Краснодар : Кубанский государственный технологический университет, 2005. – Режим доступа: World Wide Web. – URL:-http://ito.su/2000/II/5/5152.html.

32. 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.

33. 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.

34. 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

35. 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.

36. Колісник М.К. Фінансова санкція і антикризове управління підприємством [текст] / М.К. Колісник, П.Г. Ільчук, П.І. Відлий – К.: Кондор, 2007. – 272 с.

37. Комплекс автоматизированных систем раннего выявления чрезвычайных ситуаций и оповещения ОАО «Запорожкокс» /Е.А. Соловьев, Л.Я. Эйдельштейн, А.Н. Севастьянов, С.С. Кацило, Ю.А. Чернышов // Матеріали 11–ї Всеукраїнської наук.–практ. конф. «Організація управління в надзвичайних ситуаціях». К.: ІДУЦЗУ УЦЗУ, 2009. – 425 с.

38. 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/.

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

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

41. Корченко А.А. Метод формирования лингвистических эталонов для систем выявления вторжений / А.А. Корченко // Захист інформації. – Т.16, №1. – 2014. – С. 5-12.

42. 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.

43. 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.

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

45. Корченко А.Г. Интегрированное представление параметров риска / А.Г. Корченко, Е.В. Иванченко, С.В. Казмирчук // Захист інформації – 2011. – №1. – С. 96-101.

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

47. Корченко А.Г. Системы анализа и оценивания рисков информационной безопасности / А.Г. Корченко, А.Е. Архипов, С.В. Казмирчук. – К. : Palmarium Academic Publishing, 2013. – 316 с.

48. Корченко А.О. Кортежная модель формирования набора базовых компонент для выявления кибератак / А.А. Корченко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2014. – В.2 (28). –

С. 29-36.

49. Корченко А.О. Метод α–рівневої номіналізації нечітких чисел для систем виявлення вторгнень / А.О. Корченко // Захист інформації. – 2014. – Т.16. – №4. – С. 304-311.

50. 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.

51. 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.

52. Корченко А.О. Система виявлення аномалій на основі нечітких моделей / А.О. Корченко, Є.В. Паціра, В.В. Волянська // Сучасні тренажерно–навчальні комплекси та системи. – Л.: Інституту проблем моделювання в енергетиці НАН України ім. Г.Є. Пухова, 2007. – Т.2. – С. 56-60.

53. 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.

54. Кузьмин С.П. Автоматизированная система централизованного оповещения категорированного города с численностью населения от 250 до 300 тысяч человек [Текст] / С.П. Кузьмин // Вестник Самарского отраслевого научно–исследовательского института радио, 2009. – С. 65-67.

55. Лігоненко Л.О. Антикризове управління підприємством: теоретико–методологічні засади та практичний інструментарій : монографія / Л.О. Логіненко. – К. : Видавничий центр КНТЕУ, 2001. – 580с.

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

57. 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..

58. 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.

59. Метод прогнозирования последствий и модель автоматизированной системы поддержки принятия решений диспетчера опасного производства при возникновении аварийных ситуаций / В.А. Лыфарь, С.А. Вамболь, Т. В. Гайденко, М.Л. Угрюмов // Открытые информационные и компьютерные интегрированные технологии. – 2011. – № 51. – С. 178-185.

60. 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.

61. Морозов А.А. Ситуационные центры – основа стратегического управления / А.А. Морозов, В.А. Ященко // Математичні машини і системи. – 2003. – № 1. – С. 3-14.

62. Обзор технологий обеспечения непрерывности ИТ–сервисов в чрезвычайных ситуациях / Б.Д. Альтерман, В.В. Задорожный [и др.] // Jet Info: информационный бюллетень. – 2005. – №11(150). – 24 с.

63. Огляд нової платформи «1С Підприємство 8.3» [Електронний ресурс]: стаття. – 05.06.2013. – Режим доступу http://erp–project.com.ua/index.php/uk/novini/item/206–obzor–novoj–platformy–1s–predpriyatie–8–3.

64. Папка Temp в Windows [Електронний ресурс]: стаття. – Режим доступу: http://remontcompa.ru/ 179–papka–temp–v–windows.html.

65. 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.

66. Патент на винахід 45896 А Україна, МПК G08B 25/00. Спеціальна система індивідуального оповіщення про надзвичайні (небезпечні) ситуації / О.Л. Радченко (UA). – № 2001106880; заявл. 10.10.2001; опубл. 15.04.2002, Бюл. № 4. – 2 с.

67. Патент на винахід 60237 А Україна, МПК G05D 16/00, G05D 27/00. Спосіб автоматичного керування в аварійній ситуації на газопроводі / А.Я. Кацеруба (UA); Ю.Г. Мокеєв (UA); О.Ф. Немчин (UA); Ф.О. Павленко (UA);

В.П. Рогатін (UA); В.С. Тарашевський (UA); В.Г. Чернишов (UA). – № 2003054939; заявл. 29.05.2003; опубл. 15.09.2003, Бюл. № 9. – 3 с.

68. Патент на винахід 65121 А Україна, МПК E21F 17/18 (2007.01), G08B 31/00. Автоматизована система протиаварійного захисту шахти / В.Г. Курносов (UA); В.В. Сіненко (UA); Я.Л. Красік (UA); П.Я. Большаков (UA); Г.В. Курносов (UA); Є.Д.Дубов (UA); П.Є.Мухін (UA); В.М.Сірченко (UA); О.А.Сіроткін (UA). – № 2003065179; заявл. 05.06.2003; опубл. 15.03.2004, Бюл. № 3. – 4 с.

69. Патент на винахід 67490 А Україна, МПК E21C 35/24 (2007.01). Спосіб протиаварійного захисту шахти / В.Г. Курносов (UA); В.В. Сіненко (UA); Г.В. Курносов (UA); В.М. Сирченко (UA); О.А. Сіроткін (UA); Я.Л. Красік (UA); П.Я. Большаков (UA); Є.Д. Дубов (UA); П.Є. Мухін (UA). – № 2003109045; заявл. 06.10.2003; опубл. 15.06.2004, Бюл. № 6. – 2 с.

70. Патент на корисну модель 20114 А Україна, МПК G06Q 10/00. Спосіб збору, аналізу інформації, прийняття рішень та оповіщення про виникнення позаштатної ситуації і пристрій для його здійснення / О.В. Грецов (UA). – № 94117818; заявл. 30.11.1994; опубл. 25.12.1997, Бюл. № 6. – 7 с.

71. Патент на корисну модель 32834 Україна, МПК G08B 19/00. Система раннього виявлення надзвичайних ситуацій / Л.П. Пашкевич (UA). – № u200805031; заявл. 04.03.2010; опубл. 12.04.2010, Бюл. № 7. – 3 с.

72. Патент на корисну модель 41967 Україна, МПК G06F 11/00. Комп'ютерна система моніторингу і визначення місця аварії силових мереж сцб / Б.С. Стогній (UA); М.Ф. Сопель (UA); О.І. Стасюк (UA); В.Л. Тутик (UA); І.О. Щербакова (UA); А.Л. Желєзняк (UA); Л.Л. Гончарова (UA); Є.Г. Подлєсних (UA). – № u20080819; заявл17.06.2008; опубл. 25.06.2009, Бюл. № 12. – 12 с.

73. Патент на корисну модель 45451 Україна, МПК E21F 5/00, E21C 39/00. Спосіб прогнозування аварійних ситуацій в підземних гірничих виробках / В.І. Муравейник (UA); С.О. Алексеєнко (UA); Ю.Ф. Булгаков (UA); В.І. Король (UA); І.А. Шайхлісламова (UA). – № u200905789; заявл. 05.06.2009; опубл. 10.11.2009, Бюл. № 21. – 5 с.

74. Патент на корисну модель № 47889 Україна, МПК (2006) E21F5/00, E21C 39/00. Спосіб прогнозування викидонебезпечності масиву гірських порід / В.І. Гаркушенко та ін. (Україна). – № 2001107074; Заявл.18.10.2001; опубл.

15.07.2002, Бюл. № 8. – 6 с.

75. Патент на корисну модель 49115 Україна, МПК G08C 19/00, G08B 19/00, G08B 21/00. Система раннього виявлення надзвичайних ситуацій (СРВНС) / А.П. Йора (UA); С.М. Сидоров (UA). – № u201002449; заявл. 04.03.2010; опубл. 26.04.2010, Бюл. № 8. – 4 с.

76. Патент на корисну модель 49154 Україна, МПК G06Q 10/00. Інтегрована інформаційно–аналітична система моніторингу та моделювання антикризового розвитку підприємства / В.А. Корестильов (UA). – № 200909074 ; заявл. 02.09.2009 ; опубл. 26.04.2010, Бюл. № 8. – 5 с.

77. Патент на корисну модель 53753 Україна, МПК G08B 19/00. Система раннього виявлення надзвичайних ситуацій / В.І. Ліпчанський (UA); І.В. Плотников (UA); Д.В. Плотніков (UA). – № u201009986; заявл. 12.08.2010; опубл. 11.10.2010, Бюл. № 19. – 4 с.

78. Патент на корисну модель 79381 Україна, МПК G08B 19/00, G08B 21/00, G01W 1/02, G08C 17/00. Система раннього виявлення надзвичайних ситуацій / Г.О. Федосов, О.О. Юр'єв, В.В. Магда, А.В. Леденьов, С.А. Матвієнков, С.М. Сидоров, О.В. Меркулов (UA). – № u201220210; опубл. 25.04.2013, Бюл. № 8. – 5 с.

79. Петренко С.А Управление информационными рисками. Экономически оправданная безопасность / С.А. Петренко, С.В. Симонов. – М.: Компания АйТи, ДМК Пресс, 2004. – 384 с.

80. Петренко С.А. Управление непрерывностью бизнеса. Ваш бизнес будет продолжаться / С.А. Петренко, А.В. Беляєв – М.: ДМК–Пресс, Компания АйТи, 2011. – 400 с.

81. Познякова, Е. И. Оценка директивного времени восстановления (RTO) информационных систем / Е. И. Познякова // Вестник РГГУ. – 2009. – № 10. – С. 122–131.

82. Про Державну програму авіаційної безпеки цивільної авіації: закон України № 545–IV / Верховна Рада України // Відомості Верховної Ради України – 25.04.2003р. – № 17. – стаття 140.

83. Про затвердження Загальних вимог до систем фізичного захисту ядерних установок та ядерних матеріалів і Загальних вимог до систем фізичного захи-

сту ядерних матеріалів при їх перевезенні : Наказ № 156 від 28.08.2008 / Держатомрегулювання України // Офіційний вісник України – 03.11.2008. – № 81. – с. 164. – ст. 2753.

84. Про затвердження Методичних рекомендацій щодо загальних підходів до застосування страховиками стрес–тестів : Розпорядження № 6496 від 05.12.2006 / Державна комісія з регулювання ринків фінансових послуг України. – Режим доступу: World Wide Web. – URL: http://uazakon.com/documents/date_8u/pg_grwksy.htm.

85. 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.

86. Про затвердження Програми підготовки авіаційного персоналу в галузі авіаційної безпеки: наказ від 17.02.2003 N 109 / Міністерство транспорту України // Офіційний вісник України. – 08.05.2003р. – № 17. – с. 276. – ст. 797.

87. Ремизова О. Управление непрерывностью вашего бизнеса / Ольга Ремизова, Сергей Петренко // IT Manager. – 2004. – №1(13). – Режим доступу: World Wide Web. – URL: http://citcity.ru/11199/

88. Рубан В.М. Теоретичні аспекти кризи та антикризового управління / В.М. Рубан // Вісник ОНУ імені І.І. Мечникова. – 2014. – Т. 19. – Вип. 2/2. – С. 154–157.

89. Самуэльсон П.А. Економіка / П.А. Самуэльсон, В.Д Нордхаус. – М.: Вильямс, 2014. – 1360 с.

90. Стасюк А.И. Базовая модель параметров для построения систем выявления атак / А.И. Стасюк, А.А. Корченко // Захист інформації. – 2012. – № 2 (55). – С. 47-51.

91. 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.

92. Суханов Д.В. Программный страт модели управления кризисными ситуациями. / Д.В. Суханов // Вестник СГУТиКД. – 2012. – № 2 (20) . – С. 106–110.

93. Теоретические основы и практика оперативного прогнозирования

аварийных ситуаций в шахтах / В.И. Муравейник, С.А. Алексеенко, Ю.Ф. Булгаков, И.А. Шайхлисламова, В.И. Король // Науковий вісник НГУ. – 2009. – № 9. – С. 46-50.

94. Цехмістрова Г.С. Основи наукових досліджень Навчальний посібник. – Київ: Видавничий Дім «Слово», 2003.– 240 с.

95. Чернявский А.Д. Антикризисное управление: Учеб. Пособие / А.Д. Чернявский. – К.:МАУП, 2000. – 208с.

96. AS/NZS 5050 Business continuity. Managinig disruption–related risk – Standards Australia, 2010. – 53p.

97. Augustine N.R. Managing the crisis you tried to prevent / N.R. Augustine // Harvard Business Review. – 1995. – 73(6). – P. 147-158.

98. BCMpedia. Definition of Business Continuity and Disaster Recovery Terminologies [electronic resource]. – 2008. – Mode of Acces: World Wide Web. – URL: http://www.bcmpedia.org.

99. Bird L. Dictionary of Business Continuity Management Terms / Lyndon Bird. – FBCI, 2011. – 37p.

100. BS25999–1:2006 Business continuity management. Code of practice– BSI British Standards, 2006 – 28p.

101. BS25999–2:2007 Business continuity management. Specification – BSI British Standards, 2007. – 38p.

102. CAN/CSAZ731 – M91 Emergency Planning for Industry/ – Canadian Standards Association, Toronto, Ontario, 1991. – (A National Standard of Canada).

103. Caplan G. Principles of Preventive Psychiatry / G. Caplan. –, New York: Basic Books, Inc., 1964. – 320p.

104. Caplan G. Support Systems and Community Mental Health: Lectures on concept development / G. Caplan. – New York: Behavioral Publications, 1974. – 267p.

105. Coombs W.T. Conceptualizing crisis communication / W.T. Coombs // Handbook of crisis and risk communication. – New York : Routledge, 2009. – P. 100 - 119.

106. Coombs W.T. Crisis Management and Communication. Institute for Public Relations / W.T. Coombs. [electronic resource]. – 2007. – Mode of Acces: World Wide Web. – URL: http://www.instituteforpr.org/topics/crisis–management–and–communi

cations/.

107. Coombs W.T. Helping Crisis Managers Protect Reputational Assets Initial Tests of the Situational Crisis Communication Theory / W.T. Coombs, S.J. Holladay // Management Communication Quarterly. – 2002. – 16(2). – P. 165-186.

108. Coombs W.T. Ongoing crisis communication: Planning, managing and responding / Coombs W.T. – 2nd edition. – CA: Sage, 2007. – 224 p.

109. Coombs W. T. Protecting organization reputations during a crisis: The development and application of situational crisis communication theory / W.T. Coombs // Corporate Reputation Review. – 2007. – 10(3). – P. 163-176.

110. CSA Z1600–14 Emergency Management and Business Continuity Programs. – Canadian Standards Association, 2014. – 84 p.

111. Di Maio Paola. An open Ontology for open source emergency response systems [Електронний ресурс] / Paola Di Maio. – Mode of Acces: World Wide Web. – URL: http:www.mfu/as/th.

112. EM–DAT: The OFDA/CRED International Disaster Database [Електронний ресурс] / UCL – Brussels, Belgium. – Mode of Acces: World Wide Web. – URL: http: //www.em–dat.net.

113. Fearn–Banks K. Crisis communications: A casebook approach / K. Fearn–Banks. Mahwah. – NJ: Lawrence Erlbaum Associates, 2007. – 408 p.

114. Fink S. Crisis management: Planning for the inevitable / S. Fink. – New York: iUniverse, 200. – 245 p.

115. 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». – Volume 1. – K.: NAU, 2014. – P. 1.11.40–1.11.44.

116. Guha–Sapir D. Annual Disaster Statistical Review 2010 [Електронний ресурс] / Debby Guha–Sapir, Femke Vos, Regina Below, Sylvain Ponserre // Centre for Research on the Epidemiology of Disasters (CRED). – Mode of Acces: World Wide Web. – URL: http://www.cred.be/sites/default/files/ADSR_2010.pdf.

117. Harris S. CISSP Certification All–in–One Exam Guide / S. Harris. – McGraw–Hill Osborne Media, 2010. – 5th edition. – 1216 p.

118. Harrison, S. Disasters and the media: managing crisis communications / S. Harrison. – Basingstoke: Macmillan Press, 1999. – 238 p.

119. Heath R.L. Strategic Issues Management: Organizations and Public Policy Challenges. / Robert L. Heath, Michael J. Palenchar. – Thousand Oaks, CA: Sage, 2008. – 403 p.

120. Hiles A. Definitive Handbook of Business Continuity Management / Andrew Hiles. – 2nd edition. – Wiley, 2008. – 666p.

121. P Hwang P. Anatomy of organizational crises / Peter Hwang, J. David Lichtenthal // ISBM Report 28. – 1999. – 37p.

122. Jaques T. Issue management and crisis management: An integrated, non–linear, relational construct / T. Jaques // Public Relations Review. – 2007. – 33(2). – P.147–157.

123. Kang C. Bayesian belief network–based advisory system for operational availability focused diagnosis of complex nuclear power systems / C. Kang, M. Golay // Expert Systems with Applications. – Volume 17. – Issue 1. – 1999. – P. 21-32.

124. Killmeyer Jan. Information Security Architecture: An Integrated Approach to Security in the Organization / Jan Killmeyer. – Second Edition. – Auerbach Publications, 2006. – 424 p.

125. Lerbinger O. The Crisis Manager: Facing Risk and Responsibility / O. Lerbinger. – New Jersey: Lawrence Elbaum Associates Publishers, 1997. – 370 p

126. Lindemanne E. Symptomatology and management of acute grief / Erich Lindemanne // American Journal of Psychiatry/ – 1944. – pp. 141 -148.

127. Mejri M. Crisis Management: Lessons Learnt from the BP Deepwater Horizon Spill Oil / Mohamed Mejri, Daniel De Wolf // Business Management and Strategy. – 2013. – Vol. 4. – №. 2. – P. 67-90.

128. Meyers G.C. Managing Crisis: A Positive Approach / G.C. Meyers. – Boston: Houghton Mifflin, 1988. – 271 p.

129. Miller D. Exposing the errors: An examination of the nature of organizational crisis, in / D. Miller. // Responding to crisis: A Rhetorical approach to crisis communication. – Mahwah, NJ, London: Lawrence Erlbaum Associates, 2004. –19 - 31 p.

130. Mitroff I.I. Can Your Company Handle a Crisis / I.I. Mitroff, T. Pauchant, P.

Shrivastava // *Business and Health* . – 1989. – №. 7. – P. 41-44.

131. Mitroff I.I. Corporate tragedies: Product tampering, sabotage, and other catastrophes / I.I. Mitroff, R.H. Kilmann. – New York: Praeger, 1984. – 140 p.

132. Myers K. N. Total Contingency Planning for Diasters: Managing Risk... Minimizing Loss... Ensuring Business Continuity / K. N. Myers. – John Wiley and Sons, Inc., 1993. – 270 p.

133. NFPA 1600. Recommended Practice on Disaster Management. – US: National Fire Prevention Association, 2000. – NFPA, 1 Batterymarch Park, Quincy, 2013. – 66 p.

134. NIST SP 800–34 Rev. 1. Contingency Planning Guide for Federal Information Systems. – Gaithersburg, MD, United States: National Institute of Standards & Technology, 2010 – 150p.

135. Patent US 006266579B1 USA, Int. Cl. G01M 1/38. System for reducing disaster damage / Mohammad Reza Baraty (USA). – № 09/022,667; declared 12.02.1998; published 24.07.2001. – 18 p.

136. Patent US 007035765B2 USA, Int. Cl. G06F 11/30. Disaster predicting method, disaster predicting apparatus, disaster predicting program, and computer–readable recording medium recorded with disaster predicting program / Shuichi Tanahashi. – № 10/341,479; declared 14.01.2003; published 25.04.2006. – 13 p.

137. Patent US 007436294B2 USA, Int. Cl. G08B 29/00. Method and apparatus for disaster prevention / Susumu Saga (JP); Yasuyuki Kawaida (JP); Hiroko Kaneko (JP). – № 11/193,454; declared 04.08.2005; published 14.10.2008. – 11 p.

138. Patent US 007603259B2 USA, Int. Cl. G06F 7/60. Method and apparatus for quantifying an impact of a disaster on a network / Ahmad M. Jrad (US); Blesson Mathews (US); Thomas B. Morawski (US); Louise F. A. Spergel (US). – № 11/238,919; declared 29.09.2005; published 13.10.2009. – 24 p.

139. Patent US 007734245B2 USA, Int. Cl. G01V3/00 , G01V 7/00, G06G 7/48, G09B 9/56, G01S13/00. Statistical–deterministic approach to natural disaster prediction / Sai Ravela (USA); Kerry A. Emanuel (USA). – № 11/388,185; declared 23.05.2006; published 08.06.2010. – 30 p.

140. Patent US 007932823B2 USA, Int. Cl. G08B 21/00. Disaster noticing system, disaster noticing server, disaster reporting terminal method, and program / Ry-

osuke Komiya (JP); Hiroaki Kuba (JP); Naoki Kuwamori (JP). – № 12/183,012; declared 30.07.2008; published 26.04.2011. – 25 p.

141. Patent US 20060079200A1 USA, Int. Cl. H04M 11/04. Disaster system control method and disaster system control apparatus / Kiyoshi Hirouchi (JP); Yayoi Itoh (JP); Naoyuki Kakizaki (JP); Saiki Kawamura (JP); Satoru Abe (JP); Yoshikazu Takeda (JP); Takahito Suzuki (JP); Hiroki Yokoyama (JP). – № 11/289,744; declared 29.11.2005; published 13.04.2006. – 46 p.

142. Patent US 20060111927A1 USA, Int. Cl. G06Q 99/00, G07G, 1/00, G06F 17/30. System, method and program for estimating risk of disaster in infrastructure / Etienne de Sereville (FR). – № 11/272,299; declared 10.11.2005; published 25.05.2006. – 11 p.

143. Patent US 20070033153A1 USA, Int. Cl. G06F 15/18. Disaster prediction system / Ryutaro Yamanaka (JP); Hiroyuki Motozuka (JP); Mitsuru Uesugi (JP). – № 10/577,473; declared 25.10.2004; published 07.02.2007. – 35 p.

144. Patent US 20080172262A1 USA, Int. Cl. G06Q 10/00. Method and system for disaster mitigation planning and business impact assessment / Lianjun An (US); Stephen John Buckley (US); Ching–Hua Chen–Ritzo (US); Pawan Raghunath Chowdhary (US); Thomas Robert Ervolina (US); Daniel A. Ford (US); Igor Frolow (US); Naveen Lamba (US); Young Min Lee (US); Prakaah Mukkarmala (US); Dharmashankar Subramanian (US). – № 11/622,705; declared 12.01.2007; published 17.07.2008. – 13 p.

145. Patent US 20110299666A1 USA, Int. Cl. H04M11/04. Dynamic emergency disaster plan / Christopher R. Hulls (USA). – № 13/214,181; declared 20.08.2011; published 08.12.2011. – 8 p.

146. Pauchant T.C. Transforming the crisis–prone organization: Preventing individual, organizational, and environmental tragedies / T.C. Pauchant, I.I. Mitroff. – San Francisco, CA: Jossey–Bass, 1992. – 275 p.

147. Pearson C. M. From crisis prone to crisis prepared: A framework for crisis management / C.M. Pearson, I.I. Mitroff. The academy of management executive. – 1993. – 7(1). – P. 48-59.

148. Pearson C. M. Reframing crisis management. / C.M. Pearson, J.A. Clair // Academy of management review. – 1998. – 23(1). – P. 59-76.

149. Poal P. Introduction to the theory and practice of crisis intervention / Pilar Poal // Quaderns de Psicologia. – 1990. – 10. – P. 121-140.

150. Regester M., Risk Issues and Crisis Management: A Casebook of Best Practice. / M. Regester, J. Larkin – London: The Institute of Public Relations, 1998. – 264 p.

151. Richardson B. Socio–technical disasters: profile and prevalence. / B. Richardson // Disaster Prevention and Management. – 1994. – 3(4). – P. 41-69.

152. Smith D. Beyond contingency planning: Towards a model of crisis management / D. Smith // Organization and environment. – 1990. – 4(4). – P. 263-275.

153. SS540:2008 Singapore Standard for Business Continuity Management – SPRING Singapore, 2008. – 54p.

154. SEVA4A: An ontology for emergency notification systems accessibility / A. Malizia, T. Onorati, P. Dias [et al.] // Expert systems with Applications. – 2010. – Vol. 37. – Is. 4. – P. 3380 – 3391.

155. Talon M. Determine an acceptable recovery time objective. Learn how to determine an acceptable recovery point objective [Электронный ресурс] / M. Talon // Сайт «TechRepublic». – M., 2008. – Mode of Acces: World Wide Web. – URL: http://articles.techrepublic.com.com/5100–22_11–5294886.html.

156. Taplinj R. Crisis Theory: critique and reformulation / R. Taplinj // Community Mental Health Journal. – 1971. – 7 (l), – P. 13-23.

157. The Federal Response Plan 9230.1–Pl. – Washington, DC: Federal Emergency Management Agency, 1992. – 304p.

158. TIA–942 Telecommunications Infrastructure Standard for Data Centers

159. Van Bon Jan. ИТ СЕРВИС–МЕНЕДЖМЕНТ. Вводный курс на основе ITIL / Jan Van Bon. – Van Haren Publishing, ITSMF Netherlands, 2003. – 72 с.

