Анна Корченко

МЕТОДИ ІДЕНТИФІКАЦІЇ АНОМАЛЬНИХ СТАНІВ ДЛЯ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Монографія

Київ 2019

УДК 004.056 (02)
К 703

Рецензенти:

Лахно В.А. – д.т.н., проф., завідувач кафедри комп'ютерних систем і мереж Національного університету біоресурсів і природокористування України.
Терейковський І.А. – д.т.н., проф., професор кафедри системного програмування і спеціалізованих комп'ютерних систем НТУУ «КПІ ім. Ігоря Сікорського».

Рекомендовано до друку Вченою радою Національного авіаційного університету (протокол № 2 від 20.02.2019 р.)

К 703 Анна Корченко, *Методи ідентифікації аномальних станів для систем виявлення вторгнень. Монографія*, Київ, ЦП «Компринт», 2019 – 361 с.
ISBN 978-966-929-874-4

Монографія присвячена теоретико-методологічним і практичним аспектам розробки методів ідентифікації аномальних станів та методології побудови систем виявлення вторгнень. У роботі проведено аналіз засобів виявлення зловживань та аномалій. Значну увагу приділено формалізації процесу створення m_i-вимірних параметричних, атакуючих, еталонних, поточних та детекційних середовищ. Це є підґрунтям для створення засобів, які дозволять автоматизувати процес детектування в слабоформалізованому нечітко визначеному середовищі аномальний стан, що породжується кібератаками, у заданий проміжок часу шляхом контролю поточного стану множини визначених параметрів. Такі засоби можуть використовуватися автономно або, як розширювач функціональних можливостей сучасних систем виявлення вторгнень.

Книга призначена для науковців, інженерів, аспірантів і студентів вищих навчальних закладів відповідного профілю.

УДК 004.056 (02)

ISBN 978-966-929-874-4

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ІТ	–	інформаційні технології
ІС	–	інформаційна система
НАС	–	неавторизована сторона
РІС	–	ресурси інформаційних систем
ПЗ	–	програмне забезпечення
СВВ	–	система виявлення вторгнень
ОС	–	операційна система
КМАС	–	кортежна модель атакуючих середовищ
ІД	–	ідентифікатор
SNF	–	сніффінг (Sniffing)
DS	–	відмова в обслуговуванні (Denial of service)
SP	–	спуфінг (Spoofing)
ESP	–	email-спуфінг (Email-spoofing)
SN	–	сканування портів (Scanning of ports)
КОП	–	кількість одночасних підключень до сервера
КПОА	–	кількість пакетів з однаковою адресою відправника та одержувача
МФЕС	–	метод формування еталонного середовища
НЧ	–	нечітке число
ФН	–	функція належності
МФП	–	метод фазифікації параметрів на еталонних підсередовищах
МАН	–	метод α-рівневої номіналізації нечітких чисел
МВІТ	–	метод визначення ідентифікуючих термів
МДП	–	метод дефазифікації параметрів детекційного середовища
ХО	–	характерна ознака
МПФН	–	метод порівняння функцій належності
ВХ	–	відстань Хеммінга
МФДС	–	метод формування базових детекційних середовищ
МПСВ	–	методологія побудови систем виявлення аномалій породжених кібератаками
СВК	–	система виявлення кібератак
БДК	–	база даних кібератак
БДП	–	база даних правил
БДЕ	–	база даних еталонів

МФПЗ – модуль формування поточних значень
МАРН – модуль α-рівневої номіналізації
МДІТ – модуль дефазифікації та формування ідентифікуючих термів
МРА – модуль формування рівня аномальності
МВ – модуль візуалізації

ВСТУП

Розвиток інформаційних технологій (ІТ) відбувається настільки швидко, що класичні механізми захисту, не здатні залишатися ефективними та забезпечувати відповідну безпеку ресурсам інформаційних систем (РІС), а шкідливе програмне забезпечення (ПЗ) та інші кіберзагрози стають все більш поширеними. Також, в останні роки, проходить значне збільшення обсягів інформації, яка накопичується, зберігається та обробляється за допомогою різних інформаційних систем (ІС). При цьому, концентрування в єдиних базах даних інформації різного призначення, а також швидке розширення кола користувачів, що мають безпосередній доступ до РІС, утворюють проблему забезпечення їх захисту від різного роду вторгнень.

Зростання складності апаратно-програмних засобів та існуючі недоліки сучасних ІТ призводять до удосконалення кібератак. Необхідно зазначити, що несанкціоновані дії щодо РІС здійснюють впив і на середовище оточення, породжуючи в ньому, як наслідок, певні аномалії. Таке середовище зазвичай гетерогенне, нечітко визначене, а для вирішення задач виявлення кібератак, які утворили аномалії в цьому середовищі, необхідні відповідні засоби. Такі засоби повинні надавати можливість виявлення вторгнень за множиною різних характерних ознак, включаючи їх динамічну складову, яка контролюється в реальному режимі часу.

У зв'язку з цим, необхідні спеціальні засоби, що дозволяють оперативно виявляти та попереджувати порушення безпеки. Для цього застосовуються системи виявлення вторгнень (СВВ), які є невід'ємною частиною будь-якої сучасної системи безпеки, а світова тенденція свідчить про те, що виявлення вторгнень, стане обов'язковою функцією операційної системи та вже застосовується в різному ПЗ.

В основному, СВВ достатньо коштовні, мають закритий код та потребують постійної кваліфікованої підтримки і налаштування під визначені вимоги організації та сервіси. Таку потребу можуть задовільнити тільки спеціалісти відповідної предметної галузі. Особливо необхідні СВВ, які орієнтовані на виявлення аномальних станів. Вони, як правило, формують (містять) профіль нормальної (ненормальної) активності в ІС та детектують відхилення від нього. Ці СВВ базуються на гіпотезі, що аномальний стан проявляється як відхи-

лення від нормального, але такий стан не завжди породжується атакою чи її частиною. Висока інерційність щодо адаптації сучасних аномальних СВВ до нових загроз, в першу чергу, пов'язана з довготривалістю процесу створення відповідного статистичного профіля нормального стану ІС, а при її реконфігурації, модифікації та інших змінах набрана статистика стає неактуальною та неповною. Необхідно також зазначити, що повні статистичні дані щодо ІС сформуються по завершенню її існування, але надалі вони не будуть актуальними. Більш ефективні в цьому відношенні є експертні підходи, що засновані на використанні досвіду спеціалістів відповідної предметної області. А побудова відповідних методів та створення засобів (СВВ, виявлення кібератак та аномалій тощо), орієнтованих на обробку слабкоструктурованих даних з метою встановлення фактів несанкціонованого доступу до РІС (наприклад, через комп'ютерні мережі) є основою для успішної протидії кібератакам.

Функціональність сучасних систем виявлення та блокування вторгнень в значній мірі залежить від їх можливостей реалізовувати такі функції в реальному режимі часу відносно нових кібератак. Засоби систем протидії достатньо розвинуті, але для їх ефективної роботи необхідна відповідна інформація, за допомогою якої можливо виявляти атакуючі дії. Формування таких даних, як правило, здійснюється постфактум і потребує певного часу. Таким чином, для процесу виявлення та блокування нових кібератак характерне протиріччя між готовністю засобів протидії до негайного реагування на вторгнення та неготовністю засобів виявлення до відповідного інформування функціоналу протидії. Для вирішення такої проблеми необхідно розробити спеціальні засоби, що дозволяють розширити функціональні можливості сучасних СВВ за рахунок апріорного формування інформації щодо аномальних станів ІС, породжених певними типами кібератак. Для цього, найбільш ефективним підходом є використання досвіду експертів, який, як правило, відображається у вигляді його суджень відносно рівня аномальності параметрів, що породжується впливами нових типів загроз.

Розширення функціональних можливостей таких систем за рахунок впровадження функцій виявлення раніше невідомих кібератак (в тому числі й 0-day атак), що характеризуються невстановленими або нечітко визначеними критеріями, дозволить їм фактично залишатися функціональними у відповідному гетерогенному середовищі.

РОЗДІЛ 1. АНАЛІЗ СУЧАСНИХ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

1.1. Базові характеристики систем виявлення вторгнень

Інтенсивний розвиток ІС та технологій всебічно впливає на всі сфери діяльності суспільства. Переважна кількість сучасних державних та приватних підприємств використовує ІС для управління виробничими процесами, підтримки прийняття рішень, пошуку необхідних даних тощо. Це забезпечує їм низку переваг, пов'язаних з: підвищенням продуктивності праці і мобільності працівників; високою оперативністю доступу до інформації та послуг; можливостями віддаленого управління ресурсами і процесами тощо.

Разом з цим збільшується кількість уразливостей та загроз ІС і тому для забезпечення їх нормального функціонування та попередження вторгнень необхідні спеціалізовані засоби безпеки.

Слід зазначити, що одним із актуальних напрямів, який активно розвивається у сфері інформаційної безпеки є виявлення кібератак і запобігання вторгнень в ІС з боку неавторизованої сторони (НАС). Також слід наголосити, що атаки на РІС з кожним роком стають все досконалішими, глобальнішими та частішими.

Наприклад, низка нещодавно реалізованих кібератак, які завдали шкоди багатьом державним установам та приватним підприємствам і організаціям (Ощадбанк, Укргазбанк, Укрпошта, Укрзалізниця, Укренерго, ДТЕК, Київенерго, Київводоканал, Міжнародні аеропорти «Бориспіль» і «Київ», Rozetka, Київстар, Vodafone Україна, Lifecell, Київський метрополітен, телеканали СТБ і ICTV, Нова пошта, мережа магазинів «Епіцентр», автозаправки WOG і ТНК тощо [1-3]) показали неготовність та недосконалість їх власних систем безпеки до раніше невідомих вторгнень.

Масовані кібератаки ініціюють створення спеціальних технічних рішень, засобів та систем протидії. Для виявлення мережевих вторгнень використовуються сучасні методи [4-12], моделі [12, 13], засоби [12, 14-16], ПЗ [12, 17-27] і комплексні технічні рішення для систем виявлення та запобігання вторгнень [8, 12, 15, 22, 27-29], які можуть залишатись ефективними при появі нових або модифікованих видів кіберзагроз. Але на практиці при появі нових загроз та аномалій, породжених атакуючими діями з невстановленими або

нечітко визначеними властивостями, зазначені засоби не завжди залишаються ефективними і вимагають тривалих часових ресурсів для їх відповідної адаптації. Тому, СВВ повинні постійно досліджуватись і удосконалюватись для забезпечення неперервності в їх ефективному функціонуванні.

Серед таких систем є спеціалізовані програмні засоби, які направлені на виявлення підозрілої активності або втручання в ІС і прийняття адекватних заходів щодо запобігання кібератакам. Ці системи та засоби, як правило, достатньо дорогі, мають закритий код та вимагають періодичної підтримки розробників (висококваліфікованих фахівців) щодо їх удосконалення і відповідного налаштування до умов конкретних організацій.

Виходячи з цього, проведення аналізу технічних рішень, спеціальних засобів та ПЗ виявлення кібератак, зловживань та аномалій в ІС для їх використання при виборі і розробці СВВ, а також визначення найбільш ефективних відповідних механізмів захисту РІС є актуальним завданням.

У [10, 20, 24, 26, 30] описано ПЗ AAFID, ASAX, NetSTAT, Prelude, Shadow, Snort та SnortNet, яке використовується для виявлення порушень за такими характеристиками, як «Клас кібератаки», «Адаптивність», «Відкритість», «Методи виявлення», «Управління системою», «Масштабованість», «Рівень спостереження», «Реакція на кібератаку», «Захищеність» та «Підтримка операційною системою (ОС)». Але для більш об'єктивної оцінки сучасного ПЗ важливо розглянути значно ширший спектр відповідних реалізацій, наприклад, Cisco IPS, OSSEC, Kaspersky Anti Targeted Attack Platform, InfoWatch ASAP, Tipping Poing NGIPS, Arbor Networks Spectrum тощо.

Крім того, в [7, 8, 12, 15, 17, 21-23, 25, 26] наведений загальний опис окремих функції та принципи роботи ПЗ EMERALD, SIEM, OSSIM, CMDS, NetStat, Bro, Shadow, Network Flight Recorder, Tripwire, Snort, Suricata, Prelude, NetProwler, NetRanger, Centrax та RealSecure, але не проведений аналіз відносно базових характеристик «Методи виявлення», «Реакція на кібератаку», «Захищеність» тощо.

Також, в [27] розкриваються основні принципи функціонування найпопулярніших СВВ 2018 року – SolarWinds Log and Event Manager, Snort, OSSEC, Suricata, Bro, Sagan, Security Onion, AIDE,

OpenWIPS-NG, Samhain і Fail2Ban та визначені ОС, якими вони підтримуються, але не проведений аналіз відносно базових характеристик «Клас кібератак», «Адаптивність», «Відкритість», «Захищеність» тощо.

У [18] порівнюються функціональності RealSecure, NetProwler, Snort та Форпост, в [24] здійснена оцінка Bro, RealSecure та Snort за функціональністю та продуктивністю, у [16] аналізуються OSSEC і Snort за можливостями моніторингу, видами сповіщень і попереджень про атаку та особливостями налаштування, а в [19] проведено аналіз СВВ з відкритим початковим кодом та порівняння конфігурації Snort 2, Snort 3 і Suricata 2 за низкою характеристик щодо кращого застосовування для захисту ІС. Але в цих роботах не проглядається узагальнювальність підходів та не проаналізовані сучасні засоби Symantec DeepSight Threat Management System, Bro, Arbor Networks Spectrum, Axoft invGUARD, DefensePro тощо, а також не визначені їх властивості відносно базових характеристик «Реакція на кібератаку», «Клас кібератак», «Адаптивність», «Методи виявлення» тощо.

В роботах [6, 7, 15, 31] описана низка методів, які використовуються в ПЗ для виявлення атак і аномалій, але не проведена оцінка відносно характеристик «Масштабованість», «Рівень спостереження», «Реакція на кібератаку» та «Відкритість».

В [16] порівнюються OSSEC і Snort за принципами налаштування, а в [32] розкривається склад СВВ та їх основні завдання, але не проведений аналіз відповідного найпоширенішого ПЗ за множиною характеристик «Захищеність», «Методи виявлення», «Масштабованість» тощо.

Також, в [33] розглянуто системи виявлення та запобігання вторгнень, функціонування яких базується на аномаліях мережевого трафіку (аномальні системи виявлення та попередження вторгнень), в [12, 15] розкриваються методи та моделі, які використовуються для виявлення вторгнень, в [4-6, 8, 9, 11, 29, 34] порівнюються методи виявлення атак та аномалій, а в [29, 35-37] акцентується увага на застосуванні нечіткої логіки для ефективного виявлення аномалій, в [38] досліджуються питання побудови інтелектуалізованих систем ідентифікації загроз, в [39] моделюються процеси несанкціонованого доступу до інформаційних ресурсів на основі методів теорій диференціальних ігор та диференціальних перетворень, в [40, 41]

розробляються нейромережеві засоби безпеки інтернет-орієнтованих ІС. Але в жодному з джерел не здійснено дослідження конкретного ПЗ, оцінки його властивостей та опису базових характеристик.

В [11, 12, 15, 17, 22, 29, 34] запропонована класифікація СВВ та систем запобігання вторгнень, зазначені їх переваги та недоліки і деякі особливості побудови, а в [7, 26] здійснена класифікація щодо виявлення мережевих вторгнень (аномалій і зловживань), але не розглядається існуюче ПЗ відносно визначених базових характеристик.

В роботах [6, 8, 10, 11, 13, 14, 18-20, 24, 26, 28, 29, 42, 43] розглянуті основні можливості, принципи побудови, механізми функціонування та порівняльний аналіз СВВ, але відсутнє конкретне дослідження ПЗ щодо характеристик «Клас кібератак», «Адаптивність», «Методи виявлення» тощо.

У [15] проведений аналіз щодо проектування систем виявлення атак, показані основні принципи створення засобів протидії кібератакам, але відсутній аналіз відносно конкретного ПЗ щодо характеристик «Масштабованість», «Рівень спостереження», «Реакція на кібератаку» тощо.

Аналіз джерел [4-43] показав, що для сучасних ІС та мереж гостро стоїть питання оперативного виявлення зловживань та аномалій. В переважній більшості зазначених робіт наведений лише частковий аналіз СВВ та їх класифікація, представлений загальний опис відповідного забезпечення, який не відображає їх широкого спектру та не містить необхідної множини характеристик для інтегрованої оцінки таких систем.

Виходячи з цього, є потреба в проведенні узагальнювального аналізу програмних засобів СВВ за визначеною базовою множиною характеристик. Це надасть певні можливості щодо вибору таких засобів та розробки для них найбільш ефективних механізмів безпеки при впливах кібератак.

Як правило, методи виявлення атак розділяють на методи виявлення зловживань і аномалій [7, 30, 44, 45]. Зловживання засновані на використанні існуючих недоліків ІС. Основною відмінністю між аномалією і зловживанням є те, що аномалія – це процес, який виникає перед можливим вторгненням в систему або вказує на наявність

вже існуючої атаки. Фактично, аномалія – це відхилення від нормального стану системи, незвичайна активність в ній, що може свідчити про певні атакуючі дії. Слід зазначити, що аномалія може виникнути і за інших причин, наприклад, внаслідок неправильної роботи системи.

Саме тому за допомогою ефективного аналізу аномалій, що виникають у системі, можна попередити кібератаки певних типів і вчасно вжити необхідних заходів щодо їх блокування та захисту ІС.

Варто сказати, що широке використання сучасних засобів захисту від кібератак не гарантує безпеки на належному рівні, оскільки останнім часом:

- зростають атаки, спрямовані на корпоративні системи, публічні, конфіденційні та державні інформаційні ресурси;
- кібератаки, постійно модифікуються, удосконалюються і стають більш регулярними;
- виявлення кібератак класичними засобами захисту не завжди є ефективним;
- частішають випадки здійснення складних атак [1-3] на ІС [28, 46, 47].

Це також пов’язане з інтенсивним розвитком програмно-апаратних засобів і глобалізації інформаційних мереж та їх повсякденного використання у всіх сферах діяльності суспільства.

Враховуючи результати відомих досліджень з подальшим їх узагальнюванням і відображенням на розширений спектр засобів виявлення зловживань та аномалій проведемо аналіз сучасних СВВ відносно базових характеристик «Клас кібератак», «Адаптивність», «Відкритість», «Методи виявлення», «Управління системою», «Масштабованість», «Рівень спостереження», «Реакція на кібератаку», «Захищеність» [30] та «Підтримка ОС» (див. таблицю 1.1-1.3). Перед початком аналізу розкриємо кожну із зазначених базових характеристик.

«Клас кібератак» – визначає здатність системи виявляти аномалії та зловживання на різних рівнях ІС. Більшість сучасних засобів мають здатність виявляти обидва класи атак (аномалії та зловживання) [30].

«Адаптивність» – дозволяє системі ефективно адаптуватись до нових атак (відсутніх у базі даних сигнатур), наприклад, 0-day та виявляти кібератаки з незначними модифікаціями [30].

«Відкритість» – відображає можливості системи бути відкритою до взаємодії з іншими програмними модулями і функціями та адаптивною до іншого ПЗ [30]. Ця характеристика відіграє важливу роль для корпоративних ІС, оскільки для забезпечення повного захисту від нових атак іноді необхідно використовувати декілька програмних засобів або додати конкретні компоненти які призначені тільки для визначеної мережі.

«Методи виявлення» – множини методів, що використовуються для виявлення атак і складають математичну основу системи. Найбільш поширеними є методи статистичного і кластерного аналізу, контролю зміни подій, графів атак, сигнатурні, динамічні, машинного навчання, поведінкові, евристичні, експертні, нечітких множин тощо [7, 30, 31, 45, 48].

«Управління системою» – визначає схему управління і його рівень. Управління може здійснюватися централізовано із одного хоста або розподілено із окремих хостів, пов'язаних однією системою. Найбільш оптимальною є організація управління за централізованою схемою з певною множиною центрів, кожний з яких може бути задіяний для управління всією структурою [30]. Централізовані системи реалізують управління всіма засобами (модулями) виявлення аномалій та зловживань з однієї станції [46], а розподілені реалізують управління окремо, де кожний модуль відповідає за свою функцію [49].

«Масштабованість» – можливість розширення системи, її адаптивність до різних мережевих структур та долучення нових аналізованих ресурсів мережі [30].

«Рівень спостереження» – визначає, на якому рівні системи отримуються дані для виявлення кібератак. Застосовуються два рівні отримання даних – мережевий та системний. Сучасні системи, як правило, підтримують обидва рівні спостереження, оскільки саме їх взаємодія дозволяє краще забезпечити захист. Від цієї характеристики залежить швидкість формування первинних даних, їх правильна обробка та отримання точної інформації про поточний стан РІС. Аналіз трафіку мережі здійснюється за допомогою спеціальних сенсорів (мережевих і системних), що застосовуються у системах

виявлення атак та аномалій. Мережеві сенсори аналізують дані на мережевому рівні (зазвичай на основі сигнатурного аналізу) і генерують повідомлення про виявлення кібератак та відправляють їх до модулів управління. Системні сенсори аналізують журнали реєстрації ОС, додатки та програмні застосунки на можливі аномалії чи загрози і генерують відповідні повідомлення, які надходять до модулів управління [30].

«Реакція на кібератаку» – визначає наявність у системі компонентів чи модулів протидії. Тобто, після реєстрації атаки ініціюються дії для редукування подальшого негативного впливу [30].

«Захищеність» – характеризує наявність власних компонентів системи, які відповідають за її захист від кібератак та зовнішнього негативного інформаційного впливу, а також за стійкість до виходу з ладу та зменшення кількості уразливостей розробки в цілому [30].

«Підтримка ОС» – характеризує тип ОС (наприклад, Unix, Linux, Windows, MacOS тощо), що підтримує відповідне ПЗ системи.

Більшість проаналізованих джерел містить лише частковий аналіз СВВ та загальний опис відповідного ПЗ, який не відображає їх широкого спектру та не містить необхідної множини характеристик для інтегрованої оцінки таких систем. А також визначено набір базових характеристик з використанням яких є можливість для розробників і користувачів обрати відповідні сучасні програмні і програмно-атаратні засоби та СВВ для ідентифікації кібератак.

1.2. Відкриті системи виявлення вторгнень

З урахуванням запропонованих характеристик розкриємо властивості відкритих СВВ.

AAFID

Система AAFID (Autonomous Agents for Intrusion Detection, розробка Purdue University, West Lafayette, Індіана, США) призначена для розподіленого контролю та виявлення вторгнень. Використовує невеликі автономні програми (агенти) для виконання функцій моніторингу в хостах мережі. Архітектура AAFID засновується на незалежних одночасно працюючих об'єктах (агентах), які направлені на

виявлення вторгнень. Вони контролюють визначену множину характеристик системи та повідомляють про нестандартну поведінку або конкретні події. Інформація, що отримана агентами, інтегрується на рівні головного комп'ютера, де здійснюється співвідношення подій (отриманих від різних агентів), які можуть бути викликані однією і тією ж атакою. Крім того, звіти, що надаються з кожного комп'ютера агрегуються на більш високому рівні (рівень мережі), що дозволяє системі виявляти кібератаки з різних джерел (рис. 1.1-1.2) [50].

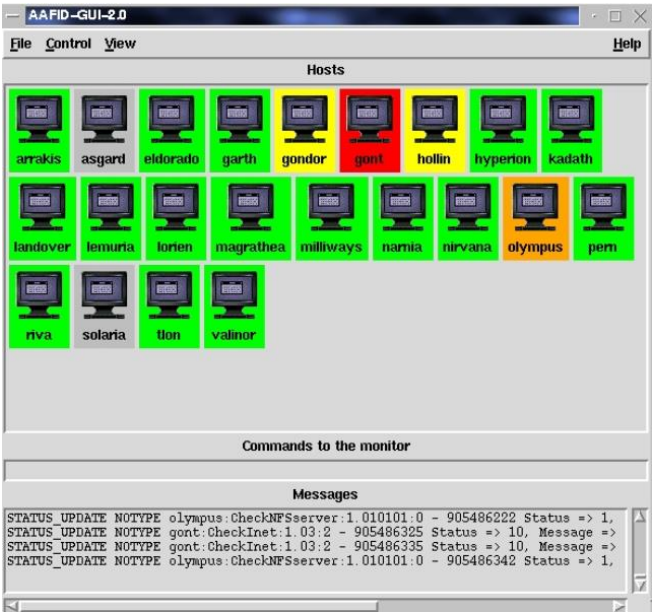

Рис. 1.1. Головне вікно прототипу ПЗ AAFID

Даний програмний засіб здійснює обробку тільки журналів реєстрації програмних застосунків та ОС, в якій він функціонує. Всі агенти працюють за сигнатурним принципом, вони виявляють відомі (заздалегідь описані) аномалії, зловживання та події на вузлах і в мережі. Система знаходиться на стадії прототипу. Множина агентів, що входить до AAFID у явному вигляді використовує характеристики атак, сформовані експертами (розробниками агентів). При

цьому не використовується ніякої формальної мови опису кібератак. Агенти є програмними модулями, написаними на алгоритмічній мові загального призначення RUSSEL, в яких жорстко визначені ознаки тих атак, на виявлення яких вони орієнтовані. Така організація бази описів відомих атак (NADF) не є гнучкою щодо розширення і відповідно не є адаптивною до нових кібератак [45].

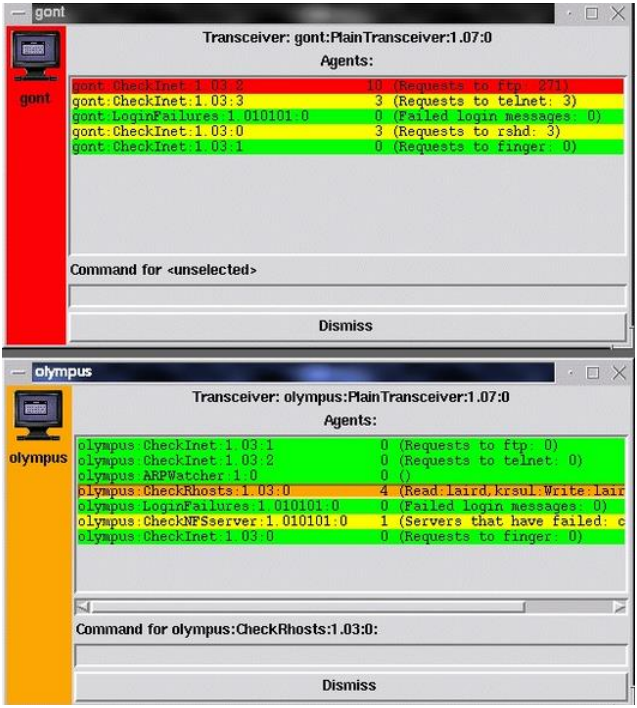

Рис. 1.2. Вікно агента прототипу ПЗ AAFID

Для збирання інформації з кожного агента або хоста (набора хостів) в AAFID використовується ієрархічна структура. Таким чином виявляється будь-яка підозріла активність в мережі, хоча зазначена властивість не завжди працює ефективно, оскільки можливості системи залежать від якості і кількості наявних агентів (програм), які використовуються для виявлення тих чи інших атак [51].

Зазначений засіб використовує експертний та сигнатурний метод виявлення аномалій і зловживань в мережевому трафіку та має централізоване управління з основного монітора [30]. Завдяки тому, що система має ієрархічну структуру, то AAFID можна легко модифікувати. Система має відкритий інтерфейс для додавання нових агентів і фільтрів, що дозволяє їй просто масштабуватись і адаптуватись під потреби мережі [52, 53].

Варто зауважити, що AAFID сама по собі не є мережевою СВВ. Частина агентів реалізують функції моніторингу мережі, а інші виконують функції моніторингу хоста. У цій архітектурі вузли СВВ розташовуються відповідно до деревовидної ієрархічної структури [51]. Слід зазначити, що AAFID не містить спеціальних механізмів захисту та реакції на вторгнення і не є стійкою до можливих кібератак, які на неї спрямовані [30, 52, 53]. Вона підтримується такими ОС як Unix та Linux [51].

Snort

Snort [54] (розробка компанії Sourcefire, США) на світовому рівні є найпоширенішою безкоштовною мережевою системою виявлення та запобігання вторгнень (рис. 1.3-1.4) [8, 12, 27, 55].

Структурно Snort підтримує декілька режимів функціонування:

- аналіз пакетів;
- журналювання (протоколювання) пакетів;
- виявлення мережевих вторгнень;
- інші вбудовані можливості [56].

Архітектура системи розроблена з урахуванням ефективності та швидкості в роботі. Тому, вона абсолютно проста і складається з:

- декодера пакетів;
- ядра виявлення;
- підсистеми оповіщення та реагування [30, 56].

Декодер реалізує набір процедур для послідовної декомпозиції пакетів відповідно до рівнів мережевого стека, тобто прийнятий кадр послідовно перетворюється в пакет, сегмент і блок даних з урахуванням специфічних для даного рівня атрибутів сигнатур. Підтримуються протоколи канального рівня Ethernet, SLIP, PPP, а також ATM [30].

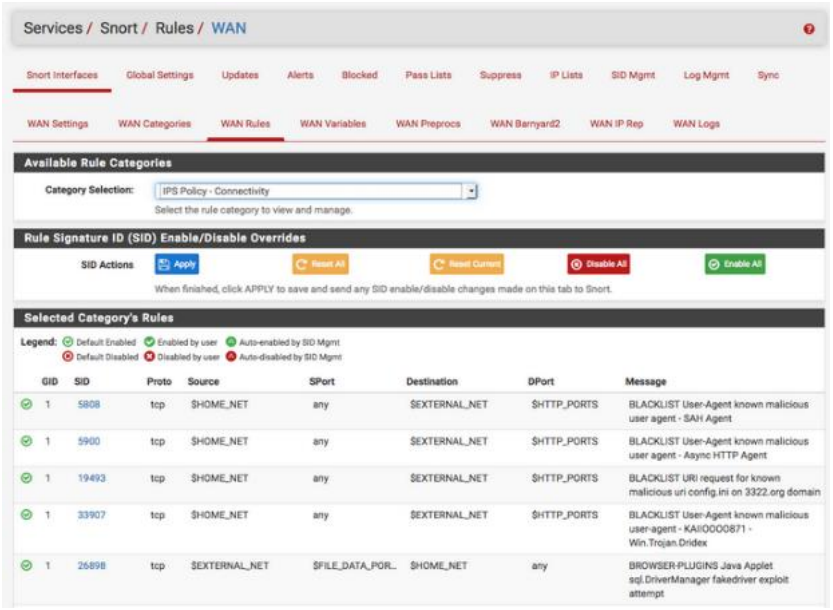

Рис. 1.3. Вікно відображення налаштування правил Snort

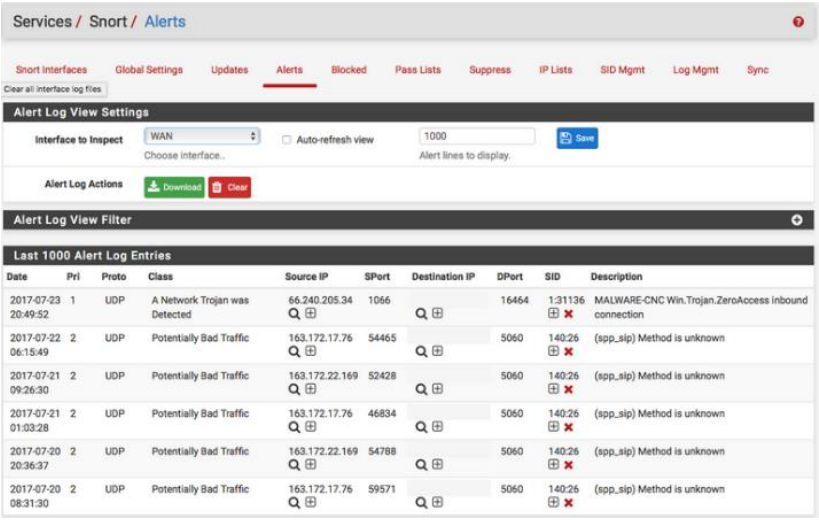

Рис. 1.4. Вікно відображення сповіщень, згенерованих Snort

Ядро інтегрує існуючі правила в ланцюги, які складають відповідні двомірні послідовності, за якими здійснюється проходження кожного пакету [30]. Підсистема оповіщення та реагування відповідає за збереження результатів аналізу трафіку у відповідних журналах Snort або передачу цієї інформації системними службами реєстрації подій ОС [30, 56].

В системі використовується проста мова опису атак, яка повністю є в документації і дозволяє адміністраторам самостійно розширювати базу сигнатур. Кожне правило складається з двох частин – умови його застосування та дії. Крім того, в останніх версіях системи з'явилася спеціальна конструкція мови сигнатур, що дозволяє класифікувати мережевий трафік за ступенем потенційної небезпеки, який визначається експертом, що формує атрибути кібератаки. Також Snort виконує функції протоколювання, аналізу і пошуку за вмістом та широко використовується для активного блокування або пасивного виявлення цілої низки зловживань і аномалій (використовуються засоби інспекції протоколів і механізми виявлення аномалій), наприклад, пов'язаних з атаками на переповнення буфера, прихованим сканування портів, атаками на веб-додатки, SMB-зондуванням, спробами визначення ОС тощо. Відповідне ПЗ в основному використовується для запобігання проникнення та блокування поточних кібератак [57].

Система функціонує на основі сигнатурного методу. Це дозволяє швидко виявляти всі задекларовані нею кібератаки. Але через неможливість повноцінного виявлення нових атак у мережі вона не є повністю адаптивною. Система Snort є програмним продуктом з відкритим вихідним кодом, що дозволяє легко змінювати її структуру. Вона здатна виконувати реєстрацію пакетів і в режимі реального часу здійснювати аналіз трафіку в IP-мережах. Також завдяки відкритій архітектурі та відкритому початковому тексту система стала швидко розвиватися (за рахунок інших розробників) і інтегруватися з різними програмними продуктами, наприклад, такими як бази даних журналів виявлення, аналізатори журналів реєстрації тощо [58].

Модуль аналізу трафіку базується на основі правил (сигнатур). До ядра виявлення можуть інтегруватися модулі сторонніх розробників (препроцесори) і проводити аналіз на одному з рівнів декомпозиції пакетів. За допомогою таких модулів можна розширити фу-

нкціональність ядра виявлення та реалізовувати різні методи виявлення. Також до складу Snort був доданий модуль статистичного аналізу, який призначений для виявлення аномалій в мережевому трафіку [8].

У системі реалізоване централізоване управління за допомогою однієї станції. Оскільки Snort є представником системи з відкритим кодом, то продукт легко масштабувати та змінювати під власні потреби. Система дозволяє ефективно використовувати існуючі та самостійно створювати нові правила для виявлення атак виключно на основі аналізу мережевого трафіку. Підсистема оповіщення та реагування включає базові методи реакції на кібератаку – розрив з'єднання з атакуючим об'єктом чи блокування його. Механізми захисту в Snort реалізуються протоколом SNMPv2, у якому застосовуються функції шифрування паролів при передачі даних [30, 56, 58]. Програмний засіб Snort працює на ОС Unix, Linux та Windows [54].

Prelude SIEM

Універсальна система Prelude SIEM (Security Information & Event Management – управління інформацією про безпеку, розробка США) (рис. 1.5-1.6) збирає, нормалізує, сортує, корелює та звітує про всі події, пов'язані з безпекою незалежно від того, що породжує ці події. Також Prelude користується підтримкою інших подібних систем (snort, samhain, ossec, auditd тощо), що дозволяє покращити її функціонування [8, 12, 59].

Зазначене ПЗ є розподіленою, гібридною системою виявлення атак, яка складається з наступних базових компонент:

- ядро;
- агент;
- модуль кореляції;
- база даних;
- підсистема обміну повідомленнями;
- основний інтерфейс;
- модуль управління [60].

Ядро системи відповідає за прийом нормалізованих подій (від агентів, модулів кореляції, сторонніх систем або підпорядкованих менеджерів), запис у базу даних та інформування через e-mail. Агент системи працює локально (на одному сервері) та віддалено і здійснює прийом логів від різних систем (через локальний файл або

syslog на UDP-порт), розбирає або нормалізує їх на основі множини правил, що складаються з регулярних виразів, а нормалізовані події направляє ядру. Модуль кореляції підключається до ядра як агент і корелює події, що надійшли до ядра на основі плагінів, реалізованих у вигляді Python-скриптів. База даних зберігає всі події, які обробляються системою. Підсистема обміну повідомленнями включає додаткові ресурси, що безпосередньо підключаються до ядра за підтримки IDMEF (Intrusion Detection Message Exchange Format – спеціальний формат обміну повідомленнями про вторгнення). Основний інтерфейс реалізований на протоколі http і призначений для відображення результатів обробки подій, їх агрегації або фільтрації, виведення статистичної інформації тощо [60].

Рис. 1.5. Головне вікно Prelude SIEM

Система включає в себе модуль управління, який отримує і обробляє повідомлення сенсорів та генерує можливу реакцію на атаку, наприклад, блокування порушника на мережевому екрані (Net/IP Filter). Агенти реагування (відповідно до згенерованої реакції) реалізують необхідні заходи протидії кібератакам. Додаткові модулі аналізу мережевих даних роблять систему стійкою до некоректних мережевих пакетів на різних рівнях стека та виходу її компонентів з

ладу. Це пов'язано з відправкою пакетів з неправильними контрольними сумами, синхронізацією сесій, випадковими відправленнями та іншими діями, що ігноруються [30].

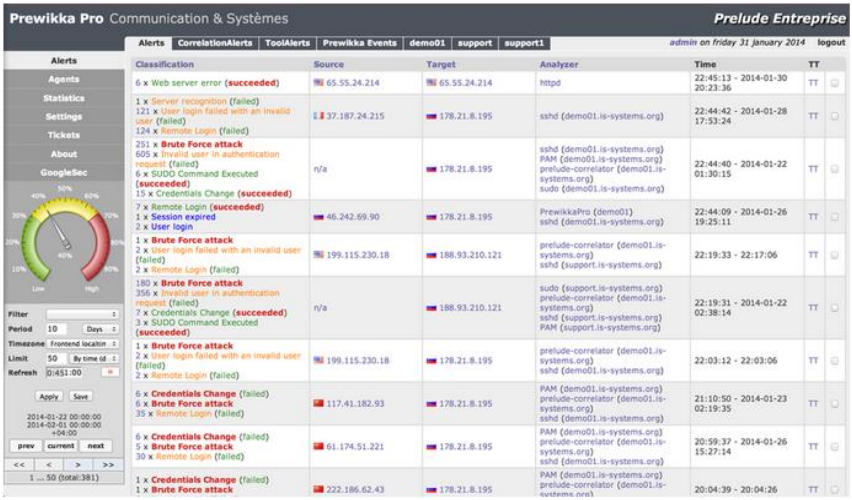

Рис. 1.6. Основний інтерфейс Prelude SIEM

Система побудована на сенсорах мережевого та вузлового рівнів. Перші аналізують вхідні данні на рівні мережі та генерують повідомлення щодо виявлення атак і відправляють їх модулям управління. Другі аналізують журнали реєстрації ОС та програмних застосунків (сенсори рівня системи), генерують повідомлення про виявлення аномалій і відправляють їх модулям управління. Мережеві сенсори орієнтовані на виявлення зловживань у системі, а вузлові на виявлення аномалій. Prelude заснована на сигнатурному підході, що дозволяє швидко виявляти всі задекларовані у системі атаки. Застосований підхід не ефективний відносно нових загроз, які не відображені у базі даних і тому система не є адаптивною до нових кібератак. Зазначена розробка є системою з відкритим початковим кодом, що дозволяє її помодульно реконфігурувати. Вона, в основному, використовує метод протоколювання подій та шаблони атак. Управління здійснюється централізовано за допомогою керуючої консолі, якій

компоненти системи самі надають ті параметри щодо їх функціонування, які можуть змінюватися. Також управління може здійснюватися через локальні конфігураційні файли на тих вузлах, де встановлені компоненти системи. Вся архітектура відкритої системи Prelude побудована за принципом використання відкритих стандартів. Підсистема обміну повідомленнями IDMEF дозволяє легко масштабувати та адаптувати зазначену розробку під різні потреби, а також інтегрувати її компоненти в системи сторонніх виробників і навпаки. Архітектура Prelude дозволяє адміністратору мережі стежити за активністю на рівні мережі та на рівні окремих вузлів. При розробці системи особливу увагу було приділено питанням безпеки та захищеності. Канали передачі даних шифруються за протоколом SSL, а також використовується спеціалізована бібліотека, яка запобігає класичним помилкам виходу за межі масивів і переповнення буферів [30]. Програмний засіб Prelude працює на ОС Linux [59].

NetSTAT

В основі системи NetSTAT (Network-based State Transition Analysis Tool, розробник кафедра комп'ютерних наук університету Каліфорнії, Санта-Барбара, США) закладена розширювана мова опису атак та їх шаблонів (STATL). Базова мова використовує найбільш абстрактні поняття і не залежить від конкретної системи та її конфігурації. Мова дозволяє самостійно добудовувати себе, є розширюваною, а додаючи специфічні для конкретної системи події, може бути легко адаптована до різних цільових середовищ. Для кожної нової події описується проникнення у вигляді послідовності дій. Такий опис групується в модуль розширення мов і його можна використовувати в описі сценаріїв кібератак для NetSTAT [23, 61].

Система має два режими функціонування. Перший заснований на тому, що для кожного стану визначається характеристика захищеності та переходи при зміні стану системи. Атаки описуються у вигляді послідовних переходів. Другий ґрунтується на сигнатурному підході, тобто описі атак у вигляді послідовності переходів та шаблонів, з якими здійснюється порівняння NetSTAT для виявлення вторгнень в мережевому середовищі орієнтована на функціонування в режимі реального часу [62].

Основною функціональною частиною системи є ядро, яке експлуатує абстрактні об'єкти та події і не залежить від конкретної системи. Тут здійснюється порівняння вхідного потоку з наявними сценаріями атак чим фактично реалізується функція виявлення. Для генерації потоку подій використовується джерело подій. Це програмний компонент системи виявлення, що здійснює перетворення інформації з системних джерел (наприклад, журналів реєстрації) у придатний для обробки формат. Також, можуть використовуватися модулі протидії, що пов'язані з ядром і реалізують реакцію на виявлену кібератаку, а при передачі даних щодо стану NetSTAT здійснюється шифрування за протоколом SSL [30, 61-63].

Особливості будови системи дають їй можливість виявляти зловживання та аномалії у мережі. Наявність двох принципів роботи дозволяє ефективно знаходити і виявляти кібератаки певного типу. Використання методу реєстрації переходів станів частково дає можливість ідентифікування нової аномалії чи атаки, але не вирішує в повній мірі проблему адаптивності системи. Дана розробка відкрита і дозволяє будувати масштабовані СВВ виходячи із задач організації. В основу функціонування NetSTAT закладено метод, що описує підзахисну систему у вигляді набору станів її компонентів з подальшим аналізом їх переходів у результаті активних зовнішніх впливів. За необхідністю для фіксації переходів створюються журнали реєстрації подій для подальшого полегшення виявлення аномалій чи зловживань у системі. Управління здійснюється розподілено, оскільки система має розгалужену і складну структуру. Архітектура NetSTAT дозволяє будувати агенти або сенсори, що призначені для виявлення атак чи зловживань на різних рівнях мережі чи системи (рис. 1.7) [30, 61-63].

Спостереження за системою виконується на системному та мережевому рівнях. Також NetSTAT може визначити точки та мережеві події, які необхідно контролювати [62].

Програмний засіб NetSTAT працює на ОС Unix, Linux та Windows.

ASAX

ASAX (Advanced Security audit trail Analyzer on uniX, спільна розробка Університету Namur та Siemens Nixdorf Software S.A., Бель-

гія) є універсальною експертною системою для виявлення вторгнень. Її принцип роботи полягає в описі початкової системи у вигляді множини станів з їх подальшим аналізом. Для ASAX розроблена проста мова RUSSEL, яка використовує спеціальні правила (рис. 1.8) для ефективної обробки великих послідовних файлів, що базуються на аналізах журналів реєстрації. RUSSEL можна розглядати як процедурну мову, включаючи конкретну, заздалегідь визначену структуру управління, яка підходить для обґрунтування послідовностей записів. Ця структура управління базується на певному механізмі, що запускає правило, до якого входить опис умови його спрацювання та наступні дії (наприклад, висновок, повідомлення або виклик іншого правила). Головне правило є основою всієї множини, яке активується першим і далі викликаються ті, що знаходяться в полі його дії. Також можливо використовувати систему для обробки даних журналів реєстрації в режимі реального часу [64, 65].

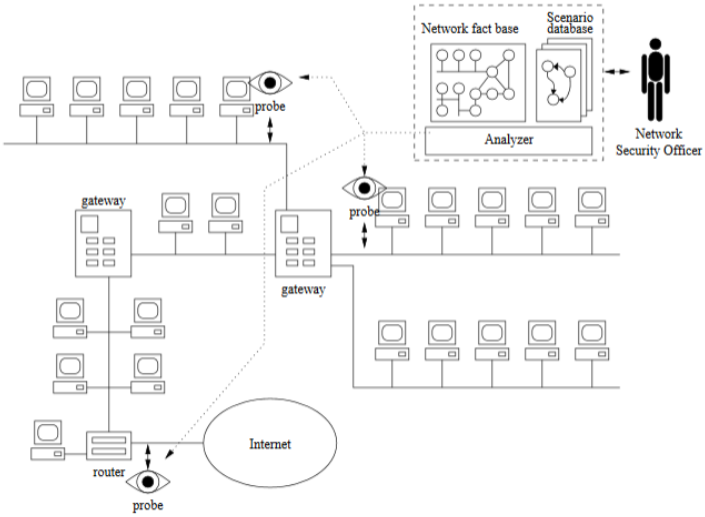

Рис. 1.7. Архітектура системи NetSTAT

ASAX орієнтована на виявлення тільки зловживань на рівні ОС, але проста реалізація експертного методу не дає можливість виявляти нові атаки на мережу та адаптовуватись до нових кібератак. В

основу ASAX закладений простий варіант реалізації експертних СВВ. Вона має відкритий інтерфейс і програмний код, що дозволяє розширяти функціональні можливості. Даний програмний засіб має централізоване управляється на вузлі його встановлення за допомогою файлів конфігурації. Простота масштабування зумовлюється простою структурою побудови ASAX. Оскільки система працює тільки з журналами реєстрації додатків і ОС, то для неї характерний системний рівень спостереження [30, 64-66].

```
rule criticalFileAccess;
begin
if
  ret_err = 0              /* success   */
  and (event = 4           /* creat(2)  */
    or event = 6           /* unlink(2) */
    or event = 10          /* chmod(2)  */
    or event = 39          /* fchmod(2) */
    or event = 42          /* rename(2) */
    or (73 <= event <= 83))/* open(2)   */
  and (isPrefix(fname, '/etc/aliases')
    or isPrefix(fname, '/etc/group')
    or isPrefix(fname, '/etc/passwd')
    or isPrefix(fname,
                '/var/spool/cron/crontabs')
    or isStartUp(fname))
  -->
  updt_fact_base(event, fname, uid, gid, mode)
fi;
trigger off for_next criticalFileAccess
end;

init_action;
begin
    trigger off for_next criticalFileAccess;
    init_fact_base('datalog.log')
end.
```

Рис. 1.8. Вікно ASAX з прикладом правила виявлення доступу до критичних файлів

ASAX не містить спеціальних механізмів захисту та реакції на кібератаки і не є стійкою до реалізації можливих загроз, які спрямовані на неї, працює на ОС Unix і Linux [67].

Bro

Система Bro (спільна розробка національної лабораторії Лоуренса та центру дослідження Інтернету ICSI в міжнародному інституті комп'ютерних наук, Каліфорнійський університет, Берклі, США) є автономним ПЗ для виявлення мережевих вторгнень у режимі реального часу шляхом пасивного контролю за мережевими посиланнями [8, 12, 23, 27].

Система (рис. 1.9-1.10) є відкритою, безкоштовною і розповсюджується за власною відкритою ліцензією та працює під управлінням декількох варіантів ОС UNIX. Bro є ключовою частиною інфраструктури безпеки центру суперкомп'ютерних застосунків NCSA. Її платформа надає широкий спектр можливостей щодо аналізу трафіку, який охоплює заголовки пакетів, регулярні вирази, фіксацію станів високорівневих з'єднань, статистичний аналіз тощо [68].

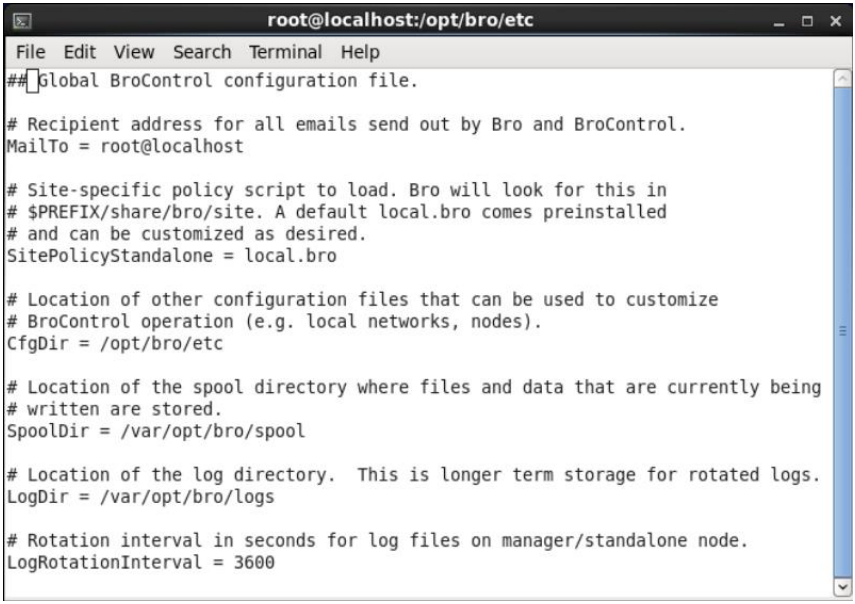

Рис. 1.9. Конфігураційний файл Bro

Основний функціонал системи направлений на:

- високошвидкісний моніторинг великого обсягу інформації;

- контроль перевантажень;
- механізм поділу;
- масштабованість;
- здатність протистояти кібератакам;
- інформування в режимі реального часу [69].

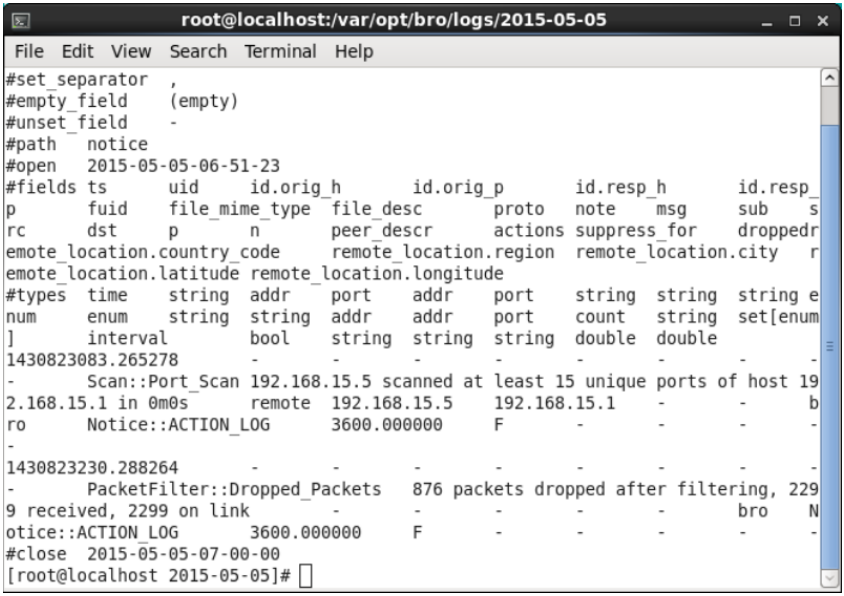

Рис. 1.10. Лог-файл з повідомленням сканування

Функція виявлення вторгнень в Bro пов'язана з етапами реєстрації та аналізу трафіку. Модуль аналізу системи має два елементи, які орієнтовані на аналіз сигнатур та виявлення аномалій [27].

Система має ієрархічну архітектуру з трьома рівнями функцій. На першому рівні використовується утиліта libpcap для вилучення з мережі пакетів з даними. На другому виконується перевірка цілісності пакетів за заголовками, а при виявленні помилок генерується відповідне повідомлення. На третьому рівні згенеровані події розміщуються в черзі, яка опрацьовується інтерпретатором сценарію політики на основі мови Bro. Зазначена множина сценаріїв є політикою

безпеки мережі, яка визначає реакцію системи на різні події. Сценарій може генерувати повідомлення, а також виконувати будь-які команди ОС і фактично реагувати на атаки. Сценарії політики можна налаштувати, але зазвичай вони працюють за стандартною схемою, яка включає підписування, виявлення аномалій та аналіз з'єднань. Виконання коду може закінчитися генерацією подальших подій, реєстрацією повідомлення в реальному режимі часу або протоколюванням. Щоб додати нову функцію до можливостей, Bro необхідно підготувати відповідний опис ідентифікації подій і обробник подій. На даний момент Bro контролює чотири прикладних сервіса – finger, ftp, portmapper і telnet [27, 69-71].

При виявленні атакуючих дій, система може повідомити оператора про підозрілу активність, записати повідомлення у відповідний журнал або виконати команди (правила) занесені до системи. Систему можна встановити на Unix, Linux або MacOS для виявлення зловживань та аномалій у мережі. Наявність модуля контроля перевантаження дає можливість обробляти великі обсяги даних без зниження пропускної здатності мережі. Якщо НАС спробує перевантажити мережу сторонніми пакетами для виведення СВВ з ладу, то Bro буде змушена пропускати пакети, серед яких можуть виявитися ті, що створені порушником для проникнення в мережу. Наявність такого модуля не вирішує проблему адаптивності системи. Розмежування процесів фільтрації даних, ідентифікації подій і політики реагування на них спрощує експлуатацію і обслуговування системи. Вона має простий механізм внесення додаткових записів про нові типи нападів і фактично заснована на сигнатурному підході виявлення атак. Дана система управляється централізовано та є зручною в управлінні завдяки певним командам взаємодії. Для виявлення нових уразливих місць, а також захисту від відомих типів загроз існує можливість швидкого додавання нових сценаріїв нападу у відповідну внутрішню бібліотеку. Bro використовують для пасивного моніторингу мережевого трафіку та пошуку підозрілої активності і аномалій в мережі. Система реалізує виявлення на прикладному рівні (використовуються ситуаційно-орієнтовані аналізатори для порівняння з шаблонами атак) та аналізує вхідний мережевий трафік (виявлення на семантичному рівні програмних застосунків). Слід зазначити, що складні сценарії нападу неодмінно включають елементи

впливу на СВВ, але в системі відсутні засоби захисту для каналів передачі даних [69, 70].

Bro підтримується ОС Unix, Linux та MacOS [72].

OSSEC

Система OSSEC (Open Source SECurity, розробка Daniel B., корпорація Atomicorp є виробником ОС Linux, яка включає OSSEC як одну з основних технологій, США) це масштабована, багатоплатформерна, вузлова СВВ на основі хоста з відкритим вхідним кодом (рис. 1.11) [12, 27, 73].

Має потужний інструмент кореляції та інтегрованого аналізу журналів, перевірки цілісності файлів, моніторингу реєстру Windows, централізованого нагляду за політикою, виявлення руткітів, оповіщення про атаки в режимі реального часу, виявлення закладок та протидії на вторгнення. Вона працює на ОС Linux, OpenBSD, FreeBSD, MacOS, Solaris, Windows та іншими [74, 75].

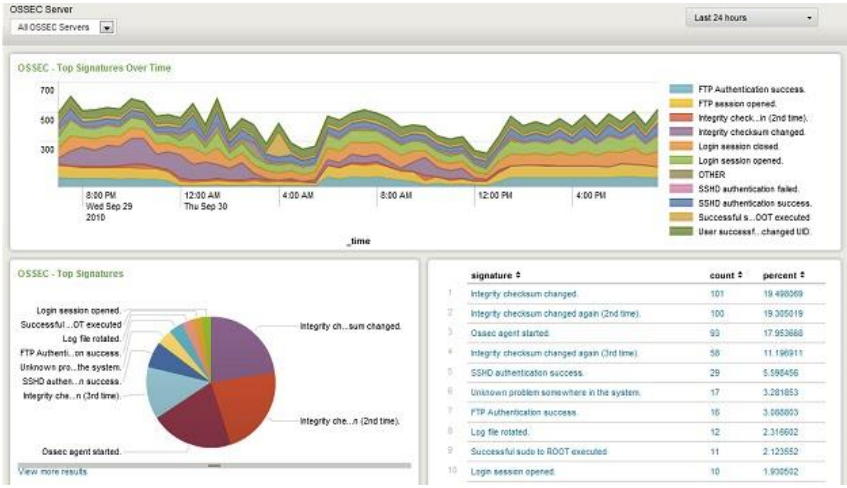

Рис. 1.11. Вікно відображення сервера OSSEC

При виникненні вторгнень завдяки відповідним журналам, що надсилаються на електронну пошту можна дізнатись про атакуючі дії та вжити необхідних заходів. Також OSSEC може експортувати попередження в будь-яку систему SIEM за допомогою системного

журналу. Це дає можливість користувачам отримувати аналітичні матеріали в реальному режимі часу та проглядати і аналізувати події в системі безпеки [74]. Система використовує агенти (сукупність невеликих програм, встановлених на систему для моніторингу), які збирають інформацію та передають її менеджеру для аналізу та кореляції (рис. 1.12) [76].

Рис. 1.12. Вікно OSSEC Agent Manager для введення IP-адреси менеджера

Частина інформації збирається в режимі реального часу, а частина з певним періодом. OSSEC може бути встановлена на Microsoft Windows платформу і виконувати функції агента [76]. Система використовується інтернет-провайдерами, університетами, урядами і великими корпоративними центрами обробки даних [74, 77].

Також OSSEC містить низку аналізаторів виявлення загроз для різних джерел даних, реалізує функції контролю цілісності файлової системи, виявлення сигнатур відомих троянських закладок (rootkits)

тощо. З урахуванням можливості контролю цілісності ресурсів у вузлах можна говорити про умовну адаптивність OSSEC. Система повністю вільна у використанні і має відкритий інтерфейс для додавання нових модулів аналізу. Її можна адаптувати до своїх потреб безпеки завдяки широким можливостям налаштування, формуючи власні правила сповіщення та написання скриптів, які вживають заходів у відповідь на порушення безпеки. OSSEC може змінювати початковий код для розширення функціональних можливостей. Система використовує сигнатурні методи виявлення кібератак і може бути встановлена в одиночній конфігурації на одному вузлі або в розподіленій на декількох вузлах (в такому випадку одна з інсталяцій стає сервером, а решта є агентами системи). При цьому управління агентами здійснюється централізовано з сервера. OSSEC на вузлах, де встановлені агенти управляється розподілено (за допомогою файлів конфігурації) або централізовано за допомогою спеціалізованої утиліти адміністрування (Manage_agents) з центрального сервера. Завдяки цьому система є добре масштабованою. OSSEC працює виключно з журналами реєстрації додатків і ОС та дозволяє використовувати довільні команди для реагування на атаку. Для цього необхідно статично задати відповідність між подією, командою і параметрами її виклику. При передачі інформації про поточний стан системи здійснюється шифрування за протоколом SSL [30, 74, 77].

Suricata

Програмний засіб Suricata (розробка компанії Open Information Security Foundation, Бостон, США) має відкритий код, є безкоштовним, швидким, надійним та перспективним засобом виявлення мережевих загроз (рис. 1.13). Він призначений для запобігання та виявлення вторгнень у режимі реального часу, моніторингу мережевої безпеки, автоматичного аналізу та обробки PCAP-файлів [8, 27, 78].

Suricata працює на рівні додатків і це дозволяє виявляти загрози, які можуть залишатися непоміченими. Контроль здійснюється на рівні протоколів TLS, ICMP, TCP, UDP, HTTP, FTP та SMB, а також є можливість виявляти спроби вторгнень, що приховуються під звичайними запитами та існує функція вилучення файлів для їх перевірки. Архітектура Suricata дозволяє оптимально розподілити обчислювальне навантаження між декількома ядрами процесора. Наприклад, якщо відеоадаптери більшість часу знаходяться в неактивному

режимі, то їх частково можна завантажити певними обчисленнями [79]. Також програмний засіб здатний виявляти уразливості в режимі реального часу, попереджувати вторгнення в систему, переглядати властивості мережевої безпеки [78] та поєднувати властивості виявлення аномалій і зловживань [80].

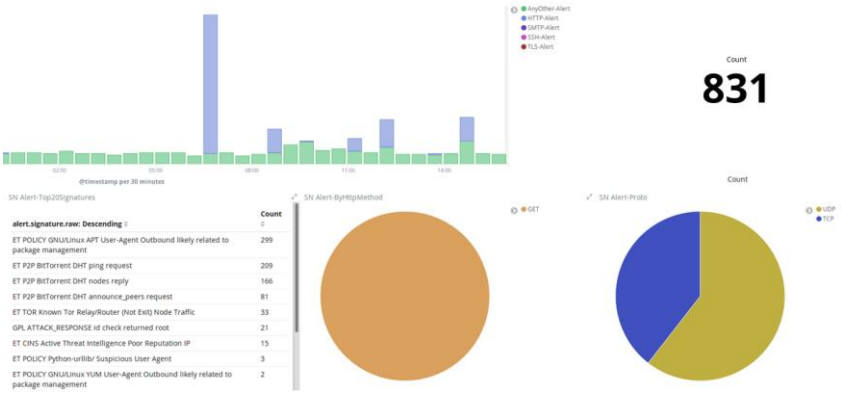

Рис. 1.13. Функціональне вікно програмного засобу Suricata

Крім того, Suricata має здатність адаптуватись до нових атак, працювати з іншим ПЗ (наприклад, Splunk, SIEM, Kibana тощо), контролювати мережевий трафік (використовуючи сигнатури та розширені правила подібні до Snort) і має потужну підтримку сценаріїв Lua для виявлення складних загроз [78].

Наявні засоби перевірки HTTP-трафіку засновуються на бібліотеці HTP. Також здійснюється контроль файлів (що передаються з використанням HTTP), розбір стисненого контенту, ідентифікація за URI, cookie, заголовками тощо. Контент в потоці можна виділяти за допомогою маски і регулярних виразів, а ідентифікація файлів можлива за іменем, типом або контрольною MD5-сумою [81]. Програмний засіб має централізоване управління [79] і швидко виявляє уразливості та атаки завдяки розподіленій роботі між ядрами процесора та потоками [80]. Спостереження за системою відбувається на системному і мережевому рівнях [27].

В Suricata реакція на кібератаку здійснюється оперативно у тому випадку, якщо порушено не меньше одного із налаштованих правил,

шляхом маркування отриманих пакетів даних, одним із трьох маркерів:

- NF_ACCESS (доступ наданий);
- NF_DROP (доступ заборонений);
- NF_REPEAT (пакети маркуються та повторно направляються на правила брандмауера, який і вирішує подальше призначення відповідного пакету) [80].

Даний програмний засіб є загальнодоступним для всіх користувачів і він не має механізмів захисту [78]. Suricata функціонує на ОС Unix, Linux, Windows та MacOS [27].

Samhain

Система Samhain (розробка компанії Samhain Services, Люнебург, Німеччина) є відкритим, безкоштовним, мультиплатформеним ПЗ для СВВ [27, 82]. Її також називають хост-системою, що забезпечує перевірку файлів, перегляд та аналіз логів, виявлення зловмисного коду (в SUID файлах), прихованих програм та процесів тощо [79].

Samhain (рис. 1.14) розроблена, як монітор для багатьох хостів з різними ОС та для локальних комп'ютерів [82]. Однією з її функцій є стелс-режим, який дозволяє маскуватися від НАС. Цей режим використовує стеганографію для приховування своїх процесів від інших. Також для запобігання вторгнень Samhain захищає свої центральні файли журналів та резервні копії конфігурацій за допомогою PGP [79].

Програмний засіб здатний працювати в реальному режимі часу, здійснювати перевірку файлів та логів системи, виявляти приховані програмні засоби, шкідливе ПЗ і аномалії [83].

Samhain завантажується як демон системи (служба) та приховано здійснює виявлення загроз. Стелс-режим дозволяє системі бути невидимою для шкідливого ПЗ і тому НАС не буде намагатися протидіяти відповідному монітору, якщо попередньо не буде знати про нього. Завдяки такому режиму вона здатна зупиняти чи перезавантажувати процеси, що дає змогу виявити можливі загрози. Зазначене ПЗ призначене більше для серверного використання і здатне здійснювати перевірку з’єднання із сервером та ідентифікацію правильності введеного паролю при вході в систему. Цілісність звітів, які

формуються Samhain забезпечується алгоритмом AES, що ускладнює їх модифікацію шкідливим ПЗ [84].

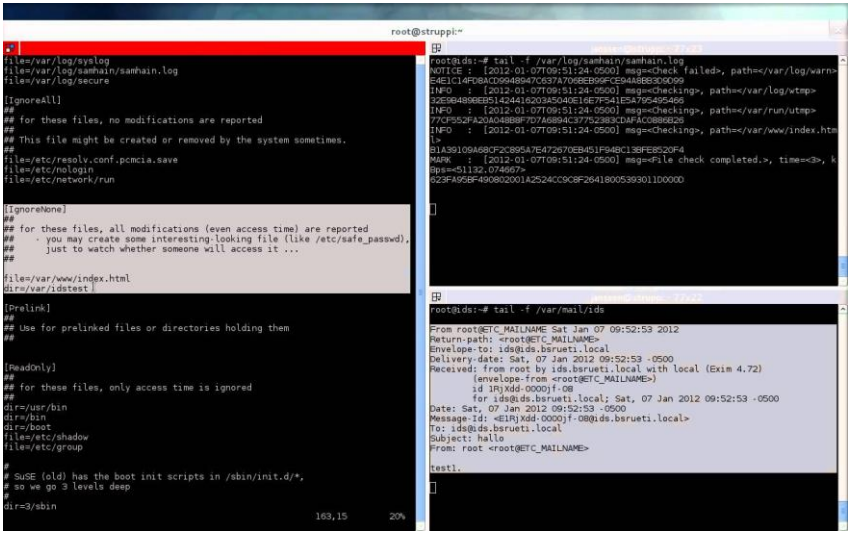

Рис. 1.14. Вікно роботи програмного застосунку Samhain

Протидія атакам в Samhain здійснюється на трьох рівнях:

- перший базується на перевірці контрольної суми (використовуються криптографічні контрольні суми файлів для виявлення модифікацій та шкідливого коду в SUID файлах, розташованих на диску);
- другий засновується на централізованому моніторингу (існує вбудована підтримка входу до центрального серверу шляхом шифрування та автентифікації підключень);
- третій забезпечує захищеність від зламування (баз даних, конфігураційних та лог-файлів, e-mail звітів що можуть підтримувати приховані операції тощо) [84].

В системі підтримується централізоване і розподілене управління [83], а також є можливість адаптування та масштабування відповідно до кількості хостів (у випадку активації даного ПЗ на серверній машині), на яких здійснюється попередження та виявлення активності НАС [84].

Спостереження за такою активністю в Samhain відбувається тільки на системному рівні [27], а реакція на кібератаку відбувається в реальному режимі часу. Крім того, Samhain підтримується ОС Unix, Linux, MacOS і Windows 2000/XP (завдяки емулятору Cygwin) [84] та використовує механізми захисту, які не розкриваються виробником [82].

Security Onion

Система Security Onion (розробка компанії Security Onion Solutions, США) є безкоштовним і відкритим ПЗ для ОС Linux, яке направлене на виявлення вторгнень, моніторинг стану безпеки підприємств, управління і перегляд системних журналів. Воно містить простий у використанні майстер налаштування розподілених давачів (рис. 1.15-1.17) та інтегрує відомі засоби безпеки Elasticsearch, Logstash, Kibana, Snort, Suricata, Bro, Wazuh, Sguil, Squert, CyberChef, NetworkMiner тощо [27, 85].

Рис. 1.15. Вікно інсталяції Security Onion

Для ефективного функціонування Security Onion потребує:

- попереджувальні дані (формуються за результатими локального спостереження за допомогою Wazuh та мережевого за допомогою Snort або Suricata);
- дані про активи (спостереження за активами підприємства здійснює Bro);
- повний вміст даних (повний перегляд пакетів даних, що циркулюють, здійснюється завдяки netshif-ng);

- локальні дані (спостереження за локальними даними здійнюється за допомогою Beats, Wazuh, syslog тощо);
- дані сесії (перегляд сесійних даних відбувається за допомогою Bro);
- дані про транзакцій (дані, що надіслані через http/ftp/dns/ssl переглядаються за участю Bro) [86].

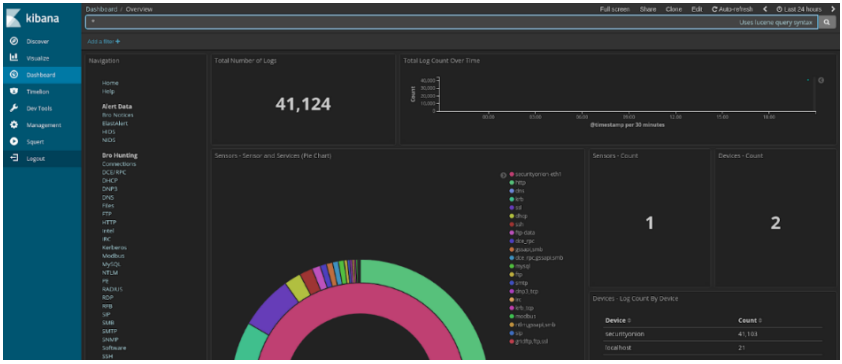

Рис. 1.16. Вікно Kibana для перегляду даних підприємства та виявлення НАС

Рис. 1.17. Фрагмент процесу аналізу та візуалізації мережевих і локальних попереджень за допомогою Squert

Після встановлення відповідного ПЗ користувач отримує комплексне рішення щодо виявлення вторгнень на мережевому і локальному рівнях. В Security Onion поєднуються різні механізми, наприклад, сигнатурний та аномальний підходи, текстовий і графічний інструментарій тощо. Оскільки функціонал системи достатньо великий, то її основним недоліком є значний часовий ресурс необхідний для налаштування ПЗ. Але для пришвидшення роботи, користувач може застосувати спрощений функціонал, для якого використовуються не всі програмні засоби [79].

Залежно від попередньо встановленого набору інструментів для виявлення вторгнень, вразливостей та інших дій НАС зазначений засіб працює в активному і пасивному режимах. Завдяки використанню в ПЗ різних детекційних методів та засобів (наприклад, Snort, Suricata, Snorby, Bro тощо), які доповнюють один одного, Security Onion містить систему оповіщення про безпеку та виявлення аномалій і шкідливих програм [87].

Відповідно до засобів аналізу (Kibana, CapME, CyberChef, Squert, ELSA, Sguil), мережевого (Snort, Suricata, Bro, Full Packet Capture) та локального перегляду (Beats, Wazup, Sysmon, Autoruns, Syslog) ПЗ має змогу реагувати на нові загрози (наприклад, шляхом блокування підозрілої IP адреси, з якої надходить велика кількість незнайомого системі трафіка) та заносити їх в особисту базу даних [88].