160. Weber P. Complex system reliability modeling with Dynamic Object Oriented Bayesian Networks (DOOBN) / P.Weber, L. Jouffe // Reliability Engineering and System Safety. – Volume 91. – Issue 2. – 2006. – PP. 149-162.

Додаток А. Відомості щодо впровадження результатів дослідження

Hazon Sp. z o.o.

ul. Poznańska 1 B/9, 71-785 Szczecin
0048 660 766 861
hazon.sp.zoo@gmail.com

Szczecin, 17.03.2015 r.

Akt

впровадження результатів дисертаційної роботи Гізуна Андрія Івановича "Методи та засоби оцінювання параметрів безпеки для виявлення кризових ситуацій в інформаційній сфері" на здобуття наукового ступеню кандидата технічних наук у діяльності компанії Hazon Sp. z o.o.

Даний акт складено про те, що результати дисертаційної роботи Гізуна Андрія Івановича "Методи та засоби оцінювання параметрів безпеки для виявлення кризових ситуацій в інформаційній сфері" впроваджено та використовуються у діяльності компанії Hazon Sp. z o.o.

У процесі написання дисертації автором були розроблені програмні засоби "Система виявлення інцидентів/потенційних кризових ситуацій" та "Система оцінки критичності ситуації", які призначені для виявлення інцидентів/потенційних кризових ситуацій та оцінки показника рівня критичності ситуації, що спричинена їх впливом. Враховуючи особливості внутрішньої побудови та розроблених методів, на яких вони засновані, дані програмні засоби дають змогу забезпечити можливість їх функціонування в умовах нечіткого слабоформалізованого середовища, підвищують ефективність, ступінь автоматизації та швидкість процесів управління кризовими ситуаціями і прийняття рішень в умовах впливу кризових ситуацій, формування планів забезпечення безперервності роботи інформаційних систем та підбору заходів та засобів з ліквідації кризових ситуацій.

Таким чином, результати, отримані Гізуном А.І. під час написання дисертації, дозволили використовувати системи виявлення та оцінювання кризових ситуацій в умовах нечіткості і підвищують ефективність та рівень автоматизації процесів управління кризовими ситуаціями, прийняття рішень та реалізації концепції управління безперервністю бізнесу.

Dyrektor operacyjny — Anna Nagi

HAZON Sp. z o.o.
71-785 Szczecin ul. Poznańska 1B/9
NIP 8513177819

Prezes Zarządu — Władysława Wolańska

HAZON Sp. z o.o.
Władysława Wolańska
Prezes Zarządu

ЗАТВЕРДЖУЮ:

В.о. ректора
Національного авіаційного університету

_____ В.Харченко

"30" червня 2015 р.

АКТ

впровадження у навчальний процес результатів дисертаційної роботи Гізуна Андрія Івановича – "Методи та засоби оцінювання параметрів безпеки для виявлення кризових ситуацій в інформаційній сфері" на здобуття наукового ступеню кандидата технічних наук.

Комісія у складі: голова – завідувач кафедри засобів захисту інформації (ЗЗІ) Козловський В.В., доцент кафедри безпеки інформаційних технологій (БІТ) Казмірчук С.В., доцент кафедри БІТ Гнатюк С.О. склали даний акт про те, що результати дисертаційного дослідження Гізуна Андрія Івановича впроваджені у навчальний процес та використовуються на кафедрах ЗЗІ і БІТ у 2014-2015 навчальному році при викладанні дисциплін "Інформаційна безпека держави", "Безпека інформації в інформаційно-комунікаційних системах" та "Методологія та організація наукових досліджень", що входять до навчальних планів підготовки фахівців у галузі знань "Інформаційна безпека".

№ з/п	Назва роботи, що впроваджується	Форма впровадження	Ефективність від впровадження
	1	2	3
1.	Сучасні системи управління кризовими ситуаціями та стратегії забезпечення безперервності бізнесу	Лекція (Інформаційна безпека держави)	Систематизація навчального матеріалу та надання студентам знань щодо сучасного програмного та апаратного забезпечення систем управління кризовими ситуаціями, основних стратегій забезпечення безперервності бізнесу.
2.	Виявлення інцидентів/потенційних кризових ситуацій та оцінка критичності ситуації, що склалася внаслідок їх впливу	Лабораторна робота (Безпека інформації в інформаційно-комунікаційних системах)	Ознайомлення і навчання студентів виявляти кризові ситуації в інформаційних системах та проводити їх оцінку з використанням комп'ютерних програми "Система виявлення інцидентів/потенційних кризових ситуацій" і "Система оцінювання критичності ситуації".
3.	Методика проведення експериментального дослідження систем виявлення та оцінювання кризових ситуацій	Лабораторна робота (Методологія та організація наукових досліджень)	Надання студентам навичок проведення наукового експерименту на основі вивчення основних положень та етапів експериментального дослідження щодо точності і достовірності виявлення інцидентів та оцінки критичності ситуації з використанням комп'ютерних програми "Система виявлення інцидентів/потенційних кризових ситуацій" і "Система оцінювання критичності ситуації".

Голова комісії,
завідувач кафедри ЗЗІ, д.т.н., проф. В. Козловський
Члени комісії:
доцент кафедри БІТ, к.т.н., доц. С. Казмірчук

доцент кафедри БІТ, к.т.н., доц. С. Гнатюк

САЙФЕР
Системи захисту інформації

ТОВ «Сайфер ЛТД»
Адреса: 04107, Київ, вул. Нагірна, 25
Тел./Факс: (044) 484-46-17, 484-46-12, 483-03-22
E-mail: sales@cipher.kiev.ua
http://www.elpay.com; http://www.cipher.kiev.ua

Вих. №_____
19.11.2014 р.

АКТ

впровадження результатів дисертаційної роботи
Гізуна Андрія Івановича «Методи та засоби оцінювання параметрів безпеки для виявлення кризових ситуацій в інформаційній сфері»
на здобуття наукового ступеню кандидата технічних наук у діяльності
ТОВ «Сайфер ЛТД»

Комісія у складі голови – директора товариства з обмеженою відповідальністю «Сайфер ЛТД», кандидата технічних наук Боровікова О.М., членів комісії – заступника директора з виробництва, кандидата технічних наук Ковтуна В.Ю., керівника продукту «Система управління банківським рахунком через Internet «ELPay» Зацепін О.В., складено цей акт про те, що при розробці продукту «Система управління банківським рахунком через Internet «ELPay» (далі Internet-банкінг «ELPay»), використані результати дисертаційної роботи Гізуна Андрія Івановича «Методи та засоби оцінювання параметрів безпеки для виявлення кризових ситуацій в інформаційній сфері».

У Internet-банкінг «ELPay» використовується система виявлення та оцінювання кризових ситуацій в інформаційній банківській сфері на основі запропонованих інтегрованої моделі представлення інцидентів/потенційних кризових ситуацій, моделей еталонів та евристичних правил, методів виявлення інцидентів/потенційних кризових ситуацій та оцінки критичності ситуації, а також процедури формування індикатора рівня критичності.

Під час розробки Internet-банкінг «ELPay», результати дисертаційної роботи дисертації Гізун А.І. використані у модулі «Anti-Fraud»:

– **Система виявлення інцидентів/потенційних кризових ситуацій**, яка призначена для виявлення інцидентів/потенційних кризових ситуацій, та підсистема захисту фінансових транзакцій. Данна система дозволяє здійснювати моніторинг поточних фінансових транзакцій на наявність ознак потенційних кризових ситуацій (несанкціонованих і підозрілих фінансових транзакцій) в реальному часі в умовах нечіткості.

– **Система оцінки критичності ситуації**, яка призначена для оцінювання показника рівня критичності поточної ситуації (несанкціонованих і підозрілих фінансових транзакцій), яка є наслідком

впливу інцидентів інформаційної безпеки, а також ступеня ймовірної загрози, що дає можливість ефективного підбору адекватних заходів та засобів реагування на них.

Проведено тестування модуля «Anti-Fraud» і встановлено її адекватність та придатність для експертного оцінювання рівня критичності ситуації в реальних умовах.

Отже, результати, отримані Гізуном А.І. під час написання дисертаційної роботи, дозволили підвищити ефективність та рівень безпеки захисту фінансової інформації клієнтів банку у Internet-банкінг «ELPay».

Директор ТОВ «Сайфер ЛТД» О.М. Боровіков

Додаток Б. Лістинг розроблених програмних засобів

1. Лістинги програмного забезпечення «СВІПКС v.1.0»

Загальний модуль ДопПроцедуры

```
&НаСервере
Функция ПолучитьКомбинациюПараметров(СписокПараметров, Инд = 0,
СтрокаТЧДокумента = Неопределено) Экспорт
	Результат = "";
	Если СписокПараметров.Количество() = 0 Тогда
		Возврат Результат;
	КонецЕсли;
	КоличествоВсегоКомбинаций = 1;
	Для Каждого СтрокаТЧ Из СписокПараметров Цикл
		КоличествоВсегоКомбинаций = КоличествоВсегоКомбинаций *
СтрокаТЧ.ІдентифікуючийПараметр.ТермиЛінгвістичнихЗмінних.Количество();
	КонецЦикла;
	ТекИнд = Инд;
	Если ТекИнд < 0 Тогда
		ТекИнд = 0;
	ИначеЕсли ТекИнд >= КоличествоВсегоКомбинаций Тогда
		ТекИнд = КоличествоВсегоКомбинаций - 1;
	КонецЕсли;
	ИндПараметра = 1;
	Для Каждого СтрокаТЧ Из СписокПараметров Цикл
		ИндСоответствия = ?( СтрокаТЧ.ІдентифікуючийПараметр.ТермиЛінгвістичнихЗмінних.Количество() = 0, 0,
ТекИнд % СтрокаТЧ.ІдентифікуючийПараметр.ТермиЛінгвістичнихЗмінних.Количество() );
		Параметр = СтрокаТЧ.ІдентифікуючийПараметр;
		Соответствие =
СтрокаТЧ.ІдентифікуючийПараметр.ТермиЛінгвістичнихЗмінних[ИндСоответствия].Терм;
		Если СтрокаТЧДокумента <> Неопределено Тогда
			СтрокаТЧДокумента["ЛПпар" + ИндПараметра] = Соответствие;
		КонецЕсли; ТекИнд = ?(
СтрокаТЧ.ІдентифікуючийПараметр.ТермиЛінгвістичнихЗмінних.Количество() = 0, 0, Цел(ТекИнд /
СтрокаТЧ.ІдентифікуючийПараметр.ТермиЛінгвістичнихЗмінних.Количество()));
		Результат = Результат + ?(ЗначениеЗаполнено(Результат), ", ", "") + Параметр + " = " + Соответствие;
		ИндПараметра = ИндПараметра + 1;
	КонецЦикла;
	Возврат Результат;
КонецФункции
```

Модуль форми документа GA_ФормуванняЕталонів

```
&НаКлиенте
Процедура ПриОткрытии(Отказ)
	ОбновитьГрафик();
КонецПроцедуры

&НаКлиенте
Процедура МножинаІдентифікуючихПараметрівПриИзменении(Элемент)
	Объект.АналітичніДаніПараметра.Очистить();
	Объект.Еталони.Очистить();
	ОбновитьГрафик();
КонецПроцедуры

&НаКлиенте
Процедура ІдентифікуючийПараметрПриИзменении(Элемент)
	ОбновитьГрафик();
КонецПроцедуры

&НаКлиенте
Процедура ЗаповнитиПоЗамовчуванніюТЧАналітичніДаніПараметра(Команда)
	Объект.АналітичніДаніПараметра.Очистить();
	Объект.Еталони.Очистить();
	МассивТермовЛЗ = ПолучитьТаблицуТермовЛЗ(Объект.ІдентифікуючийПараметр);
	МассивИнтервалов = ПолучитьТаблицуИнтервалов(Объект.ІдентифікуючийПараметр);
	Для Каждого ЭлементЛЗ Из МассивТермовЛЗ Цикл
		Для Каждого ЭлементИ Из МассивИнтервалов Цикл
```

```
                        НоваяСтрока = Объект.АналітичніДаніПараметра.Добавить();
                        НоваяСтрока.ТермЛінгвістичноїЗмінної        = ЭлементЛЗ;
                        НоваяСтрока.Інтервал        = ЭлементИ;
                        НоваяСтрока.Значення        = 0;
                КонецЦикла;
        КонецЦикла;
        ОбновитьГрафик();
КонецПроцедуры

&НаСервере
Функция ПолучитьТаблицуТермовЛЗ(Параметр)
        Возврат Параметр.ТермиЛінгвістичнихЗмінних.ВыгрузитьКолонку("Терм");
КонецФункции

&НаСервере
Функция ПолучитьТаблицуИнтервалов(Параметр)
        Возврат Параметр.Інтервали.ВыгрузитьКолонку("Інтеравал");
КонецФункции

&НаКлиенте
Процедура РозрахуватиЕталон(Команда)
        РозрахунокЕталону();
        ОбновитьГрафик();
КонецПроцедуры

&НаСервере
Процедура РозрахунокЕталону()
        Объект.Еталони.Очистить();
        Если Объект.АналітичніДаніПараметра.Количество() = 0 Тогда
                Возврат;
        КонецЕсли;
        МассивИнтервалов        = ПолучитьМассив("Інтервал");
        МассивТермовЛЗ          = ПолучитьМассив("ТермЛінгвістичноїЗмінної");
        КоличествоИ             = МассивИнтервалов.Количество();
        КоличествоЛЗ            = МассивТермовЛЗ.Количество();
        ТзК = ПолучитьТаблицуЗначений("Інтервал","Значення");
        Кмакс = -1;
        Для Каждого СтрокаТз Из ТзК Цикл
                Если СтрокаТз.Значення > Кмакс Тогда
                        Кмакс = СтрокаТз.Значення;
                КонецЕсли;
        КонецЦикла;
        ТзС = ПолучитьТаблицуЗначений("ТермЛінгвістичноїЗмінної, Інтервал","Значення");
        ТзС.Очистить();
        ИндИ = 0;
        Пока ИндИ < КоличествоИ Цикл
                МассивПоиска1 = ТзК.НайтиСтроки(Новый Структура("Інтервал",  МассивИнтервалов[ИндИ]));
                КСтолбца = МассивПоиска1[0].Значення;
                ИндЛП = 0;
                Пока ИндЛП < КоличествоЛЗ Цикл
                        Если КСтолбца <> 0 Тогда
                                МассивПоиска2           =           Объект.АналітичніДаніПараметра.НайтиСтроки(Новый
Структура("ТермЛінгвістичноїЗмінної, Інтервал", МассивТермовЛЗ[ИндЛП], МассивИнтервалов[ИндИ]));
                                НоваяСтрока = ТзС.Добавить();
                                НоваяСтрока.ТермЛінгвістичноїЗмінної        = МассивТермовЛЗ[ИндЛП];
                                НоваяСтрока.Інтервал        = МассивИнтервалов[ИндИ];
                                НоваяСтрока.Значення        = МассивПоиска2[0].Значення * Кмакс / КСтолбца;
                        Иначе
                                НоваяСтрока = ТзС.Добавить();
                                НоваяСтрока.ТермЛінгвістичноїЗмінної        = МассивТермовЛЗ[ИндЛП];
                                НоваяСтрока.Інтервал        = МассивИнтервалов[ИндИ];
                                Инд1 = ?((ИндИ-1) < 0, КоличествоИ -1, ИндИ-1);
                                Инд2 = ?((ИндИ+1) >= КоличествоИ, 0, ИндИ+1);
                                МассивПоиска3           =           Объект.АналітичніДаніПараметра.НайтиСтроки(Новый
Структура("ТермЛінгвістичноїЗмінної, Інтервал", МассивТермовЛЗ[ИндЛП], МассивИнтервалов[Инд1]));
                                МассивПоиска4           =           Объект.АналітичніДаніПараметра.НайтиСтроки(Новый
Структура("ТермЛінгвістичноїЗмінної, Інтервал", МассивТермовЛЗ[ИндЛП], МассивИнтервалов[Инд2]));
                                НоваяСтрока.Значення = (МассивПоиска3[0].Значение + МассивПоиска4[0].Значение)/2;
                        КонецЕсли;
                        ИндЛП = ИндЛП + 1;
```

```
                КонецЦикла;
                ИндИ = ИндИ + 1;
        КонецЦикла;
        ТЗМ = ТзС.Скопировать();
        ТзМ.Очистить();
        ИндИ = 0;
        Пока ИндИ < КоличествоИ Цикл
                МаксЕл = 0;
                ИндЛП = 0;
                МассивПоиска1 = ТзС.НайтиСтроки(Новый Структура("Інтервал",  МассивИнтервалов[ИндИ]));
                Пока ИндЛП < КоличествоЛЗ Цикл
                        Если МассивПоиска1[ИндЛП].Значення > МаксЕл Тогда
                                МаксЕл = МассивПоиска1[ИндЛП].Значення;
                        КонецЕсли;
                        ИндЛП = ИндЛП + 1;
                КонецЦикла;
                ИндЛП = 0;
                Пока ИндЛП < КоличествоЛЗ Цикл
                        МассивПоиска2 = ТзС.НайтиСтроки(Новый Структура("ТермЛінгвістичноїЗмінної, Інтервал",
МассивТермовЛЗ[ИндЛП], МассивИнтервалов[ИндИ]));
                        НоваяСтрока = ТЗМ.Добавить();
                        НоваяСтрока.ТермЛінгвістичноїЗмінної = МассивТермовЛЗ[ИндЛП];
                        НоваяСтрока.Інтервал = МассивИнтервалов[ИндИ];
                        НоваяСтрока.Значення = ?(МаксЕл = 0, 0, МассивПоиска2[0].Значення / МаксЕл);
                        ИндЛП = ИндЛП + 1;
                КонецЦикла;
                ИндИ = ИндИ + 1;
        КонецЦикла;
        Для Каждого ЭлементЛЗ Из МассивТермовЛЗ Цикл
                Для Каждого ЭлементИ Из МассивИнтервалов Цикл
                        НоваяСтрока = Объект.Еталони.Добавить();
                        НоваяСтрока.ТермЛінгвістичноїЗмінної = ЭлементЛЗ;
                        НоваяСтрока.Інтервал = ЭлементИ;
                        МассивПоиска1 = ТзМ.НайтиСтроки(Новый Структура( "ТермЛінгвістичноїЗмінної,
Інтервал", ЭлементЛЗ, ЭлементИ));
                        //НоваяСтрока.КоордХ = МассивПоиска1[0].Значення;
                        НоваяСтрока.КоордУ = МассивПоиска1[0].Значення;
                        МассивПоиска = Объект.ІдентифікуючийПараметр.Інтервали.НайтиСтроки( Новый
Структура("Інтеравал", ЭлементИ));
                        Если МассивПоиска.Количество() <> 0 Тогда
                                //НоваяСтрока.КоордУ = МассивПоиска[0].Коефіцієнт;
                                НоваяСтрока.КоордХ = МассивПоиска[0].Коефіцієнт;
                        КонецЕсли;
                КонецЦикла;
        КонецЦикла;
КонецПроцедуры

&НаСервере
Функция ПолучитьМассив(ИмяРеквизита)
        Тз = Объект.АналітичніДаніПараметра.Выгрузить();
        Тз.Свернуть(ИмяРеквизита,"");
        Массив = Тз.ВыгрузитьКолонку(ИмяРеквизита);
        Возврат Массив;
КонецФункции

&НаСервере
Функция ПолучитьТаблицуЗначений(ИмяРеквизита, ИмяРесурса)
        Тз = Объект.АналітичніДаніПараметра.Выгрузить();
        Тз.Свернуть(ИмяРеквизита,ИмяРесурса);
        Возврат Тз;
КонецФункции

&НаКлиенте
Процедура ОбновитиГрафік(Команда)
        ОбновитьГрафик();
КонецПроцедуры

&НаСервере
Процедура ОбновитьГрафик()
        ЭтаФорма.ГрафікЕталонів.Очистить();
```

```
        МассивИнтервалов        = ПолучитьМассивИзТЧ(Объект.Еталони, "Інтервал");
        МассивТермовЛЗ          = ПолучитьМассивИзТЧ(Объект.Еталони, "ТермЛінгвістичноїЗмінної");
        ТзДляВывода = Новый ТаблицаЗначений;
        ТзДляВывода.Колонки.Добавить("Серия");
        Для Каждого Элемент Из МассивИнтервалов Цикл
                ИмяКолонки = "" + Элемент;
                ИмяКолонки = СтрЗаменить(ИмяКолонки, " ", "");
                ИмяКолонки = СтрЗаменить(ИмяКолонки, ".", "");
                ИмяКолонки = СтрЗаменить(ИмяКолонки, ",", "");
                ТзДляВывода.Колонки.Добавить(ИмяКолонки);
        КонецЦикла;
        ТзКопия = Объект.Еталони.Выгрузить();
        ТзКопия.Сортировать("ТермЛінгвістичноїЗмінної Возр, Інтервал Возр");
        Для Каждого ЭлементЛП Из МассивТермовЛЗ Цикл
                НоваяСтрока = ТзДляВывода.Добавить();
                НоваяСтрока.Серия = ЭлементЛП;
                МассивПоиска = ТзКопия.НайтиСтроки(Новый Структура("ТермЛінгвістичноїЗмінної", ЭлементЛП));
                Для Каждого ЭлементПоиска Из МассивПоиска Цикл
                        ИмяКолонки = "" + ЭлементПоиска.Інтервал;
                        ИмяКолонки = СтрЗаменить(ИмяКолонки, " ", "");
                        ИмяКолонки = СтрЗаменить(ИмяКолонки, ".", "");
                        ИмяКолонки = СтрЗаменить(ИмяКолонки, ",", "");
                        НоваяСтрока[ИмяКолонки] = ЭлементПоиска.КоордY;
                        ТзДляВывода.Колонки[ИмяКолонки].Заголовок = "" + ЭлементПоиска.КоордX;
                КонецЦикла;
        КонецЦикла;
        ЭтаФорма.ГрафікЕталонів.ТипДиаграммы    = ТипДиаграммы.График;
        ЭтаФорма.ГрафікЕталонів.СерииВСтроках   = Истина;
        ЭтаФорма.ГрафікЕталонів.ИсточникДанных  = ТзДляВывода;
КонецПроцедуры

&НаСервере
Функция ПолучитьМассивИзТЧ(ТЧ, ИмяРеквизита)
        Тз = ТЧ.Выгрузить();
        Тз.Свернуть(ИмяРеквизита,"");
        Массив = Тз.ВыгрузитьКолонку(ИмяРеквизита);
        Возврат Массив;
КонецФункции
```

Модуль об'єкта GA_ФормуванняЕталонів

```
Процедура ОбработкаПроведения(Отказ, РежимПроведения)
        ПроверитьЗаполнениеПолей(Отказ);
        Если Не Отказ ТОгда
                ДвиженияДокумента();
        КонецЕсли;
КонецПроцедуры

Процедура ПроверитьЗаполнениеПолей(Отказ)
        Если Не ЗначениеЗаполнено(МножинаІдентифікуючихПараметрів) Тогда
                Сообщить("Заповніть реквізит <Множина ідентифікуючих параметрів>", СтатусСообщения.Важное);
                Отказ = Истина;
        КонецЕсли;
        Если Не ЗначениеЗаполнено(ІдентифікуючийПараметр) Тогда
                Сообщить("Заповніть реквізит <Ідентифікуючий параметр>", СтатусСообщения.Важное);
                Отказ = Истина;
        КонецЕсли;
        Если АналітичніДаніПараметра.Количество() = 0 Тогда
                Сообщить("Заповніть ТЧ <Аналітичні дані параметра>", СтатусСообщения.Важное);
                Отказ = Истина;
        КонецЕсли;
        Если Еталони.Количество() = 0 Тогда
                Сообщить("Заповніть ТЧ <Еталони>", СтатусСообщения.Важное);
                Отказ = Истина;
        КонецЕсли;
КонецПроцедуры

Процедура ДвиженияДокумента()
        Движения.GA_Еталони.Очистить();
        Для Каждого Строка Из Еталони Цикл
```

```
                Движение = Движения.GA_Еталони.Добавить();
                Движение.Период                                 = Дата;
                Движение.Регистратор                            = Ссылка;
                Движение.МножинаІдентифікуючихПараметрів        = МножинаІдентифікуючихПараметрів;
                Движение.ІдентифікуючийПараметр                 = ІдентифікуючийПараметр;
                Движение.ТермЛінгвістичноїЗмінної                = Строка.ТермЛінгвістичноїЗмінної;
                Движение.Інтервал                               = Строка.Інтервал;
                Движение.КоордX                                 = Строка.КоордX;
                Движение.КоордY                                 = Строка.КоордY;
        КонецЦикла;
        Движения.GA_Еталони.Записать();
КонецПроцедуры
```

Модуль форми документа GA_НаборИЕвристичнихПравил

```
&НаКлиенте
Процедура ПриОткрытии(Отказ)
        УстановитьВидимость();
КонецПроцедуры

&НаКлиенте
Процедура УстановитьВидимость()
        УстановитьВидимостьСинонимКолонкиТЧ(1, "ПравилаЛПпар1");
        УстановитьВидимостьСинонимКолонкиТЧ(2, "ПравилаЛПпар2");
        УстановитьВидимостьСинонимКолонкиТЧ(3, "ПравилаЛПпар3");
        УстановитьВидимостьСинонимКолонкиТЧ(4, "ПравилаЛПпар4");
        УстановитьВидимостьСинонимКолонкиТЧ(5, "ПравилаЛПпар5");
        УстановитьВидимостьСинонимКолонкиТЧ(6, "ПравилаЛПпар6");
        УстановитьВидимостьСинонимКолонкиТЧ(7, "ПравилаЛПпар7");
        УстановитьВидимостьСинонимКолонкиТЧ(8, "ПравилаЛПпар8");
        УстановитьВидимостьСинонимКолонкиТЧ(9, "ПравилаЛПпар9");
        УстановитьВидимостьСинонимКолонкиТЧ(10, "ПравилаЛПпар10");
        УстановитьВидимостьСинонимКолонкиТЧ(11, "ПравилаЛПпар11");
        УстановитьВидимостьСинонимКолонкиТЧ(12, "ПравилаЛПпар12");
        УстановитьВидимостьСинонимКолонкиТЧ(13, "ПравилаЛПпар13");
        УстановитьВидимостьСинонимКолонкиТЧ(14, "ПравилаЛПпар14");
        УстановитьВидимостьСинонимКолонкиТЧ(15, "ПравилаЛПпар15");
КонецПроцедуры

&НаКлиенте
Процедура УстановитьВидимостьСинонимКолонкиТЧ(НомерПараметра = 1, ИмяКолонкиТЧ = "ПравилаЛПпар1")
        ВидимостьКолонкиПравил = Ложь;
        ЗаголовокКолонкиПравил  = "";
        КоличествоПараметров = Объект.СписокПараметрів.Количество();
        Если КоличествоПараметров >= НомерПараметра Тогда
                СтрокаПараметра = Объект.СписокПараметрів[НомерПараметра-1];
                Если ЗначениеЗаполнено(СтрокаПараметра.ІдентифікуючийПараметр) Тогда
                        ВидимостьКолонкиПравил = Истина;
                        ЗаголовокКолонкиПравил  = "" + СтрокаПараметра.ІдентифікуючийПараметр;
                КонецЕсли;
        КонецЕсли;
        ЭтаФорма.Элементы[ИмяКолонкиТЧ].Видимость       = ВидимостьКолонкиПравил;
        ЭтаФорма.Элементы[ИмяКолонкиТЧ].Заголовок       = ЗаголовокКолонкиПравил;
КонецПроцедуры

&НаКлиенте
Процедура ЗаполнитьСписокПараметров(Команда)
        Объект.СписокПараметрів.Очистить();
        Объект.Правила.Очистить();
        МассивПараметровИПКС  = ПолучитьМассивПараметровИПКС(Объект.ВидІПКС);
        Для Каждого ПараметрИПКС Из МассивПараметровИПКС Цикл
                НоваяСтрока = Объект.СписокПараметрів.Добавить();
                НоваяСтрока.ІдентифікуючийПараметр       = ПараметрИПКС;
        КонецЦикла;
        УстановитьВидимость();
КонецПроцедуры

&НаСервере
Функция ПолучитьМассивПараметровИПКС(ВидИПКС)
        Возврат ВидИПКС.СписокПараметрів.ВыгрузитьКолонку("ІдентифікуючийПараметр");
```

```
КонецФункции

&НаКлиенте
Процедура МножинаІдентифікуючихПараметрівПриИзменении(Элемент)
	Объект.СписокПараметрів.Очистить();
	Объект.ЛінгвістичніІдентифікаториЙмовірностіІПКС.Очистить();
	Объект.Правила.Очистить();
	УстановитьВидимость();
КонецПроцедуры

&НаКлиенте
Процедура ВидІПКСПриИзменении(Элемент)
	Объект.СписокПараметрів.Очистить();
	Объект.ЛінгвістичніІдентифікаториЙмовірностіІПКС.Очистить();
	Объект.Правила.Очистить();
	УстановитьВидимость();
КонецПроцедуры

&НаКлиенте
Процедура ЗаповнитьСписокЛИ(Команда)
	ПолучитьСписокЛИ();
КонецПроцедуры

&НаСервере
Процедура ПолучитьСписокЛИ()
	Объект.ЛінгвістичніІдентифікаториЙмовірностіІПКС.Очистить();
	Объект.Правила.Очистить();
	Выборка = Справочники.GA_ЛінгвістичніІдентифікаториЙмовірностіІПКС.Выбрать();
	Пока Выборка.Следующий() Цикл
		Если Выборка.ПометкаУдаления Тогда
			Продолжить;
		КонецЕсли;
		НоваяСтрока = Объект.ЛінгвістичніІдентифікаториЙмовірностіІПКС.Добавить();
		НоваяСтрока.ЛІ    = Выборка.Ссылка;
		НоваяСтрока.Порядок = Выборка.Порядок;
	КонецЦикла;
	Объект.ЛінгвістичніІдентифікаториЙмовірностіІПКС.Сортировать("Порядок Возвр");
КонецПроцедуры

&НаКлиенте
Процедура СформироватьПравила(Команда)
	СформироватьПравилаНаСервере();
КонецПроцедуры

&НаСервере
Процедура СформироватьПравилаНаСервере()
	ПроверкаПройдена = Истина;
	Если Объект.СписокПараметрів.Количество() = 0 Тогда
		Сообщить("Заполните список параметров!");
		ПроверкаПройдена = Ложь;
	КонецЕсли;
	Если Объект.ЛінгвістичніІдентифікаториЙмовірностіІПКС.Количество() = 0 Тогда
		Сообщить("Заполните ТЧ ЛінгвістичніІдентифікаториЙмовірностіІПКС!");
		ПроверкаПройдена = Ложь;
	КонецЕсли;
	Если Не ПроверкаПройдена Тогда
		Возврат;
	КонецЕсли;
	КоличествоВсегоКомбинаций = 1;
	Для Каждого СтрокаТЧ Из Объект.СписокПараметрів Цикл
		КоличествоВсегоКомбинаций = КоличествоВсегоКомбинаций *
СтрокаТЧ.ІдентифікуючийПараметр.ТермиЛінгвістичнихЗмінних.Количество();
	КонецЦикла;
	Объект.Правила.Очистить();
	Инд = 0;
	Пока Инд < КоличествоВсегоКомбинаций Цикл
		НоваяСтрока = Объект.Правила.Добавить();
		НоваяСтрока.ИндКомбинацииПараметра = Инд + 1;
		НоваяСтрока.НаименованиеКомбинации =
ДопПроцедуры.ПолучитьКомбинациюПараметров(Объект.СписокПараметрів, Инд, НоваяСтрока);
```

```
                Инд = Инд + 1;
        КонецЦикла;
КонецПроцедуры

&НаКлиенте
Процедура ОчиститьПравила(Команда)
        Объект.Правила.Очистить();
КонецПроцедуры

&НаКлиенте
Процедура ОчиститьЛИ(Команда)
        Для Каждого СтрокаТЧ Из Объект.Правила Цикл
                СтрокаТЧ.ЛИ             = Неопределено;
                СтрокаТЧ.Учитывать      = Неопределено;
        КонецЦикла;
КонецПроцедуры

&НаКлиенте
Процедура СписокПараметрівПередОкончаниемРедактирования(Элемент, НоваяСтрока, ОтменаРедактирования, Отказ)
        Объект.Правила.Очистить();
        УстановитьВидимость();
КонецПроцедуры

&НаКлиенте
Процедура ЛінгвістичніІдентифікаториЙмовірностіІПКСПриОкончанииРедактирования(Элемент, НоваяСтрока,
ОтменаРедактирования)
        Объект.Правила.Очистить();
        УстановитьВидимость();
КонецПроцедуры

&НаКлиенте
Процедура ЗаполнитьПравила(Команда)
        Для Каждого СтрокаТЧ Из Объект.Правила Цикл
                СтрокаТЧ.ЛИ             = Неопределено;
                СтрокаТЧ.Учитывать      = Неопределено;
        КонецЦикла;
        КоличествоЛИ                    = 0;
        МассивЛИ                        = Новый Массив;
        Для Каждого Строка Из Объект.ЛінгвістичніІдентифікаториЙмовірностіІПКС Цикл
                КоличествоЛИ    = КоличествоЛИ + 1;
                МассивЛИ.Добавить(Строка.ЛІ);
        КонецЦикла;
        ГСЧ = Новый ГенераторСлучайныхЧисел();
        Для Каждого СтрокаТЧ Из Объект.Правила Цикл
                СлучЧисло = ГСЧ.СлучайноеЧисло(1, 4294967295);
                СлучЧисло = СлучЧисло % 50;
                Если СлучЧисло <= 2 Тогда
                        СлучЧисло1 = ГСЧ.СлучайноеЧисло(1, 4294967295);
                        СлучЧисло2 = ГСЧ.СлучайноеЧисло(1, 4294967295);
                        СлучЧисло1 = СлучЧисло1 % КоличествоЛИ;
                        СтрокаТЧ.ЛИ             = МассивЛИ[СлучЧисло1];
                        СтрокаТЧ.Учитывать      = Истина;
                КонецЕсли;
        КонецЦикла;
КонецПроцедуры
```

Модуль об'єкта GA_НаборИЕвристичнихПравил

```
Процедура ОбработкаПроведения(Отказ, РежимПроведения)
        ПроверитьЗаполнениеПолей(Отказ);
        Если Не Отказ ТОгда
                ДвиженияДокумента();
        КонецЕсли;
КонецПроцедуры

Процедура ПроверитьЗаполнениеПолей(Отказ)
        Если Не ЗначениеЗаполнено(МножинаІдентифікуючихПараметрів) Тогда
                Сообщить("Заповніть реквізит <Множина ідентифікуючих параметрів>", СтатусСообщения.Важное);
                Отказ = Истина;
        КонецЕсли;
```

```
        Если Не ЗначениеЗаполнено(ВидІПКС) Тогда
                Сообщить("Заповніть реквізит <Вид ІПКС>", СтатусСообщения.Важное);
                Отказ = Истина;
        КонецЕсли;
        Если СписокПараметрів.Количество() = 0 Тогда
                Сообщить("Заповніть ТЧ <Список параметрів>", СтатусСообщения.Важное);
                Отказ = Истина;
        КонецЕсли;
        Если ЛінгвістичніІдентифікаториЙмовірностіІПКС.Количество() = 0 Тогда
                Сообщить("Заповніть ТЧ <Лінгвістичн ідентифікатори ймовірності ІПКС>", СтатусСообщения.Важное);
                Отказ = Истина;
        КонецЕсли;
        Если Правила.Количество() = 0 Тогда
                Сообщить("Заповніть ТЧ <Правила>", СтатусСообщения.Важное);
                Отказ = Истина;
        КонецЕсли;
КонецПроцедуры

Процедура ДвиженияДокумента()
        Движения.GA_НаборПравил.Очистить();
        МассивПоиска = Правила.НайтиСтроки(Новый Структура("Учитывать", Истина));
        Для Каждого СтрокаПоиска Из МассивПоиска Цикл
                Если Не ЗначениеЗаполнено(СтрокаПоиска.ЛИ) Тогда
                        Продолжить;
                КонецЕсли;
                Движение = Движения.GA_НаборПравил.Добавить();
                Движение.Период = Дата;
                Движение.Регистратор = Ссылка;
                Движение.МножинаІдентифікуючихПараметрів = МножинаІдентифікуючихПараметрів;
                Движение.ВидІПКС = ВидІПКС;
                Движение.ИндКомбинацииПараметра = СтрокаПоиска.ИндКомбинацииПараметра;
                Движение.НаименованиеКомбинации = СтрокаПоиска.НаименованиеКомбинации;
                Движение.ЛИ = СтрокаПоиска.ЛИ;
        КонецЦикла;
        Движения.GA_НаборПравил.Записать();
КонецПроцедуры
```

Модуль форми документа GA_ОцінкаПоточногоСтануСередовища

```
&НаКлиенте
Процедура ПриОткрытии(Отказ)
        УстановитьВидимость();
КонецПроцедуры

&НаКлиенте
Процедура МножинаІдентифікуючихПараметрівПриИзменении(Элемент)
        Объект.СписокПараметрів.Очистить();
        Объект.ВидиІПКС.Очистить();
        Объект.ТаблицяДанихСтатистики.Очистить();
        Объект.ТаблицяСгрупованихДаних.Очистить();
        УстановитьВидимость();
КонецПроцедуры

&НаКлиенте
Процедура КількістьДанихДляГрупуванняПриИзменении(Элемент)
        Объект.ТаблицяСгрупованихДаних.Очистить();
        УстановитьВидимость();
КонецПроцедуры

&НаКлиенте
Процедура КількістьЗаписівСтатистикиПриИзменении(Элемент)
        Объект.ТаблицяДанихСтатистики.Очистить();
        Объект.ТаблицяСгрупованихДаних.Очистить();
        УстановитьВидимость();
КонецПроцедуры

&НаКлиенте
Процедура СписокПараметрівПриОкончанииРедактирования(Элемент, НоваяСтрока, ОтменаРедактирования)
        Объект.ТаблицяДанихСтатистики.Очистить();
        Объект.ТаблицяСгрупованихДаних.Очистить();
```

```
        УстановитьВидимость();
КонецПроцедуры

&НаКлиенте
Процедура ВидиІПКСПриОкончанииРедактирования(Элемент, НоваяСтрока, ОтменаРедактирования)
        Объект.ТаблицяДанихСтатистики.Очистить();
        Объект.ТаблицяСгрупованихДаних.Очистить();
        УстановитьВидимость();
КонецПроцедуры

&НаКлиенте
Процедура ТаблицяДанихСтатистикиПриОкончанииРедактирования(Элемент, НоваяСтрока, ОтменаРедактирования)
        Объект.ТаблицяСгрупованихДаних.Очистить();
        УстановитьВидимость();
КонецПроцедуры

&НаКлиенте
Процедура ЗаповнитиСписокПараметрів(Команда)
        Объект.СписокПараметрів.Очистить();
        Объект.ТаблицяДанихСтатистики.Очистить();
        Объект.ТаблицяСгрупованихДаних.Очистить();
        МассивПараметров = ПолучитьМассивПараметров(Объект.МножинаІдентифікуючихПараметрів);
        Для Каждого Параметр Из МассивПараметров Цикл
                НоваяСтрока = Объект.СписокПараметрів.Добавить();
                НоваяСтрока.ІдентифікуючийПараметр = Параметр;
        КонецЦикла;
        УстановитьВидимость();
КонецПроцедуры

&НаКлиенте
Процедура ЗаповнитиСписокВидівІПКС(Команда)
        Объект.ВидиІПКС.Очистить();
        Объект.ТаблицяДанихСтатистики.Очистить();
        Объект.ТаблицяСгрупованихДаних.Очистить();
        МассивВидівІПКС = ПолучитьМассивВидівІПКС(Объект.МножинаІдентифікуючихПараметрів);
        Для Каждого ВидІПКС Из МассивВидівІПКС Цикл
                НоваяСтрока = Объект.ВидиІПКС.Добавить();
                НоваяСтрока.ВидІПКС = ВидІПКС;
        КонецЦикла;
        УстановитьВидимость();
КонецПроцедуры

&НаКлиенте
Процедура ЗаповнитиТаблицюДанихСтатистики(Команда)
        ПроверкаПройдена = Истина;
        Объект.ТаблицяДанихСтатистики.Очистить();
        Объект.ТаблицяСгрупованихДаних.Очистить();
        Если Не ЗначениеЗаполнено(Объект.МножинаІдентифікуючихПараметрів) Тогда
                Сообщить("Заполните поле ІдентифікуючихПараметрів!");
                ПроверкаПройдена = Ложь;
        КонецЕсли;
        Если Не ЗначениеЗаполнено(Объект.КількістьЗаписівСтатистики) Тогда
                Сообщить("Заполните поле КількістьЗаписівСтатистики!");
                ПроверкаПройдена = Ложь;
        КонецЕсли;
        Если Не ПроверкаПройдена Тогда
                Возврат;
        КонецЕсли;
        ЗаповнитиТаблицюДанихСтатистикиНаСервере();
КонецПроцедуры

&НаКлиенте
Процедура ОчиститиТаблицюДанихСтатистики(Команда)
        Объект.ТаблицяДанихСтатистики.Очистить();
        Объект.ТаблицяСгрупованихДаних.Очистить();
КонецПроцедуры

&НаКлиенте
Процедура СгруповатьДані(Команда)
        ПроверкаПройдена = Истина;
```

```
	Объект.ТаблицяСгрупованихДаних.Очистить();
	Если Не ЗначениеЗаполнено(Объект.МножинаІдентифікуючихПараметрів) Тогда
		Сообщить("Заполните поле ІдентифікуючихПараметрів!");
		ПроверкаПройдена = Ложь;
	КонецЕсли;
	Если Не ЗначениеЗаполнено(Объект.КількістьДанихДляГрупування) Тогда
		Сообщить("Заполните поле КількістьДанихДляГрупування!");
		ПроверкаПройдена = Ложь;
	КонецЕсли;
	Если Не ПроверкаПройдена Тогда
		Возврат;
	КонецЕсли;
	СгруппироватьДаніНаСервере();
КонецПроцедуры

&НаКлиенте
Процедура ВизначитиВидиІПКС(Команда)
	ВизначитиВидиІПКСНаСервере();
КонецПроцедуры

&НаСервере
Функция ПолучитьМассивПараметров(МножинаІдентифікуючихПараметрів)
	Возврат МножинаІдентифікуючихПараметрів.СписокПараметрів.ВыгрузитьКолонку("ІдентифікуючийПараметр");
КонецФункции

&НаСервере
Функция ПолучитьМассивВидівІПКС(МножинаІдентифікуючихПараметрів)
	Массив = Новый Массив;
	Выборка = Справочники.GA_ВидиІПКС.Выбрать(,Объект.МножинаІдентифікуючихПараметрів);
	Пока Выборка.Следующий() Цикл
		Если Выборка.ПометкаУдаления Тогда
			Продолжить;
		КонецЕсли;
		Массив.Добавить(Выборка.Ссылка);
	КонецЦикла;
	Возврат Массив;
КонецФункции

&НаКлиенте
Процедура УстановитьВидимость()
	УстановитьВидимостьСинонимКолонкиТЧ(1);
	УстановитьВидимостьСинонимКолонкиТЧ(2);
	УстановитьВидимостьСинонимКолонкиТЧ(3);
	УстановитьВидимостьСинонимКолонкиТЧ(4);
	УстановитьВидимостьСинонимКолонкиТЧ(5);
	УстановитьВидимостьСинонимКолонкиТЧ(6);
	УстановитьВидимостьСинонимКолонкиТЧ(7);
	УстановитьВидимостьСинонимКолонкиТЧ(8);
	УстановитьВидимостьСинонимКолонкиТЧ(9);
	УстановитьВидимостьСинонимКолонкиТЧ(10);
	УстановитьВидимостьСинонимКолонкиТЧ(11);
	УстановитьВидимостьСинонимКолонкиТЧ(12);
	УстановитьВидимостьСинонимКолонкиТЧ(13);
	УстановитьВидимостьСинонимКолонкиТЧ(14);
	УстановитьВидимостьСинонимКолонкиТЧ(15);
КонецПроцедуры

&НаКлиенте
Процедура УстановитьВидимостьСинонимКолонкиТЧ(НомерПараметра = 1)
	ВидимостьКолонки		= Ложь;
	ЗаголовокКолонки		= "";
	КоличествоПараметров = Объект.СписокПараметрів.Количество();
	Если КоличествоПараметров >= НомерПараметра Тогда
		СтрокаПараметра = Объект.СписокПараметрів[НомерПараметра-1];
		Если ЗначениеЗаполнено(СтрокаПараметра.ІдентифікуючийПараметр) Тогда
			ВидимостьКолонки = Истина;
			ЗаголовокКолонки = "" + СтрокаПараметра.ІдентифікуючийПараметр;
		КонецЕсли;
	КонецЕсли;
	ГрупаТаблицяДанихСтатистикиГруппа = "ТаблицяДанихСтатистикиГруппа"	+ НомерПараметра;
```

```
	ГрупаТаблицяСгрупованихДанихГруппа  = "ТаблицяСгрупованихДанихГруппа"    + НомерПараметра;
	ИмяПараметраТаблицяДанихСтатистикиЗначПар = "ТаблицяДанихСтатистикиЗначПар"     + НомерПараметра;
	ИмяПараметраТаблицяДанихСтатистикиЛППар = "ТаблицяДанихСтатистикиЛППар"          + НомерПараметра;
	ИмяПараметраТаблицяСгрупованихДанихЛППар = "ТаблицяСгрупованихДанихЛППар"     + НомерПараметра;
	ЭтаФорма.Элементы[ГрупаТаблицяДанихСтатистикиГруппа].Видимость = ВидимостьКолонки;
	ЭтаФорма.Элементы[ГрупаТаблицяСгрупованихДанихГруппа].Видимость = ВидимостьКолонки;
	ЭтаФорма.Элементы[ИмяПараметраТаблицяДанихСтатистикиЗначПар].Заголовок = ЗаголовокКолонки + " знач.";
	ЭтаФорма.Элементы[ИмяПараметраТаблицяДанихСтатистикиЛППар].Заголовок   = ЗаголовокКолонки + " ЛП";
	ЭтаФорма.Элементы[ИмяПараметраТаблицяСгрупованихДанихЛППар].Заголовок = ЗаголовокКолонки + " ЛП";
КонецПроцедуры

&НаСервере
Процедура ЗаповнитиТаблицюДанихСтатистикиНаСервере()
	Запрос = Новый Запрос;
	Запрос.Текст =
	"ВЫБРАТЬ
	|	GA_Еталони.МножинаІдентифікуючихПараметрів,
	|	GA_Еталони.ІдентифікуючийПараметр,
	|	GA_Еталони.ТермЛінгвістичноїЗмінної,
	|	GA_Еталони.Інтервал,
	|	GA_Еталони.КоордY,
	|	GA_Еталони.КоордX
	|ИЗ
	|	РегистрСведений.GA_Еталони.СрезПоследних(&Дата, МножинаІдентифікуючихПараметрів =
&МножинаІдентифікуючихПараметрів) КАК GA_Еталони";
	Запрос.УстановитьПараметр("Дата", Объект.Дата);
	Запрос.УстановитьПараметр("МножинаІдентифікуючихПараметрів", Объект.МножинаІдентифікуючихПараметрів);
	ТзЭталонов = Запрос.Выполнить().Выгрузить();
	ГСЧ = Новый ГенераторСлучайныхЧисел();
	Инд1 = 0;
	Пока Инд1 < Объект.КількістьЗаписівСтатистики Цикл
		НоваяСтрока = Объект.ТаблицяДанихСтатистики.Добавить();
		Инд2 = 1;
		Для Каждого СтрокаТЧ Из Объект.СписокПараметрів Цикл
			СлучЧисло = ГСЧ.СлучайноеЧисло(0, 100000000);
			СлучЧисло = СлучЧисло * 0.00000001;
			НоваяСтрока["ЗначПар" + Инд2] = СлучЧисло;
			НоваяСтрока["ЛППар"+ Инд2] = УстановитьЛП(ТзЭталонов,
Объект.МножинаІдентифікуючихПараметрів, Объект.СписокПараметрів[Инд2-1].ІдентифікуючийПараметр, СлучЧисло);
			Инд2 = Инд2 + 1;
		КонецЦикла;
		Инд1 = Инд1 + 1;
	КонецЦикла;
КонецПроцедуры

&НаСервере
Функция УстановитьЛП(ТзЭталонов, МножинаІдентифікуючихПараметрів, Параметр, ЗначениеПараметра)
	Результат = Неопределено;
	Если Не ЗначениеЗаполнено(Параметр) Тогда
		Возврат Результат;
	КонецЕсли;
	Интервал = Справочники.GA_Інтервали.ПустаяСсылка();
	НомерСТрокиИнтервала  = 0;
	ЗначПрошлогоИнтервала  = 0;
	Для Каждого СтрокаТч Из Параметр.Інтервали Цикл
		Если ( ЗначПрошлогоИнтервала <= ЗначениеПараметра ) И ( ЗначениеПараметра <= СтрокаТч.Коефіцієнт )
Тогда
			Интервал = СтрокаТч.Інтеравал;
			НомерСТрокиИнтервала  = СтрокаТЧ.НомерСтроки;
			Прервать;
		КонецЕсли;
		ЗначПрошлогоИнтервала  = СтрокаТч.Коефіцієнт;
	КонецЦикла;
	ТЗЛП = Новый ТаблицаЗначений;
	ТЗЛП.Колонки.Добавить("ЛП");
	ТЗЛП.Колонки.Добавить("Коорд");
	Для Каждого СтрокаЛП Из Параметр.ТермиЛінгвістичнихЗмінних Цикл
		МассивПоискаКон = ТзЭталонов.НайтиСтроки(Новый Структура("МножинаІдентифікуючихПараметрів,
ІдентифікуючийПараметр, ТермЛінгвістичноїЗмінної, Інтервал", Объект.МножинаІдентифікуючихПараметрів, Параметр,
СтрокаЛП.Терм, Интервал));
```

```
                Если МассивПоискаКон.Количество() = 0 Тогда
                        Продолжить;
                КонецЕсли;
                X2 = МассивПоискаКон[0].КоордX;
                Y2 = МассивПоискаКон[0].КоордY;
                Если (НомерСТрокиИнтервала-2) < 0 Тогда
                        X1      = 0;
                        Y1      = Y2;
                Иначе
                        МассивПоискаНач = ТзЭталонов.НайтиСтроки(Новый
Структура("МножинаІдентифікуючихПараметрів, ІдентифікуючийПараметр, ТермЛінгвістичноїЗмінної, Інтервал",
Объект.МножинаІдентифікуючихПараметрів, Параметр, СтрокаЛП.Терм, Параметр.Інтервали[НомерСТрокиИнтервала-
2].Інтеравал));
                        X1      = МассивПоискаНач[0].КоордX;
                        Y1      = МассивПоискаНач[0].КоордY;
                КонецЕсли;
                Попытка
                        Yкоорд = (ЗначениеПараметра - X1) * (Y2 - Y1) / (X2 - X1) + Y1;
                Исключение
                        Yкоорд = 0;
                КонецПопытки;
                НоваяСтрока = ТЗЛП.Добавить();
                НоваяСтрока.ЛП          = СтрокаЛП.Терм;
                НоваяСтрока.Коорд       = Yкоорд;
        КонецЦикла;
        ТЗЛП.Сортировать("Коорд Убыв, ЛП Убыв");
        Возврат ТЗЛП[0].ЛП;
КонецФункции

&НаСервере
Процедура СгрупироватьДаніНаСервере()
        КоличествоСгрупированихСтрок = Окр(Объект.ТаблицяДанихСтатистики.Количество() /
Объект.КількістьДанихДляГрупування, 0, РежимОкругления.Окр15как20);
        Инд = 0;
        Пока Инд < КоличествоСгрупированихСтрок Цикл
                ИндНач = Инд * Объект.КількістьДанихДляГрупування;
                ИндКон = Мин(ИндНач + Объект.КількістьДанихДляГрупування - 1,
Объект.ТаблицяДанихСтатистики.Количество());
                ПосчитатьСреднее(ИндНач, ИндКон);
                Инд = Инд + 1;
        КонецЦикла;
КонецПроцедуры

&НаСервере
Процедура ПосчитатьСреднее(ИндНач, ИндКон)
        НоваяСтрока = Объект.ТаблицяСгрупованихДаних.Добавить();
        ЗаполнитьЗначенияСвойств(НоваяСтрока, Объект.ТаблицяДанихСтатистики[ИндНач]);
        ПолноеНаименованиеКомбинации = "";
        Для Каждого Параметр Из Объект.СписокПараметрів Цикл
                ИндПараметра = Параметр.НомерСтроки;
                ПолноеНаименованиеКомбинации = ПолноеНаименованиеКомбинации +
?(ЗначениеЗаполнено(ПолноеНаименованиеКомбинации), ", ", "") + Параметр + " = " + НоваяСтрока["ЛПпар"+ИндПараметра];
        КонецЦикла;
        НоваяСтрока.ПолноеНаименованиеКомбинации = ПолноеНаименованиеКомбинации;
КонецПроцедуры

&НаСервере
Процедура ВизначитиВидиІПКСНаСервере()
        Запрос = Новый Запрос;
        Запрос.Текст =
        "ВЫБРАТЬ
        |       GA_НаборПравилСрезПоследних.МножинаІдентифікуючихПараметрів,
        |       GA_НаборПравилСрезПоследних.ВидІПКС,
        |       GA_НаборПравилСрезПоследних.ИндКомбинацииПараметра,
        |       GA_НаборПравилСрезПоследних.НаименованиеКомбинации,
        |       GA_НаборПравилСрезПоследних.ЛИ
        |ИЗ
        |       РегистрСведений.GA_НаборПравил.СрезПоследних(&Дата, МножинаІдентифікуючихПараметрів =
&МножинаІдентифікуючихПараметрів) КАК GA_НаборПравилСрезПоследних";
        Запрос.УстановитьПараметр("Дата", Объект.Дата);
```

```
        Запрос.УстановитьПараметр("МножинаІдентифікуючихПараметрів", Объект.МножинаІдентифікуючихПараметрів);
        ТзПравил = Запрос.Выполнить().Выгрузить();
        Для Каждого СтрокаТЧ Из Объект.ТаблицяСгрупованихДаних Цикл
                Для Каждого СтрокаВидИПКС Из Объект.ВидиІПКС Цикл
                        НаименованиеПоиска = "";
                        Для Каждого СтрокаПараметрВидИПКС Из СтрокаВидИПКС.ВидІПКС.СписокПараметрів Цикл
                                МассивПоискаПараметра = Объект.СписокПараметрів.НайтиСтроки(Новый
Структура("ІдентифікуючийПараметр", СтрокаПараметрВидИПКС.ІдентифікуючийПараметр));
                                ИндПараметра = МассивПоискаПараметра[0].НомерСтроки;
                                НаименованиеПоиска = НаименованиеПоиска +
?(ЗначениеЗаполнено(НаименованиеПоиска), ", ", "") + СтрокаПараметрВидИПКС.ІдентифікуючийПараметр + " = " +
СтрокаТЧ["ЛППар"+ИндПараметра];
                                КонецЦикла;
                                МассивПоиска = ТзПравил.НайтиСтроки(Новый Структура("ВидІПКС, НаименованиеКомбинации",
СтрокаВидИПКС.ВидІПКС, НаименованиеПоиска));
                                Если МассивПоиска.Количество() > 0 Тогда
                                        СтрокаТЧ.ВидІПКС = СтрокаВидИПКС.ВидІПКС;
                                        СтрокаТЧ.ИндКомбинацииПараметра = МассивПоиска[0].ИндКомбинацииПараметра;
                                        СтрокаТЧ.НаименованиеКомбинации = МассивПоиска[0].НаименованиеКомбинации;
                                        СтрокаТЧ.ЛИ = МассивПоиска[0].ЛИ;
        КонецЕсли;
                КонецЦикла;
        КонецЦикла;
КонецПроцедуры

&НаКлиенте
Процедура ТаблицяСгрупованихДанихПередНачаломИзменения(Элемент, Отказ)
        Отказ = Истина;
КонецПроцедуры
```