Відповідно до наявних програмних засобів, дане ПЗ здатне зчитувати різні формати даних та інтегруватися в різні системи [88] (наприклад, CapME може переглядати дані аналізу ПЗ Squert та логів і часових відміток ПЗ Kibana [89]; Squert здатне переглядати HTTP логи, що сформовані ПЗ Bro [90]; ELSA може інтегрувати свої рішення в логи програм Bro, NIDS alerts, OSSEC, syslog, а також інтегруватися в веб-браузери Chromium/Chrome [91] тощо).

Виявлення кібератак на систему відбується за рахунок набору встановлених засобів в ПЗ і засноване на сигнатурних базах даних, статистичних даних та повному контролі змін в системі. Також вбудовані засоби здатні динамічно реагувати на виникнення загроз і їх поведінку [88]. Управління системою може бути централізоване (наприклад, для Snort, Bro, Suricata тощо) і розподілене (наприклад, для OSSEC), а також є можливість адаптування та масштабування відповідно до потреб окремого користувача чи підприємства [85].

За допомогою сукупності програмних засобів спостереження за системою відбувається на системному і мережевому рівнях [27].

Реакція на кібератаку в реальному режимі часу здійснюється тільки у випадку використання в Security Onion відповідного функціоналу, що підтримується необхідним ПЗ із наданого списку [86]. Спеціальні механізми захисту Security Onion не розкриті розробниками, вона підтримується ОС Unix та Linux [27].

Результати аналізу відкритих СВВ відповідно до запропонованих характеристик зведемо в табл. 1.1.

Таблиця 1.1

Зведені дані результатів аналізу відкритих СВВ

№	СВВ	Класи кібератак		Адаптивність	Методи виявлення											Управління системою		Масштабованість	Рівень спостереження		Реакція на кібератаку	Захищеність	Підтримка ОС			
		Зловживання	Аномалії		Експертний	Статистичний	Сигнатурний	Графи сценаріїв	Контроль зміни подій	Кластерний	Динамічний	Машинного навчання	Поведінковий	Евристичний	Нечітких множин	Централізоване	Розподілене		Системний	Мережевий			Unix	Linux	Windows	MacOS
1	AAFID	+	+	-	+	-	+	-	-	-	-	-	-	-	-	+	-	+	+	-	-	-	+	+	-	-
2	Snort	+	+	-	-	+	+	-	-	-	-	-	-	-	-	+	-	+	-	+	+	+	+	+	+	-
3	Prelude SIEM	+	+	-	-	-	+	-	-	-	-	-	-	-	-	+	-	+	-	+	+	+	+	+	-	-
4	NetSTAT	+	+	+	-	-	+	-	+	-	-	-	-	-	-	-	+	+	+	+	+	+	+	+	-	-
5	ASAX	+	-	-	+	-	-	-	-	-	-	-	-	-	-	+	-	+	+	-	-	-	+	+	-	-
6	Bro	+	+	-	-	-	+	-	-	-	-	-	-	-	-	+	-	-	-	+	+	-	+	+	-	+
7	OSSEC	+	+	-	-	-	+	-	-	-	-	-	-	-	-	+	+	+	+	-	+	+	+	+	+	+
8	Suricata	+	+	+	-	+	+	-	-	-	-	-	-	-	-	+	-	+	-	+	+	-	+	+	+	+
9	Samhain	+	+	+	-	+	-	-	-	-	+	-	+	-	-	+	+	+	+	-	+	+	+	+	+	+
10	Security Onion	+	+	+	-	+	+	-	+	-	+	-	+	-	-	+	+	+	+	+	+	-	+	+	-	-

Проведений аналіз відкритих СВВ, за рахунок базових характеристик, як-от клас атак, адаптивність, методи виявлення атак, управління системою, масштабованість, рівень спостереження за системою, реакція на атаку, захищеність та підтримувана ОС. Це надасть певні можливості для розробників і користувачів обрати відповідне сучасне ПЗ для захисту ІС.

1.3. Програмні та програмно-апаратні засоби виявлення вторгнень

Відповідно до визначеного набору базових характеристик також розкриємо властивості програмних та програмно-апаратні засоби виявлення вторгнень.

Shadow

Мережева СВВ Shadow (Secondary Heuristic Analysis for Defensive Online Warfare, розробник Naval Surface Warfare Center (військово-морський центр), Вірджинія, США) містить станції-давачі і станції-аналізатори [23]. Перші розташовані на зовнішній стороні міжмережевих екранів, а другі у внутрішньому захищеному сегменті мережі. Станція-давач – це сервер, на якому активізований tcpdump, який записує трафік у файл. Давачі виокремлюють заголовки пакетів і зберігають їх у спеціальному файлі. Станція-аналізатор зчитує цю інформацію, фільтрує її і генерує відповідний журнал. Якщо події ідентифіковані і для них існує стратегія реагування, то попереджувальні повідомлення не генеруються. Давачі використовуються для вилучення пакетів утиліти libpcap, а основний аналіз відбувається в модулі tcpdump, який містить фільтри пакетів, що поділяються на прості та складні (з декількох фільтрів). Фактично система використовує низку фільтрів мовою Perl, сенсори і аналізатори. Також Shadow (рис. 1.18) функціонує на багатьох UNIX-системах, включаючи FreeBSD і Linux та використовує веб-інтерфейс для відображення інформації [92-94]. Завдяки гнучкості мови Perl архітектура, що використовується в Shadow є однією з кращих серед мережевих СВВ.

Система орієнтована на виявлення зловживань та простих аномалій за допомогою методу контролю станів мережі, який не забезпечує систему в повній мірі можливістю адаптивності до нових кібератак. Shadow має закритий початковий код, а відповідні розширення здійснюються лише розробником. Система давачів та сенсорів дозволяє виявляти кібератаки на основі контролю зміни характеристик мережі за допомогою використання журналів стану та певних програмних фільтрів. Управління системою проводиться розподілено через файли конфігурації на всіх вузлах, де розташовані ком-

поненти системи. Архітектура Shadow дозволяє будувати давачі (розташовані у вузлах мережі для збору інформації і запису у журнал) та аналізатори (аналізують всі події зареєстровані у журналі за допомогою давачів) для виявлення атак на різних рівнях мережі незалежно від її розміру [30, 92, 93].

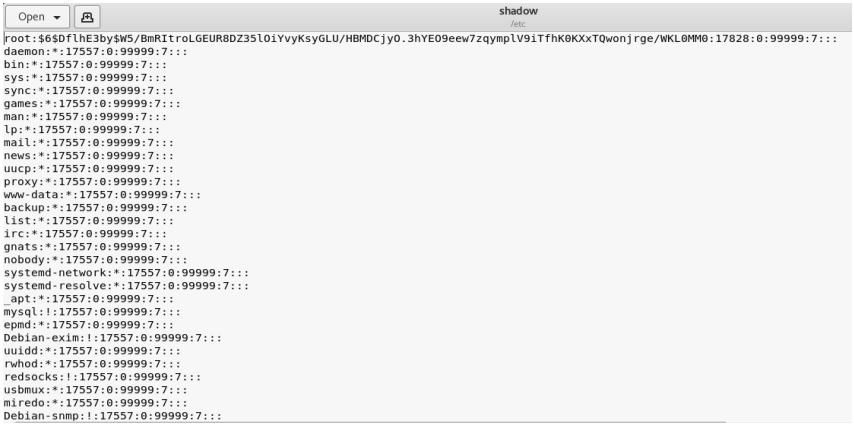

Рис. 1.18. Робоче вікно Shadow

Особливості будови даної системи дозволяють виявляти кібератаки лише на мережевому рівні [95]. Для своєї безпеки Shadow використовує протокол SSH, але не містить спеціальних механізмів протидії вторгненням і не є стійкою до можливих спрямованих на неї кібератак. Вона підтримується ОС Kali Linux (Unix та Linux), є частиною програмного продукту Snort та працює в пасивному режимі для збирання даних про систему [96].

Cisco IPS

Система запобігання вторгнень Cisco IPS (Cisco Intrusion Prevention System, розробка компанії Cisco, США) функціонує в режимі реального часу та забезпечує ідентифікацію і блокування шкідливого трафіку, черв'яків, вірусів, а також запобігання порушенню роботи додатків, інтелектуальне виявлення загроз і захист від них, фільтрацію на основі репутації і глобальні перевірки для запобігання загрозам (рис. 1.19) [12, 97, 98].

Рис. 1.19. Моніторинг IPS-давачів з
використанням Cisco IPS

Cisco IPS реалізує функцію глибокого пакетного спостереження, яка ефективно протидіє широкому спектру мережевих кібератак. Елемент управління представлений інтегральною системою контролю за загрозою Cisco IOS і доповнений функцією Cisco IOS Flexible Packet Matching. Даний засіб дозволяє ефективно функціонувати комп'ютерній мережі з урахуванням таких чинників:

- контроль доступності мережі (забезпечує мережевий (розподілений) захист від багатьох атак, експлойтів, хробаків та вірусів);
- швидкість виявлення джерела мережевих кібератак та оперативна реалізація контрзаходів;
- гнучкість розгортання та масштабованість (інтерактивне інспектування трафіку за допомогою будь-якої комбінації ін-

терфейсів локальної мережі та WAN маршрутизатора з налаштованими на протидію визначеним множинам кібератак відповідно до рівня ризику);
- робота з брандмауером Cisco IOS (контроль за функціями безпеки Cisco IOS Software) [99].

Системна архітектура даного програмного засобу складається з чотирьох основних модулів:
- виявлення загроз;
- виявлення мережевих пристроїв (підключень) та неперервний контроль їх роботи;
- комплексного аналізу атак, аномалій та системних подій;
- моніторингу комп'ютерної системи.

Програмний засіб Cisco IOS забезпечує виявлення DoS і DDoS-атак, кібератак на інфраструктуру мережі та нульового дня, моніторинг широкомовних пакетів, виявлення неавторизованих мережевих додатків та захист від шкідливих доменів і IP-адрес. Останні розробки забезпечують:
- спеціалізований захист датацентрів для веб-серверів, баз даних і сховищ;
- безпеку додатків корпоративного класу Oracle, SAP тощо;
- безперервний захист критично важливих серверів від уразливостей ОС і додатків;
- зменшення часу на реагування та IT-витрати;
- легкість розгортання і управління (майстер розгортання включає шаблон сигнатур, орієнтований на дата центр) [97].

Даний програмно-апаратний комплекс призначений для виявлення зловживань та аномалій у мережі. Він частково адаптивний до нових кібератак, оскільки повністю залежний від структури та частоти оновлення бази даних атак. Cisco IPS є закритим програмно-апаратним комплексом з великим спектром налаштувань під особливості мережі і для виявлення вторгнень використовує наявні шаблони сигнатур та певну статистичну інформацію. Управління системою може здійснюватися централізовано або розподілено, залежно від складності побудови мережі. Швидке масштабоване розгортання системи здійснюються за допомогою динамічного управління політиками і установкою необхідних компонент з урахуванням струк-

тури та особливості мережі. Даний засіб здійснює безперервний захист критично важливих ресурсів мережі від різного роду уразливостей на рівні ОС та мережі. Cisco IPS дозволяє швидко виявляти джерела мережевих атак та визначати протидію, наприклад, ідентифікувати кібератаку, блокувати її і генерувати відповідне повідомлення. Також система забезпечує захищеність каналів передачі даних про атаку чи аномалію [97, 100, 101].

Cisco IPS працює тільки на FTP і HTTP/HTTPS серверах з ОС Unix, Linux та Windows [102].

Arbor Networks Spectrum

Система Arbor Networks Spectrum (розробник компанія Arbor Networks, Массачусетс, США) є високопродуктивним рішенням для аналізу мережевого трафіку, визначення шкоди від інцидентів інформаційної безпеки, виявлення вторгнень за допомогою поєднання статистичного, динамічного та сигнатурного методів аналізу. Основним функціоналом Arbor Networks Spectrum (рис. 1.20) [103] є виявлення DoS і DDoS атак, троянів та їх похідних.

Рис. 1.20. Вікно перегляду індикаторів загроз у часі

Arbor може бути розгорнута як пристрій або віртуальне рішення стеження за мережевим трафіком забезпечуючи постійне виявлення кібератак та зменшення їх наслідків. Запатентована в Arbor технологія Cloud Signaling успішно інтегрує цей захист за допомогою хмарних технологій, автоматизуючи ключовий компонент захисту щодо DDoS та скорочуючи час, необхідний для редукування атак. Застосований гібридний багатошаровий захист є достатньо ефективним підходом для захисту даних від DDoS, що забезпечує безпеку корпоративних мереж незалежно від того, який тип DDoS-атак на них направлений [104].

Також Arbor має високоефективні служби управління, що забезпечують високий рівень захисту від відповідних кібератак по всьому світу. Ці служби в режимі онлайн в глобальному просторі мають цілодобову підтримку фахівців щодо редукування DDoS-атак та ведення безперервної розвідки у сфері загроз [105].

Arbor Networks Spectrum забезпечує:

- швидкий і легкий доступ до величин, що характеризують загрози в мережі та створення архіву трафіку;
- візуалізацію характеристик трафіку та загрози;
- централізоване управління щодо виявлення кібератак;
- постійне поновлення бази даних новими видами потенційних атак;
- масштабованість та простоту використання.

Програмний засіб забезпечує повний перегляд всієї активності в мережі з можливістю аналізу пакетних і потокових даних в режимі реального часу. Саме це дозволяє виявляти аномалії та атаки різного рівня. За допомогою функції ATLAS кожен користувач системи може з легкістю отримувати інформацію про нові кібератаки у глобальній мережі у режимі реального часу, що і забезпечує певний рівень адаптивності даної системи. Крім інформації про кібератаки, користувач отримує оновлену політику безпеки і контрзаходи для попередження атак. Часткова відкритість Arbor Networks Spectrum дозволяє покращувати адаптивність системи до нових кібератак, хоча повне оновлення і удосконалення різних модулів централізовано здійснюється розробниками. Система використовує статистичний, динамічний та сигнатурний методи виявлення атак і має централізоване управління за допомогою зручного інтерфейсу Arbor

Spectrum. Гнучкі параметри розгортання системи дозволяють організаціям легко масштабувати та налаштувати даний засіб під потреби своєї мережі. Архітектура Arbor Networks Spectrum дозволяє виявляти атаки на мережевому і системному рівнях. Інтелектуальні схеми роботи і засоби аналізу в режимі реального часу дозволяють службам безпеки розслідувати та підтверджувати відповідні загрози і оперативно вживати необхідних заходів протидії [104, 105]. Система не містить спеціальних механізмів захисту або вони не розкриті розробниками, а також працює на платформі vSphere Hypervisor, яка підтримує ОС Unix, Linux та Windows [106].

InfoWatch ASAP

Спеціалізований програмно-апаратний комплекс InfoWatch ASAP (InfoWatch Automation System Advanced Protector, розробник компанія InfoWatch, Росія) позиціонує себе, як інтелектуальне рішення для виявлення і запобігання кібератак, спрямованих на інформаційну інфраструктуру систем автоматичного управління виробничими і технологічними процесами. Завдяки запропонованому підходу і запатентованим технологіям захисту, рішення має низку переваг перед штатними засобами запобігання вторгнень, які реалізуються виробниками сучасного обладнання [107].

Комплекс InfoWatch ASAP (рис. 1.21) призначений для створення систем безпеки, адаптований до використання в технологічних мережах і здатний виявляти:

- цілеспрямовані атаки на рівні автоматичного управління та введення або виведення даних виконавчими пристроями;
- вторгнення (сигнатурний і статистичний аналіз) та аномалії в характеристиках технологічної ІС;
- команди для зміни налаштувань і мікропрограм технологічного обладнання;
- несанкціоновані підключення до мережі;
- витік інформації щодо стану технологічного процесу;
- уразливості в технологічних ІС [108].

Важливою складовою InfoWatch ASAP є методологічна база, що дозволяє будувати засоби захисту та ефективно протидіяти реально існуючим загрозам. Перевагою комплексу є захист від атак на всіх

рівнях, незалежно від точки її виникнення. Комплексом підтримується більше 20 протоколів (з урахуванням галузевої специфіки), а також методологія аудиту та побудова моделі загроз, що забезпечує ефективний захист від кібератак [107, 109].

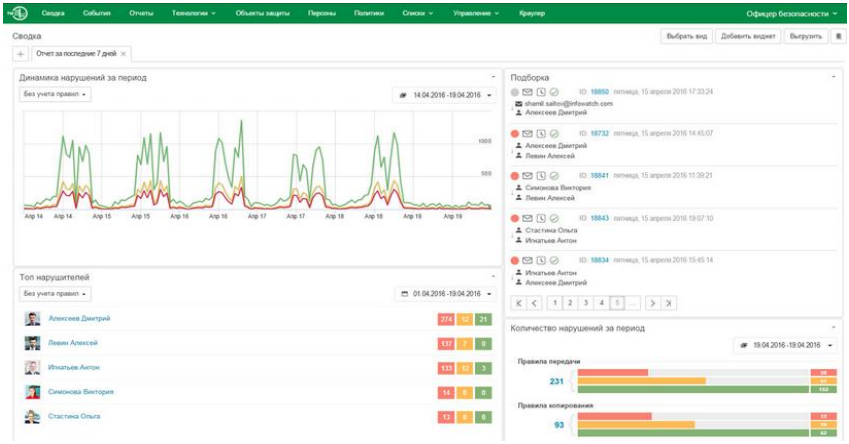

Рис. 1.21. Вікно звіту InfoWatch Traffic Monitor

Даний програмно-апаратний засіб має модульну архітектуру (основні і допоміжні модулі), що дозволяє легко адаптуватись та масштабуватись в залежності від потреб комп'ютерної мережі.

До основних компонентів InfoWatch ASAP належать модулі:

- міжмережевого екранування;
- моніторингу та аналізу захищеності;
- виявлення і запобігання вторгнень;
- контролю коректності виконання;
- технологічного процесу.

Також до InfoWatch ASAP належать допоміжні компоненти:

- модуль забезпечення мережевої безпеки;
- підсистема аналітики і зберігання даних;
- графічний інтерфейс користувача.

Модульна структура дозволяє InfoWatch ASAP функціонувати в режимах моніторингу, інформування і попередження та виявляти кібератаки і аномалії на різних рівнях мережі (зовнішні і внутрішні

атаки на інформаційну структуру підприємства). Постійне оновлення бази даних атак та наявність підсистеми їх моніторингу говорить про умовну адаптивність розробки, а підтримка ПЗ комплексу здійснюється лише його розробниками. InfoWatch ASAP використовує сигнатурний та статистичний методи виявлення вторгнень, а управління здійснюється централізовано за допомогою адміністраторів. Оскільки даний комплекс в основному орієнтований на внутрішню організацію мережі підприємства і попередження атак внутрішнього сегменту, то він доволі легко адаптується до зазначеної мережі та є легко масштабованим. Особливості його будови дозволяють виявляти кібератаки на мережевому і системному рівнях. Розробники InfoWatch ASAP не розкривають спеціальних механізмів захисту та протидії атакам, які спрямовані на комплекс, який підтримується ОС Unix, Linux, Windows та MacOS [108].

Symantec DeepSight

Система Symantec DeepSight (Symantec DeepSight Threat Management System, розробник компанія Symantec, Каліфорнія, США) дозволяє розширити можливості захисту шляхом забезпечення раннього оповіщення про активні атаки, потенційні загрози, нові уразливі місця, шпигунські програми, рекламне ПЗ, що дає можливість адміністраторам більш точно передбачити і оцінити ступінь ризику, а також визначити пріоритетність інформаційних ресурсів, яким необхідний першочерговий захист від вторгнень. Також наявність розсилки персоніфікованих повідомлень, які доповнені професійним аналізом загроз, узагальнювальними оцінками і підтримкою вибору дій роблять Symantec DeepSight Threat Management System (рис. 1.22) провідною системою раннього оповіщення про глобальні кібератаки. Система має достатньо розгалужену інфраструктуру у глобальному кіберпросторі, яка складається з низки мереж honeypot [110-112].

За допомогою даної системи можна аналізувати вхідні потоки даних, що надходять до комп'ютерів через мережу та блокувати загрози до їх реалізації в системі.

Серед особливостей роботи даного програмного засобу слід віднести:

- автоматичне визначення пріоритетів серед існуючих загроз та ресурсів системи, що дозволяє оперативно встановити необхідний рівень протидії чи захисту;
- експертний аналіз даних, які збираються з тисяч джерел у глобальному кіберпросторі, включаючи інформацію про активні глобальні атаки;
- постійне збільшення та розширення баз даних існуючих мережевих загроз, через широке поширення даного програмного продукту;
- автоматизований моніторинг комп'ютерних мереж в реальному режимі часу, з можливістю швидкого сповіщення про загрозу;
- аналіз існуючих потенційних загроз в системі та створення базової стратегії їх попередження;
- здійснення управління програмним засобом спеціальними моніторами контролю функціонування в залежності від особливостей системи;
- стратегію редукування наслідків загроз, яка дозволяє забезпечити кращу пріоритетність, розподіл і розгортання персоналу та відповідних ресурсів безпеки;
- точний аналіз, який відповідає вимогам конкретної системи з урахуванням її мережевої структури, особливостей організації та виду діяльності [110, 112].

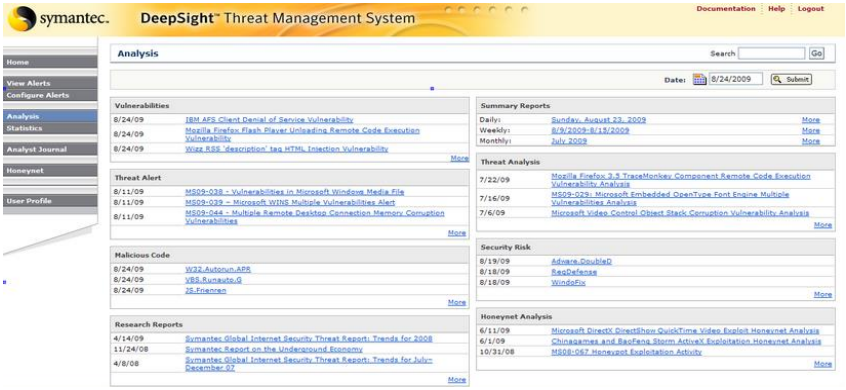

Рис. 1.22. Вікно Symantec DeepSight Threat Management System

Дане ПЗ здатне виявляти атаки і аномалії. Завдяки постійному оновлення бази даних мережевих загроз та розширенню можливостей виявлення кібератак система достатньо легко адаптується до нових видів вторгнень. Підтримка та оновлення Symantec DeepSight здійснюється централізовано розробниками ПЗ. Система використовує експертний, статистичний, динамічний, машинного навчання та сигнатурний методи виявлення кібератак. Залежно від складності побудови системи та мережевої структури, управління може бути централізованим або розподіленим. Система є масштабованою, оскільки має чітку ієрархічну структуру, тобто при розширенні мережі збільшується лише кількість даних для аналізу, які необхідно опрацювати. Зазначена розробка здатна виявляти різного роду кібератаки, які були здійсненні на мережевому рівні, а також в певній мірі аналізувати журнали реєстрації низки програмних засобів та додатків. Symantec DeepSight Threat Management System дозволяє здійснювати завчасне (до нанесення шкоди підприємству) попередження щодо кібератак. Система дозволяє адміністраторам реалізувати превентивні заходи для захисту інфраструктури і компонентів мережі, а також протидіяти втратам продуктивності та нанесенню шкоди репутації компанії. За допомогою автоматизованих сповіщень із заданим пріоритетом на глобальному рівні система формує статистично надійну і дуже детальну інформацію про атаки, з можливістю відстеження даних у часі, країни, галузі промисловості та інших параметрів. Існуючі можливості щодо виявлення кібератак, реалізації контрзаходів і використання методів протидії та додаткових джерел довідкової інформації дозволяє системі діяти негайно та ефективно [110].

Symantec DeepSight Threat Management System не містить спеціальних механізмів захисту або вони не розкриті розробниками. Система підтримується ОС Unix, Linux, Windows і MacOS [113].

IPS

Система IPS (Intrusion Prevention System Software Blade, розробник компанія CheckPoint, США) призначена для запобігання вторгнень та орієнтована на доповнення функцій безпеки міжмережевих екранів для захисту від шкідливого та небажаного мережевого трафіку, включаючи DoS- та DDoS-атаки, уразливості в додатках і серверах (Application and server vulnerabilities), інсайдерські загрози

тощо. Intrusion Protection System забезпечує повне та активне попередження вторгнень і складається з базового продукту IPS (рис. 1.23) та низки додаткових програмних модулів Check Point Software. За їх допомогою достатньо легко можна масштабувати та адаптувати систему під потреби мережі. Також IPS дозволяє здійснювати автоматичну активацію мережевого і системного захисту, навіть за відсутності адміністративного контролю. Система також забезпечує комплексний захист мережі (без погіршення продуктивності шлюзу) від небажаного трафіку в IM і P2P, у тому числі виявлення та попередження існуючих експлойтів, відомих і не відомих уразливостей, спроб тунелювання (які можуть свідчити про витік даних), а також виявлення і запобігання неправильному використанню протоколу, що може вказувати на потенційні загрози та стороннє ПЗ. Також забезпечує захист від інсайдерських загроз та уразливостей додатків і серверів [114, 115].

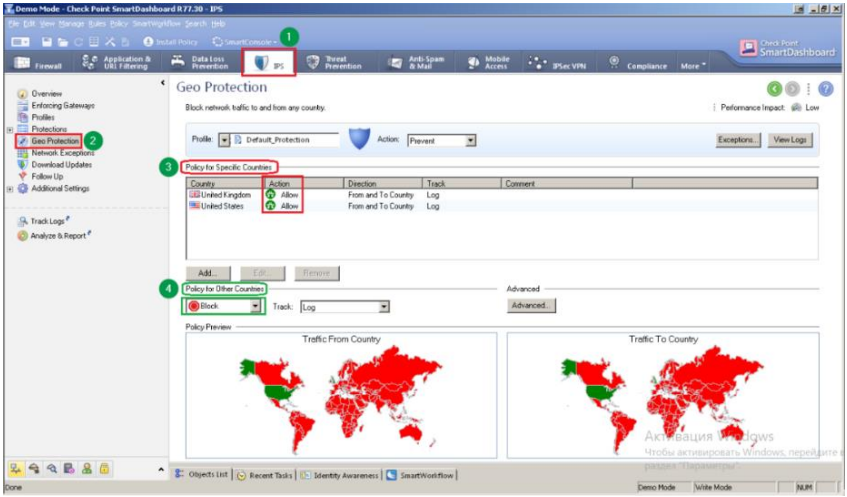

Рис. 1.23. Функція контролю управління трафіком
в IPS (Geo-Protection)

Даний програмний засіб має можливість виявляти кібератаки та аномалії і забезпечувати захист в режимі реального часу. Він постійно оновлює інструментарій протидії новим загрозам, до яких

легко адаптується. Інструментарій є превентивним і забезпечує захист до того, як уразливості будуть виявлені, а експлойти створені. Підтримка та оновлення даного ПЗ здійснюється лише його розробниками. Використання системою додаткових модулів розширення (SmartEvent та інші), крім статистичного і сигнатурного аналізу дозволяє здійснювати і динамічний, що покращує механізми виявлення кібератак та протидії їм. В IPS здійснюється централізоване управління з основного монітора за допомогою відповідного зручного інтерфейсу користувача. Розробка характеризується простим процесом масштабованості системи під потреби мережі. Також є можливість інтеграції з існуючими міжмережевими екранами на підприємстві та подібними програмними засобами. Архітектура системи дозволяє виявляти кібератаки на мережевому і системному рівнях. Реакція на атаку визначається адміністратором безпеки або здійснюється автоматично, відповідно до політики безпеки IPS. Захист трафіку програмного засобу забезпечується протоколом SSL, а гранулярність дозволяє встановлювати винятки для інспекції SSL, щоб не порушити конфіденційність і забезпечити виконання політик безпеки. Зашифрований контент перевіряється, але адміністратор може встановити певні виключення з правил верифікації [114, 115]. IPS працює на ОС Windows [116].

TippingPoing NGIPS

Система TippingPoing NGIPS (TippingPoing Next Generation Intrution Prevention System, розробка компанії TrendMicro, США) є продуктом нового покоління, призначеним для попередження та запобігання вторгнень. Використовується для мережевої безпеки і реалізує комплексний захист від відомих та невідомих уразливостей, запобігає цілеспрямованим атакам, блокує загрози й шкідливі програми, що впроваджуються або поширюються в дата-центрах і корпоративних мережах. Система TippingPoing NGIPS є гнучкою та високопродуктивною і інтегрує технології захисту різних поколінь, включаючи глибокий аналіз пакетів, загроз, репутації URL-адрес та шкідливого ПЗ для клієнтських платформ і додатків [117-119].

Даний продукт розрахований на масштабні комп'ютерні мережі та має високу адаптивність. Серія TippingPoint NX (рис. 1.24-1.25) допомагає зменшити витрати часу на адміністрування і розставити пріоритети щодо мережевої безпеки за допомогою рішення

Enterprise Vulnerability Remediation (eVR), яке дозволяє клієнтам імпортувати дані сканерів уразливостей в TippingPoint Security Management System, провести їх через фільтри служби цифрової вакцинації Digital Vaccine і оперативно вжити відповідні заходи. Реалізований в системі аналіз загроз забезпечує такий рівень прозорості, який необхідний для оптимізації стану інформаційної безпеки в межах всієї організації [117, 120].

Рис. 1.24. Інформаційна панель TippingPoint NGIPS
(сканування даних в режимі реального часу
для пошуку потенційних загроз)

Даний програмно-апаратний комплекс орієнтований на виявлення зловживань та аномалій у мережі, він адаптується до нових кібератак (містить адаптивний інтелект), оскільки використовує статистичні моделі машинного навчання та динамічні методи аналізу трафіку. Це дозволяє на основі отриманих мережевих даних в режимі реального часу приймати рішення щодо стану безпеки мережі для захисту її від нових та складних атак [117, 119].

Tipping Poing NGIPS є закритим програмно-апаратним комплексом з широкими можливостями і легко адаптується під особливості мережі. Він, на основі отриманих в режимі реального часу мережевих даних, приймає рішення про шкідливість мережевого трафіку

для даної системи. Комплекс, також застосовує технології машинного навчання для визначення і блокування відомих і невідомих видів шкідливих програм, які використовують алгоритми генерації доменів (Domain Generation Algorithms, DGAs) для створення доменних імен командних серверів. Також застосовується статистичний та динамічний методи виявлення атак, використання яких допомагає ефективно виявляти загрози в мережі [117].

Комплекс має модульну архітектуру, що полегшує управління розгалуженими і складними за структурою мережами. Саме тому, залежно від потреб підприємства, управління системою може здійснюватися централізовано або розподіллено.

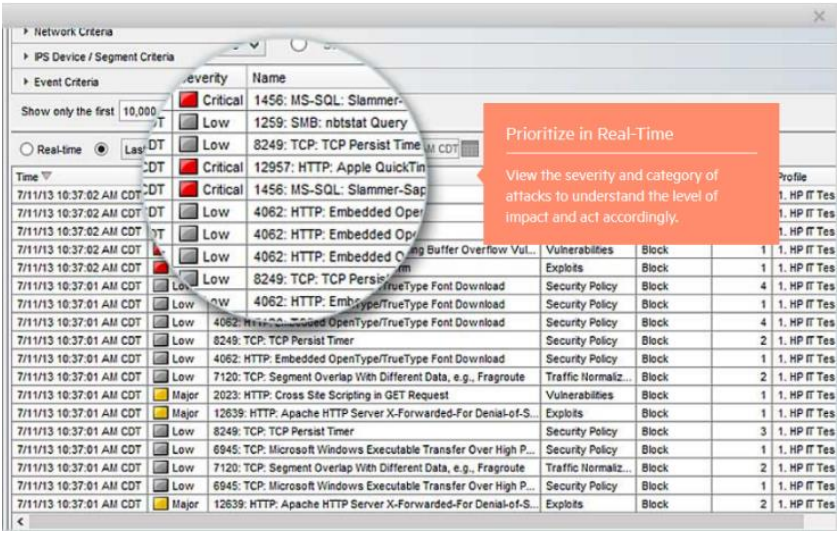

Рис. 1.25. Функціонування TippingPoint NGIPS
в режимі реального часу
(режим перегляду рівня впливу і категорій кібератак)

Масштабована NGIPS динамічно захищає всі програми, мережу та дані від нових і розширених загроз. Оперативність щодо масштабованості забезпечується модульною архітектурою, простотою інтеграції політики безпеки під конкретні потреби підприємства та можливістю спільного використання з іншим ПЗ [119].

TippingPoing NGIPS здійснює безперервний захист критично важливих ресурсів мережі, бізнес-процесів та додатків від різного роду уразливостей. Також реалізовані функції інформування про додатки і їх контролю за допомогою глибокого аналізу трафіку, здійснюється перевірка певних типів файлів і захист критично важливої інформації. Саме тому, NGIPS забезпечує комплексний захист на мережевому і системному рівнях. Комплекс NGIPS дозволяє швидко виявляти джерела мережевих кібератак та визначати реакцію на них. Наприклад, інтелектуалізоване блокування за контекстом визначених IP-адрес з урахуванням їх репутації. Захищеність каналів передачі даних щодо атак чи аномалій забезпечується шляхом використання новітніх засобів шифрування [117-119]. Комплекс підтримується ОС Windows та MacOS [121].

Axoft invGUARD

Програмно-апаратний комплекс Axoft invGUARD (розробка компанії Axoft, Росія) здійснює моніторинг мережевого трафіку за допомогою протоколів SNMP, NetFlow, BGP та детектує аномалії і мережеві атаки [122]. Він складається з двох базових компонент:

- система програмно-апаратного комплексу аналізу мережевого трафіку (invGUARD AS);
- система фільтрації та очищення мережевого трафіку (invGUARD CS/CS-01).

Axoft invGUARD орієнтований на аналіз вхідних потоків даних, що надходять в ІС через мережу з метою виявлення DOS- і DDOS-атак, BGP і SNMP аномалій, кібератак на інфраструктуру мережі, широкомовних пакетів та атак на програмні додатки [122, 123].

До основних функцій invGUARD відносять:

- неперервний моніторинг і аналіз трафіку;
- очищення вхідного трафіку з використанням статистичних та сигнатурних моделей;
- блокування зовнішніх мережевих атак на підзахисні сегменти мережі;
- забезпечення функціонування підзахисних сегментів мережі при реалізованих загрозах безпеки;
- централізація управління;

- можливість масштабування та адаптації комплексу до особливостей побудови і сфери функціонування мережі;
- розбір трафіку прикладних протоколів для блокування кібератак, пов'язаних з впливами на веб-інтерфейси і прикладну частину ІС;
- формування звітів за різною інформацією (рис. 1.26) [123].

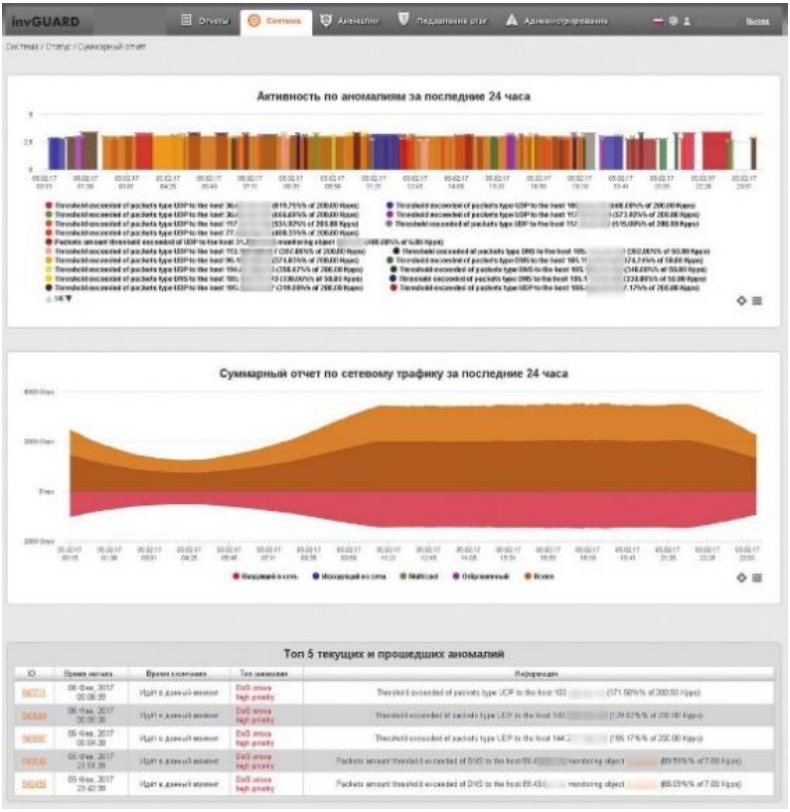

Рис. 1.26. Вікно звіту системи Axoft invGUARD

Особливості будови Axoft invGUARD дозволяють ефективно виявляти зловживання та аномалії у мережі. Це здійснюється завдяки використанню методів статистичного, сигнатурного, евристичного, поведінкового та динамічного аналізу, що певною мірою забезпечує

властивість адаптивності. Комплекс є закритим і має широкі можливості щодо адаптації до особливостей мережі. Управління системою здійснюється централізовано, воно направлене на збирання і аналіз мережевих даних та блокування кібератак [123].

Також є можливість адаптування і масштабування шляхом збільшення кількості засобів фільтрації трафіку. Особливості будови Axoft invGUARD дозволяють виявляти атаки на мережевому і системному рівнях [123, 124].

Комплекс не містить спеціальних механізмів захисту та реакції на атаку (або вони не розкриті розробниками) і працює на ОС Unix і Linux.

DefensePro

Програмно-апаратний засіб DefensePro (DefensePro DDoS Defense & DDoS Prevention Device, розробник компанія RadWare, Ізраїль) призначений для попередження і запобігання мережевим вторгненням та атакам у режимі реального часу, що забезпечує неперервність роботи мережі і додатків (рис. 1.27). Він захищає від використання уразливостей додатків (неправильне використання додатків), поширення шкідливого ПЗ, мережевих аномалій, шкідливих доменів та IP-адрес, крадіжки інформації, троянів та від кібератак DDoS (DoS), спуфінг, фішинг, нульового дня, на основі SSL і сторінки авторизації та CDN [125, 126].

В DefensePro вбудовано два апаратних компонента, перший з яких DoS Mitigation Engine (DME), що призначений для відбиття масованих DoS- і DDoS-атак без впливу на нормальний трафік комп'ютерної мережі, а другий – StringMatch Engine (SME), який направлений на прискорення виявлення сигнатур, що є характерними для певної комп'ютерної мережі [125, 127].

Також комплекс захищає онлайн послуги, що базуються на вебдодатках та працює з іншими засобами забезпечення безпеки, що дозволяє підвищити рівень захищеності всіх сервісів і додатків [126].

DefensePro інтегрує функції запобігання вторгнень та аналізу поведінки мереж, а постійне оновлення бази даних мережевих загроз та розширення можливостей виявлення кібератак за допомогою операційного центру безпеки Radware дозволяє забезпечити користувачів автоматичною щотижневою доставкою сигнатурних фільтрів, а також необхідними фільтрами для критичних ситуацій. Підтримка

та оновлення даного ПЗ здійснюється лише його розробниками. DefensePro заснований на стандартній технології виявлення сигнатур для запобігання відомих уразливостей, та складається з запатентованої технології на основі поведінкового аналізу, що автоматично генерує сигнатури в режимі реального часу. Це дозволяє оперативно запобігти, виявляти або блокувати мережеві атаки [125, 126].

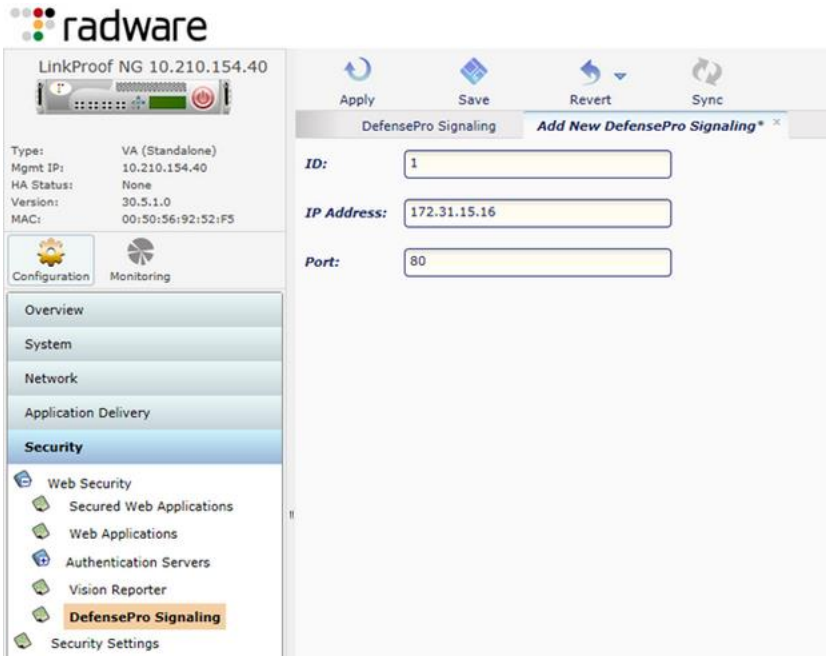

Рис. 1.27. Вікно ПЗ DefensePro

Програмну частину системи складає APSolute Vision з централізованим управлінням і моніторингом та функцією звітності на багатьох пристроях і місцях розташування DefensePro. Це рішення орієнтоване в режимі реального часу здійснювати ідентифікацію, пріоритизацію та протидію порушенням політик безпеки, кібератакам та внутрішнім загрозам [125].

Масштабованість зумовлюється простою структурою побудови системи DefensePro. Модуль реагування програмно-апаратного комплексу на кібератаки здійснює розрив з'єднання з атакуючим об'єктом або його блокування. У поєднанні з SSL Radware AppXcel зазначений комплекс надає потужне і здатне до масштабування рішення для захисту від зашифрованих (заснованих на SSL) атак, які можуть обійти неперервний контроль безпеки. При утворенні оригінального SSL-тунелю між клієнтом і сервером DefensePro копіює SSL трафік на AppXcel, який розшифровує його і передає для перевірки в DefensePro. При виявленні атаки в розшифрованому SSL трафіку DefensePro (в режимі реального часу) блокує шкідливе мережеве з'єднання [125, 126].

Комплекс працює в програмних емуляторах KVM kernel 3.19 (Unix, Linux), QEMU 2.0 (Unix, Linux, Windows, MacOS), VMware (ESX server versions: 5.1, 5.5, 6.0) (Unix, Linux, Windows) [128].

KATA Platform

Система KATA Platform (Kaspersky Anti Targeted Attack Platform, розробка компанії Kaspersky, Росія) орієнтована на розвиток новітніх технологій у сфері корпоративних комп'ютерних мереж і використовується для захисту від комплексних цільових атак будь-якої складності. Рішення KATA Platform інтегрує новітні технології та глобальну аналітику, що дозволяє своєчасно реагувати на цілеспрямовані дії НАС, а також протидіяти атакам на всіх етапах їх реалізації [129]. Програмний засіб реалізує функції контролю мережевої активності, аналізу поводження об'єктів системи, виявлення комплексних цільових кібератак та аналіз аномалій в комп'ютерних мережах [129, 130].

Для збору первинної інформації про аномалії в KATA Platform (рис. 1.28) використовуються сенсори (спеціальні агенти), які аналізують IP, веб і e-mail трафік та події на робочих станціях і серверах. Агенти KATA Platform сумісні з іншим програмними засобами захисту і здійснюють мінімальний вплив на продуктивність мережі та комп'ютерів [131].

Функціонування KATA Platform базується на чотирьох етапах і є частиною комплексного стратегічного підходу для створення адаптивної моделі захисту від нових загроз і реагування на інциденти інформаційної безпеки:

Етап 1 – виявлення:

- постійний моніторинг активностей, які сигналізують про початок атаки;
- викривання уразливостей в системі безпеки і спроб проникнення в мережу;
- викривання інцидентів, оцінка збитку і пріоритизація подальших дій;
- тренінги з розслідування цільових атак;
- звіти про цільові атаки.

Етап 2 – реагування:

- аналіз шкідливого ПЗ;
- оперативна протидія атакам і редукування пов'язаної з ними шкоди;
- протидія інцидентам та їх розслідування;
- проведення глибокої цифрової криміналістики.

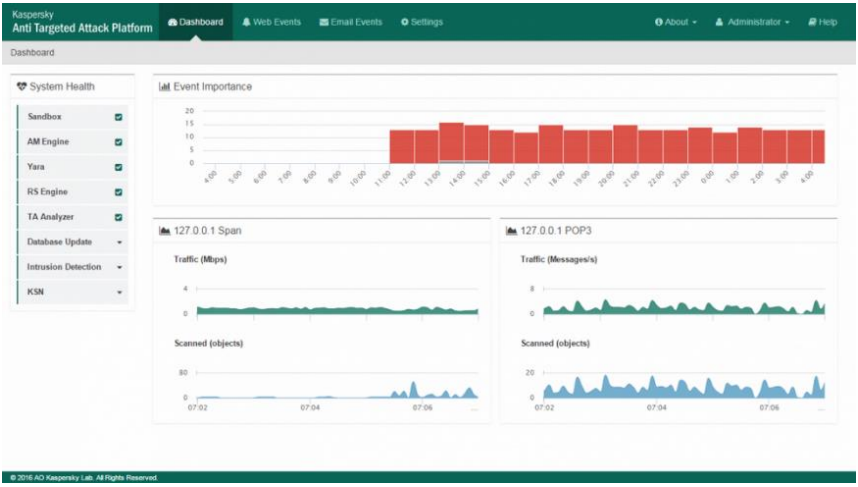

Рис. 1.28. Вікно ПЗ Kaspersky Anti Targeted Attack Platform

Етап 3 – прогнозування:

- тестування на проникнення;
- оцінка рівня захищеності системи;

- оцінка потенційних ризиків для безпеки в поточній інфраструктурі;
- рекомендації щодо удосконалення заходів захисту і усунення уразливостей;
- проактивний захист, який адаптується до нових і невідомих загроз.

Етап 4 – протидія:

- підвищення обізнаності співробітників про актуальні кіберзагрози (навчальні ігри, симуляція загроз тощо);
- тренінги з кібербезпеки для фахівців, що підвищують ефективність протидії цільовим атакам [130, 132].

Система KATA Platform здатен виявляти аномалії та комплексні цільові атаки різного роду, а постійне і оперативне оновлення бази даних мережевих загроз та розширення можливостей щодо виявлення кібератак, дозволяє забезпечувати користувачам адаптивність до нових вторгнень. Підтримка та оновлення даного ПЗ реалізується лише розробником. Аналіз цільових атак здійснюється на основі інформації від мережевих сенсорів, робочих станцій і серверів для створення типових шаблонів поведінки програм. Далі на основі відхилень від цих шаблонів визначається, чи є активність потенційною частиною цільової атаки. Також підозрілі об'єкти, які виявлені в поштовому і інтернет-трафіку передаються сенсорами в «пісочницю», де кожен такий об'єкт аналізується на предмет шкідливої активності, що дозволяє виявляти атаку на ранній стадії [129].

Система має централізоване та розподілене управління, а також можливості адаптування і масштабування платформи до кількісті вхідного трафіку та архітектури мережі. Особливості будови KATA Platform дозволяють виявляти кібератаки на мережевому і системному рівнях. Також сенсори мережі і робочих станцій дають можливість розташовувати точки контролю в різних сегментах мережі і швидко виявити комплексні загрози. Система оперативно реагує на атаки, що визначені нею у відповідній базі даних, а також дає можливість проведення цифрової криміналістики [129, 130, 132].

Спеціальні механізми захисту, що містяться в KATA Platform не розкриті розробниками. Система функціонує на основі ОС Unix, Linux, Windows та MacOS.

За аналогією з п. 1.2 результати аналізу програмних та програмно-апаратних засобів виявлення вторгнень відповідно до запропонованих характеристик зведемо в табл. 1.2.

Таблиця 1.2

Зведені дані результатів аналізу засобів виявлення вторгнень

№	СВВ	Класи кібератак		Адаптивність	Методи виявлення										Управління системою		Масштабованість	Рівень спостереження		Реакція на кібератаку	Захищеність	Підтримка ОС			
		Зловживання	Аномалії		Експертний	Статистичний	Сигнатурний	Графи сценаріїв	Контроль зміни подій	Кластерний	Динамічний	Машинного навчання	Поведінковий	Евристичний	Нечітких множин	Централізоване	Розподілене		Системний	Мережевий			Unix	Linux	Windows	MacOS
1	Shadow	+	+	-	-	-	-	-	+	-	-	-	-	-	-	-	+	+	-	+	-	+	+	+	-	-
2	Cisco IPS	+	+	+	-	+	+	-	-	+	-	-	-	-	-	+	+	+	+	+	+	+	+	+	+	-
3	Arbor Networks Spectrum	+	+	+	-	+	+	-	-	-	+	-	-	-	-	+	-	+	+	+	+	-	+	+	+	-
4	InfoWatch ASAP	+	+	+	-	+	+	-	-	-	-	-	-	-	-	+	-	+	+	+	-	-	+	+	+	+
5	Symantec DeepSight Threat Management System	+	+	+	+	+	+	-	-	-	+	+	-	-	-	+	+	+	+	+	+	-	+	+	+	+
6	IPS	+	+	+	-	+	+	-	-	-	+	-	+	-	-	+	-	+	+	+	+	+	-	-	+	-
7	Tipping Poing NGIPS	+	+	+	-	-	+	-	-	-	+	+	-	-	-	-	+	+	+	+	+	+	-	-	+	+
8	Axoft invGUARD	+	+	-	-	+	+	-	-	-	+	-	+	+	-	+	-	+	+	+	-	-	+	+	-	-
9	DefensePro	+	+	+	-	+	+	-	-	-	-	-	+	-	-	+	-	+	-	+	+	+	+	+	+	+
10	KATA Platform	+	+	+	-	+	+	-	-	-	+	-	+	-	-	-	+	+	+	+	+	+	+	+	+	+

Далі необхідно інтегрувати результати проведеного аналізу всіх засобів виявлення вторгнень за визначеними в п. 1.1 базовими характеристиками для відображення їх існуючих переваг і недоліків з метою створення найбільш ефективних механізмів безпеки при впливах кібератак.

1.4. Узагальнювання результатів аналізу систем виявлення вторгнень та постановка задач дослідження

З урахуванням проведених досліджень (див. п. 1.2 і п. 1.3) узагальнемо результати аналізу відкритих СВВ та програмних і програмно-апаратних засобів виявлення вторгнень (відповідно до базових характеристик «Клас кібератак», «Адаптивність», «Відкритість», «Методи виявлення», «Управління системою», «Масштабованість», «Рівень спостереження», «Реакція на кібератаку», «Захищеність» [30] та «Підтримка ОС») за допомогою таблиці 1.3. При цьому, розглядались можливості систем щодо реалізації методів виявлення, як-от експертний, статистичний, сигнатурний, графи сценаріїв, контроль зміни подій, кластерний, динамічний, машинного навчання, поведінковий, евристичний і нечітких множин.

Також, відповідно до проведеного аналізу можна зазначити, що сучасні СВВ аномального принципу, в основному, засновані на математичних моделях, що потребують багато часу для отримання статистичних даних, реалізацію процесу навчання (в основному для нейромережевих систем) та здійснення інших складних і довготривалих підготовчих процедур, також, в жодній з проаналізованих систем не використовуються методи нечітких множин які показали свою ефективність при вирішенні такого класу задач [48, 133].

Одним з недоліків аномальних СВВ є закладений в неї процес створення відповідного профіля нормального стану ІС, а при її модифікації та інших змінах набрана статистика не має необхідної повноти та є неактуальною. Більш ефективні у цьому відношенні є експертні підходи, що засновані на використанні знань та досвіду спеціалістів відповідної предметної області.

Крім того, побудова відповідних методів, технічних рішень та створення засобів (СВВ, виявлення кібератак та інші), орієнтованих на обробку слабкоструктурованих даних з метою встановлення фактів несанкціонованого доступу до РІС є основою для успішної протидії відповідним кібератакам.

Більшість СВВ достатньо дорогі, мають закритий код, потребують кваліфікованого налаштування (під певні вимоги організації та сервіси), яке можуть здійснити тільки висококваліфіковані фахівці.

Таблиця 1.3

Зведені дані результатів аналізу СВВ

№	СВВ	Класи кібератак				Методи виявлення											Управління системою			Рівень спостереження		Реакція на кібератаку	Захищеність	Підтримка ОС			
		Зловживання	Аномалії	Адаптивність	Відкритість	Експертний	Статистичний	Сигнатурний	Графи сценаріїв	Контроль зміни подій	Кластерний	Динамічний	Машинного навчання	Поведінковий	Евристичний	Нечітких множин	Централізоване	Розподілене	Масштабованість	Системний	Мережевий			Unix	Linux	Windows	MacOS
1	AAFID	+	+	-	+	+	-	+	-	-	-	-	-	-	-	-	+	-	+	+	-	-	-	+	+	-	-
2	Snort	+	+	-	+	-	+	+	-	-	-	-	-	-	-	-	+	-	+	-	+	+	+	+	+	+	-
3	Prelude SIEM	+	+	-	+	-	-	+	-	-	-	-	-	-	-	-	+	-	+	-	+	+	+	+	+	-	-
4	NetSTAT	+	+	+	+	-	-	+	-	+	-	-	-	-	-	-	-	+	+	+	+	+	+	+	+	-	-
5	Shadow	+	+	-	-	-	-	-	-	+	-	-	-	-	-	-	-	+	+	-	+	-	+	+	+	-	-
6	ASAX	+	-	-	+	+	-	-	-	-	-	-	-	-	-	-	+	-	+	+	-	-	-	+	+	-	-
7	Bro	+	+	-	+	-	-	+	-	-	-	-	-	-	-	-	+	-	-	-	+	+	-	+	+	-	+
8	OSSEC	+	+	-	+	-	-	+	-	-	-	-	-	-	-	-	+	+	+	+	-	+	+	+	+	+	+
9	Cisco IPS	+	+	+	-	-	+	+	-	-	+	-	-	-	-	-	+	+	+	+	+	+	+	+	+	+	-
10	Arbor Networks Spectrum	+	+	+	-	-	+	+	-	-	-	+	-	-	-	-	+	-	+	+	+	+	-	+	+	+	-
11	InfoWatch ASAP	+	+	+	-	-	+	+	-	-	-	-	-	-	-	-	+	-	+	+	+	-	-	+	+	+	+
12	Symantec DeepSight Threat Management System	+	+	+	-	+	+	+	-	-	-	+	+	-	-	-	+	+	+	+	+	+	-	+	+	+	+
13	IPS	+	+	+	-	-	+	+	-	-	-	+	-	+	-	-	+	-	+	+	+	+	+	+	-	-	+	-
14	Tipping Poing NGIPS	+	+	+	-	-	-	+	-	-	-	+	+	-	-	-	-	+	+	+	+	+	+	-	-	+	+
15	Axoft invGUARD	+	+	-	-	-	+	+	-	-	-	+	-	+	+	-	+	-	+	+	+	-	-	+	+	-	-
16	DefensePro	+	+	+	-	-	+	+	-	-	-	-	-	+	-	-	+	-	+	-	+	+	+	+	+	+	+
17	KATA Platform	+	+	+	-	-	+	+	-	-	-	+	-	+	-	-	-	+	+	+	+	+	+	+	+	+	+
18	Suricata	+	+	+	+	-	+	+	-	-	-	-	-	-	-	-	+	-	+	-	+	+	-	+	+	+	+
19	Samhain	+	+	+	+	-	+	-	-	-	-	+	-	+	-	-	+	+	+	+	-	+	+	+	+	+	+
20	Security Onion	+	+	+	+	-	+	+	-	+	-	+	-	+	-	-	+	+	+	+	+	+	-	+	+	-	-

Такі системи переважно не орієнтовані на виявлення раніше невідомих кібератак (0-day атак), а їх спроможність реалізувати таку можливість тільки декларується і теоретично не обґрунтовується та не розкривається сам механізм виявлення таких кібератак.

Тому, для побудови таких систем необхідний відповідний математичний апарат, наприклад, з використанням теорії нечітких множим, який би дав можливість вирішити проблему виявлення нових типів кібератак.

Зазначена проблема обумовлюється об'єктивним протиріччям між існуючою необхідністю моніторингу та блокування нових видів кібератак за максимально короткий час і високою інерційністю існуючих СВВ щодо їх адаптації до виявлення аномалій, що породжуються реалізацією нових типів загроз РІС.

Практика показує (див. п. 1.1), що на сьогодні існуючі засоби не є ефективними проти нових типів вторгнень. Тому, розробка відповідних методів ідентифікації аномальних станів для СВВ з метою розширення їх функціональних можливостей (за рахунок засобів, що використовують відповідний математичний апарат, наприклад, нечітких множим), дозволить цим системам бути дієвими щодо виявлення нових типів кібератак (у тому числі 0-day атак), які характеризуються невстановленими або нечітко визначеними критеріями у відповідному гетерогенному середовищі. Такі розширені можливості СВВ дозволять їм, фактично, залишатися функціональними у потенційно небезпечному оточенні характерному впливам різноманітних загроз.

Для вирішення такої проблеми необхідно розв’язати наукові завдання, як-от розробка:

– кортежної моделі формування атакуючих середовищ для відображення процесу виявлення аномального стану у заданий часовий проміжок в m-вимірному гетерогенному параметричному середовищі;

– методу формування еталонів для формалізації процесу отримання еталонних середовищ, що містять множини значень фіксованих параметрів заданих груп лінгвістичних змінних;

– методу фазифікації на еталонних підсередовищах для перетворення поточних значень параметрів, направлених на виявлення аномального стану;

– методу номіналізації нечітких чисел для визначення ідентифікуючих термів, що відображають стан поточних середовищ, характерних для реалізації визначених типів кібератак;

– методу визначення ідентифікуючих термів, для пошуку в заданих лінгвістичних змінних перетворених еталонних термів, що характеризують певні рівні аномальності;

– методу дефазифікації параметрів детекційного середовища, для отримання числових оцінок, що характеризують лінгвістичні величини відносно суджень експерта;

– методу формування детекційного середовища для визначення поточних рівнів аномальних станів, характерних дії визначених типів кібератак;

– методології побудови систем виявлення аномалій, породжених кібератаками для розширення функціональних можливостей сучасних систем виявлення вторгнень;

– структурного рішення обчислювальної системи для створення засобів виявлення кібератак на ресурси інформаційних систем;

– алгоритмічного та програмного забезпечення системи виявлення кібератак.

СПИСОК ЛІТЕРАТУРИ ДО РОЗДІЛУ 1

1. Хакерські атаки на Україну [Електронний ресурс] // Вікіпедія : [сайт]. Київ, 2017. URL: https://is.gd/6lkWHY (дата звернення: 17.04. 2018).

2. Пострадавшие от кибератаки банки и компании: перечень [Електронний ресурс] // Дзеркало тижня. Україна : [сайт]. Київ, 2017. URL: https://zn.ua/UKRAINE/postradavshiy-ot-kiberataki-banki-i-kompanii-perechen-252717_.html (дата звернення: 17.04.2018).

3. Хакерська атака на Україну: подробиці [Електронний ресурс] // «РБК-Україна» укр. інформ. портал : [сайт]. Київ, 2017. URL: https://www.rbc.ua/ukr/news/hakerskaya-ataka-ukrainu-podrobnosti-1498566985.html (дата звернення: 17.04.2018).

4. Нейросетевая система обнаружения компьютерных атак на основе анализа сетевого трафика [Электронный ресурс] / А. Г. Мустафаев // Вопросы безопасности. Калининград : ИД «Янтарный терем», 2016. № 2. С. 1-7. URL: http://e-notabene.ru/nb/article_ 18834 .html (дата обращения: 18.04.2018).

5. Системы и методы обнаружения вторжений: современное состояние и направления совершенствования [Электронный ресурс] / А. А. Корниенко, И. М. Слюсаренко // CIT forum : [сайт]. Москва, 2009. URL: http://citforum.ru/security/internet/ids_overview/ (дата обращения: 18.04.2018).

6. Аналіз систем та методів виявлення несанкціонованих вторгнень у комп'ютерні мережі [Електронний ресурс] / В. В. Литвинов [та ін.] // Математичні машини і системи. К : ІПММС НАН України, 2018. № 1. С. 31-40. URL: https://cyberleninka.ru/article/v/ analiz-system-ta-metodiv-viyavlennya-nesanktsionovanih-vtorgnen-u-komp-yuterni-merezhi (дата звернення: 03.07.2018).

7. Анализ и классификация методов обнаружения сетевых атак / А. А. Браницкий, А. В. Котенко // Тр. СПИИРАН. 2016. № 2 (45). С. 207-244.

8. Краткий анализ решений в сфере СОВ и разработка нейросетевого детектора аномалий в сетях передачи данных [Электронный ресурс] // Хабр : [сайт]. 2018. URL: https://habr.com/post/358200/ (дата обращения: 03.07.2018).

9. Сучасні методи виявлення аномалій в системах виявлення вторгнень / О. М. Колодчак // Вісник Національного ун-т «Львівська

політехніка». Комп'ютерні системи та мережі. 2012. № 745. С. 98-104.

10. Дослідження методів виявлення вторгнень в телекомунікаційні системи та мережі / Д. О. Даниленко, О. А. Смірнов, Є. В. Мелешко // Системи озброєння і військова техніка. Х. : Харк. нац. ун-т Повітряних Сил ім. І. Кожедуба, 2012. № 1. С. 92-100.

11. A Survey and Comparative Analysis of Data Mining Techniques for Network Intrusion Detection Systems / R. Patel, A. Thakkar, A. Ganatra. India : International Journal of Soft Computing and Engineering (IJSCE), 2012. Vol. 2. Issue 1. 265-260 pp.

12. The State of the Art in Intrusion Prevention and Detection [Electronic resourse] / Al-Sakib Khan Pathan. New York : Auerbach Publications, 2014. 516 p. URL: http://docshare03.docshare.tips/files/ 20579/ 205795770.pdf (viewed on August 4, 2018).

13. Розробка моделі інтелектуального розпізнавання аномалій і кібератак з використанням логічних процедур, які базуються на покриттях матриць ознак / Г. Бекетова, Б. Ахметов, О. Корченко, В. Лахно // Безпека інформації. К : НАУ, 2016. Т. 22, № 3. С. 242-254.

14. Огляд систем виявлення атак в мережевому трафіку / К. М. Носенко, О. І. Півторак, Т. А. Ліхоузова // Адаптивні системи автоматичного управління. К : НТУУ КПІ, 2014. № 1 (24). С. 67-75.

15. Аналіз системи виявлення вторгнень та комп'ютерних атак / М. М. Радченко [та ін.] // Междисциплинарные исследования в науке и образовании. 2013. № 2.

16. Analysis of Host-Based and Network-Based Intrusion Detection System / Amrit Pal Singh, Manik Deep Singh. India : I. J. Computer Network and Information Security, 2014. Vol. 8. 41-47 pp.

17. Аналіз сучасних систем виявлення та запобігання вторгнень в інформаційно-телекомунікаційних системах [Електронний ресурс] / В. І. Мєшков, В. О. Віролайнен // Проблеми безпеки інформації в інформаційно-комунікаційних системах. Д. : НТУУ КПІ РТФ, 2015. 4 с. URL: http://ela.kpi.ua/bitstream/123456789/17609/1/meshkov.pdf (дата звернення: 06.07.2018).

18. Сравнительный анализ систем обнаружения вторжений, представленных на отечественном рынке / А. Б. Лось, Ю. Ю. Даниелян // Вестник Московского финасово-юридического университета. 2014. № 3. С. 181-187.

19. Сравнительный анализ систем обнаружения вторжений / А.Л. Белова, Д. А. Бородавкин // Актуальные проблемы авиации и космонавтики. Сибирь : СФУ, 2016. Т. 1, № 12. С. 742-744.

20. Аналіз сучасних систем виявлення атак і запобігання вторгненням / А. А. Завада, О. В. Самчишин, В. В. Охрімчук // Інформаційні системи. Житомир : Збірник наукових праць ЖВІ НАУ, 2012. Т. 6, № 12. С. 97-106.

21. Обзор систем обнаружения вторжений [Электронный ресурс] // Металургический журнал. Отрасли народного хозяйства. Исследования рынка : [сайт]. 2003. URL: http://www.metclad.ru/pat-a-587-list/ (дата обращения: 10.07.2018).

22. Обзор зарубежных и отечественных систем обнаружения компьютерных атак / В. А. Бабошин, В. А. Васильев // Информация и космос. СПб : Санкт-Петербургская научно-техническая общественная организация «Институт телекоммуникаций», 2015. № 2. С. 36-41.

23. Системы обнаружения вторжений [Электронный ресурс] / С. Гриняев // Byte/Россия. Москва : СК Пресс, 2001. № 10 (39). URL: https://www.bytemag.ru/articles/detail.php?ID=6563 (дата обращения: 10.07.2018).

24. Выбор характеристик систем обнаружения атак для выработки заключения о функциональных возможностях / Е. С. Абрамов, И. Ю. Половко // Известия Южного федерального университета. Технические науки. Таганрог : ЮФУ, 2011. № 12 (125). С. 88-96.

25. An implementation of intrusion detection system using genetic algorithm / Mohammad Sazzadul Hoque, Md. Abdul Mukit, Md., Abu Naser Bikas // International Journal of Network Security & Its Applications (IJNSA). Sylhet, 2012. Vol. 4, No. 2. P. 109-120.

26. Analysis and Evaluation of Network-Based Intrusion Detection-and Prevention System in an Enterprise Network Using Snort Freeware / O. B. Lawal [et al.] // African Journal of Computing & ICT. Ibadan, 2013. Vol. 6, No. 2. P. 169-184.

27. 11 Top Intrusion Detection Tools for 2018 [Electronic resourse] / S. Cooper. Maidstone, Kent : Comparitech, 2018. URL: https://www.comparitech.com/net-admin/network-intrusion-detection-tools/ (viewed on August 12, 2018).

28. Системи виявлення і запобігання атак в комп'ютерних мережах / Т. І. Зоріна // Вісник східноукраїнського національного університету імені Володимира Даля. 2013. № 15 (204). С. 48-52.

29. Understanding modern intrusion detection systems: a survey [Electronic resourse] / Liu Hua Yeo [et al.]. Michigan : Eastern Michigan University, 2017. URL: https://arxiv.org/ftp/arxiv/papers/1708/1708.07174.pdf (viewed on August 12, 2018).

30. Современные некоммерческие средства обнаружения атак / Д. Ю. Гамаюнов, Р. Л. Смелянский // Программные системы и инструменты. Тематический сборник. М. : Ф-т ВМиК МГУ, 2002. 20 с.

31. Системы и методы обнаружения вторжений: современное состояние и направления совершенствования / А.А. Корниенко, И.М. Слюсаренко // CIT forum : [сайт]. Москва, 2009. URL: http://citforum.ru/security/internet/ids_overview/ (дата обращения: 15.07.2018).

32. Анализ систем обнаружения вторжений на основе интеллектуальных технологий [Электронный ресурс] / Е. Ю. Явтуховский // Технические науки: теория и практика : материалы III Междунар. науч. конф. Чита : Издательство Молодой ученый, 2016. С. 27-30. URL: https://moluch.ru/conf/tech/archive/165/10049/ (дата обращения: 17.07.2018).

33. The statistical analysis of a network traffic for the intrusion detection and prevention systems / A. A. Kuznetsov [et al.] // Telecommunications and Radio Engineering. Kharkiv, 2015. Vol. 74, No. 1.

34. Intrusion Detection By Data Mining Algorithms: A Review / Marjan Kuchaki Rafsanjani, Zahra Asghari Varzaneh // Journal of New Results in Science. Tokat : Gaziosmanpasa University, 2013. No. 2. P. 76-91.

35. А.И. Стасюк, А.А. Корченко, «Базовая модель параметров для построения систем выявления атак», *Захист інформації*, №2 (55), С. 47-51, 2012.

36. М.Г. Луцкий, А.В. Гавриленко, А.А. Корченко, А.А Охрименко, «Модели эталонов лингвистических переменных для систем выявления атак», *Захист інформації*, №2 (55), С. 71-78, 2012.

37. А.А. Корченко, «Модель эвристических правил на логико-лингвистических связках для обнаружения аномалий в компьютерных системах», *Захист інформації*, № 4 (57), С. 112-118, 2012.

38. O Petrov, B Borowik, M Karpinskyy, O Korchenko, V Lakhno, «Immune and defensive corporate systems with intellectual identification of threats», Pszczyna : lska Oficyna Drukarska, 2016, P. 222.

39. Теоретичні основи моделювання процесів нападу на інормацію методами теорій диференціальних ігор та диференціальних перетворень : монографія / Р.В. Грищук. Житомир : ПП «Рута», 2010. С. 279.

40. Нейросетевые модели, методы и средства оценки параметров безопасности и Интернет-ориентированных информационных систем / А.Г. Корченко, И.А. Терейковкий, Н.П. Карпинский, С.Т. Тнымбаев. К. : ТОВ «Наш Формат», 2016. С. 276.

41. Методологія розроблення нейромережевих засобів інформаційної безпеки Інтернет-орінєтованих інформаційних систем / О.Г. Корченко, І.А. Терейковський, А.О. Білощинський. К. : ТОВ «Наш Формат», 2016. С. 249.

42. Дисперсійний аналіз мережевого трафіку для виявлення та запобінання вторгнень в телекомунікаційних системах і мережах / О. О. Кузнецов, О. А. Смірнов, Д. О. Даниленко // Системи обробки інформації. Х. : Харк. нац. ун-т Повітряних Сил ім. І. Кожедуба, 2014. Вип. 2. С. 124-133.

43. A Review of Intrusion Detection Systems / Neyole Misiko Jacob, Muchelule Yusuf Wanjala // Global Journal of Computer Science and Information Technology Research. Framingham : Global Journals Inc., 2017. Vol. 5, No. 4. P. 1-5.

44. Подход к обнаружению аномального трафика в компьтерных сетях с использованием методов кластерного анализа / А. К. Большев, В. В. Яновский // Известия Государственного Электротехнического Университета, серия Информатика, управления и компьютерные технологии. СПб. : Изд-во СПбЭТУ, 2006. Вып. 3. С. 38-45.

45. Классификация систем обнаружения вторжений / А. А. Корченко, С. Т. Ахметова // Інформаційна безпека. К. : НАУ, 2014. № 1 (13); № 2 (14). С. 168-175.

46. Аналіз сучасних систем виявлення та запобігання вторгнень в інформаційно-телекомунікаційних системах / В. І. Мєшков, В. О. Віролайнен // Проблеми безпеки інформації в інформаційно-комунікаційних системах. К. : НТУУ КПІ РТФ, 2015. №. 1. С. 1-4.

47. Безпека інформаційно-комунікаційних систем : навч. посіб. / М. В. Грайворонський, О. М. Новіков. К. : Видавнича група BHV, 2009. – 608 с.

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

49. Модель загроз у розподілених мережах / О. Я. Матов, В. С. Василенко // Реєстрація, зберігання та обробка даних. К. : НАУ, 2008. Т. 10, № 1. С. 91-102.

50. Security Research Laboratory and Education Center [Electronic resourse] / Sofie Nystrom. West Lafayette : Purdue University, 1999. URL: https://www.linuxjournal.com/article/3175 (viewed on August 20, 2018).

51. CERIAS – Autonomous Agents for Intrusion Detection [Electronic resourse] / E. H. Spafford, D. Zamboni. West Lafayette : Purdue University, 2000. URL: http://www.cerias.purdue.edu/site/about /history/coast/projects/aafid.php (viewed on August 20, 2018).

52. An architecture for intrusion detection using autonomous agents [Electronic resourse] / J.S. Balasubramaniyan [et al.] // Proceedings 14th Annual Computer Security Applications Conference. Phoenix : IEEE, 2002. URL: https://ieeexplore.ieee.org/abstract/ document/738563 (viewed on August 20, 2018).