Модуль об'єкта GA_ОцінкаПоточногоСтануСередовища

```
Процедура ОбработкаПроведения(Отказ, РежимПроведения)
        ПроверитьЗаполнениеПолей(Отказ);
        Если Не Отказ ТОгда
                ДвиженияДокумента();
        КонецЕсли;
КонецПроцедуры

Процедура ПроверитьЗаполнениеПолей(Отказ)
        Если Не ЗначениеЗаполнено(МножинаІдентифікуючихПараметрів) Тогда
                Сообщить("Заповніть реквізит <Множина ідентифікуючих параметрів>", СтатусСообщения.Важное);
                Отказ = Истина;
        КонецЕсли;
        Если ТаблицяСгрупованихДаних.Количество() = 0 Тогда
                Сообщить("Заповніть ТЧ <ТаблицяСгрупованихДаних>", СтатусСообщения.Важное);
                Отказ = Истина;
        КонецЕсли;
КонецПроцедуры

Процедура ДвиженияДокумента()
        Движения.GA_ОцінкиСтанів.Очистить();
        Для Каждого СтрокаТЧ Из ТаблицяСгрупованихДаних Цикл
                Движение = Движения.GA_ОцінкиСтанів.Добавить();
                Движение.Период = Дата;
                Движение.Регистратор = Ссылка;
                Движение.МножинаІдентифікуючихПараметрів = МножинаІдентифікуючихПараметрів;
                Движение.НомерЕкспериментy = СтрокаТЧ.НомерСтроки;
                Движение.ЛИ = СтрокаТЧ.ЛИ;
                Движение.ВидІПКС = СтрокаТЧ.ВидІПКС;
                Движение.НаименованиеКомбинации = СтрокаТЧ.НаименованиеКомбинации;
                Движение.ПолноеНаименованиеКомбинации = СтрокаТЧ.ПолноеНаименованиеКомбинации;
                Движение.Кількість = 1;
        КонецЦикла;
        Движения.GA_ОцінкиСтанів.Записать();
КонецПроцедуры
```

2. Лістинги програмного забезпечення «СОКС v.1.0»

Модуль форми елемента довідника GA_МножинаІдентифікуючихПараметрів

```
&НаКлиенте
Процедура ПриОткрытии(Отказ)
	УстановитьВидимость();
КонецПроцедуры

&НаКлиенте
Процедура НаименованиеПриИзменении(Элемент)
	Объект.ПовнаНазва = Объект.Наименование;
КонецПроцедуры

&НаКлиенте
Процедура ЗаповнитиСписокПараметрів(Команда)
	Объект.СписокПараметрів.Очистить();
	Объект.КоефіцієнтиВажливості.Очистить();
	МассивПараметров = ПолучитьМассивПараметров();
	Для Каждого Параметр Из МассивПараметров Цикл
		НоваяСтрока = Объект.СписокПараметрів.Добавить();
		НоваяСтрока.ІдентифікуючийПараметр = Параметр;
	КонецЦикла;
	УстановитьВидимость();
КонецПроцедуры

&НаКлиенте
Процедура ЗаповнитиТаблицюКоефіцієнтівВажливості(Команда)
	Объект.КоефіцієнтиВажливості.Очистить();
	КоличествоПараметров = Объект.СписокПараметрів.Количество();
	Инд = 1;
	Пока Инд <= 15 Цикл
		Если КоличествоПараметров >= Инд Тогда
			СтрокаПараметра = Объект.СписокПараметрів[Инд-1];
			НоваяСтрокаКВ = Объект.КоефіцієнтиВажливості.Добавить();
			НоваяСтрокаКВ.ІдентифікуючийПараметр = СтрокаПараметра.ІдентифікуючийПараметр;
			НоваяСтрокаКВ["Значення" + Инд] = 1;
		КонецЕсли;
		Инд = Инд + 1;
	КонецЦикла;
КонецПроцедуры

&НаКлиенте
Процедура РозрахуватиВаговіКоефіцієнти(Команда)
	КоличествоПараметров = Объект.СписокПараметрів.Количество();
	КоличествоСтрокКоефВажности = Объект.КоефіцієнтиВажливості.Количество();
	ВаговийКоефіцієнтИтого = 0;
	Для Каждого Строка Из Объект.КоефіцієнтиВажливості Цикл
		ПроизведениеПараметров = 1;
		Инд = 1;
		Пока Инд <= КоличествоПараметров Цикл
			Если Инд > 15 Тогда
				Прервать;
			КонецЕсли;
			ПроизведениеПараметров = ПроизведениеПараметров * Строка["Значення" + Инд];
			Инд = Инд + 1;
		КонецЦикла;
		Строка.ВаговийКоефіцієнт = ВычислитьКореньСтепениN(ПроизведениеПараметров,
КоличествоПараметров);
		ВаговийКоефіцієнтИтого = ВаговийКоефіцієнтИтого + Строка.ВаговийКоефіцієнт;
	КонецЦикла;
	ОстаточныйКоеф = 1;
	Инд = 0;
	Пока Инд < Объект.КоефіцієнтиВажливості.Количество() Цикл
		Строка = Объект.КоефіцієнтиВажливості[Инд];
		Если (Инд + 1) = Объект.КоефіцієнтиВажливості.Количество() Тогда
			Строка.ВаговийКоефіцієнтПісляНормування = ОстаточныйКоеф;
		Иначе
			Строка.ВаговийКоефіцієнтПісляНормування = Строка.ВаговийКоефіцієнт /
ВаговийКоефіцієнтИтого;
		КонецЕсли;
		ОстаточныйКоеф = ОстаточныйКоеф - Строка.ВаговийКоефіцієнтПісляНормування;
		Инд = Инд + 1;
	КонецЦикла;
```

```
КонецПроцедуры

&НаКлиенте
Процедура СписокПараметрівПриОкончанииРедактирования(Элемент, НоваяСтрока, ОтменаРедактирования)
	Объект.КоефіцієнтиВажливості.Очистить();
	УстановитьВидимость();
КонецПроцедуры

&НаКлиенте
Процедура СписокПараметрівПослеУдаления(Элемент)
	Объект.КоефіцієнтиВажливості.Очистить();
	УстановитьВидимость();
КонецПроцедуры

&НаКлиенте
Процедура СписокПараметрівОкончаниеПеретаскивания(Элемент, ПараметрыПеретаскивания, СтандартнаяОбработка)
	Объект.КоефіцієнтиВажливості.Очистить();
	УстановитьВидимость();
КонецПроцедуры

&НаКлиенте
Процедура ЗаповнитиКоефіцієнти(Команда)
	КоличествоПараметров = Объект.СписокПараметрів.Количество();
	КоличествоСтрокКоефВажности = Объект.КоефіцієнтиВажливості.Количество();
	Если КоличествоПараметров <> КоличествоСтрокКоефВажности Тогда
		Возврат;
	КонецЕсли;
	ГСЧ = Новый ГенераторСлучайныхЧисел();
	Инд1 = 0;
	Пока Инд1 < КоличествоСтрокКоефВажности Цикл
		Строка1 = Объект.КоефіцієнтиВажливості[Инд1];
		Инд2 = 0;
		Пока Инд2 < КоличествоПараметров Цикл
			Если Инд2 > 15 Тогда
				Прервать;
			КонецЕсли;
			Если ЗначениеЗаполнено(Строка1["Значення" + (Инд2+1)]) Тогда
				Инд2 = Инд2 + 1;
				Продолжить;
			КонецЕсли;
			Строка2 = Объект.КоефіцієнтиВажливості[Инд2];
			СлучЧисло1 = ГСЧ.СлучайноеЧисло(1, 30);
			СлучЧисло2 = ГСЧ.СлучайноеЧисло(0, 30);
			СлучЧисло2 = СлучЧисло2 % 2;
			Если СлучЧисло2 = 0 Тогда
				Строка1["Значення" + (Инд2+1)] = СлучЧисло1;
				Строка2["Значення" + (Инд1+1)] = 1/СлучЧисло1;
			Иначе
				Строка2["Значення" + (Инд1+1)] = СлучЧисло1;
				Строка1["Значення" + (Инд2+1)] = 1/СлучЧисло1;
			КонецЕсли;
			Инд2 = Инд2 + 1;
		КонецЦикла;
		Инд1 = Инд1 + 1;
	КонецЦикла;
КонецПроцедуры

&НаСервере
Функция ПолучитьМассивПараметров()
	Массив = Новый Массив;
	Запрос = Новый Запрос;
	Запрос.Текст =
	"ВЫБРАТЬ
	|	GA_ІдентифікуючіПараметри.Ссылка
	|ИЗ
	|	Справочник.GA_ІдентифікуючіПараметри КАК GA_ІдентифікуючіПараметри
	|ГДЕ
	|	GA_ІдентифікуючіПараметри.ПометкаУдаления = ЛОЖЬ
	|
	|УПОРЯДОЧИТЬ ПО
```

```
	|	GA_ІдентифікуючіПараметри.Код";
	Выборка = Запрос.Выполнить().Выбрать();
	Пока Выборка.Следующий() Цикл
		Массив.Добавить(Выборка.Ссылка);
	КонецЦикла;
	Возврат Массив;
КонецФункции

&НаКлиенте
Процедура УстановитьВидимость()
	КоличествоПараметров = Объект.СписокПараметрів.Количество();
	Инд = 1;
	Пока Инд <= 15 Цикл
		ВидимостьКолонки	= Ложь;
		ЗаголовокКолонки	= "";
		Если КоличествоПараметров >= Инд Тогда
			СтрокаПараметра = Объект.СписокПараметрів[Инд-1];
			Если ЗначениеЗаполнено(СтрокаПараметра.ІдентифікуючийПараметр) Тогда
				ВидимостьКолонки	= Истина;
				ЗаголовокКолонки	= "" + СтрокаПараметра.ІдентифікуючийПараметр;
			КонецЕсли;
		КонецЕсли;
		ЭтаФорма.Элементы["КоефіцієнтиВажливостіЗначення" + Инд].Видимость	= ВидимостьКолонки;
		ЭтаФорма.Элементы["КоефіцієнтиВажливостіЗначення" + Инд].Заголовок	= ЗаголовокКолонки;
		Инд = Инд + 1;
	КонецЦикла;
КонецПроцедуры

&НаКлиенте
Функция ВычислитьКореньСтепениN(ЧислоДляВычисленияКореня, СтепеньКореня)
	Если ЧислоДляВычисленияКореня <= 0 Тогда
		Возврат 0;
	КонецЕсли;
	Результат = 1;
	Инд = 0;
	Пока Инд < 1000 Цикл
		РезультатТемп = (((СтепеньКореня - 1) * Результат) + (ЧислоДляВычисленияКореня / Pow(Результат,
СтепеньКореня - 1))) * 1 / СтепеньКореня;
		Разница = Результат - РезультатТемп;
		Разница = ?(Разница < 0, Разница * -1, Разница);
		Если Разница < 0.001 Тогда
			Прервать;
		КонецЕсли;
		Результат = РезультатТемп;
		Инд = Инд + 1;
	КонецЦикла;
	Возврат Результат;
КонецФункции
```

Модуль форми документа GA_Еталони

```
&НаКлиенте
Процедура ПриОткрытии(Отказ)
	ОбновитьГрафик();
КонецПроцедуры

&НаКлиенте
Процедура МножинаІдентифікуючихПараметрівПриИзменении(Элемент)
	Объект.Еталони.Очистить();
	ОбновитьГрафик();
КонецПроцедуры

&НаКлиенте
Процедура ІдентифікуючийПараметрПриИзменении(Элемент)
	ОбновитьГрафик();
КонецПроцедуры

&НаСервере
Функция ПолучитьТаблицуТермовЛЗ(Параметр)
	Возврат Параметр.ТермиЛінгвістичнихЗмінних.ВыгрузитьКолонку("Терм");
```

```
КонецФункции

&НаСервере
Функция ПолучитьТаблицуИнтервалов(Параметр)
	Возврат Параметр.Інтервали.ВыгрузитьКолонку("Інтеравал");
онецФункции

&НаКлиенте
Процедура Заповнити(Команда)
	Объект.Еталони.Очистить();
	МассивТермовЛЗ		= ПолучитьТаблицуТермовЛЗ(Объект.ІдентифікуючийПараметр);
	МассивИнтервалов		= ПолучитьТаблицуИнтервалов(Объект.ІдентифікуючийПараметр);
	Для Каждого ЭлементЛЗ Из МассивТермовЛЗ Цикл
		Для Каждого ЭлементИ Из МассивИнтервалов Цикл
			НоваяСтрока = Объект.Еталони.Добавить();
			НоваяСтрока.ТермЛінгвістичноїЗмінної		= ЭлементЛЗ;
			НоваяСтрока.Інтервал	= ЭлементИ;
			НоваяСтрока.КоордХ	= 0;
			НоваяСтрока.КоордУ	= 0;
		КонецЦикла;
	КонецЦикла;
	ОбновитьГрафик();
КонецПроцедуры

&НаКлиенте
Процедура ОбновитиГрафік(Команда)
	ОбновитьГрафик();
КонецПроцедуры

&НаСервере
Процедура ОбновитьГрафик()
	ЭтаФорма.ГрафікЕталонів.Очистить();
	МассивИнтервалов		= ПолучитьМассивИзТЧ(Объект.Еталони, "КоордХ");
	МассивТермовЛЗ		= ПолучитьМассивИзТЧ(Объект.Еталони, "ТермЛінгвістичноїЗмінної");
	ТзДляВывода = Новый ТаблицаЗначений;
	ТзДляВывода.Колонки.Добавить("Серия");
	Для Каждого Элемент Из МассивИнтервалов Цикл
		ИмяКолонки = "Колонка" + Элемент;
		ИмяКолонки = СтрЗаменить(ИмяКолонки, " ", "_");
		ИмяКолонки = СтрЗаменить(ИмяКолонки, ".", "_");
		ИмяКолонки = СтрЗаменить(ИмяКолонки, ",", "_");
		Если ТзДляВывода.Колонки.Найти(ИмяКолонки) = Неопределено Тогда
			ТзДляВывода.Колонки.Добавить(ИмяКолонки);
			ТзДляВывода.Колонки[ИмяКолонки].Заголовок = "" + Элемент;
		КонецЕсли;
	КонецЦикла;
	ТзКопия = Объект.Еталони.Выгрузить();
	ТзКопия.Сортировать("ТермЛінгвістичноїЗмінної Возр, КоордХ Возр");
	Для Каждого ЭлементЛП Из МассивТермовЛЗ Цикл
		НоваяСтрока = ТзДляВывода.Добавить();
		НоваяСтрока.Серия = ЭлементЛП;
		МассивПоиска = ТзКопия.НайтиСтроки(Новый Структура("ТермЛінгвістичноїЗмінної", ЭлементЛП));
		Для Каждого ЭлементПоиска Из МассивПоиска Цикл
			ИмяКолонки = "Колонка" + ЭлементПоиска.КоордХ;
			ИмяКолонки = СтрЗаменить(ИмяКолонки, " ", "_");
			ИмяКолонки = СтрЗаменить(ИмяКолонки, ".", "_");
			ИмяКолонки = СтрЗаменить(ИмяКолонки, ",", "_");
			НоваяСтрока[ИмяКолонки]	=	?(НоваяСтрока[ИмяКолонки]	=	Неопределено,
ЭлементПоиска.КоордУ, Макс(ЭлементПоиска.КоордУ, НоваяСтрока[ИмяКолонки]));
		КонецЦикла;
	КонецЦикла;
	ЭтаФорма.ГрафікЕталонів.ТипДиаграммы	= ТипДиаграммы.График;
	ЭтаФорма.ГрафікЕталонів.СерииВСтроках	= Истина;
	ЭтаФорма.ГрафікЕталонів.ИсточникДанных	= ТзДляВывода;
КонецПроцедуры

&НаСервере
Функция ПолучитьМассивИзТЧ(ТЧ, ИмяРеквизита)
	Тз = ТЧ.Выгрузить();
	Тз.Сортировать("" + ИмяРеквизита + " Возр");
```

```
        Тз.Свернуть(ИмяРеквизита,"");
        Массив = Тз.ВыгрузитьКолонку(ИмяРеквизита);
        Возврат Массив;
КонецФункции

&НаКлиенте
Процедура ЕталониПриОкончанииРедактирования(Элемент, НоваяСтрока, ОтменаРедактирования)
        ОбновитьГрафик();
КонецПроцедуры

&НаКлиенте
Процедура ЕталониПослеУдаления(Элемент)
        ОбновитьГрафик();
КонецПроцедуры
```

Модуль об'єкта документа GA_Еталони

```
Процедура ОбработкаПроведения(Отказ, РежимПроведения)
        ПроверитьЗаполнениеПолей(Отказ);
        Если Не Отказ ТОгда
                ДвиженияДокумента();
        КонецЕсли;
КонецПроцедуры

Процедура ПроверитьЗаполнениеПолей(Отказ)
        Если Не ЗначениеЗаполнено(МножинаІдентифікуючихПараметрів) Тогда
                Сообщить("Заповніть реквізит <Множина ідентифікуючих параметрів>", СтатусСообщения.Важное);
                Отказ = Истина;
        КонецЕсли;
        Если Не ЕталонРівняКритичності И Не ЗначениеЗаполнено(ІдентифікуючийПараметр) Тогда
                Сообщить("Заповніть реквізит <Ідентифікуючий параметр>", СтатусСообщения.Важное);
                Отказ = Истина;
        КонецЕсли;
        Если Еталони.Количество() = 0 Тогда
                Сообщить("Заповніть ТЧ <Еталони>", СтатусСообщения.Важное);
                Отказ = Истина;
        КонецЕсли;
КонецПроцедуры

Процедура ДвиженияДокумента()
        Движения.GA_Еталони.Очистить();
        Для Каждого Строка Из Еталони Цикл
                Движение = Движения.GA_Еталони.Добавить();
                Движение.Период             = Дата;
                Движение.Регистратор        = Ссылка;
                Движение.МножинаІдентифікуючихПараметрів          = МножинаІдентифікуючихПараметрів;
                Движение.ІдентифікуючийПараметр = ?(ЕталонРівняКритичності, Неопределено, ІдентифікуючийПараметр);
                Движение.ТермЛінгвістичноїЗмінної = Строка.ТермЛінгвістичноїЗмінної;
                Движение.Інтервал           = Строка.Інтервал;
                Движение.КоордХ             = Строка.КоордХ;
                Движение.КоордУ             = Строка.КоордУ;
        КонецЦикла;
        Движения.GA_Еталони.Записать();
КонецПроцедуры

Процедура ПередЗаписью(Отказ, РежимЗаписи, РежимПроведения)
        Если ЕталонРівняКритичності Тогда
                ІдентифікуючийПараметр = Неопределено;
        КонецЕсли;
КонецПроцедуры
```