53. An Architecture for Intrusion Detection using Autonomous Agents [Electronic resourse] / J.S. Balasubramaniyan [et al.]. West Lafayette : COAST Laboratory; Purdue University, 1998. URL: https://pdfs.semanticscholar.org/bb4b/a3a4e8b850011844c00aa0fa964bf4664b23.pdf (viewed on August 20, 2018).

54. SNORT [Electronic resourse] / Snort team. San Jose : Cisco Systems Inc, 2018. URL: https://www.snort.org/ (viewed on August 23, 2018).

55. IDS / IPS // Netgate Documentation: [website]. Washington : Rubicon Communications LLC, 2017. URL: https://www.netgate.com/docs/pfsense/ids-ips/ (viewed on August 23, 2018).

56. Snort 2.1. Обнаружение вторжений : книга / Джей Бил [и др.]. М. : Бином-пресс, 2006. Изд. 2. 656 с.

57. Snort [Электронный ресурс] // Spy-Soft.net : Информационная безопасность на практике : [сайт]. Москва, 2016. URL: http://www.spy-soft.net/snort/ (дата обращения: 24.07.2018).

58. Snort / Snort team // Snort Blog : the Official Blog of the World Leading Open-Source IDS/IPS Snort : [website]. San Jose : Cisco Systems Inc, 2017. URL: https://blog.snort.org/2017/10/snort-29110-has-been-released.html (viewed on August 24, 2018).

59. Обзор – Prelude SIEM [Electronic resourse] // Prelude SIEM : [website]. Paris : CS Communication & Systemes, 2018. URL: https://www.prelude-siem.org/ (viewed on August 26, 2018).

60. SIEM на практике: дружим Prelude + Cisco IPS и выявляем эксплуатацию HeartBleed через корреляцию [Электронный ресурс] // Хабр : [сайт]. 2014. URL: https://habr.com/post/220449/ (дата обращения: 26.07.2018).

61. STATL: An Attack Language for State-based Intrusion Detection / S. T. Eckmann, G. Vigna, R. A. Remmerer // Journal of Computer Security. Santa Barbara : Dept. of Computer Science University of California, 2000. P. 1-29.

62. NetSTAT: A Network-based Intrusion Detection Approach / G. Vigna, R. A. Kemmerer // Proceedings 14th Annual Computer Security Applications Conference. Phoenix : IEEE, 1998. P. 1-10.

63. USTAT: A real-time intrusion detection system for UNIX / Koral Ilgun // Proceedings 1993 IEEE Computer Society Symposium on Research in Security and Privacy. Oakland : IEEE, 1993. P. 16-28.

64. ASAX: Software architecture and rule-based language for universal audit trail analysis / Naji Habra, Baudouin Le Charlier, Abdelaziz Mounhji, Isabelle Mathieu // Proceedings of ESORICS`92 European Symposium on Research in Computer Security. Toulouse, 1992. Vol. 648. P. 435-450.

65. Preliminary Report on Distributed ASAX / A. Mounji [et al.] // Research Report, Computer Science Institute. Namur : University of Namur, 1994.

66. Advanced Security Audit Trail Analysis on Unix. Implementation Design of the NADF Evaluator / N. Habra, B. Le Charlier, A. Mounji // Technical report. Namur : University of Namur, 1993.

67. Advanced Security Audit Trail Analysis on Unix (ASAX also called SAT-X). Implemention design of the NADF Evaluator [Electronic resourse] / N. Habra, B. Le Charlier, A. Mounji // Institute D`Informatique. Namur : University of Namur, 1994. P. 1-62. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.51.7971&rep=rep1&type=pdf (viewed on September 3, 2018).

68. Большой Брат: обзор системы обнаружения вторжений Bro [Электронный ресурс] / Р. Ярыженко // Хакер.Ру : [сайт]. М. : ООО Медиа Кар, 2015. URL: https://xakep.ru/2015/06/28/big-bro-197/ (дата обращения: 05.09.2018).

69. Bro: A system for detecting network intruders in real-time / Vern Paxson // Proceedings of the 7th USENIX Security Symposium. San Antonio : USENIX, 1998. 22 p.

70. Bro: A system for detecting network intruders in real-time / Vern Paxson // Computer Networks. Amsterdam : Elsevier, 1999. No. 31 (23-24). P. 2435-2463.

71. Critique of Article Bro: A system for Detecting Network Intruders in Real-Time [Electronic resourse] // 24hourAnNews : [website]. New York : Parker Paradigms, Inc, 2000. URL: https://www.24houranswers.com/college-homework-library/Computer-Science/Network-Management-and-Data-Communication/25914 (viewed on September 6, 2018).

72. Zeek [Electronic resourse] / Vern Paxson// Zeek.org : [website]. Geneva : Zeek (Bro), 2018. URL: https://www.bro.org/download/index.html (viewed on September 6, 2018).

73. Installing the Splunk for OSSEC App [Electronic resourse] / James Nelson // Grep: The Linux Blog : [website]. Kansas City : Grep, 2012. URL: http://grepthelinuxblog.blogspot.com/2012/03/installing-splunk-for-ossec-app.html (viewed on September 8, 2018).

74. Home – OSSEC [Electronic resourse] / OSSEC Project Team // OSSEC.net : [website]. New York, 2018. URL: https://www.ossec.net/ (viewed on September 8, 2018).

75. Downloads – OSSEC [Electronic resourse] / OSSEC Project Team // OSSEC.net : [website]. New York, 2018. URL: https://www.ossec.net/downloads.html (viewed on September 8, 2018).

76. OSSEC and attacking through the firewall [Electronic resourse] // Intrusion detection and firewall security. Oslo, 2016. URL: https://www.cs.hioa.no/teaching/materials/MS004A/html/L65.en.pdf (viewed on September 8, 2018).

77. OSSEC-HIDS Capabilities, Architecture and plans / Ozturk. Ahmet // Presentation at the 5th Linux and Free Software Festival. Ankara, 2006.

78. Suricata | Open Source IDS/IPs/NSM engine [Electronic resourse] // Suricata-IDS : [website]. Boston : Open Information Security Foundation, 2018. URL: https://suricata-ids.org/ (viewed on October 10, 2018).

79. Top 10 Intrusion Detection Tools: Your Best Free Options for 2019 [Electronic resourse] / Renaud Larue-Langlois // Network Admin : [website]. Verdun : AddictiveTips, 2018. URL: https://www. addictivetips.com/net-admin/intrusion-detection-tools/ (viewed on October 11, 2018).

80. Suricata как IPS [Электронный ресурс] // Хабр : [сайт]. 2013. URL: https://habr.com/post/192884/ (дата обращения: 11.10.2018).

81. День сурка. Осваиваем сетевую IDS/IPS Suricata [Электронный ресурс] / Мартин Пранкевич // Хакер.Ру : [сайт]. М. : ООО Медиа Кар, 2015. URL: https://xakep.ru/2015/06/28/suricata-ids-ips-197/ (дата обращения: 11.10.2018).

82. The SAMHAIN file integrity / host-based intrusion detection system [Electronic resourse] / Rainer Wichmann // Samhain : [website]. Boston : Samhain Services, 2011. URL: https://www.la-samhna.de/ samhain/index.html (viewed on October 14, 2018).

83. Examining Tripwire And Samhain IDS Files Information Technology Essay [Electronic resourse] // Information Technology. Huddersfield : UKEssays, 2016. URL: https://www.ukessays.com/ essays/information-technology/examining-tripwire-and-samhain-ids-files-information-technology-essay.php (viewed on October 14, 2018).

84. The SAMHAIN file integrity / host-based intrusion detection system [Electronic resourse] / Rainer Wichmann // Fact Sheet : [website]. Boston : Samhain Services, 2011. URL: https://la-samhna.de/samhain/s_faq.html (viewed on October 14, 2018).

85. Security Onion [Electronic resourse] / Phil Plantamura [et al.] // Security Onion : [website]. Augusta : Security Onion Solutions, 2016. URL: https://securityonion.net/ (viewed on October 16, 2018).

86. Security Onion Solutions [Electronic resourse] / Phil Plantamura [et al.] // Security Onion Solutions : [website]. Augusta : Security Onion Solutions, 2016. URL: https://securityonionsolutions.com/ (viewed on October 16, 2018).

87. Security Onion – Intrusion Detection and Network Security Monitoring [Electronic resourse] // Security Onion : [website]. Brussels : BiASC, 2017. URL: https://honim.typepad.com/biasc/2017/12/security-onion-.html (viewed on October 16, 2018).

88. IntroductionToSecurityOnion [Electronic resourse] // Security Onion. San Francisco : GitHub Inc., 2018. URL: https://github.com/Security-Onion-Solutions/security-onion/wiki/IntroductionToSecurityOnion (viewed on Octiber 16, 2018).

89. CapMe [Electronic resourse] // Security Onion. San Francisco : GitHub Inc., 2018. URL: https://github.com/Security-Onion-Solutions/security-onion/wiki/CapMe (viewed on Octiber 16, 2018).

90. Squert [Electronic resourse] // Security Onion. San Francisco : GitHub Inc., 2018. URL: https://github.com/Security-Onion-Solutions/security-onion/wiki/Squert (viewed on Octiber 16, 2018).

91. ELSA [Electronic resourse] // Security Onion. San Francisco : GitHub Inc., 2018. URL: https://github.com/Security-Onion-Solutions/security-onion/wiki/ELSA (viewed on Octiber 16, 2018).

92. Intrusion Detection: Shadow Style-Step by Step Guide / Stephen Northcutt. Dahlgren : SANS Institute, 1998.

93. Build an IDS with Snort, Shadow, and ACID [Electronic resourse] / Mark Alexander Bain // Security. San Francisco : The Linux Foundation, 2005. URL: https://www.linux.com/news/build-ids-snort-shadow-and-acid (viewed on August 28, 2018).

94. About the Technical Reviewers [Electronic resourse] / Guy Bruneau [et al.] // Dertified Information Systems Security Professional : Training Guide. Indianapolis : Que Publishing, 2002. URL: https://books.google.com.ua/books?id=_n_fSGV-RQ0C&pg=PR23&lpg=PR23&dq=SHADOW+IDS&source=bl&ots=YToUgD4Ck7&sig=FaiNiC0yodIwB-N2MapMoEC5EuE&hl=ru&sa=X&ved=2ahUKEwjFreCI2eDfAhWQoBQKHbQ5C2sQ6AEwD3oECAgQAQ#v=onepage&q=SHADOW%20IDS&f=false (viewed on August 29, 2018).

95. Naval Surface Warfare Center SHADOW Arbitrary Code Execution Vulnerability [Electronic resourse] // Security Abvisories and Alerts : [website]. San Jose : Cisco Multivendor Vulnerability Alerts, 2002. URL: https://tools.cisco.com/security/center/viewAlert.x?alertId= 3711 (viewed on August 30, 2018).

96. Index of /downloads/ids/shadow-slack [Electronic resourse] // WhiteHats : [website]. Ottawa, 2012. URL: http://www.whitehats.ca/downloads/ids/shadow-slack/ (viewed on August 30, 2018).

97. Cisco IPS 4500 Series. Описание продукта Cisco IPS 4500 [Електронний ресурс] // Аппаратные межсетевые экраны : [сайт]. Київ : ТОВ Інфобезпека, 2018. URL: http://www.infobezpeka.com/

products/apatnye/Cisco_IPS_4500_Series/ (дата звернення: 11.09. 2018).

98. Cisco IPS Initialization, Inline, & Managed [Electronic resourse] / David Burns [et al.] // Intrusion Prevention System/IDS. Security Documents : [website]. San Jose : Cisco Press, 2011. URL: https://community.cisco.com/t5/security-documents/cisco-ips-initialization-inline-managed/ta-p/3127040 (viewed on September 12, 2018).

99. Cisco IOS Intrusion Prevention System (IPS) [Electronic resourse] // Security : [website]. San Jose : Cisco Systems Inc, 2008. URL: https://www.cisco.com/c/en/us/products/security/ios-intrusion-prevention-system-ips/index.html (viewed on September 12, 2018).

100. Cisco IDS/IPS. Безопасная настройка / Андрій Дугин // Системный администратор. М. : ООО Издательский дом «Положевец и партнеры», 2009. № 8 (81). URL: http://samag.ru/archive/article/2075 (дата обращения: 12.09.2018).

101. CCNP Security IPS 642-627 Official Cert Guide [Electronic resourse] / D. Burns, O. Adesina, K. Barker. San Jose : Cisco Press, 2011. 672 p. URL: http://www.ciscopress.com/store/ccnp-security-ips-642-627-official-cert-guide-9781587142550 (viewed on September 12, 2018).

102. Cisco Intrusion prevention system sensor CLI Configuration Guide for IPS 7.0 [Electronic resourse] // Configuration Guides. San Jose : Cisco Press, 2014. URL: https://www.cisco.com/c/en/us/td/docs/security/ips/7-0/configuration/guide/cli/cliguide7/cli_system_images.html.

103. Arbor Networks Spectrum [Электронный ресурс] // Технические данные системы Arbor. Burlignton : Arbor Networks Inc., 2016. 4 с. URL: http://netwell.net.ua/content/uploads/ds_spectrum_rus2016.pdf (дата обращения: 15.09.2018).

104. Arbor networks is 2017 award winner [Electronic resourse] / Kevin Whalen // News : [website]. Burlington : NetScout Systems Inc., 2017. URL: https://www.netscout.com/news/press-release/ddos-2017-award-winner (viewed on September 16, 2018).

105. Arbor DDoS Solutions [Electronic resourse] // DDoS & Network Visibility Solutions : [website]. Westford : NetScout Systems Inc., 2017. URL: https://www.netscout.com/arbor-ddos (viewed on September 16, 2018).

106. Arbor Networks Spectrum [Electronic resourse] // Data Sheet. Burlington : Arbor Networks Inc., 2017. URL: http://resources. arbornetworks.com/wp-content/uploads/DS_Spectrum_EN.pdf (viewed on September 16, 2018).

107. InfoWatch automation system advanced protector [Электронный ресурс] // Защита от атак на информационную инфраструктуру АСУ ТП. Москва : ГК InfoWatch, 2018. URL: http://m.infowatch.ru/ sites/default/files/products/asap/ InfoWatch_asap_Datasheet.pdf (дата обращения: 16.09.2018).

108. InfoWatch Automation System Advanced Protector [Электронный ресурс] // Обнаружение и предотвращение вторжений и аномалий технологических процессов. Москва : ГК InfoWatch, 2018. URL: https://www.infowatch.ru/products/asap (дата обращения: 17.09.2018).

109. InfoWatch ASAP [Электронный ресурс] // Для защиты АСУ ТП. СПб : AIM Systems, 2018. URL: https://www.aimsys.ru/ solutions/ actualasp (дата обращения: 17.09.2018).

110. Symantec DeepSight Threat Management System [Электронный ресурс] // Системы раннего оповещения : [website]. Cupertino : Symantec Corporation, 2003. URL: http://www.symantec. com/region/ru/earlyalert/images/RussianThreatManagementSys.pdf (дата обращения: 20.09.2018).

111. Online Threat Management Services [Electronic resourse] // Security : [website]. 2012. URL: https://thejimmahknows.com/online-threat-management-services/ (viewed on September 21, 2018).

112. Introduction to Symantec DeepSight Threat Management System 7.0 [Electronic resourse] // Technical Support : [website]. Cupertino : Symantec Corporation, 2003. URL:https://support.symantec. com/en_US/article.TECH112914.html (viewed on September 21, 2018).

113. Symantec DeepSight Threat Management System [Electronic resourse] // Data Sheet. Cupertino : Symantec Corporation, 2007. 3 p. URL: http://eval.symantec.com/mktginfo/enterprise/fact_sheets/ent-datasheet _symantec_deepsight_threat_management_system_09-2007. en-us.pdf (viewed on September 22, 2018).

114. IPS Software Blade contracts [Electronic resourse] // SecureKnowledge Details : [website]. San Carlos : Check Point Software Technologies Ltd., 2015. URL: https://supportcenter.checkpoint.com/ sup-

portcenter/portal?js_peid=P-14d3e69bf07-10000&eventSubmit_ doGoviewsolutiondetails&solutionid=sk44175 (viewed on September 23, 2018).

115. Check Point IPS Software Blade [Electronic resourse] // Datasheet. Tel Aviv-Yafo : Check Point Software Technologies Ltd., 2013. 2 p. URL: https://www.checkpoint.com/downloads/product-related/datasheets/ds-ips.pdf (viewed on September 24, 2018).

116. IPS Geo Protection drops the wrong traffic when it is configured as a whitelist [Electronic resourse] // SecureKnowledge Details : [website]. San Carlos : Check Point Software Technologies Ltd., 2016. URL: https://supportcenter.checkpoint.com/supportcenter/ portal?event Submit_doGoviewsolutiondetails=&solutionid=sk110683 (viewed on September 25, 2018).

117. Trend Micro TippingPoint [Электронный ресурс] // TAdviser – Государство. Бизнес. ИТ : [website]. Москва, 2017. URL: http:// www.tadviser.ru/index.php/Продукт:Trend_Micro_TippingPoint (дата обращения: 27.09.2018).

118. TippingPoint Threat Protection System [Electronic resourse] // Intrusion prevention : [website]. Irving : Trend Micro Incorporated, 2017. URL: https://www.trendmicro.com/en_hk/business/products/network/intrusion-prevention/tipping-point-threat-protection-system.html(viewed on September 27, 2018).

119. HP TippingPoint Next Generation Intrusion Prevention System [Electronic resourse] / Geert Busse. Vilvoorde : Westcon-Comstor, 2018. URL: http://be.westcon.com/content/vendors/hp-enterprise-security-solutions/hp-tippingpoint-ngips (viewed on September 27, 2018).

120. SANS – Intrusion Prevention with TippingPoint [Electronic resourse] / Dave Shackleford // SANS Analyst Program. Swansea : SANS Institute by Trend Micro, 2015. URL: https://www.trendmicro.com/ content/dam/trendmicro/global/en/business/products/network/integrated -atp/SANS_TrendMicroTippingPoint2600NX.pdf (viewed on September 27, 2018).

121. Darktrace vs. Trend Micro TippingPoint NGIPS [Electronic resourse] // Intrusion Detecting and Prevention Software. New York : IT Central Station, 2018. URL: https://www.itcentralstation.com/ products/ comparisons/darktrace_vs_trend-micro-tippingpoint-ngips (viewed on September 27, 2018).

122. Система invGUARD AS [Электронный ресурс] // Средства централизованного управление и др. : [сайт]. М. : Axoft, 2017. URL: https://axoft.ru/vendors/inoventika-tehnolodjes/sistema-invGUARD-AS/ (дата обращения: 01.10.2018).

123. Система защиты от сетевых атак invGuard [Электронный ресурс] // 9th Annual Worldwide Infrastructure Security Report. M. : Inoventica Technologies, 2014. 36 p. URL: https://www.runnet.ru/ docs/crimea2015/crimea-innoventica-invguard2015.pdf (viewed on October 1, 2018).

124. Система invGUARD AS [Электронный ресурс] // Отчет. М. : Inoventica Technologies, 2014. 10 p. URL: http://www.inoventica-tech.ru/doc_reestr/Описание применения ПК invGuard AS-SW.pdf (дата обращения: 01.10.2018).

125. DefensePro DDoS Defense & DDoS Prevention Device [Electronic resourse] / Chris Rodriguez // DefensePro : [website]. Mahwah : Radware, 2018. URL: https://www.radware.com/products/ defensepro/ (viewed on October 3, 2018).

126. Radware Defense Pro [Электронный ресурс] // Аппаратные межсетевые экраны : [сайт]. Київ : ТОВ Інфобезпека, 2018. URL: http://www.infobezpeka.com/products/apatnye/?view=395 (Дата звернення : 03.10.2018).

127. Radware DefensePro Series [Electronic resourse] // RadAppliances.com : [website]. Irvine : Virtual Graffiti Inc, 2014. URL: https:// www.radappliances.com/DefensePro.asp (viewed on October 3, 2018).

128. Radware DefensePro [Electronic resourse] // DefensePro Tech Specs. Tel Aviv : Radware, 2018. 3 p.

129. Kaspersky Anti Targeted Attack (KATA) Platform // Kaspersky Lab : [сайт]. М. : АО Лаборатория Касперского, 2017. URL: http:// webcache.googleusercontent.com/search?q=cache:DUbVaOAeaBEJ: https://support.kaspersky.ru/13882&hl=en&gl=ua&strip=1& vwsrc=0 (дата обращения: 07.10.2018).

130. Передовая платформа для защиты от целевых атак и сложных угроз [Электронный ресурс] // Kaspersky Anti Targeted Attack Platform : [сайт]. Минск : Газета Правда, 2017. URL: https://squalio.com/by-ru/programmnoe-obespechenie/kaspersky-anti-targeted-attack-platform/ (дата обращения: 07.10.2018).

131. Большая картина. [Электронный ресурс] / Е. Касперский. М. : LiveJournal, 2016. URL: https://e-kaspersky.livejournal.com/ 297341. html (дата обращения: 07.10.2018).

132. Kaspersky Anti Targeted Attack Platform [Электронный ресурс] // Kaspersky Lab. M. : АО Лаборатория Касперского, 2016. С. 1-12. URL: https://www.all-smety.ru/upload/KATA%20-%20 Kaspersky_Anti_Targeted%20_Attack_Platform_WhitePaper_RU.PDF (дата обращения: 07.10.2018).

133. Корченко А.О. Моделі аномального стану для систем виявлення кібератак в комп'ютерних мережах: Автореф. дис. канд. техн. наук. – К., 2013. – 20 с.

РОЗДІЛ 2. МЕТОДИ ФОРМУВАННЯ ЕТАЛОННОГО СЕРЕДОВИЩА ДЛЯ ІДЕНТИФІКАЦІЇ АНОМАЛЬНИХ СТАНІВ

2.1. Кортежна модель формування атакуючих середовищ

В останні роки відбувається значне збільшення обсягів інформації, що накопичується, зберігається та обробляється за допомогою ІС. При цьому концентрація в єдиних базах даних інформації різного призначення і належності, а також різке розширення кола користувачів, що мають безпосередній доступ до РІС, породжують проблему забезпечення їх захисту від різного роду вторгнень. Зростання складності апаратно-програмних засобів та існуючі недоліки сучасних інформаційних технологій пов'язані з удосконаленням та виникненням нових кібератак на РІС.

Слід зазначити, що несанкціоновані дії щодо РІС впливають і на середовище оточення, породжуючи в ньому, як наслідок, певні аномалії. Таке середовище зазвичай складноформалізоване, нечітко визначене і для вирішення завдань виявлення кібератак, що породили аномалії в цьому середовищі необхідні відповідні засоби, які дають можливість виявити вторгнення за множиною різних характерних ознак.

Один з підходів до вирішення такого роду завдань ґрунтується на використанні відповідних моделей, методів і систем виявлення вторгнень, які базуються на нечітких множинах, орієнтованих на обробку слабкоструктурованих даних з метою встановлення фактів несанкціонованого доступу до РІС, наприклад, через комп'ютерні мережі.

Здійснимо формалізацію підходу до формування набору базових компонент, за допомогою якого можна ефективно виявити в слабоформалізованому нечітко визначеному середовищі аномальний стан за заданий часовий проміжок.

Для цього введемо наступну термінологію:

- аномальний стан – стан поточного середовища, що характерний дії визначеного типу кібератак;
- атакуюче середовище – можлива множина кібератак ($\mathbf{CA}^{\tau_i}$), які можуть впливати на РІС за певний часовий проміжок;

- m-вимірне гетерогенне (узагальнювальне) параметричне середовище – це необхідна множина з m-параметрів ($\mathbf{P}$), що використовується для виявлення заданої множини кібератак, наприклад, для виявлення **SN**, **DS**, **SP** атаки необхідне 6-ти вимірне параметричне середовище $\mathbf{P} = \{ \bigcup_{j=1}^{6} P_j \} = \{ P_1, ..., P_6 \};$
- m_i-вимірне параметричне підсередовище – необхідна підмножина з m_i-параметрів ($\mathbf{P_i}$), які використовуються для виявлення i-ї (заданої) кібератаки;
- еталонне середовище – необхідна множина еталонів параметрів ($\mathbf{T^e}$), за допомогою яких здійснюється виявлення заданої множини кібератак ($\mathbf{CA^{\tau_f}}$);
- m_i-еталонне підсередовище – необхідна підмножина еталонів параметрів ($\mathbf{T_i^e}$), за допомогою яких здійснюється виявлення i-ї (заданої) кібератаки $\mathbf{CA_i^{\tau_f}}$;
- поточне середовище – необхідна множина поточних значень параметрів ($\mathbf{P^{\tau_f}}$), які використовуються для виявлення заданої множини кібератак ($\mathbf{CA^{\tau_f}}$);
- m_i-поточне підсередовище – необхідна підмножина поточних значень параметрів ($\mathbf{P_i^{\tau_f}}$), які використовуються для виявлення i-ї (заданої) кібератаки ($\mathbf{CA_i^{\tau_f}}$);
- детекційне середовище – необхідна множина детекційних правил (**DR**), які використовуються для виявлення заданої множини кібератак ($\mathbf{CA^{\tau_f}}$);
- i-те детекційне підсередовище – необхідна підмножина детекційних правил ($\mathbf{DR_i}$), що використовується для виявлення i-ї (заданої) кібератаки ($\mathbf{CA_i^{\tau_f}}$);
- слабоформалізоване нечітко визначене середовище – середовище яке характеризується великим ступенем невизначеності, випадковості, нестабільності, впливом різноманітних змін в часі та ін., а для формалізації її процесів використовується математичний апарат теорії нечітких множин.

Далі пропонується математична модель формування величин (або базова кортежна модель) [1], основу якої складає кортеж, що містить ідентифікатор (ІД) кібератаки та підмножини:

- можливих параметрів;
- можливих нечітких (лінгвістичних) еталонів;
- поточних значень нечітких параметрів;
- базових детекційних правил.

Для формалізації процесу формування зазначених компонент введемо множину можливих кібератак **CA** утворюючих атакуюче середовище ($\mathbf{CA}^{\tau_f}$), які можуть діяти на РІС за визначений часовий проміжок τ_h з можливістю їх виявлення в момент часу τ_f ($f = \overline{1,max_\tau}$, де max_τ – максимальний номер часового проміжку f) тобто:

$$\mathbf{CA}^{\tau_f} = \{\bigcup_{i=1}^{n} \mathbf{CA}_i^{\tau_f}\} = \{\mathbf{CA}_1^{\tau_f}, \mathbf{CA}_2^{\tau_f}, \ldots, \mathbf{CA}_n^{\tau_f}\} \quad (i = \overline{1,n}), \tag{2.1}$$

де n визначає кількість можливих кібератак, кожна з яких відображається узагальнювальним кортежем, елементи якого утворюють i-е атакуюче підсередовище

$$\mathbf{CA}_i^{\tau_f} = < CA_i, \mathbf{P}_i, \mathbf{T}_i^e, \mathbf{P}_i^{\tau_f}, \mathbf{DR}_i >, \tag{2.2}$$

в якому:

- CA_i – ІД i-ї кібератаки;
- $\mathbf{P}_i$ – підмножина можливих параметрів, утворюючих m_i-вимірне параметричне підсередовище, що використовується для виявлення i-ї кібератаки;
- $\mathbf{T}_i^e$ – підмножини можливих нечітких (лінгвістичних) еталонів, утворюючих m_i-вимірне еталонне підсередовище, що відображає характерні судження експерта відносно аномальності стану відповідних параметрів із підмножини $\mathbf{P}_i$ в m_i-вимірному параметричному підсередовищі;

- $\mathbf{P_i^{\tau_f}}$ – підмножина поточних значень нечітких параметрів утворюючих m_i-вимірне параметричне підсередовище, яке формується на основі $\mathbf{T_i^e}$ в момент часу τ_f ($f = \overline{1, max_\tau}$) за часовий проміжок $\tau_h = \tau_f - \tau_{f-1}$;
- $\mathbf{DR_i}$ – підмножина базових детекційних правил, утворюючих *i*-е детекційне підсередовище, що необхідне для виявлення *i*-ї кібератаки.

Зазначимо, що у сукупності всі елементи підмножини $\mathbf{CA^{\tau_f}}$ визначають атакуюче середовище на PIC, стан якої фіксується часовим проміжком τ_f. Розглянемо підходи до формування кожного із компонентів кортежу (2.2).

Формування CA_i.

Ідентифікатори CA_i визначимо на основі того, що кожний елемент множини $\mathbf{CA^{\tau_f}}$ зв'язаний із визначеною кібератакою, яку ідентифікують за відповідним ім'ям.

Наприклад, при $n = 5$ формулу (2.1) можна визначити як:

$$\begin{gathered}\mathbf{CA^{\tau_f}} = \{\bigcup_{i=1}^{5} \mathbf{CA_i^{\tau_f}}\} = \\ \{\mathbf{CA_1^{\tau_f}}, \mathbf{CA_2^{\tau_f}}, \mathbf{CA_3^{\tau_f}}, \mathbf{CA_4^{\tau_f}}, \mathbf{CA_5^{\tau_f}}\} = \\ \{\mathbf{CA_{SNF}^{\tau_f}}, \mathbf{CA_{DS}^{\tau_f}}, \mathbf{CA_{SP}^{\tau_f}}, \mathbf{CA_{ESP}^{\tau_f}}, \mathbf{CA_{SN}^{\tau_f}}\} = \\ \{\mathbf{SNF^{\tau_f}}, \mathbf{DS^{\tau_f}}, \mathbf{SP^{\tau_f}}, \mathbf{ESP^{\tau_f}}, \mathbf{SN^{\tau_f}}\},\end{gathered} \tag{2.3}$$

де $\mathbf{CA_1^{\tau_f}} = \mathbf{CA_{SNF}^{\tau_f}} = \mathbf{SNF^{\tau_f}}$, $\mathbf{CA_2^{\tau_f}} = \mathbf{CA_{DS}^{\tau_f}} = \mathbf{DS^{\tau_f}}$, $\mathbf{CA_3^{\tau_f}} = \mathbf{CA_{SP}^{\tau_f}} = \mathbf{SP^{\tau_f}}$, $\mathbf{CA_4^{\tau_f}} = \mathbf{CA_{ESP}^{\tau_f}} = \mathbf{ESP^{\tau_f}}$ та $\mathbf{CA_5^{\tau_f}} = \mathbf{CA_{SN}^{\tau_f}} = \mathbf{SN^{\tau_f}}$ відображають стан атакуючого середовища ($\mathbf{CA^{\tau_f}}$) (SNF-DS-SP-ESP-SN-середовища) в момент τ_f та відповідно визначають кібератаки з іменами:

- «Сніффінг (Sniffing (SNF))»,
- «Відмова в обслуговуванні (Denial of service (DS))»,
- «Спуфінг (Spoofing (SP))»,
- «Email-Спуфінг (Email-spoofing (ESP))»,

- «Сканування портів (Scanning of ports (SN))»,

яким відповідно будуть присвоєні ІД:

- $CA_1 = CA_{SNF} = SNF$,
- $CA_2 = CA_{DS} = DS$,
- $CA_3 = CA_{SP} = SP$,
- $CA_4 = CA_{ESP} = ESP$,
- $CA_5 = CA_{SN} = SN$.

Формування $\mathbf{P_i}$.

Побудова підмножини $\mathbf{P_i}$ здійснюється на основі множини всіх можливих параметрів $\mathbf{P}$, що відображаються як:

$$\mathbf{P} = \{\bigcup_{j=1}^{m} P_j\} = \{P_1,\ P_2,\ ...,\ P_m\}, \quad (j = \overline{1,m}), \tag{2.4}$$

характеризують стан оточуючого середовища, за значеннями яких можна виявити аномальний стан, породжений впливом певних кібератак, тобто елементів з множини $\mathbf{CA}^{\tau_f}$.

Враховуючи, що множина $\mathbf{P}$ містить різнорідні за своєю природою параметри, що характеризують різні стани оточуючого середовища, то сукупність усіх членів цієї множини визначимо як *m*-вимірне (або загальне) гетерогенне параметричне середовище ($\mathbf{P}$).

Наприклад, *12*-вимірне гетерогенне параметричне середовище (тобто $m = 12$) за допомогою множини (2.4) можна представити у такому вигляді:

$$\begin{gathered}\mathbf{P} = \{\bigcup_{j=1}^{12} P_j\} = \\ \{P_1,\ P_2,\ P_3,\ P_4,\ P_5,\ P_6,\ P_7,\ P_8,\ P_9,\ P_{10},\ P_{11},\ P_{12}\} = \\ \{P_{КВП},\ P_{СОП},\ P_{ТП},\ P_{КОП},\ P_{СОЗ},\ P_{ЗМЗ},\ P_{КПОА}, \\ P_{КСБ},\ P_{КСТ},\ P_{КСС},\ P_{КВК},\ P_{ВВК}\} = \\ \{КВП,\ СОП,\ ТП,\ КОП,\ СОЗ,\ ЗМЗ,\ КПОА, \\ КСБ,\ КСТ,\ КСС,\ КВК,\ ВВК\},\end{gathered} \tag{2.5}$$

де:

- $P_1 = P_{КВП} = КВП,$
- $P_2 = P_{СОП} = СОП,$
- $P_3 = P_{ТП} = ТП,$
- $P_4 = P_{КОП} = КОП,$
- $P_5 = P_{СОЗ} = СОЗ,$
- $P_6 = P_{ЗМЗ} = ЗМЗ,$
- $P_7 = P_{КПОА} = КПОА,$
- $P_8 = P_{КСБ} = КСБ,$
- $P_9 = P_{КСТ} = КСТ,$
- $P_{10} = P_{КСС} = КСС,$
- $P_{11} = P_{КВК} = КВК,$
- $P_{12} = P_{ВВК} = ВВК$

відповідно є ІД параметрів, як-от:

- «Кількість вхідних пакетів в мережі» або «Количество входных пакетов в сети (КВП)» (при $j = 1$);
- «Швидкість обробки пакетів на стороні одержувача» або «Скорость обработки пакетов на стороне получателя (СОП)» (при $j = 2$);
- «Таймінг пакетів в каналі» або «Тайминг пакетов в канале (ТП)» (при $j = 3$);
- «Кількість одночасних підключень до серверу» або «Количество одновременных подключений к серверу (КОП)» (при $j = 4$);
- «Швидкість обробки запитів від клієнтів» або «Скорость обработки запросов от клиентов (СОЗ)» (при $j = 5$);
- «Затримка між запитами від одного користувача» або «Задержка между запросами от одного пользователя (ЗМЗ)» (при $j = 6$);
- Кількість пакетів з однаковою адресою відправника та одержувача» або «Количество пакетов с одинаковым адресом отправителя и получателя (КПОА)» (при $j = 7$);

- «Кількість виявлених IP-адрес у спам базах» або «Количество выявленных IP-адресов в спам базах (КСБ)» (при $j = 8$);
- «Кількість спам слів у темі» або «Количество спам слов в теме (КСТ)» (при $j = 9$);
- «Кількість спам слів у повідомленні» або «Количество спам слов в сообщении (КСС)», (при $j = 10$);
- «Кількість віртуальних каналів» або «Количество виртуальных каналов (КВК)» (при $j = 11$);
- «Вік віртуального каналу» або «Возраст виртуального канала (ВВК)» (при $j = 12$).

Далі сформуємо підмножини параметрів

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{P_i}\} = \{\mathbf{P_1}, \mathbf{P_2}, \ldots, \mathbf{P_n}\}, \tag{2.6}$$

де $\mathbf{P_i} \subseteq \mathbf{P}$, $(i = \overline{1,n})$ визначимо як:

$$\mathbf{P_i} = \{\bigcup_{j=1}^{m_i} P_{ij}\} = \{P_{i1}, P_{i2}, \ldots, P_{im_i}\}, \tag{2.7}$$

при цьому m_i означає кількість параметрів у (2.8), за допомогою яких здійснюється виявлення аномального стану, породженого кібератакою з ІД CA_i.

Таким чином, (2.6) з урахуванням (2.7) представимо в наступному вигляді:

$$\begin{gathered}\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{P_i}\} = \{\bigcup_{i=1}^{n} \{\bigcup_{j=1}^{m_i} P_{ij}\}\} = \\ \{\{P_{11}, P_{12}, \ldots, P_{1m_1}\}, \\ \{P_{21}, P_{22}, \ldots, P_{2m_2}\}, \\ \ldots, \\ \{P_{n1}, P_{n2}, \ldots, P_{nm_n}\}\}.\end{gathered} \tag{2.8}$$

Фактично, конкретні значення членів підмножини $\mathbf{P_i}$ визначають m_i-вимірне параметричне підсередовище ($\mathbf{P_i}$), що використовується для виявлення кібератаки з ІД CA_i або CA_i-атаки.

Наприклад, якщо $n=5,\ m_1=m_2=m_4=3$ та $m_3=m_5=2$ з урахуванням (2.3) та (2.5) визначимо необхідні параметри для виявлення відповідних кібератак, тобто

$$P_{11}=P_1,\ P_{12}=P_2,\ P_{13}=P_3,$$
$$P_{21}=P_4,\ P_{22}=P_5,\ P_{23}=P_6,$$
$$P_{31}=P_4,\ P_{32}=P_7,$$
$$P_{41}=P_8,\ P_{42}=P_9,\ P_{43}=P_{10}\ \text{та}$$
$$P_{51}=P_{11},\ P_{52}=P_{12}.$$

Тоді, вираз (2.8) з урахуванням (2.5) буде мати наступний вигляд:

$$\begin{gathered}\{\bigcup_{\mathbf{i=1}}^{\mathbf{5}}\mathbf{P_i}\}=\{\bigcup_{i=1}^{5}\{\bigcup_{j=1}^{m_i}P_{ij}\}\}=\\ \{\{P_{11},\ P_{12},\ P_{13}\},\ \{P_{21},\ P_{22},\ P_{23}\},\ \{P_{31},\ P_{32}\},\\ \{P_{41},\ P_{42},\ P_{43}\},\ \{P_{51},\ P_{52}\}\}=\\ \{\{P_{SNFKBП},\ P_{SNFCOП},\ P_{SNFTП}\},\\ \{P_{DSKOП},\ P_{DSCO3},\ P_{DS3M3}\},\ \{P_{SPKOП},\ P_{SPKПOA}\},\\ \{P_{ESPKCБ},\ P_{ESPKCT},\ P_{ESPKCC}\},\ \{P_{SNKBK},\ P_{SNBBK}\}\}=\\ \{\{КВП,\ СОП,\ ТП\},\\ \{КОП,\ СО3,\ 3М3\},\ \{КОП,\ КПОА\},\\ \{КСБ,\ КСТ,\ КСС\},\ \{КВК,\ ВВК\}\},\end{gathered}\qquad(2.9)$$

де:

- $P_{11}=P_{SNFKBП}=КВП,\ P_{12}=P_{SNFCOП}=СОП$ та $P_{13}=P_{SNFTП}=ТП$ є параметрами, які визначають *3*-вимірне параметричне підсередовище ($\mathbf{P_i=P_1=P_{SNF}}$ – КВП-СОП-ТП-підсередовище) і відповідно відображають «КВП», «СОП» та «ТС», за допомогою яких виявляється кібератака з ІД CA_{SNF} або *SNF*-атаки;
- $P_{21}=P_{DSKOП}=КОП,\ \ P_{22}=P_{DSCO3}=СО3$ та $P_{23}=P_{DS3M3}=3М3$ є параметрами, які визначають *3*-вимірне параметричне підсередовище ($\mathbf{P_i=P_2=P_{DS}}$ – КОП-СОЗ-ЗМЗ-підсередовище) і відповідно відображають «КОП», «СОЗ» та «ЗМЗ», за допомогою яких виявляється кібератака з ІД CA_{DS} або *DS*-атаки;

- $P_{31} = P_{SPKOP} = KOP$ та $P_{32} = P_{SPKPOA} = KPOA$ є параметрами, що визначають *2*-вимірне параметричне підсередовище ($\mathbf{P_i} = \mathbf{P_3} = \mathbf{P_{SP}}$ – КОП-КПОА-підсередовище) і відповідно відображають «КОП» та «КПОА», за допомогою яких здійснюється виявлення кібератаки з ІД CA_{SP} або *SP*-атаки;
- $P_{41} = P_{ESPKCB} = KCB$, $P_{42} = P_{ESPKCT} = KCT$ та $P_{43} = P_{ESPKCC} = KCC$ є параметрами, які визначають *3*-вимірне параметричне підсередовище ($\mathbf{P_i} = \mathbf{P_4} = \mathbf{P_{ESP}}$ – КСБ-КСТ-КСС-підсередовище) і відповідно відображають «КСБ», «КСТ» та «КСС», за допомогою яких виявляється кібератака з ІД CA_{ESP} або *ESP*-атаки;
- $P_{51} = P_{SNKBK} = KBK$ та $P_{52} = P_{SNBBK} = BBK$ є параметрами, що визначають *2*-вимірне параметричне підсередовище ($\mathbf{P_i} = \mathbf{P_5} = \mathbf{P_{SN}}$ – КВК-ВВК-підсередовище) і відповідно відображають «КВК» та «ВВК», за допомогою яких здійснюється виявлення кібератаки з ІД CA_{SN} або *SP*-атаки.

Формування $\mathbf{T_i^e}$.

Побудова підмножин можливих нечітких (лінгвістичних) еталонів $\mathbf{T_i^e}$ здійснюється на основі множини всіх можливих еталонів $\mathbf{T^e}$, що відображають характерні стани відповідних параметрів з $\mathbf{P_i}$ в заданому середовищі оточення, тобто:

$$\{\bigcup_{i=1}^{n} \mathbf{T_i^e}\} = \{\mathbf{T_1^e}, \mathbf{T_2^e}, \ldots, \mathbf{T_n^e}\}, \tag{2.10}$$

де $\mathbf{T_i^e} \subseteq \mathbf{T^e}$, $(i = \overline{1,n})$, а

$$\mathbf{T_i^e} = \{\bigcup_{j=1}^{m_i} \mathbf{T_{ij}^e}\} = \{\mathbf{T_{i1}^e}, \mathbf{T_{i2}^e}, \ldots, \mathbf{T_{im_i}^e}\}, \tag{2.11}$$

при цьому $\mathbf{T_{ij}^e}$ $(j = \overline{1,m_i})$ – підмножина лінгвістичних еталонів, яка відображає характерні судження експерта відносно аномальності стану параметра P_{ij}.

З урахуванням (2.11) формулу (2.10) запишемо в наступному вигляді:

$$\{\bigcup_{i=1}^{n}\mathbf{T}_i^e\}=\{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\mathbf{T}_{ij}^e\}\}=$$
$$\{\{\mathbf{T}_{11}^e,\ \mathbf{T}_{12}^e,\ \ldots,\ \mathbf{T}_{1m_1}^e\},$$
$$\{\mathbf{T}_{21}^e,\ \mathbf{T}_{22}^e,\ \ldots,\ \mathbf{T}_{2m_2}^e\},\qquad(2.12)$$
$$\ldots,$$
$$\{\mathbf{T}_{n1}^e,\ \mathbf{T}_{n2}^e,\ \ldots,\ \mathbf{T}_{nm_n}^e\}\},$$
$$(\ j=\overline{1,m_i}\ ).$$

Підмножину $\mathbf{T}_{ij}^e \subseteq \mathbf{T}_i^e$ визначимо як:

$$\mathbf{T}_{ij}^e=\{\bigcup_{s=1}^{r_j}\underset{\sim}{T}_{ijs}^e\}=\{\underset{\sim}{T}_{ij1}^e,\ \underset{\sim}{T}_{ij2}^e,\ \ldots,\ \underset{\sim}{T}_{ijr_j}^e\},\qquad(2.13)$$

де $\underset{\sim}{T}_{ijs}^e$ $(s=\overline{1,r_j})$ – еталонні нечіткі числа, а r_j – кількість членів в $\mathbf{T}_{ij}^e$.

Тоді, формула (2.12) з урахуванням (2.13) приймає наступний вигляд:

$$\{\bigcup_{i=1}^{n}\mathbf{T}_i^e\}=\{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\mathbf{T}_{ij}^e\}\}=\{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\{\bigcup_{s=1}^{r_j}\underset{\sim}{T}_{ijs}^e\}\}\}=$$
$$\{\{\{\underset{\sim}{T}_{111}^e,\ \underset{\sim}{T}_{112}^e,\ \ldots,\ \underset{\sim}{T}_{11r_1}^e\},$$
$$\{\underset{\sim}{T}_{121}^e,\ \underset{\sim}{T}_{122}^e,\ \ldots,\ \underset{\sim}{T}_{12r_2}^e\},\ \ldots,$$
$$\{\underset{\sim}{T}_{1m_1 1}^e,\ \underset{\sim}{T}_{1m_1 2}^e,\ \ldots,\ \underset{\sim}{T}_{1m_1 r_{m_1}}^e\}\},$$
$$\{\{\underset{\sim}{T}_{211}^e,\ \underset{\sim}{T}_{212}^e,\ \ldots,\ \underset{\sim}{T}_{21r_1}^e\},\qquad(2.14)$$
$$\{\underset{\sim}{T}_{221}^e,\ \underset{\sim}{T}_{222}^e,\ \ldots,\ \underset{\sim}{T}_{22r_2}^e\},\ \ldots,$$
$$\{\underset{\sim}{T}_{2m_2 1}^e,\ \underset{\sim}{T}_{2m_2 2}^e,\ \ldots,\ \underset{\sim}{T}_{2m_2 r_{m_2}}^e\}\},$$
$$\ldots,$$
$$\{\{\underset{\sim}{T}_{n11}^e,\ \underset{\sim}{T}_{n12}^e,\ \ldots,\ \underset{\sim}{T}_{n1r_1}^e\},$$
$$\{\underset{\sim}{T}_{n21}^e,\ \underset{\sim}{T}_{n22}^e,\ \ldots,\ \underset{\sim}{T}_{n2r_2}^e\},\ \ldots,$$
$$\{\underset{\sim}{T}_{nm_n 1}^e,\ \underset{\sim}{T}_{nm_n 2}^e,\ \ldots,\ \underset{\sim}{T}_{nm_n r_{m_n}}^e\}\}\}.$$

Необхідно зазначити, що сукупність визначених величин всіх членів підмножини $\mathbf{T}_{\mathbf{i}}^{\mathbf{e}}$ (по аналогії з параметричним підсередовищем ($\mathbf{P}_{\mathbf{i}}$)) складають еталонне підсередовище ($\mathbf{T}_{\mathbf{i}}^{\mathbf{e}}$), орієнтоване на виявлення кібератаки з ІД CA_i або CA_i-атаки.

Наприклад, якщо $n=5$ ($\mathbf{CA}_{\mathbf{1}}^{\boldsymbol{\tau}_{\mathbf{f}}}=\mathbf{CA}_{\mathbf{SNF}}^{\boldsymbol{\tau}_{\mathbf{f}}}=\mathbf{SNF}^{\boldsymbol{\tau}_{\mathbf{f}}}$ $(m_1=3,\ r_1=5,\ r_2=3,\ r_3=4)$, $\mathbf{CA}_{\mathbf{2}}^{\boldsymbol{\tau}_{\mathbf{f}}}=\mathbf{CA}_{\mathbf{DS}}^{\boldsymbol{\tau}_{\mathbf{f}}}=\mathbf{DS}^{\boldsymbol{\tau}_{\mathbf{f}}}$ $(m_2=3,\ r_1=5,\ r_2=r_3=3)$, $\mathbf{CA}_{\mathbf{3}}^{\boldsymbol{\tau}_{\mathbf{f}}}=\mathbf{CA}_{\mathbf{SP}}^{\boldsymbol{\tau}_{\mathbf{f}}}=\mathbf{SP}^{\boldsymbol{\tau}_{\mathbf{f}}}$ $(m_3=2,\ r_1=5,\ r_2=3)$, $\mathbf{CA}_{\mathbf{4}}^{\boldsymbol{\tau}_{\mathbf{f}}}=\mathbf{CA}_{\mathbf{ESP}}^{\boldsymbol{\tau}_{\mathbf{f}}}=\mathbf{ESP}^{\boldsymbol{\tau}_{\mathbf{f}}}$ $(m_4=3,\ r_1=4,\ r_2=r_3=3)$ та $\mathbf{CA}_{\mathbf{5}}^{\boldsymbol{\tau}_{\mathbf{f}}}=\mathbf{CA}_{\mathbf{SN}}^{\boldsymbol{\tau}_{\mathbf{f}}}=\mathbf{SN}^{\boldsymbol{\tau}_{\mathbf{f}}}$ $(m_5=2,\ r_1=5,\ r_2=3)$) та з урахування [2-4] вираз (2.14) можна визначити як:

$$\begin{gathered}
\{\bigcup_{\mathbf{i=1}}^{\mathbf{5}}\mathbf{T}_{\mathbf{i}}^{\mathbf{e}}\}=\{\bigcup_{\mathbf{i=1}}^{\mathbf{5}}\{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}}\mathbf{T}_{\mathbf{ij}}^{\mathbf{e}}\}\}=\{\bigcup_{i=1}^{5}\{\bigcup_{j=1}^{m_i}\{\bigcup_{s=1}^{r_j}\underset{\sim}{T}_{jis}^{e}\}\}\}= \\
\{\{\{\underset{\sim}{T}_{111}^{e},\ \underset{\sim}{T}_{112}^{e},\ \underset{\sim}{T}_{113}^{e},\ \underset{\sim}{T}_{114}^{e},\ \underset{\sim}{T}_{11r_1}^{e}\},\{\underset{\sim}{T}_{121}^{e},\ \underset{\sim}{T}_{122}^{e},\ \underset{\sim}{T}_{12r_2}^{e}\}, \\
\{\underset{\sim}{T}_{1m_11}^{e},\ \underset{\sim}{T}_{1m_12}^{e},\ \underset{\sim}{T}_{1m_13}^{e},\ \underset{\sim}{T}_{1m_1r_3}^{e}\}\}, \\
\{\{\underset{\sim}{T}_{211}^{e},\ \underset{\sim}{T}_{212}^{e},\ \underset{\sim}{T}_{213}^{e},\ \underset{\sim}{T}_{214}^{e},\ \underset{\sim}{T}_{21r_1}^{e}\},\{\underset{\sim}{T}_{221}^{e},\ \underset{\sim}{T}_{222}^{e},\ \underset{\sim}{T}_{22r_2}^{e}\}, \\
\{\underset{\sim}{T}_{2m_21}^{e},\ \underset{\sim}{T}_{2m_22}^{e},\ \underset{\sim}{T}_{2m_2r_3}^{e}\}\}, \\
\{\{\underset{\sim}{T}_{311}^{e},\ \underset{\sim}{T}_{312}^{e},\ \underset{\sim}{T}_{313}^{e},\ \underset{\sim}{T}_{314}^{e},\ \underset{\sim}{T}_{31r_1}^{e}\},\{\underset{\sim}{T}_{3m_31}^{e},\ \underset{\sim}{T}_{3m_32}^{e},\ \underset{\sim}{T}_{3m_3r_2}^{e}\}\}, \\
\{\{\underset{\sim}{T}_{411}^{e},\ \underset{\sim}{T}_{412}^{e},\ \underset{\sim}{T}_{413}^{e},\ \underset{\sim}{T}_{41r_1}^{e}\},\{\underset{\sim}{T}_{421}^{e},\ \underset{\sim}{T}_{422}^{e},\ \underset{\sim}{T}_{42r_2}^{e}\}, \\
\{\underset{\sim}{T}_{4m_41}^{e},\ \underset{\sim}{T}_{4m_42}^{e},\ \underset{\sim}{T}_{4m_4r_3}^{e}\}\}, \\
\{\{\underset{\sim}{T}_{511}^{e},\ \underset{\sim}{T}_{512}^{e},\ \underset{\sim}{T}_{513}^{e},\ \underset{\sim}{T}_{514}^{e},\ \underset{\sim}{T}_{51r_1}^{e}\},\{\underset{\sim}{T}_{5m_51}^{e},\ \underset{\sim}{T}_{5m_52}^{e},\ \underset{\sim}{T}_{5m_5r_2}^{e}\}\}= \\
\{\{\{\underset{\sim}{T}_{111}^{e},\ \underset{\sim}{T}_{112}^{e},\ \underset{\sim}{T}_{113}^{e},\ \underset{\sim}{T}_{114}^{e},\ \underset{\sim}{T}_{115}^{e}\},\{\underset{\sim}{T}_{121}^{e},\ \underset{\sim}{T}_{122}^{e},\ \underset{\sim}{T}_{123}^{e}\}\}, \\
\{\underset{\sim}{T}_{131}^{e},\ \underset{\sim}{T}_{132}^{e},\ \underset{\sim}{T}_{133}^{e},\ \underset{\sim}{T}_{134}^{e}\}\}, \\
\{\{\underset{\sim}{T}_{211}^{e},\ \underset{\sim}{T}_{212}^{e},\ \underset{\sim}{T}_{213}^{e},\ \underset{\sim}{T}_{214}^{e},\ \underset{\sim}{T}_{215}^{e}\},\{\underset{\sim}{T}_{221}^{e},\ \underset{\sim}{T}_{222}^{e},\ \underset{\sim}{T}_{223}^{e}\}, \\
\{\underset{\sim}{T}_{231}^{e},\ \underset{\sim}{T}_{232}^{e},\ \underset{\sim}{T}_{233}^{e}\}\}, \\
\{\{\underset{\sim}{T}_{311}^{e},\ \underset{\sim}{T}_{312}^{e},\ \underset{\sim}{T}_{313}^{e},\ \underset{\sim}{T}_{314}^{e},\ \underset{\sim}{T}_{315}^{e}\},\{\underset{\sim}{T}_{321}^{e},\ \underset{\sim}{T}_{322}^{e},\ \underset{\sim}{T}_{323}^{e}\}\}, \\
\{\{\underset{\sim}{T}_{411}^{e},\ \underset{\sim}{T}_{412}^{e},\ \underset{\sim}{T}_{413}^{e},\ \underset{\sim}{T}_{414}^{e}\},\{\underset{\sim}{T}_{421}^{e},\ \underset{\sim}{T}_{422}^{e},\ \underset{\sim}{T}_{423}^{e}\}, \\
\{\underset{\sim}{T}_{431}^{e},\ \underset{\sim}{T}_{432}^{e},\ \underset{\sim}{T}_{433}^{e}\}\}, \\
\{\{\underset{\sim}{T}_{511}^{e},\ \underset{\sim}{T}_{512}^{e},\ \underset{\sim}{T}_{613}^{e},\ \underset{\sim}{T}_{514}^{e},\ \underset{\sim}{T}_{615}^{e}\},\{\underset{\sim}{T}_{521}^{e},\ \underset{\sim}{T}_{522}^{e},\ \underset{\sim}{T}_{623}^{e}\}\}\}=
\end{gathered} \tag{2.15}$$

$$\{\{\{\underset{\sim}{QM}^e_{11},\ \underset{\sim}{M}^e_{11},\ \underset{\sim}{C}^e_{11},\ \underset{\sim}{B}^e_{11},\ \underset{\sim}{QB}^e_{11}\},\{\underset{\sim}{H}^e_{12},\ \underset{\sim}{C}^e_{12},\ \underset{\sim}{B}^e_{12}\},$$
$$\{\underset{\sim}{H}^e_{13},\ \underset{\sim}{C}^e_{13},\ \underset{\sim}{B}^e_{13},\ \underset{\sim}{QB}^e_{13}\}\},$$
$$\{\{\underset{\sim}{QM}^e_{21},\ \underset{\sim}{M}^e_{21},\ \underset{\sim}{C}^e_{21},\ \underset{\sim}{B}^e_{21},\ \underset{\sim}{QB}^e_{21}\},\{\underset{\sim}{H}^e_{22},\ \underset{\sim}{C}^e_{22},\ \underset{\sim}{B}^e_{22}\},$$
$$\{\underset{\sim}{M}^e_{23},\ \underset{\sim}{C}^e_{23},\ \underset{\sim}{B}^e_{23}\}\},$$
$$\{\{\underset{\sim}{QM}^e_{31},\ \underset{\sim}{M}^e_{31},\ \underset{\sim}{C}^e_{31},\ \underset{\sim}{B}^e_{31},\ \underset{\sim}{QB}^e_{31}\},\{\underset{\sim}{M}^e_{32},\ \underset{\sim}{C}^e_{32},\ \underset{\sim}{B}^e_{32}\}\},$$
$$\{\{\underset{\sim}{M}^e_{41},\ \underset{\sim}{C}^e_{41},\ \underset{\sim}{B}^e_{41},\ \underset{\sim}{QB}^e_{41}\},\{\underset{\sim}{H}^e_{42},\ \underset{\sim}{C}^e_{42},\ \underset{\sim}{B}^e_{42}\},$$
$$\{\underset{\sim}{H}^e_{43},\ \underset{\sim}{C}^e_{43},\ \underset{\sim}{B}^e_{43}\}\},$$
$$\{\{\underset{\sim}{QM}^e_{51},\ \underset{\sim}{M}^e_{51},\ \underset{\sim}{C}^e_{51},\ \underset{\sim}{B}^e_{51},\ \underset{\sim}{QB}^e_{51}\},\{\underset{\sim}{M}^e_{52},\ \underset{\sim}{CP}^e_{52},\ \underset{\sim}{CT}^e_{52}\}\}\}=$$
$$\{\{\{\underset{\sim}{T}^e_{SNFKBП1},\ \underset{\sim}{T}^e_{SNFKBП2},\ \underset{\sim}{T}^e_{SNFKBП3},\ \underset{\sim}{T}^e_{SNFKBП4},\ \underset{\sim}{T}^e_{SNFKBП5}\},$$
$$\{\underset{\sim}{T}^e_{SNFCOП1},\ \underset{\sim}{T}^e_{SNFCOП2},\ \underset{\sim}{T}^e_{SNFCOП3}\},$$
$$\{\underset{\sim}{T}^e_{SNFTП1},\ \underset{\sim}{T}^e_{SNFTП2},\ \underset{\sim}{T}^e_{SNFTП3},\ \underset{\sim}{T}^e_{SNFTП4}\}\},$$
$$\{\{\underset{\sim}{T}^e_{DSKOП1},\ \underset{\sim}{T}^e_{DSKOП2},\ \underset{\sim}{T}^e_{DSKOП3},\ \underset{\sim}{T}^e_{DSKOП4},\ \underset{\sim}{T}^e_{DSKOП5}\},$$
$$\{\underset{\sim}{T}^e_{DSCO31},\ \underset{\sim}{T}^e_{DSCO32},\ \underset{\sim}{T}^e_{DSCO33}\},\{\underset{\sim}{T}^e_{DS3M31},\ \underset{\sim}{T}^e_{DS3M32},\ \underset{\sim}{T}^e_{DS3M33}\}\},$$
$$\{\{\underset{\sim}{T}^e_{SPKOП1},\ \underset{\sim}{T}^e_{SPKOП2},\ \underset{\sim}{T}^e_{SPKOП3},\ \underset{\sim}{T}^e_{SPKOП4},\ \underset{\sim}{T}^e_{SPKOП5}\},$$
$$\{\underset{\sim}{T}^e_{SPKПOA1},\ \underset{\sim}{T}^e_{SPKПOA2},\ \underset{\sim}{T}^e_{SPKПOA3}\}\},$$
$$\{\{\underset{\sim}{T}^e_{ESPKCБ1},\ \underset{\sim}{T}^e_{ESPKCБ2},\ \underset{\sim}{T}^e_{ESPKCБ3},\ \underset{\sim}{T}^e_{ESPKCБ4}\},$$
$$\{\underset{\sim}{T}^e_{ESPKCT1},\ \underset{\sim}{T}^e_{ESPKCT2},\ \underset{\sim}{T}^e_{ESPKCT3}\},$$
$$\{\underset{\sim}{T}^e_{ESPKCC1},\ \underset{\sim}{T}^e_{ESPKCC2},\ \underset{\sim}{T}^e_{ESPKCC3}\}\},$$
$$\{\{\underset{\sim}{T}^e_{SNKBK1},\ \underset{\sim}{T}^e_{SNKBK2},\ \underset{\sim}{T}^e_{SNKBK3},\ \underset{\sim}{T}^e_{SNKBK3},\ \underset{\sim}{T}^e_{SNKBK5}\},$$
$$\{\underset{\sim}{T}^e_{SNBBK1},\ \underset{\sim}{T}^e_{SNBBK2},\ \underset{\sim}{T}^e_{SNBBK3}\}\}=$$
$$\{\{\underset{\sim}{QM}^e_{SNFKBП},\ \underset{\sim}{M}^e_{SNFKBП},\ \underset{\sim}{C}^e_{SNFKBП},\ \underset{\sim}{B}^e_{SNFKBП},\ \underset{\sim}{QB}^e_{SNFKBП}\},$$
$$\{\underset{\sim}{H}^e_{SNFCOП},\ \underset{\sim}{C}^e_{SNFCOП},\ \underset{\sim}{B}^e_{SNFCOП}\},$$
$$\{\underset{\sim}{H}^e_{SNFTП},\ \underset{\sim}{C}^e_{SNFTП},\ \underset{\sim}{B}^e_{SNFTП},\ \underset{\sim}{QB}^e_{SNFTП}\}\},$$
$$\{\{\underset{\sim}{QM}^e_{DSKOП},\ \underset{\sim}{M}^e_{DSKOП},\ \underset{\sim}{C}^e_{DSKOП},\ \underset{\sim}{B}^e_{DSKOП},\ \underset{\sim}{QB}^e_{DSKOП}\},$$
$$\{\underset{\sim}{H}^e_{DSCO3},\ \underset{\sim}{C}^e_{DSCO3},\ \underset{\sim}{B}^e_{DSCO3}\},\{\underset{\sim}{M}^e_{DS3M3},\ \underset{\sim}{C}^e_{DS3M3},\ \underset{\sim}{B}^e_{DS3M3}\}\},$$
$$\{\{\underset{\sim}{QM}^e_{SPKOП},\ \underset{\sim}{M}^e_{SPKOП},\ \underset{\sim}{C}^e_{SPKOП},\ \underset{\sim}{B}^e_{SPKOП},\ \underset{\sim}{QB}^e_{SPKOП}\},$$
$$\{\underset{\sim}{M}^e_{SPKПOA},\ \underset{\sim}{C}^e_{SPKПOA},\ \underset{\sim}{B}^e_{SPKПOA}\}\},$$
$$\{\{\underset{\sim}{M}^e_{ESPKCБ},\ \underset{\sim}{C}^e_{ESPKCБ},\ \underset{\sim}{B}^e_{ESPKCБ},\ \underset{\sim}{QB}^e_{ESPKCБ}\},$$

$$\{\underset{\sim}{H}^{e}_{ESPKCT},\ \underset{\sim}{C}^{e}_{ESPKCT},\ \underset{\sim}{B}^{e}_{ESPKCT}\},\{\underset{\sim}{H}^{e}_{ESPKCC},\ \underset{\sim}{C}^{e}_{ESPKCC},\ \underset{\sim}{B}^{e}_{ESPKCC}\}\},$$

$$\{\{\underset{\sim}{OM}^{e}_{SNKBK},\ \underset{\sim}{M}^{e}_{SNKBK},\ \underset{\sim}{C}^{e}_{SNKBK},\ \underset{\sim}{Б}^{e}_{SNKBK},\ \underset{\sim}{OБ}^{e}_{SNKBK}\},\{\underset{\sim}{M}^{e}_{SNBBK},\ \underset{\sim}{CP}^{e}_{SNBBK},\ \underset{\sim}{CT}^{e}_{SNBBK}\}\}\},$$

де:

- $\underset{\sim}{T}^{e}_{111} = \underset{\sim}{OM}^{e}_{11} = \underset{\sim}{T}^{e}_{SNFKBII1} = \underset{\sim}{OM}^{e}_{SNFKBII}$,
- $\underset{\sim}{T}^{e}_{112} = \underset{\sim}{M}^{e}_{11} = \underset{\sim}{T}^{e}_{SNFKBII2} = \underset{\sim}{M}^{e}_{SNFKBII}$,
- $\underset{\sim}{T}^{e}_{113} = \underset{\sim}{C}^{e}_{11} = \underset{\sim}{T}^{e}_{SNFKBII3} = \underset{\sim}{C}^{e}_{SNFKBII}$,
- $\underset{\sim}{T}^{e}_{114} = \underset{\sim}{Б}^{e}_{11} = \underset{\sim}{T}^{e}_{SNFKBII4} = \underset{\sim}{Б}^{e}_{SNFKBII}$,
- $\underset{\sim}{T}^{e}_{115} = \underset{\sim}{OБ}^{e}_{11} = \underset{\sim}{T}^{e}_{SNFKBII5} = \underset{\sim}{OБ}^{e}_{SNFKBII}$,
- $\underset{\sim}{T}^{e}_{121} = \underset{\sim}{H}^{e}_{12} = \underset{\sim}{T}^{e}_{SNFCOII1} = \underset{\sim}{H}^{e}_{SNFCOII}$,
- $\underset{\sim}{T}^{e}_{122} = \underset{\sim}{C}^{e}_{12} = \underset{\sim}{T}^{e}_{SNFCOII2} = \underset{\sim}{C}^{e}_{SNFCOII}$,
- $\underset{\sim}{T}^{e}_{123} = \underset{\sim}{B}^{e}_{12} = \underset{\sim}{T}^{e}_{SNFCOII3} = \underset{\sim}{B}^{e}_{SNFCOII}$

та

- $\underset{\sim}{T}^{e}_{131} = \underset{\sim}{H}^{e}_{13} = \underset{\sim}{T}^{e}_{SNFTII1} = \underset{\sim}{H}^{e}_{SNFTII}$,
- $\underset{\sim}{T}^{e}_{132} = \underset{\sim}{C}^{e}_{13} = \underset{\sim}{T}^{e}_{SNFTII2} = \underset{\sim}{C}^{e}_{SNFTII}$,
- $\underset{\sim}{T}^{e}_{133} = \underset{\sim}{B}^{e}_{13} = \underset{\sim}{T}^{e}_{SNFTII3} = \underset{\sim}{B}^{e}_{SNFTII}$,
- $\underset{\sim}{T}^{e}_{134} = \underset{\sim}{OB}^{e}_{13} = \underset{\sim}{T}^{e}_{SNFTII4} = \underset{\sim}{OB}^{e}_{SNFTII}$ –

є компонентами лінгвістичних еталонів, які відображають параметри $P_{11} = P_{SNFKBII} = KBII,\ P_{12} = P_{SNFCOII} = COII,\ P_{13} = P_{SNFTII} = TII$ або відповідно «КВП», «СОП», «ТП» та в сукупності визначають еталонне КВП-СОП-ТП-підсередовище ($\mathbf{T}^{e}_{i} = \mathbf{T}^{e}_{1} = \mathbf{T}^{e}_{SNF}$), за допомогою якого здійснюється виявлення кібератаки з ІД CA_{SNF} або *SNF*-атаки;

- $\underset{\sim}{T}^{e}_{211} = \underset{\sim}{OM}^{e}_{21} = \underset{\sim}{T}^{e}_{DSKOII1} = \underset{\sim}{OM}^{e}_{DSKOII}$,
- $\underset{\sim}{T}^{e}_{212} = \underset{\sim}{M}^{e}_{21} = \underset{\sim}{T}^{e}_{DSKOII2} = \underset{\sim}{M}^{e}_{DSKOII}$,
- $\underset{\sim}{T}^{e}_{213} = \underset{\sim}{C}^{e}_{21} = \underset{\sim}{T}^{e}_{DSKOII3} = \underset{\sim}{C}^{e}_{DSKOII}$,
- $\underset{\sim}{T}^{e}_{214} = \underset{\sim}{Б}^{e}_{21} = \underset{\sim}{T}^{e}_{DSKOII4} = \underset{\sim}{Б}^{e}_{DSKOII}$,
- $\underset{\sim}{T}^{e}_{215} = \underset{\sim}{OБ}^{e}_{21} = \underset{\sim}{T}^{e}_{DSKOII5} = \underset{\sim}{OБ}^{e}_{DSKOII}$,
- $\underset{\sim}{T}^{e}_{221} = \underset{\sim}{H}^{e}_{22} = \underset{\sim}{T}^{e}_{DSCO31} = \underset{\sim}{H}^{e}_{DSCO3}$,
- $\underset{\sim}{T}^{e}_{222} = \underset{\sim}{C}^{e}_{22} = \underset{\sim}{T}^{e}_{DSCO32} = \underset{\sim}{C}^{e}_{DSCO3}$,

- $\underset{\sim}{T}^{e}_{223} = \underset{\sim}{B}^{e}_{22} = \underset{\sim}{T}^{e}_{DSCO33} = \underset{\sim}{B}^{e}_{DSCO3}$

та

- $\underset{\sim}{T}^{e}_{231} = \underset{\sim}{M}^{e}_{23} = \underset{\sim}{T}^{e}_{DS3M31} = \underset{\sim}{M}^{e}_{DS3M3}$,
- $\underset{\sim}{T}^{e}_{232} = \underset{\sim}{C}^{e}_{23} = \underset{\sim}{T}^{e}_{DS3M32} = \underset{\sim}{C}^{e}_{DS3M3}$,
- $\underset{\sim}{T}^{e}_{233} = \underset{\sim}{Б}^{e}_{23} = \underset{\sim}{T}^{e}_{DS3M33} = \underset{\sim}{Б}^{e}_{DS3M3}$ –

є компонентами лінгвістичних еталонів, які відображають параметри $P_{21} = P_{DSKOП} = KOП$, $P_{22} = P_{DSCO3} = CO3$, $P_{23} = P_{DS3M3} = 3M3$ або відповідно «КОП», «СОЗ», «ЗМЗ» та в сукупності визначають еталонне КОП-СОЗ-ЗМЗ-підсередовище ($\mathbf{T}^{e}_{i} = \mathbf{T}^{e}_{2} = \mathbf{T}^{e}_{DS}$), шляхом якого здійснюється виявлення кібератаки з ІД CA_{DS} або *DS*-атаки;

- $\underset{\sim}{T}^{e}_{311} = \underset{\sim}{OM}^{e}_{31} = \underset{\sim}{T}^{e}_{SPKOП1} = \underset{\sim}{OM}^{e}_{SPKOП}$,
- $\underset{\sim}{T}^{e}_{312} = \underset{\sim}{M}^{e}_{31} = \underset{\sim}{T}^{e}_{SPKOП2} = \underset{\sim}{M}^{e}_{SPKOП}$,
- $\underset{\sim}{T}^{e}_{313} = \underset{\sim}{C}^{e}_{31} = \underset{\sim}{T}^{e}_{SPKOП3} = \underset{\sim}{C}^{e}_{SPKOП}$,
- $\underset{\sim}{T}^{e}_{314} = \underset{\sim}{Б}^{e}_{31} = \underset{\sim}{T}^{e}_{SPKOП4} = \underset{\sim}{Б}^{e}_{SPKOП}$,
- $\underset{\sim}{T}^{e}_{315} = \underset{\sim}{OБ}^{e}_{31} = \underset{\sim}{T}^{e}_{SPKOП5} = \underset{\sim}{OБ}^{e}_{SPKOП}$

та

- $\underset{\sim}{T}^{e}_{321} = \underset{\sim}{M}^{e}_{32} = \underset{\sim}{T}^{e}_{SPKПОА1} = \underset{\sim}{M}^{e}_{SPKПОА}$,
- $\underset{\sim}{T}^{e}_{322} = \underset{\sim}{C}^{e}_{32} = \underset{\sim}{T}^{e}_{SPKПОА2} = \underset{\sim}{C}^{e}_{SPKПОА}$,
- $\underset{\sim}{T}^{e}_{323} = \underset{\sim}{Б}^{e}_{32} = \underset{\sim}{T}^{e}_{SPKПОА3} = \underset{\sim}{Б}^{e}_{SPKПОА}$ –

є компонентами лінгвістичних еталонів, які відображають параметри $P_{31} = P_{SPKOП} = KOП$, $P_{32} = P_{SPKПОА} = KПОА$ або відповідно «КОП», «КПОА» та в сукупності визначають еталонне КОП-КПОА-підсередовище ($\mathbf{T}^{e}_{i} = \mathbf{T}^{e}_{3} = \mathbf{T}^{e}_{SP}$), за допомогою якого здійснюється виявлення кібератаки з ІД CA_{SP} або *SP*-атаки;

- $\underset{\sim}{T}^{e}_{411} = \underset{\sim}{M}^{e}_{41} = \underset{\sim}{T}^{e}_{ESPKСБ1} = \underset{\sim}{M}^{e}_{ESPKСБ}$,
- $\underset{\sim}{T}^{e}_{412} = \underset{\sim}{C}^{e}_{41} = \underset{\sim}{T}^{e}_{ESPKСБ2} = \underset{\sim}{C}^{e}_{ESPKСБ}$,
- $\underset{\sim}{T}^{e}_{413} = \underset{\sim}{Б}^{e}_{41} = \underset{\sim}{T}^{e}_{ESPKСБ3} = \underset{\sim}{Б}^{e}_{ESPKСБ}$,
- $\underset{\sim}{T}^{e}_{414} = \underset{\sim}{OБ}^{e}_{41} = \underset{\sim}{T}^{e}_{ESPKСБ4} = \underset{\sim}{OБ}^{e}_{ESPKСБ}$,
- $\underset{\sim}{T}^{e}_{421} = \underset{\sim}{H}^{e}_{42} = \underset{\sim}{T}^{e}_{ESPKCT1} = \underset{\sim}{H}^{e}_{ESPKCT}$,
- $\underset{\sim}{T}^{e}_{422} = \underset{\sim}{C}^{e}_{42} = \underset{\sim}{T}^{e}_{ESPKCT2} = \underset{\sim}{C}^{e}_{ESPKCT}$,

- $\underset{\sim}{T}^{e}_{423} = \underset{\sim}{B}^{e}_{42} = \underset{\sim}{T}^{e}_{ESPKCT3} = \underset{\sim}{B}^{e}_{ESPKCT}$

та

- $\underset{\sim}{T}^{e}_{431} = \underset{\sim}{H}^{e}_{43} = \underset{\sim}{T}^{e}_{ESPKCC1} = \underset{\sim}{H}^{e}_{ESPKCC}$,
- $\underset{\sim}{T}^{e}_{432} = \underset{\sim}{C}^{e}_{43} = \underset{\sim}{T}^{e}_{ESPKCC2} = \underset{\sim}{C}^{e}_{ESPKCC}$,
- $\underset{\sim}{T}^{e}_{433} = \underset{\sim}{B}^{e}_{43} = \underset{\sim}{T}^{e}_{ESPKCC3} = \underset{\sim}{B}^{e}_{ESPKCC}$ –

є компонентами лінгвістичних еталонів, які відображають параметри $P_{41} = P_{ESPKCБ} = КСБ,\ P_{42} = P_{ESPKCT} = КСТ$ та $P_{43} = P_{ESPKCC} = КСС$ або відповідно «КСБ», «КСТ», «КСС» та в сукупності визначають еталонне КСБ-КСТ-КСС-підсередовище ($\mathbf{T}^{e}_{i} = \mathbf{T}^{e}_{4} = \mathbf{T}^{e}_{ESP}$), шляхом якого здійснюється виявлення кібератаки з ІД CA_{ESP} або *ESP*-атаки; де:

- $\underset{\sim}{T}^{e}_{511} = \underset{\sim}{OM}^{e}_{51} = \underset{\sim}{T}^{e}_{SNKBK1} = \underset{\sim}{OM}^{e}_{SNKBK}$,
- $\underset{\sim}{T}^{e}_{512} = \underset{\sim}{M}^{e}_{51} = \underset{\sim}{T}^{e}_{SNKBK2} = \underset{\sim}{M}^{e}_{SNKBK}$,
- $\underset{\sim}{T}^{e}_{513} = \underset{\sim}{C}^{e}_{51} = \underset{\sim}{T}^{e}_{SNKBK3} = \underset{\sim}{C}^{e}_{SNKBK}$,
- $\underset{\sim}{T}^{e}_{514} = \underset{\sim}{Б}^{e}_{51} = \underset{\sim}{T}^{e}_{SNKBK4} = \underset{\sim}{Б}^{e}_{SNKBK}$,
- $\underset{\sim}{T}^{e}_{115} = \underset{\sim}{QБ}^{e}_{51} = \underset{\sim}{T}^{e}_{SNKBK5} = \underset{\sim}{QБ}^{e}_{SNKBK}$

та

- $\underset{\sim}{T}^{e}_{521} = \underset{\sim}{M}^{e}_{52} = \underset{\sim}{T}^{e}_{SNBBK1} = \underset{\sim}{M}^{e}_{SNBBK}$,
- $\underset{\sim}{T}^{e}_{522} = \underset{\sim}{CP}^{e}_{52} = \underset{\sim}{T}^{e}_{SNBBK2} = \underset{\sim}{CP}^{e}_{SNBBK}$,
- $\underset{\sim}{T}^{e}_{523} = \underset{\sim}{CT}^{e}_{52} = \underset{\sim}{T}^{e}_{SNBBK3} = \underset{\sim}{CT}^{e}_{SNBBK}$ –

є компонентами лінгвістичних еталонів, які відображають параметри $P_{51} = P_{SNKBK} = КВК,\ P_{52} = P_{SNBBK} = ВВК$ або відповідно «КВК», «ВВК» та в сукупності визначають еталонне КВК-ВВК-підсередовище ($\mathbf{T}^{e}_{i} = \mathbf{T}^{e}_{5} = \mathbf{T}^{e}_{SN}$), за допомогою якого здійснюється виявлення кібератаки з ІД CA_{SN} або *SN*-атаки.

Формування $\mathbf{P}^{\tau_f}_{i}$.

Побудова підмножини $\mathbf{P}^{\tau_f}_{i} \subseteq \mathbf{P}^{\tau_f}$ ($\mathbf{P}^{\tau_f}$ – множина всіх можливих поточних значень нечітких параметрів) здійснюється шляхом $\mathbf{T}^{e}_{i}$ в

момент часу τ_f за часовий проміжок, протяжність якого $\tau_h = \tau_f - \tau_{f-1}$ ($f = \overline{1, max_\tau}$), при цьому f є номером часового інтервалу, максимальне значення якого визначається величиною max_τ.

Таким чином, $\mathbf{P_i^{\tau_f}}$ визначимо як:

$$\mathbf{P_i^{\tau_f}} = \{ \bigcup_{j=1}^{m_i} \underset{\sim}{P}_{ij}^{\tau_f} \} =$$

$$\{ \underset{\sim}{P}_{i1}^{\tau_f}, \ \underset{\sim}{P}_{i2}^{\tau_f}, \ ..., \ \underset{\sim}{P}_{im_i}^{\tau_f} \}, \qquad (2.16)$$

$$(j = \overline{1, m_i}),$$

де $\underset{\sim}{P}_{ij}^{\tau_f}$ – поточний нечіткий параметр, який формується в момент часу τ_f, а m_i – кількість нечітких поточних параметрів, за станом аномальності яких здійснюється виявлення кібератак з ІД CA_i.

За аналогією з параметричним та еталонним підсередовищем ($\mathbf{P_i}$ та $\mathbf{T_i^e}$) сукупність визначених значень всіх членів підмножини $\mathbf{P_i^{\tau_f}}$ визначають поточне підсередовище ($\mathbf{P_i^{\tau_f}}$), що використовується для виявлення аномального стану в загальному гетерогенному параметричному середовищі та, як наслідок, в m_i-вимірному параметричному підсередовищі ($\mathbf{P_i}$), породженого кібератакою з ІД CA_i в момент часу τ_f.

Наприклад, якщо $n = 5, \ i = \overline{1,5}$ ($\mathbf{CA_1^{\tau_f} = CA_{SNF}^{\tau_f} = SNF^{\tau_f}}$, $\mathbf{CA_2^{\tau_f} = CA_{DS}^{\tau_f} = DS^{\tau_f}}$, $\mathbf{CA_3^{\tau_f} = CA_{SP}^{\tau_f} = SP^{\tau_f}}$, $\mathbf{CA_4^{\tau_f} = CA_{ESP}^{\tau_f} = ESP^{\tau_f}}$ та $\mathbf{CA_5^{\tau_f} = CA_{SN}^{\tau_f} = SN^{\tau_f}}$), $m_1 = m_2 = m_4 = 3$ і $m_3 = m_5 = 2$, то вираз (2.16) можна визначити як:

$$\mathbf{P_1^{\tau_f}} = \{ \bigcup_{j=1}^{3} \underset{\sim}{P}_{1j}^{\tau_f} \} = \{ \underset{\sim}{P}_{11}^{\tau_f}, \ \underset{\sim}{P}_{12}^{\tau_f}, \ \underset{\sim}{P}_{13}^{\tau_f} \} =$$

$$\{ \underset{\sim}{P}_{SNFKBII}^{\tau_f}, \ \underset{\sim}{P}_{SNFCOII}^{\tau_f}, \ \underset{\sim}{P}_{SNFTII}^{\tau_f} \}, \qquad (2.17)$$

$$(\text{для } i = 1, \ m_1 = 3);$$

$$\mathbf{P}_{\mathbf{2}}^{\boldsymbol{\tau}_{\mathbf{f}}} = \{\bigcup_{j=1}^{3} \underset{\sim}{P}_{2j}^{\tau_f}\} = \{\underset{\sim}{P}_{21}^{\tau_f},\ \underset{\sim}{P}_{22}^{\tau_f},\ \underset{\sim}{P}_{23}^{\tau_f}\} =$$

$$\{\underset{\sim}{P}_{DSKOП}^{\tau_f},\ \underset{\sim}{P}_{DSCO3}^{\tau_f},\ \underset{\sim}{P}_{DS3M3}^{\tau_f}\},$$

$$(\text{для } i = 2,\ m_2 = 3);$$

$$\mathbf{P}_{\mathbf{3}}^{\boldsymbol{\tau}_{\mathbf{f}}} = \{\bigcup_{j=1}^{2} \underset{\sim}{P}_{3j}^{\tau_f}\} = \{\underset{\sim}{P}_{31}^{\tau_f},\ \underset{\sim}{P}_{32}^{\tau_f}\} =$$

$$\{\underset{\sim}{P}_{SPKOП}^{\tau_f},\ \underset{\sim}{P}_{SPKПOA}^{\tau_f}\},$$

$$(\text{для } i = 3,\ m_3 = 2),$$

$$\mathbf{P}_{\mathbf{4}}^{\boldsymbol{\tau}_{\mathbf{f}}} = \{\bigcup_{j=1}^{3} \underset{\sim}{P}_{4j}^{\tau_f}\} = \{\underset{\sim}{P}_{41}^{\tau_f},\ \underset{\sim}{P}_{42}^{\tau_f},\ \underset{\sim}{P}_{43}^{\tau_f}\} =$$

$$\{\underset{\sim}{P}_{ESPKCБ}^{\tau_f},\ \underset{\sim}{P}_{ESPKCT}^{\tau_f},\ \underset{\sim}{P}_{ESPKCC}^{\tau_f}\},$$

$$(\text{для } i = 4,\ m_4 = 3);$$

$$\mathbf{P}_{\mathbf{5}}^{\boldsymbol{\tau}_{\mathbf{f}}} = \{\bigcup_{j=1}^{2} \underset{\sim}{P}_{5j}^{\tau_f}\} = \{\underset{\sim}{P}_{51}^{\tau_f},\ \underset{\sim}{P}_{52}^{\tau_f}\} =$$

$$\{\underset{\sim}{P}_{SNKBK}^{\tau_f},\ \underset{\sim}{P}_{SNBBK}^{\tau_f}\},$$

$$(\text{для } i = 5,\ m_5 = 2),$$

де:

- $\underset{\sim}{P}_{11}^{\tau_f} = \underset{\sim}{P}_{SNFKBП}^{\tau_f}$, $\underset{\sim}{P}_{12}^{\tau_f} = \underset{\sim}{P}_{SNFCOП}^{\tau_f}$ та $\underset{\sim}{P}_{13}^{\tau_f} = \underset{\sim}{P}_{SNFTП}^{\tau_f}$ – є нечіткими поточними значеннями, які відображають параметри $P_{11} = P_{SNFKBП} = КВП,\ \ P_{12} = P_{SNFCOП} = СОП,\ \ P_{13} = P_{SNFTП} = ТП,$ тобто «КВП», «СОП» та «ТП» відповідно, конкретні значення яких в сукупності складають поточне КВП-СОП-ТП-підсередовище ($\mathbf{P}_{\mathbf{i}}^{\boldsymbol{\tau}_{\mathbf{f}}} = \mathbf{P}_{\mathbf{1}}^{\boldsymbol{\tau}_{\mathbf{f}}} = \mathbf{P}_{\mathbf{SNF}}^{\boldsymbol{\tau}_{\mathbf{f}}}$), яке використовується для виявлення аномального стану в *3*-вимірному параметричному підсередовищі ($\mathbf{P}_{\mathbf{i}} = \mathbf{P}_{\mathbf{1}} = \mathbf{P}_{\mathbf{SNF}}$), що породжено *SNF*-атакою;
- $\underset{\sim}{P}_{21}^{\tau_f} = \underset{\sim}{P}_{DSKOП}^{\tau_f}$, $\underset{\sim}{P}_{22}^{\tau_f} = \underset{\sim}{P}_{DSCO3}^{\tau_f}$ та $\underset{\sim}{P}_{23}^{\tau_f} = \underset{\sim}{P}_{DS3M3}^{\tau_f}$ – є нечіткими поточними значеннями, які відображають параметри $P_{21} =$

$P_{DSКОП} = КОП,\ \ P_{22} = P_{DSСОЗ} = СОЗ$ і $P_{23} = P_{DSЗМЗ} = ЗМЗ,$ тобто «КОП», «СОЗ» та «ЗМЗ» відповідно, конкретні значення яких в сукупності складають поточне КОП-СОЗ-ЗМЗ-підсередовище ($\mathbf{P}_{\mathbf{i}}^{\boldsymbol{\tau}_{\mathbf{f}}} = \mathbf{P}_{\mathbf{2}}^{\boldsymbol{\tau}_{\mathbf{f}}} = \mathbf{P}_{\mathbf{DS}}^{\boldsymbol{\tau}_{\mathbf{f}}}$), яке використовується для виявлення аномального стану в *3*-вимірному параметричному підсередовищі ($\mathbf{P}_{\mathbf{i}} = \mathbf{P}_{\mathbf{2}} = \mathbf{P}_{\mathbf{DS}}$), що породжено *DS*-атакою;

- $\underset{\sim}{P}_{31}^{\tau_f} = \underset{\sim}{P}_{SPКОП}^{\tau_f}$ та $\underset{\sim}{P}_{32}^{\tau_f} = \underset{\sim}{P}_{SPКПОА}^{\tau_f}$ – є нечіткими поточними значеннями, які відображають параметри $P_{31} = P_{SPКОП} = КОП$ і $P_{32} = P_{SPКПОА} = КПОА,$ тобто «КОП» та «КПОА» відповідно, конкретні значення яких в сукупності складають поточне КОП-КПОА-підсередовище ($\mathbf{P}_{\mathbf{i}}^{\boldsymbol{\tau}_{\mathbf{f}}} = \mathbf{P}_{\mathbf{3}}^{\boldsymbol{\tau}_{\mathbf{f}}} = \mathbf{P}_{\mathbf{SP}}^{\boldsymbol{\tau}_{\mathbf{f}}}$), яке використовується для виявлення аномального стану в *2*-вимірному параметричному підсередовищі ($\mathbf{P}_{\mathbf{i}} = \mathbf{P}_{\mathbf{3}} = \mathbf{P}_{\mathbf{SP}}$), що породжено *SP*-атакою;
- $\underset{\sim}{P}_{41}^{\tau_f} = \underset{\sim}{P}_{ESPКСБ}^{\tau_f},\ \underset{\sim}{P}_{42}^{\tau_f} = \underset{\sim}{P}_{ESPКСТ}^{\tau_f}$ та $\underset{\sim}{P}_{43}^{\tau_f} = \underset{\sim}{P}_{ESPКСС}^{\tau_f}$ – є нечіткими поточними значеннями, які відображають параметри $P_{41} = P_{ESPКСБ} = КСБ,\ \ P_{42} = P_{ESPКСТ} = КСТ$ та $P_{43} = P_{ESPКСС} = КСС,$ тобто «КСБ», «КСТ», «КСС» відповідно, конкретні значення яких в сукупності складають поточне КСБ-КСТ-КСС-підсередовище ($\mathbf{P}_{\mathbf{i}}^{\boldsymbol{\tau}_{\mathbf{f}}} = \mathbf{P}_{\mathbf{4}}^{\boldsymbol{\tau}_{\mathbf{f}}} = \mathbf{P}_{\mathbf{ESP}}^{\boldsymbol{\tau}_{\mathbf{f}}}$), яке використовується для виявлення аномального стану в *3*-вимірному параметричному підсередовищі ($\mathbf{P}_{\mathbf{i}} = \mathbf{P}_{\mathbf{4}} = \mathbf{P}_{\mathbf{ESP}}$), що породжено *ESP*-атакою;
- $\underset{\sim}{P}_{51}^{\tau_f} = \underset{\sim}{P}_{SNKBK}^{\tau_f}$ та $\underset{\sim}{P}_{52}^{\tau_f} = \underset{\sim}{P}_{SNBBK}^{\tau_f}$ – є нечіткими поточними значеннями, які відображають параметри $P_{51} = P_{SNKBK} = КВК$ і $P_{52} = P_{SNBBK} = ВВК,$ тобто «КВК» та «ВВК» відповідно, конкретні значення яких в сукупності складають поточне КВК-ВВК-підсередовище ($\mathbf{P}_{\mathbf{i}}^{\boldsymbol{\tau}_{\mathbf{f}}} = \mathbf{P}_{\mathbf{5}}^{\boldsymbol{\tau}_{\mathbf{f}}} = \mathbf{P}_{\mathbf{SN}}^{\boldsymbol{\tau}_{\mathbf{f}}}$), яке використовується для виявлення аномального стану в *2*-вимірному параметричному підсередовищі ($\mathbf{P}_{\mathbf{i}} = \mathbf{P}_{\mathbf{5}} = \mathbf{P}_{\mathbf{SN}}$), що породжено *SN*-атакою.

Формування $\mathbf{DR_i}$.

Побудова підмножин базових детекційних правил $\mathbf{DR_i} \subseteq \mathbf{DR}$, $i=\overline{1,n}$ ($\mathbf{DR}$ – множина всіх можливих правил, що утворює детекційне середовище ($\mathbf{DR}$)), які використовуються для виявлення *i*-ї кібератаки здійснюється на основі виразу

$$\{\bigcup_{i=1}^{n}\mathbf{DR_i}\}=\{\mathbf{DR_1},\ \mathbf{DR_2},\ \ldots,\ \mathbf{DR_n}\}, \tag{2.18}$$

де

$$\mathbf{DR_i}=\{\bigcup_{a=1}^{w_i}\mathbf{DR_{ia}}\}=\{\mathbf{DR_{i1}},\ \mathbf{DR_{i2}},\ \ldots,\ \mathbf{DR_{iw_i}}\},\quad (a=\overline{1,w_i}), \tag{2.19}$$

а w_i – кількість базових детекційних правил, які використовуються для виявлення *i*-ї кібератаки.

З урахуванням (2.19) формулу (2.18) запишемо в наступному вигляді:

$$\begin{gathered}\{\bigcup_{i=1}^{n}\mathbf{DR_i}\}=\{\bigcup_{i=1}^{n}\{\bigcup_{a=1}^{w_i}\mathbf{DR_{ia}}\}\}=\\ \{\{\mathbf{DR_{11}},\ \mathbf{DR_{12}},\ \ldots,\ \mathbf{DR_{1w_1}}\},\\ \{\mathbf{DR_{21}},\ \mathbf{DR_{22}},\ \ldots,\ \mathbf{DR_{2w_2}}\},\\ \ldots,\\ \{\mathbf{DR_{n1}},\ \mathbf{DR_{n2}},\ \ldots,\ \mathbf{DR_{nw_n}}\},\\ (i=\overline{1,n},\ a=\overline{1,w_i}).\end{gathered} \tag{2.20}$$

Зазначимо, що в сукупності всі елементи підмножини $\mathbf{DR_i}$ визначають детекційне підсередовище ($\mathbf{DR_i}$), яке використовується для виявлення кібератаки з ІД CA_i в атакуючому середовищі ($\mathbf{CA}^{\tau_f}$).

Наприклад, при $n=5$ ($\mathbf{CA_1^{\tau_f}}=\mathbf{CA_{SNF}^{\tau_f}}=\mathbf{SNF}^{\tau_f}$, $\mathbf{CA_2^{\tau_f}}=\mathbf{CA_{DS}^{\tau_f}}=\mathbf{DS}^{\tau_f}$, $\mathbf{CA_3^{\tau_f}}=\mathbf{CA_{SP}^{\tau_f}}=\mathbf{SP}^{\tau_f}$, $\mathbf{CA_4^{\tau_f}}=\mathbf{CA_{ESP}^{\tau_f}}=\mathbf{ESP}^{\tau_f}$ та $\mathbf{CA_5^{\tau_f}}=\mathbf{CA_{SN}^{\tau_f}}=\mathbf{SN}^{\tau_f}$) та $w_1=w_2=w_3=w_4=w_5=5$ вираз (2.20) можна визначити як:

$$\{\bigcup_{i=1}^{5}\mathbf{DR}_i\} = \{\mathbf{DR}_1,\ \mathbf{DR}_2,\ \mathbf{DR}_3,\ \mathbf{DR}_4,\ \mathbf{DR}_5\} =$$

$$\{\bigcup_{i=1}^{5}\{\bigcup_{a=1}^{w_i}\mathbf{DR}_{ia}\}\} =$$

$$\begin{gathered}\{\{\mathbf{DR}_{11},\ \mathbf{DR}_{12},\ \mathbf{DR}_{13},\ \mathbf{DR}_{14},\ \mathbf{DR}_{15}\},\\ \{\mathbf{DR}_{21},\ \mathbf{DR}_{22},\ \mathbf{DR}_{23},\ \mathbf{DR}_{24},\ \mathbf{DR}_{25}\},\\ \{\mathbf{DR}_{31},\ \mathbf{DR}_{32},\ \mathbf{DR}_{33},\ \mathbf{DR}_{34},\ \mathbf{DR}_{35}\},\\ \{\mathbf{DR}_{41},\ \mathbf{DR}_{42},\ \mathbf{DR}_{43},\ \mathbf{DR}_{44},\ \mathbf{DR}_{45}\},\\ \{\mathbf{DR}_{51},\ \mathbf{DR}_{52},\ \mathbf{DR}_{53},\ \mathbf{DR}_{54},\ \mathbf{DR}_{55}\}\},\end{gathered} \tag{2.21}$$

де в сукупності всі елементи відповідних підмножин

- $\mathbf{DR}_1 = \{\mathbf{DR}_{11},\ \mathbf{DR}_{12},\ \mathbf{DR}_{13},\ \mathbf{DR}_{14},\ \mathbf{DR}_{15}\}$,
- $\mathbf{DR}_2 = \{\mathbf{DR}_{21},\ \mathbf{DR}_{22},\ \mathbf{DR}_{23},\ \mathbf{DR}_{24},\ \mathbf{DR}_{25}\}$,
- $\mathbf{DR}_3 = \{\mathbf{DR}_{31},\ \mathbf{DR}_{32},\ \mathbf{DR}_{33},\ \mathbf{DR}_{34},\ \mathbf{DR}_{35}\}$,
- $\mathbf{DR}_4 = \{\mathbf{DR}_{41},\ \mathbf{DR}_{42},\ \mathbf{DR}_{43},\ \mathbf{DR}_{44},\ \mathbf{DR}_{45}\}$,
- $\mathbf{DR}_5 = \{\mathbf{DR}_{51},\ \mathbf{DR}_{52},\ \mathbf{DR}_{53},\ \mathbf{DR}_{54},\ \mathbf{DR}_{55}\}$

визначають детекційне середовище ($\mathbf{DR}$), що містить безпосередньо базові детекційні правила, які відповідно використовуються для виявлення *SNF*-, *DS*-, *SP*-, *ESP*- та *SN*-атак.

Таким чином, сформовані всі компоненти кортежу (2.2), які дають змогу визначити m_i-вимірні параметричні підсередовища ($\mathbf{P}_i$), а також атакуючі, еталонні, поточні та детекційні підсередовища ($\mathbf{CA}_i^{\tau_f}$, $\mathbf{T}_i^{e}$, $\mathbf{P}_i^{\tau_f}$ та $\mathbf{DR}_i$).

Наприклад, при $n = 5$ на основі узагальнювального кортежу (2.2) можна сформувати його часткові відображення в $\mathbf{CA}_1^{\tau_f} = \mathbf{CA}_{\mathbf{SNF}}^{\tau_f} = \mathbf{SNF}^{\tau_f}$, $\mathbf{CA}_2^{\tau_f} = \mathbf{CA}_{\mathbf{DS}}^{\tau_f} = \mathbf{DS}^{\tau_f}$, $\mathbf{CA}_3^{\tau_f} = \mathbf{CA}_{\mathbf{SP}}^{\tau_f} = \mathbf{SP}^{\tau_f}$, $\mathbf{CA}_4^{\tau_f} = \mathbf{CA}_{\mathbf{ESP}}^{\tau_f} = \mathbf{ESP}^{\tau_f}$, $\mathbf{CA}_5^{\tau_f} = \mathbf{CA}_{\mathbf{SN}}^{\tau_f} = \mathbf{SN}^{\tau_f}$, тобто:

$$\begin{aligned}\mathbf{CA}_1^{\tau_f} &= <CA_1,\ \mathbf{P}_1,\ \mathbf{T}_1^{e},\ \mathbf{P}_1^{\tau_f},\ \mathbf{DR}_1>,\\ \mathbf{CA}_2^{\tau_f} &= <CA_2,\ \mathbf{P}_2,\ \mathbf{T}_2^{e},\ \mathbf{P}_2^{\tau_f},\ \mathbf{DR}_2>,\\ \mathbf{CA}_3^{\tau_f} &= <CA_3,\ \mathbf{P}_3,\ \mathbf{T}_3^{e},\ \mathbf{P}_3^{\tau_f},\ \mathbf{DR}_3>,\end{aligned} \tag{2.22}$$

$$\mathbf{CA}_4^{\tau_f} = < CA_4,\ \mathbf{P}_4,\ \mathbf{T}_4^e,\ \mathbf{P}_4^{\tau_f},\ \mathbf{DR}_4 >,$$

$$\mathbf{CA}_5^{\tau_f} = < CA_5,\ \mathbf{P}_5,\ \mathbf{T}_5^e,\ \mathbf{P}_5^{\tau_f},\ \mathbf{DR}_5 >,$$

а з урахуванням (2.9), (2.15), (2.17), (2.21) вираз (2.22) прийме вигляд:

$$\mathbf{CA}_1^{\tau_f} = < CA_1,\ \{P_{11},\ P_{12},\ P_{13}\},$$
$$\{\{\underset{\sim}{T}^e_{111},\ \underset{\sim}{T}^e_{112},\ \underset{\sim}{T}^e_{113},\ \underset{\sim}{T}^e_{114},\ \underset{\sim}{T}^e_{115}\},$$
$$\{\underset{\sim}{T}^e_{121},\ \underset{\sim}{T}^e_{122},\ \underset{\sim}{T}^e_{123}\},$$
$$\{\underset{\sim}{T}^e_{131},\ \underset{\sim}{T}^e_{132},\ \underset{\sim}{T}^e_{133},\ \underset{\sim}{T}^e_{134}\}\},$$
$$\{\underset{\sim}{P}^{\tau_f}_{11},\ \underset{\sim}{P}^{\tau_f}_{12},\ \underset{\sim}{P}^{\tau_f}_{13}\},$$
$$\{\ \mathbf{DR}_{11},\ \mathbf{DR}_{12},\ \mathbf{DR}_{13},\ \mathbf{DR}_{14},\ \mathbf{DR}_{15}\ \} > \text{ або}$$

$$\mathbf{CA}_{\mathbf{SNF}}^{\tau_f} = < CA_{SNF},\ \{P_{SNFKBП},\ P_{SNFCOП},\ P_{SNFTIП}\},$$
$$\{\{\underset{\sim}{T}^e_{SNFKBП1},\ \underset{\sim}{T}^e_{SNFKBП2},\ \underset{\sim}{T}^e_{SNFKBП3},\ \underset{\sim}{T}^e_{SNFKBП4},\ \underset{\sim}{T}^e_{SNFKBП5}\},$$
$$\{\underset{\sim}{T}^e_{SNFCOП1},\ \underset{\sim}{T}^e_{SNFCOП2},\ \underset{\sim}{T}^e_{SNFCOП3}\},$$
$$\{\underset{\sim}{T}^e_{SNFTIП1},\ \underset{\sim}{T}^e_{SNFTIП2},\ \underset{\sim}{T}^e_{SNFTIП3},\ \underset{\sim}{T}^e_{SNFTIП4}\}\},$$
$$\{\underset{\sim}{P}^{\tau_f}_{SNFKBП},\ \underset{\sim}{P}^{\tau_f}_{SNFCOП},\ \underset{\sim}{P}^{\tau_f}_{SNFTIП}\},$$
$$\{\ \mathbf{DR}_{11},\ \mathbf{DR}_{12},\ \mathbf{DR}_{13},\ \mathbf{DR}_{14},\ \mathbf{DR}_{15}\ \} >$$
(при $m_1 = 3$, $r_1 = 5$, $r_2 = 3$, $r_3 = 4$ та $w_1 = 5$); (2.23)

$$\mathbf{CA}_2^{\tau_f} = < CA_2,\ \{P_{21},\ P_{22},\ P_{23}\},$$
$$\{\{\underset{\sim}{T}^e_{211},\ \underset{\sim}{T}^e_{212},\ \underset{\sim}{T}^e_{213},\ \underset{\sim}{T}^e_{214},\ \underset{\sim}{T}^e_{215}\},$$
$$\{\underset{\sim}{T}^e_{221},\ \underset{\sim}{T}^e_{222},\ \underset{\sim}{T}^e_{223}\},$$
$$\{\underset{\sim}{T}^e_{231},\ \underset{\sim}{T}^e_{232},\ \underset{\sim}{T}^e_{233}\}\},$$
$$\{\underset{\sim}{P}^{\tau_f}_{21},\ \underset{\sim}{P}^{\tau_f}_{22},\ \underset{\sim}{P}^{\tau_f}_{23}\},$$
$$\{\ \mathbf{DR}_{21},\ \mathbf{DR}_{22},\ \mathbf{DR}_{23},\ \mathbf{DR}_{24},\ \mathbf{DR}_{25}\ \} > \text{ або}$$

$$\mathbf{CA}_{\mathbf{DS}}^{\tau_f} = < CA_{DS},\ \{P_{DSKOП},\ P_{DSCO3},\ P_{DS3M3}\},$$
$$\{\{\underset{\sim}{T}^e_{DSKOП1},\ \underset{\sim}{T}^e_{DSKOП2},\ \underset{\sim}{T}^e_{DSKOП3},\ \underset{\sim}{T}^e_{DSKOП4},\ \underset{\sim}{T}^e_{DSKOП5}\},$$
$$\{\underset{\sim}{T}^e_{DSCO31},\ \underset{\sim}{T}^e_{DSCO32},\ \underset{\sim}{T}^e_{DSCO33}\},$$
$$\{\underset{\sim}{T}^e_{DS3M31},\ \underset{\sim}{T}^e_{DS3M32},\ \underset{\sim}{T}^e_{DS3M33}\}\},$$
$$\{\underset{\sim}{P}^{\tau_f}_{DSKOП},\ \underset{\sim}{P}^{\tau_f}_{DSCO3},\ \underset{\sim}{P}^{\tau_f}_{DS3M3}\},$$

$\{\ \mathbf{DR_{21}}, \mathbf{DR_{22}}, \mathbf{DR_{23}}, \mathbf{DR_{24}}, \mathbf{DR_{25}}\ \}>$

(при $m_2 = 3,\ r_1 = 5,\ r_2 = r_3 = 3$ та $w_2 = 5$);

$\mathbf{CA_3^{\tau_f}} =< CA_3, \{P_{31}, P_{32}\},$

$\{\{\underset{\sim}{T}^e_{311}, \underset{\sim}{T}^e_{312}, \underset{\sim}{T}^e_{313}, \underset{\sim}{T}^e_{314}, \underset{\sim}{T}^e_{315}\},$

$\{\underset{\sim}{T}^e_{321}, \underset{\sim}{T}^e_{322}, \underset{\sim}{T}^e_{323}\}\},$

$\{\underset{\sim}{P}^{\tau_f}_{31}, \underset{\sim}{P}^{\tau_f}_{32}\},$

$\{\ \mathbf{DR_{31}}, \mathbf{DR_{32}}, \mathbf{DR_{33}}, \mathbf{DR_{34}}, \mathbf{DR_{35}}\ \}>$ або

$\mathbf{CA_{SP}^{\tau_f}} =< CA_{SP}, \{P_{SPKOП}, P_{SPKПOA}\},$

$\{\{\underset{\sim}{T}^e_{SPKOП1}, \underset{\sim}{T}^e_{SPKOП2}, \underset{\sim}{T}^e_{SPKOП3}, \underset{\sim}{T}^e_{SPKOП4}, \underset{\sim}{T}^e_{SPKOП5}\},$

$\{\underset{\sim}{T}^e_{SPKПOA1}, \underset{\sim}{T}^e_{SPKПOA2}, \underset{\sim}{T}^e_{SPKПOA3}\}\},$

$\{\underset{\sim}{P}^{\tau_f}_{SPKOП}, \underset{\sim}{P}^{\tau_f}_{SPKПOA}\},$

$\{\ \mathbf{DR_{31}}, \mathbf{DR_{32}}, \mathbf{DR_{33}}, \mathbf{DR_{34}}, \mathbf{DR_{35}}\ \}>$

(при $m_3 = 2,\ r_1 = 5,\ r_2 = 3$ та $w_3 = 5$);

$\mathbf{CA_4^{\tau_f}} =< CA_4, \{P_{41}, P_{42}, P_{43}\},$

$\{\{\underset{\sim}{T}^e_{411}, \underset{\sim}{T}^e_{412}, \underset{\sim}{T}^e_{413}, \underset{\sim}{T}^e_{414}\},$

$\{\underset{\sim}{T}^e_{421}, \underset{\sim}{T}^e_{422}, \underset{\sim}{T}^e_{423}\},$

$\{\underset{\sim}{T}^e_{431}, \underset{\sim}{T}^e_{432}, \underset{\sim}{T}^e_{433}\}\},$

$\{\underset{\sim}{P}^{\tau_f}_{41}, \underset{\sim}{P}^{\tau_f}_{42}, \underset{\sim}{P}^{\tau_f}_{43}\},$

$\{\ \mathbf{DR_{41}}, \mathbf{DR_{42}}, \mathbf{DR_{43}}, \mathbf{DR_{44}}, \mathbf{DR_{45}}\ \}>$ або

$\mathbf{CA_{ESP}^{\tau_f}} =< CA_{ESP}, \{P_{ESPKCБ}, P_{ESPKCT}, P_{ESPKCC}\},$

$\{\{\underset{\sim}{T}^e_{ESPKCБ1}, \underset{\sim}{T}^e_{ESPKCБ2}, \underset{\sim}{T}^e_{ESPKCБ3}, \underset{\sim}{T}^e_{ESPKCБ4}\},$

$\{\underset{\sim}{T}^e_{ESPKCT1}, \underset{\sim}{T}^e_{ESPKCT2}, \underset{\sim}{T}^e_{ESPKCT3}\},$

$\{\underset{\sim}{T}^e_{ESPKCC1}, \underset{\sim}{T}^e_{ESPKCC2}, \underset{\sim}{T}^e_{ESPKCC3}\}\},$

$\{\underset{\sim}{P}^{\tau_f}_{ESPKCБ}, \underset{\sim}{P}^{\tau_f}_{ESPKCT}, \underset{\sim}{P}^{\tau_f}_{ESPKCC}\},$

$\{\ \mathbf{DR_{41}}, \mathbf{DR_{42}}, \mathbf{DR_{43}}, \mathbf{DR_{44}}, \mathbf{DR_{45}}\ \}>$

(при $m_4 = 3,\ r_1 = 4,\ r_2 = r_3 = 3$ та $w_4 = 5$);

$\mathbf{CA_5^{\tau_f}} =< CA_5, \{P_{51}, P_{52}\},$

$$\{\{\underset{\sim}{T}^{e}_{Б11}, \underset{\sim}{T}^{e}_{Б12}, \underset{\sim}{T}^{e}_{Б13}, \underset{\sim}{T}^{e}_{Б14}, \underset{\sim}{T}^{e}_{Б15}\},$$
$$\{\underset{\sim}{T}^{e}_{Б21}, \underset{\sim}{T}^{e}_{Б22}, \underset{\sim}{T}^{e}_{Б23}\}\},$$
$$\{\underset{\sim}{P}^{\tau_f}_{51}, \underset{\sim}{P}^{\tau_f}_{52}\},$$
$$\{\mathbf{DR_{51}}, \mathbf{DR_{52}}, \mathbf{DR_{53}}, \mathbf{DR_{54}}, \mathbf{DR_{55}}\} > \text{або}$$
$$\mathbf{CA^{\tau_f}_{SN}} = < CA_{SN}, \{P_{SNKBK}, P_{SNBBK}\},$$
$$\{\{\underset{\sim}{T}^{e}_{SNKBK1}, \underset{\sim}{T}^{e}_{SNKBK2}, \underset{\sim}{T}^{e}_{SNKBK3}, \underset{\sim}{T}^{e}_{SNKBK3}, \underset{\sim}{T}^{e}_{SNKBK5}\},$$
$$\{\underset{\sim}{T}^{e}_{SNBBK1}, \underset{\sim}{T}^{e}_{SNBBK2}, \underset{\sim}{T}^{e}_{SNBBK3}\}\},$$
$$\{\underset{\sim}{P}^{\tau_f}_{SNKBK}, \underset{\sim}{P}^{\tau_f}_{SNBBK}\},$$
$$\{\mathbf{DR_{51}}, \mathbf{DR_{52}}, \mathbf{DR_{53}}, \mathbf{DR_{54}}, \mathbf{DR_{55}}\} >$$
(при $m_5 = 2,\ r_1 = 5,\ r_2 = 3$ та $w_5 = 5$).

Виходячи із запропонованих теоретичних положень (які описують структуру кортежної моделі) та з наведеного прикладу можна зазначити, що за допомогою сформованих множин узагальнювальних кортежів визначається стан аномальності в *m*-вимірному гетерогенному параметричному середовищі ($\mathbf{P}$), яке утворюється не тільки атакуючим SNF-DS-SP-ESP-SN-середовищем ($\mathbf{CA^{\tau_f}}$) в момент часу τ_f, але і середовищами з іншими класами кібератак, для яких можливо сформувати подібні кортежі.

Таким чином, запропонована кортежна модель формування атакуючих середовищ (КМАС) (або набору базових компонент або базова кортежна модель) [1], яка за рахунок формалізації процесу створення m_i-вимірних параметричних, атакуючих, еталонних, поточних та детекційних підсередовищ, дозволяє сформувати набір часткових кортежів, за якими здійснюється симуляція процесу виявлення аномального стану в *m*-вимірному гетерогенному параметричному середовищі, утвореного відповідним атакуючим середовищем у заданий часовий проміжок.

З урахуванням цього для практичного використання КМАС, при удосконаленні СВВ, необхідно створити відповідний метод для формування еталонних середовищ, з урахуванням якого можна в подальшому будувати еталони параметрів для певних груп лінгвістичних змінних у визначеному середовищі оточення.

2.2. Метод формування еталонного середовища для систем виявлення вторгнень

Для побудови підмножини нечітких (лінгвістичних) еталонів $\mathbf{T}_{ij}^{e}$ (див. (2.13)), які відображають характерні судження експерта відносно аномального стану параметра P_{ij} згідно КМАС (див. п. 2.1. та [1]) пропонується відповідний метод, який дозволяє формувати процес отримання еталонів параметрів для зазначених груп лінгвістичних змінних визначеного середовища оточення.

З урахуванням [5, 6] і їх розвитком в [7-11] пропонується узагальнювальний метод формування еталонних середовищ (МФЕС) [7].

Він орієнтований на вирішення задач виявлення кібератак в ІС і є узагальнюванням методу лінгвістичних термів з використанням статистичних даних (МЛТС) [12]. Метод ґрунтується на шести етапах:

- визначення підмножин ідентифікаторів лінгвістичних оцінок;
- формування базової матриці частот;
- формування похідної матриці частот;
- побудова нечітких термів;
- побудова нечітких чисел еталонного середовища;
- візуалізація еталонних підсередовищ.

Опишемо кожен з етапів.

Визначення підмножин ідентифікаторів лінгвістичних оцінок

Етап 1 – визначення підмножин ідентифікаторів лінгвістичних оцінок. Побудова підмножини $\mathbf{LE}_{i}$ здійснюється на основі множини всіх можливих ІД лінгвістичних оцінок (суджень) експерта $\mathbf{LE}$ представлених як

$$\begin{gathered}\mathbf{LE} = \{\bigcup_{l=1}^{c} LE_l\} = \\ \{LE_1,\ LE_2,\ \ldots,\ LE_c\}, \\ (l = \overline{1,c}),\end{gathered} \tag{2.24}$$

та які відображають використані експертом судження для характеристики стану параметрів $\mathbf{P_i}$ (див. п. 2.1 та [1-3]) при їх спостереженні в m_l-вимірному параметричному підсередовищі ($\mathbf{P_i}$), а c – кількість таких ІД.

Наприклад, при $c = 11$ відповідно до (2.24) множину **LE** можна представити в наступному вигляді:

$$\begin{gathered}\mathbf{LE} = \{\bigcup_{l=1}^{11} LE_l\} = \\ \{LE_1,\ LE_2,\ ...,\ LE_{11}\} = \\ \{LE_{ОМ},\ LE_{М},\ LE_{С},\ LE_{Б},\ LE_{ОБ},\ LE_{МЛ},\ \\ LE_{СР},\ LE_{СТ},\ LE_{Н},\ LE_{В},\ LE_{ОВ}\} = \\ \{"ОМ",\ "М",\ "С",\ "Б",\ "ОБ",\ "МЛ",\ \\ "СР",\ "СТ",\ "Н",\ "В",\ "ОВ"\},\end{gathered} \tag{2.25}$$

де:

- $LE_1 = LE_{ОМ} = "ОМ"$,
- $LE_2 = LE_{М} = "М"$,
- $LE_3 = LE_{С} = "С"$,
- $LE_4 = LE_{Б} = "Б"$,
- $LE_5 = LE_{ОБ} = "ОБ"$,
- $LE_6 = LE_{МЛ} = "МЛ"$,
- $LE_7 = LE_{СР} = "СР"$,
- $LE_8 = LE_{СТ} = "СТ"$,
- $LE_9 = LE_{Н} = "Н"$,
- $LE_{10} = LE_{В} = "В"$,
- $LE_{11} = LE_{ОВ} = "ОВ"$

відповідно є ІД лінгвістичних оцінок (суджень) експерта, як-от:

- «ДУЖЕ МАЛЕ» або «ОЧЕНЬ МАЛОЕ (ОМ)» (при $l = 1$),
- «МАЛЕ» або «МАЛОЕ (М)» (при $l = 2$),
- «СЕРЕДНЄ» або «СРЕДНЕЕ (С)» (при $l = 3$),
- «ВЕЛИКЕ» або «БОЛЬШОЕ (Б)» (при $l = 4$),
- «ДУЖЕ ВЕЛИКЕ» або «ОЧЕНЬ БОЛЬШОЕ (ОБ)» (при $l = 5$),

- «МОЛОДИЙ» або «МОЛОДОЙ (МЛ)» (при $l=6$),
- «СЕРЕДНІЙ» або «СРЕДНИЙ (СР)» (при $l=7$),
- «СТАРИЙ» або «СТАРЫЙ (СТ)» (при $l=8$),
- «НИЗЬКИЙ» або «НИЗКАЯ (Н)» (при $l=9$),
- «ВИСОКИЙ» або «ВЫСОКАЯ (В)» (при $l=10$),
- «ДУЖЕ ВИСОКИЙ» або «ОЧЕНЬ ВЫСОКАЯ (ОВ)» (при $l=11$).

Далі, сформуємо підмножини ІД суджень експерта

$$\{\bigcup_{i=1}^{n}\mathbf{LE_i}\}=\{\mathbf{LE_1},\ \mathbf{LE_2},\ \ldots,\ \mathbf{LE_n}\}, \tag{2.26}$$

де $\mathbf{LE_i}\subseteq\mathbf{LE}$, $(i=\overline{1,n})$ визначимо як:

$$\mathbf{LE_i}=\{\bigcup_{j=1}^{m_i}\mathbf{LE_{ij}}\}=\{\mathbf{LE_{i1}},\ \mathbf{LE_{i2}},\ \ldots,\ \mathbf{LE_{im_i}}\}, \tag{2.27}$$

при цьому $\mathbf{LE_{ij}}$ $(j=\overline{1,m_i})$ є підмножиною ІД суджень експерта відносно значень параметрів P_{ij} (див. вираз (2.8)) в m_i-вимірному параметричному підсередовищі ($\mathbf{P_i}$).

З урахуванням (2.27) формулу (2.26) запишемо у наступному вигляді:

$$\begin{gathered}\{\bigcup_{i=1}^{n}\mathbf{LE_i}\}=\{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\mathbf{LE_{ij}}\}\}=\\ \{\{\mathbf{LE_{11}},\ \mathbf{LE_{12}},\ \ldots,\ \mathbf{LE_{1m_1}}\},\\ \{\mathbf{LE_{21}},\ \mathbf{LE_{22}},\ \ldots,\ \mathbf{LE_{2m_2}}\},\\ \ldots,\\ \{\mathbf{LE_{n1}},\ \mathbf{LE_{n2}},\ \ldots,\ \mathbf{LE_{nm_n}}\}\}.\end{gathered} \tag{2.28}$$

Таким чином, з урахуванням $\mathbf{LE_{ij}}\subseteq\mathbf{LE_i}$, відносно j-го параметра експерт може застосувати набір з r_j висловлювань (лінгвістичних оцінок), що відображається підмножиною

$$\mathbf{LE_{ij}}=\{\bigcup_{k=1}^{r_j}LE_{ijk}\}= \tag{2.29}$$

$$\{ LE_{ij1},\ LE_{ij2},\ ...,\ LE_{ijk},\ ...,\ LE_{ijr_j} \},$$

де LE_{ijk} $(k = \overline{1, r_j})$ – k-й ідентифікатор лінгвістичної оцінки експерта відносно стану j-го параметра при i-й атаці на РІС, а r_j – кількість ідентифікаторів в $\mathbf{LE_{ij}}$.

Далі, вираз (2.28) з урахуванням (2.29) приймає наступний вигляд:

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{LE_i}\} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}} \mathbf{LE_{ij}}\}\} =$$

$$\{\bigcup_{i=1}^{n} \{\bigcup_{j=1}^{m_i} \{\bigcup_{k=1}^{r_j} LE_{ijk}\}\}\} =$$

$$\{\{\{ LE_{111},\ LE_{112},\ ...,\ LE_{11r_1} \},\ \{ LE_{121},\ LE_{122},\ ...,\ LE_{12r_2} \},$$

$$...,$$

$$\{ LE_{1m_1 1},\ LE_{1m_1 2},\ ...,\ LE_{1m_1 r_{m_1}} \}\},$$

$$\{\{ LE_{211},\ LE_{212},\ ...,\ LE_{21r_1} \},\ \{ LE_{221},\ LE_{222},\ ...,\ LE_{22r_2} \},$$

$$...,$$

$$\{ LE_{2m_2 1},\ LE_{2m_2 2},\ ...,\ LE_{2m_2 r_{m_2}} \}\},$$

$$...,$$

$$\{\{ LE_{n11},\ LE_{n12},\ ...,\ LE_{n1r_1} \},\ \{ LE_{n21},\ LE_{n22},\ ...,\ LE_{n2r_2} \},\ ...,$$

$$\{ LE_{nm_n 1},\ LE_{nm_n 2},\ ...,\ LE_{nm_n r_{m_n}} \}\}\}. \qquad (2.30)$$

Наприклад, якщо $n = 3$ (тобто для кібератак з ІД $CA_1 = CA_{SN} = SN$, $CA_2 = CA_{DS} = DS$ та $CA_3 = CA_{SP} = SP$), $m_1 = m_3 = 2,\ m_2 = 3,\ r_1 = 5,\ r_2 = r_3 = 3$ вираз (2.30) можна визначити як:

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{3}} \mathbf{LE_i}\} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{3}} \{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}} \mathbf{LE_{ij}}\}\} =$$

$$\{\bigcup_{i=1}^{3} \{\bigcup_{j=1}^{m_i} \{\bigcup_{k=1}^{r_j} LE_{ijk}\}\}\} =$$

$$\{\{\{ LE_{111},\ LE_{112},\ LE_{113},\ LE_{114},\ LE_{115} \},\ \{ LE_{121},\ LE_{122},\ LE_{123} \}\},$$

$$\{\{ LE_{211},\ LE_{212},\ LE_{213},\ LE_{214},\ LE_{215} \},$$

$$\{LE_{221},\ LE_{222},\ LE_{223}\},\ \{LE_{231},\ LE_{232},\ LE_{233}\}\},$$
$$\{\{LE_{311},\ LE_{312},\ LE_{313},\ LE_{314},\ LE_{315}\},\ \{LE_{321},\ LE_{322},\ LE_{323}\}\}\}=$$
$$\{\{\{LE_{SNKBK1},\ LE_{SNKBK2},\ LE_{SNKBK3},\ LE_{SNKBK4},\ LE_{SNKBK5}\},$$
$$\{LE_{SNBBK1},\ LE_{SNBBK2},\ LE_{SNBBK3}\}\},$$
$$\{\{LE_{DSKOП1},\ LE_{DSKOП2},\ LE_{DSKOП3},\ LE_{DSKOП4},\ LE_{DSKOП5}\},$$
$$\{LE_{DSCO31},\ LE_{DSCO32},\ LE_{DSCO33}\},\ \{LE_{DS3M31},\ LE_{DS3M32},\ LE_{DS3M33}\}\},$$
$$\{\{LE_{SPKOП1},\ LE_{SPKOП2},\ LE_{SPKOП3},\ LE_{SPKOП4},\ LE_{SPKOП5}\},$$
$$\{LE_{SPKПОА1},\ LE_{SPKПОА2},\ LE_{SPKПОА3}\}\}\}=$$
$$\{\{\{"ОМ", "М", "С", "Б", "ОБ"\}, \{"МЛ", "СР", "СТ"\}\},$$
$$\{\{"ОМ", "М", "С", "Б", "ОБ"\},$$
$$\{"Н", "С", "В"\}, \{"М", "С", "Б"\}\},$$
$$\{\{"ОМ", "М", "С", "Б", "ОБ"\}, \{"М", "С", "Б"\}\}\}.$$

де:

- $LE_{111} = LE_{SNKBK1} = "ОМ",$
- $LE_{112} = LE_{SNKBK2} = "М",$
- $LE_{113} = LE_{SNKBK3} = "С",$
- $LE_{114} = LE_{SNKBK4} = "Б",$
- $LE_{115} = LE_{SNKBK5} = "ОБ"$

та

- $LE_{121} = LE_{SNBBK1} = "МЛ",$
- $LE_{122} = LE_{SNBBK2} = "СР",$
- $LE_{123} = LE_{SNBBK3} = "СТ"$ –

відповідно є ІД таких лінгвістичних оцінок експерта, які відображають стан параметрів $P_{11} = P_{SNKBK} = КВК$ та $P_{12} = P_{SNBBK} = ВВК$ в *2*-вимірному параметричному підсередовищі ($\mathbf{P_i = P_1 = P_{SN}}$);

- $LE_{211} = LE_{DSKOП1} = "ОМ",$
- $LE_{212} = LE_{DSKOП2} = "М",$
- $LE_{213} = LE_{DSKOП3} = "С",$
- $LE_{214} = LE_{DSKOП4} = "Б",$
- $LE_{215} = LE_{DSKOП5} = "ОБ"$

та

- $LE_{221} = LE_{DSCO31} = "H",$
- $LE_{222} = LE_{DSCO32} = "C",$
- $LE_{223} = LE_{DSCO33} = "B",$

а також

- $LE_{231} = LE_{DS3M31} = "M",$
- $LE_{232} = LE_{DS3M32} = "C",$
- $LE_{233} = LE_{DS3M33} = "Б"$ –

відповідно ІД лінгвістичних оцінок експерта, що відображають стан параметрів $P_{21} = P_{DSKOП} = КОП,\ P_{22} = P_{DSCO3} = СО3$ та $P_{23} = P_{DS3M3} = ЗМЗ$ в *3*-вимірному параметричному підсередовищі ($\mathbf{P_i = P_2 = P_{DS}}$);

- $LE_{311} = LE_{SP\,KOП1} = "OM",$
- $LE_{312} = LE_{SP\,KOП2} = "M",$
- $LE_{313} = LE_{SP\,KOП3} = "C",$
- $LE_{314} = LE_{SP\,KOП4} = "Б",$
- $LE_{315} = LE_{SP\,KOП5} = "OБ"$

та

- $LE_{321} = LE_{SPKПOA1} = "M",$
- $LE_{322} = LE_{SPKПOA2} = "C",$
- $LE_{323} = LE_{SPKПOA3} = "Б"$ –

відповідно є ІД таких суджень експерта, які відображають стан параметрів $P_{31} = P_{SPKOП} = КОП$ та $P_{32} = P_{SPKПOA} = КПОА$ в *2*-вимірному параметричному підсередовищі ($\mathbf{P_i = P_3 = P_{SP}}$).

Необхідно зазначити, що експерт висловлює свої судження про стан спостережуваних ним фактичних значень різних параметрів в *m*-вимірному гетерогенному параметричному середовищі ($\mathbf{P}$), але при цьому він може використовувати однакові висловлювання з множини $\mathbf{LE}$, які відображаються відповідними лінгвістичними ідентифікаторами.

Наприклад, ІД лінгвістичної оцінки експерта *"OM"* для параметрів

$$P_{11} = P_{SNKBK} = КВК$$

$$(LE_{111} = LE_{SNKBKI} = "OM") \text{ та}$$
$$P_{31} = P_{SPKOП} = KOП$$
$$(LE_{311} = LE_{SP\,KOП1} = "OM")$$

є лише всього лінгвістичними еквівалентами визначених значень цих величин та фактично характеризують їх певні відносні стани, які відображаються оцінками експертів.

Формування базової матриці частот

Етап 2 – формування базової матриці частот. Для отримання такої матриці вводиться множина ідентифікаторів інтервалів $\mathbf{N}$ та підмножини таких ідентифікаторів $\mathbf{N_i}$, які відображаються як

$$\{\bigcup_{i=1}^{n}\mathbf{N_i}\} = \{\mathbf{N_1}, \mathbf{N_2}, \ldots, \mathbf{N_n}\}, \tag{2.31}$$

де $\mathbf{N_i} \subseteq \mathbf{N}$, $(i = \overline{1,n})$ визначимо як

$$\mathbf{N_i} = \{\bigcup_{j=1}^{m_i}\mathbf{N_{ij}}\} = \{\mathbf{N_{i1}}, \mathbf{N_{i2}}, \ldots, \mathbf{N_{im_i}}\}, \tag{2.32}$$

при цьому $\mathbf{N_{ij}}$ $(j = \overline{1,m_i})$ – підмножина ІД інтервалів, на області визначення яких експерт здійснює лінгвістичне оцінювання відносно значень параметрів P_{ij} (див. (2.8)) в m_i-вимірному параметричному підсередовищі ($\mathbf{P_i}$).

З урахуванням (2.32) формулу (2.31) запишемо в наступному вигляді:

$$\{\bigcup_{i=1}^{n}\mathbf{N_i}\} = \{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\mathbf{N_{ij}}\}\} = \{\{\mathbf{N_{11}}, \mathbf{N_{12}}, \ldots, \mathbf{N_{1m_1}}\}, \{\mathbf{N_{21}}, \mathbf{N_{22}}, \ldots, \mathbf{N_{2m_2}}\}, \ldots, \{\mathbf{N_{n1}}, \mathbf{N_{n2}}, \ldots, \mathbf{N_{nm_n}}\}\}. \tag{2.33}$$

Далі, з урахуванням $\mathbf{N_{ij}} \subseteq \mathbf{N_i}$, відносно *j*-го параметра експерт для формування границь своїм оцінкам може використовувати набір з r_j інтервалів, що відображається підмножиною

$$\mathbf{N_{ij}} = \{\bigcup_{k=1}^{r_j} N_{ijk}\} = \{N_{ij1},\ N_{ij2},\ ...,\ N_{ijk},\ ...,\ N_{ijr_j}\}, \tag{2.34}$$

де N_{ijk} $(k = \overline{1,r_j})$ – ідентифікатор *k*-го інтервалу, який використовується для формування на ньому частот зустрічальності оцінок експерта за поточним станом *j*-го параметра відносно *i*-ї атаки на РІС, а r_j – кількість ідентифікаторів фіксованих інтервалів, на яких здійснюється зазначена оцінка.

Тоді, вираз (2.33) з урахуванням (2.34) приймає наступний вигляд:

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{N_i}\} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}} \mathbf{N_{ij}}\}\} = \{\bigcup_{i=1}^{n} \{\bigcup_{j=1}^{m_i} \{\bigcup_{k=1}^{r_j} N_{ijk}\}\}\} =$$

$$\{\{\{N_{111},\ N_{112},\ ...,\ N_{11r_1}\},\ \{N_{121},\ N_{122},\ ...,\ N_{12r_2}\},\ ...,$$
$$\{N_{1m_11},\ N_{1m_12},\ ...,\ N_{1m_1r_{m1}}\}\},$$
$$\{\{N_{211},\ N_{212},\ ...,\ N_{21r_1}\},\ \{N_{221},\ N_{222},\ ...,\ N_{22r_2}\},\ ...,$$
$$\{N_{2m_21},\ N_{2m_22},\ ...,\ N_{2m_2r_{m_2}}\}\},$$
$$...,$$
$$\{\{N_{n11},\ N_{n12},\ ...,\ N_{n1r_1}\},\ \{N_{n21},\ N_{n22},\ ...,\ N_{n2r_2}\},\ ...,$$
$$\{N_{nm_n1},\ N_{nm_n2},\ ...,\ N_{nm_nr_{m_n}}\}\}\}. \tag{2.35}$$

На основі елементів підмножин $\mathbf{LE_{ij}}$ та $\mathbf{N_{ij}}$ формується узагальнювальна таблиця оцінок (табл. 2.1), вміст якої ґрунтується на поточному фіксуванні свідоцтв (суджень, оцінок) експерта, де f_{ijsq}

$(s,q=\overline{1,r_j})$ – елементи емпіричних даних, які відображають кількість (частоту) однакових висловлювань (використання лінгвістичної оцінки підмножини $\mathbf{LE_{ij}}$) експерта, які характеризують стан *j*-го параметра на інтервалі з відповідним ідентифікатором

$$N_{ijq} \stackrel{\text{def}}{=} [N_{ijq}^{min}; N_{ijq}^{max}],\ (q=\overline{1,r_j}),$$

де N_{ijq}^{min} та N_{ijq}^{max} відповідно нижня та верхня границя *q*-го інтервалу.

Таблиця 2.1

Узагальнювальна таблиця оцінок за $\mathbf{LE_{ij}}$

$\mathbf{LE_{ij}}$	$\mathbf{N_{ij}}$					
	N_{ij1}	N_{ij2}	…	N_{ijq}	…	N_{ijr_j}
LE_{ij1}	f_{ij11}	f_{ij12}	…	f_{ij1q}	…	f_{ij1r_j}
LE_{ij2}	f_{ij21}	f_{ij22}	…	f_{ij2q}	…	f_{ij2r_j}
…	…	…	…	…	…	…
LE_{ijs}	f_{ijs1}	f_{ijs2}	…	f_{ijsq}	…	f_{ijsr_j}
…	…	…	…	…	…	…
LE_{ijr_j}	f_{ijr_j1}	f_{ijr_j2}	…	f_{ijr_jq}	…	$f_{ijr_jr_j}$

Далі, на основі узагальнювальної таблиці оцінок за елементами підмножини $\mathbf{LE_{ij}}$ (див. табл. 2.1) формується базова матриця частот

$$F_{ij} = \left\| f_{ijsq} \right\|_{(s,q=\overline{1,r_j})} = \begin{vmatrix} f_{ij11} & f_{ij12} & \dots & f_{ij1q} & \dots & f_{ij1r_j} \\ f_{ij21} & f_{ij22} & \dots & f_{ij2q} & \dots & f_{ij2r_j} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ f_{ijs1} & f_{ijs2} & \dots & f_{ijsq} & \dots & f_{ijsr_j} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ f_{ijr_j1} & f_{ijr_j2} & \dots & f_{ijr_jq} & \dots & f_{ijr_jr_j} \end{vmatrix}. \quad (2.36)$$

Наприклад, якщо вимагається сформувати матрицю F_{ij}, яка буде основною для побудови еталонів $\mathbf{T}^{\mathbf{e}}_{\mathbf{ij}}$, при $n=3$ (тобто для кібератак з ІД $CA_1 = CA_{SN} = SN$, $CA_2 = CA_{DS} = DS$ та $CA_3 = CA_{SP} = SP$), $m_1 = m_3 = 2$, $m_2 = 3$, $r_1 = 5$, $r_2 = r_3 = 3$, то (2.35) можна визначити як:

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{3}} \mathbf{N_i}\} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{3}} \{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}} \mathbf{N_{ij}}\}\} =$$

$$\{\bigcup_{i=1}^{3} \{\bigcup_{j=1}^{m_i} \{\bigcup_{k=1}^{r_j} N_{ijk}\}\}\} =$$

$$\begin{gathered}
\{\{\{N_{111},\ N_{112},\ N_{113},\ N_{114},\ N_{115}\},\ \{N_{121},\ N_{122},\ N_{123}\}\},\\
\{N_{211},\ N_{212},\ N_{213},\ N_{214},\ N_{215}\},\\
\{N_{221},\ N_{222},\ N_{223}\},\ \{N_{231},\ N_{232},\ N_{233}\}\},\\
\{N_{311},\ N_{312},\ N_{313},\ N_{314},\ N_{315}\},\ \{N_{321},\ N_{322},\ N_{323}\}\}\},\\
\{\{\{N_{SNKBK1},\ N_{SNKBK2},\ N_{SNKBK3},\ N_{SNKBK4},\ N_{SNKBK5}\},\\
\{N_{SNBBK1},\ N_{SNBBK2},\ N_{SNBBK3}\}\},\\
\{\{N_{DSKOП1},\ N_{DSKOП2},\ N_{DSKOП3},\ N_{DSKOП4},\ N_{DSKOП5}\},\\
\{N_{DSCO31},\ N_{DSCO32},\ N_{DSCO33}\},\ \{N_{DS3M31},\ N_{DS3M32},\ N_{DS3M33}\}\},\\
\{\{N_{SPKOП1},\ N_{SPKOП2},\ N_{SPKOП3},\ N_{SPKOП4},\ N_{SPKOП5}\},\\
\{N_{SPKПOA1},\ N_{SPKПOA2},\ N_{SPKПOA3}\}\}\}.
\end{gathered} \tag{2.37}$$

Наприклад, відповідно до (2.37) при $n=1$ ($i=3$, тобто для кібератаки з ІД $CA_3 = CA_{SP} = SP$),

$$j=1,\ r_j=5 \text{ для } \{N_{311},\ N_{312},\ N_{313},\ N_{314},\ N_{315}\} \text{ та}$$

$$j=2,\ r_j=3 \text{ для } \{N_{321},\ N_{322},\ N_{323}\}$$

на основі узагальнювальної таблиці (див. табл. 2.1) побудуємо поточні оцінки (табл. 2.2-2.3) за елементами підмножини

$$LE_{ijk} = LE_{31k} = LE_{SPKOПk} \ (r_1 = 5,\ k = \overline{1,5}),$$

де:

- $LE_{311} = LE_{SPKOП1} = "OM"$,
- $LE_{312} = LE_{SPKOП2} = "M"$,
- $LE_{313} = LE_{SPKOП3} = "C"$,

- $LE_{314} = LE_{SPKOП4} = "Б"$,
- $LE_{315} = LE_{SPKOП5} = "ОБ"$

та $N_{ijk} = N_{31k} = N_{SPKOПk}$, а

- $N_{ij1} = N_{311} = N_{SPKOП1} \stackrel{def}{=} [N^{min}_{SPKOП1}; N^{max}_{SPKOП1}] <=> [0; 8]$,
- $N_{ij2} = N_{312} = N_{SPKOП2} \stackrel{def}{=} [N^{min}_{SPKOП2}; N^{max}_{SPKOП2}] <=> [9; 64]$,
- $N_{ij3} = N_{313} = N_{SPKOП3} \stackrel{def}{=} [N^{min}_{SPKOП3}; N^{max}_{SPKOП3}] <=> [65; 256]$,
- $N_{ij4} = N_{314} = N_{SPKOП4} \stackrel{def}{=} [N^{min}_{SPKOП4}; N^{max}_{SPKOП4}] <=> [257; 512]$,
- $N_{ij5} = N_{315} = N_{SPKOП5} \stackrel{def}{=} [N^{min}_{SPKOП5}; N^{max}_{SPKOП5}] <=> [513; 1024]$.

Також за елементами підмножини

$$LE_{ijk} = LE_{32k} = LE_{SPKПОАk} \ (r_2 = 3, \ k = \overline{1,3}),$$

де:

- $LE_{321} = LE_{SPKПОА1} = "М"$,
- $LE_{322} = LE_{SPKПОА2} = "С"$,
- $LE_{323} = LE_{SPKПОА3} = "Б"$

та $N_{ijk} = N_{32k} = N_{SPKПОАk}$, а

- $N_{ij1} = N_{321} = N_{SPKПОА1} \stackrel{def}{=} [N^{min}_{SPKПОА1}; N^{max}_{SPKПОА1}] <=> [0; 10]$,
- $N_{ij2} = N_{322} = N_{SPKПОА2} \stackrel{def}{=} [N^{min}_{SPKПОА2}; N^{max}_{SPKПОА2}] <=> [11; 100]$,
- $N_{ij3} = N_{323} = N_{SPKПОА3} \ [N^{min}_{SPKПОА3}; N^{max}_{SPKПОА3}] <=> [101; 1000]$.

Таблиця 2.2

Поточна таблиця оцінок за $\mathbf{LE_{31}}$

$\mathbf{LE_{31}} = \mathbf{LE_{SPKOП}}$	$\mathbf{N_{31} = N_{SPKOП}}$				
	$N_{SPKOП1}$	$N_{SPKOП2}$	$N_{SPKOП3}$	$N_{SPKOП4}$	$N_{SPKOП5}$
$"ОМ"$	4	1	0	0	0
$"М"$	2	3	1	0	0
$"С"$	0	1	4	2	0
$"Б"$	0	0	2	5	3
$"ОБ"$	0	0	0	4	6

Таблиця 2.3

Поточна таблиця оцінок за $\mathbf{LE_{32}}$

$\mathbf{LE_{32}}$ = $\mathbf{LE_{SPKПОА}}$	$\mathbf{N_{32} = N_{SPKПОА}}$		
	$N_{SPKПОА1}$	$N_{SPKПОА2}$	$N_{SPKПОА3}$
$"M"$	3	1	0
$"C"$	1	4	2
$"Б"$	0	2	3

Далі, якщо $n=1,\ m_1=2,\ s,q=\overline{1,r_1}$ (тобто $s,q=\overline{1,5}$) та $s,q=\overline{1,r_2}$ (тобто $s,q=\overline{1,3}$) відповідно до виразу (2.36) з використанням даних табл. 2.2-2.3 сформуємо матриці частот, тобто

$$F_{31}=F_{SPKOП}=$$

$$\left\| f_{31sq} \right\| = \left\| f_{SPKOПsq} \right\| =$$

$$\begin{vmatrix} f_{3111} & f_{3112} & f_{3113} & f_{3114} & f_{3115} \\ f_{3121} & f_{3122} & f_{3123} & f_{3124} & f_{3125} \\ f_{3131} & f_{3132} & f_{3133} & f_{3134} & f_{3135} \\ f_{3141} & f_{3142} & f_{3143} & f_{3144} & f_{3145} \\ f_{3151} & f_{3152} & f_{3153} & f_{3154} & f_{3155} \end{vmatrix} = \begin{Vmatrix} 4 & 1 & 0 & 0 & 0 \\ 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 4 & 2 & 0 \\ 0 & 0 & 2 & 5 & 3 \\ 0 & 0 & 0 & 4 & 6 \end{Vmatrix}.$$

$$F_{32}=F_{SPKПОА}=$$

$$\left\| f_{32sq} \right\| = \left\| f_{SPKПОАsq} \right\| =$$

$$\begin{Vmatrix} f_{3211} & f_{3212} & f_{3213} \\ f_{3221} & f_{3222} & f_{3223} \\ f_{3231} & f_{3232} & f_{3233} \end{Vmatrix} = \begin{Vmatrix} 3 & 1 & 0 \\ 1 & 4 & 2 \\ 0 & 2 & 3 \end{Vmatrix}.$$

Формування похідної матриці частот

Етап 3 – формування похідної матриці частот. Для реалізації цього етапу створюється вектор сум (VS_{ij}) за відповідними стовпцями матриці частот (2.36), тобто

$$VS_{ij} = \left\| vs_{ijq} \right\| = \left\| vs_{ij1}, vs_{ij2}, ..., vs_{ijq}, ..., vs_{ijr_j} \right\| = \left\| \sum_{s=1}^{r_j} f_{ijs1}, \sum_{s=1}^{r_j} f_{ijs2}, ..., \sum_{s=1}^{r_j} f_{ijsq}, ..., \sum_{s=1}^{r_j} f_{ijsr_j} \right\| = \left\| \bigcup_{q=1}^{r_j} \sum_{s=1}^{r_j} f_{ijsq} \right\| \quad (s, q = \overline{1, r_j}), \tag{2.38}$$

де f_{ijsq} – елементи матриці F_{ij}. Далі серед членів VS_{ij} визначаємо максимальне значення за формулою

$$vsm_{ij} = \bigvee_{q=1}^{r_j} vs_{ijq}, \tag{2.39}$$

яке використовується для формування похідної матриці частот

$$F_{ij}^{'} = \left\| f_{ijsq}^{'} \right\| = (vsm_{ij} / vs_{ijq}) \left\| f_{ijsq} \right\| \Leftrightarrow$$

$$F_{ij}^{'} = (vsm_{ij} / vs_{ijq}) F_{ij} = \begin{Vmatrix} f_{ij11}^{'} & f_{ij12}^{'} & \dots & f_{ij1q}^{'} & \dots & f_{ij1r_j}^{'} \\ f_{ij21}^{'} & f_{ij22}^{'} & \dots & f_{ij2q}^{'} & \dots & f_{ij2r_j}^{'} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ f_{ijs1}^{'} & f_{ijs2}^{'} & \dots & f_{ijsq}^{'} & \dots & f_{ijsr_j}^{'} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ f_{ijr_j1}^{'} & f_{ijr_j2}^{'} & \dots & f_{ijr_jq}^{'} & \dots & f_{ijr_jr_j}^{'} \end{Vmatrix}. \tag{2.40}$$

Розглянемо формування $F_{ij}^{'}$ на конкретному прикладі.