Модуль форми документа GA_ОцінкарівняКритичності

```
&НаКлиенте
Процедура ПриОткрытии(Отказ)
        УстановитьВидимость();
КонецПроцедуры

&НаКлиенте
Процедура МножинаІдентифікуючихПараметрівПриИзменении(Элемент)
```

```
	ОчиститьТЧ();
КонецПроцедуры

&НаКлиенте
Процедура КількістьДанихДляГрупуванняПриИзменении(Элемент)
	ОчиститьТЧ();
КонецПроцедуры

&НаКлиенте
Процедура СписокПараметрівПриОкончанииРедактирования(Элемент, НоваяСтрока, ОтменаРедактирования)
	ОчиститьТЧ(Ложь);
КонецПроцедуры

&НаКлиенте
Процедура СписокПараметрівПослеУдаления(Элемент)
	ОчиститьТЧ(Ложь);
КонецПроцедуры

&НаКлиенте
Процедура СписокПараметрівОкончаниеПеретаскивания(Элемент, ПараметрыПеретаскивания, СтандартнаяОбработка)
	ОчиститьТЧ(Ложь);
КонецПроцедуры

&НаКлиенте
Процедура ЗаповнитиСписокПараметрів(Команда)
	ОчиститьТЧ();
	МассивПараметров = ПолучитьМассивПараметров(Объект.МножинаІдентифікуючихПараметрів);
	Для Каждого Параметр Из МассивПараметров Цикл
		НоваяСтрока = Объект.СписокПараметрів.Добавить();
		НоваяСтрока.ІдентифікуючийПараметр	= Параметр;
	КонецЦикла;
	УстановитьВидимость();
КонецПроцедуры

&НаКлиенте
Процедура ЗаповнитиТаблицю(Команда)
	ОчиститьТЧ(Ложь);
	ЗаповнитиТаблицюДанихНаСервере();
КонецПроцедуры

&НаКлиенте
Процедура ОчиститиТаблицю(Команда)
	ОчиститьТЧ(Ложь);
КонецПроцедуры

&НаКлиенте
Процедура СгрупироватьДанные(Команда)
	ОчиститьТЧ(Ложь,Ложь);
	СгрупироватьДаніНаСервере();
КонецПроцедуры

&НаКлиенте
Процедура ТаблицяСгрупованихДанихПередОкончаниемРедактирования(Элемент, НоваяСтрока, ОтменаРедактирования,
Отказ)
	ОчиститьТЧ(Ложь,Ложь,Ложь);
КонецПроцедуры

&НаКлиенте
Процедура ТаблицяСгрупованихДанихПослеУдаления(Элемент)
	ОчиститьТЧ(Ложь,Ложь,Ложь);
КонецПроцедуры

&НаКлиенте
Процедура РасчитатьДанныеЛЦС(Команда)
	ОчиститьТЧ(Ложь,Ложь,Ложь);
	Если Объект.ТаблицяСгрупованихДаних.Количество() > 0 Тогда
		НоваяСтрока = Объект.ТаблицяДанихЛЦС.Добавить();
		НоваяСтрока.КоордХ1 = Объект.ТаблицяСгрупованихДаних[0].КоордХ1;
		НоваяСтрока.КоордХ2 = Объект.ТаблицяСгрупованихДаних[0].КоордХ2;
		НоваяСтрока.КоордХ3 = Объект.ТаблицяСгрупованихДаних[0].КоордХ3;
```

```
                НоваяСтрока.КоордY1 = Объект.ТаблицяСгрупованихДаних[0].КоордY1;
                НоваяСтрока.КоордY2 = Объект.ТаблицяСгрупованихДаних[0].КоордY2;
                НоваяСтрока.КоордY3 = Объект.ТаблицяСгрупованихДаних[0].КоордY3;
        КонецЕсли;
КонецПроцедуры

&НаКлиенте
Процедура ТаблицяДанихЛЦСПередОкончаниемРедактирования(Элемент, НоваяСтрока, ОтменаРедактирования, Отказ)
        ОчиститьТЧ(Ложь,Ложь,Ложь,Ложь);
КонецПроцедуры

&НаКлиенте
Процедура ТаблицяДанихЛЦСПослеУдаления(Элемент)
        ОчиститьТЧ(Ложь,Ложь,Ложь,Ложь);
КонецПроцедуры

&НаКлиенте
Процедура ЗаполнитиАльфаРівні(Команда)
        ОчиститьТЧ(Ложь,Ложь,Ложь,Ложь);
        НоваяСтрока = Объект.АльфаРівні.Добавить();
        НоваяСтрока.КоордY = 0;
        НоваяСтрока = Объект.АльфаРівні.Добавить();
        НоваяСтрока.КоордY = 1;
        НоваяСтрока = Объект.АльфаРівні.Добавить();
        НоваяСтрока.КоордY = 0;
КонецПроцедуры

&НаКлиенте
Процедура АльфаРівніПриОкончанииРедактирования(Элемент, НоваяСтрока, ОтменаРедактирования)
        ОчиститьТЧ(Ложь,Ложь,Ложь,Ложь,Ложь);
КонецПроцедуры

&НаКлиенте
Процедура ПорівнятиРівніКритичності(Команда)
        ОчиститьТЧ(Ложь,Ложь,Ложь,Ложь,Ложь);
        ПорівнятиРівніКритичностіНаСервере();
КонецПроцедуры

&НаКлиенте
Процедура ПорівнянняРівнівКритичностіПриОкончанииРедактирования(Элемент, НоваяСтрока, ОтменаРедактирования)
        ОчиститьТЧ(Ложь,Ложь,Ложь,Ложь,Ложь,Ложь);
КонецПроцедуры

&НаКлиенте
Процедура РасгруповатьДанные(Команда)
        ОчиститьТЧ(Ложь,Ложь,Ложь,Ложь,Ложь,Ложь);
        РасгруповатьДанныеНаСервере();
КонецПроцедуры

&НаКлиенте
Процедура ТаблицяРозгрупованихДанихПередОкончаниемРедактирования(Элемент, НоваяСтрока, ОтменаРедактирования,
Отказ)
        ОчиститьТЧ(Ложь,Ложь,Ложь,Ложь,Ложь,Ложь,Ложь);
КонецПроцедуры

&НаКлиенте
Процедура РасгруповатьДанныеЛЦС(Команда)
        ОчиститьТЧ(Ложь,Ложь,Ложь,Ложь,Ложь,Ложь,Ложь);
        РасгруповатьДанныеЛЦСНаСервере();
КонецПроцедуры

&НаКлиенте
Процедура ОчиститьТЧ(ОчищатьСписокПараметрів = Истина, ОчищатьТаблицяДанихСтатистики = Истина,
        ОчищатьТаблицяСгрупованихДаних = Истина, ОчищатьТаблицяДанихЛЦС = Истина,
        ОчищатьАльфаРівні = Истина, ОчищатьПорівнянняРівнівКритичності = Истина,
        ОчищатьТаблицяРозгрупованихДаних = Истина, ОчищатьТаблицяРозгрупованихДанихЛЦС = Истина)
        Если ОчищатьСписокПараметрів Тогда
                Объект.СписокПараметрів.Очистить();
        КонецЕсли;
        Если ОчищатьТаблицяДанихСтатистики Тогда
```

```
                Объект.ТаблицяДанихСтатистики.Очистить();
        КонецЕсли;
        Если ОчищатьТаблицяСгрупованихДаних Тогда
                Объект.ТаблицяСгрупованихДаних.Очистить();
        КонецЕсли;
        Если ОчищатьТаблицяДанихЛЦС Тогда
                Объект.ТаблицяДанихЛЦС.Очистить();
        КонецЕсли;
        Если ОчищатьАльфаРівні Тогда
                Объект.АльфаРівні.Очистить();
        КонецЕсли;
        Если ОчищатьПорівнянняРівнівКритичності Тогда
                Объект.ПорівнянняРівнівКритичності.Очистить();
        КонецЕсли;
        Если ОчищатьТаблицяРозгрупованихДаних Тогда
                Объект.ТаблицяРозгрупованихДаних.Очистить();
        КонецЕсли;
        Если ОчищатьТаблицяРозгрупованихДанихЛЦС Тогда
                Объект.ТаблицяРозгрупованихДанихЛЦС.Очистить();
        КонецЕсли;
        УстановитьВидимость();
КонецПроцедуры

&НаКлиенте
Процедура УстановитьВидимость()
        УстановитьВидимостьСинонимКолонкиТЧ(1);
        УстановитьВидимостьСинонимКолонкиТЧ(2);
        УстановитьВидимостьСинонимКолонкиТЧ(3);
        УстановитьВидимостьСинонимКолонкиТЧ(4);
        УстановитьВидимостьСинонимКолонкиТЧ(5);
        УстановитьВидимостьСинонимКолонкиТЧ(6);
        УстановитьВидимостьСинонимКолонкиТЧ(7);
        УстановитьВидимостьСинонимКолонкиТЧ(8);
        УстановитьВидимостьСинонимКолонкиТЧ(9);
        УстановитьВидимостьСинонимКолонкиТЧ(10);
        УстановитьВидимостьСинонимКолонкиТЧ(11);
        УстановитьВидимостьСинонимКолонкиТЧ(12);
        УстановитьВидимостьСинонимКолонкиТЧ(13);
        УстановитьВидимостьСинонимКолонкиТЧ(14);
        УстановитьВидимостьСинонимКолонкиТЧ(15);
КонецПроцедуры

&НаКлиенте
Процедура УстановитьВидимостьСинонимКолонкиТЧ(НомерПараметра = 1)
        ВидимостьКолонки        = Ложь;
        ЗаголовокКолонки        = "";
        КоличествоПараметров = Объект.СписокПараметрів.Количество();
        Если КоличествоПараметров >= НомерПараметра Тогда
                СтрокаПараметра = Объект.СписокПараметрів[НомерПараметра-1];
                Если ЗначениеЗаполнено(СтрокаПараметра.ІдентифікуючийПараметр) Тогда
                        ВидимостьКолонки        = Истина;
                        ЗаголовокКолонки        = "" + СтрокаПараметра.ІдентифікуючийПараметр;
                КонецЕсли;
        КонецЕсли;
        ЭтаФорма.Элементы["ТаблицяДанихСтатистикиЛППар" + НомерПараметра].Заголовок = ЗаголовокКолонки;
        ЭтаФорма.Элементы["ТаблицяДанихСтатистикиЛППар" + НомерПараметра].Видимость = ВидимостьКолонки;
КонецПроцедуры

&НаСервере
Функция ПолучитьМассивПараметров(МножинаІдентифікуючихПараметрів)
        Возврат МножинаІдентифікуючихПараметрів.СписокПараметрів.ВыгрузитьКолонку("ІдентифікуючийПараметр");
КонецФункции

&НаСервере
Процедура ЗаповнитиТаблицюДанихНаСервере()
        Запрос = Новый Запрос;
        Запрос.Текст =
        "ВЫБРАТЬ
        |       GA_Еталони.МножинаІдентифікуючихПараметрів,
        |       GA_Еталони.ІдентифікуючийПараметр,
```

```
	|	GA_Еталони.ТермЛінгвістичноїЗмінної
	|ИЗ
	|	РегистрСведений.GA_Еталони.СрезПоследних(&Дата, МножинаІдентифікуючихПараметрів = &МножинаІдентифікуючихПараметрів) КАК GA_Еталони
	|
	|СГРУППИРОВАТЬ ПО
	|	GA_Еталони.ІдентифікуючийПараметр,
	|	GA_Еталони.ТермЛінгвістичноїЗмінної,
	|	GA_Еталони.МножинаІдентифікуючихПараметрів";
	Запрос.УстановитьПараметр("Дата", Объект.Дата);
	Запрос.УстановитьПараметр("МножинаІдентифікуючихПараметрів", Объект.МножинаІдентифікуючихПараметрів);
	ТзЭталонов = Запрос.Выполнить().Выгрузить();
	ГСЧ = Новый ГенераторСлучайныхЧисел();
	Инд1 = 0;
	Пока Инд1 < Объект.КількістьДанихДляГрупування Цикл
		НоваяСтрока = Объект.ТаблицяДанихСтатистики.Добавить();
		Инд2 = 1;
		Для Каждого СтрокаТЧ Из Объект.СписокПараметрів Цикл
			СлучЧисло = ГСЧ.СлучайноеЧисло(0, 4294967295);
			МассивПоискаТермов = ТзЭталонов.НайтиСтроки(Новый Структура("ІдентифікуючийПараметр", СтрокаТЧ.ІдентифікуючийПараметр));
			КоличествоТермов = МассивПоискаТермов.Количество();
			Если КоличествоТермов > 0 Тогда
				СлучЧисло = СлучЧисло % КоличествоТермов;
				НоваяСтрока["ЛППар" + Инд2] = МассивПоискаТермов[СлучЧисло].ТермЛінгвістичноїЗмінної;
			КонецЕсли;
			Инд2 = Инд2 + 1;
		КонецЦикла;
		Инд1 = Инд1 + 1;
	КонецЦикла;
КонецПроцедуры

&НаСервере
Процедура СгрупироватьДаніНаСервере()
	Запрос = Новый Запрос;
	Запрос.Текст =
	"ВЫБРАТЬ
	|	GA_Еталони.МножинаІдентифікуючихПараметрів,
	|	GA_Еталони.ІдентифікуючийПараметр,
	|	GA_Еталони.ТермЛінгвістичноїЗмінної,
	|	GA_Еталони.Інтервал КАК Інтервал,
	|	GA_Еталони.КоордX,
	|	GA_Еталони.КоордY
	|ИЗ
	|	РегистрСведений.GA_Еталони.СрезПоследних(&Дата, МножинаІдентифікуючихПараметрів = &МножинаІдентифікуючихПараметрів) КАК GA_Еталони
	|
	|УПОРЯДОЧИТЬ ПО
	|	GA_Еталони.Інтервал.Наименование";
	Запрос.УстановитьПараметр("Дата", Объект.Дата);
	Запрос.УстановитьПараметр("МножинаІдентифікуючихПараметрів", Объект.МножинаІдентифікуючихПараметрів);
	ТзЭталонов = Запрос.Выполнить().Выгрузить();
	Инд = 1;
	Для Каждого СтрокаПараметра Из Объект.СписокПараметрів Цикл
		ТЗПараметров = Объект.ТаблицяДанихСтатистики.Выгрузить(,"ЛППар" + Инд);
		НоваяСтрока = Объект.ТаблицяСгрупованихДаних.Добавить();
		НоваяСтрока.ІдентифікуючийПараметр = СтрокаПараметра.ІдентифікуючийПараметр;
		ПерваяСтрока = Истина;
		Для Каждого Строка Из Объект.ТаблицяДанихСтатистики Цикл
			МассивПоискаЕталона = ТзЭталонов.НайтиСтроки(Новый Структура("ІдентифікуючийПараметр,ТермЛінгвістичноїЗмінної", СтрокаПараметра.ІдентифікуючийПараметр, Строка["ЛППар"+Инд]));
			Если МассивПоискаЕталона.Количество() >=3 Тогда
				Если ПерваяСтрока Тогда
					НоваяСтрока.КоордX1 = МассивПоискаЕталона[0].КоордX;
					НоваяСтрока.КоордY1 = МассивПоискаЕталона[0].КоордY;
					НоваяСтрока.КоордX2 = МассивПоискаЕталона[1].КоордX;
					НоваяСтрока.КоордY2 = МассивПоискаЕталона[1].КоордY;
					НоваяСтрока.КоордX3 = МассивПоискаЕталона[2].КоордX;
```

```
                                        НоваяСтрока.КоордY3 = МассивПоискаЕталона[2].КоордY;
                                        ПерваяСтрока = Ложь;
                                Иначе
                                        Прервать;
                                КонецЕсли;
                        КонецЕсли;
                КонецЦикла;
                Инд = Инд + 1;
        КонецЦикла;
КонецПроцедуры

&НаСервере
Процедура ПорівнятиРівніКритичностіНаСервере()
        Если Объект.ТаблицяДанихЛЦС.Количество() = 0 Или
                Объект.АльфаРівні.Количество() = 0 Тогда
                Возврат;
        КонецЕсли;
        СтрокаДанныхЛЦС = Объект.ТаблицяДанихЛЦС[0];
        Запрос = Новый Запрос;
        Запрос.Текст =
        "ВЫБРАТЬ
        |       GA_Еталони.МножинаІдентифікуючихПараметрів,
        |       GA_Еталони.ІдентифікуючийПараметр,
        |       GA_Еталони.ТермЛінгвістичноїЗмінної,
        |       GA_Еталони.Інтервал КАК Інтервал,
        |       GA_Еталони.КоордX,
        |       GA_Еталони.КоордY
        |ИЗ
        |       РегистрСведений.GA_Еталони.СрезПоследних(&Дата, ІдентифікуючийПараметр =
&ІдентифікуючийПараметр И МножинаІдентифікуючихПараметрів = &МножинаІдентифікуючихПараметрів) КАК
GA_Еталони
        |
        |УПОРЯДОЧИТЬ ПО
        |       GA_Еталони.Інтервал.Наименование";
        Запрос.УстановитьПараметр("Дата", Объект.Дата);
        Запрос.УстановитьПараметр("МножинаІдентифікуючихПараметрів", Объект.МножинаІдентифікуючихПараметрів);
        Запрос.УстановитьПараметр("ІдентифікуючийПараметр",
Справочники.GA_ІдентифікуючіПараметри.ПустаяСсылка());
        ТзЭталонов = Запрос.Выполнить().Выгрузить();
        ТзЭталонов.Колонки.Добавить("Учтено", Новый ОписаниеТипов("Булево"));
        Если ТзЭталонов.Количество() = 0 Тогда
                Возврат;
        КонецЕсли;
        ТзЭталоновКопия = ТзЭталонов.Скопировать();
        ТзЭталоновКопия.Свернуть("ТермЛінгвістичноїЗмінної");
        Для Каждого СтрокаТерма Из ТзЭталоновКопия Цикл
                НоваяСтрока = Объект.ПорівнянняРівнівКритичності.Добавить();
                НоваяСтрока.Терм = СтрокаТерма.ТермЛінгвістичноїЗмінної;
                РастояниеХеменга = 0; Инд = 1;
                Для Каждого СтрокаАльфаУровеня Из Объект.АльфаРівні Цикл
                        ВремЧисло = 0;
                        МассивПоиска = ТзЭталонов.НайтиСтроки(Новый Структура("ТермЛінгвістичноїЗмінної, КоордY,
Учтено", СтрокаТерма.ТермЛінгвістичноїЗмінної, СтрокаАльфаУровеня.КоордY, Ложь));
                        Если МассивПоиска.Количество() > 0 Тогда
                                ВремЧисло = СтрокаДанныхЛЦС["КоордX" + Инд] - МассивПоиска[0].КоордX;
                                МассивПоиска[0].Учтено = Истина
                        КонецЕсли;
                        РастояниеХеменга = РастояниеХеменга + ?(ВремЧисло < 0, ВремЧисло * -1, ВремЧисло);
                        Инд = Инд + 1;
                КонецЦикла;
                НоваяСтрока.ВідстаньХемінга = РастояниеХеменга;
        КонецЦикла;
        Объект.ПорівнянняРівнівКритичності.Сортировать("ВідстаньХемінга Возр");
        Объект.ПорівнянняРівнівКритичності[0].ВизначенийРівеньКритичності = Истина;
КонецПроцедуры

&НаСервере
Процедура РасгруппироватьДанныеНаСервере()
        Для Каждого Строка Из Объект.ТаблицяСгрупованихДаних Цикл
                СуммаКоорлинатY = Строка.КоордY1 + Строка.КоордY2 + Строка.КоордY3;
```

```
                НоваяСтрока = Объект.ТаблицяРозгрупованихДаних.Добавить();
                НоваяСтрока.ІдентифікуючийПараметр = Строка.ІдентифікуючийПараметр;
                НоваяСтрока.Значення = 100 * ?(СуммаКоорлинатY = 0, 0, ( Строка.КоордY1 * Строка.КоордX1 +
Строка.КоордY2 * Строка.КоордX2 + Строка.КоордY3 * Строка.КоордX3 ) / СуммаКоорлинатY);
        КонецЦикла;
КонецПроцедуры

&НаСервере
Процедура РасгрупироватьДанныеЛЦСНаСервере()
        Если Объект.ТаблицяДанихЛЦС.Количество() = 0 Тогда
                Возврат;
        КонецЕсли;
        Строка = Объект.ТаблицяДанихЛЦС[0];
        СуммаКоорлинатY = Строка.КоордY1 + Строка.КоордY2 + Строка.КоордY3;
        НоваяСтрока = Объект.ТаблицяРозгрупованихДанихЛЦС.Добавить();
        НоваяСтрока.Значення = 100 * ?(СуммаКоорлинатY = 0, 0, ( Строка.КоордY1 * Строка.КоордX1 + Строка.КоордY2 *
Строка.КоордX2 + Строка.КоордY3 * Строка.КоордX3 ) / СуммаКоорлинатY);
КонецПроцедуры
```

Модуль об'єкта документа GA_ОцінкарівняКритичності

```
Процедура ОбработкаПроведения(Отказ, РежимПроведения)
        ПроверитьЗаполнениеПолей(Отказ);
        Если Не Отказ ТОгда
                ДвиженияДокумента();
        КонецЕсли;
КонецПроцедуры

Процедура ПроверитьЗаполнениеПолей(Отказ)
        Если Не ЗначениеЗаполнено(МножинаІдентифікуючихПараметрів) Тогда
                Сообщить("Заповніть реквізит <Множина ідентифікуючих параметрів>", СтатусСообщения.Важное);
                Отказ = Истина;
        КонецЕсли;
КонецПроцедуры
```

Додаток В. Множини евристичних правил для СВІПКС

Таблиця 1

Множина правил ER_1 для виявлення злому ІС

p	P_{Tlog}	P_{Nlog}	P_{CPU}	P_{MU}	P_{NEr}	P_{RTPr}	Результат
1	Л	Н	Н	Н	М	М	С
2	Л	Н	Н	Н	М	С	Н
3	Л	Н	Н	Н	М	В	Н
4	Л	Н	Н	Н	С	М	С
5	Л	Н	Н	Н	С	С	С
6	Л	Н	Н	Н	С	В	Н
7	Л	Н	Н	Н	В	М	С
8	Л	Н	Н	Н	В	С	С
9	Л	Н	Н	Н	В	В	С
10	Л	Н	Н	С	М	М	С
11	Л	Н	Н	С	М	С	С
12	Л	Н	Н	С	М	В	Н
13	Л	Н	Н	С	С	М	С
14	Л	Н	Н	С	С	С	С
15	Л	Н	Н	С	С	В	С
16	Л	Н	Н	С	В	М	П
17	Л	Н	Н	С	В	С	С
18	Л	Н	Н	С	В	В	С
19	Л	Н	Н	В	М	М	С
20	Л	Н	Н	В	М	С	С
21	Л	Н	Н	В	М	В	С
22	Л	Н	Н	В	С	М	П
23	Л	Н	Н	В	С	С	С
24	Л	Н	Н	В	С	В	С
25	Л	Н	Н	В	В	М	П
26	Л	Н	Н	В	В	С	П
27	Л	Н	Н	В	В	В	С
28	Л	Н	С	Н	М	М	С
29	Л	Н	С	Н	М	С	С
30	Л	Н	С	Н	М	В	Н
31	Л	Н	С	Н	С	М	С
32	Л	Н	С	Н	С	С	С
33	Л	Н	С	Н	С	В	С
34	Л	Н	С	Н	В	М	П
35	Л	Н	С	Н	В	С	С
36	Л	Н	С	Н	В	В	С
37	Л	Н	С	С	М	М	С
38	Л	Н	С	С	М	С	С
39	Л	Н	С	С	М	В	С
40	Л	Н	С	С	С	М	П
41	Л	Н	С	С	С	С	С
42	Л	Н	С	С	С	В	С
43	Л	Н	С	С	В	М	П
44	Л	Н	С	С	В	С	П
45	Л	Н	С	С	В	В	С
46	Л	Н	С	В	М	М	П
47	Л	Н	С	В	М	С	П
48	Л	Н	С	В	М	В	С
49	Л	Н	С	В	С	М	П
50	Л	Н	С	В	С	С	П
51	Л	Н	С	В	С	В	П
52	Л	Н	С	В	В	М	В
53	Л	Н	С	В	В	С	П
54	Л	Н	С	В	В	В	П
55	Л	Н	В	Н	М	М	С
56	Л	Н	В	Н	М	С	С
57	Л	Н	В	Н	М	В	Н
58	Л	Н	В	Н	С	М	С
59	Л	Н	В	Н	С	С	С
60	Л	Н	В	Н	С	В	С
61	Л	Н	В	Н	В	М	П
62	Л	Н	В	Н	В	С	С
63	Л	Н	В	Н	В	В	С
64	Л	Н	В	С	М	М	П
65	Л	Н	В	С	М	С	С
66	Л	Н	В	С	М	В	С
67	Л	Н	В	С	С	М	П
68	Л	Н	В	С	С	С	П
69	Л	Н	В	С	С	В	С
70	Л	Н	В	С	В	М	П
71	Л	Н	В	С	В	С	П
72	Л	Н	В	С	В	В	П
73	Л	Н	В	В	М	М	П
74	Л	Н	В	В	М	С	П
75	Л	Н	В	В	М	В	С
76	Л	Н	В	В	С	М	П
77	Л	Н	В	В	С	С	П
78	Л	Н	В	В	С	В	П
79	Л	Н	В	В	В	М	В
80	Л	Н	В	В	В	С	П
81	Л	Н	В	В	В	В	П
82	Л	С	Н	Н	М	М	С
83	Л	С	Н	Н	М	С	С
84	Л	С	Н	Н	М	В	Н
85	Л	С	Н	Н	С	М	С
86	Л	С	Н	Н	С	С	С
87	Л	С	Н	Н	С	В	С
88	Л	С	Н	Н	В	М	П
89	Л	С	Н	Н	В	С	С
90	Л	С	Н	Н	В	В	С
91	Л	С	Н	С	М	М	С

92	Л	С	Н	С	М	С	С
93	Л	С	Н	С	М	В	С
94	Л	С	Н	С	С	М	П
95	Л	С	Н	С	С	С	С
96	Л	С	Н	С	С	В	С
97	Л	С	Н	С	В	М	П
98	Л	С	Н	С	В	С	П
99	Л	С	Н	С	В	В	С
100	Л	С	Н	В	М	М	П
101	Л	С	Н	В	М	С	С
102	Л	С	Н	В	М	В	С
103	Л	С	Н	В	С	М	П
104	Л	С	Н	В	С	С	П
105	Л	С	Н	В	С	В	С
106	Л	С	Н	В	В	М	П
107	Л	С	Н	В	В	С	П
108	Л	С	Н	В	В	В	П
109	Л	С	С	Н	М	М	С
110	Л	С	С	Н	М	С	С
111	Л	С	С	Н	М	В	С
112	Л	С	С	Н	С	М	П
113	Л	С	С	Н	С	С	С
114	Л	С	С	Н	С	В	С
115	Л	С	С	Н	В	М	П
116	Л	С	С	Н	В	С	П
117	Л	С	С	Н	В	В	С
118	Л	С	С	С	М	М	П
119	Л	С	С	С	М	С	С
120	Л	С	С	С	М	В	С
121	Л	С	С	С	С	М	П
122	Л	С	С	С	С	С	П
123	Л	С	С	С	С	В	С
124	Л	С	С	С	В	М	П
125	Л	С	С	С	В	С	П
126	Л	С	С	С	В	В	П
127	Л	С	С	В	М	М	П
128	Л	С	С	В	М	С	П
129	Л	С	С	В	М	В	С
130	Л	С	С	В	С	М	П
131	Л	С	С	В	С	С	П
132	Л	С	С	В	С	В	П
133	Л	С	С	В	В	М	В
134	Л	С	С	В	В	С	П
135	Л	С	С	В	В	В	П
136	Л	С	В	Н	М	М	П
137	Л	С	В	Н	М	С	С
138	Л	С	В	Н	М	В	С
139	Л	С	В	Н	С	М	П
140	Л	С	В	Н	С	С	П
141	Л	С	В	Н	С	В	С
142	Л	С	В	Н	В	М	П
143	Л	С	В	Н	В	С	П
144	Л	С	В	Н	В	В	П
145	Л	С	В	С	М	М	П
146	Л	С	В	С	М	С	П
147	Л	С	В	С	М	В	С
148	Л	С	В	С	С	М	П
149	Л	С	В	С	С	С	П
150	Л	С	В	С	С	В	П
151	Л	С	В	С	В	М	В
152	Л	С	В	С	В	С	П
153	Л	С	В	С	В	В	П
154	Л	С	В	В	М	М	П
155	Л	С	В	В	М	С	П
156	Л	С	В	В	М	В	П
157	Л	С	В	В	С	М	В
158	Л	С	В	В	С	С	П
159	Л	С	В	В	С	В	П
160	Л	С	В	В	В	М	В
161	Л	С	В	В	В	С	В
162	Л	С	В	В	В	В	П
163	Л	В	Н	Н	М	М	С
164	Л	В	Н	Н	М	С	С
165	Л	В	Н	Н	М	В	С
166	Л	В	Н	Н	С	М	П
167	Л	В	Н	Н	С	С	С
168	Л	В	Н	Н	С	В	С
169	Л	В	Н	Н	В	М	П
170	Л	В	Н	Н	В	С	П
171	Л	В	Н	Н	В	В	С
172	Л	В	Н	С	М	М	П
173	Л	В	Н	С	М	С	С
174	Л	В	Н	С	М	В	С
175	Л	В	Н	С	С	М	П
176	Л	В	Н	С	С	С	П
177	Л	В	Н	С	С	В	С
178	Л	В	Н	С	В	М	П
179	Л	В	Н	С	В	С	П
180	Л	В	Н	С	В	В	П
181	Л	В	Н	В	М	М	П
182	Л	В	Н	В	М	С	П
183	Л	В	Н	В	М	В	С
184	Л	В	Н	В	С	М	П
185	Л	В	Н	В	С	С	П
186	Л	В	Н	В	С	В	П
187	Л	В	Н	В	В	М	В
188	Л	В	Н	В	В	С	П
189	Л	В	Н	В	В	В	П
190	Л	В	С	Н	М	М	П
191	Л	В	С	Н	М	С	С
192	Л	В	С	Н	М	В	С
193	Л	В	С	Н	С	М	П
194	Л	В	С	Н	С	С	П
195	Л	В	С	Н	С	В	С