Для цього при $(n=1,\ m_1=2)$ створюємо вектори сум $VS_{ij}=VS_{31}$ та $VS_{ij}=VS_{32}$ за відповідними стовпцями матриці частот (2.36) з використанням (2.38), тобто

$$VS_{31}=\left\|vs_{31q}\right\|=$$

$$\left\|vs_{311},vs_{312},vs_{313},vs_{314},vs_{315}\right\|=\left\|\bigcup_{q=1}^{5}\sum_{s=1}^{5}f_{31sq}\right\|\Longleftrightarrow$$

$$VS_{SPKOП}=\left\|vs_{SPKOПq}\right\|=$$

$$\left\|vs_{SPKOП1},vs_{SPKOП2},vs_{SPKOП3},vs_{SPKOП4},vs_{SPKOП5}\right\|=$$

$$\left\|\bigcup_{q=1}^{5}\sum_{s=1}^{5}f_{SPKOПsq}\right\|=\left\|6,5,7,11,9\right\|,$$

$(q=\overline{1,5})$ та

$$VS_{32}=\left\|vs_{32q}\right\|=\left\|vs_{321},vs_{322},vs_{323}\right\|=\left\|\bigcup_{q=1}^{3}\sum_{s=1}^{3}f_{32sq}\right\|\Longleftrightarrow$$

$$VS_{SPKПOA}=\left\|vs_{SPKПOAq}\right\|=$$

$$\left\|vs_{SPKПOA1},vs_{SPKПOA2},vs_{SPKПOA3}\right\|=$$

$$\left\|\bigcup_{q=1}^{3}\sum_{s=1}^{3}f_{SPKПOAsq}\right\|=\left\|4,7,5\right\|,$$

$(q=\overline{1,3}).$

Далі, в $VS_{31}=VS_{SPKOП}$ та $VS_{32}=VS_{SPKПOA}$ за формулою (2.39) визначаємо максимальні елементи

$$vsm_{31}=\bigvee_{q=1}^{5}vs_{31q}=vs_{311}\vee vs_{312}\vee vs_{313}\vee vs_{314}\vee vs_{315}=$$

$$6\vee 5\vee 7\vee 11\vee 9=$$

$$vsm_{SPKOП}=11 \text{ та}$$

$$vsm_{32}=\bigvee_{q=1}^{3}vs_{32q}=vs_{321}\vee vs_{322}\vee vs_{323}=$$

$$4\vee 7\vee 5=$$

$$vsm_{SPKПОА} = 7,$$

а похідні матриці частот

$$F'_{31} = \left\| f'_{31sq} \right\| = (vsm_{31} / vs_{31q}) \left\| f_{31sq} \right\| = F'_{SP\,KOП} \text{ та}$$

$$F'_{32} = \left\| f'_{32sq} \right\| = (vsm_{32} / vs_{32q}) \left\| f_{32sq} \right\| = F'_{SPKПОА}$$

отримаємо відповідно до (2.40)

$$F'_{SPKOП} = (vsm_{SPKOП} / vs_{SPKOП\,q}) F_{SPKOП} = \begin{vmatrix} 7,3 & 2,2 & 0 & 0 & 0 \\ 3,7 & 6,6 & 1,6 & 0 & 0 \\ 0 & 2,2 & 6,3 & 2 & 0 \\ 0 & 0 & 3,1 & 5 & 3,7 \\ 0 & 0 & 0 & 4 & 7,3 \end{vmatrix}$$

та

$$F'_{SPKПОА} = (vsm_{SPKПОА} / vs_{SPKПОА\,q}) F_{SPKПОА} = \begin{Vmatrix} 5,3 & 1 & 0 \\ 1,8 & 4 & 2,8 \\ 0 & 2 & 4,2 \end{Vmatrix}.$$

Побудова нечітких термів

Етап 4 – побудова нечітких термів. Формування підмножин нечітких термів $\mathbf{T_i}$ здійснюється на основі множини всіх можливих термів $\mathbf{T}$, які відображають визначені стани параметрів з $\mathbf{P_i}$ у m_i-вимірному параметричному підсередовищі ($\mathbf{P_i}$), тобто

$$\{\bigcup_{i=1}^{n} \mathbf{T_i}\} = \{\mathbf{T_1}, \mathbf{T_2}, \ldots, \mathbf{T_n}\}, \qquad (2.41)$$

де $\mathbf{T_i} \subseteq \mathbf{T}$, $(i = \overline{1,n})$, а

$$\mathbf{T_i} = \{\bigcup_{j=1}^{m_i} \mathbf{T_{ij}}\} = \{\mathbf{T_{i1}}, \mathbf{T_{i2}}, \ldots, \mathbf{T_{im_i}}\}, \qquad (2.42)$$

при цьому $\mathbf{T_{ij}}$ $(j = \overline{1,m_i})$ є підмножиною нечітких термів відносно значень параметрів P_{ij} (див. (2.8)). З урахуванням (2.42) формулу (2.41) запишемо в наступному вигляді:

$$\{\bigcup_{i=1}^{n}\mathbf{T_i}\}=\{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\mathbf{T_{ij}}\}\}=$$
$$\{\{\mathbf{T_{11}},\ \mathbf{T_{12}},\ \ldots,\ \mathbf{T_{1m_1}}\},$$
$$\{\mathbf{T_{21}},\ \mathbf{T_{22}},\ \ldots,\ \mathbf{T_{2m_2}}\},\qquad(2.43)$$
$$\ldots,$$
$$\{\mathbf{T_{n1}},\ \mathbf{T_{n2}},\ \ldots,\ \mathbf{T_{nm_n}}\}\},$$
$$(\ j=\overline{1,m_i}\ ).$$

Таким чином, з урахуванням $\mathbf{T_{ij}} \subseteq \mathbf{T_i}$ та (2.43), підмножину нечітких термів визначимо як:

$$\mathbf{T_{ij}}=\{\bigcup_{s=1}^{r_j}\underset{\sim}{T}_{ijs}\}=$$
$$\{\underset{\sim}{T}_{ij1},\ \underset{\sim}{T}_{ij2},\ \ldots,\ \underset{\sim}{T}_{ijs},\ \ldots,\ \underset{\sim}{T}_{ijr_j}\},\qquad(2.44)$$

де $\underset{\sim}{T}_{ijs}$ $(\ s=\overline{1,r_j}\ )$ – нечіткі терми, а r_j – кількість членів в $\mathbf{T_{ij}}$.

Далі, вираз (2.43) з урахуванням (2.44) приймає наступний вигляд:

$$\{\bigcup_{i=1}^{n}\mathbf{T_i}\}=\{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\mathbf{T_{ij}}\}\}=$$
$$\{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\{\bigcup_{s=1}^{r_j}\underset{\sim}{T}_{ijs}\}\}\}=$$
$$\{\{\{\underset{\sim}{T}_{111},\ \underset{\sim}{T}_{112},\ \ldots,\ \underset{\sim}{T}_{11r_1}\},\ \{\underset{\sim}{T}_{121},\ \underset{\sim}{T}_{122},\ \ldots,\ \underset{\sim}{T}_{12r_2}\},\ \ldots,$$
$$\{\underset{\sim}{T}_{1m_11},\ \underset{\sim}{T}_{1m_12},\ \ldots,\ \underset{\sim}{T}_{1m_1r_{m_1}}\}\},$$
$$\{\{\underset{\sim}{T}_{211},\ \underset{\sim}{T}_{212},\ \ldots,\ \underset{\sim}{T}_{21r_1}\},\ \{\underset{\sim}{T}_{221},\ \underset{\sim}{T}_{222},\ \ldots,\ \underset{\sim}{T}_{22r_2}\},\ \ldots,\qquad(2.45)$$
$$\{\underset{\sim}{T}_{2m_21},\ \underset{\sim}{T}_{2m_22},\ \ldots,\ \underset{\sim}{T}_{2m_2r_{m_2}}\}\},$$
$$\ldots,$$
$$\{\{\underset{\sim}{T}_{n11},\ \underset{\sim}{T}_{n12},\ \ldots,\ \underset{\sim}{T}_{n1r_1}\},\ \{\underset{\sim}{T}_{n21},\ \underset{\sim}{T}_{n22},\ \ldots,\ \underset{\sim}{T}_{n2r_2}\},\ \ldots,$$
$$\{\underset{\sim}{T}_{nm_n1},\ \underset{\sim}{T}_{nm_n2},\ \ldots,\ \underset{\sim}{T}_{nm_nr_{m_n}}\}\}\}.$$

На черзі, необхідно сформувати значення компонент $\underset{\sim}{T}_{ijs}$, для чого скористаємось наступними перетвореннями. За елементами матриці $F_{ij}^{'}$ відповідно до (2.46) будується вектор максимумів

$$FM_{ij} = \left\| fm_{ijq} \right\| =$$
$$\left\| fm_{ij1}, fm_{ij2}, ..., fm_{ijq}, ..., fm_{ijr_j} \right\| =$$
$$\left\| \bigvee_{s=1}^{r_j} f_{ijs1}^{'}, \bigvee_{s=1}^{r_j} f_{ijs2}^{'}, ..., \bigvee_{s=1}^{r_j} f_{ijsq}^{'}, ..., \bigvee_{s=1}^{r_j} f_{ijsr_j}^{'} \right\| = \quad (2.46)$$
$$\left\| \bigcup_{q=1}^{r_j} \bigvee_{s=1}^{r_j} f_{ijsq}^{'} \right\|,$$
$$(s,q = \overline{1,r_j}).$$

На основі FM_{ij} сформуємо матрицю функцій належності (ФН)

$$M_{ij} = \left\| \mu_{ijsq} \right\| = \begin{Vmatrix} \mu_{ij11} & \mu_{ij12} & \dots & \mu_{ij1q} & \dots & \mu_{ij1r_j} \\ \mu_{ij21} & \mu_{ij22} & \dots & \mu_{ij2q} & \dots & \mu_{ij2r_j} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \mu_{ijs1} & \mu_{ijs2} & \dots & \mu_{ijsq} & \dots & \mu_{ijsr_j} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \mu_{ijr_j1} & \mu_{ijr_j2} & \dots & \mu_{ijr_jq} & \dots & \mu_{ijr_jr_j} \end{Vmatrix}, \quad (2.47)$$

кожний елемент якої обчислюється відповідно до виразу

$$\mu_{ijsq} = f_{ijsq}^{'} / fm_{ijs},$$
$$(s,q = \overline{1,r_j}).$$

Використовуючи (2.47) визначимо набори нечітких термів (чисел) $\underset{\sim}{T}_{ijs}$ на основі виразу

$$\underset{\sim}{T}_{ijs} = \{ \bigcup_{q=1}^{r_j} \mu_{ijsq} / x_{ijsq} \} =$$
$$\{ \mu_{ijs1} / x_{ijs1}, \mu_{ijs2} / x_{ijs2}, ..., \mu_{ijsr_j} / x_{ijsr_j} \}, \quad (2.48)$$
$$(q = \overline{1,r_j}),$$

де

$$x_{ijsq} = N_{ijq}^{max} / N_{ijr_j}^{max}, \quad (q = \overline{1, r_j}). \tag{2.49}$$

Зазначимо що, нечіткі числа (НЧ) $\underset{\sim}{T}_{ijs}$ $(s = \overline{1, r_j})$ відповідно є інтерпретацією лінгвістичних висловлювань експертів LE_{ijk} $(k = \overline{1, r_j})$, що відображаються елементами підмножини $\mathbf{LE_{ij} \subseteq LE}$ (2.30).

Покажемо процес формування $\mathbf{T_{ij}}$ на конкретному прикладі, при $n = 3$ (тобто для кібератак з ІД $CA_1 = CA_{SN} = SN$, $CA_2 = CA_{DS} = DS$ та $CA_3 = CA_{SP} = SP$), $m_1 = m_3 = 2$, $m_2 = 3$, $r_1 = 5$, $r_2 = r_3 = 3$, де (2.45) можна визначити як:

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{3}} \mathbf{T_i}\} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{3}} \{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}} \mathbf{T_{ij}}\}\} =$$

$$\{\bigcup_{i=1}^{3} \{\bigcup_{j=1}^{m_i} \{\bigcup_{s=1}^{r_j} \underset{\sim}{T}_{ijs}\}\}\} =$$

$$\{\{\{\underset{\sim}{T}_{111}, \underset{\sim}{T}_{112}, \underset{\sim}{T}_{113}, \underset{\sim}{T}_{114}, \underset{\sim}{T}_{115}\},$$

$$\{\underset{\sim}{T}_{121}, \underset{\sim}{T}_{122}, \underset{\sim}{T}_{123}\}\},$$

$$\{\{\underset{\sim}{T}_{211}, \underset{\sim}{T}_{212}, \underset{\sim}{T}_{213}, \underset{\sim}{T}_{214}, \underset{\sim}{T}_{215}\}, \{\underset{\sim}{T}_{221}, \underset{\sim}{T}_{222}, \underset{\sim}{T}_{223}\},$$

$$\{\underset{\sim}{T}_{231}, \underset{\sim}{T}_{232}, \underset{\sim}{T}_{233}\}\},$$

$$\{\{\underset{\sim}{T}_{311}, \underset{\sim}{T}_{312}, \underset{\sim}{T}_{313}, \underset{\sim}{T}_{314}, \underset{\sim}{T}_{315}\},$$

$$\{\underset{\sim}{T}_{321}, \underset{\sim}{T}_{322}, \underset{\sim}{T}_{323}\}\} = \tag{2.50}$$

$$\{\{\{\underset{\sim}{OM}_{11}, \underset{\sim}{M}_{11}, \underset{\sim}{C}_{11}, \underset{\sim}{B}_{11}, \underset{\sim}{OB}_{11}\}, \{\underset{\sim}{M}_{12}, \underset{\sim}{CP}_{12}, \underset{\sim}{CT}_{12}\}\},$$

$$\{\{\underset{\sim}{OM}_{21}, \underset{\sim}{M}_{21}, \underset{\sim}{C}_{21}, \underset{\sim}{B}_{21}, \underset{\sim}{OB}_{21}\},$$

$$\{\underset{\sim}{H}_{22}, \underset{\sim}{C}_{22}, \underset{\sim}{B}_{22}\}, \{\underset{\sim}{M}_{23}, \underset{\sim}{C}_{23}, \underset{\sim}{B}_{23}\}\},$$

$$\{\{\underset{\sim}{OM}_{31}, \underset{\sim}{M}_{31}, \underset{\sim}{C}_{31}, \underset{\sim}{B}_{31}, \underset{\sim}{OB}_{31}\}, \{\underset{\sim}{M}_{32}, \underset{\sim}{C}_{32}, \underset{\sim}{B}_{32}\}\}\} =$$

$$\{\{\{\underset{\sim}{T}_{SNKBK1}, \underset{\sim}{T}_{SNKBK2}, \underset{\sim}{T}_{SNKBK3}, \underset{\sim}{T}_{SNKBK3}, \underset{\sim}{T}_{SNKBK5}\},$$

$$\{\underset{\sim}{T}_{SNBBK1},\ \underset{\sim}{T}_{SNBBK2},\ \underset{\sim}{T}_{SNBBK3}\}\},$$

$$\{\{\underset{\sim}{T}_{DSKOП1},\ \underset{\sim}{T}_{DSKOП2},\ \underset{\sim}{T}_{DSKOП3},\ \underset{\sim}{T}_{DSKOП4},\ \underset{\sim}{T}_{DSKOП5}\},$$

$$\{\underset{\sim}{T}_{DSCO31},\ \underset{\sim}{T}_{DSCO32},\ \underset{\sim}{T}_{DSCO33}\},$$

$$\{\underset{\sim}{T}_{DS3M31},\ \underset{\sim}{T}_{DS3M32},\ \underset{\sim}{T}_{DS3M33}\}\},$$

$$\{\{\underset{\sim}{T}_{SPKOП1},\ \underset{\sim}{T}_{SPKOП2},\ \underset{\sim}{T}_{SPKOП3},\ \underset{\sim}{T}_{SPKOП4},\ \underset{\sim}{T}_{SPKOП5}\},$$

$$\{\underset{\sim}{T}_{SPKПОА1},\ \underset{\sim}{T}_{SPKПОА2},\ \underset{\sim}{T}_{SPKПОА3}\}\}\} =$$

$$\{\{\{\underset{\sim}{OM}_{SNKBK},\ \underset{\sim}{M}_{SNKBK},\ \underset{\sim}{C}_{SNKBK},\ \underset{\sim}{Б}_{SNKBK},\ \underset{\sim}{OБ}_{SNKBK}\},$$

$$\{\underset{\sim}{M}_{SNBBK},\ \underset{\sim}{CP}_{SNBBK},\ \underset{\sim}{CT}_{SNBBK}\}\},$$

$$\{\{\underset{\sim}{OM}_{DSKOП},\ \underset{\sim}{M}_{DSKOП},\ \underset{\sim}{C}_{DSKOП},\ \underset{\sim}{Б}_{DSKOП},\ \underset{\sim}{OБ}_{DSKOП}\},$$

$$\{\underset{\sim}{H}_{DSCO3},\ \underset{\sim}{C}_{DSCO3},\ \underset{\sim}{B}_{DSCO3}\},$$

$$\{\underset{\sim}{M}_{DS3M3},\ \underset{\sim}{C}_{DS3M3},\ \underset{\sim}{Б}_{DS3M3}\}\},$$

$$\{\{\underset{\sim}{OM}_{SPKOП},\ \underset{\sim}{M}_{SPKOП},\ \underset{\sim}{C}_{SPKOП},\ \underset{\sim}{Б}_{SPKOП},\ \underset{\sim}{OБ}_{SPKOП}\},$$

$$\{\underset{\sim}{M}_{SPKПОА},\ \underset{\sim}{C}_{SPKПОА},\ \underset{\sim}{Б}_{SPKПОА}\}\}\}.$$

Відповідно до (2.50) при $n=1,\ (i=3$ тобто для кібератаки з ІД $CA_3 = CA_{SP} = SP)$,

$$j=1,\ r_1=5 \text{ для } \{\underset{\sim}{T}_{311},\ \underset{\sim}{T}_{312},\ \underset{\sim}{T}_{313},\ \underset{\sim}{T}_{314},\ \underset{\sim}{T}_{315}\}$$

та

$$j=2,\ r_2=3 \text{ для } \{\underset{\sim}{T}_{321},\ \underset{\sim}{T}_{322},\ \underset{\sim}{T}_{323}\}$$

сформуємо $\mathbf{T_{31}} \subseteq \mathbf{T}$ та $\mathbf{T_{32}} \subseteq \mathbf{T}$ тобто:

$$\mathbf{T_{31}} = \{\bigcup_{s=1}^{5} \underset{\sim}{T}_{31s}\} =$$

$$\{\underset{\sim}{T}_{311},\ \underset{\sim}{T}_{312},\ \underset{\sim}{T}_{313},\ \underset{\sim}{T}_{314},\ \underset{\sim}{T}_{315}\} =$$

$$\{\underset{\sim}{T}_{SPKOП1},\ \underset{\sim}{T}_{SPKOП2},\ \underset{\sim}{T}_{SPKOП3},\ \underset{\sim}{T}_{SPKOП4},\ \underset{\sim}{T}_{SPKOП5}\} =$$

$$\{\underset{\sim}{OM}_{31},\ \underset{\sim}{M}_{31},\ \underset{\sim}{C}_{31},\ \underset{\sim}{Б}_{31},\ \underset{\sim}{OБ}_{31}\},$$

$$(s=\overline{1,5})$$

та

$$\mathbf{T_{32}} = \{\bigcup_{s=1}^{3} \underset{\sim}{T}_{32s}\} =$$

$$\{\underset{\sim}{T}_{321},\ \underset{\sim}{T}_{322},\ \underset{\sim}{T}_{323}\} =$$

$$\{\underset{\sim}{T}_{SPKPOA1},\ \underset{\sim}{T}_{SPKPOA2},\ \underset{\sim}{T}_{SPKPOA3}\} =$$

$$\{\underset{\sim}{M}_{32},\ \underset{\sim}{C}_{32},\ \underset{\sim}{Б}_{32}\},$$

$$(s = \overline{1,3}),$$

де:

- $\underset{\sim}{T}_{311} = \underset{\sim}{T}_{SPKOP1} = \underset{\sim}{OM}_{31}$, $\underset{\sim}{T}_{312} = \underset{\sim}{T}_{SPKOP2} = \underset{\sim}{M}_{31}$, $\underset{\sim}{T}_{313} = \underset{\sim}{T}_{SPKOP3} = \underset{\sim}{C}_{31}$, $\underset{\sim}{T}_{314} = \underset{\sim}{T}_{SPKOP4} = \underset{\sim}{Б}_{31}$ та $\underset{\sim}{T}_{315} = \underset{\sim}{T}_{SPKOP5} = \underset{\sim}{OБ}_{31}$ відповідно є НЧ $\underset{\sim}{OM}_{31}$, $\underset{\sim}{M}_{31}$, $\underset{\sim}{C}_{31}$, $\underset{\sim}{Б}_{31}$ та $\underset{\sim}{OБ}_{31}$, які інтерпретують висловлювання експерта, що відображаються за допомогою $LE_{SPKOP1} = "OM"$, $LE_{SPKOP2} = "M"$, $LE_{SPKOP3} = "C"$, $LE_{SPKOP4} = "Б"$ та $LE_{SPKOP5} = "OБ"$,

а також

- $\underset{\sim}{T}_{321} = \underset{\sim}{T}_{SPKPOA1} = \underset{\sim}{M}_{32}$, $\underset{\sim}{T}_{322} = \underset{\sim}{T}_{SPKPOA2} = \underset{\sim}{C}_{32}$ та $\underset{\sim}{T}_{323} = \underset{\sim}{T}_{SPKPOA3} = \underset{\sim}{Б}_{32}$ відповідно є НЧ $\underset{\sim}{M}_{32}$, $\underset{\sim}{C}_{32}$ та $\underset{\sim}{Б}_{32}$, які інтерпретують висловлювання експерта, що відображаються шляхом $LE_{SPKPOA1} = "M"$, $LE_{SPKPOA2} = "C"$ та $LE_{SPKPOA3} = "Б"$.

Далі, на основі (2.46) побудуємо вектор максимумів за відповідними рядками $F'_{31} = F'_{SPKOP}$ та $F'_{32} = F'_{SPKPOA}$, тобто

$$FM_{SPKOP} = \left\| fm_{SPKOPs} \right\| =$$

$$\left\| fm_{SPKOP1}, fm_{SPKOP2}, fm_{SPKOP3}, fm_{SPKOP4}, fm_{SPKOP5} \right\| =$$

$$\|7{,}3;\ 6{,}6;\ 6{,}3;\ 5;\ 7{,}3\|$$

та

$$FM_{SPKPOA} = \left\| fm_{SPKPOAs} \right\| =$$

$$\left\| fm_{SPKPOA1}, fm_{SPKPOA2}, fm_{SPKPOA3} \right\| =$$

$$\|5{,}3;\ 4;\ 4{,}2\|.$$

На основі $FM_{SPKOП}$ та $FM_{SPKПОА}$ за виразом (2.47) сформуємо матрицю функцій належності $M_{SPKOП}$ та $M_{SPKПОА}$ отримавши таким чином:

$$M_{SPKOП} = \left\| \mu_{SPKOПsq} \right\| = \left\| \begin{array}{ccccc} 1 & 0,3 & 0 & 0 & 0 \\ 0,6 & 1 & 0,2 & 0 & 0 \\ 0 & 0,4 & 1 & 0,3 & 0 \\ 0 & 0 & 0,6 & 1 & 0,7 \\ 0 & 0 & 0 & 0,6 & 1 \end{array} \right\|$$

та

$$M_{SPKПОА} = \left\| \mu_{SPKПОА\,sq} \right\| = \left\| \begin{array}{ccc} 1 & 0,2 & 0 \\ 0,5 & 1 & 0,7 \\ 0 & 0,5 & 1 \end{array} \right\|,$$

де

$$\mu_{SPKOПsq} = f'_{SPKOПsq} / fm_{SPKOПs},\ (s,q = \overline{1,5})$$ та

$$\mu_{SPKПОАsq} = f'_{SPKПОАsq} / fm_{SPKПОАs},\ (s,q = \overline{1,3}).$$

Обчислених на основі виразу (2.47) $\mu_{SPKOПsq}$, $\mu_{SPKПОАsq}$ та виразу (2.49) $x_{SPKOПsq}$, $x_{SPKПОАsq}$ визначимо набори нечітких термів $\underset{\sim}{T}_{SPKOП}$, $\underset{\sim}{T}_{SPKПОА}$ за формулою (2.48), тобто

$$\underset{\sim}{T}_{31s} = \{ \mu_{31s1} / x_{31s1}, \mu_{31s2} / x_{31s2}, \mu_{31s3} / x_{31s3}, \mu_{31s4} / x_{31s4},$$
$$\mu_{31s5} / x_{31s5} \} <=>$$
$$\underset{\sim}{T}_{SPKOПs} = \{ \mu_{SPKOПs1} / x_{SPKOПs1}, \mu_{SPKOПs2} / x_{SPKOПs2}, \mu_{SPKOПs3} / x_{SPKOПs3},$$
$$\mu_{SPKOПs4} / x_{SPKOПs4}, \mu_{SPKOПs5} / x_{SPKOПs5} \},$$
$$(s = \overline{1,5})$$

та

$$\underset{\sim}{T}_{32s} = \{ \mu_{32s1} / x_{32s1},\ \mu_{32s2} / x_{32s2},\ \mu_{32s3} / x_{32s3} \} <=>$$
$$\underset{\sim}{T}_{SPKПОАs} = \{ \mu_{SPKПОАs1} / x_{SPKПОАs1}, \mu_{SPKПОАs2} / x_{SPKПОАs2},$$
$$\mu_{SPKПОАs3} / x_{SPKПОАs3} \},$$
$$(s = \overline{1,3}),$$

де відповідно до (2.49)

$$x_{SPKOПsq} = N^{max}_{SPKOПq} / N^{max}_{SPKOПr_j} \ (q = \overline{1,5}) \text{ або}$$

$$\{\bigcup_{q=1}^{5} x_{SPKOПsq} \} = \{0{,}008;\ 0{,}063;\ 0{,}25;\ 0{,}5;\ 1\},$$

а також

$$x_{SPKПOAsq} = N^{max}_{SPKПOAq} / N^{max}_{SPKПOAr_j}, \ (q = \overline{1,3}) \text{ або}$$

$$\{\bigcup_{q=1}^{3} x_{SPKПOAsq}\} = \{0{,}01;\ 0{,}1;\ 1\}.$$

Таким чином, отримані члени підмножини $\mathbf{T_{31}}$, $\mathbf{T_{32}}$ (числова форма) відповідно є відображенням членів підмножини $\mathbf{LE_{31}}$, $\mathbf{LE_{32}}$ (2.30) (лінгвістична форма) та представляються у наступному вигляді:

$$\underset{\sim}{T}_{311} = \underset{\sim}{T}_{SPKOП\,1} = \underset{\sim}{OM}_{31} =$$
$$\{1/0{,}008;\ 0{,}3/0{,}063;\ 0/0{,}25;\ 0/0{,}5;\ 0/1\},$$

$$\underset{\sim}{T}_{312} = \underset{\sim}{T}_{SPKOП2} = \underset{\sim}{M}_{31} =$$
$$\{0{,}6/0{,}008\ ;\ 1/0{,}063;\ 0{,}2/0{,}25;\ 0/0{,}5;\ 0/1\},$$

$$\underset{\sim}{T}_{313} = \underset{\sim}{T}_{SPKOП3} = \underset{\sim}{C}_{31} =$$
$$\{0/0{,}008;\ 0{,}4/0{,}063;\ 1/0{,}25;\ 0{,}3\ /0{,}5;\ 0/1\},$$

$$\underset{\sim}{T}_{314} = \underset{\sim}{T}_{SPKOП4} = \underset{\sim}{B}_{31} =$$
$$\{0/0{,}008;\ 0/0{,}063;\ 0{,}6/0{,}25;\ 1/0{,}5;\ 0{,}7/1\},$$

$$\underset{\sim}{T}_{315} = \underset{\sim}{T}_{SPKOП\,5} = \underset{\sim}{OB}_{31} =$$
$$\{0/0{,}008;\ 0/0{,}063;\ 0/0{,}25;\ 0{,}6/0{,}5;\ 1/1\} \text{ та}$$

$$\underset{\sim}{T}_{321} = \underset{\sim}{T}_{SPKПOA1} = \underset{\sim}{M}_{32} = \{1/0{,}01;\ 0{,}2/0{,}1;\ 0/1\},$$

$$\underset{\sim}{T}_{322} = \underset{\sim}{T}_{SPKПOA2} = \underset{\sim}{C}_{32} = \{0{,}5/0{,}01;\ 1/0{,}1;\ 0{,}7/1\},$$

$$\underset{\sim}{T}_{323} = \underset{\sim}{T}_{SPKПOA3} = \underset{\sim}{B}_{32} = \{0/0{,}01;\ 0{,}5/0{,}1;\ 0/1\}.$$

Побудова нечітких чисел еталонного середовища

Етап 5 – побудова НЧ еталонного середовища. Для реалізації цього етапу скористаємося підмножиною нечітких (лінгвістичних)

еталонів $\mathbf{T}_{\mathbf{ij}}^{\mathbf{e}}$ (див. (2.13)), кожна з яких відображає характерні судження експерта (див. етап 1 в п. 2.1) відносно аномальності стану параметра P_{ij}.

Формування нечітких еталонів ґрунтується на перетворенні НЧ (2.48) із підмножини $\mathbf{T}_{\mathbf{ij}} \subseteq \mathbf{T}$ та реалізується шляхом трьох кроків.

Крок 1. Перетворення нечітких термів (2.48) таким чином, щоб для всіх $\underset{\sim}{T}_{ijs}$ було справедливе відношення порядку, тобто

$$\forall x_{ijsq} : x_{ijsq} < x_{ijsq+1} \ \ (q = \overline{1, r_j - 1}).$$

Крок 2. У кожному $\underset{\sim}{T}_{ijs}$ здійснюється поглинання компонентом

$$0/x_{ijs}^{min} \text{ та } 0/x_{ijs}^{max}$$

низки інших компонентів відповідно до виразів

$$x_{ijs}^{min} = \bigvee_{\substack{q=1 \\ при\ U1}}^{M-1} x_{ijsq} \text{ та } x_{ijs}^{max} = \bigwedge_{\substack{q=M \\ при\ U2}}^{r_j} x_{ijsq},$$

де

$$U_1 \overset{\text{def}}{=} \forall x_{ijsq} < x_{ijsM} : \mu_{ijsq} = 0, \ U_2 \overset{\text{def}}{=} \forall x_{ijsq} > x_{ijsM} : \mu_{ijsq} = 0,$$

а x_{ijsM} та M – відповідно мода $\underset{\sim}{T}_{ijs}$ та її порядковий номер.

Далі, з урахуванням цих перетворень та (2.48), визначимо набір проміжних термів у вигляді

$$\begin{aligned} \underset{\sim}{T}'_{ijs} = \{ \mu_{ijs\beta} / x_{ijs\beta}, ..., \bigcup_{q=\beta+1}^{r_j-\gamma} \mu_{ijsq} / x_{ijsq}, ..., \mu_{ijsr_j-\gamma+1} / x_{ijsr_j-\gamma+1} \} = \\ \{ \mu_{ijs\beta} / x_{ijs\beta}, \mu_{ijs\beta+1} / x_{ijs\beta+1}, ..., \\ \mu_{ijsr_j-\gamma} / x_{ijsr_j-\gamma}, \mu_{ijsr_j-\gamma+1} / x_{ijsr_j-\gamma+1} \}, \end{aligned} \tag{2.51}$$

де

$$\mu_{ijs\beta} / x_{ijs\beta} = 0 / x_{ijs\beta} = 0/x_{ijs}^{min} \text{ та}$$

$$\mu_{ijsr_j-\gamma+1} / x_{ijsr_j-\gamma+1} = 0 / x_{ijsr_j-\gamma+1} = 0/x_{ijs}^{max},$$

а β та γ – кількість $0 / x_{ijsq}$ що поглинаються відповідно ліворуч та праворуч від $x_{ijs(M)}$.

Таким чином, формуються підмножини еталонів

$$\underset{\sim}{T}^{e}_{ijs} = \{ \bigcup_{q=1}^{r_{js}} \mu^{e}_{ijsq} \,/\, x^{e}_{ijsq} \} =$$

$$\{ \mu^{e}_{ijs1} \,/\, x^{e}_{ijs1}, \mu^{e}_{ijs2} \,/\, x^{e}_{ijs2}, \ldots, \mu^{e}_{ijsr_{js}-1} \,/\, x^{e}_{ijsr_{js}-1}, \mu^{e}_{ijsr_{js}} \,/\, x^{e}_{ijsr_{js}} \}, \quad (2.52)$$

$$(q = \overline{1, r_{js}}),$$

де

$$\mu^{e}_{ijs1} \,/\, x^{e}_{ijs1} = \mu_{ijs\beta} \,/\, x_{ijs\beta}, \;\; \mu^{e}_{ijs2} \,/\, x^{e}_{ijs2} = \mu_{ijs\beta+1} \,/\, x_{ijs\beta+1},$$

$$\ldots,$$

$$\mu^{e}_{ijsr_{js}-1} \,/\, x^{e}_{ijsr_{js}-1} = \mu_{ijsr_j-\gamma} \,/\, x_{ijsr_j-\gamma}, \;\; \mu^{e}_{ijsr_{js}} \,/\, x^{e}_{ijsr_{js}} = \mu_{ijsr_j-\gamma+1} \,/\, x_{ijsr_j-\gamma+1},$$

r_{js} $(s = \overline{1, r_j})$ – кількість компонент в $\underset{\sim}{T}^{e}_{ijs}$.

Крок 3. Якщо при реалізації другого кроку для (2.51)

$$\exists \, \underset{\sim}{T}^{'}_{ijs} : \{0/x^{\,min}_{ijs}\} \in \varnothing \text{ або}$$

$$\exists \, \underset{\sim}{T}^{'}_{ijs} : \{0/x^{\,max}_{ijs}\} \in \varnothing$$

$$(\text{тобто } \mu_{ijs\beta} \neq 0, \;\; \mu_{ijsr_j-\gamma+1} \neq 0),$$

то для таких термів подальше формування підмножини $\underset{\sim}{T}^{e}_{ijs}$ здійснюється шляхом розширення $\underset{\sim}{T}^{'}_{ijs}$ за допомогою введення додаткових

$$\mu_{ijs\beta-1} \,/\, x_{ijs\beta-1} \text{ та } \mu_{ijsr_j-\gamma+2} \,/\, x_{ijsr_j-\gamma+2}$$

після чого компоненти НЧ переіндексовуються (розпочинаючи з $q = 1$).

З урахуванням цього, набори проміжних термів будуть мати наступний вигляд

$$\underset{\sim}{T}^{'}_{ijs} = \{ \mu_{ijs\beta-1} \,/\, x_{ijs\beta-1}, \mu_{ijs\beta} \,/\, x_{ijs\beta}, \ldots, \bigcup_{q=\beta+1}^{r_j-\gamma} \mu_{ijsq} \,/\, x_{ijsq}, \ldots,$$

$$\mu_{ijsr_j-\gamma+1} \,/\, x_{ijsr_j-\gamma+1}, \mu_{ijsr_j-\gamma+2} \,/\, x_{ijsr_j-\gamma+2} \} =$$

$$\{ \mu_{ijs\beta-1} \,/\, x_{ijs\beta-1}, \mu_{ijs\beta} \,/\, x_{ijs\beta}, \ldots, \mu_{ijsr_j-\gamma+1} \,/\, x_{ijsr_j-\gamma+1}, \mu_{ijsr_j-\gamma+2} \,/\, x_{ijsr_j-\gamma+2} \},$$

де $x_{ijs\beta-1} = x_{ijs\beta}$, $x_{ijsr_j-\gamma+2} = x_{ijsr_j-\gamma+1}$, а $\mu_{ijs\beta-1} = \mu_{ijsr_j-\gamma+2} = 0$.

Таким чином, компоненти підмножини еталонів $\underset{\sim}{T}^{e}_{ijs}$ у (2.52) будуть визначатися як

$$\mu^e_{ijs1} / x^e_{ijs1} = \mu_{ijs\beta-1} / x_{ijs\beta-1},\ \mu^e_{ijs2} / x^e_{ijs2} = \mu_{ijs\beta} / x_{ijs\beta},$$

$$\ldots,$$

$$\mu^e_{ijsr_{js}-1} / x^e_{ijsr_{js}-1} = \mu_{ijsr_j-\gamma+1} / x_{ijsr_j-\gamma+1},\ \mu^e_{ijsr_{js}} / x^e_{ijsr_{js}} = \mu_{ijsr_j-\gamma+2} / x_{ijsr_j-\gamma+2}.$$

Розглянемо процес формування НЧ еталонного підсередовища ($\mathbf{T^e_i}$) на конкретному прикладі. Відповідно до виразу (2.13) при $n=1$ ($i=3$, тобто для кібератак з ІД $CA_3 = CA_{SP} = SP$),

$$j=1,\ r_1=5 \text{ для } \{\underset{\sim}{T}^e_{311},\ \underset{\sim}{T}^e_{312},\ \underset{\sim}{T}^e_{313},\ \underset{\sim}{T}^e_{314},\ \underset{\sim}{T}^e_{315}\} \text{ та при}$$

$$j=2,\ r_2=3 \text{ для } \{\underset{\sim}{T}_{321},\ \underset{\sim}{T}_{322},\ \underset{\sim}{T}_{323}\}$$

сформуємо $\mathbf{T^e_{31}} \subseteq \mathbf{T^e}$ та $\mathbf{T^e_{32}} \subseteq \mathbf{T^e}$ тобто

$$\mathbf{T^e_{31}} = \{\bigcup_{s=1}^{5} \underset{\sim}{T}^e_{31s}\} =$$

$$\{\underset{\sim}{T}^e_{311},\ \underset{\sim}{T}^e_{312},\ \underset{\sim}{T}^e_{313},\ \underset{\sim}{T}^e_{314},\ \underset{\sim}{T}^e_{315}\} =$$

$$\{\underset{\sim}{T}^e_{SPKOП1},\ \underset{\sim}{T}^e_{SPKOП2},\ \underset{\sim}{T}^e_{SPKOП3},\ \underset{\sim}{T}^e_{SPKOП4},\ \underset{\sim}{T}^e_{SPKOП5}\} =$$

$$\{\underset{\sim}{OM}^e_{31},\ \underset{\sim}{M}^e_{31},\ \underset{\sim}{C}^e_{31},\ \underset{\sim}{Б}^e_{31},\ \underset{\sim}{OБ}^e_{31}\},$$

$$(s=\overline{1,5}) \text{ та}$$

$$\mathbf{T^e_{32}} = \{\bigcup_{s=1}^{3} \underset{\sim}{T}^e_{32s}\} =$$

$$\{\underset{\sim}{T}_{321},\ \underset{\sim}{T}_{322},\ \underset{\sim}{T}_{323}\} =$$

$$\{\underset{\sim}{T}^e_{SPKПOA1},\ \underset{\sim}{T}^e_{SPKПOA2},\ \underset{\sim}{T}^e_{SPKПOA3}\} =$$

$$\{\underset{\sim}{M}^e_{32},\ \underset{\sim}{C}^e_{32},\ \underset{\sim}{Б}^e_{32}\},$$

$$(s=\overline{1,3}),$$

де члени підмножини $\mathbf{T^e_{31}}$ – $\underset{\sim}{OM}^e_{31},\ \underset{\sim}{M}^e_{31},\ \underset{\sim}{C}^e_{31},\ \underset{\sim}{Б}^e_{31},\ \underset{\sim}{OБ}^e_{31}$ та $\mathbf{T^e_{32}}$ – $\underset{\sim}{M}^e_{32},\ \underset{\sim}{C}^e_{32},\ \underset{\sim}{Б}^e_{32}$ є НЧ еталонного підсередовища ($\mathbf{T^e_i} = \mathbf{T^e_3} = \mathbf{T^e_{SP}}$).

Крок 1. Перетворимо нечіткі терми

$$\underset{\sim}{OM}_{31},\ \underset{\sim}{M}_{31},\ \underset{\sim}{C}_{31},\ \underset{\sim}{Б}_{31},\ \underset{\sim}{OБ}_{31} \text{ та}$$

$$\underset{\sim}{M}_{32},\ \underset{\sim}{C}_{32},\ \underset{\sim}{Б}_{32}$$

таким чином, щоб для всіх $\underset{\sim}{T}_{31s}$ та $\underset{\sim}{T}_{32s}$ було справедливе відношення порядку, тобто

$$\forall x_{31sq} : x_{31sq} < x_{31sq+1},\ (q = \overline{1,4}) \text{ та}$$

$$\forall x_{32sq} : x_{32sq} < x_{32sq+1},\ (q = \overline{1,2}).$$

Якщо за компоненти таких термів використовувати конкретні значення отримані в прикладі етапу 4, то для них таке відношення буде істинним.

Так, наприклад, для $O\underset{\sim}{M}_{31}$ це

$$x_{3111} < x_{3112} < x_{3113} < x_{3114} < x_{3115} =$$
$$0{,}008 < 0{,}063 < 0{,}25 < 0{,}5 < 1,$$

для $\underset{\sim}{M}^{e}_{32}$ це

$$x_{3211} < x_{3212} < x_{3213} =$$
$$0{,}01 < 0{,}1 < 1.$$

Крок 2. Для $O\underset{\sim}{M}_{31}$ (де мода $x_{311M} = x_{3111} = 0{,}008$, а її порядковий номер $M = 1$) при умові U_2 (тобто $\mu_{3113} = \mu_{3114} = \mu_{3115} = 0$) здійснюється поглинання одним компонентом $0/x^{max}_{311}$ низки інших відповідно до виразу

$$x^{max}_{311} = x_{3113} \wedge x_{3114} \wedge x_{3115} =$$
$$0{,}25 \wedge 0{,}5 \wedge 1 = 0{,}25\ \ (q = \overline{1,5}).$$

Таким чином,

$$\mu_{3113} / x_{3113} = 0 / 0{,}25,\ \mu_{3114} / x_{3114} =$$
$$0 / 0{,}5 \text{ та } \mu_{3115} / x_{3115} = 0 / 1$$

поглинаються компонентом

$$\mu_{3113} / x_{3113} = 0 / 0{,}25.$$

Аналогічним чином, для $\underset{\sim}{M}_{31}$ (де $x_{312M} = x_{3122} = 0{,}063$, а $M = 2$) при умові U_2 (тобто $\mu_{3124} = \mu_{3125} = 0$) компонент $0/x^{max}_{312} = \mu_{3124} / x_{3124} = 0 / 0{,}5$ відносно виразу

$$x^{max}_{312} = x_{3124} \wedge x_{3125} = 0{,}5 \wedge 1 = 0{,}5,\ (q = \overline{2,5})$$

поглинає компоненти

$$\mu_{3124} / x_{3124} = 0 / 0{,}5 \text{ та}$$

$$\mu_{3125} \ / \ x_{3125} = 0 / 1.$$

Далі видно, що для НЧ $\underset{\sim}{C}_{31}$ умова U_1 та U_2 не виконується і тому операція поглинання не здійснюється.

Аналогічним чином, для НЧ $\underset{\sim}{M}^{e}_{32}$, $\underset{\sim}{C}^{e}_{32}$, $\underset{\sim}{Б}^{e}_{32}$ умова U_1 та U_2 також не виконується і тому операція поглинання не здійснюється.

Для $\underset{\sim}{Б}_{31}$ (де $x_{314M} = x_{3144} = 0{,}5, \ \ M = 4$) при умові U_1 ($\mu_{3141} = \mu_{3142} = 0$) компонент $0/x^{min}_{314} = \mu_{3142} \ / \ x_{3142} = 0/0{,}063$ відповідно до виразу

$$x^{min}_{314} = x_{3141} \vee x_{3142} = 0{,}008 \vee 0{,}063 = 0{,}063, \ (q = \overline{1,3})$$

поглинає компоненти

$$\mu_{3141} \ / \ x_{3141} = 0/0{,}008 \ \text{ та}$$

$$\mu_{3142} \ / \ x_{3142} = 0 / 0{,}063.$$

Аналогічно, для $Q\underset{\sim}{Б}_{31}$ ($x_{315M} = x_{3155} = 1, \ \ M = 5$) при умові U_1 ($\mu_{3151} = \mu_{3152} = \mu_{3153} = 0$) компонент $0/x^{min}_{315} = \mu_{3153} \ / \ x_{3153} = 0/0{,}25$ відповідно до виразу

$$x^{min}_{315} = x_{3151} \vee x_{3152} \vee x_{3153} =$$

$$0{,}008 \vee 0{,}063 \vee 0{,}25 = 0{,}25, \ (q = \overline{1,4})$$

поглинає компоненти

$$\mu_{3151} \ / \ x_{3151} = 0{,}008, \ \ \mu_{3152} \ / \ x_{3152} = 0/0{,}063 \ \text{ та}$$

$$\mu_{3153} \ / \ x_{3153} = 0/0{,}25.$$

Далі, з урахуванням цих перетворень та (2.51) визначимо набір проміжних термів у вигляді:

$$\underset{\sim}{T}'_{311} = \underset{\sim}{T}'_{SPKOП1} = O\underset{\sim}{M}'_{31} =$$

$$\{ \mu_{3111} / x_{3111} \ , \mu_{3112} / x_{3112} \ , \mu_{3113} / x_{3113} \} =$$

$$\{1/0{,}008; \ 0{,}3/0{,}063; \ 0/0{,}25\},$$

$$\underset{\sim}{T}'_{312} = \underset{\sim}{T}'_{SPKOП2} = \underset{\sim}{M}'_{31} =$$

$$\{ \mu_{3121} / x_{3121} \ , \mu_{3122} / x_{3122} \ , \mu_{3123} / x_{3123} \ , \mu_{3124} / x_{3124} \} =$$

$$\{0{,}6/0{,}008; \ 1/0{,}063; \ 0{,}2/0{,}25; \ 0/0{,}5\},$$

$$\underset{\sim}{T}'_{313} = \underset{\sim}{T}'_{SPKOП3} = \underset{\sim}{C}'_{31} =$$

$$\{ \mu_{3131} / x_{3131} \ , \mu_{3132} / x_{3132} \ , \mu_{3133} / x_{3133} \ , \mu_{3134} / x_{3134} \ , \mu_{3135} / x_{3135} \} =$$

$$\{0/0{,}008;\ 0{,}4/0{,}063;\ 1/0{,}25;\ 0{,}3\ /0{,}5;\ 0/1\},$$

$$\underset{\sim}{T}'_{314} = \underset{\sim}{T}'_{SPKOP4} = \underset{\sim}{Б}'_{31} =$$

$$\{\mu_{3142} / x_{3142}, \mu_{3143} / x_{3143}, \mu_{3144} / x_{3144}, \mu_{3145} / x_{3145}\} =$$

$$\{0/0{,}063;\ 0{,}6/0{,}25;\ 1/0{,}5;\ 0{,}7/1\},$$

$$\underset{\sim}{T}'_{315} = \underset{\sim}{T}'_{SPKOP5} = \underset{\sim}{QБ}'_{31} =$$

$$\{\mu_{3153} / x_{3153}, \mu_{3154} / x_{3154}, \mu_{3155} / x_{3155}\} =$$

$$\{0/0{,}25;\ 0{,}6/0{,}5;\ 1/1\}$$

та

$$\underset{\sim}{T}'_{321} = \underset{\sim}{T}'_{SPKPOA1} = \underset{\sim}{M}'_{32} = \{\mu_{3211} / x_{3211}, \mu_{3212} / x_{3212}, \mu_{3213} / x_{3213}\} =$$

$$\{1/0{,}01;\ 0{,}2/0{,}1;\ 0/1\},$$

$$\underset{\sim}{T}'_{322} = \underset{\sim}{T}'_{SPKPOA2} = \underset{\sim}{C}'_{32} = \{\mu_{3221} / x_{3221}, \mu_{3222} / x_{3222}, \mu_{3223} / x_{3223}\} =$$

$$\{0{,}5/0{,}01;\ 1/0{,}1;\ 0{,}7/1\},$$

$$\underset{\sim}{T}'_{323} = \underset{\sim}{T}'_{SPKPOA3} = \underset{\sim}{Б}'_{32} = \{\mu_{3231} / x_{3231}, \mu_{3232} / x_{3232}, \mu_{3233} / x_{3233}\} =$$

$$\{0/0{,}01;\ 0{,}5/0{,}1;\ 1/1\}.$$

Оскільки,

$$\mu_{3131} / x_{3131} = 0 / x_{313}^{min} = 0 / x_{3131} \text{ та}$$

$$\mu_{3135} / x_{3135} = 0 / x_{313}^{max} = 0 / x_{2135},$$

то після кроку 2 для $\underset{\sim}{C}'_{31}$ відповідно до (2.52) формуються еталонні значення, тобто:

$$\underset{\sim}{T}^{e}_{313} = \underset{\sim}{T}^{e}_{SPKOP3} = \underset{\sim}{C}^{e}_{31} =$$

$$\{\mu^{e}_{3131} / x^{e}_{3131}, \mu^{e}_{3132} / x^{e}_{3132}, \mu^{e}_{3133} / x^{e}_{3133}, \mu^{e}_{3134} / x^{e}_{3134}, \mu^{e}_{3135} / x^{e}_{3135}\} =$$

$$\{0/0{,}008;\ 0{,}4/0{,}063;\ 1/0{,}25;\ 0{,}3\ /0{,}5;\ 0/1\},$$

де:

- $\mu^{e}_{3131} / x^{e}_{3131} = \mu_{3131} / x_{3131}$,
- $\mu^{e}_{3132} / x^{e}_{3132} = \mu_{3132} / x_{3132}$,
- $\mu^{e}_{3133} / x^{e}_{3133} = \mu_{3133} / x_{3133}$,
- $\mu^{e}_{3134} / x^{e}_{3134} = \mu_{3134} / x_{3134}$,
- $\mu^{e}_{3135} / x^{e}_{3135} = \mu_{3135} / x_{3135}$.

Крок 3. При реалізації другого кроку у виразі (2.51) для набору проміжних термів $\underset{\sim}{OM}'_{31}$ та $\underset{\sim}{M}'_{31}$

$$\exists\, \underset{\sim}{T}'_{311} : \{0/x_{311}^{min}\} \in \varnothing \text{ та}$$

$$\exists\, \underset{\sim}{T}'_{312} : \{0/x_{312}^{min}\} \in \varnothing$$

(тобто $\mu_{3111} = 1 \neq 0$ та $\mu_{3121} = 0{,}6 \neq 0$),

а для $\underset{\sim}{Б}'_{31}$ і $\underset{\sim}{OБ}'_{31}$

$$\exists\, \underset{\sim}{T}'_{314} : \{0/x_{314}^{max}\} \in \varnothing \text{ та}$$

$$\exists\, \underset{\sim}{T}'_{315} : \{0/x_{315}^{max}\} \in \varnothing$$

(тобто $\mu_{3145} = 0{,}7 \neq 0$ та $\mu_{3155} = 1 \neq 0$),

то формування підмножин $\underset{\sim}{T}^{e}_{311}$, $\underset{\sim}{T}^{e}_{312}$ і $\underset{\sim}{T}^{e}_{314}$, $\underset{\sim}{T}^{e}_{315}$ здійснимо за рахунок розширення $\underset{\sim}{T}'_{311}$, $\underset{\sim}{T}'_{312}$ і $\underset{\sim}{T}'_{314}$, $\underset{\sim}{T}'_{315}$ (див. (2.51)) шляхом введення додаткових

$$\mu_{311\beta-1} / x_{311\beta-1} = 0 / 0{,}008,\ \mu_{312\beta-1} / x_{312\beta-1} = 0 / 0{,}008 \text{ та}$$

$$\mu_{314 r_j - \gamma + 2} / x_{314 r_j - \gamma + 2} = 0 / 1,\ \mu_{315 r_j - \gamma + 2} / x_{315 r_j - \gamma + 2} = 0 / 1$$

відповідно, після чого в НЧ здійснюється переіндексація компонент розпочинаючи з першої.

Аналогічним чином, для набору проміжних термів $\underset{\sim}{M}'_{32}$ та $\underset{\sim}{C}'_{32}$

$$\exists\, \underset{\sim}{T}'_{321} : \{0/x_{321}^{min}\} \in \varnothing \text{ та}$$

$$\exists\, \underset{\sim}{T}'_{322} : \{0/x_{322}^{min}\} \in \varnothing$$

(тобто $\mu_{3211} = 1 \neq 0$ та $\mu_{3221} = 0{,}5 \neq 0$),

а також для $\underset{\sim}{C}'_{32}$ і $\underset{\sim}{Б}'_{32}$

$$\exists\, \underset{\sim}{T}'_{322} : \{0/x_{322}^{max}\} \in \varnothing \text{ та}$$

$$\exists\, \underset{\sim}{T}'_{323} : \{0/x_{323}^{max}\} \in \varnothing$$

(тобто $\mu_{3223} = 0{,}7 \neq 0$ та $\mu_{3233} = 1 \neq 0$),

то формування підмножин $\underset{\sim}{T}^{e}_{321}$, $\underset{\sim}{T}^{e}_{322}$ і $\underset{\sim}{T}^{e}_{323}$ здійснимо за рахунок розширення $\underset{\sim}{T}'_{321}$, $\underset{\sim}{T}'_{322}$ і $\underset{\sim}{T}'_{323}$ (див. (2.51)) шляхом введення додаткових

$$\mu_{321\beta-1} / x_{321\beta-1} = 0 / 0{,}01,\ \ \mu_{322\beta-1} / x_{322\beta-1} = 0 / 0{,}01,$$

$$\mu_{322r_j-\gamma+2} / x_{322\,r_j-\gamma+2} = 0 / 1 \text{ та } \mu_{323r_j-\gamma+2} / x_{323\,r_j-\gamma+2} = 0 / 1$$

відповідно, після чого в НЧ здійснюється переіндексація компонент.

З урахуванням цього, набір проміжних термів для $\underset{\sim}{OM}'_{31}$ та $\underset{\sim}{M}'_{32}$ буде мати наступний вигляд

$$\underset{\sim}{T}'_{311} = \underset{\sim}{T}'_{SPKOPI} = \underset{\sim}{OM}'_{31} =$$

$$\{\mu_{3111} / x_{3111}, \mu_{3112} / x_{3112}, \mu_{3113} / x_{3113}, \mu_{3114} / x_{3114}\} =$$

$$\{0/0{,}008;\ 1/0{,}008;\ 0{,}3/0{,}063;\ 0/0{,}25\}$$

та

$$\underset{\sim}{T}'_{321} = \underset{\sim}{T}'_{SPKPOA1} = \underset{\sim}{M}'_{32} =$$

$$\{\mu_{3211} / x_{3211}, \mu_{3212} / x_{3212}, \mu_{3213} / x_{3213}, \mu_{3214} / x_{3214}\} =$$

$$\{0/0{,}01;\ \ 1/0{,}01;\ 0{,}2/0{,}1;\ 0/1\},$$

де $\mu_{311\beta-1} = 0$ та $\mu_{321\beta-1} = 0.$

Аналогічним чином, отримуємо проміжні терми для $\underset{\sim}{M}'_{31}$, $\underset{\sim}{B}'_{31}$ і $\underset{\sim}{OB}'_{31}$, де $\mu_{312\beta-1} = \mu_{314r_j-\gamma+2} = \mu_{315r_j-\gamma+2} = 0$, а також для $\underset{\sim}{C}'_{32}$ і $\underset{\sim}{B}'_{32}$ де $\mu_{322\beta-1} = \mu_{322r_j-\gamma+2} = \mu_{323r_j-\gamma+2} = 0.$

Таким чином, компоненти підмножини еталонів $\underset{\sim}{T}^e_{311}$ та $\underset{\sim}{T}^e_{321}$ відповідно до (2.52) будуть визначатися як

$$\mu^e_{3111} / x^e_{3111} = 0/0{,}008,\ \ \mu^e_{3112} / x^e_{3112} = 1/0{,}008,$$

$$\mu^e_{3113} / x^e_{3113} = 0{,}3/0{,}063,\ \ \mu^e_{3114} / x^e_{3114} = 0/0{,}25$$

та, аналогічним чином, для $\underset{\sim}{T}^e_{312}$, $\underset{\sim}{T}^e_{314}$, $\underset{\sim}{T}^e_{315}$, а також

$$\mu^e_{3211} / x^e_{3211} = 0/0{,}01,\ \ \mu^e_{3212} / x^e_{3212} = 1/0{,}01,$$

$$\mu^e_{3213} / x^e_{3213} = 0{,}2/0{,}1,\ \ \mu^e_{3214} / x^e_{3214} = 0/1$$

та, аналогічно, для $\underset{\sim}{T}^e_{322}$ та $\underset{\sim}{T}^e_{323}$.

Далі, відносно виразу (2.52) для $\underset{\sim}{OM}'_{31}$, $\underset{\sim}{M}'_{31}$, $\underset{\sim}{B}'_{31}$, $\underset{\sim}{QB}'_{31}$ та $\underset{\sim}{M}'_{32}$, $\underset{\sim}{C}'_{32}$, $\underset{\sim}{B}'_{32}$ можемо сформувати еталонні значення, тобто:

$$\underset{\sim}{T}^e_{311} = \underset{\sim}{T}^e_{SPKOPI} = \underset{\sim}{OM}^e_{31} =$$

$$\{\mu^e_{3111} / x^e_{3111}, \mu^e_{3112} / x^e_{3112}, \mu^e_{3113} / x^e_{3113}, \mu^e_{3114} / x^e_{3114}\} =$$

$$\{0/0{,}008;\ 1/0{,}008;\ 0{,}3/0{,}063;\ 0/0{,}25\},$$

$$\underset{\sim}{T}^{e}_{312} = \underset{\sim}{T}^{e}_{SPKOP2} = \underset{\sim}{M}^{e}_{31} =$$

$$\{\mu^{e}_{3121} / x^{e}_{3121}, \mu^{e}_{3122} / x^{e}_{3122}, \mu^{e}_{3123} / x^{e}_{3123}, \mu^{e}_{3124} / x^{e}_{3124}, \mu^{e}_{3125} / x^{e}_{3125}\} =$$

$$\{0/0{,}008;\ 0{,}6/0{,}008;\ 1/0{,}063;\ 0{,}2/0{,}25;\ 0/0{,}5\},$$

$$\underset{\sim}{T}^{e}_{314} = \underset{\sim}{T}^{e}_{SPKOP4} = \underset{\sim}{B}^{e}_{31} =$$

$$\{\mu^{e}_{3141} / x^{e}_{3141}, \mu^{e}_{3142} / x^{e}_{3142}, \mu^{e}_{3143} / x^{e}_{3143}, \mu^{e}_{3144} / x^{e}_{3144}, \mu^{e}_{3145} / x^{e}_{3145}\} =$$

$$\{0/0{,}063;\ 0{,}6/0{,}25;\ 1/0{,}5;\ 0{,}7/1;\ 0/1\},$$

$$\underset{\sim}{T}^{e}_{315} = \underset{\sim}{T}^{e}_{SPKOP5} = \underset{\sim}{QB}^{e}_{31} =$$

$$\{\mu^{e}_{3151} / x^{e}_{3151}, \mu^{e}_{3152} / x^{e}_{3152}, \mu^{e}_{3153} / x^{e}_{3153}, \mu^{e}_{3154} / x^{e}_{3154}\} =$$

$$\{0/0{,}25;\ 0{,}6/0{,}5;\ 1/1;\ 0/1\}.$$

За результатами розрахунків із прикладу, очевидно що, $r_1 = 4$, $r_2 = r_3 = r_4 = 5$, $r_5 = 4$, а також

$$\underset{\sim}{T}^{e}_{321} = \underset{\sim}{T}^{e}_{SPKTPOA1} = \underset{\sim}{M}^{e}_{32} =$$

$$\{\mu^{e}_{3211} / x^{e}_{3211}, \mu^{e}_{3212} / x^{e}_{3212}, \mu^{e}_{3213} / x^{e}_{3213}, \mu^{e}_{3214} / x^{e}_{3214}\} =$$

$$\{0/0{,}01;\ 1/0{,}01;\ 0{,}2/0{,}1;\ 0/1\},$$

$$\underset{\sim}{T}^{e}_{322} = \underset{\sim}{T}^{e}_{SPKTPOA2} = \underset{\sim}{C}^{e}_{32} =$$

$$\{\mu^{e}_{3221} / x^{e}_{3221}, \mu^{e}_{3222} / x^{e}_{3222}, \mu^{e}_{3223} / x^{e}_{3223}, \mu^{e}_{3224} / x^{e}_{3224}, \mu^{e}_{3225} / x^{e}_{3225}\} =$$

$$\{0/0{,}01;\ 0{,}5/0{,}01;\ 1/0{,}1;\ 0{,}7/1;\ 0/1\},$$

$$\underset{\sim}{T}^{e}_{323} = \underset{\sim}{T}^{e}_{SPKTPOA3} = \underset{\sim}{B}^{e}_{32} =$$

$$\{\mu^{e}_{3231} / x^{e}_{3231}, \mu^{e}_{3232} / x^{e}_{3232}, \mu^{e}_{3233} / x^{e}_{3233}, \mu^{e}_{3234} / x^{e}_{3234}\} =$$

$$\{0/0{,}01;\ 0{,}5/0{,}1;\ 1/1;\ 0/1\},$$

де, наприклад,

- $\mu^{e}_{3231} / x^{e}_{3231} = \mu_{3231} / x_{3231}$,
- $\mu^{e}_{3232} / x^{e}_{3232} = \mu_{3232} / x_{3232}$,
- $\mu^{e}_{3233} / x^{e}_{3233} = \mu_{3233} / x_{3233}$,
- $\mu^{e}_{3234} / x^{e}_{3234} = \mu_{3234} / x_{3234}$,

також із прикладу, видно що, $r_1 = r_3 = 4$, $r_2 = 5$.

Візуалізація еталонних підсередовищ

Етап 6 – візуалізація еталонних підсередовищ. Реалізація цього етапу ґрунтується на побудові геометричного образу всіх еталонних НЧ (2.52), які належать підмножині $\mathbf{T}^{\mathbf{e}}_{\mathbf{ij}}$ (див. (2.13)).

Геометричне місце точок на площині визначається за допомогою ламаної з'єднуючої точки, що відображають компоненти НЧ $\underset{\sim}{T}^{e}_{ijs}$ у порядку зростання їх супортів (носіїв) x^{e}_{ijsq}.

Візуалізація одного типового еталонного терму (2.52) представлена у вигляді ламаної ⟵● на рис. 2.1.

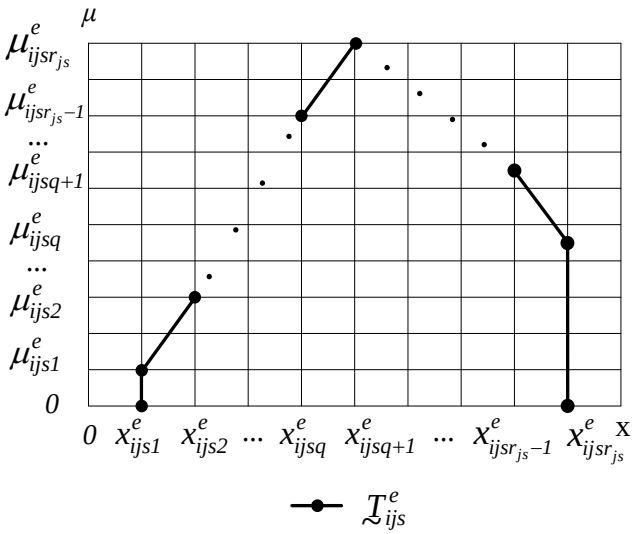

Рис. 2.1. НЧ $\underset{\sim}{T}^{e}_{ijs}$ еталонного підсередовища ($\mathbf{T}^{\mathbf{e}}_{\mathbf{i}}$)

Наприклад, для візуалізації підмножини еталонів $\mathbf{T}^{\mathbf{e}}_{\mathbf{31}} = \mathbf{T}^{\mathbf{e}}_{\mathbf{SPKOП}}$ та $\mathbf{T}^{\mathbf{e}}_{\mathbf{32}} = \mathbf{T}^{\mathbf{e}}_{\mathbf{SPKПОА}}$ скористаємося НЧ еталонного підсередовища ($\mathbf{T}^{\mathbf{e}}_{\mathbf{i}} = \mathbf{T}^{\mathbf{e}}_{\mathbf{3}} = \mathbf{T}^{\mathbf{e}}_{\mathbf{SP}}$) сформованого на етапі 5 (див. приклад):

$$\underset{\sim}{OM}^{e}_{31} = \{ 0/0{,}008;\ 1/0{,}008;\ 0{,}3/0{,}063;\ 0/0{,}25 \},$$

$$\underset{\sim}{M}^{e}_{31} = \{ 0/0{,}008;\ 0{,}6/0{,}008;\ 1/0{,}063;\ 0{,}2/0{,}25;\ 0/0{,}5 \},$$

$$\underset{\sim}{С}^{e}_{З1} = \{0/0{,}008;\ 0{,}4/0{,}063;\ 1/0{,}25;\ 0{,}3/0{,}5;\ 0/1\},$$

$$\underset{\sim}{Б}^{e}_{З1} = \{0/0{,}063;\ 0{,}6/0{,}25;\ 1/0{,}5;\ 0{,}7/1;\ 0/1\},$$

$$\underset{\sim}{ОБ}^{e}_{З1} = \{0/0{,}25;\ 0{,}6/0{,}5;\ 1/1;\ 0/1\}$$

та

$$\underset{\sim}{М}^{e}_{З2} = \{0/0{,}01;\ 1/0{,}01;\ 0{,}2/0{,}1;\ 0/1\},$$

$$\underset{\sim}{С}^{e}_{З2} = \{0/0{,}01;\ 0{,}5/0{,}01;\ 1/0{,}1;\ 0{,}7/1;\ 0/1\},$$

$$\underset{\sim}{Б}^{e}_{З2} = \{0/0{,}01;\ 0{,}5/0{,}1;\ 1/1;\ 0/1\}.$$

На їх основі (шляхом з'єднання точок, що відображаються відповідними компонентами НЧ $\underset{\sim}{ОМ}^{e}_{З1}$, $\underset{\sim}{М}^{e}_{З1}$, $\underset{\sim}{С}^{e}_{З1}$, $\underset{\sim}{Б}^{e}_{З1}$, $\underset{\sim}{ОБ}^{e}_{З1}$ еталонного підсередовища ($\mathbf{T}^{e}_{i} = \mathbf{T}^{e}_{З} = \mathbf{T}^{e}_{SP}$)) будуються п'ять ламаних (рис. 2.2) —●—, —■—, —○—, —□—, —▮— та для НЧ $\underset{\sim}{М}^{e}_{З2}$, $\underset{\sim}{С}^{e}_{З2}$, $\underset{\sim}{Б}^{e}_{З2}$ будуються три ламані —●—, —□—, —△—, які графічно інтерпретуються на рис. 2.3.

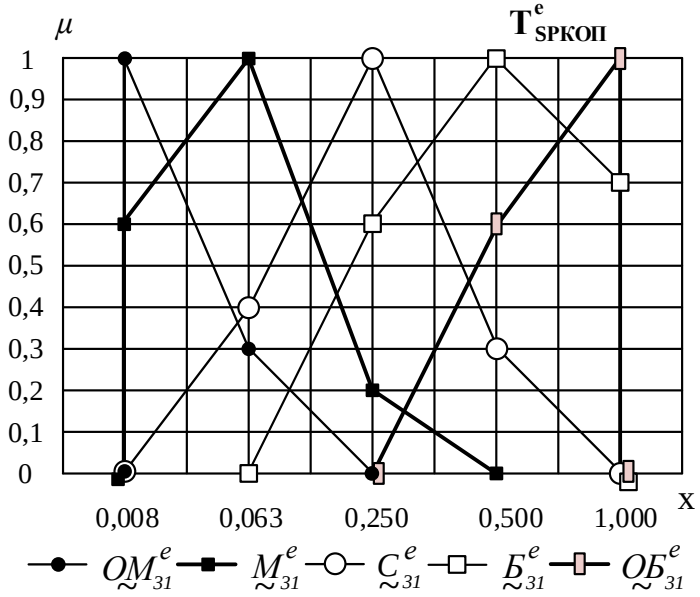

Рис. 2.2. Лінгвістичні еталони підмножини $\mathbf{T}^{e}_{SPКОП}$

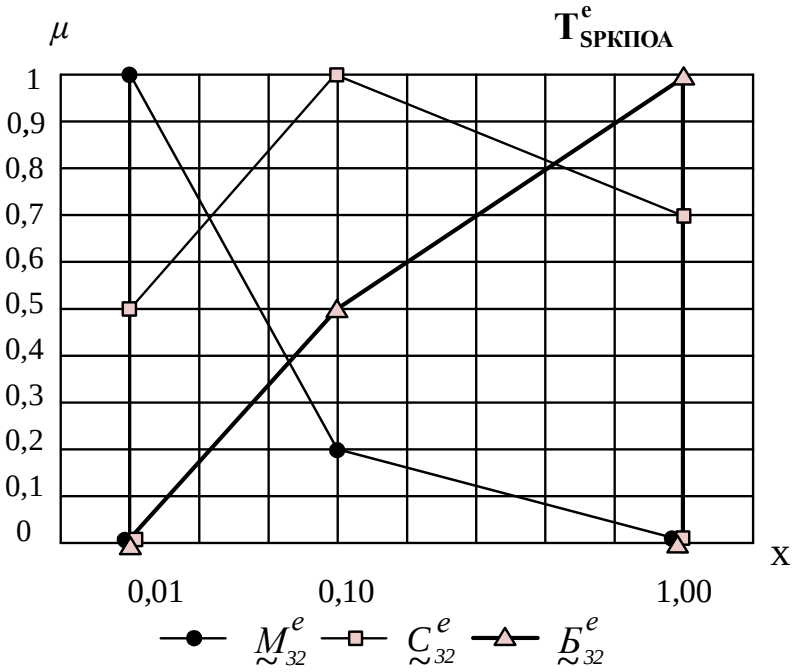

Рис. 2.3. Лінгвістичні еталони підмножини $\mathbf{T}^{\mathbf{e}}_{\mathbf{SPKПОА}}$

Запропонований в роботі МФЕС [7-10] для СВВ, який за рахунок використання множини ідентифікаторів лінгвістичних оцінок та ідентифікаторів інтервалів, базової та похідної матриці частот, формального відображення суджень експерта для характеристики поточного стану параметрів відносно кібератаки, процесу формування на заданих інтервалах частот зустрічальності експертних оцінок та підмножин нечітких термів, дозволяє формалізувати процес отримання еталонних значень фіксованих параметрів заданих груп лінгвістичних змінних, що характеризує конкретне еталонне підсередовище.

Для використання МФЕС необхідно створити відповідний метод формалізації процесу перетворення поточних значень нечітких параметрів, утворюючих m_i-вимірне параметричне підсередовищ, з метою його подальшого застосування для виявлення аномального стану.

2.3. Метод формування еталонного підсередовища для виявлення сніфінг-атак

Одним із небезпечних засобів, які направлені на перехоплення паролів в мережі є сніфери – спеціалізоване ПЗ. Для ефективного функціонування достатньо бути йому встановленим на одному комп'ютері в мережі. Його принцип роботи полягає в тому, що він отримує доступ до мережевої карти, наприклад, переключає її в режим PROMISC (режим прослуховування). В даному випадку мережева карта буде приймати всі пакети (включаючи ті, які їй не адресуються), що знаходяться в каналі зв'язку. Якщо в мережі здійснюється активний обмін пакетів, то за достатньо короткий час сніфер зможе зібрати різні дані, наприклад, логіни, паролі, email-переписку тощо.

Головна небезпека полягає в тому, що сніфери досить складно виявити, так як вони працюють в пасивному режимі та, як правило, користувачі не здогадуються, що в даний момент проходить сніфінг-атака. Як показує практика, такі атаки, в основному, залишаються непоміченими (див. рис. 2.4).

Розглянемо вид сніфінга, при якому НАС, проникнувши в мережу, аналізує велику кількість пакетів. Схема реалізації такої атаки у певному середовищі оточення показана на рисунку 2.4.

В даному прикладі, НАС впроваджує сніфер на ПК2 (здійснюється перемикання його мережевої карти в режим PROMISC), внаслідок чого сніфер контролює весь трафік пов'язаний з ПК2. Зі схеми видно, що НАС отримує не тільки дані, які надіслані на ПК2, але, наприклад, email повідомлення, яке було відправлено з ПК3 на ПК2.

Також продемонстровано, що користувач ПК2 отримає тільки дані, які призначені йому (зображення з ПК1), у той час як НАС за допомогою сніфера отримає всі дані, які знаходилися в мережі (аудіофайл, зображення та email повідомлення), що наочно показує його функціонування.

Оскільки, пряме виявлення сніфінг-атаки є дещо проблемне, то для ідентифікації подібних вторгнень необхідно досліджувати можливі зміни параметрів середовища оточення системи, значення яких при виникненні деяких подій відрізняються від штатно допустимих.

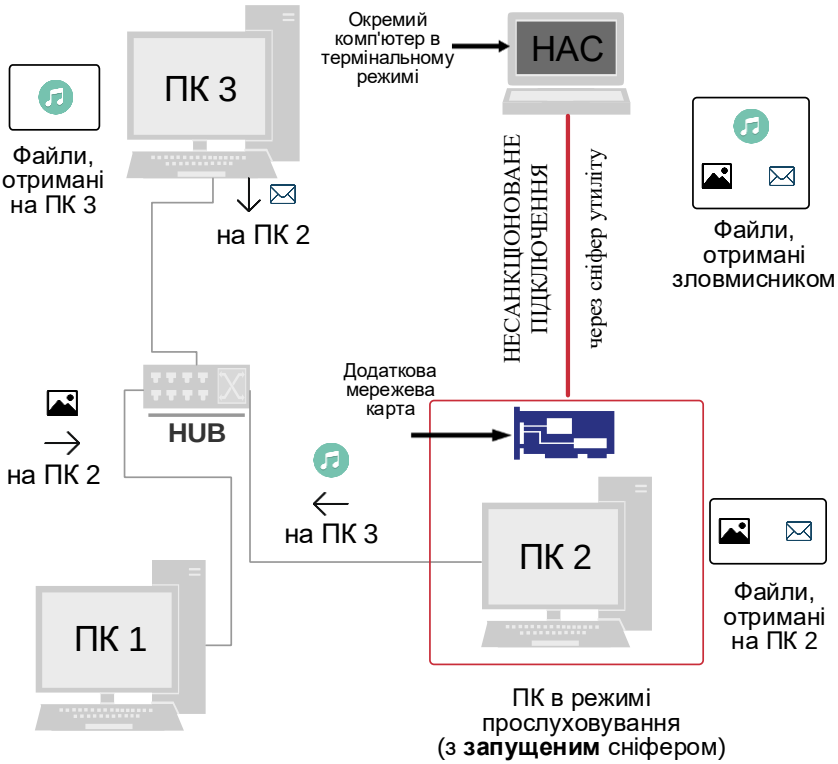

Рис. 2.4. Схема проведення сніфінг-атаки

Наприклад, для виявлення описаної атаки найбільш доцільно використовувати наступні параметри: КВП, СОП, ТП (див. п. 2.1 та [1]), які визначають час очікування для обробки нового пакету на стороні отримувача.

Оскільки сніферу для аналізу пакетів, які знаходяться в мережі, потрібний час, то збільшення значень параметра ТП може бути ознакою наявності в даній мережі сніфера. Для успішного проведення відповідної атаки НАС повинна впровадити сніфер на один із комп’ютерів, що підключений до мережі, дані з якої необхідні НАС.

Якщо при нормальному режимі роботи мережі значення обраних параметрів виходять за визначені межі, то це може свідчити про те, що здійснюється сніфінг-атака в даному мережевому каналі.

Для отримання конкретних числових параметрів було проведено моделювання на працюючому Web-сервері. В якості прикладу серверу, для тестування використовувався комп'ютер з наступними характеристиками:

- процесор Intel(R) Core 2 Duo T5800 CPU 2,00GHz з частотою шини 800 МГц;
- оперативна пам'ять 6 Гб DDR2 800 МГц;
- мережеве підключення 100 Мбит/с;
- операційна система 64-бітна Windows 10.

Також, для здійснення симуляції було встановлено та використано наступне ПЗ:

- VirtualBox;
- Nmap 7.12;
- WireShark;
- WIcd,

яке на даний момент містить великий набір інструментів для мережевого менеджменту.

Для дослідження параметрів КВП, СОП та ТП в тестовій локальній мережі, в якій функціонує сніфер, відповідно використовуються WIcd, WireShark та Nmap.

Як показує практика, для отримання необхідних даних потрібен тривалий час роботи сніфера в мережі. Завдяки цьому стає можливим його виявлення за допомогою аналізу сукупності вищезазначених величин. Наприклад, параметр КВП при певному збільшенні кількості пакетів в мережі може бути використаний як одна з ознак наявності руйнівного ПЗ. Максимальна кількість пакетів, яку може пропустити канал, залежить від його фізичних характеристик, а також може бути обмежена програмно. Максимальне значення КВП $(max_{КВП})$, зазвичай, визначається в налаштуваннях серверу.

Система, що використовується для моделювання, конфігурована так аби підтримувати одночасно не більше *256* підключень, тобто $max_{КВП} = 256$. Відповідно до статистики, яка сформована за допомогою додатку *WIcd*, для даного серверу середня кількість таких підключень не перевищувала *100*.

Для зручності оцінювання параметрів на основі суджень експерта та їх відображення прийнято вважати, що достатньо використовувати *3-7* термів для кожного параметра [13]. Більшість застосувань

цілком вичерпується використанням мінімальної кількості термів. Таке визначення містить два граничних значення (мінімальне та максимальне), а також середнє. Що стосується максимальної кількості термів, то воно не обмежене та залежить від необхідної адекватності опису параметрів. Число *7* обумовлено ємністю короткочасної пам'яті людини, в якій, як відомо, може міститися до семи одиниць інформації [13].

Виходячи з цього, доцільно використовувати п'ять термів з наступними інтервалами $[0;8]$, $[9;32]$, $[33;64]$, $[65;128]$, $[129;256]$.

Після моніторингу мережі було виявлено, що кількість вхідних пакетів (RX packets) *269*, що перевищує нормальні показники. Також було визначено число відправлених пакетів (TX packets) *136* (див. рис. 2.5), така зміна може свідчити про роботу сніфера в мережі, оскільки налаштуваннями мережевого адаптера визначено (зафіксовано) максимальне значення даного параметра – *256*.

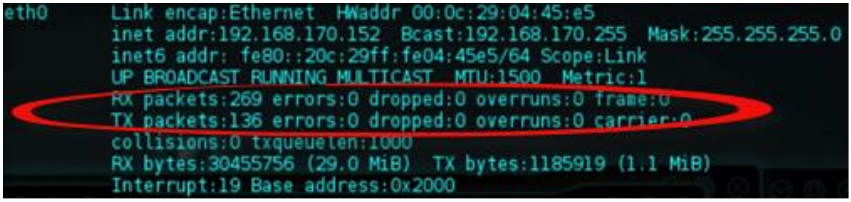

Рис. 2.5. Відображення параметра КВП за допомогою утиліти WIcd

Параметр СОП – один з найбільш важливих у механізмі виявлення снiфінг-атаки, оскільки він показує час, необхідний для обробки вхідних пакетів. Якщо сніфер був впроваджений на комп'ютері, то цей параметр зміниться одним з перших, так як перевимкнувши мережеву карту в режим PROMISC, сніфер збільшує час обробки в *2* рази. В достатньо навантаженому мережевому каналі подібний параметр зміниться через короткий час після початку роботи сніфера в мережі. Максимальна швидкість обробки пакетів визначається на практиці за допомогою утиліти dsniff для конкретного користувача в мережі та задається величиною $max_{СОП}$.

Значення параметра СОП були отримані за результатами тесту, що здійснювався за допомогою утиліти WireShark, яка є поширеним

засобом для аналізу трафіка комп'ютерних мереж. Виміри проводилися при великій кількості пакетів, які показали, що даний web-сервер може опрацювати до *3600* запитів в секунду в локальній мережі і від *200* до *400* отриманих з мережі Internet. В нормальному режимі роботи сервер за одну секунду обслуговує до *25* Internet-запитів, а максимальна кількість, яка може бути оброблена – *80*.

На основі цього, для параметру СОП візьмемо наступні інтервали $[0;8]$, $[9;24]$, $[25;80]$, які наглядно показують діапазони мінімальних, середньо допустимих та максимальних значень для визначеної величини.

Виходячи з цього, найбільш коректним буде визначення максимального значення для параметра СОП – *80*.

Для виявлення сніфера з використанням СОП можна застосовувати утиліту для моніторингу параметрів мережі WireShark. Вона дозволяє відслідкувати швидкість обробки пакетів в мережі. На представленому рисунку (див. рис. 2.6) спостерігається стрибок швидкості до *42* секунд, що відповідно вище зазначених інтервалів, це може бути наслідком роботи сніфера в мережі.

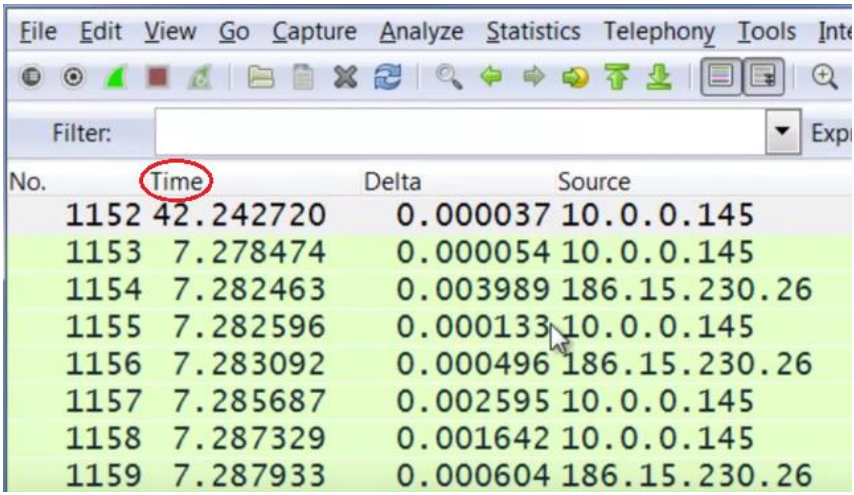

Рис. 2.6. Відображення значення параметра СОП за допомогою утиліти WireShark

Параметр ТП характеризує час між послідовним отриманням пакетів на стороні отримувача від адресата. Збільшення часу між вхідними пакетами може свідчити про роботу сніфера, метою якого є аналіз пакетів в мережі. Значення ТП визначається величиною $max_{ТП}$, яка залежить від ПЗ та призначення сервера.

При нормальному навантаженні комп'ютерної мережі значення параметра ТП не перевищує *25* мс, а максимальний час затримки між пакетами – *64* с. З цього слідує, що найбільш коректними інтервалами, які описують параметр ТП, будуть $[0;5]$, $[6;24]$, $[25;32]$, $[33;64]$.

Для виявлення сніфера за визначеним параметром використовувалась утиліта Nmap, завдяки якій експерт, може прогнозувати час затримки між пакетами. Як видно з наведеного рисунку (див. рис. 2.7), затримка склала *63* секунди, що свідчить про роботу сніфера в мережі.

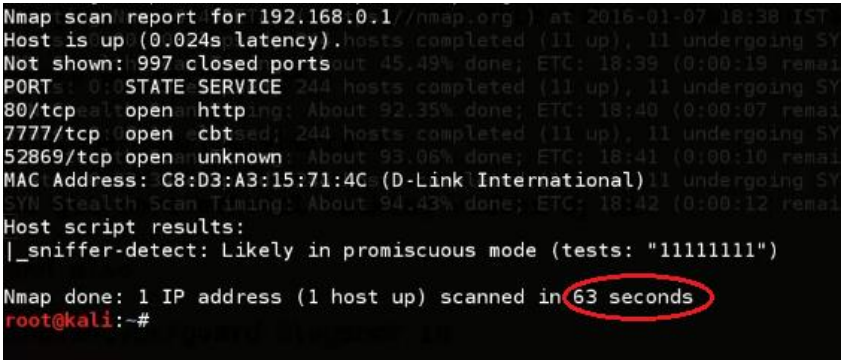

Рис. 2.7. Відображення значення параметра ТП за допомогою утиліти Nmap

Інтервали, що визначені для значень параметрів КВП, СОП, ТП базуються відповідно на:

- максимальній кількості пакетів, які здатний пропустити даний канал за одиницю часу;
- максимальній швидкості обробки пакетів даною системою;
- максимальному часі затримки пакетів у каналі.

Слід зазначити, що свідченням роботи сніфера в мережі є величини всіх параметрів, значення яких знаходяться в діапазоні від середньо допустимого до максимального.

Таким чином, мінімальні та максимальні значення, які будуть свідчити про потенційну наявність сніфера є: КВП $[129;256]$, СОП $[25;80]$ та ТП $[25;64]$.

Виходячи з цього, розробимо метод формування еталонного підсередовища для виявлення снiфінг-атак (МФЕПСА) [14], що дозволить формалізувати процес отримання еталонів параметрів для конкретних лінгвістичних змінних визначеного середовища оточення при вирішенні задач, щодо виявлення снiфінг-атак на інформаційні системи. Запропонований МФЕПСА [14-16] базується на МФЕС (див. п. 2.2 та [7, 8, 11]).

З урахуванням цього, сформуємо підмножину ІД суджень експертів при $n=1$ для кібератаки з ІД $CA_1 = CA_{SNF} = SNF$ $(m_1 = 3,$ $r_1 = 5,\ r_2 = 3,\ r_3 = 4)$ відповідно до етапу 1 виразу (2.30) (див. п. 2.2 та [7, 10])

$$\{\bigcup_{i=1}^{1} \mathbf{LE_1}\} = \{\bigcup_{i=1}^{1}\{\bigcup_{j=1}^{m_i} \mathbf{LE_{ij}}\}\} =$$

$$\{\bigcup_{i=1}^{1}\{\bigcup_{j=1}^{m_i}\{\bigcup_{k=1}^{r_j} LE_{ijk}\}\}\} =$$

$$\begin{gathered}\{\{LE_{SNFKBII1},\ LE_{SNFKBII2},\ LE_{SNFKBII3},\\ LE_{SNFKBII4},\ LE_{SNFKBII5}\},\\ \{LE_{SNFCOII1},\ LE_{SNFCOII2},\ LE_{SNFCOII3}\},\\ \{LE_{SNFTII1},\ LE_{SNFTII2},\ LE_{SNFTII3},\ LE_{SNFTII4}\}\} =\\ \{\{"ОМ",\ "М",\ "С",\ "Б",\ "ОБ"\},\\ \{"Н",\ "С",\ "В"\},\\ \{"Н",\ "С",\ "В",\ "ОВ"\}\},\end{gathered} \tag{2.53}$$

де:

- $LE_{SNFKBII1} = "ОМ",$
- $LE_{SNFKBII2} = "М",$
- $LE_{SNFKBII3} = "С",$

- $LE_{SNFKBII4} = "Б"$,
- $LE_{SNFKBII5} = "ОБ"$,
- $LE_{SNFCOII1} = "Н"$,
- $LE_{SNFCOII2} = "С"$,
- $LE_{SNFCOII3} = "В"$

та

- $LE_{SNFTII1} = "Н"$,
- $LE_{SNFTII2} = "С"$,
- $LE_{SNFTII3} = "В"$,
- $LE_{SNFTII4} = "ОВ"$

відповідно є ІД лінгвістичних оцінок експерта, які відображають стан параметрів $P_{SNFKBII} = KBII$, $P_{SNFCOII} = COII$ та $P_{SNFTII} = TII$ в 3-вимірному параметричному підсередовищі ($\mathbf{P_i} = \mathbf{P_{SNF}}$) (див. п. 2.1 та [1]).

Наступним, відповідно до етапу 2 (див. п. 2.2) необхідно сформувати базову матрицю частот.

Для цього побудуємо підмножину ІД інтервалів $\mathbf{N_{ij}}$ $(j = \overline{1, m_i})$ (див. (2.35)), що характеризують кібератаку з ІД $CA_1 = CA_{SNF} = SNF$, на області визначення яких експерт здійснює лінгвістичну оцінку відносно значень параметрів $P_{SNFKBII}$, $P_{SNFCOII}$ та P_{SNFTII} (див. п. 2.1).

При $n = 1$, $m_1 = 3$, $r_1 = 5$, $r_2 = 3$, $r_3 = 4$ отримаємо

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{1}} \mathbf{N_i}\} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{1}} \{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}} \mathbf{N_{ij}}\}\} =$$

$$\{\bigcup_{i=1}^{1} \{\bigcup_{j=1}^{m_i} \{\bigcup_{k=1}^{k_j} N_{ijk}\}\}\} = \tag{2.54}$$

$$\{\{N_{SNFKBII1}, N_{SNFKBII2}, N_{SNFKBII3}, N_{SNFKBII4}, N_{SNFKBII5}\},$$
$$\{N_{SNFCOII1}, N_{SNFCOII2}, N_{SNFCOII3}\},$$
$$\{N_{SNFTII1}, N_{SNFTII2}, N_{SNFTII3}, N_{SNFTII4}\}\}.$$

З урахування елементів підмножин $\mathbf{LE_{ij}}$ та $\mathbf{N_{ij}}$ на основі узагальнювальної матриці (див. табл. 2.1) побудуємо поточні оцінки (див. табл. 2.4-2.6) за елементами підмножин

$$LE_{SNFKBII_k}\ (r_1 = 5,\ k = \overline{1,5}),\ \ N_{SNFKBII_k},\ \text{тобто}$$

- $N_{SNFKBII1} = [N^{min}_{SNFKBII1}; N^{max}_{SNFKBII1}] \Leftrightarrow [0;8]$,
- $N_{SNFKBII2} = [N^{min}_{SNFKBII2}; N^{max}_{SNFKBII2}] \Leftrightarrow [9;32]$,
- $N_{SNFKBII3} = [N^{min}_{SNFKBII3}; N^{max}_{SNFKBII3}] \Leftrightarrow [33;64]$,
- $N_{SNFKBII4} = [N^{min}_{SNFKBII4}; N^{max}_{SNFKBII4}] \Leftrightarrow [65;128]$,
- $N_{SNFKBII5} = [N^{min}_{SNFKBII5}; N^{max}_{SNFKBII5}] \Leftrightarrow [129;256]$

та

$$LE_{SNFCOII_k}\ (r_2 = 3,\ k = \overline{1,3}),\ \ N_{SNFCOII_k},\ \text{тобто}$$

- $N_{SNFCOII1} = [N^{min}_{SNFCOII1}; N^{max}_{SNFCOII1}] \Leftrightarrow [0;8]$,
- $N_{SNFCOII2} = [N^{min}_{SNFCOII2}; N^{max}_{SNFCOII2}] \Leftrightarrow [9;24]$,
- $N_{SNFCOII3} = [N^{min}_{SNFCOII3}; N^{max}_{SNFCOII3}] \Leftrightarrow [25;80]$,

а також

$$LE_{SNFTII_k}\ (r_3 = 4,\ k = \overline{1,4}),\ \ N_{SNFTII_k},\ \text{тобто}$$

- $N_{SNFTII1} = [N^{min}_{SNFTII1}; N^{max}_{SNFTII1}] \Leftrightarrow [0;5]$,
- $N_{SNFTII2} = [N^{min}_{SNFTII2}; N^{max}_{SNFTII2}] \Leftrightarrow [6;24]$,
- $N_{SNFTII3} = [N^{min}_{SNFTII3}; N^{max}_{SNFTII3}] \Leftrightarrow [25;32]$,
- $N_{SNFTII4} = [N^{min}_{SNFTII4}; N^{max}_{SNFTII4}] \Leftrightarrow [33;64]$.

Поточна таблиця оцінок за $\mathbf{LE_{SNFKBII}}$ Таблиця 2.4

$\mathbf{LE_{SNFKBII}}$	$\mathbf{N_{SNFKBII}}$				
	$N_{SNFKBII1}$	$N_{SNFKBII2}$	$N_{SNFKBII3}$	$N_{SNFKBII4}$	$N_{SNFKBII5}$
“ОМ”	5	3	0	0	0
“М”	1	6	1	0	0
“С”	0	1	4	1	0
“Б”	0	0	2	6	4
“ОБ”	0	0	0	4	6

Поточна таблиця оцінок за $\mathbf{LE_{SNFCOII}}$ Таблиця 2.5

$\mathbf{LE_{SNFCOII}}$	$\mathbf{N_{SNFCOII}}$		
	$N_{SNFCOII1}$	$N_{SNFCOII2}$	$N_{SNFCOII3}$
“H”	4	1	0
“C”	1	2	1
“B”	0	1	3

Поточна таблиця оцінок за $\mathbf{LE_{SNFTII}}$ Таблиця 2.6

$\mathbf{LE_{SNFTII}}$	$\mathbf{N_{SNFTII}}$			
	$N_{SNFTII1}$	$N_{SNFTII2}$	$N_{SNFTII3}$	$N_{SNFTII4}$
“H”	3	1	0	0
“C”	2	3	3	0
“B”	0	2	4	3
“OB”	0	1	3	4

Далі, з урахуванням даних таблиць 2.4-2.6, а також виразу (2.36), сформуємо матриці частот (при $n=1,\ m_1=3,\ s,q=\overline{1,r_1},\ s,q=\overline{1,r_2},$ $s,q=\overline{1,r_3}$)

$$F_{11}=F_{SNFKBII}=\left\|f_{11sq}\right\|=$$

$$\left\|\begin{matrix} f_{1111} & f_{1112} & f_{1113} & f_{1114} & f_{1115} \\ f_{1121} & f_{1122} & f_{1123} & f_{1124} & f_{1125} \\ f_{1131} & f_{1132} & f_{1133} & f_{1134} & f_{1135} \\ f_{1141} & f_{1142} & f_{1143} & f_{1144} & f_{1145} \\ f_{1151} & f_{1152} & f_{1153} & f_{1154} & f_{1155} \end{matrix}\right\|=\left\|\begin{matrix} 5 & 3 & 0 & 0 & 0 \\ 1 & 6 & 1 & 0 & 0 \\ 0 & 1 & 4 & 1 & 0 \\ 0 & 0 & 2 & 6 & 4 \\ 0 & 0 & 0 & 4 & 6 \end{matrix}\right\|,$$

$$F_{12}=F_{SNFCOII}=\left\|f_{12sq}\right\|=\left\|\begin{matrix} f_{1211} & f_{1212} & f_{1213} \\ f_{1221} & f_{1222} & f_{1223} \\ f_{1231} & f_{1232} & f_{1233} \end{matrix}\right\|=\left\|\begin{matrix} 4 & 1 & 0 \\ 1 & 2 & 1 \\ 0 & 1 & 3 \end{matrix}\right\|$$ та

$$F_{13} = F_{SNFTII} = \left\| f_{13sq} \right\| = \left\| \begin{matrix} f_{1311} & f_{1312} & f_{1313} & f_{1314} \\ f_{1321} & f_{1322} & f_{1322} & f_{1322} \\ f_{1331} & f_{1332} & f_{1333} & f_{1334} \\ f_{1341} & f_{1342} & f_{1343} & f_{1344} \end{matrix} \right\| = \left\| \begin{matrix} 3 & 1 & 0 & 0 \\ 2 & 3 & 3 & 0 \\ 0 & 2 & 4 & 3 \\ 0 & 0 & 3 & 4 \end{matrix} \right\|.$$

Далі, для формування похідної матриці частот (при $n=1$, $m_1 = 3$) побудуємо, за відповідними стовпцями матриць $F_{SNFKBII}$, $F_{SNFCOII}$ і F_{SNFTII} з урахуванням виразу (2.38) вектори сум

$$VS_{SNFKBII} = \left\| vs_{SNFKBIIq} \right\| =$$

$$\left\| vs_{SNFKBII1}, vs_{SNFKBII2}, vs_{SNFKBII3}, vs_{SNFKBII4}, vs_{SNFKBII5} \right\| =$$

$$\left\| \bigcup_{q=1}^{5} \sum_{s=1}^{5} f_{SNFKBIIsq} \right\| = \left\| 6,10,7,11,10 \right\|,$$

$$(q = \overline{1,5}),$$

$$VS_{SNFCOII} = \left\| vs_{SNFCOIIq} \right\| = \left\| vs_{SNFCOII1}, vs_{SNFCOII2}, vs_{SNFCOII3} \right\| =$$

$$\left\| \bigcup_{q=1}^{3} \sum_{s=1}^{3} f_{SNFCOIIsq} \right\| = \left\| 5,4,4 \right\|,$$

$$(q = \overline{1,3}),$$

а також

$$VS_{SNFTII} = \left\| vs_{SNFTIIq} \right\| = \left\| vs_{SNFTII1}, vs_{SNFTII2}, vs_{SNFTII3}, vs_{SNFTII4} \right\| =$$

$$\left\| \bigcup_{q=1}^{4} \sum_{s=1}^{4} f_{SNFTIIsq} \right\| = \left\| 5,7,10,7 \right\|,$$

$$(q = \overline{1,4}).$$

Наступним, з урахуванням (2.39) з $VS_{SNFKBII}$, $VS_{SNFCOII}$ і VS_{SNFTII} визначимо максимальний елемент

$$vsm_{SNFKBII} = \bigvee_{q=1}^{5} vs_{SNFKBIIq} =$$

$$vs_{SNFKBII1} \vee vs_{SNFKBII2} \vee vs_{SNFKBII3} \vee vs_{SNFKBII4} \vee vs_{SNFKBII5} =$$

$$6 \vee 10 \vee 7 \vee 11 \vee 10 =$$
$$vsm_{SNFKBII} = 11,$$

$$vsm_{SNFCOII} = \bigvee_{q=1}^{3} vs_{SNFCOIIq} =$$
$$vs_{SNFCOII1} \vee vs_{SNFCOII2} \vee vs_{SNFCOII3} = 5 \vee 4 \vee 4 =$$
$$vsm_{SNFCOII} = 5,$$

а також

$$vsm_{SNFTII} = \bigvee_{q=1}^{4} vs_{SNFTIIq} =$$
$$vs_{SNFTII1} \vee vs_{SNFTII2} \vee vs_{SNFTII3} \vee vs_{SNFTII4} = 5 \vee 7 \vee 10 \vee 7 =$$
$$vsm_{SNFTII} = 10,$$

а відповідно до (2.40) отримаємо похідну матрицю частот,

$$F'_{SNFKBII} =$$
$$(vsm_{SNFKBII} / vsm_{SNFKBIIq})F_{SNFKBII} = \begin{Vmatrix} 9,2 & 3,3 & 0 & 0 & 0 \\ 1,8 & 6,6 & 1,6 & 0 & 0 \\ 0 & 1,1 & 6,3 & 1 & 0 \\ 0 & 0 & 3,1 & 6 & 4,4 \\ 0 & 0 & 0 & 4 & 6,6 \end{Vmatrix},$$

$$F'_{SNFCOII} =$$
$$(vsm_{SNFCOII} / vsm_{SNFCOIIq})F_{SNFCOII} = \begin{Vmatrix} 4 & 1,3 & 0 \\ 1 & 2,5 & 1,3 \\ 0 & 1,3 & 3,8 \end{Vmatrix} \text{ і}$$

$$F'_{SNFTII} =$$
$$(vsm_{SNFTII} / vsm_{SNFTIIq})F_{SNFTII} = \begin{Vmatrix} 6 & 1,4 & 0 & 0 \\ 4 & 4,3 & 3 & 0 \\ 0 & 2,9 & 4 & 4,3 \\ 0 & 1,4 & 3 & 5,7 \end{Vmatrix}.$$

Далі, з урахуванням (2.45) сформуємо підмножину нечітких термів $\mathbf{T_{SNFKBII}}$, $\mathbf{T_{SNFCOII}}$, $\mathbf{T_{SNFTII}}$, що відображають певні стани параметрів $P_{SNFKBII}$, $P_{SNFCOII}$ та P_{SNFTII} в 3-вимірному параметричному підсередовищі ($\mathbf{P_i = P_{SNF}}$), а також при $n=1$ (для кібератак з ІД $CA_1 = CA_{SNF} = SNF$), $m_1 = 3,\ r_1 = 5,\ r_2 = 3,\ r_3 = 4$

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

$$\{\{\underset{\sim}{T}_{SNFKBII1}, \underset{\sim}{T}_{SNFKBII2}, \underset{\sim}{T}_{SNFKBII3}, \underset{\sim}{T}_{SNFKBII4}, \underset{\sim}{T}_{SNFKBII5}\},$$

$$\{\underset{\sim}{T}_{SNFCOII1}, \underset{\sim}{T}_{SNFCOII2}, \underset{\sim}{T}_{SNFCOII3}\},$$

$$\{\underset{\sim}{T}_{SNFTII1}, \underset{\sim}{T}_{SNFTII2}, \underset{\sim}{T}_{SNFTII3}, \underset{\sim}{T}_{SNFTII4}\}\} =$$

$$\{\{\underset{\sim}{ОМ}_{SNFKBII}, \underset{\sim}{М}_{SNFKBII}, \underset{\sim}{С}_{SNFKBII}, \underset{\sim}{Б}_{SNFKBII}, \underset{\sim}{ОБ}_{SNFKBII}\},$$

$$\{\underset{\sim}{Н}_{SNFCOII}, \underset{\sim}{С}_{SNFCOII}, \underset{\sim}{В}_{SNFCOII}\},$$

$$\{\underset{\sim}{Н}_{SNFTII}, \underset{\sim}{С}_{SNFTII}, \underset{\sim}{В}_{SNFTII}, \underset{\sim}{ОВ}_{SNFTII}\}\}.$$

де:

- $\underset{\sim}{T}_{SNFKBII1} = \underset{\sim}{ОМ}_{SNFKBII}$, $\underset{\sim}{T}_{SNFKBII2} = \underset{\sim}{М}_{SNFKBII}$, $\underset{\sim}{T}_{SNFKBII3} = \underset{\sim}{С}_{SNFKBII}$, $\underset{\sim}{T}_{SNFKBII4} = \underset{\sim}{Б}_{SNFKBII}$ та $\underset{\sim}{T}_{SNFKBII5} = \underset{\sim}{ОБ}_{SNFKBII}$ відповідно є НЧ $\underset{\sim}{ОМ}_{SNFKBII}$, $\underset{\sim}{М}_{SNFKBII}$, $\underset{\sim}{С}_{SNFKBII}$, $\underset{\sim}{Б}_{SNFKBII}$, $\underset{\sim}{ОБ}_{SNFKBII}$, які інтерпретують висловлювання експерта, що відображаються за допомогою $LE_{SNFKBII1} = "ОМ",\ LE_{SNFKBII2} = "М",\ LE_{SNFKBII3} = "С",\ LE_{SNFKBII4} = "Б"$ та $LE_{SNFKBII5} = "ОБ"$,
- $\underset{\sim}{T}_{SNFCOII1} = \underset{\sim}{Н}_{SNFCOII}$, $\underset{\sim}{T}_{SNFCOII2} = \underset{\sim}{С}_{SNFCOII}$ і $\underset{\sim}{T}_{SNFCOII3} = \underset{\sim}{В}_{SNFCOII}$ відповідно є НЧ $\underset{\sim}{Н}_{SNFCOII}$, $\underset{\sim}{С}_{SNFCOII}$, $\underset{\sim}{В}_{SNFCOII}$, що інтерпретують висловлювання експерта, які відображаються за допомогою $LE_{SNFCOII1} = "Н",\ LE_{SNFCOII2} = "С"$ і $LE_{SNFCOII3} = "В"$,

а також

- $\underset{\sim}{T}_{SNFTII1} = \underset{\sim}{H}_{SNFTII}$, $\underset{\sim}{T}_{SNFTII2} = \underset{\sim}{C}_{SNFTII}$, $\underset{\sim}{T}_{SNFTII3} = \underset{\sim}{B}_{SNFTII}$ та $\underset{\sim}{T}_{SNFTII4} = \underset{\sim}{OB}_{SNFTII}$ відповідно є НЧ $\underset{\sim}{H}_{SNFTII}$, $\underset{\sim}{C}_{SNFTII}$, $\underset{\sim}{B}_{SNFTII}$, $\underset{\sim}{OB}_{SNFTII}$, які інтерпретують висловлювання експерта, що відображаються за допомогою $LE_{SNFTII1} = "H"$, $LE_{SNFTII2} = "C"$ $LE_{SNFTII3} = "B"$ і $LE_{SNFTII4} = "OB"$.

З урахуванням (2.46) за відповідними рядками $F'_{SNFKBII}$, $F'_{SNFCOII}$ та F'_{SNFTII} побудуємо вектори максимумів

$$FM_{SNFKBII} = \| fm_{SNFKBIIs} \| =$$
$$\| fm_{SNFKBII1},\ fm_{SNFKBII2},\ fm_{SNFKBII3},\ fm_{SNFKBII4},\ fm_{SNFKBII5} \| =$$
$$\|9{,}2;\ 6{,}6;\ 6{,}3;\ 6;\ 6{,}6\|,$$
$$FM_{SNFCOII} = \| fm_{SNFCOIIs} \| =$$
$$\| fm_{SNFCOII1},\ fm_{SNFCOII2},\ fm_{SNFCOII3} \| =$$
$$\|4;\ 2{,}5;\ 3{,}8\|,$$
$$FM_{SNFTII} = \| fm_{SNFTIIs} \| =$$
$$\| fm_{SNFTII1},\ fm_{SNFTII2},\ fm_{SNFTII3},\ fm_{SNFTII4} \| =$$
$$\|6;\ 4{,}3;\ 4;\ 5{,}7\|.$$

На основі $FM_{SNFKBII}$, $FM_{SNFCOII}$ та FM_{SNFTII} за виразом (2.47) сформуємо матриці функцій належності:

$$M_{SNFKBII} = \left\| \mu_{SNFKBIIsq} \right\| = \begin{Vmatrix} 1 & 0{,}5 & 0 & 0 & 0 \\ 0{,}2 & 1 & 0{,}3 & 0 & 0 \\ 0 & 0{,}2 & 1 & 0{,}2 & 0 \\ 0 & 0 & 0{,}5 & 1 & 0{,}7 \\ 0 & 0 & 0 & 0{,}7 & 1 \end{Vmatrix},$$

$$M_{SNFCOII} = \left\| \mu_{SNFCOIIsq} \right\| = \begin{Vmatrix} 1 & 0{,}5 & 0 \\ 0{,}3 & 1 & 0{,}3 \\ 0 & 0{,}5 & 1 \end{Vmatrix},$$

а також

$$M_{SNFTII} = \left\| \mu_{SNFTIIsq} \right\| = \begin{Vmatrix} 1 & 0,3 & 0 & 0 \\ 0,7 & 1 & 0,8 & 0 \\ 0 & 0,7 & 1 & 0,8 \\ 0 & 0,3 & 0,8 & 1 \end{Vmatrix},$$

де:

- $\mu_{SNFKBIIsq} = f'_{SNFKBIIsq} / fm_{SNFKBIIs}$, $(s,q = \overline{1,5})$,
- $\mu_{SNFCOIIsq} = f'_{SNFCOIIsq} / fm_{SNFCOIIs}$, $(s,q = \overline{1,3})$,
- $\mu_{SNFTIIsq} = f'_{SNFTIIsq} / fm_{SNFTIIs}$, $(s,q = \overline{1,4})$.

На основі отриманих даних $\mu_{SNFKBIIsq}$, $\mu_{SNFCOIIsq}$, $\mu_{SNFTIIsq}$ та обчислених за виразом (2.49) $x_{SNFKBIIsq}$, $x_{SNFCOIIsq}$, $x_{SNFTIIsq}$ визначимо набори нечітких термів відповідно до (2.48)

$$\underset{\sim}{T}_{SNFKBIIs} = \{ \mu_{SNFKBIIs1} / x_{SNFKBIIs1}, \ \mu_{SNFKBIIs2} / x_{SNFKBIIs2}, \ \mu_{SNFKBIIs3} / x_{SNFKBIIs3}, \ \mu_{SNFKBIIs4} / x_{SNFKBIIs4}, \ \mu_{SNFKBIIs5} / x_{SNFKBIIs5} \}, \quad (s,q = \overline{1,5}),$$

де, з урахуванням (2.49),

$$X_{SNFKBIIsq} = N^{max}_{SNFKBIIq} / N^{max}_{SNFKBIIr}, \ (q = \overline{1,5}) \text{ або}$$

$$\{ \bigcup_{q=1}^{5} X_{SNFKBIIsq} \} = \{0,03;0,13;0,25;0,5;1\}.$$

Далі, аналогічно, визначимо

$$\underset{\sim}{T}_{SNFCOIIs} = \{ \mu_{SNFCOIIs1} / x_{SNFCOIIs1}, \ \mu_{SNFCOIIs2} / x_{SNFCOIIs2}, \ \mu_{SNFCOIIs3} / x_{SNFCOIIs3} \}, \quad (s,q = \overline{1,3}),$$

де

$$X_{SNFCOIIsq} = N^{max}_{SNFCOIIq} / N^{max}_{SNFCOIIr}, \ (q = \overline{1,3}) \text{ або}$$

$$\{ \bigcup_{q=1}^{3} X_{SNFCOIIsq} \} = \{0,1;0,3;1\},$$

а також

$$\underset{\sim}{T}_{SNFTIIs} = \{ \mu_{SNFTIIs1} / x_{SNFTIIs1}, \ \mu_{SNFTIIs2} / x_{SNFTIIs2}, \ \mu_{SNFTIIs3} / x_{SNFTIIs3}, \ \mu_{SNFTIIs4} / x_{SNFTIIs4} \},$$

$$(s,q=\overline{1,4}),$$

де

$$X_{SNFTIIsq} = N^{max}_{SNFTIIq} / N^{max}_{SNFTIIr},\ (q=\overline{1,4})\text{ або}$$

$$\{\bigcup_{q=1}^{4} X_{SNFTIIsq}\} = \{0{,}08;0{,}4;0{,}5;1\}.$$

Таким чином, отримані члени підмножини $\mathbf{T_{SNFKBII}}$, $\mathbf{T_{SNFCOII}}$, $\mathbf{T_{SNFTII}}$ (числова форма), відповідно є відображенням членів підмножини $\mathbf{LE_{SNFKBII}}$, $\mathbf{LE_{SNFCOII}}$, $\mathbf{LE_{SNFTII}}$ (лінгвістична форма) та представляються у наступному вигляді:

$$\underset{\sim}{T}_{SNFKBII1} = \underset{\sim}{OM}_{SNFKBII} = \{1/0{,}03;\ 0{,}5/0{,}13;\ 0/0{,}25;\ 0/0{,}5;\ 0/1\};$$

$$\underset{\sim}{T}_{SNFKBII2} = \underset{\sim}{M}_{SNFKBII} = \{0{,}2/0{,}03;\ 1/0{,}13;\ 0{,}3/0{,}25;\ 0/0{,}5;\ 0/1\};$$

$$\underset{\sim}{T}_{SNFKBII3} = \underset{\sim}{C}_{SNFKBII} = \{0/0{,}03;\ 0{,}2/0{,}13;\ 1/0{,}25;\ 0{,}2/0{,}5;\ 0/1\};$$

$$\underset{\sim}{T}_{SNFKBII4} = \underset{\sim}{Б}_{SNFKBII} = \{0/0{,}03;\ 0/0{,}13;\ 0{,}5/0{,}25;\ 1/0{,}5;\ 0{,}7/1\};$$

$$\underset{\sim}{T}_{SNFKBII5} = \underset{\sim}{OБ}_{SNFKBII} = \{0/0{,}03;\ 0/0{,}13;\ 0/0{,}25;\ 0{,}7/0{,}5;\ 1/1\}\ \text{та}$$

$$\underset{\sim}{T}_{SNFCOII1} = \underset{\sim}{H}_{SNFCOII} = \{1/0{,}1;\ 0{,}5/0{,}3;\ 0/1\};$$

$$\underset{\sim}{T}_{SNFCOII2} = \underset{\sim}{C}_{SNFCOII} = \{0{,}3/0{,}1;\ 1/0{,}3;\ 0{,}3/1\};$$

$$\underset{\sim}{T}_{SNFCOII3} = \underset{\sim}{B}_{SNFCOII} = \{0/0{,}1;\ 0{,}5/0{,}3;\ 1/1\},$$

а також

$$\underset{\sim}{T}_{SNFTII1} = \underset{\sim}{H}_{SNFTII} = \{1/0{,}08;\ 0{,}3/0{,}4;\ 0/0{,}5;\ 0/1\};$$

$$\underset{\sim}{T}_{SNFTII2} = \underset{\sim}{C}_{SNFTII} = \{0{,}7/0{,}08;\ 1/0{,}4;\ 0{,}8/0{,}5;\ 0/1\};$$

$$\underset{\sim}{T}_{SNFTII3} = \underset{\sim}{B}_{SNFTII} = \{0/0{,}08;\ 0{,}7/0{,}4;\ 1/0{,}5;\ 0{,}8/1\};$$

$$\underset{\sim}{T}_{SNFTII4} = \underset{\sim}{OB}_{SNFTII} = \{0/0{,}08;\ 0{,}3/0{,}4;\ 0{,}8/0{,}5;\ 1/1\}.$$

Далі, відповідно до етапу 5 виразу (2.52) сформуємо НЧ $\mathbf{T^e_{SNFKBII} \subseteq T^e}$, $\mathbf{T^e_{SNFCOII} \subseteq T^e}$, $\mathbf{T^e_{SNFTII} \subseteq T^e}$ еталонного підсередовища ($\mathbf{T^e_i = T^e_{SNF}}$):

$$\mathbf{T}^{\mathbf{e}}_{\mathbf{SNFKBII}} = \{\bigcup_{s=1}^{5} \underset{\sim}{T}^{e}_{SNFKBIIs}\} =$$

$$\{\underset{\sim}{T}^{e}_{SNFKBII1}, \underset{\sim}{T}^{e}_{SNFKBII2}, \underset{\sim}{T}^{e}_{SNFKBII3}, \underset{\sim}{T}^{e}_{SNFKBII4}, \underset{\sim}{T}^{e}_{SNFKBII5}\} =$$

$$\{\underset{\sim}{OM}^{e}_{SNFKBII}, \underset{\sim}{M}^{e}_{SNFKBII}, \underset{\sim}{C}^{e}_{SNFKBII}, \underset{\sim}{Б}^{e}_{SNFKBII}, \underset{\sim}{OБ}^{e}_{SNFKBII}\},$$

$$(s = \overline{1,5}),$$

$$\mathbf{T}^{\mathbf{e}}_{\mathbf{SNFCOII}} = \{\bigcup_{s=1}^{3} \underset{\sim}{T}^{e}_{SNFCOIIs}\} = \{\underset{\sim}{T}^{e}_{SNFCOII1}, \underset{\sim}{T}^{e}_{SNFCOII2}, \underset{\sim}{T}^{e}_{SNFCOII3}\} =$$

$$\{\underset{\sim}{H}^{e}_{SNFCOII}, \underset{\sim}{C}^{e}_{SNFCOII}, \underset{\sim}{B}^{e}_{SNFCOII}\},$$

$$(s = \overline{1,3}),$$

$$\mathbf{T}^{\mathbf{e}}_{\mathbf{SNFTII}} = \{\bigcup_{s=1}^{4} \underset{\sim}{T}^{e}_{SNFTIIs}\} =$$

$$\{\underset{\sim}{T}^{e}_{SNFTII1}, \underset{\sim}{T}^{e}_{SNFTII2}, \underset{\sim}{T}^{e}_{SNFTII3}, \underset{\sim}{T}^{e}_{SNFTII4}\} =$$

$$\{\underset{\sim}{H}^{e}_{SNFTII}, \underset{\sim}{C}^{e}_{SNFTII}, \underset{\sim}{B}^{e}_{SNFTII}, \underset{\sim}{OB}^{e}_{SNFTII}\},$$

$$(s = \overline{1,4}),$$

де члени підмножини

- $\mathbf{T}^{\mathbf{e}}_{\mathbf{SNFKBII}} - \underset{\sim}{OM}^{e}_{SNFKBII}, \underset{\sim}{M}^{e}_{SNFKBII}, \underset{\sim}{C}^{e}_{SNFKBII}, \underset{\sim}{Б}^{e}_{SNFKBII}, \underset{\sim}{OБ}^{e}_{SNFKBII}$;
- $\mathbf{T}^{\mathbf{e}}_{\mathbf{SNFCOII}} - \underset{\sim}{H}^{e}_{SNFCOII}, \underset{\sim}{C}^{e}_{SNFCOII}, \underset{\sim}{B}^{e}_{SNFCOII}$;
- $\mathbf{T}^{\mathbf{e}}_{\mathbf{SNFTII}} - \underset{\sim}{H}^{e}_{SNFTII}, \underset{\sim}{C}^{e}_{SNFTII}, \underset{\sim}{B}^{e}_{SNFTII}, \underset{\sim}{OB}^{e}_{SNFTII}$

є НЧ, що складають основу еталонного підсередовища ($\mathbf{T}^{\mathbf{e}}_{\mathbf{i}} = \mathbf{T}^{\mathbf{e}}_{\mathbf{SNF}}$).

Далі перетворимо нечіткі терми

$$\underset{\sim}{OM}_{SNFKBII}, \underset{\sim}{M}_{SNFKBII}, \underset{\sim}{C}_{SNFKBII}, \underset{\sim}{Б}_{SNFKBII}, \underset{\sim}{OБ}_{SNFKBII},$$

$$\underset{\sim}{H}_{SNFCOII}, \underset{\sim}{C}_{SNFCOII}, \underset{\sim}{B}_{SNFCOII} \text{ та}$$

$$\underset{\sim}{H}_{SNFTII}, \underset{\sim}{C}_{SNFTII}, \underset{\sim}{B}_{SNFTII}, \underset{\sim}{OB}_{SNFTII}.$$

таким чином, щоб для всіх $\underset{\sim}{T}_{SNFKBIIs}$, $\underset{\sim}{T}_{SNFCOIIs}$ та $\underset{\sim}{T}_{SNFTIIs}$ було справедливо відношення порядку, тобто

$$\forall x_{SNFKBIIsq} : x_{SNFKBIIsq} < x_{SNFKBIIsq+1},\ (q = \overline{1,5}),$$

$$\forall x_{SNFCOIIsq} : x_{SNFCOIIsq} < x_{SNFCOIIsq+1},\ (q = \overline{1,3})\ \text{і}$$

$$\forall x_{SNFTIIsq} : x_{SNFTIIsq} < x_{SNFTIIsq+1},\ (q = \overline{1,4})$$

(відповідно до кроку 1, етапу 5 (див. п. 2.2)).

Якщо за компоненти таких термів використовувати конкретні значення, отримані у вище описаному прикладі, то для них таке відношення буде істинним. Так, наприклад, для $\underset{\sim}{OM}_{SNFKBII}$ це

$$x_{SNFKBII1} < x_{SNFKBII2} < x_{SNFKBII3} < x_{SNFKBII4} < x_{SNFKBII5} =$$
$$0{,}03 < 0{,}13 < 0{,}25 < 0{,}5 < 1.$$

Також, аналогічно, буде істинним відношення для $\underset{\sim}{H}_{SNFCOII}$, тобто

$$x_{SNFCOII1} < x_{SNFCOII2} < x_{SNFCOII3} =$$
$$0{,}1 < 0{,}3 < 1,$$

та для $\underset{\sim}{H}_{SNFTII}$ це

$$x_{SNFTII1} < x_{SNFTII2} < x_{SNFTII3} < x_{SNFTII4} =$$
$$0{,}08 < 0{,}4 < 0{,}5 < 1.$$

Далі, відповідно до кроку 2 етапу 5 (див. п. 2.2), для кожного $\underset{\sim}{T}_{SNFKBIIs}$ реалізуємо процедуру поглинання.

Для $\underset{\sim}{OM}_{SNFKBII}$ (де мода $x_{SNFKBII1M} = x_{SNFKBII1} = 0{,}03$, а її порядковий номер $M = 1$) при умові U_2 (тобто $\mu_{SNFKBII3} = \mu_{SNFKBII4} = \mu_{SNFKBII5} = 0$) здійснюється поглинання одним компонентом $0 / x^{max}_{SNFKBII1}$ низку інших відповідно до виразу

$$x^{max}_{SNFKBII1} = x_{SNFKBII3} \wedge x_{SNFKBII4} \wedge x_{SNFKBII5} =$$
$$0{,}25 \wedge 0{,}5 \wedge 1 = 0{,}25,$$
$$(q = \overline{1,5}).$$

Таким чином,

$$\mu_{SNFKBII3} / x_{SNFKBII3} = 0 / 0{,}25,$$

$$\mu_{SNFKBП14} / x_{SNFKBП14} = 0 / 0{,}5,$$
$$\mu_{SNFKBП15} / x_{SNFKBП15} = 0 / 1$$

поглинаються компонентом

$$\mu_{SNFKBП13} / x_{SNFKBП13} = 0 / 0{,}25.$$

Аналогічно, для $\underset{\sim}{M}_{SNFKBП}$ (де мода $x_{SNFKBП2M} = x_{SNFKBП21} = 0{,}13$, а її порядковий номер $M = 2$) при умові U_2 (тобто $\mu_{SNFKBП24} = \mu_{SNFKBП25} = 0$) здійснюється поглинання одним компонентом

$$0 / x^{max}_{SNFKBП2} = \mu_{SNFKBП24} / x_{SNFKBП24} = 0 / 0{,}5$$

відповідно до виразу

$$x^{max}_{SNFKBП2} = x_{SNFKBП24} \wedge x_{SNFKBП25} = 0{,}5 \wedge 1 = 0{,}5.$$

Таким чином,

$$\mu_{SNFKBП24} / x_{SNFKBП24} = 0 / 0{,}5 \text{ та}$$
$$\mu_{SNFKBП25} / x_{SNFKBП25} = 0 / 1$$

поглинаються компонентом

$$\mu_{SNFKBП24} / x_{SNFKBП24} = 0 / 0{,}5.$$

Далі видно, що для НЧ $\underset{\sim}{C}_{SNFKBП}$ умови U_1 та U_2 не виконуються і тому операція поглинання не здійснюється.

Для $\underset{\sim}{Б}_{SNFKBП}$ (де мода $x_{SNFKBП4M} = x_{SNFKBП41} = 0{,}5$, а її порядковий номер $M = 4$) при умові U_1 (тобто $\mu_{SNFKBП41} = \mu_{SNFKBП42} = 0$) компонент

$$0 / x^{min}_{SNFKBП4} = \mu_{SNFKBП42} / x_{SNFKBП42} = 0 / 0{,}13$$

відповідно до виразу

$$x^{min}_{SNFKBП4} = x_{SNFKBП41} \vee x_{SNFKBП42} = 0{,}03 \vee 0{,}13 = 0{,}13,$$

а отримане значення

$$\mu_{SNFKBП41} / x_{SNFKBП42} = 0 / 0{,}03 \text{ та}$$
$$\mu_{SNFKBП42} / x_{SNFKBП42} = 0 / 0{,}13$$

поглинається компонентом

$$\mu_{SNFKBП41} / x_{SNFKBП42} = 0 / 0{,}03.$$

Аналогічно, для $\underset{\sim}{ОБ}_{SNFKBП}$ ($x_{SNFKBП5M} = x_{SNFKBП55} = 1,$ а її порядковий номер $M = 5$) при умові U_1 (тобто $\mu_{SNFKBП51} = \mu_{SNFKBП52} = \mu_{SNFKBП53} = 0$) здійснюється поглинання одним компонентом

$$0 / x^{min}_{SNFKBП5}$$

низки інших відповідно до виразу

$$x^{min}_{SNFKBП5} = x_{SNFKBП51} \vee x_{SNFKBП52} \vee x_{SNFKBП53} = 0,03 \vee 0,13 \vee 0,25 = 0,25.$$

Таким чином,

$$\mu_{SNFKBП51} / x_{SNFKBП51} = 0 / 0,03,$$
$$\mu_{SNFKBП52} / x_{SNFKBП52} = 0 / 0,13,$$
$$\mu_{SNFKBП53} / x_{SNFKBП53} = 0 / 0,25$$

поглинаються компонентом

$$\mu_{SNFKBП53} / x_{SNFKBП53} = 0 / 0,25.$$

Далі, для кожного $\underset{\sim}{Н}_{SNFCOП}$, $\underset{\sim}{С}_{SNFCOП}$, $\underset{\sim}{В}_{SNFCOП}$ умова U_1 та U_2 не виконуються та тому операція поглинання на здійснюється, а для $\underset{\sim}{Н}_{SNFTП}$, $\underset{\sim}{С}_{SNFTП}$, $\underset{\sim}{В}_{SNFTП}$, $\underset{\sim}{ОВ}_{SNFTП}$ виконується тільки умова U_1.

З урахуванням описаних перетворень, а також виразу (2.51), визначимо проміжні терми у вигляді:

$$\underset{\sim}{Т}'_{SNFKBП1} = \underset{\sim}{ОМ}'_{SNFKBП} = \{1 / 0,03; 0,5 / 0,13; 0 / 0,25\};$$

$$\underset{\sim}{Т}'_{SNFKBП2} = \underset{\sim}{М}'_{SNFKBП} = \{0,2 / 0,03; 1 / 0,13; 0,3 / 0,25; 0 / 0,5\};$$

$$\underset{\sim}{Т}'_{SNFKBП3} = \underset{\sim}{С}'_{SNFKBП} = \{0 / 0,03; 0,2 / 0,13; 1 / 0,25; 0,2 / 0,5; 0 / 1\};$$

$$\underset{\sim}{Т}'_{SNFKBП4} = \underset{\sim}{Б}'_{SNFKBП} = \{0 / 0,13; 0,5 / 0,25; 1 / 0,5; 0,7 / 1\};$$

$$\underset{\sim}{Т}'_{SNFKBП5} = \underset{\sim}{ОБ}'_{SNFKBП} = \{0 / 0,25; 0,7 / 0,5; 1 / 1\}$$

та

$$\underset{\sim}{Т}'_{SNFCOП1} = \underset{\sim}{Н}'_{SNFCOП} = \{1 / 0,1; 0,5 / 0,3; 0 / 1\};$$

$$\underset{\sim}{Т}'_{SNFCOП2} = \underset{\sim}{С}'_{SNFCOП} = \{0,3 / 0,1; 1 / 0,3; 0,3 / 1\};$$

$$\underset{\sim}{Т}'_{SNFCOП3} = \underset{\sim}{В}'_{SNFCOП} = \{0 / 0,1; 0,5 / 0,3; 1 / 1\},$$

а також

$$\underset{\sim}{T}'_{SNFTII1} = \underset{\sim}{H}'_{SNFTII} = \{1 / 0{,}08; 0{,}3 / 0{,}4; 0 / 0{,}5\};$$

$$\underset{\sim}{T}'_{SNFTII2} = \underset{\sim}{C}'_{SNFTII} = \{0{,}7 / 0{,}08; 1 / 0{,}4; 0{,}8 / 0{,}5; 0 / 1\};$$

$$\underset{\sim}{T}'_{SNFTII3} = \underset{\sim}{B}'_{SNFTII} = \{0 / 0{,}08; 0{,}7 / 0{,}4; 1 / 0{,}5; 0{,}8 / 1\};$$

$$\underset{\sim}{T}'_{SNFTII4} = \underset{\sim}{QB}'_{SNFTII} = \{0 / 0{,}08; 0{,}3 / 0{,}4; 0{,}8 / 0{,}5; 1 / 1\}.$$

Відповідно до кроку 3 етапу 5 (див. п. 2.2), при реалізації другого кроку у формулі (2.51) для набору проміжних термів $\underset{\sim}{QM}'_{SNFKBII}$ та $\underset{\sim}{M}'_{SNFKBII}$

$$\exists \underset{\sim}{T}'_{SNFKBII1} : \{0 / x^{min}_{SNFKBII1}\} \in \varnothing \text{ та}$$

$$\exists \underset{\sim}{T}'_{SNFKBII2} : \{0 / x^{min}_{SNFKBII2}\} \in \varnothing$$

(тобто $\mu_{SNFKBII11} = 1 \neq 0$ і

$\mu_{SNFKBII21} = 0{,}2 \neq 0$),

а для $\underset{\sim}{Б}'_{SNFKBII}$ та $\underset{\sim}{QБ}'_{SNFKBII}$

$$\exists \underset{\sim}{T}'_{SNFKBII4} : \{0 / x^{max}_{SNFKBII4}\} \in \varnothing \text{ та}$$

$$\exists \underset{\sim}{T}'_{SNFKBII5} : \{0 / x^{max}_{SNFKBII5}\} \in \varnothing$$

(тобто $\mu_{SNFKBII45} = 0{,}67 \neq 0$ і

$\mu_{SNFKBII55} = 1 \neq 0$),

то формування підмножин

$$\underset{\sim}{T}^{e}_{SNFKBII1},\ \underset{\sim}{T}^{e}_{SNFKBII2} \text{ та } \underset{\sim}{T}^{e}_{SNFKBII4},\ \underset{\sim}{T}^{e}_{SNFKBII5}$$

здійснимо за рахунок розширення

$$\underset{\sim}{T}'_{SNFKBII1},\ \underset{\sim}{T}'_{SNFKBII2} \text{ та } \underset{\sim}{T}'_{SNFKBII4},\ \underset{\sim}{T}'_{SNFKBII5}$$

(див. (2.51)) шляхом введення додаткових

$$\mu_{SNFKBII1\beta-1} / x_{SNFKBII1\beta-1} = 0 / 0{,}3,$$

$$\mu_{SNFKBII2\beta-1} / x_{SNFKBII2\beta-1} = 0 / 0{,}3 \text{ та}$$

$$\mu_{SNFKBII4r_j-\gamma+2} / x_{SNFKBII4r_j-\gamma+2} = 0 / 1,$$

$$\mu_{SNFKBII5r_j-\gamma+2} / x_{SNFKBII5r_j-\gamma+2} = 0 / 1$$

і відповідно, після чого в НЧ здійснюється переіндексація компонент починаючи з першої.

З урахування цього, набір проміжних термів для $\underset{\sim}{QM}'_{SNFKBП}$ буде мати наступний вигляд

$$\underset{\sim}{T}'_{SNFKBП1} = \underset{\sim}{QM}'_{SNFKBП} =$$
$$\{\mu_{SNFKBП11} / x_{SNFKBП11},\ \mu_{SNFKBП12} / x_{SNFKBП12},$$
$$\mu_{SNFKBП13} / x_{SNFKBП13},\ \mu_{SNFKBП14} / x_{SNFKBП14}\} =$$
$$\{0 / 0{,}03; 1 / 0{,}03; 0{,}5 / 0{,}13; 0 / 0{,}25\},$$

де $\mu_{SNFKBП1\beta\text{-}1} = 0.$

Аналогічним чином, отримуємо проміжні терми для

$$\underset{\sim}{M}'_{SNFKBП},\ \underset{\sim}{Б}'_{SNFKBП} \text{ та } \underset{\sim}{QБ}'_{SNFKBП},$$

де $\mu_{SNFKBП2\beta\text{-}1} = \mu_{SNFKBП4r_j\text{-}\gamma+2} = \mu_{SNFKBП5r_j\text{-}\gamma+2} = 0.$

Таким чином, компоненти підмножини еталонів $\underset{\sim}{T}^e_{SNFKBП1}$ відповідно до (2.52) будуть визначатися як

$$\mu^e_{SNFKBП11} / x^e_{SNFKBП11} = 0 / 0{,}03,$$
$$\mu^e_{SNFKBП12} / x^e_{SNFKBП12} = 1 / 0{,}03,$$
$$\mu^e_{SNFKBП13} / x^e_{SNFKBП13} = 0{,}5 / 0{,}13,$$
$$\mu^e_{SNFKBП14} / x^e_{SNFKBП14} = 0 / 0{,}25$$

Та, аналогічним чином, для $\underset{\sim}{T}^e_{SNFKBП2}$, $\underset{\sim}{T}^e_{SNFKBП4}$, $\underset{\sim}{T}^e_{SNFKBП5}$.

Далі, відповідно до (2.52), для $\underset{\sim}{QM}'_{SNFKBП}$, $\underset{\sim}{M}'_{SNFKBП}$, $\underset{\sim}{Б}'_{SNFKBП}$, $\underset{\sim}{QБ}'_{SNFKBП}$ сформуємо еталонні значення, тобто:

$$\underset{\sim}{T}^e_{SNFKBП1} = \underset{\sim}{QM}^e_{SNFKBП} = \{0 / 0{,}03; 1 / 0{,}03; 0{,}5 / 0{,}13; 0 / 0{,}25\};$$
$$\underset{\sim}{T}^e_{SNFKBП2} = \underset{\sim}{M}^e_{SNFKBП} = \{0 / 0{,}03; 0{,}2 / 0{,}03; 1 / 0{,}13; 0{,}3 / 0{,}25; 0 / 0{,}5\};$$
$$\underset{\sim}{T}^e_{SNFKBП3} = \underset{\sim}{C}^e_{SNFKBП} = \{0 / 0{,}03; 0{,}2 / 0{,}13; 1 / 0{,}25; 0{,}2 / 0{,}5; 0 / 1\};$$
$$\underset{\sim}{T}^e_{SNFKBП4} = \underset{\sim}{Б}^e_{SNFKBП} = \{0 / 0{,}13; 0{,}5 / 0{,}25; 1 / 0{,}5; 0{,}7 / 1; 0 / 1\};$$
$$\underset{\sim}{T}^e_{SNFKBП5} = \underset{\sim}{QБ}^e_{SNFKBП} = \{0 / 0{,}25; 0{,}7 / 0{,}5; 1 / 1; 0 / 1\}.$$

Також, за аналогією формуються і наступні еталонні значення:

$$\underset{\sim}{T}^{e}_{SNFCOII1} = \underset{\sim}{H}^{e}_{SNFCOII} = \{0 / 0,1; 1 / 0,1; 0,5 / 0,3; 0 / 1\};$$

$$\underset{\sim}{T}^{e}_{SNFCOII2} = \underset{\sim}{C}^{e}_{SNFCOII} = \{0 / 0,1; 0,3 / 0,1; 1 / 0,3; 0,3 / 1; 0 / 1\};$$

$$\underset{\sim}{T}^{e}_{SNFCOII3} = \underset{\sim}{B}^{e}_{SNFCOII} = \{0 / 0,1; 0,5 / 0,3; 1 / 1; 0 / 1\}$$

та

$$\underset{\sim}{T}^{e}_{SNFTII1} = \underset{\sim}{H}^{e}_{SNFTII} = \{0 / 0,08; 1 / 0,08; 0,3 / 0,4; 0 / 0,5\};$$

$$\underset{\sim}{T}^{e}_{SNFTII2} = \underset{\sim}{C}^{e}_{SNFTII} = \{0 / 0,08; 0,7 / 0,08; 1 / 0,4; 0,8 / 0,5; 0 / 1\};$$

$$\underset{\sim}{T}^{e}_{SNFTII3} = \underset{\sim}{B}^{e}_{SNFTII} = \{0 / 0,08; 0,7 / 0,4; 1 / 0,5; 0,8 / 1\};$$

$$\underset{\sim}{T}^{e}_{SNFTII4} = \underset{\sim}{QB}^{e}_{SNFTII} = \{0 / 0,08; 0,3 / 0,4; 0,8 / 0,5; 1 / 1\}.$$

Далі, з урахуванням етапу 6 (див. п. 2.2) для підмножини еталонів $\mathbf{T}^{e}_{SNFKBII}$, $\mathbf{T}^{e}_{SNFCOII}$ і $\mathbf{T}^{e}_{SNFTII}$ з використанням отриманих конкретних значень можна реалізувати їх графічну інтерпретацію, скориставшись необхідними НЧ еталонного підсередовища ($\mathbf{T}^{e}_{i} = \mathbf{T}^{e}_{SNF}$), будуються п'ять (див. рис. 2.8), три (див. рис. 2.9) та чотири (див. рис. 2.10) ламані відповідно.

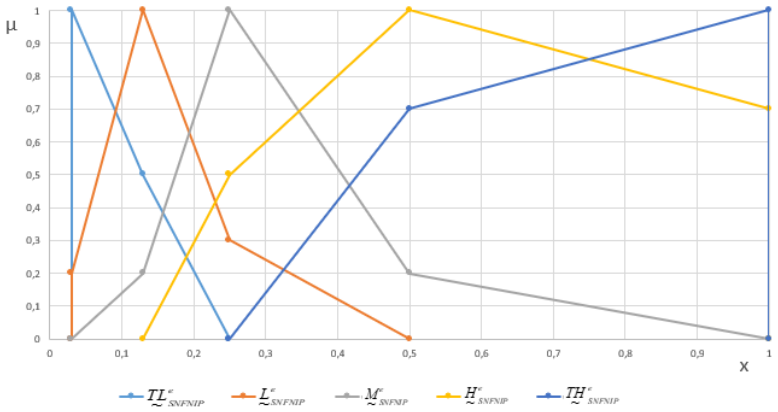

Рис. 2.8. Лінгвістичні еталони підмножини $\mathbf{T}^{e}_{SNFKBII}$

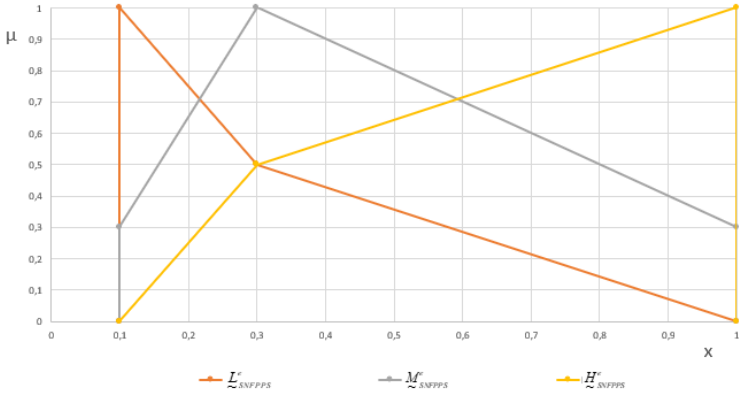

Рис. 2.9. Лінгвістичні еталони підмножини $\mathbf{T}^{e}_{\mathbf{SNFCOП}}$

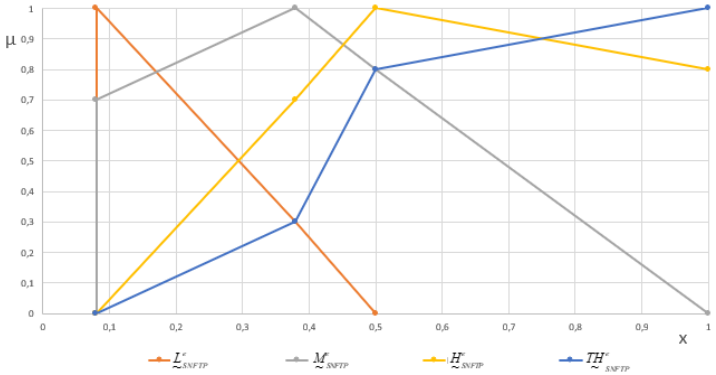

Рис. 2.10. Лінгвістичні еталони підмножини $\mathbf{T}^{e}_{\mathbf{SNFTП}}$

Запропонований в роботі МФЕПСА [14], який за рахунок сформованого набору параметрів КВП, СОП, ТП та експертного оцінювання стану середовища оточення інформаційної системи дозволить формалізувати процес формування параметрів еталонного підсередовища для вирішення задач, щодо виявлення сніфінг-атак на ІС.

Запропонований метод може бути використаний для підвищення ефективності засобів захисту інформації, що спрямовані на протидію сніфінг-атакам в ІС.

2.4. Метод побудови еталонів лінгвістичних змінних для систем виявлення email-спуфінг-атак

Як зазначалося, спуфінг-атаки є одними з найнебезпечніших засобів реалізації хакерських вторгнень. Спуфінгове ПЗ вводить користувача в оману, маскуючись під реально існуючі web-сервіси та інші програмні застосунки. Одним із поширених видів спуфінгу є email-спуфінг – вид атаки, направлений на підробку email даних (адреса відправника, тема, текст чи вкладення). При такому впливі користувачу надсилається лист на електронну пошту, який майже нічим не відрізняється від авторизованих (рис. 2.11).

Подібний лист, зазвичай, містить посилання чи вкладення, які часто активує користувач, в результаті чого НАС може отримати доступ, наприклад, до персональних даних користувача, як-от логіни та паролі, номери банківських рахунків, особистої інформації тощо.

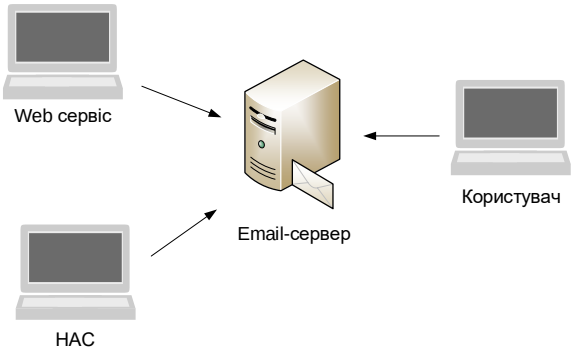

Рис. 2.11. Схема реалізації email-спуфінгу

Зазвичай, фальсифікована адреса є частиною більш масштабної фішингової атаки, метою якої є отримання даних доступу користувача до певних сервісів чи ПЗ, однак подібні атаки можуть використовуватись і для розповсюдження неліцензійного ПЗ.

Головна мета email-спуфінгу направлена на змушення користувача довіряти отриманому електронному листу. Тому подібні листи мають оформлення і наповнення максимально подібне до листів, що надсилають аутентичні сервіси. Зазвичай, подібні спуфінгові листи

містять посилання, які здійснюють переадресацію на фальсифікований сайт чи web-сервіс, який теж буде максимально схожий на автентичний. Такими сервісами можуть бути платні web-служби, онлайн банки тощо. Після переходу на такий сайт користувач, як правило, вводить свої особисті дані (логін, пароль, банківські реквізити тощо). Ця інформація одразу буде доступна НАС і може бути використана нею для протиправних дій на автентичному web-сервісі чи сайті. Зазвичай, користувач у такому випадку отримує повідомлення про відмову в обробці даних.

Оскільки пряме виявлення email-спуфінгу є досить складним завданням, то для ідентифікації таких кібератак необхідно визначити можливі варіації певних величин середовища оточення, значення яких при проведенні атаки буде відрізнятись від нормального стану.

Як показує практика, електронні листи, що пересилаються під час зазначеної атаки можна виявити шляхом контроля параметрів КСБ, КСТ та КСС (див. п. 2.1).

Для успішного проведення кібератаки з урахуванням [17, 18] НАС необхідно лише знати email користувача та сайт, що буде імітувати роботу автентичного web-сервісу, на який його буде перенаправлено за допомогою інформації з електронного листа. Якщо в значення описаних параметрів характерних для нормальної роботи клієнта будуть певні відхилення від допустимих меж, то це може бути сигналом, що даний лист є частиною email-спуфінг-атаки.