196	Л	В	С	Н	В	М	П	248	П	Н	Н	Н	С	С	С
197	Л	В	С	Н	В	С	П	249	П	Н	Н	Н	С	В	С
198	Л	В	С	Н	В	В	П	250	П	Н	Н	Н	В	М	П
199	Л	В	С	С	М	М	П	251	П	Н	Н	Н	В	С	С
200	Л	В	С	С	М	С	П	252	П	Н	Н	Н	В	В	С
201	Л	В	С	С	М	В	С	253	П	Н	Н	С	М	М	С
202	Л	В	С	С	С	М	П	254	П	Н	Н	С	М	С	С
203	Л	В	С	С	С	С	П	255	П	Н	Н	С	М	В	С
204	Л	В	С	С	С	В	П	256	П	Н	Н	С	С	М	П
205	Л	В	С	С	В	М	В	257	П	Н	Н	С	С	С	С
206	Л	В	С	С	В	С	П	258	П	Н	Н	С	С	В	С
207	Л	В	С	С	В	В	П	259	П	Н	Н	С	В	М	П
208	Л	В	С	В	М	М	П	260	П	Н	Н	С	В	С	П
209	Л	В	С	В	М	С	П	261	П	Н	Н	С	В	В	С
210	Л	В	С	В	М	В	П	262	П	Н	Н	В	М	М	П
211	Л	В	С	В	С	М	В	263	П	Н	Н	В	М	С	С
212	Л	В	С	В	С	С	П	264	П	Н	Н	В	М	В	С
213	Л	В	С	В	С	В	П	265	П	Н	Н	В	С	М	П
214	Л	В	С	В	В	М	В	266	П	Н	Н	В	С	С	П
215	Л	В	С	В	В	С	В	267	П	Н	Н	В	С	В	С
216	Л	В	С	В	В	В	П	268	П	Н	Н	В	В	М	П
217	Л	В	В	Н	М	М	П	269	П	Н	Н	В	В	С	П
218	Л	В	В	Н	М	С	П	270	П	Н	Н	В	В	В	П
219	Л	В	В	Н	М	В	С	271	П	Н	С	Н	М	М	С
220	Л	В	В	Н	С	М	П	272	П	Н	С	Н	М	С	С
221	Л	В	В	Н	С	С	П	273	П	Н	С	Н	М	В	С
222	Л	В	В	Н	С	В	П	274	П	Н	С	Н	С	М	П
223	Л	В	В	Н	В	М	В	275	П	Н	С	Н	С	С	С
224	Л	В	В	Н	В	С	П	276	П	Н	С	Н	С	В	С
225	Л	В	В	Н	В	В	П	277	П	Н	С	Н	В	М	П
226	Л	В	В	С	М	М	П	278	П	Н	С	Н	В	С	П
227	Л	В	В	С	М	С	П	279	П	Н	С	Н	В	В	С
228	Л	В	В	С	М	В	П	280	П	Н	С	С	М	М	П
229	Л	В	В	С	С	М	В	281	П	Н	С	С	М	С	С
230	Л	В	В	С	С	С	П	282	П	Н	С	С	М	В	С
231	Л	В	В	С	С	В	П	283	П	Н	С	С	С	М	П
232	Л	В	В	С	В	М	В	284	П	Н	С	С	С	С	П
233	Л	В	В	С	В	С	В	285	П	Н	С	С	С	В	С
234	Л	В	В	С	В	В	П	286	П	Н	С	С	В	М	П
235	Л	В	В	В	М	М	В	287	П	Н	С	С	В	С	П
236	Л	В	В	В	М	С	П	288	П	Н	С	С	В	В	П
237	Л	В	В	В	М	В	П	289	П	Н	С	В	М	М	П
238	Л	В	В	В	С	М	В	290	П	Н	С	В	М	С	П
239	Л	В	В	В	С	С	В	291	П	Н	С	В	М	В	С
240	Л	В	В	В	С	В	П	292	П	Н	С	В	С	М	П
241	Л	В	В	В	В	М	В	293	П	Н	С	В	С	С	П
242	Л	В	В	В	В	С	В	294	П	Н	С	В	С	В	П
243	Л	В	В	В	В	В	В	295	П	Н	С	В	В	М	В
244	П	Н	Н	Н	М	М	С	296	П	Н	С	В	В	С	П
245	П	Н	Н	Н	М	С	С	297	П	Н	С	В	В	В	П
246	П	Н	Н	Н	М	В	Н	298	П	Н	В	Н	М	М	П
247	П	Н	Н	Н	С	М	С	299	П	Н	В	Н	М	С	С

300	П	Н	В	Н	М	В	С
301	П	Н	В	Н	С	М	П
302	П	Н	В	Н	С	С	П
303	П	Н	В	Н	С	В	С
304	П	Н	В	Н	В	М	П
305	П	Н	В	Н	В	С	П
306	П	Н	В	Н	В	В	П
307	П	Н	В	С	М	М	П
308	П	Н	В	С	М	С	П
309	П	Н	В	С	М	В	С
310	П	Н	В	С	С	М	П
311	П	Н	В	С	С	С	П
312	П	Н	В	С	С	В	П
313	П	Н	В	С	В	М	В
314	П	Н	В	С	В	С	П
315	П	Н	В	С	В	В	П
316	П	Н	В	В	М	М	П
317	П	Н	В	В	М	С	П
318	П	Н	В	В	М	В	П
319	П	Н	В	В	С	М	В
320	П	Н	В	В	С	С	П
321	П	Н	В	В	С	В	П
322	П	Н	В	В	В	М	В
323	П	Н	В	В	В	С	В
324	П	Н	В	В	В	В	П
325	П	С	Н	Н	М	М	С
326	П	С	Н	Н	М	С	С
327	П	С	Н	Н	М	В	С
328	П	С	Н	Н	С	М	П
329	П	С	Н	Н	С	С	С
330	П	С	Н	Н	С	В	С
331	П	С	Н	Н	В	М	П
332	П	С	Н	Н	В	С	П
333	П	С	Н	Н	В	В	С
334	П	С	Н	С	М	М	П
335	П	С	Н	С	М	С	С
336	П	С	Н	С	М	В	С
337	П	С	Н	С	С	М	П
338	П	С	Н	С	С	С	П
339	П	С	Н	С	С	В	С
340	П	С	Н	С	В	М	П
341	П	С	Н	С	В	С	П
342	П	С	Н	С	В	В	П
343	П	С	Н	В	М	М	П
344	П	С	Н	В	М	С	П
345	П	С	Н	В	М	В	С
346	П	С	Н	В	С	М	П
347	П	С	Н	В	С	С	П
348	П	С	Н	В	С	В	П
349	П	С	Н	В	В	М	В
350	П	С	Н	В	В	С	П
351	П	С	Н	В	В	В	П
352	П	С	С	Н	М	М	П
353	П	С	С	Н	М	С	С
354	П	С	С	Н	М	В	С
355	П	С	С	Н	С	М	П
356	П	С	С	Н	С	С	П
357	П	С	С	Н	С	В	С
358	П	С	С	Н	В	М	П
359	П	С	С	Н	В	С	П
360	П	С	С	Н	В	В	П
361	П	С	С	С	М	М	П
362	П	С	С	С	М	С	П
363	П	С	С	С	М	В	С
364	П	С	С	С	С	М	П
365	П	С	С	С	С	С	П
366	П	С	С	С	С	В	П
367	П	С	С	С	В	М	В
368	П	С	С	С	В	С	П
369	П	С	С	С	В	В	П
370	П	С	С	В	М	М	П
371	П	С	С	В	М	С	П
372	П	С	С	В	М	В	П
373	П	С	С	В	С	М	В
374	П	С	С	В	С	С	П
375	П	С	С	В	С	В	П
376	П	С	С	В	В	М	В
377	П	С	С	В	В	С	В
378	П	С	С	В	В	В	П
379	П	С	В	Н	М	М	П
380	П	С	В	Н	М	С	П
381	П	С	В	Н	М	В	С
382	П	С	В	Н	С	М	П
383	П	С	В	Н	С	С	П
384	П	С	В	Н	С	В	П
385	П	С	В	Н	В	М	В
386	П	С	В	Н	В	С	П
387	П	С	В	Н	В	В	П
388	П	С	В	С	М	М	П
389	П	С	В	С	М	С	П
390	П	С	В	С	М	В	П
391	П	С	В	С	С	М	В
392	П	С	В	С	С	С	П
393	П	С	В	С	С	В	П
394	П	С	В	С	В	М	В
395	П	С	В	С	В	С	В
396	П	С	В	С	В	В	П
397	П	С	В	В	М	М	В
398	П	С	В	В	М	С	П
399	П	С	В	В	М	В	П
400	П	С	В	В	С	М	В
401	П	С	В	В	С	С	В
402	П	С	В	В	С	В	П
403	П	С	В	В	В	М	В

404	П	С	В	В	В	С	В
405	П	С	В	В	В	В	В
406	П	В	Н	Н	М	М	П
407	П	В	Н	Н	М	С	С
408	П	В	Н	Н	М	В	С
409	П	В	Н	Н	С	М	П
410	П	В	Н	Н	С	С	П
411	П	В	Н	Н	С	В	С
412	П	В	Н	Н	В	М	П
413	П	В	Н	Н	В	С	П
414	П	В	Н	Н	В	В	П
415	П	В	Н	С	М	М	П
416	П	В	Н	С	М	С	П
417	П	В	Н	С	М	В	С
418	П	В	Н	С	С	М	П
419	П	В	Н	С	С	С	П
420	П	В	Н	С	С	В	П
421	П	В	Н	С	В	М	В
422	П	В	Н	С	В	С	П
423	П	В	Н	С	В	В	П
424	П	В	Н	В	М	М	П
425	П	В	Н	В	М	С	П
426	П	В	Н	В	М	В	П
427	П	В	Н	В	С	М	В
428	П	В	Н	В	С	С	П
429	П	В	Н	В	С	В	П
430	П	В	Н	В	В	М	В
431	П	В	Н	В	В	С	В
432	П	В	Н	В	В	В	П
433	П	В	С	Н	М	М	П
434	П	В	С	Н	М	С	П
435	П	В	С	Н	М	В	С
436	П	В	С	Н	С	М	П
437	П	В	С	Н	С	С	П
438	П	В	С	Н	С	В	П
439	П	В	С	Н	В	М	В
440	П	В	С	Н	В	С	П
441	П	В	С	Н	В	В	П
442	П	В	С	С	М	М	П
443	П	В	С	С	М	С	П
444	П	В	С	С	М	В	П
445	П	В	С	С	С	М	В
446	П	В	С	С	С	С	П
447	П	В	С	С	С	В	П
448	П	В	С	С	В	М	В
449	П	В	С	С	В	С	В
450	П	В	С	С	В	В	П
451	П	В	С	В	М	М	В
452	П	В	С	В	М	С	П
453	П	В	С	В	М	В	П
454	П	В	С	В	С	М	В
455	П	В	С	В	С	С	В
456	П	В	С	В	С	В	П
457	П	В	С	В	В	М	В
458	П	В	С	В	В	С	В
459	П	В	С	В	В	В	В
460	П	В	В	Н	М	М	П
461	П	В	В	Н	М	С	П
462	П	В	В	Н	М	В	П
463	П	В	В	Н	С	М	В
464	П	В	В	Н	С	С	П
465	П	В	В	Н	С	В	П
466	П	В	В	Н	В	М	В
467	П	В	В	Н	В	С	В
468	П	В	В	Н	В	В	П
469	П	В	В	С	М	М	В
470	П	В	В	С	М	С	П
471	П	В	В	С	М	В	П
472	П	В	В	С	С	М	В
473	П	В	В	С	С	С	В
474	П	В	В	С	С	В	П
475	П	В	В	С	В	М	В
476	П	В	В	С	В	С	В
477	П	В	В	С	В	В	В
478	П	В	В	В	М	М	В
479	П	В	В	В	М	С	В
480	П	В	В	В	М	В	П
481	П	В	В	В	С	М	В
482	П	В	В	В	С	С	В
483	П	В	В	В	С	В	В
484	П	В	В	В	В	М	К
485	П	В	В	В	В	С	В
486	П	В	В	В	В	В	В
487	Н	Н	Н	Н	М	М	С
488	Н	Н	Н	Н	М	С	С
489	Н	Н	Н	Н	М	В	С
490	Н	Н	Н	Н	С	М	П
491	Н	Н	Н	Н	С	С	С
492	Н	Н	Н	Н	С	В	С
493	Н	Н	Н	Н	В	М	П
494	Н	Н	Н	Н	В	С	П
495	Н	Н	Н	Н	В	В	С
496	Н	Н	Н	С	М	М	П
497	Н	Н	Н	С	М	С	С
498	Н	Н	Н	С	М	В	С
499	Н	Н	Н	С	С	М	П
500	Н	Н	Н	С	С	С	П
501	Н	Н	Н	С	С	В	С
502	Н	Н	Н	С	В	М	П
503	Н	Н	Н	С	В	С	П
504	Н	Н	Н	С	В	В	П
505	Н	Н	Н	В	М	М	П
506	Н	Н	Н	В	М	С	П
507	Н	Н	Н	В	М	В	С

508	Н	Н	Н	В	С	М	П
509	Н	Н	Н	В	С	С	П
510	Н	Н	Н	В	С	В	П
511	Н	Н	Н	В	В	М	В
512	Н	Н	Н	В	В	С	П
513	Н	Н	Н	В	В	В	П
514	Н	Н	С	Н	М	М	П
515	Н	Н	С	Н	М	С	С
516	Н	Н	С	Н	М	В	С
517	Н	Н	С	Н	С	М	П
518	Н	Н	С	Н	С	С	П
519	Н	Н	С	Н	С	В	С
520	Н	Н	С	Н	В	М	П
521	Н	Н	С	Н	В	С	П
522	Н	Н	С	Н	В	В	П
523	Н	Н	С	С	М	М	П
524	Н	Н	С	С	М	С	П
525	Н	Н	С	С	М	В	С
526	Н	Н	С	С	С	М	П
527	Н	Н	С	С	С	С	П
528	Н	Н	С	С	С	В	П
529	Н	Н	С	С	В	М	В
530	Н	Н	С	С	В	С	П
531	Н	Н	С	С	В	В	П
532	Н	Н	С	В	М	М	П
533	Н	Н	С	В	М	С	П
534	Н	Н	С	В	М	В	П
535	Н	Н	С	В	С	М	В
536	Н	Н	С	В	С	С	П
537	Н	Н	С	В	С	В	П
538	Н	Н	С	В	В	М	В
539	Н	Н	С	В	В	С	В
540	Н	Н	С	В	В	В	П
541	Н	Н	В	Н	М	М	П
542	Н	Н	В	Н	М	С	П
543	Н	Н	В	Н	М	В	С
544	Н	Н	В	Н	С	М	П
545	Н	Н	В	Н	С	С	П
546	Н	Н	В	Н	С	В	П
547	Н	Н	В	Н	В	М	В
548	Н	Н	В	Н	В	С	П
549	Н	Н	В	Н	В	В	П
550	Н	Н	В	С	М	М	П
551	Н	Н	В	С	М	С	П
552	Н	Н	В	С	М	В	П
553	Н	Н	В	С	С	М	В
554	Н	Н	В	С	С	С	П
555	Н	Н	В	С	С	В	П
556	Н	Н	В	С	В	М	В
557	Н	Н	В	С	В	С	В
558	Н	Н	В	С	В	В	П
559	Н	Н	В	В	М	М	В
560	Н	Н	В	В	М	С	П
561	Н	Н	В	В	М	В	П
562	Н	Н	В	В	С	М	В
563	Н	Н	В	В	С	С	В
564	Н	Н	В	В	С	В	П
565	Н	Н	В	В	В	М	В
566	Н	Н	В	В	В	С	В
567	Н	Н	В	В	В	В	В
568	Н	С	Н	Н	М	М	П
569	Н	С	Н	Н	М	С	С
570	Н	С	Н	Н	М	В	С
571	Н	С	Н	Н	С	М	П
572	Н	С	Н	Н	С	С	П
573	Н	С	Н	Н	С	В	С
574	Н	С	Н	Н	В	М	П
575	Н	С	Н	Н	В	С	П
576	Н	С	Н	Н	В	В	П
577	Н	С	Н	С	М	М	П
578	Н	С	Н	С	М	С	П
579	Н	С	Н	С	М	В	С
580	Н	С	Н	С	С	М	П
581	Н	С	Н	С	С	С	П
582	Н	С	Н	С	С	В	П
583	Н	С	Н	С	В	М	В
584	Н	С	Н	С	В	С	П
585	Н	С	Н	С	В	В	П
586	Н	С	Н	В	М	М	П
587	Н	С	Н	В	М	С	П
588	Н	С	Н	В	М	В	П
589	Н	С	Н	В	С	М	В
590	Н	С	Н	В	С	С	П
591	Н	С	Н	В	С	В	П
592	Н	С	Н	В	В	М	В
593	Н	С	Н	В	В	С	В
594	Н	С	Н	В	В	В	П
595	Н	С	С	Н	М	М	П
596	Н	С	С	Н	М	С	П
597	Н	С	С	Н	М	В	С
598	Н	С	С	Н	С	М	П
599	Н	С	С	Н	С	С	П
600	Н	С	С	Н	С	В	П
601	Н	С	С	Н	В	М	В
602	Н	С	С	Н	В	С	П
603	Н	С	С	Н	В	В	П
604	Н	С	С	С	М	М	П
605	Н	С	С	С	М	С	П
606	Н	С	С	С	М	В	П
607	Н	С	С	С	С	М	В
608	Н	С	С	С	С	С	П
609	Н	С	С	С	С	В	П
610	Н	С	С	С	В	М	В
611	Н	С	С	С	В	С	В

612	Н	С	С	С	В	В	П	664	Н	В	Н	С	В	М	В
613	Н	С	С	В	М	М	В	665	Н	В	Н	С	В	С	В
614	Н	С	С	В	М	С	П	666	Н	В	Н	С	В	В	П
615	Н	С	С	В	М	В	П	667	Н	В	Н	В	М	М	В
616	Н	С	С	В	С	М	В	668	Н	В	Н	В	М	С	П
617	Н	С	С	В	С	С	В	669	Н	В	Н	В	М	В	П
618	Н	С	С	В	С	В	П	670	Н	В	Н	В	С	М	В
619	Н	С	С	В	В	М	В	671	Н	В	Н	В	С	С	В
620	Н	С	С	В	В	С	В	672	Н	В	Н	В	С	В	П
621	Н	С	С	В	В	В	В	673	Н	В	Н	В	В	М	В
622	Н	С	В	Н	М	М	П	674	Н	В	Н	В	В	С	В
623	Н	С	В	Н	М	С	П	675	Н	В	Н	В	В	В	В
624	Н	С	В	Н	М	В	П	676	Н	В	С	Н	М	М	П
625	Н	С	В	Н	С	М	В	677	Н	В	С	Н	М	С	П
626	Н	С	В	Н	С	С	П	678	Н	В	С	Н	М	В	П
627	Н	С	В	Н	С	В	П	679	Н	В	С	Н	С	М	В
628	Н	С	В	Н	В	М	В	680	Н	В	С	Н	С	С	П
629	Н	С	В	Н	В	С	В	681	Н	В	С	Н	С	В	П
630	Н	С	В	Н	В	В	П	682	Н	В	С	Н	В	М	В
631	Н	С	В	С	М	М	В	683	Н	В	С	Н	В	С	В
632	Н	С	В	С	М	С	П	684	Н	В	С	Н	В	В	П
633	Н	С	В	С	М	В	П	685	Н	В	С	С	М	М	В
634	Н	С	В	С	С	М	В	686	Н	В	С	С	М	С	П
635	Н	С	В	С	С	С	В	687	Н	В	С	С	М	В	П
636	Н	С	В	С	С	В	П	688	Н	В	С	С	С	М	В
637	Н	С	В	С	В	М	В	689	Н	В	С	С	С	С	В
638	Н	С	В	С	В	С	В	690	Н	В	С	С	С	В	П
639	Н	С	В	С	В	В	В	691	Н	В	С	С	В	М	В
640	Н	С	В	В	М	М	В	692	Н	В	С	С	В	С	В
641	Н	С	В	В	М	С	В	693	Н	В	С	С	В	В	В
642	Н	С	В	В	М	В	П	694	Н	В	С	В	М	М	В
643	Н	С	В	В	С	М	В	695	Н	В	С	В	М	С	В
644	Н	С	В	В	С	С	В	696	Н	В	С	В	М	В	П
645	Н	С	В	В	С	В	В	697	Н	В	С	В	С	М	В
646	Н	С	В	В	В	М	К	698	Н	В	С	В	С	С	В
647	Н	С	В	В	В	С	В	699	Н	В	С	В	С	В	В
648	Н	С	В	В	В	В	В	700	Н	В	С	В	В	М	К
649	Н	В	Н	Н	М	М	П	701	Н	В	С	В	В	С	В
650	Н	В	Н	Н	М	С	П	702	Н	В	С	В	В	В	В
651	Н	В	Н	Н	М	В	С	703	Н	В	В	Н	М	М	В
652	Н	В	Н	Н	С	М	П	704	Н	В	В	Н	М	С	П
653	Н	В	Н	Н	С	С	П	705	Н	В	В	Н	М	В	П
654	Н	В	Н	Н	С	В	П	706	Н	В	В	Н	С	М	В
655	Н	В	Н	Н	В	М	В	707	Н	В	В	Н	С	С	В
656	Н	В	Н	Н	В	С	П	708	Н	В	В	Н	С	В	П
657	Н	В	Н	Н	В	В	П	709	Н	В	В	Н	В	М	В
658	Н	В	Н	С	М	М	П	710	Н	В	В	Н	В	С	В
659	Н	В	Н	С	М	С	П	711	Н	В	В	Н	В	В	В
660	Н	В	Н	С	М	В	П	712	Н	В	В	С	М	М	В
661	Н	В	Н	С	С	М	В	713	Н	В	В	С	М	С	В
662	Н	В	Н	С	С	С	П	714	Н	В	В	С	М	В	П
663	Н	В	Н	С	С	В	П	715	Н	В	В	С	С	М	В

716	Н	В	В	С	С	С	В	723	Н	В	В	В	М	В	В
717	Н	В	В	С	С	В	В	724	Н	В	В	В	С	М	К
718	Н	В	В	С	В	М	К	725	Н	В	В	В	С	С	В
719	Н	В	В	С	В	С	В	726	Н	В	В	В	С	В	В
720	Н	В	В	С	В	В	В	727	Н	В	В	В	В	М	К
721	Н	В	В	В	М	М	В	728	Н	В	В	В	В	С	К
722	Н	В	В	В	М	С	В	729	Н	В	В	В	В	В	В

Таблиця 2

Множина правил ER_2 для виявлення спаму

p	P_{CPU}	P_{MU}	P_{NEr}	P_{RTPr}	P_{CNCh}	Результат
1	Н	Н	М	М	Н	С
2	Н	Н	М	М	С	С
3	Н	Н	М	М	В	П
4	Н	Н	М	С	Н	Н
5	Н	Н	М	С	С	С
6	Н	Н	М	С	В	С
7	Н	Н	М	В	Н	Н
8	Н	Н	М	В	С	Н
9	Н	Н	М	В	В	С
10	Н	Н	С	М	Н	С
11	Н	Н	С	М	С	П
12	Н	Н	С	М	В	П
13	Н	Н	С	С	Н	С
14	Н	Н	С	С	С	С
15	Н	Н	С	С	В	П
16	Н	Н	С	В	Н	Н
17	Н	Н	С	В	С	С
18	Н	Н	С	В	В	С
19	Н	Н	В	М	Н	П
20	Н	Н	В	М	С	П
21	Н	Н	В	М	В	П
22	Н	Н	В	С	Н	С
23	Н	Н	В	С	С	П
24	Н	Н	В	С	В	П
25	Н	Н	В	В	Н	С
26	Н	Н	В	В	С	С
27	Н	Н	В	В	В	П
28	Н	С	М	М	Н	С
29	Н	С	М	М	С	П
30	Н	С	М	М	В	П
31	Н	С	М	С	Н	С
32	Н	С	М	С	С	С
33	Н	С	М	С	В	П
34	Н	С	М	В	Н	Н
35	Н	С	М	В	С	С
36	Н	С	М	В	В	С
37	Н	С	С	М	Н	П
38	Н	С	С	М	С	П
39	Н	С	С	М	В	П
40	Н	С	С	С	Н	С
41	Н	С	С	С	С	П
42	Н	С	С	С	В	П
43	Н	С	С	В	Н	С
44	Н	С	С	В	С	С
45	Н	С	С	В	В	П
46	Н	С	В	М	Н	П
47	Н	С	В	М	С	П
48	Н	С	В	М	В	В
49	Н	С	В	С	Н	П
50	Н	С	В	С	С	П
51	Н	С	В	С	В	П
52	Н	С	В	В	Н	С
53	Н	С	В	В	С	П
54	Н	С	В	В	В	П
55	Н	В	М	М	Н	П
56	Н	В	М	М	С	П
57	Н	В	М	М	В	П
58	Н	В	М	С	Н	С
59	Н	В	М	С	С	П
60	Н	В	М	С	В	П
61	Н	В	М	В	Н	С
62	Н	В	М	В	С	С
63	Н	В	М	В	В	П
64	Н	В	С	М	Н	П
65	Н	В	С	М	С	П
66	Н	В	С	М	В	В
67	Н	В	С	С	Н	П
68	Н	В	С	С	С	П
69	Н	В	С	С	В	П
70	Н	В	С	В	Н	С
71	Н	В	С	В	С	П
72	Н	В	С	В	В	П
73	Н	В	В	М	Н	П
74	Н	В	В	М	С	В
75	Н	В	В	М	В	В
76	Н	В	В	С	Н	П
77	Н	В	В	С	С	П

78	Н	В	В	С	В	В
79	Н	В	В	В	Н	П
80	Н	В	В	В	С	П
81	Н	В	В	В	В	П
82	С	Н	М	М	Н	С
83	С	Н	М	М	С	П
84	С	Н	М	М	В	П
85	С	Н	М	С	Н	С
86	С	Н	М	С	С	С
87	С	Н	М	С	В	П
88	С	Н	М	В	Н	Н
89	С	Н	М	В	С	С
90	С	Н	М	В	В	С
91	С	Н	С	М	Н	П
92	С	Н	С	М	С	П
93	С	Н	С	М	В	П
94	С	Н	С	С	Н	С
95	С	Н	С	С	С	П
96	С	Н	С	С	В	П
97	С	Н	С	В	Н	С
98	С	Н	С	В	С	С
99	С	Н	С	В	В	П
100	С	Н	В	М	Н	П
101	С	Н	В	М	С	П
102	С	Н	В	М	В	В
103	С	Н	В	С	Н	П
104	С	Н	В	С	С	П
105	С	Н	В	С	В	П
106	С	Н	В	В	Н	С
107	С	Н	В	В	С	П
108	С	Н	В	В	В	П
109	С	С	М	М	Н	П
110	С	С	М	М	С	П
111	С	С	М	М	В	П
112	С	С	М	С	Н	С
113	С	С	М	С	С	П
114	С	С	М	С	В	П
115	С	С	М	В	Н	С
116	С	С	М	В	С	С
117	С	С	М	В	В	П
118	С	С	С	М	Н	П
119	С	С	С	М	С	П
120	С	С	С	М	В	В
121	С	С	С	С	Н	П
122	С	С	С	С	С	П
123	С	С	С	С	В	П
124	С	С	С	В	Н	С
125	С	С	С	В	С	П
126	С	С	С	В	В	П
127	С	С	В	М	Н	П
128	С	С	В	М	С	В
129	С	С	В	М	В	В

130	С	С	В	С	Н	П
131	С	С	В	С	С	П
132	С	С	В	С	В	В
133	С	С	В	В	Н	П
134	С	С	В	В	С	П
135	С	С	В	В	В	П
136	С	В	М	М	Н	П
137	С	В	М	М	С	П
138	С	В	М	М	В	В
139	С	В	М	С	Н	П
140	С	В	М	С	С	П
141	С	В	М	С	В	П
142	С	В	М	В	Н	С
143	С	В	М	В	С	П
144	С	В	М	В	В	П
145	С	В	С	М	Н	П
146	С	В	С	М	С	В
147	С	В	С	М	В	В
148	С	В	С	С	Н	П
149	С	В	С	С	С	П
150	С	В	С	С	В	В
151	С	В	С	В	Н	П
152	С	В	С	В	С	П
153	С	В	С	В	В	П
154	С	В	В	М	Н	В
155	С	В	В	М	С	В
156	С	В	В	М	В	К
157	С	В	В	С	Н	П
158	С	В	В	С	С	В
159	С	В	В	С	В	В
160	С	В	В	В	Н	П
161	С	В	В	В	С	П
162	С	В	В	В	В	В
163	В	Н	М	М	Н	П
164	В	Н	М	М	С	П
165	В	Н	М	М	В	П
166	В	Н	М	С	Н	С
167	В	Н	М	С	С	П
168	В	Н	М	С	В	П
169	В	Н	М	В	Н	С
170	В	Н	М	В	С	С
171	В	Н	М	В	В	П
172	В	Н	С	М	Н	П
173	В	Н	С	М	С	П
174	В	Н	С	М	В	В
175	В	Н	С	С	Н	П
176	В	Н	С	С	С	П
177	В	Н	С	С	В	П
178	В	Н	С	В	Н	С
179	В	Н	С	В	С	П
180	В	Н	С	В	В	П
181	В	Н	В	М	Н	П

182	B	H	B	M	C	B
183	B	H	B	M	B	B
184	B	H	B	C	H	П
185	B	H	B	C	C	П
186	B	H	B	C	B	B
187	B	H	B	B	H	П
188	B	H	B	B	C	П
189	B	H	B	B	B	П
190	B	C	M	M	H	П
191	B	C	M	M	C	П
192	B	C	M	M	B	B
193	B	C	M	C	H	П
194	B	C	M	C	C	П
195	B	C	M	C	B	П
196	B	C	M	B	H	C
197	B	C	M	B	C	П
198	B	C	M	B	B	П
199	B	C	C	M	H	П
200	B	C	C	M	C	B
201	B	C	C	M	B	B
202	B	C	C	C	H	П
203	B	C	C	C	C	П
204	B	C	C	C	B	B
205	B	C	C	B	H	П
206	B	C	C	B	C	П
207	B	C	C	B	B	П
208	B	C	B	M	H	B
209	B	C	B	M	C	B
210	B	C	B	M	B	K
211	B	C	B	C	H	П
212	B	C	B	C	C	B
213	B	C	B	C	B	B

214	B	C	B	B	H	П
215	B	C	B	B	C	П
216	B	C	B	B	B	B
217	B	B	M	M	H	П
218	B	B	M	M	C	B
219	B	B	M	M	B	B
220	B	B	M	C	H	П
221	B	B	M	C	C	П
222	B	B	M	C	B	B
223	B	B	M	B	H	П
224	B	B	M	B	C	П
225	B	B	M	B	B	П
226	B	B	C	M	H	B
227	B	B	C	M	C	B
228	B	B	C	M	B	K
229	B	B	C	C	H	П
230	B	B	C	C	C	B
231	B	B	C	C	B	B
232	B	B	C	B	H	П
233	B	B	C	B	C	П
234	B	B	C	B	B	B
235	B	B	B	M	H	B
236	B	B	B	M	C	K
237	B	B	B	M	B	K
238	B	B	B	C	H	B
239	B	B	B	C	C	B
240	B	B	B	C	B	K
241	B	B	B	B	H	П
242	B	B	B	B	C	B
243	B	B	B	B	B	B

Таблиця 3

Множина правил ER_3 для виявлення атаки типу відмова в обслуговувані

p	P_{CPU}	P_{MU}	P_{NEr}	P_{CNCh}	P_{NCC}	P_{DbR}	Результат
1	H	H	M	H	M	M	C
2	H	H	M	H	M	C	H
3	H	H	M	H	M	B	H
4	H	H	M	H	C	M	C
5	H	H	M	H	C	C	C
6	H	H	M	H	C	B	H
7	H	H	M	H	B	M	C
8	H	H	M	H	B	C	C
9	H	H	M	H	B	B	C
10	H	H	M	C	M	M	C
11	H	H	M	C	M	C	C
12	H	H	M	C	M	B	H
13	H	H	M	C	C	M	C

14	H	H	M	C	C	C	C
15	H	H	M	C	C	B	C
16	H	H	M	C	B	M	П
17	H	H	M	C	B	C	C
18	H	H	M	C	B	B	C
19	H	H	M	B	M	M	C
20	H	H	M	B	M	C	C
21	H	H	M	B	M	B	C
22	H	H	M	B	C	M	П
23	H	H	M	B	C	C	C
24	H	H	M	B	C	B	C
25	H	H	M	B	B	M	П
26	H	H	M	B	B	C	П
27	H	H	M	B	B	B	C

28	Н	Н	С	Н	М	М	С	80	Н	Н	В	В	В	С	П
29	Н	Н	С	Н	М	С	С	81	Н	Н	В	В	В	В	П
30	Н	Н	С	Н	М	В	Н	82	Н	С	М	Н	М	М	С
31	Н	Н	С	Н	С	М	С	83	Н	С	М	Н	М	С	С
32	Н	Н	С	Н	С	С	С	84	Н	С	М	Н	М	В	Н
33	Н	Н	С	Н	С	В	С	85	Н	С	М	Н	С	М	С
34	Н	Н	С	Н	В	М	П	86	Н	С	М	Н	С	С	С
35	Н	Н	С	Н	В	С	С	87	Н	С	М	Н	С	В	С
36	Н	Н	С	Н	В	В	С	88	Н	С	М	Н	В	М	П
37	Н	Н	С	С	М	М	С	89	Н	С	М	Н	В	С	С
38	Н	Н	С	С	М	С	С	90	Н	С	М	Н	В	В	С
39	Н	Н	С	С	М	В	С	91	Н	С	М	С	М	М	С
40	Н	Н	С	С	С	М	П	92	Н	С	М	С	М	С	С
41	Н	Н	С	С	С	С	С	93	Н	С	М	С	М	В	С
42	Н	Н	С	С	С	В	С	94	Н	С	М	С	С	М	П
43	Н	Н	С	С	В	М	П	95	Н	С	М	С	С	С	С
44	Н	Н	С	С	В	С	П	96	Н	С	М	С	С	В	С
45	Н	Н	С	С	В	В	С	97	Н	С	М	С	В	М	П
46	Н	Н	С	В	М	М	П	98	Н	С	М	С	В	С	П
47	Н	Н	С	В	М	С	П	99	Н	С	М	С	В	В	С
48	Н	Н	С	В	М	В	С	100	Н	С	М	В	М	М	П
49	Н	Н	С	В	С	М	П	101	Н	С	М	В	М	С	С
50	Н	Н	С	В	С	С	П	102	Н	С	М	В	М	В	С
51	Н	Н	С	В	С	В	П	103	Н	С	М	В	С	М	П
52	Н	Н	С	В	В	М	В	104	Н	С	М	В	С	С	П
53	Н	Н	С	В	В	С	П	105	Н	С	М	В	С	В	С
54	Н	Н	С	В	В	В	П	106	Н	С	М	В	В	М	П
55	Н	Н	В	Н	М	М	С	107	Н	С	М	В	В	С	П
56	Н	Н	В	Н	М	С	С	108	Н	С	М	В	В	В	П
57	Н	Н	В	Н	М	В	Н	109	Н	С	С	Н	М	М	С
58	Н	Н	В	Н	С	М	С	110	Н	С	С	Н	М	С	С
59	Н	Н	В	Н	С	С	С	111	Н	С	С	Н	М	В	С
60	Н	Н	В	Н	С	В	С	112	Н	С	С	Н	С	М	П
61	Н	Н	В	Н	В	М	П	113	Н	С	С	Н	С	С	С
62	Н	Н	В	Н	В	С	С	114	Н	С	С	Н	С	В	С
63	Н	Н	В	Н	В	В	С	115	Н	С	С	Н	В	М	П
64	Н	Н	В	С	М	М	П	116	Н	С	С	Н	В	С	П
65	Н	Н	В	С	М	С	С	117	Н	С	С	Н	В	В	С
66	Н	Н	В	С	М	В	С	118	Н	С	С	С	М	М	П
67	Н	Н	В	С	С	М	П	119	Н	С	С	С	М	С	С
68	Н	Н	В	С	С	С	П	120	Н	С	С	С	М	В	С
69	Н	Н	В	С	С	В	С	121	Н	С	С	С	С	М	П
70	Н	Н	В	С	В	М	П	122	Н	С	С	С	С	С	П
71	Н	Н	В	С	В	С	П	123	Н	С	С	С	С	В	С
72	Н	Н	В	С	В	В	П	124	Н	С	С	С	В	М	П
73	Н	Н	В	В	М	М	П	125	Н	С	С	С	В	С	П
74	Н	Н	В	В	М	С	П	126	Н	С	С	С	В	В	П
75	Н	Н	В	В	М	В	С	127	Н	С	С	В	М	М	П
76	Н	Н	В	В	С	М	П	128	Н	С	С	В	М	С	П
77	Н	Н	В	В	С	С	П	129	Н	С	С	В	М	В	С
78	Н	Н	В	В	С	В	П	130	Н	С	С	В	С	М	П
79	Н	Н	В	В	В	М	В	131	Н	С	С	В	С	С	П

132	Н	С	С	В	С	В	П
133	Н	С	С	В	В	М	В
134	Н	С	С	В	В	С	П
135	Н	С	С	В	В	В	П
136	Н	С	В	Н	М	М	П
137	Н	С	В	Н	М	С	С
138	Н	С	В	Н	М	В	С
139	Н	С	В	Н	С	М	П
140	Н	С	В	Н	С	С	П
141	Н	С	В	Н	С	В	С
142	Н	С	В	Н	В	М	П
143	Н	С	В	Н	В	С	П
144	Н	С	В	Н	В	В	П
145	Н	С	В	С	М	М	П
146	Н	С	В	С	М	С	П
147	Н	С	В	С	М	В	С
148	Н	С	В	С	С	М	П
149	Н	С	В	С	С	С	П
150	Н	С	В	С	С	В	П
151	Н	С	В	С	В	М	В
152	Н	С	В	С	В	С	П
153	Н	С	В	С	В	В	П
154	Н	С	В	В	М	М	П
155	Н	С	В	В	М	С	П
156	Н	С	В	В	М	В	П
157	Н	С	В	В	С	М	В
158	Н	С	В	В	С	С	П
159	Н	С	В	В	С	В	П
160	Н	С	В	В	В	М	В
161	Н	С	В	В	В	С	В
162	Н	С	В	В	В	В	П
163	Н	В	М	Н	М	М	С
164	Н	В	М	Н	М	С	С
165	Н	В	М	Н	М	В	С
166	Н	В	М	Н	С	М	П
167	Н	В	М	Н	С	С	С
168	Н	В	М	Н	С	В	С
169	Н	В	М	Н	В	М	П
170	Н	В	М	Н	В	С	П
171	Н	В	М	Н	В	В	С
172	Н	В	М	С	М	М	П
173	Н	В	М	С	М	С	С
174	Н	В	М	С	М	В	С
175	Н	В	М	С	С	М	П
176	Н	В	М	С	С	С	П
177	Н	В	М	С	С	В	С
178	Н	В	М	С	В	М	П
179	Н	В	М	С	В	С	П
180	Н	В	М	С	В	В	П
181	Н	В	М	В	М	М	П
182	Н	В	М	В	М	С	П
183	Н	В	М	В	М	В	С
184	Н	В	М	В	С	М	П
185	Н	В	М	В	С	С	П
186	Н	В	М	В	С	В	П
187	Н	В	М	В	В	М	В
188	Н	В	М	В	В	С	П
189	Н	В	М	В	В	В	П
190	Н	В	С	Н	М	М	П
191	Н	В	С	Н	М	С	С
192	Н	В	С	Н	М	В	С
193	Н	В	С	Н	С	М	П
194	Н	В	С	Н	С	С	П
195	Н	В	С	Н	С	В	С
196	Н	В	С	Н	В	М	П
197	Н	В	С	Н	В	С	П
198	Н	В	С	Н	В	В	П
199	Н	В	С	С	М	М	П
200	Н	В	С	С	М	С	П
201	Н	В	С	С	М	В	С
202	Н	В	С	С	С	М	П
203	Н	В	С	С	С	С	П
204	Н	В	С	С	С	В	П
205	Н	В	С	С	В	М	В
206	Н	В	С	С	В	С	П
207	Н	В	С	С	В	В	П
208	Н	В	С	В	М	М	П
209	Н	В	С	В	М	С	П
210	Н	В	С	В	М	В	П
211	Н	В	С	В	С	М	В
212	Н	В	С	В	С	С	П
213	Н	В	С	В	С	В	П
214	Н	В	С	В	В	М	В
215	Н	В	С	В	В	С	В
216	Н	В	С	В	В	В	П
217	Н	В	В	Н	М	М	П
218	Н	В	В	Н	М	С	П
219	Н	В	В	Н	М	В	С
220	Н	В	В	Н	С	М	П
221	Н	В	В	Н	С	С	П
222	Н	В	В	Н	С	В	П
223	Н	В	В	Н	В	М	В
224	Н	В	В	Н	В	С	П
225	Н	В	В	Н	В	В	П
226	Н	В	В	С	М	М	П
227	Н	В	В	С	М	С	П
228	Н	В	В	С	М	В	П
229	Н	В	В	С	С	М	В
230	Н	В	В	С	С	С	П
231	Н	В	В	С	С	В	П
232	Н	В	В	С	В	М	В
233	Н	В	В	С	В	С	В
234	Н	В	В	С	В	В	П
235	Н	В	В	В	М	М	В

236	Н	В	В	В	М	С	П
237	Н	В	В	В	М	В	П
238	Н	В	В	В	С	М	В
239	Н	В	В	В	С	С	В
240	Н	В	В	В	С	В	П
241	Н	В	В	В	В	М	В
242	Н	В	В	В	В	С	В
243	Н	В	В	В	В	В	В
244	С	Н	М	Н	М	М	С
245	С	Н	М	Н	М	С	С
246	С	Н	М	Н	М	В	Н
247	С	Н	М	Н	С	М	С
248	С	Н	М	Н	С	С	С
249	С	Н	М	Н	С	В	С
250	С	Н	М	Н	В	М	П
251	С	Н	М	Н	В	С	С
252	С	Н	М	Н	В	В	С
253	С	Н	М	С	М	М	С
254	С	Н	М	С	М	С	С
255	С	Н	М	С	М	В	С
256	С	Н	М	С	С	М	П
257	С	Н	М	С	С	С	С
258	С	Н	М	С	С	В	С
259	С	Н	М	С	В	М	П
260	С	Н	М	С	В	С	П
261	С	Н	М	С	В	В	С
262	С	Н	М	В	М	М	П
263	С	Н	М	В	М	С	С
264	С	Н	М	В	М	В	С
265	С	Н	М	В	С	М	П
266	С	Н	М	В	С	С	П
267	С	Н	М	В	С	В	С
268	С	Н	М	В	В	М	П
269	С	Н	М	В	В	С	П
270	С	Н	М	В	В	В	П
271	С	Н	С	Н	М	М	С
272	С	Н	С	Н	М	С	С
273	С	Н	С	Н	М	В	С
274	С	Н	С	Н	С	М	П
275	С	Н	С	Н	С	С	С
276	С	Н	С	Н	С	В	С
277	С	Н	С	Н	В	М	П
278	С	Н	С	Н	В	С	П
279	С	Н	С	Н	В	В	С
280	С	Н	С	С	М	М	П
281	С	Н	С	С	М	С	С
282	С	Н	С	С	М	В	С
283	С	Н	С	С	С	М	П
284	С	Н	С	С	С	С	П
285	С	Н	С	С	С	В	С
286	С	Н	С	С	В	М	П
287	С	Н	С	С	В	С	П
288	С	Н	С	С	В	В	П
289	С	Н	С	В	М	М	П
290	С	Н	С	В	М	С	П
291	С	Н	С	В	М	В	С
292	С	Н	С	В	С	М	П
293	С	Н	С	В	С	С	П
294	С	Н	С	В	С	В	П
295	С	Н	С	В	В	М	В
296	С	Н	С	В	В	С	П
297	С	Н	С	В	В	В	П
298	С	Н	В	Н	М	М	П
299	С	Н	В	Н	М	С	С
300	С	Н	В	Н	М	В	С
301	С	Н	В	Н	С	М	П
302	С	Н	В	Н	С	С	П
303	С	Н	В	Н	С	В	С
304	С	Н	В	Н	В	М	П
305	С	Н	В	Н	В	С	П
306	С	Н	В	Н	В	В	П
307	С	Н	В	С	М	М	П
308	С	Н	В	С	М	С	П
309	С	Н	В	С	М	В	С
310	С	Н	В	С	С	М	П
311	С	Н	В	С	С	С	П
312	С	Н	В	С	С	В	П
313	С	Н	В	С	В	М	В
314	С	Н	В	С	В	С	П
315	С	Н	В	С	В	В	П
316	С	Н	В	В	М	М	П
317	С	Н	В	В	М	С	П
318	С	Н	В	В	М	В	П
319	С	Н	В	В	С	М	В
320	С	Н	В	В	С	С	П
321	С	Н	В	В	С	В	П
322	С	Н	В	В	В	М	В
323	С	Н	В	В	В	С	В
324	С	Н	В	В	В	В	П
325	С	С	М	Н	М	М	С
326	С	С	М	Н	М	С	С
327	С	С	М	Н	М	В	С
328	С	С	М	Н	С	М	П
329	С	С	М	Н	С	С	С
330	С	С	М	Н	С	В	С
331	С	С	М	Н	В	М	П
332	С	С	М	Н	В	С	П
333	С	С	М	Н	В	В	С
334	С	С	М	С	М	М	П
335	С	С	М	С	М	С	С
336	С	С	М	С	М	В	С
337	С	С	М	С	С	М	П
338	С	С	М	С	С	С	П
339	С	С	М	С	С	В	С

340	С	С	М	С	В	М	П	392	С	С	В	С	С	С	П
341	С	С	М	С	В	С	П	393	С	С	В	С	С	В	П
342	С	С	М	С	В	В	П	394	С	С	В	С	В	М	В
343	С	С	М	В	М	М	П	395	С	С	В	С	В	С	В
344	С	С	М	В	М	С	П	396	С	С	В	С	В	В	П
345	С	С	М	В	М	В	С	397	С	С	В	В	М	М	В
346	С	С	М	В	С	М	П	398	С	С	В	В	М	С	П
347	С	С	М	В	С	С	П	399	С	С	В	В	М	В	П
348	С	С	М	В	С	В	П	400	С	С	В	В	С	М	В
349	С	С	М	В	В	М	В	401	С	С	В	В	С	С	В
350	С	С	М	В	В	С	П	402	С	С	В	В	С	В	П
351	С	С	М	В	В	В	П	403	С	С	В	В	В	М	В
352	С	С	С	Н	М	М	П	404	С	С	В	В	В	С	В
353	С	С	С	Н	М	С	С	405	С	С	В	В	В	В	В
354	С	С	С	Н	М	В	С	406	С	В	М	Н	М	М	П
355	С	С	С	Н	С	М	П	407	С	В	М	Н	М	С	С
356	С	С	С	Н	С	С	П	408	С	В	М	Н	М	В	С
357	С	С	С	Н	С	В	С	409	С	В	М	Н	С	М	П
358	С	С	С	Н	В	М	П	410	С	В	М	Н	С	С	П
359	С	С	С	Н	В	С	П	411	С	В	М	Н	С	В	С
360	С	С	С	Н	В	В	П	412	С	В	М	Н	В	М	П
361	С	С	С	С	М	М	П	413	С	В	М	Н	В	С	П
362	С	С	С	С	М	С	П	414	С	В	М	Н	В	В	П
363	С	С	С	С	М	В	С	415	С	В	М	С	М	М	П
364	С	С	С	С	С	М	П	416	С	В	М	С	М	С	П
365	С	С	С	С	С	С	П	417	С	В	М	С	М	В	С
366	С	С	С	С	С	В	П	418	С	В	М	С	С	М	П
367	С	С	С	С	В	М	В	419	С	В	М	С	С	С	П
368	С	С	С	С	В	С	П	420	С	В	М	С	С	В	П
369	С	С	С	С	В	В	П	421	С	В	М	С	В	М	В
370	С	С	С	В	М	М	П	422	С	В	М	С	В	С	П
371	С	С	С	В	М	С	П	423	С	В	М	С	В	В	П
372	С	С	С	В	М	В	П	424	С	В	М	В	М	М	П
373	С	С	С	В	С	М	В	425	С	В	М	В	М	С	П
374	С	С	С	В	С	С	П	426	С	В	М	В	М	В	П
375	С	С	С	В	С	В	П	427	С	В	М	В	С	М	В
376	С	С	С	В	В	М	В	428	С	В	М	В	С	С	П
377	С	С	С	В	В	С	В	429	С	В	М	В	С	В	П
378	С	С	С	В	В	В	П	430	С	В	М	В	В	М	В
379	С	С	В	Н	М	М	П	431	С	В	М	В	В	С	В
380	С	С	В	Н	М	С	П	432	С	В	М	В	В	В	П
381	С	С	В	Н	М	В	С	433	С	В	С	Н	М	М	П
382	С	С	В	Н	С	М	П	434	С	В	С	Н	М	С	П
383	С	С	В	Н	С	С	П	435	С	В	С	Н	М	В	С
384	С	С	В	Н	С	В	П	436	С	В	С	Н	С	М	П
385	С	С	В	Н	В	М	В	437	С	В	С	Н	С	С	П
386	С	С	В	Н	В	С	П	438	С	В	С	Н	С	В	П
387	С	С	В	Н	В	В	П	439	С	В	С	Н	В	М	В
388	С	С	В	С	М	М	П	440	С	В	С	Н	В	С	П
389	С	С	В	С	М	С	П	441	С	В	С	Н	В	В	П
390	С	С	В	С	М	В	П	442	С	В	С	С	М	М	П
391	С	С	В	С	С	М	В	443	С	В	С	С	М	С	П