Для отримання конкретних значень необхідних параметрів було проведене відповідне моделювання з використанням наступного ПЗ:

- MXToolBox SuperTool7,
- Subject Line,
- Mailing Check.

Дане ПЗ має достатню кількість засобів для ідентифікації email-спуфінг атак за описаними параметрами.

Наприклад, значна величина КСБ може служити ознакою того, що лист, який аналізується, є частиною email-спуфінг атаки. Максимальний показник цього параметра $(max_{КСБ})$ обмежений кількістю актуальних спам-баз, за якими здійснюється сканування.

В процесі моделювання, під час аналізу спуфінгового листа було зафіксовано *32* IP-адреси у спам-базах, тобто можемо припустити

що $max_{КСБ} = 32$ (рис. 2.12). При аналізі нормальних листів, здійсненого за допомогою утиліти MXToolBox SuperTool7 [19] величина зазначеного параметру не перевищувала *7* (рис. 2.13-2.14).

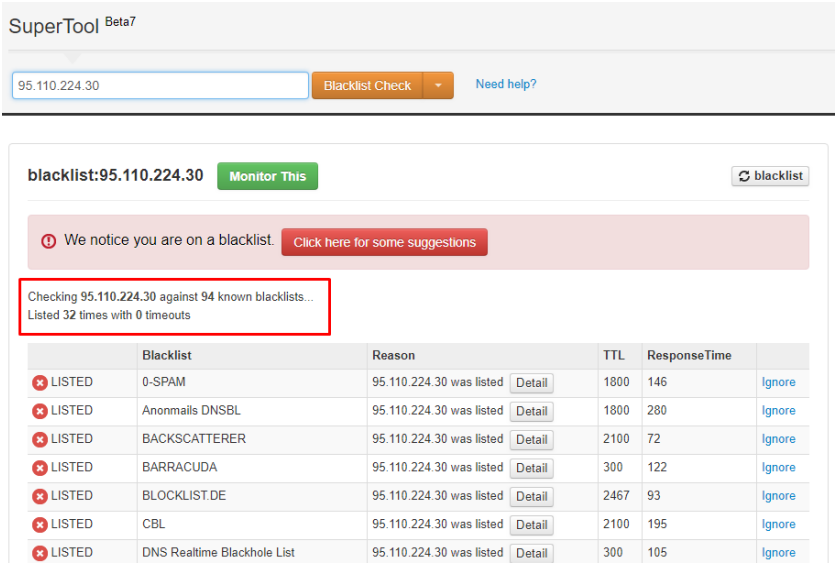

Рис. 2.12. Моделювання максимальної величини КСБ за допомогою утиліти MXToolBox SuperTool7

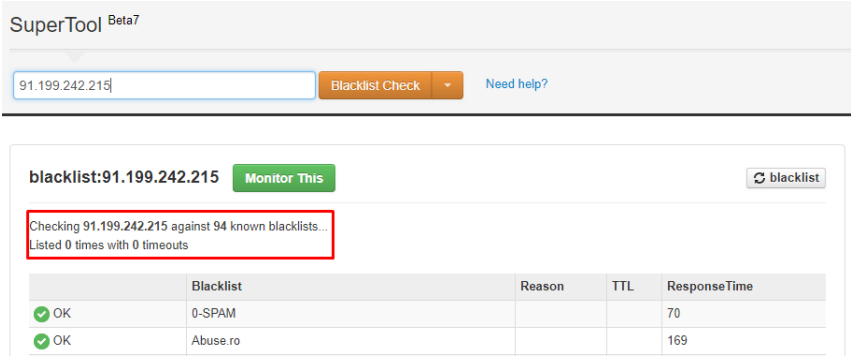

Рис. 2.13. Моделювання мінімальної величини КСБ за допомогою утиліти MXToolBox SuperTool7

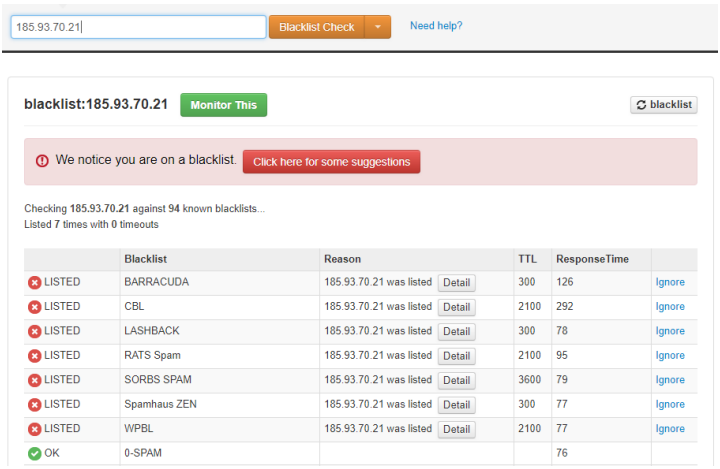

Рис. 2.14. Моделювання малої величини КСБ за допомогою утиліти MXToolBox SuperTool7

Також встановлені середні та високі показники таких IP-адрес, їх значення *11* та *21* відповідно (рис. 2.15-2.16).

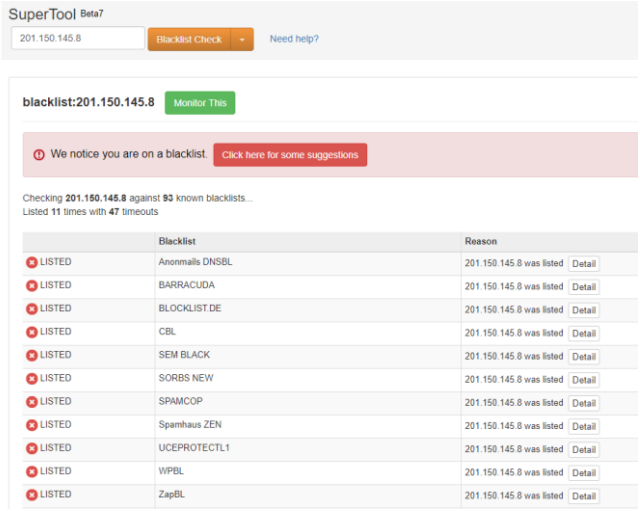

Рис. 2.15. Моделювання середньої величини КСБ за допомогою утиліти MXToolBox SuperTool7

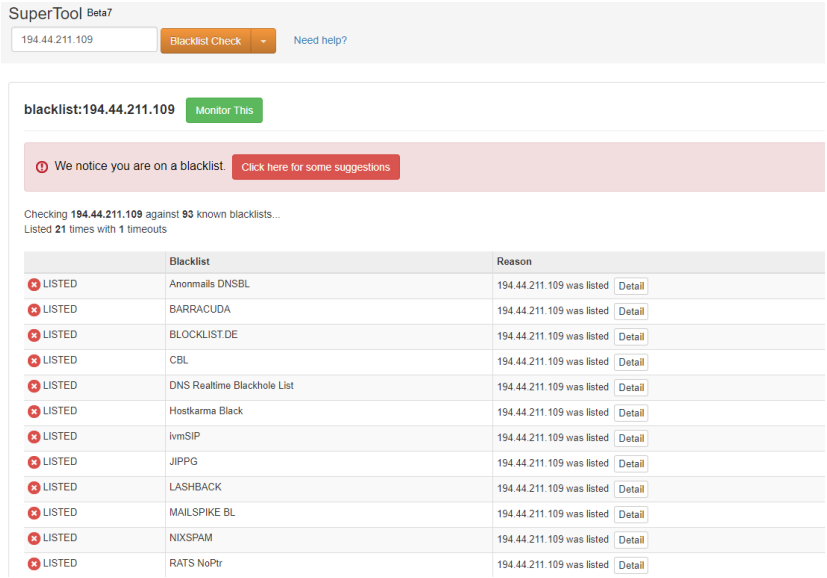

Рис. 2.16. Моделювання високої величини КСБ за допомогою утиліти MXToolBox SuperTool7

Для оцінювання різних величин на основі суджень експерта найбільш раціонально використовувати від *3*-х до *5*-ти градацій (термів) їх певної характеристики, але багато програмних застосунків в основному засновуються на мінімальній кількості термів [13], за допомогою яких характеризують визначену величину. Виходячи з результатів моделювання параметра КСБ використаємо *4* терма, які відображаються на інтервалах – $[0;8]$, $[9;16]$, $[17;24]$, $[25;32]$.

Параметр КСТ є одним за найважливіших при перевірці електронних листів на предмет причетності до email-спуфінг атак, оскільки відображає кількість спам-слів у темі повідомлення. Зазвичай, користувач у власному email-клієнті приймає рішення про відкриття листа на основі його теми, оскільки вона, як і відправник, відображаються у швидкому перегляді в переліку листів. Велика кількість спам-слів у темі листа може бути свідченням того, що він є фальсифікованим і може бути частиною відповідної атаки. Утиліта Subject Line [20] дає можливість проаналізувати тему на предмет наявності

спам слів, максимальна кількість яких у даному випадку визначається параметром max_{KCT}. В ході моделювання з використанням відповідного ПЗ значення $max_{KCT} = 12$ спам-ознакам (рис. 2.17). При аналізі було виявлено такі ознаки, як помилка першого слова та символа у темі, повторення великих літер, послідовність пробілів, повторювання одних і тих самих слів у темі тощо. Відповідно до цього і визначається максимальна величина параметра КСТ. Слід зазначити, що при аналізі нормального електронного листа, відповідний показник не перевищував *3*-х спам-ознак (рис. 2.18), які включають цифровий символ на початку теми, довжину теми та наявність послідовних цифрових символів.

На основі цього, для параметру КСТ сформовані інтервали $[0;4]$, $[5;8]$, $[9;12]$, які відображають діапазони мінімальних, середніх та максимальних можливих значень для даного параметру.

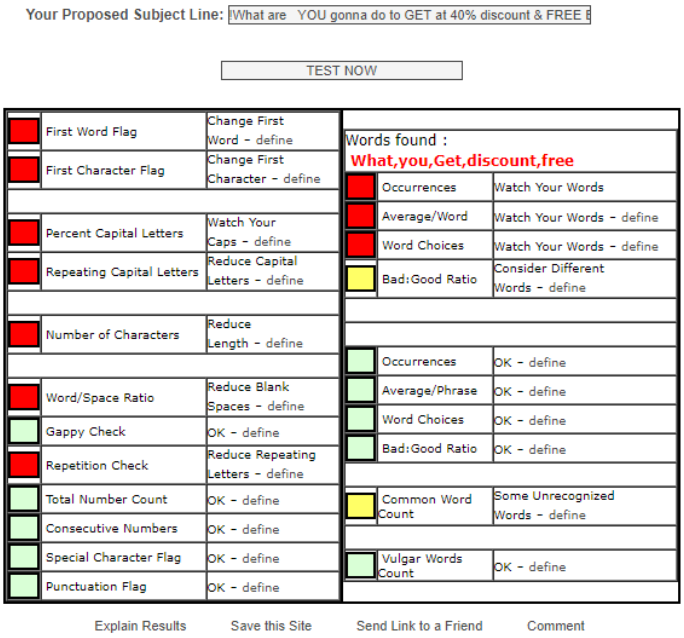

Рис. 2.17. Моделювання величини КСТ за допомогою утиліти Subject Line tester

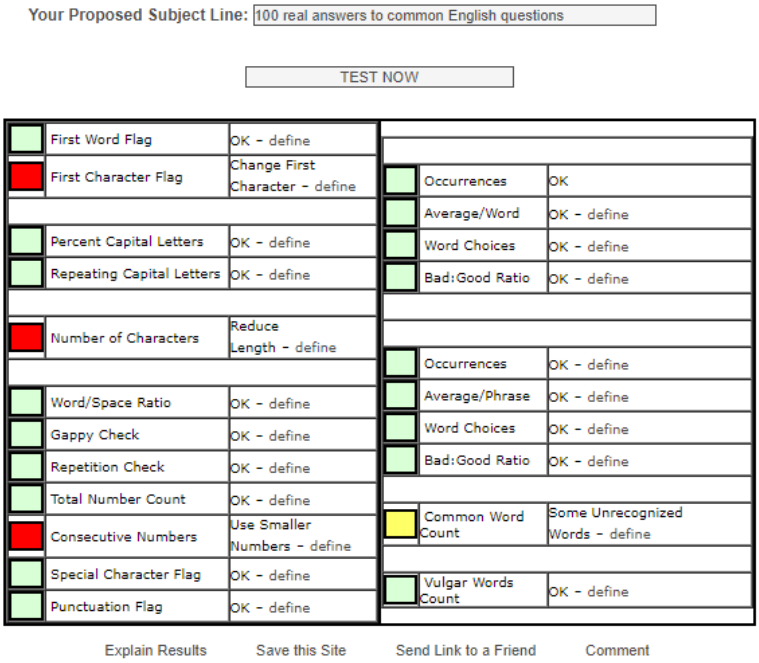

Рис. 2.18. Моделювання величини КСТ у нормальному режимі за допомогою утиліти Subject Line tester

Для роботи з КСС необхідно проводити більш детальний аналіз, оскільки текст повідомлення може містити не тільки символи, а і зображення, html розмітку, посилання тощо.

Даний параметр описує кількість виявлених спам-ознак у повідомленні і може сигналізувати про реалізацію email-спуфінгу на користувача.

Максимальна величина КСС (max_{KCC}) визначається максимальною кількістю спам-ознак, що можуть бути виявлені у відповідному повідомленні. Для їх ідентифікації необхідно скористатись утилітою Mailing Check. Для цього потенційний спам-лист завантажується до утиліти у форматі .eml і далі вона аналізує його вміст та формує виявлені спам-ознаки. Кожна така ознака має певну кількість спам-балів, що впливають на загальну оцінку листа. Проаналізувавши усі

спам-ознаки отримаємо інтегровані спам-бали, що відображають параметр КСС.

При аналізі безпечного електронного листа значення КСС, як правило, не перевищує *2* (рис. 2.19). При цьому у листі було виявлено такі *4* потенційні спам-ознаки, як велика кількість html розмітки та вставлених зображень, велика довжина рядка в листі та наявність у ньому табличних даних.

Таким чином, за допомогою утиліти було отримано спам-рейтинг листа *1,4*.

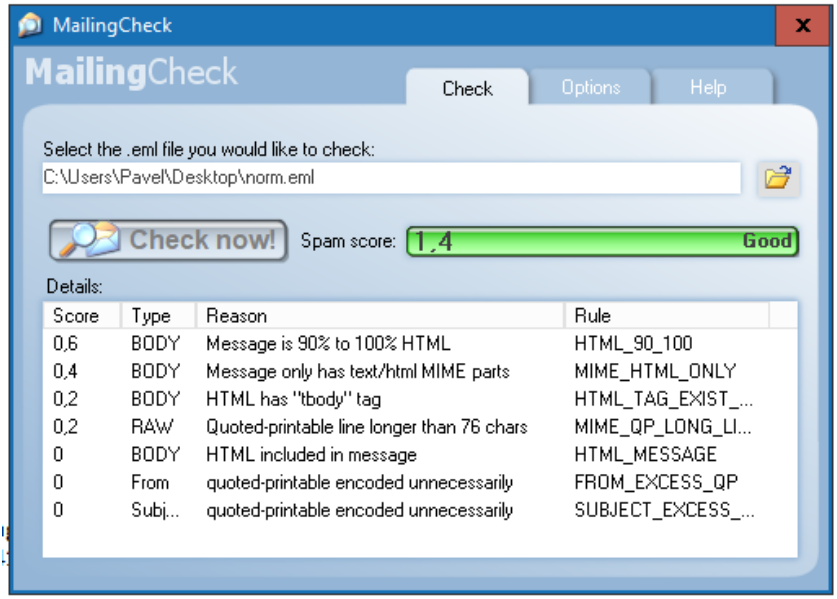

Рис. 2.19. Моделювання величини КСС при аналізі безпечного email-листа

Експертний аналіз листа дозволив ідентифікувати *8* спам-ознак, що характерно для середнього значення параметра КСС. Ознаки пов'язані з кольором html-розмітки, що співпав з фоном, помилками кодування символів, великою кількістю вставлених зображень і html-розмітки, помилками html-розмітки тощо. Отримане значення при цьому становило *3,3* спам ознак (рис. 2.20).

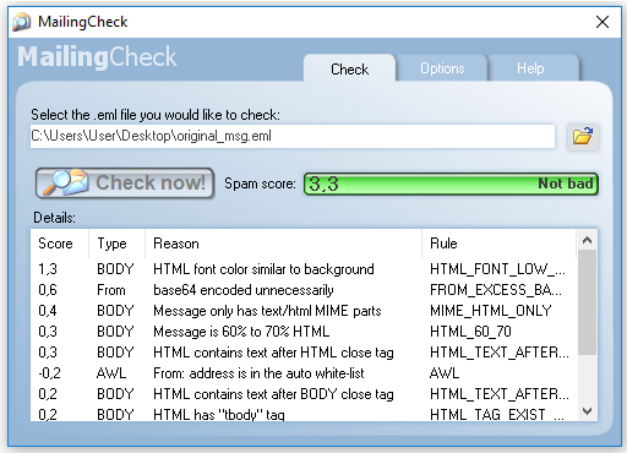

Рис. 2.20. Моделювання середньої величини КСС

Значення max_{KCC}, отримане в процесі з використанням утиліти Mailing Check дорівнює *5,7* (рис. 2.21). На основі цього визначені наступні інтервали, що найбільш коректно описують даний параметр – *[0;2], [3;4], [5;6].*

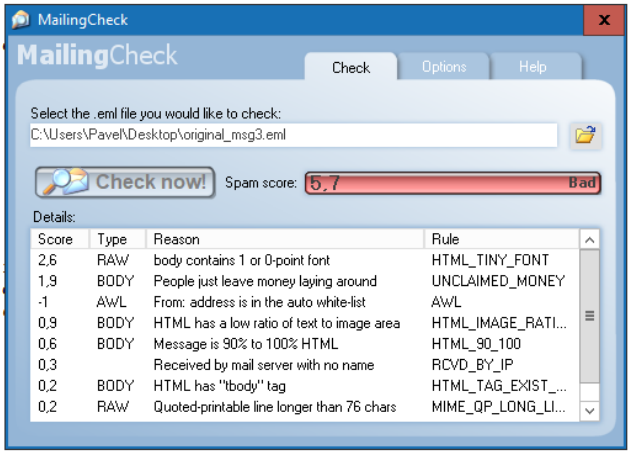

Рис. 2.21. Моделювання максимальної величини КСС за допомогою утиліти Mailing Check

Логічно припустити, що для усіх параметрів значення в діапазоні від середнього до максимального може бути свідченням реалізації email-спуфінг атаки. Відповідно до результатів моделювання, мінімальні та максимальні граничні значення, що з великою впевненістю щодо суджень експерта можуть бути сигналом фальсифікації email-листа наступні: КСБ – $[25;32];$ КСТ – $[9;12];$ КСС – $[5;6].$

З урахуванням зазначеного, розробимо метод формування еталонного підсередовища (МФЕПЕА) [21], що дозволить формалізувати процес отримання еталонів параметрів для заданих лінгвістичних змінних певного середовища оточення при вирішенні задач щодо виявлення email-спуфінг-атак на інформаційні системи.

Опишемо МФЕПЕА [21, 22], який базується на МФЕС (див. п. 2.2 та [7, 8, 10, 11]).

Для цього, сформуємо підмножину ІД лінгвістичних оцінок або експертних суджень при $n=1$ для кібератаки з ІД $CA_1 = CA_{ESP} = ESP$ (див. п. 2.1) $(m_1=3,\ r_1=4,\ r_2=r_3=3)$ відповідно до етапу 1 виразу (2.30) (див. п. 2.2)

$$\begin{gathered}\{\bigcup_{\mathbf{i=1}}^{\mathbf{1}}\mathbf{LE_1}\}=\{\bigcup_{\mathbf{i=1}}^{\mathbf{1}}\{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}}\mathbf{LE_{ij}}\}\}=\{\bigcup_{i=1}^{1}\{\bigcup_{j=1}^{m_i}\{\bigcup_{k=1}^{r_j}LE_{ijk}\}\}\}= \\ \{\{LE_{ESPKCБ1},\ LE_{ESPKCБ2},\ LE_{ESPKCБ3},\ LE_{ESPKCБ4}\}, \\ \{LE_{ESPKCT1},\ LE_{ESPKCT2},\ LE_{ESPKCT3}\}, \\ \{LE_{ESPKCC1},\ LE_{ESPKCC2},\ LE_{ESPKCC3}\}\}= \\ \{\{"М",\ "С",\ "Б",\ "ОБ"\}, \\ \{\{"Н",\ "С",\ "В"\}, \\ \{"Н",\ "С",\ "В"\}\},\end{gathered} \tag{2.55}$$

де:

- $LE_{ESPKCБ1}="М",$
- $LE_{ESPKCБ2}="С",$
- $LE_{ESPKCБ3}="Б",$
- $LE_{ESPKCБ4}="ОБ",$

- $LE_{ESPKCT1} = "H"$,
- $LE_{ESPKCT2} = "C"$,
- $LE_{ESPKCT3} = "B"$

та

- $LE_{ESPKCC1} = "H"$,
- $LE_{ESPKCC2} = "C"$,
- $LE_{ESPKCC3} = "B"$

відповідно є ІД таких лінгвістичних оцінок експерта, що відображають стан параметрів $P_{ESPKCБ} = KCБ$, $P_{ESPKCT} = KCT$ та $P_{ESPKCC} = KCC$ в *3*-вимірному параметричному підсередовищі ($\mathbf{P_i} = \mathbf{P_{ESP}}$) (див. п. 2.1).

Далі, відповідно етапу 2 (див. п. 2.2 та [7]), необхідно сформувати базову матрицю частот. Для цього побудуємо підмножину ІД інтервалів $\mathbf{N_{ij}}$ $(j = \overline{1,m_i})$ (див. (2.35)), що характеризують кібератаку з ІД $CA_1 = CA_{ESP} = ESP$, на області визначення яких експерт виконує лінгвістичне оцінювання відносно значень параметрів $P_{ESPKCБ}$, P_{ESPKCT} та P_{ESPKCC} (див. п. 2.1).

При $n = 1,\ m_1 = 3,\ r_1 = 4,\ r_2 = r_3 = 3$ отримаємо

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{1}} \mathbf{N_i}\} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{1}} \{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}} \mathbf{N_{ij}}\}\} =$$

$$\{\bigcup_{i=1}^{1} \{\bigcup_{j=1}^{m_i} \{\bigcup_{k=1}^{k_j} N_{ijk}\}\}\} = \tag{2.56}$$

$$\{N_{ESPKCБ1},\ N_{ESPKCБ2},\ N_{ESPKCБ3},\ N_{ESPKCБ4}\},$$
$$\{N_{ESPKCT1},\ N_{ESPKCT2},\ N_{ESPKCT3}\},$$
$$\{N_{ESPKCC1},\ N_{ESPKCC2},\ N_{ESPKCC3}\}\}.$$

Враховуючи елементи підмножин LE_{ij} та NE_{ij} на основі узагальнювальної таблиці (див. табл. 2.1 в п. 2.2) побудуємо поточні таблиці оцінок (див. табл. 2.7-2.9) за елементами підмножин,

$LE_{ESPKCБk}$ $(r_1 = 4,\ k = \overline{1,4})$ та $N_{ESPKCБk}$, тобто

- $N_{ESPKCБ1} = [N^{min}_{ESPKCБ1}; N^{max}_{ESPKCБ1}] \Leftrightarrow [0;8]$,
- $N_{ESPKCБ2} = [N^{min}_{ESPKCБ2}; N^{max}_{ESPKCБ2}] \Leftrightarrow [9;16]$,
- $N_{ESPKCБ3} = [N^{min}_{ESPKCБ3}; N^{max}_{ESPKCБ3}] \Leftrightarrow [17;24]$,
- $N_{ESPKCБ4} = [N^{min}_{ESPKCБ4}; N^{max}_{ESPKCБ4}] \Leftrightarrow [25;32]$

та

$LE_{ESPKCTk}$ $(r_2 = 3,\ k = \overline{1,3})$ та $N_{ESPKCTk}$, тобто

- $N_{ESPKCT1} = [N^{min}_{ESPKCT1}; N^{max}_{ESPKCT1}] \Leftrightarrow [0;4]$,
- $N_{ESPKCT2} = [N^{min}_{ESPKCT2}; N^{max}_{ESPKCT2}] \Leftrightarrow [5;8]$,
- $N_{ESPKCT3} = [N^{min}_{ESPKCT3}; N^{max}_{ESPKCT3}] \Leftrightarrow [9;12]$,

а також

$LE_{ESPKCCk}$ $(r_2 = 3,\ k = \overline{1,3})$ та $N_{ESPKCCk}$, тобто

- $N_{ESPKCC1} = [N^{min}_{ESPKCC1}; N^{max}_{ESPKCC1}] \Leftrightarrow [0;2]$,
- $N_{ESPKCC2} = [N^{min}_{ESPKCC2}; N^{max}_{ESPKCC2}] \Leftrightarrow [3;4]$,
- $N_{ESPKCC3} = [N^{min}_{ESPKCC3}; N^{max}_{ESPKCC3}] \Leftrightarrow [5;6]$.

Поточна таблиця оцінок за $\mathbf{LE_{ESPKCБ}}$ Таблиця 2.7

$\mathbf{LE_{ESPKCБ}}$	$\mathbf{N_{ESPKCБ}}$			
	$N_{ESPKCБ1}$	$N_{ESPKCБ2}$	$N_{ESPKCБ3}$	$N_{ESPKCБ4}$
“М”	2	1	0	0
“С”	1	4	2	0
“Б”	0	1	4	2
“ОБ”	0	0	1	6

Поточна таблиця оцінок за $\mathbf{LE_{ESPKCT}}$ Таблиця 2.8

$\mathbf{LE_{ESPKCT}}$	$\mathbf{N_{ESPKCT}}$		
	$N_{ESPKCT1}$	$N_{ESPKCT2}$	$N_{ESPKCT3}$
“Н”	3	1	0
“С”	1	2	1
“В”	0	1	2

Поточна таблиця оцінок за $\mathbf{LE}_{\mathbf{ESPKCC}}$ Таблиця 2.9

$\mathbf{LE}_{\mathbf{ESPKCC}}$	$\mathbf{N}_{\mathbf{ESPKCC}}$		
	$N_{ESPKCC1}$	$N_{ESPKCC2}$	$N_{ESPKCC3}$
"H"	2	1	0
"C"	1	4	3
"B"	0	3	5

Далі, з урахуванням даних таблиць 2.1-2.3 та (2.36) сформуємо матриці частот при $n=1,\ m_1=\overline{1,3},\ s,q=\overline{1,r_1}$ (тобто $s,q=\overline{1,4}$), а також $s,q=\overline{1,r_2},\ s,q=\overline{1,r_3}$ (тобто $s,q=\overline{1,3}$);

$$F_{11}=F_{ESPKCB}=\left\|f_{11sq}\right\|=\begin{Vmatrix} f_{1111} & f_{1112} & f_{1113} & f_{1114} \\ f_{1121} & f_{1122} & f_{1123} & f_{1124} \\ f_{1131} & f_{1132} & f_{1133} & f_{1134} \\ f_{1141} & f_{1142} & f_{1143} & f_{1144} \end{Vmatrix}=\begin{Vmatrix} 2 & 1 & 0 & 0 \\ 1 & 4 & 2 & 0 \\ 0 & 1 & 4 & 2 \\ 0 & 0 & 1 & 6 \end{Vmatrix},$$

$$F_{12}=F_{ESPKCT}=\left\|f_{12sq}\right\|=\begin{Vmatrix} f_{1211} & f_{1212} & f_{1213} \\ f_{1221} & f_{1222} & f_{1223} \\ f_{1231} & f_{1232} & f_{1233} \end{Vmatrix}=\begin{Vmatrix} 3 & 1 & 0 \\ 1 & 2 & 1 \\ 0 & 1 & 2 \end{Vmatrix}$$ та

$$F_{13}=F_{ESPKCC}=\left\|f_{13sq}\right\|=\begin{Vmatrix} f_{1311} & f_{1312} & f_{1313} \\ f_{1321} & f_{1322} & f_{1323} \\ f_{1331} & f_{1332} & f_{1333} \end{Vmatrix}=\begin{Vmatrix} 2 & 1 & 0 \\ 1 & 4 & 3 \\ 0 & 3 & 5 \end{Vmatrix}.$$

Далі, для формування похідної матриці частот при $n=1,\ m_1=3$ побудуємо за відповідними стовпчиками матриць F_{ESPKCB}, F_{ESPKCT} та F_{ESPKCC} з урахуванням етапу 3 виразу (2.38) вектори сум:

$$VS_{ESPKCB}=\left\|vs_{ESPKCBq}\right\|=$$

$$\left\|vs_{ESPKCB1},vs_{ESPKCB2},vs_{ESPKCB3},vs_{ESPKCB4}\right\|=$$

$$\left\| \bigcup_{q=1}^{4} \sum_{s=1}^{4} f_{ESPKCБsq} \right\| = \|3,6,7,8\|,$$

$$(q = \overline{1,4}),$$

$$VS_{ESPKCT} = \left\| vs_{ESPKCTq} \right\| = \left\| vs_{ESPKCT1}, vs_{ESPKCT2}, vs_{ESPKCT3} \right\| =$$

$$\left\| \bigcup_{q=1}^{3} \sum_{s=1}^{3} f_{ESPKCTsq} \right\| = \|4,4,3\|,$$

$$(q = \overline{1,3}) \text{ та}$$

$$VS_{ESPKCC} = \left\| vs_{ESPKCCq} \right\| = \left\| vs_{ESPKCC1}, vs_{ESPKCC2}, vs_{ESPKCC3} \right\| =$$

$$\left\| \bigcup_{q=1}^{3} \sum_{s=1}^{3} f_{ESPKCCsq} \right\| = \|3,8,8\|,$$

$$(q = \overline{1,3}).$$

Далі, з урахуванням (2.39) з $VS_{ESPKCБ}$, VS_{ESPKCT}, VS_{ESPKCC} визначимо максимальний елемент

$$vsm_{ESPKCБ} = \bigvee_{q=1}^{4} vs_{ESPKCБq} =$$

$$vs_{ESPKCБ1} \vee vs_{ESPKCБ2} \vee vs_{ESPKCБ3} \vee vs_{SPFKCБ4} = 3 \vee 6 \vee 7 \vee 8 =$$

$$vsm_{SPFKCБ} = 8,$$

$$vsm_{ESPKCT} = \bigvee_{q=1}^{3} vs_{ESPKCTq} =$$

$$vs_{ESPKCT1} \vee vs_{ESPKCT2} \vee vs_{ESPKCT3} = 4 \vee 4 \vee 3 =$$

$$vsm_{ESPKCT} = 4 \text{ та}$$

$$vsm_{ESPKCC} = \bigvee_{q=1}^{3} vs_{ESPKCCq} =$$

$$vs_{ESPKCC1} \vee vs_{ESPKCC2} \vee vs_{ESPKCC3} = 3 \vee 8 \vee 8 =$$

$$vsm_{ESPKCC} = 8,$$

а відповідно до (2.40) отримаємо похідну матрицю частот

$$F'_{ESPKCБ} = (vsm_{ESPKCБ} / vsm_{ESPKCБq})F_{ESPKCБ} = \left\| \begin{matrix} 5,3 & 1,3 & 0 & 0 \\ 2,7 & 5,3 & 2,3 & 0 \\ 0 & 1,3 & 4,6 & 2 \\ 0 & 0 & 1,1 & 6 \end{matrix} \right\|,$$

$$F'_{ESPKCT} = (vsm_{ESPKCT} / vsm_{ESPKCTq})F_{ESPKCT} = \left\| \begin{matrix} 3 & 1 & 0 \\ 1 & 2 & 1,3 \\ 0 & 1 & 2,7 \end{matrix} \right\| \text{ та}$$

$$F'_{ESPKCC} = (vsm_{ESPKCC} / vsm_{ESPKCCq})F_{ESPKCC} = \left\| \begin{matrix} 5,3 & 1 & 0 \\ 2,7 & 4 & 3 \\ 0 & 3 & 5 \end{matrix} \right\|,$$

Далі, відповідно до (2.45) сформуємо підмножину нечітких термів $\mathbf{T_{ESPKCБ}}$, $\mathbf{T_{ESPKCT}}$, $\mathbf{T_{ESPKCC}}$, які відображають визначені стани параметрів $P_{ESPKCБ} = KCБ$, $P_{ESPKCT} = KCT$ та $P_{ESPKCC} = KCC$ в 3-вимірному параметричному підсередовищі ($\mathbf{P_i} = \mathbf{P_{ESP}}$). При $n = 1$ (тобто для кібератак з ІД $CA_{ESP} = ESP$), $m_1 = 3$, $r_1 = 4$, $r_2 = r_3 = 3$ визначимо

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{1}} \mathbf{T_i}\} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{1}} \{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}} \mathbf{T_{ij}}\}\} = \{\bigcup_{i=1}^{1} \{\bigcup_{j=1}^{m_i} \{\bigcup_{s=1}^{r_j} \underset{\sim}{T}_{ijs}\}\}\} =$$

$$\{\{\underset{\sim}{T}_{ESPKCБ1}, \underset{\sim}{T}_{ESPKCБ2}, \underset{\sim}{T}_{ESPKCБ3}, \underset{\sim}{T}_{ESPKCБ4}\},$$

$$\{\underset{\sim}{T}_{ESPKCT1}, \underset{\sim}{T}_{ESPKCT2}, \underset{\sim}{T}_{ESPKCT3}\},$$

$$\{\underset{\sim}{T}_{ESPKCC1}, \underset{\sim}{T}_{ESPKCC2}, \underset{\sim}{T}_{ESPKCC3}\}\} =$$

$$\{\{\underset{\sim}{M}_{ESPKCБ}, \underset{\sim}{C}_{ESPKCБ}, \underset{\sim}{Б}_{ESPKCБ}, \underset{\sim}{OБ}_{ESPKCБ}\},$$

$$\{\underset{\sim}{H}_{ESPKCT}, \underset{\sim}{C}_{ESPKCT}, \underset{\sim}{B}_{ESPKCT}\},$$

$$\{\underset{\sim}{H}_{ESPKCC}, \underset{\sim}{C}_{ESPKCC}, \underset{\sim}{B}_{ESPKCC}\}\}$$

де:

- $\underset{\sim}{T}_{ESPKCБ1} = \underset{\sim}{M}_{ESPKCБ}$, $\underset{\sim}{T}_{ESPKCБ2} = \underset{\sim}{C}_{ESPKCБ}$, $\underset{\sim}{T}_{ESPKCБ3} = \underset{\sim}{Б}_{ESPKCБ}$ та $\underset{\sim}{T}_{ESPKCБ4} = \underset{\sim}{ОБ}_{ESPKCБ}$ відповідно є НЧ $\underset{\sim}{M}_{ESPKCБ}$, $\underset{\sim}{C}_{ESPKCБ}$, $\underset{\sim}{Б}_{ESPKCБ}$, $\underset{\sim}{ОБ}_{ESPKCБ}$, які інтерпретують висловлювання експерта, що відображаються за допомогою $LE_{ESPKCБ1} = "M"$, $LE_{ESPKCБ2} = "C"$, $LE_{ESPKCБ3} = "Б"$ та $LE_{ESPKCБ4} = "ОБ"$,
- $\underset{\sim}{T}_{ESPKCT1} = \underset{\sim}{H}_{ESPKCT}$, $\underset{\sim}{T}_{ESPKCT2} = \underset{\sim}{C}_{ESPKCT}$ і $\underset{\sim}{T}_{ESPKCT3} = \underset{\sim}{B}_{ESPKCT}$ відповідно є НЧ $\underset{\sim}{H}_{ESPKCT}$, $\underset{\sim}{C}_{ESPKCT}$ і $\underset{\sim}{B}_{ESPKCT}$, що інтерпретують висловлювання експерта, які відображаються за допомогою $LE_{ESPKCT1} = "H"$, $LE_{ESPKCT2} = "C"$ і $LE_{ESPKCT3} = "B"$,

а також

- $\underset{\sim}{T}_{ESPKCC1} = \underset{\sim}{H}_{ESPKCC}$, $\underset{\sim}{T}_{ESPKCC2} = \underset{\sim}{C}_{ESPKCC}$ та $\underset{\sim}{T}_{ESPKCC3} = \underset{\sim}{B}_{ESPKCC}$ відповідно є НЧ $\underset{\sim}{H}_{ESPKCC}$, $\underset{\sim}{C}_{ESPKCC}$ та $\underset{\sim}{B}_{ESPKCC}$, які інтерпретують висловлювання експерта, що відображаються за допомогою $LE_{ESPKCC1} = "H"$, $LE_{ESPKCC2} = "C"$ та $LE_{ESPKCC3} = "B"$.

На основі (2.46) за відповідними рядками $F'_{ESPKCБ}$, F'_{ESPKCT}, F'_{ESPKCC} побудуємо вектори максимумів, тобто

$$FM_{ESPKCБ} = \| fm_{ESPKCБs} \| =$$
$$\| fm_{ESPKCБ1},\ fm_{ESPKCБ2},\ fm_{ESPKCБ3},\ fm_{ESPKCБ4} \| =$$
$$\|5{,}3;\ 5{,}3;\ 4{,}6;\ 6\|,$$
$$FM_{ESPKCT} = \| fm_{ESPKCTs} \| =$$
$$\| fm_{ESPKCT1},\ fm_{ESPKCT2},\ fm_{ESPKCT3} \| =$$
$$\|3;\ 2;\ 2{,}7\|,$$
$$FM_{ESPKCC} = \| fm_{ESPKCCs} \| =$$
$$\| fm_{ESPKCC1},\ fm_{ESPKCC2},\ fm_{ESPKCC3} \| =$$
$$\|5{,}3;\ 4;\ 5\|.$$

На основі $FM_{ESPKCБ}$, FM_{ESPKCT} та FM_{ESPKCC} за виразом (2.47) сформуємо матриці функцій належності:

$$M_{ESPKCБ} = \left\| \mu_{ESPKCБsq} \right\| = \begin{Vmatrix} 1 & 0,25 & 0 & 0 \\ 0,5 & 1 & 0,5 & 0 \\ 0 & 0,25 & 1 & 0,3 \\ 0 & 0 & 0,24 & 1 \end{Vmatrix},$$

$$M_{ESPKCT} = \left\| \mu_{ESPKCTsq} \right\| = \begin{Vmatrix} 1 & 0,5 & 0 \\ 0,3 & 1 & 0,5 \\ 0 & 0,5 & 1 \end{Vmatrix} \text{ та}$$

$$M_{ESPKCC} = \left\| \mu_{ESPKCCsq} \right\| = \begin{Vmatrix} 1 & 0,3 & 0 \\ 0,5 & 1 & 0,6 \\ 0 & 0,8 & 1 \end{Vmatrix},$$

де

- $\mu_{ESPKCБsq} = f'_{ESPKCБsq} / fm_{ESPKCБs}$, $(s,q = \overline{1,4})$,
- $\mu_{ESPKCTsq} = f'_{ESPKCTsq} / fm_{ESPKCTs}$, $(s,q = \overline{1,3})$, а також
- $\mu_{ESPKCCsq} = f'_{ESPKCCsq} / fm_{ESPKCCs}$, $(s,q = \overline{1,3})$.

На основі отриманих даних $\mu_{ESPKCБsq}$, $\mu_{ESPKCTsq}$, $\mu_{ESPKCCsq}$ і обчислених за виразом (2.49) в $x_{ESPKCБsq}$, $x_{ESPKCTsq}$, $x_{ESPKCCsq}$ визначимо набори нечітких термів відповідно до (2.48)

$$\underset{\sim}{T}_{ESPKCБs} = \{ \mu_{ESPKCБs1} / x_{ESPKCБs1}, \ \mu_{ESPKCБs2} / x_{ESPKCБs2}, \ \mu_{ESPKCБs3} / x_{ESPKCБs3}, \ \mu_{ESPKCБs4} / x_{ESPKCБs4} \}, \quad (s,q = \overline{1,4}),$$

де відповідно до (2.49)

$$X_{ESPKCБsq} = N^{max}_{ESPKCБq} / N^{max}_{ESPKCБr}, \ (q = \overline{1,4}) \text{ або}$$

$$\{ \bigcup_{q=1}^{4} X_{ESPKCБsq} \} = \{0,25;0,5;0,75;1\}.$$

Аналогічним чином визначимо

$$\underset{\sim}{T}_{ESPKCTs} = \{ \mu_{ESPKCTs1} / x_{ESPKCTs1}, \ \mu_{ESPKCTs2} / x_{ESPKCTs2},$$

$$\mu_{ESPKCTs3} / x_{ESPKCTs3} \}, \ (s,q = \overline{1,3}),$$

де

$$X_{ESPKCTsq} = N^{max}_{ESPKCTq} / N^{max}_{ESPKCTr}, \ (q = \overline{1,3}) \text{ або}$$

$$\{\bigcup_{q=1}^{3} X_{ESPKCTsq} \} = \{0,33;0,67;1\},$$

а також

$$\underset{\sim}{T}_{ESPKCCs} = \{ \mu_{ESPKCCs1} / x_{ESPKCCs1}, \ \mu_{ESPKCCs2} / x_{ESPKCCs2},$$

$$\mu_{ESPKCCs3} / \ x_{ESPKCCs3}, \ (s,q = \overline{1,3}),$$

де

$$X_{ESPKCCsq} = N^{max}_{ESPKCCq} / N^{max}_{ESPKCCr}, \ (q = \overline{1,3}) \text{ або}$$

$$\{\bigcup_{q=1}^{3} X_{ESPKCCsq} \} = \{0,33;0,67;1\}.$$

Таким чином, отримані члени підмножини $\mathbf{T_{ESPKCБ}}$, $\mathbf{T_{ESPKCT}}$ і $\mathbf{T_{ESPKCC}}$ (числова форма), відповідно є відображенням членів підмножини $\mathbf{LE_{ESPKCБ}}$, $\mathbf{LE_{ESPKCT}}$ і $\mathbf{LE_{ESPKCC}}$ (лінгвістична форма) та подані у наступному вигляді:

$$\underset{\sim}{T}_{ESPKCБ1} = \underset{\sim}{M}_{ESPKCБ} = \{1 / 0,25; 0,25 / 0,5; 0 / 0,75; 0 / 1\};$$

$$\underset{\sim}{T}_{ESPKCБ2} = \underset{\sim}{C}_{ESPKCБ} = \{0,5 / 0,25; \ 1 / 0,5; 0,5 / 0,75; 0 / 1\};$$

$$\underset{\sim}{T}_{ESPKCБ3} = \underset{\sim}{Б}_{ESPKCБ} = \{0 / 0,25; 0,25 / 0,5; \ 1 / 0,75; 0,3 / 1\};$$

$$\underset{\sim}{T}_{ESPKCБ4} = \underset{\sim}{ОБ}_{ESPKCБ} = \{0 / 0,25; 0 / 0,5; 0,24 / 0,75; 1 / 1\} \text{ та}$$

$$\underset{\sim}{T}_{ESPKCT1} = \underset{\sim}{H}_{ESPKCT} = \{1 / 0,33; 0,5 / 0,67; 1 / 1\};$$

$$\underset{\sim}{T}_{ESPKCT2} = \underset{\sim}{C}_{ESPKCT} = \{0,3 / 0,33; 1 / 0,67; 0,5 / 1\};$$

$$\underset{\sim}{T}_{ESPKCT3} = \underset{\sim}{B}_{ESPKCT} = \{0 / 0,33; 0,5 / 0,67; 1 / 1\},$$

а також

$$\underset{\sim}{T}_{ESPKCC1} = \underset{\sim}{H}_{ESPKCC} = \{1 / 0,33; 0,3 / 0,67; 0 / 1\};$$

$$\underset{\sim}{T}_{ESPKCC2} = \underset{\sim}{C}_{ESPKCC} = \{0,5 / 0,33; 1 / 0,67; 0,6 / 1\};$$

$$\underset{\sim}{T}_{ESPKCC3} = \underset{\sim}{B}_{ESPKCC} = \{0 / 0{,}33;\ 0{,}8 / 0{,}67;\ 1 / 1\}.$$

Далі, відповідно до етапу 5 виразу (2.52), сформуємо еталонні НЧ $\mathbf{T}^{e}_{\mathbf{ESPKCБ}} \subseteq \mathbf{T}^{e}$, $\mathbf{T}^{e}_{\mathbf{ESPKCT}} \subseteq \mathbf{T}^{e}$, $\mathbf{T}^{e}_{\mathbf{ESPKCC}} \subseteq \mathbf{T}^{e}$:

$$\mathbf{T}^{e}_{\mathbf{ESPKCБ}} = \{\bigcup_{s=1}^{4} \underset{\sim}{T}^{e}_{ESPKCБs}\} =$$

$$\{\underset{\sim}{T}^{e}_{ESPKCБ1}, \underset{\sim}{T}^{e}_{ESPKCБ2}, \underset{\sim}{T}^{e}_{ESPKCБ3}, \underset{\sim}{T}^{e}_{ESPKCБ4}\} =$$

$$\{\underset{\sim}{M}^{e}_{ESPKCБ}, \underset{\sim}{C}^{e}_{ESPKCБ}, \underset{\sim}{Б}^{e}_{ESPKCБ}, \underset{\sim}{ОБ}^{e}_{ESPKCБ}\},$$

$$(s = \overline{1,4}),$$

$$\mathbf{T}^{e}_{\mathbf{ESPKCT}} = \{\bigcup_{s=1}^{3} \underset{\sim}{T}^{e}_{ESPKCTs}\} =$$

$$\{\underset{\sim}{T}^{e}_{ESPKCT1}, \underset{\sim}{T}^{e}_{ESPKCT2}, \underset{\sim}{T}^{e}_{ESPKCT3}\} =$$

$$\{\underset{\sim}{H}^{e}_{ESPKCT}, \underset{\sim}{C}^{e}_{ESPKCT}, \underset{\sim}{B}^{e}_{ESPKCT}\},$$

$$(s = \overline{1,3}) \text{ та}$$

$$\mathbf{T}^{e}_{\mathbf{ESPKCC}} = \{\bigcup_{s=1}^{3} \underset{\sim}{T}^{e}_{ESPKCCs}\} =$$

$$\{\underset{\sim}{T}^{e}_{ESPKCC1}, \underset{\sim}{T}^{e}_{ESPKCC2}, \underset{\sim}{T}^{e}_{ESPKCC3}\} =$$

$$\{\underset{\sim}{H}^{e}_{ESPKCC}, \underset{\sim}{C}^{e}_{ESPKCC}, \underset{\sim}{B}^{e}_{ESPKCC}\},$$

$$(s = \overline{1,3}),$$

де члени підмножини:

- $\mathbf{T}^{e}_{\mathbf{ESPKCБ}}$ – $\underset{\sim}{M}^{e}_{ESPKCБ}$, $\underset{\sim}{C}^{e}_{ESPKCБ}$, $\underset{\sim}{Б}^{e}_{ESPKCБ}$, $\underset{\sim}{ОБ}^{e}_{ESPKCБ}$,
- $\mathbf{T}^{e}_{\mathbf{ESPKCT}}$ – $\underset{\sim}{H}^{e}_{ESPKCT}$, $\underset{\sim}{C}^{e}_{ESPKCT}$, $\underset{\sim}{B}^{e}_{ESPKCT}$,
- $\mathbf{T}^{e}_{\mathbf{ESPKCC}}$ – $\underset{\sim}{H}^{e}_{ESPKCC}$, $\underset{\sim}{C}^{e}_{ESPKCC}$, $\underset{\sim}{B}^{e}_{ESPKCC}$ є НЧ еталонного підсередовища ($\mathbf{T}^{e}_{i} = \mathbf{T}^{e}_{ESP}$).

Далі, відповідно кроку 1 етапу 5 (див. п. 2.2), перетворимо нечіткі терми

$$\underset{\sim}{M}_{ESPKCБ},\ \underset{\sim}{C}_{ESPKCБ},\ \underset{\sim}{Б}_{ESPKCБ},\ \underset{\sim}{ОБ}_{ESPKCБ},$$
$$\underset{\sim}{H}_{ESPKCT},\ \underset{\sim}{C}_{ESPKCT},\ \underset{\sim}{B}_{ESPKCT}\ \text{та}$$
$$\underset{\sim}{H}_{ESPKCC},\ \underset{\sim}{C}_{ESPKCC},\ \underset{\sim}{B}_{ESPKCC}$$

таким чином, щоб для всіх $\underset{\sim}{T}_{ESPKCБs}$, $\underset{\sim}{T}_{ESPKCTs}$ і $\underset{\sim}{T}_{ESPKCCs}$, було справедливим відношення порядку, тобто

$$\forall x_{ESPKCБsq} : x_{ESPKCБsq} < x_{ESPKCБsq+1},\ (q = \overline{1,4}),$$
$$\forall x_{ESPKCTsq} : x_{ESPKCTsq} < x_{ESPKCTsq+1},\ (q = \overline{1,3})\ \text{та}$$
$$\forall x_{ESPKCCsq} : x_{ESPKCCsq} < x_{ESPKCCsq+1},\ (q = \overline{1,3}).$$

Якщо за компоненти таких термів використовувати конкретні значення, отримані в прикладі вище, то для них таке відношення буде істинним.

Так, наприклад, для $\underset{\sim}{M}_{ESPKCБ}$ це

$$x_{ESPKCБ11} < x_{ESPKCБ12} < x_{ESPKCБ13} < x_{ESPKCБ14} =$$
$$0{,}25 < 0{,}5 < 0{,}75 < 1.$$

Також, аналогічно, буде істинним відношення для $\underset{\sim}{H}_{ESPKCT}$ –

$$x_{ESPKCT11} < x_{ESPKCT12} < x_{ESPKCT13} =$$
$$0{,}33 < 0{,}67 < 1,$$

та для $\underset{\sim}{H}_{ESPKCП}$ –

$$x_{ESPKCП11} < x_{ESPKCП12} < x_{ESPKCП13} =$$
$$0{,}33 < 0{,}67 < 1.$$

Далі, відповідно кроку 2 етапу 5 (див. п. 2.2) для $\underset{\sim}{T}_{ESPKCБs}$ виконаємо процедуру поглинання.

Для $\underset{\sim}{M}_{ESPKCБ}$ (де мода $x_{ESPKCБ1M} = x_{ESPKCБ11} = 0{,}25$, а її порядковий номер $M = 1$) при умові U_2 (тобто $\mu_{ESPKCБ13} = \mu_{ESPKCБ14} = 0$) виконується поглинання одним компонентом $0 / x^{max}_{ESPKCБ1}$ ряду інших відповідно до виразу

$$x^{max}_{ESPKCБ1} = x_{ESPKCБ13} \wedge x_{ESPKCБ14} =$$

$$0{,}75 \wedge 1 = 0{,}75,$$
$$(q = \overline{1{,}4}).$$

Таким чином,

$$\mu_{ESPKCБ13} / x_{ESPKCБ13} = 0 / 0{,}75,$$
$$\mu_{ESPKCБ14} / x_{ESPKCБ14} = 0 / 1$$

поглинаються компонентом

$$\mu_{ESPKCБ13} / x_{ESPKCБ13} = 0 / 0{,}75.$$

Далі, для $\underset{\sim}{ОБ}_{ESPKCБ}$ (де мода $x_{ESPKCБ4M} = x_{ESPKCБ44} = 1$, а її порядковий номер $M = 4$) при умові U_1 ($\mu_{ESPKCБ41} = \mu_{ESPKCБ42} = 0$) відбувається поглинання одним компонентом, $0 / x^{min}_{ESPKCБ4}$ іншого відповідно до виразу

$$x^{min}_{ESPKCБ4} = x_{ESPKCБ41} \vee x_{ESPKCБ42} =$$
$$0{,}25 \vee 0{,}5 = 0{,}5.$$

Таким чином,

$$\mu_{ESPKCБ41} / x_{ESPKBCБ41} = 0 / 0{,}25,$$
$$\mu_{ESPKCБ42} / x_{ESPKCБ42} = 0 / 0{,}5$$

поглинається компонентом

$$\mu_{ESPKCБ42} / x_{ESPKCБ42} = 0 / 0{,}5.$$

Далі, для кожного $\underset{\sim}{Н}_{ESPKCT}$, $\underset{\sim}{С}_{ESPKCT}$, $\underset{\sim}{В}_{ESPKCT}$ і $\underset{\sim}{Н}_{ESPKCC}$, $\underset{\sim}{С}_{ESPKCC}$, $\underset{\sim}{В}_{ESPKCC}$ умови U_1 та U_2 не виконуються і тому операція поглинання не відбувається.

Враховуючи описані перетворення, а також (2.51) визначимо проміжні терми у вигляді:

$$\underset{\sim}{Т}'_{ESPKCБ1} = \underset{\sim}{М}'_{ESPKCБ} = \{1 / 0{,}25; 0{,}25 / 0{,}5; 0 / 0{,}75\};$$

$$\underset{\sim}{Т}'_{ESPKCБ2} = \underset{\sim}{С}'_{ESPKCБ} = \{0{,}5 / 0{,}25;\ 1 / 0{,}5; 0{,}5 / 0{,}75; 0 / 1\};$$

$$\underset{\sim}{Т}'_{ESPKCБ3} = \underset{\sim}{Б}'_{ESPKCБ} = \{0 / 0{,}25; 0{,}25 / 0{,}5;\ 1 / 0{,}75; 0{,}3 / 1\};$$

$$\underset{\sim}{Т}'_{ESPKCБ4} = \underset{\sim}{ОБ}'_{ESPKCБ} = \{0 / 0{,}5; 0{,}24 / 0{,}75; 1 / 1\}$$ та

$$\underset{\sim}{Т}'_{ESPKCT1} = \underset{\sim}{Н}'_{ESPKCT} = \{1 / 0{,}2; 0{,}5 / 0{,}5; 1 / 1\};$$

$$\underset{\sim}{T}'_{ESPKCT2} = \underset{\sim}{C}'_{ESPKCT} = \{0,3 / 0,2; 1 / 0,5; 0,5 / 1\};$$

$$\underset{\sim}{T}'_{ESPKCT3} = \underset{\sim}{B}'_{ESPKCT} = \{0 / 0,2; 0,5 / 0,5; 1 / 1\},$$

а також

$$\underset{\sim}{T}'_{ESPKCC1} = \underset{\sim}{H}'_{ESPKCC} = \{1 / 0,3; 0,3 / 0,6; 0 / 1\};$$

$$\underset{\sim}{T}'_{ESPKCC2} = \underset{\sim}{C}'_{ESPKCC} = \{0,5 / 0,3; 1 / 0,6; 0,6 / 1\};$$

$$\underset{\sim}{T}'_{ESPKCC3} = \underset{\sim}{B}'_{ESPKCC} = \{0 / 0,3; 0,8 / 0,6; 1 / 1\}.$$

Відповідно до етапу 5 кроку 3 (див. п. 2.2) та (2.51) для набору проміжних термів $\underset{\sim}{M}'_{ESPKCБ}$ та $\underset{\sim}{C}'_{ESPKCБ}$

$$\exists \underset{\sim}{T}'_{ESPKCБ1} : \{0 / x^{min}_{ESPKCБ1}\} \in \varnothing \text{ і}$$

$$\exists \underset{\sim}{T}'_{ESPKCБ2} : \{0 / x^{min}_{ESPKCБ2}\} \in \varnothing$$

(тобто $\mu_{ESPKCБ11} = 1 \neq 0$ та $\mu_{ESPKCБ21} = 0,5 \neq 0$),

а для $\underset{\sim}{Б}'_{ESPKCБ}$ і $\underset{\sim}{ОБ}'_{ESPKCБ}$

$$\exists \underset{\sim}{T}'_{ESPKCБ3} : \{0 / x^{max}_{ESPKCБ3}\} \in \varnothing \text{ та}$$

$$\exists \underset{\sim}{T}'_{ESPKCБ4} : \{0 / x^{max}_{ESPKCБ4}\} \in \varnothing$$

(тобто $\mu_{ESPKCБ34} = 0,3 \neq 0$ і $\mu_{ESPKCБ44} = 1 \neq 0$),

то формування підмножин

$$\underset{\sim}{T}^{e}_{ESPKCБ1},\ \underset{\sim}{T}^{e}_{ESPKCБ2} \text{ та } \underset{\sim}{T}^{e}_{ESPKCБ3},\ \underset{\sim}{T}^{e}_{ESPKCБ4}$$

здійснимо за рахунок розширення

$$\underset{\sim}{T}'_{ESPKCБ1},\ \underset{\sim}{T}'_{ESPKCБ2} \text{ та } \underset{\sim}{T}'_{ESPKCБ3},\ \underset{\sim}{T}'_{ESPKCБ4}$$

(див. (2.51)) шляхом введення додаткових

$$\mu_{ESPKCБ1\beta\text{-}1} / x_{ESPKCБ1\beta\text{-}1} = 0 / 0,25,\ \mu_{ESPKCБ1r_j\text{-}\gamma+2} / x_{ESPKCБ1r_j\text{-}\gamma+2} = 0 / 1,$$

$$\mu_{ESPKCБ2\beta\text{-}1} / x_{ESPKCБ2\beta\text{-}1} = 0 / 0,25 \text{ та}$$

$$\mu_{ESPKCБ3r_j\text{-}\gamma+2} / x_{ESPKCБ3r_j\text{-}\gamma+2} = 0 / 1,\ \mu_{ESPKCБ4r_j\text{-}\gamma+2} / x_{ESPKCБ4r_j\text{-}\gamma+2} = 0 / 1$$

відповідно, після чого в складі НЧ відбувається (починаючи з першої) переіндексація компонент.

З урахуванням цього, набір проміжних термів для $\underset{\sim}{M}'_{ESPKCБ}$ буде мати наступний вигляд

$$\underset{\sim}{T}'_{ESPKCБ1} = \underset{\sim}{M}'_{ESPKCБ} =$$
$$\{\mu_{ESPKCБ11} / x_{ESPKCБ11},\ \mu_{ESPKCБ12} / x_{ESPKCБ12},$$
$$\mu_{ESPKCБ13} / x_{ESPKCБ13},\ \mu_{ESPKCБ14} / x_{ESPKCБ14}\} =$$
$$\{0 / 0{,}25; 1 / 0{,}25; 0{,}25 / 0{,}5; 0 / 0{,}75\},$$

де $\mu_{ESPKCБ1\beta\text{-}1} = 0$. Аналогічним способом отримуємо проміжні терми для

$$\underset{\sim}{C}'_{ESPKCБ},\ \underset{\sim}{Б}'_{ESPKCБ} \text{ та } \underset{\sim}{ОБ}'_{ESPKCБ},$$

де $\mu_{ESPKCБ2\beta\text{-}1} = \mu_{ESPKCБ3r_j\text{-}\gamma+2} = \mu_{ESPKCБ4r_j\text{-}\gamma+2} = 0.$

Таким чином, компоненти підмножини еталонів $\underset{\sim}{T}^e_{ESPKCБ1}$ відповідно до (2.52) будуть визначатись як

$$\mu^e_{ESPKCБ11} / x^e_{ESPKCБ11} = 0 / 0{,}25,\ \mu^e_{ESPKCБ12} / x^e_{ESPKCБ12} = 1 / 0{,}25,$$
$$\mu^e_{ESPKCБ13} / x^e_{ESPKCБ13} = 0{,}25 / 0{,}5,\ \mu^e_{ESPKCБ14} / x^e_{ESPKCБ14} = 0 / 0{,}75$$

та аналогічно для $\underset{\sim}{T}^e_{ESPKCБ2}$, $\underset{\sim}{T}^e_{ESPKCБ3}$, $\underset{\sim}{T}^e_{ESPKCБ4}$.

Далі, відповідно до (2.52) для $\underset{\sim}{M}'_{ESPKCБ}$, $\underset{\sim}{C}'_{ESPKCБ}$, $\underset{\sim}{Б}'_{ESPKCБ}$, $\underset{\sim}{ОБ}'_{ESPKCБ}$ сформуємо еталонні значення, тобто:

$$\underset{\sim}{T}^e_{ESPKCБ1} = \underset{\sim}{M}^e_{ESPKCБ} = \{0 / 0{,}25; 1 / 0{,}25; 0{,}25 / 0{,}5; 0 / 0{,}75; 0 / 1\};$$
$$\underset{\sim}{T}^e_{ESPKCБ2} = \underset{\sim}{C}^e_{ESPKCБ} = \{0 / 0{,}25; 0{,}5 / 0{,}25;\ 1 / 0{,}5; 0{,}5 / 0{,}75;\ 0 / 1\};$$
$$\underset{\sim}{T}^e_{ESPKCБ3} = \underset{\sim}{Б}^e_{ESPKCБ} = \{0 / 0{,}25; 0{,}25 / 0{,}5;\ 1 / 0{,}75; 0{,}3 / 1;\ 0 / 1\};$$
$$\underset{\sim}{T}^e_{ESPKCБ4} = \underset{\sim}{ОБ}^e_{ESPKCБ} = \{0 / 0{,}5; 0{,}24 / 0{,}75; 1 / 1; 0 / 1\}.$$

Також, аналогічно, формуються і наступні еталонні значення:

$$\underset{\sim}{T}^e_{ESPKCT1} = \underset{\sim}{H}^e_{ESPKCT} = \{0 / 0{,}2; 1 / 0{,}2; 0{,}5 / 0{,}5; 1 / 1; 0 / 1\};$$
$$\underset{\sim}{T}^e_{ESPKCT2} = \underset{\sim}{C}^e_{ESPKCT} = \{0 / 0{,}2; 0{,}3 / 0{,}2; 1 / 0{,}5; 0{,}5 / 1; 0 / 1\};$$
$$\underset{\sim}{T}^e_{ESPKCT3} = \underset{\sim}{B}^e_{ESPKCT} = \{0 / 0{,}2; 0{,}5 / 0{,}5; 1 / 1; 0 / 1\} \text{ та}$$

$$\underset{\sim}{T}^{e}_{ESPKCC1} = \underset{\sim}{H}^{e}_{ESPKCC} = \{0 / 0,3; 1 / 0,3; 0,3 / 0,6; 0 / 1\};$$

$$\underset{\sim}{T}^{e}_{ESPTKCC2} = \underset{\sim}{C}^{e}_{ESPKCC} = \{0 / 0,3; 0,5 / 0,3; 1 / 0,6; 0,6 / 1; 0 / 1\};$$

$$\underset{\sim}{T}^{e}_{ESPKCC3} = \underset{\sim}{B}^{e}_{ESPKCC} = \{0 / 0,3; 0,8 / 0,6; 1 / 1; 0 / 1\}.$$

На базі етапу 6 (див. п. 2.2 та [7, 10]) для підмножини еталонів $\mathbf{T}^{e}_{ESPKCБ}$, $\mathbf{T}^{e}_{ESPKCT}$ та $\mathbf{T}^{e}_{ESPKCC}$ з урахуванням отриманих конкретних значень можна реалізувати їх графічну інтерпретацію (див. рис. 2.22-2.24), скориставшись НЧ еталонного підсередовища ($\mathbf{T}^{e}_{i} = \mathbf{T}^{e}_{ESP}$) для $\underset{\sim}{M}^{e}_{ESPKCБ}$, $\underset{\sim}{C}^{e}_{ESPKCБ}$, $\underset{\sim}{Б}^{e}_{ESPKCБ}$, $\underset{\sim}{ОБ}^{e}_{ESPKCБ}$ будуються чотири ламані —●—, —■—, —○—, —□—, а також для $\underset{\sim}{H}^{e}_{ESPKCT}$, $\underset{\sim}{C}^{e}_{ESPKCT}$, $\underset{\sim}{B}^{e}_{ESPKCT}$ і $\underset{\sim}{H}^{e}_{ESPKCC}$, $\underset{\sim}{C}^{e}_{ESPKCC}$, $\underset{\sim}{B}^{e}_{ESPKCC}$ будуються по три ламані —●—, —□—, —△— відповідно.

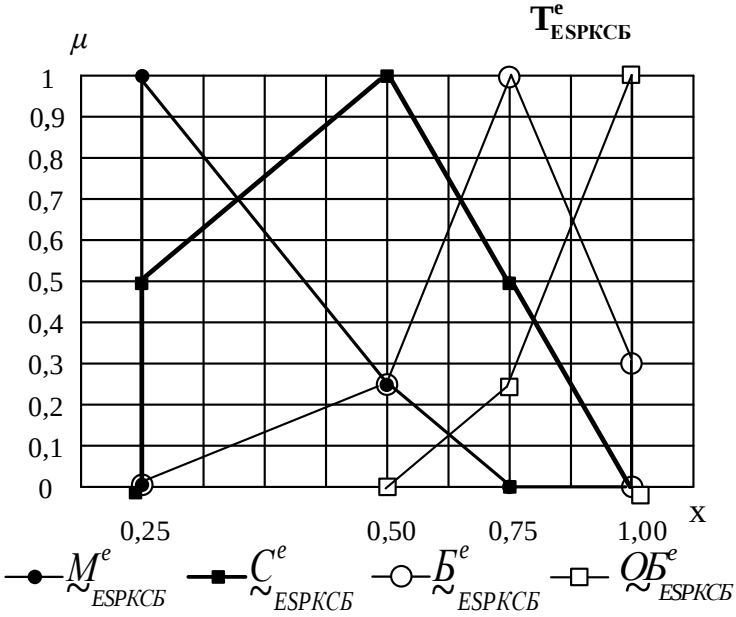

Рис. 2.22 Лінгвістичні еталони підмножини $\mathbf{T}^{e}_{ESPKCБ}$

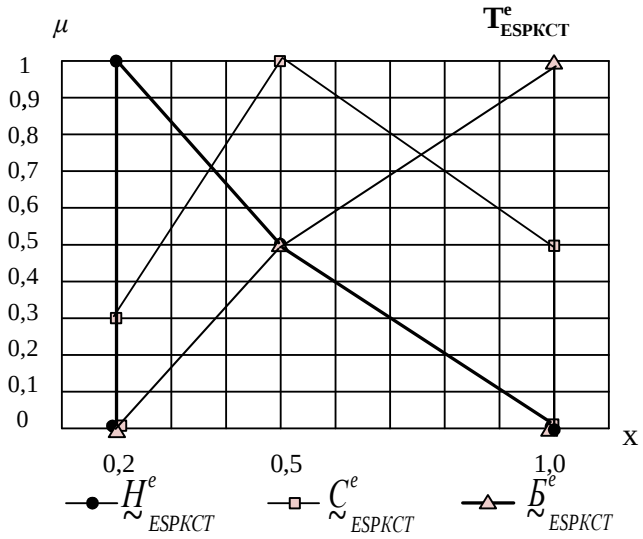

Рис. 2.23 Лінгвістичні еталони підмножини $\mathbf{T}^{\mathbf{e}}_{\mathbf{ESPKCT}}$

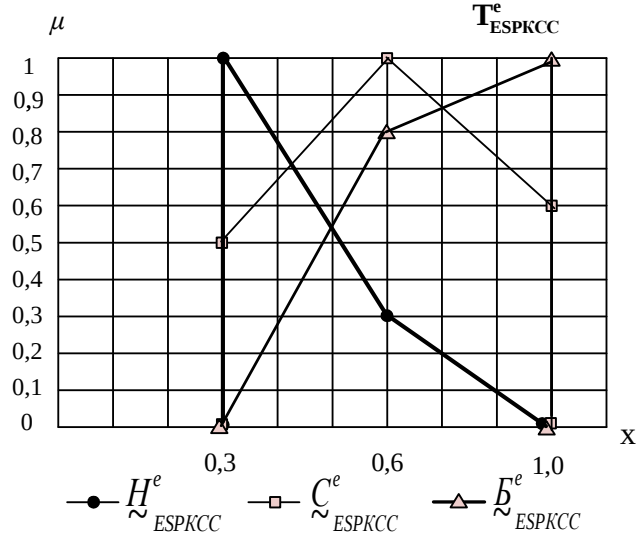

Рис. 2.24 Лінгвістичні еталони підмножини $\mathbf{T}^{\mathbf{e}}_{\mathbf{ESPKCC}}$

Запропонований в роботі МФЕПЕА [21, 22], який за рахунок сформованого набору параметрів КСБ, КСТ, КСС та експертного оцінювання стану середовища оточення інформаційної системи дозволить формалізувати процес формування параметрів еталонного середовища для вирішенні задач, щодо виявлення email-спуфінг атак на інформаційні системи. Метод може бути застосований для підвищення ефективності систем захисту інформації для протидії email-спуфінг атакам.

СПИСОК ЛІТЕРАТУРИ ДО РОЗДІЛУ 2

1. А. Корченко, «Кортежная модель формирования набора базовых компонент для выявления кибератак», *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, В.2 (28), С. 29-36, 2014.

2. A. Korchenko, K. Warwas, A. Kłos-Witkowska, «The Tupel Model of Basic Components' Set Formation for Cyberattacks», in *Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2015 IEEE 8th International Conference on*, 2015, pp. 478-483.

3. А. Корченко, «Модель базових компонент для виявлення кібератак на ресурси інформаційних систем», *Актуальні проблеми управління інформаційною безпекою держави: VI наук.-практ. конф.*, Київ, 2015, С. 274-275.

4. А. Корченко, «Узагальнена модель параметрів для синтезу систем виявлення кібератак», *Актуальні проблеми управління інформаційною безпекою держави: V наук.-практ. конф.*, НА СБ України, Київ, 2014, Ч. 2, С. 103-107.

5. Б.С. Ахметов, Р.Б. Абдрахманов, А.А. Корченко, Н.К. Жумангалиева, «Базовые модели эталонных величин для систем обнаружения вторжений», *Вестник Международного Казахско-Турецкого университета. им. А.Ясави*, №5-6 (97-98), С. 15-26, 2015.

6. Б.С. Ахметов, А.А. Корченко, Н.К. Жумангалиева, «Модель базовых величин для контроля аномальности состояния среды окружения», *Известия Национальной Академии наук Республики Казахстан. Серия физико-математическая*, №1 (305), С. 26-33, 2016.

7. А. Корченко, «Метод формирования лингвистических эталонов для систем выявления вторжений», *Захист інформації*, Т.16, №1, С. 5-12, 2014.

8. А. Корченко, «Формирование лингвистических эталонов на основе кортежной модели для систем выявления вторжений», *Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS`2015): 7-та Всеук. наук.-практ. конф.*, с. Коблево Миколаївської обл., 2015, С. 43-46.

9. А. Корченко, А. Гизун, «Моделирование эталонов параметров для систем выявления кибератак», *ABIA-2015: XII міжнар. наук.-техн. конф.*, НАУ, 2015, С. 2.27-2.29.

10. B. Akhemetov, A. Korchenko, S. Akhmetova, N. Zhumangalieva, «Improved method for the formation of linguistic standards for of intrusion detection systems», *Journal of Theoretical and Applied Information Technology*, vol. 87, no. 2, pp. 221-232, 2016.

11. Anna Korchenko, «Formation of linguistic standards for of intrusion detection systems», *Безопасность в авиации и космические технологии: VIII Всемирный конгресс «Авиация в XXI столетии»*, Киев, 2018, С. 3.2.1.-3.2.6.

12. А.Г Корченко, «Построение систем защиты информации на нечетких множествах», *Теория и практические решения,* Киев, 2006, 320 с.

13 С.Я. Гродзенский, Я.С. Гродзенский, А.Н. Чесалин, «Средства и методы управления качеством. Учебное пособие», 2018, 111 стр.

14. И. Терейковский, А. Корченко, П. Викулов, А. Шаховал, «Модели эталонов лингвистических переменных для обнаружения сниффинг-атак», *Захист інформації*, Т.19, №3, С. 228-242, 2017.