444	С	В	С	С	М	В	П	496	В	Н	М	С	М	М	П
445	С	В	С	С	С	М	В	497	В	Н	М	С	М	С	С
446	С	В	С	С	С	С	П	498	В	Н	М	С	М	В	С
447	С	В	С	С	С	В	П	499	В	Н	М	С	С	М	П
448	С	В	С	С	В	М	В	500	В	Н	М	С	С	С	П
449	С	В	С	С	В	С	В	501	В	Н	М	С	С	В	С
450	С	В	С	С	В	В	П	502	В	Н	М	С	В	М	П
451	С	В	С	В	М	М	В	503	В	Н	М	С	В	С	П
452	С	В	С	В	М	С	П	504	В	Н	М	С	В	В	П
453	С	В	С	В	М	В	П	505	В	Н	М	В	М	М	П
454	С	В	С	В	С	М	В	506	В	Н	М	В	М	С	П
455	С	В	С	В	С	С	В	507	В	Н	М	В	М	В	С
456	С	В	С	В	С	В	П	508	В	Н	М	В	С	М	П
457	С	В	С	В	В	М	В	509	В	Н	М	В	С	С	П
458	С	В	С	В	В	С	В	510	В	Н	М	В	С	В	П
459	С	В	С	В	В	В	В	511	В	Н	М	В	В	М	В
460	С	В	В	Н	М	М	П	512	В	Н	М	В	В	С	П
461	С	В	В	Н	М	С	П	513	В	Н	М	В	В	В	П
462	С	В	В	Н	М	В	П	514	В	Н	С	Н	М	М	П
463	С	В	В	Н	С	М	В	515	В	Н	С	Н	М	С	С
464	С	В	В	Н	С	С	П	516	В	Н	С	Н	М	В	С
465	С	В	В	Н	С	В	П	517	В	Н	С	Н	С	М	П
466	С	В	В	Н	В	М	В	518	В	Н	С	Н	С	С	П
467	С	В	В	Н	В	С	В	519	В	Н	С	Н	С	В	С
468	С	В	В	Н	В	В	П	520	В	Н	С	Н	В	М	П
469	С	В	В	С	М	М	В	521	В	Н	С	Н	В	С	П
470	С	В	В	С	М	С	П	522	В	Н	С	Н	В	В	П
471	С	В	В	С	М	В	П	523	В	Н	С	С	М	М	П
472	С	В	В	С	С	М	В	524	В	Н	С	С	М	С	П
473	С	В	В	С	С	С	В	525	В	Н	С	С	М	В	С
474	С	В	В	С	С	В	П	526	В	Н	С	С	С	М	П
475	С	В	В	С	В	М	В	527	В	Н	С	С	С	С	П
476	С	В	В	С	В	С	В	528	В	Н	С	С	С	В	П
477	С	В	В	С	В	В	В	529	В	Н	С	С	В	М	В
478	С	В	В	В	М	М	В	530	В	Н	С	С	В	С	П
479	С	В	В	В	М	С	В	531	В	Н	С	С	В	В	П
480	С	В	В	В	М	В	П	532	В	Н	С	В	М	М	П
481	С	В	В	В	С	М	В	533	В	Н	С	В	М	С	П
482	С	В	В	В	С	С	В	534	В	Н	С	В	М	В	П
483	С	В	В	В	С	В	В	535	В	Н	С	В	С	М	В
484	С	В	В	В	В	М	К	536	В	Н	С	В	С	С	П
485	С	В	В	В	В	С	В	537	В	Н	С	В	С	В	П
486	С	В	В	В	В	В	В	538	В	Н	С	В	В	М	В
487	В	Н	М	Н	М	М	С	539	В	Н	С	В	В	С	В
488	В	Н	М	Н	М	С	С	540	В	Н	С	В	В	В	П
489	В	Н	М	Н	М	В	С	541	В	Н	В	Н	М	М	П
490	В	Н	М	Н	С	М	П	542	В	Н	В	Н	М	С	П
491	В	Н	М	Н	С	С	С	543	В	Н	В	Н	М	В	С
492	В	Н	М	Н	С	В	С	544	В	Н	В	Н	С	М	П
493	В	Н	М	Н	В	М	П	545	В	Н	В	Н	С	С	П
494	В	Н	М	Н	В	С	П	546	В	Н	В	Н	С	В	П
495	В	Н	М	Н	В	В	С	547	В	Н	В	Н	В	М	В

548	В	Н	В	Н	В	С	П	600	В	С	С	Н	С	В	П
549	В	Н	В	Н	В	В	П	601	В	С	С	Н	В	М	В
550	В	Н	В	С	М	М	П	602	В	С	С	Н	В	С	П
551	В	Н	В	С	М	С	П	603	В	С	С	Н	В	В	П
552	В	Н	В	С	М	В	П	604	В	С	С	С	М	М	П
553	В	Н	В	С	С	М	В	605	В	С	С	С	М	С	П
554	В	Н	В	С	С	С	П	606	В	С	С	С	М	В	П
555	В	Н	В	С	С	В	П	607	В	С	С	С	С	М	В
556	В	Н	В	С	В	М	В	608	В	С	С	С	С	С	П
557	В	Н	В	С	В	С	В	609	В	С	С	С	С	В	П
558	В	Н	В	С	В	В	П	610	В	С	С	С	В	М	В
559	В	Н	В	В	М	М	В	611	В	С	С	С	В	С	В
560	В	Н	В	В	М	С	В	612	В	С	С	С	В	В	П
561	В	Н	В	В	М	В	П	613	В	С	С	В	М	М	В
562	В	Н	В	В	С	М	В	614	В	С	С	В	М	С	П
563	В	Н	В	В	С	С	В	615	В	С	С	В	М	В	П
564	В	Н	В	В	С	В	П	616	В	С	С	В	С	М	В
565	В	Н	В	В	В	М	В	617	В	С	С	В	С	С	В
566	В	Н	В	В	В	С	В	618	В	С	С	В	С	В	П
567	В	Н	В	В	В	В	В	619	В	С	С	В	В	М	В
568	В	С	М	Н	М	М	П	620	В	С	С	В	В	С	В
569	В	С	М	Н	М	С	С	621	В	С	С	В	В	В	В
570	В	С	М	Н	М	В	С	622	В	С	В	Н	М	М	П
571	В	С	М	Н	С	М	П	623	В	С	В	Н	М	С	П
572	В	С	М	Н	С	С	П	624	В	С	В	Н	М	В	П
573	В	С	М	Н	С	В	С	625	В	С	В	Н	С	М	В
574	В	С	М	Н	В	М	П	626	В	С	В	Н	С	С	П
575	В	С	М	Н	В	С	П	627	В	С	В	Н	С	В	П
576	В	С	М	Н	В	В	П	628	В	С	В	Н	В	М	В
577	В	С	М	С	М	М	П	629	В	С	В	Н	В	С	В
578	В	С	М	С	М	С	П	630	В	С	В	Н	В	В	П
579	В	С	М	С	М	В	С	631	В	С	В	С	М	М	В
580	В	С	М	С	С	М	П	632	В	С	В	С	М	С	П
581	В	С	М	С	С	С	П	633	В	С	В	С	М	В	П
582	В	С	М	С	С	В	П	634	В	С	В	С	С	М	В
583	В	С	М	С	В	М	В	635	В	С	В	С	С	С	В
584	В	С	М	С	В	С	П	636	В	С	В	С	С	В	П
585	В	С	М	С	В	В	П	637	В	С	В	С	В	М	В
586	В	С	М	В	М	М	П	638	В	С	В	С	В	С	В
587	В	С	М	В	М	С	П	639	В	С	В	С	В	В	В
588	В	С	М	В	М	В	П	640	В	С	В	В	М	М	В
589	В	С	М	В	С	М	В	641	В	С	В	В	М	С	В
590	В	С	М	В	С	С	П	642	В	С	В	В	М	В	П
591	В	С	М	В	С	В	П	643	В	С	В	В	С	М	В
592	В	С	М	В	В	М	В	644	В	С	В	В	С	С	В
593	В	С	М	В	В	С	В	645	В	С	В	В	С	В	В
594	В	С	М	В	В	В	П	646	В	С	В	В	В	М	К
595	В	С	С	Н	М	М	П	647	В	С	В	В	В	С	В
596	В	С	С	Н	М	С	П	648	В	С	В	В	В	В	В
597	В	С	С	Н	М	В	С	649	В	В	М	Н	М	М	П
598	В	С	С	Н	С	М	П	650	В	В	М	Н	М	С	П
599	В	С	С	Н	С	С	П	651	В	В	М	Н	М	В	С

652	В	В	М	Н	С	М	П
653	В	В	М	Н	С	С	П
654	В	В	М	Н	С	В	П
655	В	В	М	Н	В	М	В
656	В	В	М	Н	В	С	П
657	В	В	М	Н	В	В	П
658	В	В	М	С	М	М	П
659	В	В	М	С	М	С	П
660	В	В	М	С	М	В	П
661	В	В	М	С	С	М	В
662	В	В	М	С	С	С	П
663	В	В	М	С	С	В	П
664	В	В	М	С	В	М	В
665	В	В	М	С	В	С	В
666	В	В	М	С	В	В	П
667	В	В	М	В	М	М	В
668	В	В	М	В	М	С	П
669	В	В	М	В	М	В	П
670	В	В	М	В	С	М	В
671	В	В	М	В	С	С	В
672	В	В	М	В	С	В	П
673	В	В	М	В	В	М	В
674	В	В	М	В	В	С	В
675	В	В	М	В	В	В	В
676	В	В	С	Н	М	М	П
677	В	В	С	Н	М	С	П
678	В	В	С	Н	М	В	П
679	В	В	С	Н	С	М	В
680	В	В	С	Н	С	С	П
681	В	В	С	Н	С	В	П
682	В	В	С	Н	В	М	В
683	В	В	С	Н	В	С	В
684	В	В	С	Н	В	В	П
685	В	В	С	С	М	М	В
686	В	В	С	С	М	С	П
687	В	В	С	С	М	В	П
688	В	В	С	С	С	М	В
689	В	В	С	С	С	С	В
690	В	В	С	С	С	В	П
691	В	В	С	С	В	М	В

692	В	В	С	С	В	С	В
693	В	В	С	С	В	В	В
694	В	В	С	В	М	М	В
695	В	В	С	В	М	С	В
696	В	В	С	В	М	В	П
697	В	В	С	В	С	М	В
698	В	В	С	В	С	С	В
699	В	В	С	В	С	В	В
700	В	В	С	В	В	М	К
701	В	В	С	В	В	С	В
702	В	В	С	В	В	В	В
703	В	В	В	Н	М	М	В
704	В	В	В	Н	М	С	П
705	В	В	В	Н	М	В	П
706	В	В	В	Н	С	М	В
707	В	В	В	Н	С	С	В
708	В	В	В	Н	С	В	П
709	В	В	В	Н	В	М	В
710	В	В	В	Н	В	С	В
711	В	В	В	Н	В	В	В
712	В	В	В	С	М	М	В
713	В	В	В	С	М	С	В
714	В	В	В	С	М	В	П
715	В	В	В	С	С	М	В
716	В	В	В	С	С	С	В
717	В	В	В	С	С	В	В
718	В	В	В	С	В	М	К
719	В	В	В	С	В	С	В
720	В	В	В	С	В	В	В
721	В	В	В	В	М	М	В
722	В	В	В	В	М	С	В
723	В	В	В	В	М	В	В
724	В	В	В	В	С	М	К
725	В	В	В	В	С	С	В
726	В	В	В	В	С	В	В
727	В	В	В	В	В	М	К
728	В	В	В	В	В	С	К
729	В	В	В	В	В	В	В

Таблиця 4

Множина правил ER_4 для виявлення вірусної атаки

p	P_{CPU}	P_{MU}	P_{NEr}	P_{CNCh}	P_{STF}	Результат
1	Н	Н	М	Н	М	Н
2	Н	Н	М	Н	С	Н
3	Н	Н	М	Н	В	С
4	Н	Н	М	С	М	Н
5	Н	Н	М	С	С	С
6	Н	Н	М	С	В	С
7	Н	Н	М	В	М	С
8	Н	Н	М	В	С	С
9	Н	Н	М	В	В	П
10	Н	Н	С	Н	М	Н
11	Н	Н	С	Н	С	С

12	Н	Н	С	Н	В	С
13	Н	Н	С	С	М	С
14	Н	Н	С	С	С	С
15	Н	Н	С	С	В	П
16	Н	Н	С	В	М	С
17	Н	Н	С	В	С	П
18	Н	Н	С	В	В	П
19	Н	Н	В	Н	М	С
20	Н	Н	В	Н	С	С
21	Н	Н	В	Н	В	П
22	Н	Н	В	С	М	С
23	Н	Н	В	С	С	П
24	Н	Н	В	С	В	П
25	Н	Н	В	В	М	П
26	Н	Н	В	В	С	П
27	Н	Н	В	В	В	П
28	Н	С	М	Н	М	Н
29	Н	С	М	Н	С	С
30	Н	С	М	Н	В	С
31	Н	С	М	С	М	С
32	Н	С	М	С	С	С
33	Н	С	М	С	В	П
34	Н	С	М	В	М	С
35	Н	С	М	В	С	П
36	Н	С	М	В	В	П
37	Н	С	С	Н	М	С
38	Н	С	С	Н	С	С
39	Н	С	С	Н	В	П
40	Н	С	С	С	М	С
41	Н	С	С	С	С	П
42	Н	С	С	С	В	П
43	Н	С	С	В	М	П
44	Н	С	С	В	С	П
45	Н	С	С	В	В	П
46	Н	С	В	Н	М	С
47	Н	С	В	Н	С	П
48	Н	С	В	Н	В	П
49	Н	С	В	С	М	П
50	Н	С	В	С	С	П
51	Н	С	В	С	В	П
52	Н	С	В	В	М	П
53	Н	С	В	В	С	П
54	Н	С	В	В	В	В
55	Н	В	М	Н	М	С
56	Н	В	М	Н	С	С
57	Н	В	М	Н	В	П
58	Н	В	М	С	М	С
59	Н	В	М	С	С	П
60	Н	В	М	С	В	П
61	Н	В	М	В	М	П
62	Н	В	М	В	С	П
63	Н	В	М	В	В	П

64	Н	В	С	Н	М	С
65	Н	В	С	Н	С	П
66	Н	В	С	Н	В	П
67	Н	В	С	С	М	П
68	Н	В	С	С	С	П
69	Н	В	С	С	В	П
70	Н	В	С	В	М	П
71	Н	В	С	В	С	П
72	Н	В	С	В	В	В
73	Н	В	В	Н	М	П
74	Н	В	В	Н	С	П
75	Н	В	В	Н	В	П
76	Н	В	В	С	М	П
77	Н	В	В	С	С	П
78	Н	В	В	С	В	В
79	Н	В	В	В	М	П
80	Н	В	В	В	С	В
81	Н	В	В	В	В	В
82	С	Н	М	Н	М	Н
83	С	Н	М	Н	С	С
84	С	Н	М	Н	В	С
85	С	Н	М	С	М	С
86	С	Н	М	С	С	С
87	С	Н	М	С	В	П
88	С	Н	М	В	М	С
89	С	Н	М	В	С	П
90	С	Н	М	В	В	П
91	С	Н	С	Н	М	С
92	С	Н	С	Н	С	С
93	С	Н	С	Н	В	П
94	С	Н	С	С	М	С
95	С	Н	С	С	С	П
96	С	Н	С	С	В	П
97	С	Н	С	В	М	П
98	С	Н	С	В	С	П
99	С	Н	С	В	В	П
100	С	Н	В	Н	М	С
101	С	Н	В	Н	С	П
102	С	Н	В	Н	В	П
103	С	Н	В	С	М	П
104	С	Н	В	С	С	П
105	С	Н	В	С	В	П
106	С	Н	В	В	М	П
107	С	Н	В	В	С	П
108	С	Н	В	В	В	В
109	С	С	М	Н	М	С
110	С	С	М	Н	С	С
111	С	С	М	Н	В	П
112	С	С	М	С	М	С
113	С	С	М	С	С	П
114	С	С	М	С	В	П
115	С	С	М	В	М	П

116	С	С	М	В	С	П
117	С	С	М	В	В	П
118	С	С	С	Н	М	С
119	С	С	С	Н	С	П
120	С	С	С	Н	В	П
121	С	С	С	С	М	П
122	С	С	С	С	С	П
123	С	С	С	С	В	П
124	С	С	С	В	М	П
125	С	С	С	В	С	П
126	С	С	С	В	В	В
127	С	С	В	Н	М	П
128	С	С	В	Н	С	П
129	С	С	В	Н	В	П
130	С	С	В	С	М	П
131	С	С	В	С	С	П
132	С	С	В	С	В	В
133	С	С	В	В	М	П
134	С	С	В	В	С	В
135	С	С	В	В	В	В
136	С	В	М	Н	М	С
137	С	В	М	Н	С	П
138	С	В	М	Н	В	П
139	С	В	М	С	М	П
140	С	В	М	С	С	П
141	С	В	М	С	В	П
142	С	В	М	В	М	П
143	С	В	М	В	С	П
144	С	В	М	В	В	В
145	С	В	С	Н	М	П
146	С	В	С	Н	С	П
147	С	В	С	Н	В	П
148	С	В	С	С	М	П
149	С	В	С	С	С	П
150	С	В	С	С	В	В
151	С	В	С	В	М	П
152	С	В	С	В	С	В
153	С	В	С	В	В	В
154	С	В	В	Н	М	П
155	С	В	В	Н	С	П
156	С	В	В	Н	В	В
157	С	В	В	С	М	П
158	С	В	В	С	С	В
159	С	В	В	С	В	В
160	С	В	В	В	М	В
161	С	В	В	В	С	В
162	С	В	В	В	В	К
163	В	Н	М	Н	М	С
164	В	Н	М	Н	С	С
165	В	Н	М	Н	В	П
166	В	Н	М	С	М	С
167	В	Н	М	С	С	П

168	В	Н	М	С	В	П
169	В	Н	М	В	М	П
170	В	Н	М	В	С	П
171	В	Н	М	В	В	П
172	В	Н	С	Н	М	С
173	В	Н	С	Н	С	П
174	В	Н	С	Н	В	П
175	В	Н	С	С	М	П
176	В	Н	С	С	С	П
177	В	Н	С	С	В	П
178	В	Н	С	В	М	П
179	В	Н	С	В	С	П
180	В	Н	С	В	В	В
181	В	Н	В	Н	М	П
182	В	Н	В	Н	С	П
183	В	Н	В	Н	В	П
184	В	Н	В	С	М	П
185	В	Н	В	С	С	П
186	В	Н	В	С	В	В
187	В	Н	В	В	М	П
188	В	Н	В	В	С	В
189	В	Н	В	В	В	В
190	В	С	М	Н	М	С
191	В	С	М	Н	С	П
192	В	С	М	Н	В	П
193	В	С	М	С	М	П
194	В	С	М	С	С	П
195	В	С	М	С	В	П
196	В	С	М	В	М	П
197	В	С	М	В	С	П
198	В	С	М	В	В	В
199	В	С	С	Н	М	П
200	В	С	С	Н	С	П
201	В	С	С	Н	В	П
202	В	С	С	С	М	П
203	В	С	С	С	С	П
204	В	С	С	С	В	В
205	В	С	С	В	М	П
206	В	С	С	В	С	В
207	В	С	С	В	В	В
208	В	С	В	Н	М	П
209	В	С	В	Н	С	П
210	В	С	В	Н	В	В
211	В	С	В	С	М	П
212	В	С	В	С	С	В
213	В	С	В	С	В	В
214	В	С	В	В	М	В
215	В	С	В	В	С	В
216	В	С	В	В	В	К
217	В	В	М	Н	М	П
218	В	В	М	Н	С	П
219	В	В	М	Н	В	П

220	В	В	М	С	М	П
221	В	В	М	С	С	П
222	В	В	М	С	В	В
223	В	В	М	В	М	П
224	В	В	М	В	С	В
225	В	В	М	В	В	В
226	В	В	С	Н	М	П
227	В	В	С	Н	С	П
228	В	В	С	Н	В	В
229	В	В	С	С	М	П
230	В	В	С	С	С	В
231	В	В	С	С	В	В

232	В	В	С	В	М	В
233	В	В	С	В	С	В
234	В	В	С	В	В	К
235	В	В	В	Н	М	П
236	В	В	В	Н	С	В
237	В	В	В	Н	В	В
238	В	В	В	С	М	В
239	В	В	В	С	С	В
240	В	В	В	С	В	К
241	В	В	В	В	М	В
242	В	В	В	В	С	К
243	В	В	В	В	В	К

Таблиця 5

Множина правил ER_5 для виявлення збоїв внаслідок мікрокліматичних умов в серверній

р	P_T	P_H	P_D	Результат
1	ДМ	ДН	ДМ	П
2	ДМ	ДН	М	П
3	ДМ	ДН	С	В
4	ДМ	ДН	В	В
5	ДМ	ДН	ДВ	К
6	ДМ	Н	ДМ	П
7	ДМ	Н	М	П
8	ДМ	Н	С	П
9	ДМ	Н	В	В
10	ДМ	Н	ДВ	В
11	ДМ	С	ДМ	С
12	ДМ	С	М	С
13	ДМ	С	С	С
14	ДМ	С	В	П
15	ДМ	С	ДВ	П
16	ДМ	В	ДМ	П
17	ДМ	В	М	П
18	ДМ	В	С	П
19	ДМ	В	В	В
20	ДМ	В	ДВ	В
21	ДМ	ДВ	ДМ	П
22	ДМ	ДВ	М	П
23	ДМ	ДВ	С	В
24	ДМ	ДВ	В	В
25	ДМ	ДВ	ДВ	К
26	М	ДН	ДМ	П
27	М	ДН	М	П
28	М	ДН	С	П
29	М	ДН	В	В
30	М	ДН	ДВ	В
31	М	Н	ДМ	С
32	М	Н	М	С

33	М	Н	С	П
34	М	Н	В	П
35	М	Н	ДВ	В
36	М	С	ДМ	Н
37	М	С	М	Н
38	М	С	С	С
39	М	С	В	С
40	М	С	ДВ	П
41	М	В	ДМ	С
42	М	В	М	С
43	М	В	С	П
44	М	В	В	П
45	М	В	ДВ	В
46	М	ДВ	ДМ	П
47	М	ДВ	М	П
48	М	ДВ	С	П
49	М	ДВ	В	В
50	М	ДВ	ДВ	В
51	С	ДН	ДМ	С
52	С	ДН	М	С
53	С	ДН	С	П
54	С	ДН	В	П
55	С	ДН	ДВ	В
56	С	Н	ДМ	С
57	С	Н	М	С
58	С	Н	С	С
59	С	Н	В	П
60	С	Н	ДВ	П
61	С	С	ДМ	Н
62	С	С	М	Н
63	С	С	С	Н
64	С	С	В	С
65	С	С	ДВ	С

66	С	В	ДМ	С
67	С	В	М	С
68	С	В	С	С
69	С	В	В	П
70	С	В	ДВ	П
71	С	ДВ	ДМ	С
72	С	ДВ	М	С
73	С	ДВ	С	П
74	С	ДВ	В	П
75	С	ДВ	ДВ	В
76	В	ДН	ДМ	П
77	В	ДН	М	П
78	В	ДН	С	В
79	В	ДН	В	В
80	В	ДН	ДВ	К
81	В	Н	ДМ	С
82	В	Н	М	С
83	В	Н	С	П
84	В	Н	В	П
85	В	Н	ДВ	В
86	В	С	ДМ	С
87	В	С	М	С
88	В	С	С	С
89	В	С	В	П
90	В	С	ДВ	П
91	В	В	ДМ	П
92	В	В	М	П
93	В	В	С	П
94	В	В	В	В
95	В	В	ДВ	В
96	В	ДВ	ДМ	П

97	В	ДВ	М	П
98	В	ДВ	С	В
99	В	ДВ	В	В
100	В	ДВ	ДВ	К
101	ДВ	ДН	ДМ	В
102	ДВ	ДН	М	В
103	ДВ	ДН	С	В
104	ДВ	ДН	В	К
105	ДВ	ДН	ДВ	К
106	ДВ	Н	ДМ	П
107	ДВ	Н	М	П
108	ДВ	Н	С	В
109	ДВ	Н	В	В
110	ДВ	Н	ДВ	К
111	ДВ	С	ДМ	С
112	ДВ	С	М	С
113	ДВ	С	С	П
114	ДВ	С	В	П
115	ДВ	С	ДВ	В
116	ДВ	В	ДМ	П
117	ДВ	В	М	П
118	ДВ	В	С	В
119	ДВ	В	В	В
120	ДВ	В	ДВ	К
121	ДВ	ДВ	ДМ	В
122	ДВ	ДВ	М	В
123	ДВ	ДВ	С	В
124	ДВ	ДВ	В	К
125	ДВ	ДВ	ДВ	К

В таблицях використані такі позначення:

Велечини параметрів: ДМ – дуже малий, ДН – дуже низький, М – малий, Н – низький, С – середній, В – високий (великий), ДВ – дуже великий (високий)

Результуючий рівень можливості реалізації ІПКС: Н – низька, С – середня, П – підвищена, В – висока, К – критична.