15. M. Karpinski, A. Korchenko, P. Vikulov, R. Kochan, «The Etalon Models of Linguistic Variables for Sniffing-Attack Detection», in *Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2017 IEEE 9th International Conference on*, 2017, pp. 258-264.

16. А. Корченко, Н. Жумангалиева, П. Викулов, «Построение лингвистических эталонов для выявления сниффинг атак», *Актуальні питання забезпечення кібернетичної безпеки та захист інформації: ІІІ міжнар. наук.-практ. конф.*, Київ, 2017, С. 93-97.

17 16. I. Bapiyev, B. Aitchanov, I. Tereikovskyi, L. Tereikovska, A. Korchenko, «Deep neural networks in cyber attack detection systems», *International Journal of Civil Engineering and Technology vol. 8*, 2017, pp. 1086-1092.

18. B. Aitchanov, A. Korchenko, I. Tereykovskiy, I. Bapiyev, «Perspectives for using classical neural network models and methods of counteracting attacks on network resources of information systems», *News of the National Academy of Sciences of the Republic of Kazakhstan, Series of Geology and Technical Sciences vol. 5*, 2017, pp. 202-212.

19. MXToolBox SuperTool7 Network Tools [Електронний ресурс] : [Веб-сайт]. – Режим доступу: https://mxtoolbox.com/ SuperTool.aspx (дата звернення 30.05.2018) – Назва з екрана.

20. Local News: Subject Line tool [Електронний ресурс] : [Вебсайт]. – Режим доступу: http://www.localnews.biz/subjectLine/ ValidateSubjectLine.asp (дата звернення 30.05.2018) – Назва з екрана.

21. І. Терейковський, А. Корченко, П. Вікулов, І. Ірейфідж, «Моделі еталонів лінгвістичних змінних для систем виявлення email-спуфінг-атак», *Безпека інформації*. Т.24, №2, С. 99-109, 2018.

22. A.O. Korchenko, P.O. Vikulov, «Etalons models of linguistic variables for spoofing attacks detection systems», *Безопасность в авиации и космические технологии: VIII Всемирный конгресс «Авиация в XXI столетии»*, Киев, 2018, С. 3.2.10.-3.2.12.

РОЗДІЛ 3. БАЗОВІ МЕТОДИ ФОРМУВАННЯ ПОТОЧНОГО СЕРЕДОВИЩА

3.1. Метод фазифікації параметрів на еталонних підсередовищах для систем виявлення кібератак

Пропонуються метод фазифікації параметрів на еталонних підсередовищах для систем виявлення кібератак (МФП) [1], який відповідно до КМАС (див. п. 2.1 та [2-4]) дозволяє формалізувати процес перетворення в нечітку форму значень параметрів *m*-вимірних поточних середовищ з метою їх подальшого застосування для виявлення аномального стану.

Основу запропонованого методу складають три базових етапи:

- формування частот зустрічальності параметрів;
- формування поправкових еталонів;
- формування нечітких параметрів.

Формування частот зустрічальності параметрів

Етап 1 – формування частот зустрічальності параметрів. Для реалізації цього етапу введемо множину всіх можливих сенсорів **S** та підмножини таких сенсорів $\mathbf{S_{ij}} \subseteq \mathbf{S}$:

$$\mathbf{S_{ij}} = \{\bigcup_{k=1}^{r_j} S_{ijk}(t_\eta)\} = \{S_{ij1}(t_\eta),\ S_{ij2}(t_\eta),\ ...,\ S_{ijr_j}(t_\eta)\}, \tag{3.1}$$

що використовуються для контролю поточного стану фізичних параметрів, які відображаються шляхом $\mathbf{P_i^{\tau_f}}$ в $\mathbf{CA_i^{\tau_f}}$ (див. п. 2.1 та [2]).

Тут $S_{ijk}(t_\eta)$ $(i=\overline{1,n},\ j=\overline{1,m_i},\ k=\overline{1,r_j})$, є сенсором N_{ijk}-го інтервалу (див. п. 2.2 та [5-9]), який відображає значення (на відповідному інтервалі) фізичного параметру $P_{ij}(t_\eta)$ в момент t_η, а r_j – кількість сенсорів.

Сенсор $S_{ijk}(t_\eta)$ є бінарною функцією, яка еквівалентна одиниці тільки у випадку, коли значення $P_{ij}(t_\eta)$ відносно кортежної моделі

(див. п. 2.1) в момент t_η (момент настання очікуваної події) буде знаходитись в інтервалі N_{ijk} тобто:

$$S_{ijk}(t_\eta)=\begin{cases}1, \text{ якщо } P_{ij}(t_\eta)\in N_{ijk}\\ 0, \text{ якщо } P_{ij}(t_\eta)\notin N_{ijk}\end{cases}, \quad (k=\overline{1,r_j}). \tag{3.2}$$

Далі, введемо множину всіх можливих лічильників сенсорів **CS** та підмножини таких лічильників $\mathbf{CS_{ij}} \subseteq \mathbf{CS}$, які відповідно до виразу (3.3) (на основі даних сенсорів $S_{ijk}(t_\eta)$, характеризують поточний стан *j*-х фізичних параметрів відносно *i*-ї атаки в моменти t_η) формують частоти зустрічальності значень $P_{ij}(t_\eta)$ на кожному з інтервалів N_{ijk} $(k=\overline{1,r_j})$ (див. п. 2.2) за допомогою підмножин

$$\mathbf{CS_{ij}}=\{\bigcup_{k=1}^{r_j} CS_{ijk}\}= \{\bigcup_{k=1}^{r_j}\sum_{\eta=1}^{\eta_{max}} S_{ijk}(t_\eta)\}, \tag{3.3}$$

де CS_{ijk} є лічильником сенсора $S_{ijk}(t_\eta)$, а η_{max} відповідає загальній кількості можливих t_η.

Далі, частоти зустрічальності, що відображені лічильниками CS_{ijk} $(k=\overline{1,r_j})$ представимо у вигляді таблиці (табл. 3.1), тобто кожний CS_{ijk} лічильник відповідає за контроль стану відповідного параметра на інтервалі N_{ijk} $(k=\overline{1,r_j})$.

Таблиця 3.1

Типова таблиця для $\mathbf{CS_{ij}}$

Лічильник сенсора	$\mathbf{N_{ij}}$ $(k=\overline{1,r_j})$			
	N_{ij1}	N_{ij2}	…	N_{ijr_j}
CS_{ij}	CS_{ij1}	CS_{ij2}	…	CS_{ijr_j}

Наприклад, для реалізації етапу формування частот зустрічальності параметрів, якщо $n=1$ ($i=3$, тобто для кібератаки з ІД $CA_З = CA_{SP} = SP$), $j=1$ та $r_j=5$ підмножина $\mathbf{S_{ij}=S_{31}}$ відповідно до виразу (3.1) приймає вигляд

$$\mathbf{S_{31}} = \{\bigcup_{k=1}^{5} S_{31k}(t_\eta)\} =$$

$$\{S_{311}(t_\eta),\ S_{312}(t_\eta),\ S_{313}(t_\eta),\ S_{314}(t_\eta),\ S_{315}(t_\eta)\} =$$

$$\{S_{SPKOП1}(t_\eta),\ S_{SPKOП2}(t_\eta),\ S_{SPKOП3}(t_\eta),\ S_{SPKOП4}(t_\eta),\ S_{SPKOП5}(t_\eta)\},$$

де:

- $S_{311}(t_\eta) = S_{SPKOП1}(t_\eta)$,
- $S_{312}(t_\eta) = S_{SPKOП2}(t_\eta)$,
- $S_{313}(t_\eta) = S_{SPKOП3}(t_\eta)$,
- $S_{314}(t_\eta) = S_{SPKOП4}(t_\eta)$,
- $S_{315}(t_\eta)\} = S_{SPKOП5}(t_\eta)$,

відповідно сенсори інтервалів

- $N_{ij1} = N_{311} = N_{SPKOП1}$,
- $N_{ij2} = N_{312} = N_{SPKOП2}$,
- $N_{ij3} = N_{313} = N_{SPKOП3}$,
- $N_{ij4} = N_{314} = N_{SPKOП4}$,
- $N_{ij5} = N_{315} = N_{SPKOП5}$,

що використовуються для контролю поточного стану параметра $P_{SPKOП}(t_\eta)$ в m_i-вимірному параметричному підсередовищі ($\mathbf{P_i = P_З = P_{SP}}$) в моменти t_η при $r_j = 5$.

Оскільки сенсори $S_{31k}(t_\eta)$ ($k=\overline{1,r_j}$), виходячи з виразу (3.2), визначаються як

$$S_{31k}(t_\eta) = S_{SPKOПk}(t_\eta) = \begin{cases} 1, \text{ якщо } P_{31}(t_\eta) \in N_{31k} \\ 0, \text{ якщо } P_{31}(t_\eta) \notin N_{31k} \end{cases},$$

$$(k=\overline{1,5}),$$

то частоти зустрічальності значень $P_{31}(t_\eta)$ відповідно до формули (3.3) сформуємо за допомогою наступного виразу:

$$\mathbf{CS_{31}} = \{\bigcup_{k=1}^{5} CS_{31k}\} =$$

$$\{\bigcup_{k=1}^{5}\sum_{\eta=1}^{\eta_{max}} S_{31k}(t_\eta)\} =$$

$$\{\sum_{\eta=1}^{\eta_{max}} S_{311}(t_\eta),\ \sum_{\eta=1}^{\eta_{max}} S_{312}(t_\eta),\ \sum_{\eta=1}^{\eta_{max}} S_{313}(t_\eta),$$

$$\sum_{\eta=1}^{\eta_{max}} S_{314}(t_\eta),\ \sum_{\eta=1}^{\eta_{max}} S_{315}(t_\eta)\} =$$

$$\{\sum_{\eta=1}^{\eta_{max}} S_{SPKOП1}(t_\eta),\ \sum_{\eta=1}^{\eta_{max}} S_{SPKOП2}(t_\eta),\ \sum_{\eta=1}^{\eta_{max}} S_{SPKOП3}(t_\eta),$$

$$\sum_{\eta=1}^{\eta_{max}} S_{SPKOП4}(t_\eta),\ \sum_{\eta=1}^{\eta_{max}} S_{SPKOП5}(t_\eta)\}.$$

Для ініціювання сенсорів їм необхідно отримати поточні значення $P_{DSKOП}(t_\eta),\ P_{SPKOП}(t_\eta),\ P_{DSCO3}(t_\eta),\ P_{DS3M3}(t_\eta)$ та $P_{SPKПЮA}(t_\eta)$.

Приклад формування

$$P_{DSKOП}(t_\eta) \text{ та } P_{SPKOП}(t_\eta)$$

відповідно для сенсорів

$$CS_{21} \text{ та } CS_{31}$$

може ґрунтуватися на використанні веб-сервера з відомою конфігурацією [10], підключення до якого переважно здійснюється за портом 80/tcp. У цьому випадку на основі утиліти netstat з параметрами: netstat -plan | grep :80 | awk '{print $10}' | cut -d: -f1 | sort | sort -n була здійснена фіксація кількості підключень, а t_η інтерпретується як час $(\eta=\overline{1,60})$, де момент

$$t_1 = 1c,\ t_2 = 2c,\ \ldots,\ t_{60} = 60c,$$

тобто інтервал дискретизації часу відповідає одній секунді (табл. 3.2).

Таблиця 3.2

Значення фізичних параметрів $P_{DSKOП}(t_\eta) = P_{SPKOП}(t_\eta)$, $P_{DSCO3}(t_\eta)$, $P_{DS3M3}(t_\eta)$, $P_{SPKПОА}(t_\eta)$ та їх сенсорів при t_η $(\eta = \overline{1,60})$

t_η $(\eta=\overline{1,60})$	$P_{DSKOП}(t_\eta)=$ $P_{SPKOП}(t_\eta)$	$P_{DSCO3}(t_\eta)$	$P_{DS3M3}(t_\eta)$	$P_{SPKПОА}(t_\eta)$	$S_{211}=$ S_{311}	$S_{212}=$ S_{312}	$S_{213}=$ S_{313}	$S_{214}=$ S_{314}	$S_{215}=$ S_{315}
1; 31	17; 234	87; 79	154; 80	82; 536	0; 0	1; 0	0; 1	0; 0	0; 0
2; 32	19; 234	80; 95	203; 74	89; 512	0; 0	1; 0	0; 1	0; 0	0; 0
3; 33	30; 180	86; 91	217; 72	95; 562	0; 0	1; 0	0; 1	0; 0	0; 0
4; 34	102; 266	101; 89	183; 92	92; 559	0; 0	0; 0	1; 0	0; 1	0; 0
5; 35	70; 195	82; 92	146; 128	96; 541	0; 0	0; 0	1; 1	0; 0	0; 0
6; 36	258; 193	86; 89	151; 93	88; 519	0; 0	0; 0	0; 1	1; 0	0; 0
7; 37	225; 208	95; 86	142; 86	86; 559	0; 0	0; 0	1; 1	0; 0	0; 0
8; 38	294; 279	99; 99	149; 94	81; 527	0; 0	0; 0	0; 0	1; 1	0; 0
9; 39	181; 283	86; 86	191; 89	99; 549	0; 0	0; 0	1; 0	0; 1	0; 0
10; 40	205; 161	100; 98	163; 41	88; 514	0; 0	0; 0	1; 1	0; 0	0; 0
11; 41	170; 161	85; 95	150; 51	99; 541	0; 0	0; 0	1; 1	0; 0	0; 0
12; 42	253; 81	85; 87	215; 35	85; 360	0; 0	0; 0	1; 1	0; 0	0; 0
13; 43	281; 74	79; 100	185; 39	524; 357	0; 0	0; 0	0; 1	1; 0	0; 0
14; 44	164; 41	81; 59	148; 38	539; 357	0; 0	0; 1	1; 0	0; 0	0; 0
15; 45	208; 51	85; 54	145; 46	543; 350	0; 0	0; 1	1; 0	0; 0	0; 0
16; 46	247; 158	82; 51	141; 90	518; 365	0; 0	0; 0	1; 1	0; 0	0; 0
17; 47	125; 26	87; 65	163; 40	542; 359	0; 0	0; 1	1; 0	0; 0	0; 0
18; 48	266; 235	100; 51	168; 60	551; 344	0; 0	0; 0	0; 1	1; 0	0; 0
19; 49	273; 198	87; 64	137; 38	540; 345	0; 0	0; 0	0; 1	1; 0	0; 0
20; 50	285; 178	84; 55	147; 82	541; 367	0; 0	0; 0	0; 1	1; 0	0; 0
21; 51	230; 167	94; 51	123; 54	554; 345	0; 0	0; 0	1; 1	0; 0	0; 0
22; 52	141; 114	92; 51	139; 33	540; 345	0; 0	0; 0	1; 1	0; 0	0; 0
23; 53	79; 253	84; 68	160; 44	537; 363	0; 0	0; 0	1; 1	0; 0	0; 0
24; 54	205; 276	86; 69	143; 57	554; 346	0; 0	0; 0	1; 0	0; 1	0; 0
25; 55	113; 160	80; 61	171; 39	543; 347	0; 0	0; 0	1; 1	0; 0	0; 0
26; 56	175; 289	90; 55	82; 51	532; 358	0; 0	0; 0	1; 0	0; 1	0; 0
27; 57	144; 163	84; 57	94; 60	564; 367	0; 0	0; 0	1; 1	0; 0	0; 0
28; 58	168; 174	94; 55	127; 28	511; 367	0; 0	0; 0	1; 1	0; 0	0; 0
29; 59	169; 174	87; 67	69; 56	563; 356	0; 0	0; 0	1; 1	0; 0	0; 0
30; 60	288; 174	86; 48	103; 33	539; 540	0; 0	0; 0	0; 1	1; 0	0; 0

Для отримання $P_{SPKTЮA}(t_\eta)$ використовувалася інформація згенерована Iptables, а значення $P_{DSCO3}(t_\eta)$ формувалися за допомогою аналізу логів веб-серверу, шляхом підрахунку кількості всіх запитів за визначені моменти t_η $(\eta = \overline{1,60})$.

При формуванні $P_{DS3M3}(t_\eta)$ використовувалася методика вимірювання, яка заснована на створенні потоку для кожного унікального для IP-адреси підключення.

Моніторинг здійснюється шляхом підрахунку кількості отриманих від клієнта запитів зазначеного типу (у даному випадку GET-запитів) за вище прийняті часові інтервали з наступним обчисленням середнього часу між послідовними запитами та занесенням (для зручності відображення даних) результатів в табл. 3.2, з якої, наприклад, видно, що після *30*-ї секунди відбувається зменшення затримки, що при великій кількості підключень може свідчити про початкові атакуючі дії.

Необхідно відмітити, що для різних атак (наприклад, при $n = 2$, $i = \overline{2,3}$) значення частот зустрічальності поточного стану параметрів можуть бути однаковими.

Так, наприклад, в сформованій табл. 3.2

$$P_{21}(t_\eta) = P_{31}(t_\eta) = P_{DSKOП}(t_\eta) = P_{SPKOП}(t_\eta),$$

при цьому значення сенсорів

$$S_{311} = S_{SPKOП1},\ S_{312} = S_{SPKOП2},\ S_{313} = N_{SPKOП3},$$
$$S_{314} = S_{SPKOП4} \text{ та } S_{315} = S_{SPKOП5}$$

для $P_{SPKOП}(t_\eta)$ попадають у відповідні інтервали

- $N_{311} = N_{SPKOП1} <=> [0; 8]$,
- $N_{312} = N_{SPKOП2} <=> [9; 64]$,
- $N_{313} = N_{SPKOП3} <=> [65; 256]$,
- $N_{314} = N_{SPKOП4} <=> [257; 512]$,
- $N_{315} = N_{SPKOП5} <=> [513; 1024]$ (див. п. 2.2),

а відмічені світло-сірим маркером значення

- $P_{SPKOП}(t_1) = 17$,

- $P_{SPKOП}(t_2)=19,$
- $P_{SPKOП}(t_3)=30,$
- $P_{SPKOП}(t_{44})=41,$
- $P_{SPKOП}(t_{45})=51,$
- $P_{SPKOП}(t_{47})=26$

попадають в інтервал

- $N_{312} = N_{SPKOП2} <=> [9; 64].$

Відповідно до (3.2) сенсор $S_{312}(t_\eta)$ визначається як:

$$S_{312}(t_\eta)= S_{SPKOП2}(t_\eta)= \begin{cases} 1, \text{ якщо } P_{SPKOП2}(t_\eta) \in N_{SPKOП2} \\ 0, \text{ якщо } P_{SPKOП2}(t_\eta) \notin N_{SPKOП2} \end{cases},$$

$$(\eta=\overline{1,60}).$$

Очевидно, що в моменти часу t_1, t_2, t_3, t_{44}, t_{45} та t_{47} значення

$$S_{312}(t_1)= S_{312}(t_2)= S_{312}(t_3)= S_{312}(t_{44})=$$
$$S_{312}(t_{45})= S_{312}(t_{47})=1,$$

а протягом інших моментів часу, відповідно дорівнюють *0*.

Для зручності сприйняття заносимо до табл. 3.2 сформовані в зазначені моменти часу стани сенсорів

$$S_{311},\ S_{312},\ S_{313},\ S_{314} \text{ та } S_{315}.$$

Далі, при $n=2$ $(i=\overline{2,3})$, $j=\overline{1,m_i}$, $m_3=2$ і $m_2=3$ визначимо CS_{3j} для

$$P_{31}(t_\eta)= P_{SPKOП}(t_\eta) \text{ та}$$
$$P_{32}(t_\eta)= P_{SPKПОА}(t_\eta)$$

на множині

$$\mathbf{N_{31}}\ (r_j=r_1=5) \text{ та } \mathbf{N_{32}}\ (r_j=r_2=3)$$

(див. табл. 3.3 та 3.4),

а також CS_{2j} для

$$P_{21}(t_\eta)= P_{DSKOП}(t_\eta),$$
$$P_{22}(t_\eta)= P_{DSCO3}(t_\eta) \text{ та}$$

$$P_{23}(t_\eta) = P_{DS3M3}(t_\eta)$$

на множині

$$\mathbf{N_{21}}\ (r_j = r_1 = 5),$$

$$\mathbf{N_{22}}\ (r_j = r_2 = 3)\ \text{та}$$

$$\mathbf{N_{23}}\ (\text{якщо}\ r_j = r_3 = 3)$$

(див. табл. 3.5 та 3.6).

Наприклад, за значення лічильника сенсорів CS_{312} відповідно до виразу (3.3) приймається $CS_{SPKOII2} = 6$ (див. табл. 3.3), а решта CS_{3j} та CS_{2j} визначені аналогічним чином і занесені відповідно в табл. 3.3 та 3.6.

Таблиця 3.3

Частоти зустрічальності поточного стану параметра $P_{SPKOII}(t_\eta)$

CS_{ij}	$\mathbf{N_{31}}\ (r_j = r_1 = 5,\ j = 1)$				
	N_{311}	N_{312}	N_{313}	N_{314}	N_{315}
CS_{3j}	0	6	42	12	0

Таблиця 3.4

Частоти зустрічальності поточного стану параметра $P_{SPKIIOA}(t_\eta)$

CS_{ij}	$\mathbf{N_{32}}\ (r_j = r_2 = 3,\ j = 2)$		
	N_{321}	N_{322}	N_{323}
CS_{3j}	0	12	48

Таблиця 3.5

Частоти зустрічальності поточного стану параметра $P_{DSKOII}(t_\eta)$

CS_{ij}	$\mathbf{N_{21}}\ (r_j = r_1 = 5,\ j = 1)$				
	N_{211}	N_{212}	N_{213}	N_{214}	N_{215}
CS_{2j}	0	6	42	12	0

Таблиця 3.6

Частоти зустрічальності поточного стану параметрів $P_{DSCO3}(t_\eta)$ та $P_{DS3M3}(t_\eta)$

CS_{ij}	$\mathbf{N_{22}}$ $(r_j = r_2 = 3,\ j = 2)$			$\mathbf{N_{23}}$ $(r_j = r_3 = 3,\ j = 3)$		
	N_{221}	N_{222}	N_{223}	N_{231}	N_{232}	N_{233}
CS_{2j}	0	60	0	0	32	28

Таким чином формуються всі частоти зустрічальності поточних параметрів, що відображаються підмножинами лічильників сенсорів $\mathbf{CS_{ij}} \subseteq \mathbf{CS}$.

Формування поправкових еталонів

Етап 2 – формування поправкових еталонів. Для реалізації цього етапу введемо підмножини поправкових еталонів $\mathbf{T^E_{ij}} \subseteq \mathbf{T^E}$, ($\mathbf{T^E}$ – множина всіх можливих поправкових еталонів), кожна з яких базується на $\mathbf{T^e_{ij}}$ (див. п. 2.2) та визначається як

$$\mathbf{T^E_{ij}} = \{\bigcup_{s=1}^{r_j} \underset{\sim}{T}^E_{ijs}\} = \{\underset{\sim}{T}^E_{ij1},\ \underset{\sim}{T}^E_{ij2},\ ...,\ \underset{\sim}{T}^E_{ijs},\ ...,\ \underset{\sim}{T}^E_{ijr_j}\}, \tag{3.4}$$

де $\underset{\sim}{T}^E_{ijs}$ $(s = \overline{1, r_j})$ – поправкові еталонні НЧ. Ці числа формуються на основі перетворення відповідних НЧ (див. (2.35)) з підмножини $\mathbf{T^e_{ij}} \subseteq \mathbf{T^e}$ за допомогою лічильників сенсорів із $\mathbf{CS_{ij}} \subseteq \mathbf{CS}$ відповідно до виразу

$$\{\bigcup_{s=1}^{r_j} \underset{\sim}{T}^E_{ijs}\} = \{\bigcup_{s=1}^{r_j} (\underset{\sim}{T}^e_{ijs} \cdot CS_{ijs})\} = \{\underset{\sim}{T}^e_{ij1} \cdot CS_{ij1},\ \underset{\sim}{T}^e_{ij2} \cdot CS_{ij2},\ ...,\ \underset{\sim}{T}^e_{ijr_j} \cdot CS_{ijr_j}\}. \tag{3.5}$$

Наприклад, для $n = 1$ $(i = 3)$, $j = 1$ відповідно до (3.4) та (3.5) поправкові еталони визначаються як

$$\mathbf{T^E_{31}} = \{\bigcup_{s=1}^{5} \underset{\sim}{T}^E_{31s}\} = \{\bigcup_{s=1}^{5} (\underset{\sim}{T}^e_{31s} \cdot CS_{31s})\} =$$

$$\{\underset{\sim}{T}^e_{311} \cdot CS_{311},\ \underset{\sim}{T}^e_{312} \cdot CS_{312},\ \underset{\sim}{T}^e_{313} \cdot CS_{313},\ \underset{\sim}{T}^e_{314} \cdot CS_{314},\ \underset{\sim}{T}^e_{315} \cdot CS_{315}\} =$$

$$\{\underset{\sim}{OM}^E_{31},\ \underset{\sim}{M}^E_{31},\ \underset{\sim}{C}^E_{31},\ \underset{\sim}{B}^E_{31},\ \underset{\sim}{OB}^E_{31}\}$$

$$\Leftrightarrow$$

$$\mathbf{T^E_{SPKOP}} = \{\bigcup_{s=1}^{5} \underset{\sim}{T}^E_{SPKOP\,s}\} = \{\bigcup_{s=1}^{5} (\underset{\sim}{T}^e_{SPKOPs} \cdot CS_{SPKOP\,s})\} =$$

$$\{\underset{\sim}{T}^e_{SPKOP\,1} \cdot CS_{SPKOP1},\ \underset{\sim}{T}^e_{SPKOP2} \cdot CS_{SPKOP\,2},\ \underset{\sim}{T}^e_{SPKOP\,3} \cdot CS_{SPKOP\,3},$$

$$\underset{\sim}{T}^e_{SPKOP\,4} \cdot CS_{SPKOP4},\ \underset{\sim}{T}^e_{SPKOP\,5} \cdot CS_{SPKOP5}\} =$$

$$\{\underset{\sim}{T}^E_{SPKOP\,1},\ \underset{\sim}{T}^E_{SPKOP2},\ \underset{\sim}{T}^E_{SPKOP\,3},\ \underset{\sim}{T}^E_{SPKOP\,4},\ \underset{\sim}{T}^E_{SPKOP\,5}\}.$$

Таким чином, фактично здійснюється множення НЧ $\underset{\sim}{OM}^e_{31}$, $\underset{\sim}{M}^e_{31}$, $\underset{\sim}{C}^e_{31}$, $\underset{\sim}{B}^e_{31}$ та $\underset{\sim}{OB}^e_{31}$ еталонного підсередовища ($\mathbf{T^e_i = T^e_3 = T^e_{SP}}$) (див. приклад етапу 5 в п. 2.2), що входять в $\mathbf{T^e_{31} = T^e_{SPKOP}}$ на значення CS_{311}, CS_{312}, CS_{313}, CS_{314} та CS_{315} відповідно. Зазначимо, що з урахуванням (3.4) і (3.5)

$$\underset{\sim}{T}^E_{311} = \underset{\sim}{T}^E_{SPKOP\,1} = \underset{\sim}{OM}^E_{31} = \underset{\sim}{OM}^e_{31} \cdot 0 =$$

$$\{\ 0/0{,}008;\ 1/0{,}008;\ 0{,}3/0{,}063;\ 0/0{,}25\ \} \cdot 0 =$$

$$\{\ 0/0;\ 1/0;\ 0{,}3/0;\ 0/0\ \},$$

$$\underset{\sim}{T}^E_{312} = \underset{\sim}{T}^E_{SPKOP2} = \underset{\sim}{M}^E_{31} = \underset{\sim}{M}^e_{31} \cdot 6 =$$

$$\{\ 0/0{,}008;\ 0{,}6/0{,}008;\ 1/0{,}063;\ 0{,}2/0{,}25;\ 0/0{,}5\ \} \cdot 6 =$$

$$\{\ 0/0{,}048;\ 0{,}6/0{,}048;\ 1/0{,}378;\ 0{,}2/1{,}5;\ 0/3\ \},$$

$$\underset{\sim}{T}^E_{313} = \underset{\sim}{T}^E_{SPKOP\,3} = \underset{\sim}{C}^E_{31} = \underset{\sim}{C}^e_{31} \cdot 42 =$$

$$\{\ 0/0{,}008;\ 0{,}4/0{,}063;\ 1/0{,}25;\ 0{,}3/0{,}5;\ 0/1\ \} \cdot 42 =$$

$$\{\ 0/0{,}336;\ 0{,}4/2{,}646;\ 1/10{,}5;\ 0{,}3/21;\ 0/42\ \},$$

$$\underset{\sim}{T}^E_{314} = \underset{\sim}{T}^E_{SPKOP\,4} = \underset{\sim}{B}^E_{31} = \underset{\sim}{B}^e_{31} \cdot 12 =$$

$$\{\ 0/0{,}063;\ 0{,}6/0{,}25;\ 1/0{,}5;\ 0{,}7/1;\ 0/1\ \} \cdot 12 =$$

$$\{\ 0/0{,}756;\ 0{,}6/3;\ 1/6;\ 0{,}7/12;\ 0/12\ \},$$ а

$$\underset{\sim}{T}^E_{315} = \underset{\sim}{T}^E_{SPKOP\,5} = \underset{\sim}{OB}^E_{31} = \underset{\sim}{OB}^e_{31} \cdot 0 =$$

$$\{\ 0/0{,}25;\ 0{,}6/0{,}5;\ 1/1;\ 0/1\ \}\cdot 0 =$$
$$\{\ 0/0;\ 0{,}6/0;\ 1/0;\ 0/0\ \}.$$

За аналогією з $\mathbf{T}^{\mathbf{E}}_{\mathbf{31}}$ реалізуємо обчислення для $\mathbf{T}^{\mathbf{E}}_{\mathbf{32}}$, якщо $n=1$ $(i=3)$ та $j=2$. Тоді, на основі (3.4) та (3.5)

$$\mathbf{T}^{\mathbf{E}}_{\mathbf{32}} = \{\bigcup_{s=1}^{3} \underset{\sim}{T}^{E}_{32\,s}\} =$$

$$\{\bigcup_{s=1}^{3} (\underset{\sim}{T}^{e}_{32s} \cdot CS_{32s})\} =$$

$$\{\underset{\sim}{T}^{e}_{321} \cdot CS_{321},\ \underset{\sim}{T}^{e}_{322} \cdot CS_{322},\ \underset{\sim}{T}^{e}_{323} \cdot CS_{323}\} =$$
$$\{\underset{\sim}{M}^{E}_{32},\ \underset{\sim}{C}^{E}_{32},\ \underset{\sim}{Б}^{E}_{32}\}$$
$$<=>$$
$$\mathbf{T}^{\mathbf{e}}_{\mathbf{SPKПOA}} = \{\bigcup_{s=1}^{3} \underset{\sim}{T}^{E}_{SPKПOA\,s}\} =$$

$$\{\bigcup_{s=1}^{3} (\underset{\sim}{T}^{e}_{SPKПOAs} \cdot CS_{SPKПOAs})\} =$$

$$\{\underset{\sim}{T}^{e}_{SPKПOA\,1} \cdot CS_{SPKПOA\,1},\ \underset{\sim}{T}^{e}_{SPKПOA\,2} \cdot CS_{SPKПOA\,2},\ \underset{\sim}{T}^{e}_{SPKПOA\,3} \cdot CS_{SPKПOA\,3}\} =$$
$$\{\underset{\sim}{T}^{E}_{SPKПOA\,1},\ \underset{\sim}{T}^{E}_{SPKПOA\,2},\ \underset{\sim}{T}^{E}_{SPKПOA\,3}\},$$

а відповідні поправкові еталони обчислюються за виразом:

$$\underset{\sim}{T}^{E}_{321} = \underset{\sim}{T}^{E}_{SPKПOA\,1} = \underset{\sim}{M}^{E}_{32} = \underset{\sim}{M}^{e}_{32} \cdot 0 =$$
$$\{0/0{,}01;\ 1/0{,}01;\ 0{,}2/0{,}1;\ 0/1\}\cdot 0 =$$
$$\{0/0;\ 1/0;\ 0{,}2/0;\ 0/0\};$$
$$\underset{\sim}{T}^{E}_{322} = \underset{\sim}{T}^{E}_{SPKПOA\,2} = \underset{\sim}{C}^{E}_{32} = \underset{\sim}{C}^{e}_{32} \cdot 12 =$$
$$\{0/0{,}01;\ 0{,}5/0{,}01;\ 1/0{,}1;\ 0{,}7/1;\ 0/1\}\cdot 12 =$$
$$\{0/0{,}12;\ 0{,}5/0{,}12;\ 1/1{,}2;\ 0{,}7/12;\ 0/12\};$$
$$\underset{\sim}{T}^{E}_{323} = \underset{\sim}{T}^{E}_{SPKПOA\,3} = \underset{\sim}{Б}^{E}_{32} = \underset{\sim}{Б}^{e}_{32} \cdot 48 =$$
$$\{0/0{,}01;\ 0{,}5/0{,}1;\ 1/1;\ 0/1\}\cdot 48 =$$
$$\{0/0{,}48;\ 0{,}5/4{,}8;\ 1/48;\ 0/48\}.$$

Таким чином, формуються всі підмножини поправкових еталонів $\mathbf{T}^{\mathbf{E}}_{\mathbf{ij}} \subseteq \mathbf{T}^{\mathbf{E}}$.

Формування нечітких параметрів поточного середовища

Етап 3 – формування нечітких параметрів поточного середовища. Реалізація цього етапу здійснюється за наступним виразом

$$\underset{\sim}{P}_{ij}^{\tau_f} = (\sum_{s=1}^{r_j} \underset{\sim}{T}_{ijs}^{E}) / \eta_{max} = \\ (\underset{\sim}{T}_{ij1}^{E} \tilde{+} \underset{\sim}{T}_{ij2}^{E} \tilde{+} ... \tilde{+} \underset{\sim}{T}_{ijs}^{E} \tilde{+} ... \tilde{+} \underset{\sim}{T}_{ijr_j}^{E}) / \eta_{max}. \quad (3.6)$$

де

$$\underset{\sim}{P}_{ij}^{\tau_f} = \{\bigcup_{q=1}^{\rho} \mu_{ijq} / x_{ijq}\} = \\ \{\mu_{ij1} / x_{ij1}, \mu_{ij2} / x_{ij2}, ..., \mu_{ij(\rho-1)} / x_{ij(\rho-1)}, \mu_{ij\rho} / x_{ij\rho}\}, \\ (q = \overline{1,\rho}),$$

ρ – кількість компонент в НЧ $\underset{\sim}{P}_{ij}^{\tau_f}$ поточного підсередовища ($\mathbf{P}_{\mathbf{i}}^{\boldsymbol{\tau}_{\mathbf{f}}}$).

Наприклад, при $n=1$ $(i=3)$ і $j=1$ вираз (3.6), для визначення $\underset{\sim}{P}_{31}^{\tau_f} = \underset{\sim}{P}_{SPKOP}^{\tau_f}$, буде мати наступний вигляд

$$\underset{\sim}{P}_{31}^{\tau_f} = (\sum_{s=1}^{5} \underset{\sim}{T}_{31s}^{E}) / \eta_{max} = \\ (\underset{\sim}{T}_{311}^{E} \tilde{+} \underset{\sim}{T}_{312}^{E} \tilde{+} \underset{\sim}{T}_{313}^{E} \tilde{+} \underset{\sim}{T}_{314}^{E} \tilde{+} \underset{\sim}{T}_{315}^{E}) / \eta_{max} = \\ (\underset{\sim}{T}_{SPKOP\,1}^{E} \tilde{+} \underset{\sim}{T}_{SPKOP\,2}^{E} \tilde{+} \underset{\sim}{T}_{SPKOP\,3}^{E} \tilde{+} \underset{\sim}{T}_{SPKOP\,4}^{E} \tilde{+} \underset{\sim}{T}_{SPKOP\,5}^{E}) / \eta_{max}.$$

Оскільки всі носії НЧ $\underset{\sim}{OM}_{32}^{E}$ та $\underset{\sim}{OB}_{32}^{E}$ (див. приклад етапу 2) мають нульові значення, то відповідно до (3.6) за допомогою методу лінійної апроксимації за локальними максимумами [11] реалізація обчислень виконується наступним чином

$$\underset{\sim}{P}_{SPKOP}^{\tau_f} = (\underset{\sim}{T}_{SPKOP2}^{E} \tilde{+} \underset{\sim}{T}_{SPKOP\,3}^{E} \tilde{+} \underset{\sim}{T}_{SPKOP\,4}^{E}) / \eta_{max} = \\ (\underset{\sim}{M}_{31}^{E} \tilde{+} \underset{\sim}{C}_{31}^{E} \tilde{+} \underset{\sim}{B}_{31}^{E}) / 60 = \\ (\{0/0{,}048;\ 0{,}6/0{,}048;\ 1/0{,}378;\ 0{,}2/1{,}5;\ 0/3\} \tilde{+} \\ \{0/0{,}336;\ 0{,}4/2{,}646;\ 1/10{,}5;\ 0{,}3/21;\ 0/42\} \tilde{+} \\ \{0/0{,}756;\ 0{,}6/3;\ 1/6;\ 0{,}7/12;\ 0/12\})/60 = \\ (\{0/0{,}384;\ 0/2{,}694;\ 0/10{,}548;\ 0/21{,}048;\ 0/42{,}048;$$

0/0,384; 0,4/2,694; 0,6/10,548; 0,3/21,048;
0/42,048; 0/0,714; 0,4/3,024; 1/10,878; 0,3/21,378;
0/42,378; 0/1,836; 0,2/4,146; 0,2/12; 0,2/22,5;
0/43,5; 0/3,336; 0/5,646; 0/13,5; 0/24; 0/45} $\tilde{+}$
{0/0,756; 0,6/3; 1/6; 0,7/12; 0/12})/60=
({*0/2,694; 0,4/2,694; 1/10,878; 0,2/22,5; 0/22,5}* $\tilde{+}$
{0/0,756; 0,6/3; 1/6; 0,7/12; 0/12})/60=
({*0/3,45; 0/5,694; 0/8,694; 0/14,694; 0/14,694;*
0/3,45; 0,4/5,694; 0,4/8,694; 0,4/14,694;
0/14,694; 0/11,634; 0,6/13,878; 1/16,878;
0,7/22,878; 0/22,878;0/23,256; 0,2/25,5;
0,2/28,5; 0,2/34,5; 0/34,5;0/23,256; 0/25,5;
0/28,5; 0/34,5; 0/34,5;})/60=
{0/5,694; 0,4/5,694; 1/16,878; 0,2/34,5; 0/34,5}/60=
{0/0,095; 0,4/0,095; 1/0,28; 0,2/0,58; 0/0,58}.

При цьому, очевидно, що $\rho = 5$.

За аналогією з $\underset{\sim}{P}^{\tau_f}_{SPKOП}$, якщо $n = 1$ $(i = 3)$ і $j = 2$ з урахуванням нульових носіїв в $\underset{\sim}{M}^{E}_{32}$ (див. приклад етапу 2) для $\underset{\sim}{P}^{\tau_f}_{32} = \underset{\sim}{P}^{\tau_f}_{SPKПОА}$ отримаємо

$$\underset{\sim}{P}^{\tau_f}_{SPKПОА} = (\underset{\sim}{T}^{E}_{SPKПОА2} \tilde{+} \underset{\sim}{T}^{E}_{SPKПОА3}) / \eta_{max} =$$
$$(\underset{\sim}{C}^{E}_{32} \tilde{+} \underset{\sim}{Б}^{E}_{32}) /60 =$$

({*0/0,12; 0,5/0,12; 1/1,2; 0,7/12; 0/12}* $\tilde{+}$
{0/0,48; 0,5/4,8; 1/48; 0/48})/60=
({*0/0,6; 0/4,92; 0/48,12; 0/48,12; 0/0,6;*
0,5/4,92; 0,5/48,12; 0/48,12; 0/1,68; 0,5/6;
1/49,2; 0/49,2; 0/12,48; 0,5/16,8; 0,7/60; 0/60;
0/12,48; 0/16,8; 0/60; 0/60})/60=
{0/4,92; 0,5/4,92; 1/49,2; 0,7/60; 0/60}/60=
{0/0,082; 0,5/0,082; 1/0,82; 0,7/1; 0/1}.

При цьому, очевидно, що $\rho = 5$.

В результаті обчислень, утворюються фазифіковані значення поточних параметрів $\mathcal{P}^{\tau_f}_{SPKOП}$ та $\mathcal{P}^{\tau_f}_{SPKПОА}$, графічна інтерпретація яких відносно лінгвістичних еталонів $\mathbf{T^e_{31} = T^e_{SPKOП}}$ та $\mathbf{T^e_{32} = T^e_{SPKПОА}}$ (див. п. 2.2) відображена на рис. 3.1.

Також, на рисунку побудовані нечіткі опорні двовимірні області, які характеризують можливі рівні аномального стану відносно лінгвістичних еталонів $\mathbf{T^e_{SPKOП}}$ та $\mathbf{T^e_{SPKПОА}}$ (див. п. 2.2) і позначаються одним з текстових значень – Н, БНВ, БВН, В, П:

- «НИЗЬКИЙ»,
  «НИЗКИЙ (Н)»,
- «БІЛЬШ НИЗЬКИЙ НІЖ ВИСОКИЙ»,
  «БОЛЬШЕ НИЗКИЙ ЧЕМ ВЫСОКИЙ (БНВ)»,
- «БІЛЬШ ВИСОКИЙ НІЖ НИЗЬКИЙ»,
  «БОЛЬШЕ ВЫСОКИЙ ЧЕМ НИЗКИЙ (БВН)»,
- «ВИСОКИЙ»,
  «ВЫСОКИЙ (В)»,
- «МЕЖЕВИЙ»,
  «ПРЕДЕЛЬНЫЙ (П)».

За допомогою цих еталонів здійснюється пошук нечітких термів

$$\{T^e_{SPKOП\,1},\ T^e_{SPKOП2},\ T^e_{SPKOП\,3},\ T^e_{SPKOП\,4},\ T^e_{SPKOП\,5}\} \text{ та}$$

$$\{T^e_{SPKПОА1},\ T^e_{SPKПОА\,2},\ T^e_{SPKПОА\,3}\},$$

які найбільш близькі до відповідних значень поточних параметрів $\mathcal{P}^{\tau_f}_{SPKOП}$ та $\mathcal{P}^{\tau_f}_{SPKПОА}$,, а також визначається опорна двовимірна область, що відображає поточний рівень аномального стану. Подальша формалізація процесу такого пошуку надає можливість автоматизувати процес виявлення атакуючих дій, ідентифікатором (образом) яких, фактично, будуть виступати сформовані опорні області (див. рис. 3.1).

Запропонований МФП [1, 12], який за рахунок введених множин сенсорів, лічильників сенсорів та поправкових еталонів, а також використання множин лінгвістичних еталонів та відповідних підмножин інтервалів для формування частот зустрічальності значень фізичних параметрів в задані моменти очікуваної події, дозволяє формалізувати процес перетворення поточних значень параме-

трів *m*-вимірних поточних середовищ для їх подальшого застосування у виявленні аномального стану в ІС.

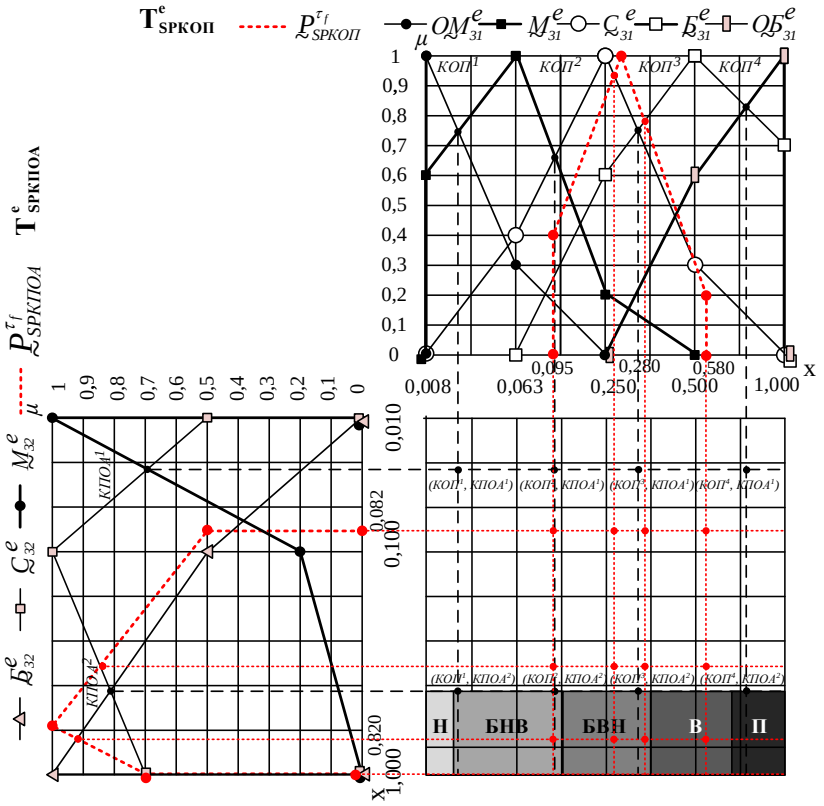

Рис. 3.1. Графічна інтерпретація ідентифікаторів (образів) атакуючих дій (які відображаються двомірними опорними областями Н, БНВ, БВН, В, П) та фазифікованих значень поточних параметрів $\underset{\sim}{P}^{\tau_f}_{SPKOП}$, $\underset{\sim}{P}^{\tau_f}_{SPKПОА}$ відносно лінгвістичних еталонів $\mathbf{T}^{e}_{\mathbf{SPKOП}}$, $\mathbf{T}^{e}_{\mathbf{SPKПОА}}$ відповідно

Маючи узагальнювальні описи процесу фазифікації поточних параметрів та еталонних середовищ для еквівалентного перетворення відповідних НЧ необхідно їх привести до однієї множини визначених α-рівнів.

3.2. Метод α-рівневої номіналізації нечітких чисел для систем виявлення вторгнень

Відповідно до КМАС (див. п. 2.1 та [2-4]) запропоновано метод α-рівневої номіналізації (МАН) [13], який дозволяє формалізувати процес формування α-рівневих інтервалів для еквівалентного перетворення НЧ з еталонних та поточних середовищ. Це надасть можливість визначати ідентифікуючі терми, які відображають поточний стан середовища оточення при вирішенні задач виявлення атак в ІС.

Основу запропонованого методу складають три базових етапи:

- формування α-рівней;
- еквівалентне перетворення НЧ;
- формування узагальнювальних таблиць та графічна інтерпретація нормалізованих НЧ еталонного та поточного підсередовища.

Розглянемо кожен із визначених етапів.

Формування α-рівней

Етап 1 – формування α-рівней. Для реалізації цього етапу створюється відповідний механізм, який заснований на введенні множини всіх можливих α-рівнів $\mathbf{AL}$ та підмножини таких α-рівнів $\mathbf{AL_{ij}} \subseteq \mathbf{AL}$:

$$\mathbf{AL_{ij}} = \{ \bigcup_{k=1}^{\pi} AL_{ijk} \} = \{ AL_{ij1},\ AL_{ij2},\ ...,\ AL_{ij\pi} \}, \tag{3.7}$$

що використовується для перетворення НЧ, які відображають $\mathbf{P_i}$ (див. (2.8), [2]) з базовою терм-множиною $\mathbf{T_{ij}}$ (див. (2.44), [5]), де π – кількість членів у множині $\mathbf{AL_{ij}}$, а AL_{ijk} $(k = \overline{1,\pi})$ – k-й член множини $\mathbf{AL_{ij}}$, що відповідає k-му α-рівню [11, 14]. Зазначимо, що всі члени множини $\mathbf{AL_{ij}}$ формуються за формулою

$$\mathbf{AL_{ij}} = \{ \bigcup_{s=1}^{r} \{ \bigcup_{q=1}^{r_s} \mu^{e}_{ijsq} \} \}, \tag{3.8}$$

значення величини якої введені в п. 2.2. (див. етап 5). З виразів (3.7) та (3.8) слідує те, що

$$\mathbf{AL_{ij}} = \{\bigcup_{k=1}^{\pi} AL_{ijk}\} = \{\bigcup_{s=1}^{r}\{\bigcup_{q=1}^{r_s} \mu^e_{ijsq}\}\}. \quad (3.9)$$

Наприклад, якщо $n=1$ $(i=3,$ тобто для кібератаки з ІД $CA_3 = CA_{SP} = SP),$ $j=1$ $(P_{31} = P_{SPKOП} = KOП),$ $r=5,$ $s=\overline{1,5},$ $r_1=4,$ $r_2=5,$ $r_3=5,$ $r_4=5$ та $r_5=4$ і при значенні μ^e_{31sq}, що відповідає μ^e_{21sq} (див. значення величин прикладу етапу 5 в п. 2.2), то підмножина $\mathbf{AL_{ij}} = \mathbf{AL_{31}}$ з урахуванням (3.9) приймає вигляд

$$\mathbf{AL_{31}} = \{\bigcup_{k=1}^{\pi} AL_{31k}\} = \{\bigcup_{s=1}^{r}\{\bigcup_{q=1}^{r_s} \mu^e_{31sq}\}\} =$$
$$\{\{\mu^e_{3111},\ \mu^e_{3112},\ \mu^e_{3113},\ \mu^e_{3114}\},$$
$$\{\mu^e_{3121},\ \mu^e_{3122},\ \mu^e_{3123},\ \mu^e_{3124},\ \mu^e_{3125}\},$$
$$\{\mu^e_{3131},\ \mu^e_{3132},\ \mu^e_{3133},\ \mu^e_{3134},\ \mu^e_{3135}\},$$
$$\{\mu^e_{3141},\ \mu^e_{3142},\ \mu^e_{3143},\ \mu^e_{3144},\ \mu^e_{3145}\},$$
$$\{\mu^e_{3151},\ \mu^e_{3152},\ \mu^e_{3153},\ \mu^e_{3154}\}\} =$$
$$\{\{0;\ 1;\ 0{,}3;\ 0\},\ \{0;\ 0{,}6;\ 1;\ 0{,}2;\ 0\},$$
$$\{0;\ 0{,}4;\ 1;\ 0{,}3\ ;\ 0\},\ \{0;\ 0{,}6;\ 1;\ 0{,}7;\ 0\},\ \{0;\ 0{,}6;\ 1;\ 0\}\} =$$
$$\{0;\ 0{,}2;\ 0{,}3;\ 0{,}4;\ 0{,}6;\ 0{,}7;\ 1\}.$$

В процесі формування членів підмножини $\mathbf{AL_{31}}$ визначається їх кількість, тобто $\pi = 7,$ отже (3.7) можна відобразити як

$$\mathbf{AL_{31}} = \{\bigcup_{k=1}^{\pi} AL_{31k}\} =$$
$$\{AL_{311},\ AL_{312},\ AL_{313},\ AL_{314},\ AL_{315},\ AL_{316},\ AL_{317}\} =$$
$$\{AL_{SPKOП1},\ AL_{SPKOП2},\ AL_{SPKOП3},\ AL_{SPKOП4},$$
$$AL_{SPKOП5},\ AL_{SPKOП6},\ AL_{SPKOП7}\} =$$
$$\{0;\ 0{,}2;\ 0{,}3;\ 0{,}4;\ 0{,}6;\ 0{,}7;\ 1\},$$

де:

- $AL_{311} = AL_{SPKOП1} = 0,$
- $AL_{312} = AL_{SPKOП2} = 0{,}2,$

- $AL_{313} = AL_{SPKOП3} = 0,3,$
- $AL_{314} = AL_{SPKOП4} = 0,4,$
- $AL_{315} = AL_{SPKOП5} = 0,6,$
- $AL_{316} = AL_{SPKOП6} = 0,7,$
- $AL_{317} = AL_{SPKOП7} = 1.$

Аналогічним чином для $n = 1$ $(i = 3,$ тобто для кібератаки з ІД $CA_3 = CA_{SP} = SP),$ $j = 2$ $(P_{32} = P_{SPKПОА} = КПОА),$ $r = 3,$ $s = \overline{1,3},$ $r_1 = 4,$ $r_2 = 5$ та $r_3 = 4$ (див. значення величин у п. 2.2), підмножина $\mathbf{AL_{ij}} = \mathbf{AL_{32}}$ відповідно до (3.9) приймає вигляд

$$\mathbf{AL_{32}} = \{\bigcup_{k=1}^{\pi} AL_{32k}\} = \{\bigcup_{s=1}^{r}\{\bigcup_{q=1}^{r_s} \mu^e_{32sq}\}\} =$$

$$\{\{\mu^e_{3211},\ \mu^e_{3212},\ \mu^e_{3213},\ \mu^e_{3214}\},$$

$$\{\mu^e_{3221},\ \mu^e_{3222},\ \mu^e_{3223},\ \mu^e_{3224},\ \mu^e_{3225}\},$$

$$\{\mu^e_{3231},\ \mu^e_{3232},\ \mu^e_{3233},\ \mu^e_{3234}\} =$$

$$\{\{0;\ 1;\ 0,2;\ 0\},\ \{0;\ 0,5;\ 1;\ 0,7;\ 0\},\ \{0;\ 0,5;\ 1;\ 0\}\} =$$

$$\{0;\ 0,2;\ 0,5;\ 0,7;\ 1\},$$

а кількість членів підмножини $\mathbf{AL_{32}}$ – $\pi = 5.$ Таким чином, (3.7) можна представити у вигляді:

$$\mathbf{AL_{32}} = \{\bigcup_{k=1}^{\pi} AL_{32k}\} =$$

$$\{AL_{321},\ AL_{322},\ AL_{323},\ AL_{324},\ AL_{325}\} =$$

$$\{AL_{SPKПОА1},\ AL_{SPKПОА2},\ AL_{SPKПОА3},\ AL_{SPKПОА4},\ AL_{SPKПОА5}\} =$$

$$\{0;\ 0,2;\ 0,5;\ 0,7;\ 1\},$$

де:

- $AL_{321} = AL_{SPKПОА1} = 0,$
- $AL_{322} = AL_{SPKПОА2} = 0,2,$
- AL_{323} ,$= AL_{SPKПОА3} = 0,5,$
- $AL_{324} = AL_{SPKПОА4} = 0,7,$

- $AL_{325} = AL_{SPKПОА5} = 1$.

Еквівалентне перетворення нечітких чисел

Етап 2 – еквівалентне перетворення НЧ. Відповідно до цього етапу зведемо всі НЧ еталонного та поточного середовища ($\mathbf{T^e}$ та $\mathbf{P^{\tau_f}}$) до номінального (одного для всіх) числа компонент шляхом їх перетворення за допомогою підмножин $\mathbf{AL_{ij}}$.

Крок 1. Введемо множину всіх можливих перетворених або номіналізованих (приведених до z) НЧ еталонних середовищ ($\mathbf{T^e}$) $\mathbf{T_{ij}^{ep}} \subseteq \mathbf{T^{ep}}$

$$\mathbf{T_{ij}^{ep}} = \{ \bigcup_{s=1}^{r} \underset{\sim}{T}_{ijs}^{ep} \} = \{ \underset{\sim}{T}_{ij1}^{ep},\ \underset{\sim}{T}_{ij2}^{ep},\ \ldots,\ \underset{\sim}{T}_{ijs}^{ep},\ \ldots,\ \underset{\sim}{T}_{ijr}^{ep} \}, \quad (s = \overline{1,r}) \tag{3.10}$$

та отримане на їх основі перетворене НЧ $\underset{\sim}{P}_{ij}^{\tau_f p}$ поточних середовищ ($\mathbf{P^{\tau_f}}$).

З урахуванням (3.10) сформуємо в загальному вигляді перетворене НЧ $\underset{\sim}{T}_{ijs}^{ep}$ еталонного (див. (3.11)) та відповідне перетворене НЧ $\underset{\sim}{P}_{ij}^{\tau_f p}$ поточного середовища ($\mathbf{T^e}$ та $\mathbf{P^{\tau_f}}$) (див. (3.12)) тобто:

$$\underset{\sim}{T}_{ijs}^{ep} = \{ \bigcup_{g=1}^{z} \mu_{ijsg}^{ep} / x_{ijsg}^{ep} \} = \{ \mu_{ijs1}^{ep} / x_{ijs1}^{ep},\ \mu_{ijs2}^{ep} / x_{ijs2}^{ep}, \ldots,\ \mu_{ijsz}^{ep} / x_{ijsz}^{ep} \}, \quad (g = \overline{1,z}),\ (z = 2\pi\text{-}1),\ (s = \overline{1,r}), \tag{3.11}$$

де:

- $\mu_{ijsg}^{ep} = \mu_{ijs(z-g+1)}^{ep} = AL_{ijg}$,
- $\mu_{ijs1}^{ep} = \mu_{ijs1}^{e}$, $x_{ijs1}^{ep} = x_{ijs1}^{e}$,

z – кількість компонент в $\underset{\sim}{T}_{ijs}^{ep}$ та

$$\underset{\sim}{P}_{ij}^{\tau_f p} = \{ \bigcup_{g=1}^{z} \mu_{ijg}^{p} / x_{ijg}^{p} \} = \{ \mu_{ij1}^{p} / x_{ij1}^{p},\ \mu_{ij2}^{p} / x_{ij2}^{p}, \ldots,\ \mu_{ijz}^{p} / x_{ijz}^{p} \}, \tag{3.12}$$

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

де:

- $\mu_{ijg}^{p}=\mu_{ij(z-g+1)}^{p}=AL_{ijg}$,
- $\mu_{ij1}^{p}=\mu_{ij1},\ x_{ij1}^{p}=x_{ij1}$,

z – кількість компонент в $\underset{\sim}{P}_{ij}^{\tau_f p}$.

Очевидно, що число компонент всіх НЧ однакове та визначається параметром z, який назвемо номінальним числом компонент або просто номіналом.

Крок 2. Номіналізація (перетворення до z) НЧ $\underset{\sim}{T}_{ijs}^{ep}$ еталонного середовища ($\mathbf{T^e}$) здійснюється шляхом введення підмножини α-рівневих інтервалів $\mathbf{AL_{ij}^{Ie}\subseteq AL}$, що складаються з r членів і відображають $\mathbf{T_{ij}^{e}}$ (див. (2.35)), тобто

$$\mathbf{AL_{ij}^{Ie}}=\{\bigcup_{s=1}^{r}\mathbf{AL_{ijs}^{Ie}}\}=$$
$$\{\mathbf{AL_{ij1}^{Ie}},\ \mathbf{AL_{ij2}^{Ie}},\ \ldots,\ \mathbf{AL_{ijr}^{Ie}}\},\qquad(3.13)$$
$$(s=\overline{1,r}),$$

де

$$\mathbf{AL_{ijs}^{Ie}}=\{\bigcup_{b=1}^{r_s-1}\mathbf{AL_{ijsb}^{Ie}}\}=$$
$$\{\mathbf{AL_{ijs1}^{Ie}},\ \mathbf{AL_{ijs2}^{Ie}},\ \ldots,\ \mathbf{AL_{ijsr_s-1}^{Ie}}\},\qquad(3.14)$$
$$(b=\overline{1,r_s-1}),$$

при цьому $\mathbf{AL_{ijs}^{Ie}\subseteq AL_{ij}^{Ie}}$, а r_s $(s=\overline{1,r})$ визначає кількість компонент в $\underset{\sim}{T}_{ijs}^{e}$ (див. (2.37)).

З урахуванням (3.14) представимо (3.13) в наступному вигляді

$$\mathbf{AL_{ij}^{Ie}}=\{\bigcup_{s=1}^{r}\mathbf{AL_{ijs}^{Ie}}\}=\{\bigcup_{s=1}^{r}\{\bigcup_{b=1}^{r_s-1}\mathbf{AL_{ijsb}^{Ie}}\}\}=\qquad(3.15)$$
$$\{\{\mathbf{AL_{ij11}^{Ie}},\ \mathbf{AL_{ij12}^{Ie}},\ \ldots,\ \mathbf{AL_{ij1r_1-1}^{Ie}}\},$$

$$\{\mathbf{AL}^{\mathbf{Ie}}_{\mathbf{ij21}},\ \mathbf{AL}^{\mathbf{Ie}}_{\mathbf{ij22}},\ \ldots,\ \mathbf{AL}^{\mathbf{Ie}}_{\mathbf{ij2\,r_2-1}}\},$$

$$\ldots,$$

$$\{\mathbf{AL}^{\mathbf{Ie}}_{\mathbf{ijs1}},\ \mathbf{AL}^{\mathbf{Ie}}_{\mathbf{ijs2}},\ \ldots,\ \mathbf{AL}^{\mathbf{Ie}}_{\mathbf{ijr\,r_r-1}}\}\},$$

при цьому $\mathbf{AL}^{\mathbf{Ie}}_{\mathbf{ijsb}} \subseteq \mathbf{AL}^{\mathbf{Ie}}_{\mathbf{ijs}}$ є підмножиною міжточкових α-рівневих інтервалів, що представляється як

$$\mathbf{AL}^{\mathbf{Ie}}_{\mathbf{ijsb}} = \{\bigcup_{c=1}^{k_b} AL^{Ie}_{ijsbc}\} = \{AL^{Ie}_{ijsb1},\ AL^{Ie}_{ijsb2},\ \ldots,\ AL^{Ie}_{ijsbk_b}\},$$
$$(b=\overline{1,r_s-1}), \tag{3.16}$$

де k_b – кількість членів в підмножині $\mathbf{AL}^{\mathbf{Ie}}_{\mathbf{ijsb}}$, значення кожного з яких знаходиться на інтервалі між двома точками μ^e_{ijsq} та μ^e_{ijsq+1}, тобто для всіх членів $\mathbf{AL}^{\mathbf{Ie}}_{\mathbf{ijsb}}$ виконується умова:

$$\begin{cases} \mu^e_{ijsq} < AL^{Ie}_{ijsbc} \le \mu^e_{ijsq+1}, якщо\ x^e_{ijsq+1} \le x^e_{ijsmax} \\ \mu^e_{ijsq} > AL^{Ie}_{ijsbc} \ge \mu^e_{ijsq+1},\ якщо\ x^e_{ijsq+1} \ge x^e_{ijsmax} \end{cases},$$
$$(c=\overline{1,k_b}),\ (q=\overline{1,r_s}),$$

де x^e_{ijsmax} є таким носієм НЧ $\underset{\sim}{T}^e_{ijs}$, значення ФН якого визначається за виразом $\mu^e_{ijsmax} = \bigvee_{q=1}^{r_s} \mu^e_{ijsq}$.

Іншими словами можна сказати, що при супорті x^e_{ijsmax} в НЧ $\underset{\sim}{T}^e_{ijs}$ міститься максимальне значення ФН μ^e_{ijsmax}, тобто існує компонент $\mu^e_{ijsmax} / x^e_{ijsmax}$.

Далі, для $\mathbf{AL}^{\mathbf{Ie}}_{\mathbf{ij}}$, з урахуванням (3.16), представимо (3.15) в наступному вигляді:

$$\mathbf{AL}^{\mathbf{Ie}}_{\mathbf{ij}} = \{\bigcup_{s=1}^{r} AL^{Ie}_{ijs}\} = \{\bigcup_{s=1}^{r}\{\bigcup_{b=1}^{r_s-1}\{\bigcup_{c=1}^{k_b} AL^{Ie}_{ijsbc}\}\}\} =$$
$$\{\{\{AL^{Ie}_{ij111},\ AL^{Ie}_{ij112},\ \ldots,\ AL^{Ie}_{ij11k_1}\},$$
$$\{AL^{Ie}_{ij121},\ AL^{Ie}_{ij122},\ \ldots,\ AL^{Ie}_{ij12k_2}\}, \tag{3.17}$$

$$
\begin{gathered}
\ldots, \\
\{ AL^{Ie}_{ij1(r_1-1)1},\ AL^{Ie}_{ij1(r_1-1)2},\ \ldots,\ AL^{Ie}_{ij1(r_1-1)k_{r_1-1}} \}\},
\end{gathered}
$$

$$
\begin{gathered}
\{\{ AL^{Ie}_{ij211},\ AL^{Ie}_{ij212},\ \ldots,\ AL^{Ie}_{ij21k_1} \}, \\
\{ AL^{Ie}_{ij221},\ AL^{Ie}_{ij222},\ \ldots,\ AL^{Ie}_{ij22k_2} \}, \\
\ldots, \\
\{ AL^{Ie}_{ij2(r_2-1)1},\ AL^{Ie}_{ij2(r_2-1)2},\ \ldots,\ AL^{Ie}_{ij2(r_2-1)k_{r_2-1}} \}\}, \\
\ldots, \\
\{\{ AL^{Ie}_{ijr11},\ AL^{Ie}_{ijr12},\ \ldots,\ AL^{Ie}_{ijr1k_1} \}, \\
\{ AL^{Ie}_{ijr21},\ AL^{Ie}_{ijr22},\ \ldots,\ AL^{Ie}_{ijr2k_2} \}, \\
\ldots, \\
\{ AL^{Ie}_{ijr(r_r-1)1},\ AL^{Ie}_{ijr(r_r-1)2},\ \ldots,\ AL^{Ie}_{ijr(r_r-1)k_{r_r-1}} \}\}\}.
\end{gathered}
$$

Крок 3. Формування перетвореного (нормалізованого) НЧ $\underset{\sim}{P}^{\tau_f p}_{ij}$ поточного середовища ($\mathbf{P}^{\boldsymbol{\tau_f}}$) за аналогією з (3.16) здійснюється шляхом введення відповідної підмножини міжточкових α-рівневих інтервалів

$$
\begin{gathered}
\mathbf{AL^{Ip}_{ijb}} = \{ \bigcup_{c=1}^{k_b} AL^{Ip}_{ijbc} \} = \\
\{ AL^{Ip}_{ijb1},\ AL^{Ip}_{ijb2},\ \ldots,\ AL^{Ip}_{ijbk_b} \}, \\
(b = \overline{1,\rho-1}),
\end{gathered}
\tag{3.18}
$$

де ρ – кількість компонент в НЧ $\underset{\sim}{P}^{\tau_f p}_{ij}$ поточного середовища ($\mathbf{P}^{\boldsymbol{\tau_f}}$) (див. (3.6), [1]), k_b – кількість членів в підмножині $\mathbf{AL^{Ip}_{ijb}}$, значення кожного з яких знаходиться між двома точками μ_{ijq} та μ_{ijq+1}, тобто для всіх членів $\mathbf{AL^{Ip}_{ijb}}$ виконується умова:

$$
\begin{gathered}
\begin{cases}
\mu_{ijq} < AL^{Ip}_{ijbc} \le \mu_{ijq+1}, якщо\ x_{ijq+1} \le x_{ijmax} \\
\mu_{ijq} > AL^{Ip}_{ijbc} \ge \mu_{ijq+1},\ якщо\ x_{ijq+1} \ge x_{ijmax}
\end{cases}, \\
(c = \overline{1,k_b}),\ (q = \overline{1,\rho}),
\end{gathered}
$$

де x_{ijmax} є таким носієм НЧ $\underset{\sim}{P}_{ij}^{\tau_f}$, значення ФН якого визначається за виразом

$$\mu_{ijmax} = \bigvee_{q=1}^{\rho} \mu_{ijq},$$

тобто супорт x_{ijmax} в НЧ $\underset{\sim}{P}_{ij}^{\tau_f}$ містить максимальне значення ФН μ_{ijmax}.

Далі, за аналогією з (3.17) та з урахуванням (3.18), здійснимо необхідні перетворення, тобто сформуємо

$$\begin{gathered}\mathbf{AL_{ij}^{Ie}} = \{\bigcup_{b=1}^{\rho-1}\{\bigcup_{c=1}^{k_b} AL_{ijbc}^{Ip}\}\} = \\ \{\{ AL_{ij11}^{Ip},\ AL_{ij12}^{Ip},\ \ldots,\ AL_{ij1k_1}^{Ip} \}, \\ \{ AL_{ij21}^{Ip},\ AL_{ij22}^{Ip},\ \ldots,\ AL_{ij2k_2}^{Ip} \}, \\ \ldots, \\ \{ AL_{ij(\rho-1)1}^{Ip},\ AL_{ij(\rho-1)2}^{Ip},\ \ldots,\ AL_{ij(\rho-1)k_{\rho-1}}^{Ip} \}\}.\end{gathered} \tag{3.19}$$

Крок 4. Обчислення значень $x_{ijsg}^{ep},\ (g = \overline{1,z})$ для номіналізованих НЧ еталонного середовища ($\mathbf{T^e}$) здійснюється за допомогою виразу

$$\begin{gathered}x_{ijsg}^{ep} = x_{ijsq}^{e} + \frac{(\mu_{ijsg}^{ep} - \mu_{ijsq}^{e})(x_{ijsq+1}^{e} - x_{ijsq}^{e})}{\mu_{ijsq+1}^{e} - \mu_{ijsq}^{e}}, \\ (g = \overline{2,z}),\end{gathered} \tag{3.20}$$

при цьому $\mu_{ijs1}^{ep} = \mu_{ijs1}^{e},\ x_{ijs1}^{ep} = x_{ijs1}^{e},$ а

$$\begin{gathered}\mu_{ijs1}^{ep} = AL_{ijs11}^{Ie},\ \mu_{ijs2}^{ep} = AL_{ijs12}^{Ie},\ \ldots,\ \mu_{ijsk_1}^{ep} = AL_{ijs1k_1}^{Ie}, \\ \mu_{ijs(k_1+1)}^{ep} = AL_{ijs21}^{Ie},\ \mu_{ijs(k_1+2)}^{ep} = AL_{ijs22}^{Ie},\ \ldots,\ \mu_{ijs(k_1+k_2)}^{ep} = AL_{ijs2k_2}^{Ie}, \\ \ldots, \\ \mu_{ijs(k_1+k_2+k_3+\ldots+k_{b-1}+1)}^{ep} = AL_{ijr(r_s-1)1}^{Ie},\ \mu_{ijs(k_1+k_2+k_3+\ldots+k_{b-1}+2)}^{ep} = AL_{ijr(r_s-1)2}^{Ie}, \\ \ldots, \\ \mu_{ijsz}^{ep} = AL_{ijr(r_s-1)k_b}^{Ie},\end{gathered} \tag{3.21}$$

де $z = \sum_{h=1}^{b} k_h$.

Крок 5. Обчислення значень x_{ijg}^{p}, $(g = \overline{1,z})$ для номіналізованих НЧ поточного середовища ($\mathbf{P}^{\tau_f}$) здійснюється аналогічно кроку 4 за виразом

$$x_{ijg}^{p} = x_{ijq} + \frac{(\mu_{ijg}^{p} - \mu_{ijq})(x_{ijq+1} - x_{ijq})}{\mu_{ijq+1} - \mu_{ijq}}, \quad (g = \overline{2,z}), \tag{3.22}$$

при цьому $\mu_{ij1}^{p} = \mu_{ij1}$, $x_{ij1}^{p} = x_{ij1}$, а

$$\begin{gathered}
\mu_{ij1}^{p} = AL_{ij11}^{Ip},\ \mu_{ij2}^{p} = AL_{ij12}^{Ip},\ \ldots,\ \mu_{ijk_1}^{p} = AL_{ij1k_1}^{Ip}, \\
\mu_{ij(k_1+1)}^{p} = AL_{ij21}^{Ip},\ \mu_{ij(k_1+2)}^{p} = AL_{ij22}^{Ip},\ \ldots,\ \mu_{ij(k_1+k_2)}^{p} = AL_{ij2k_2}^{Ip}, \\
\ldots, \\
\mu_{ij(k_1+k_2+k_3+\ldots+k_{b-1}+1)}^{p} = AL_{ij(\rho-1)1}^{Ip},\ \mu_{ij(k_1+k_2+k_3+\ldots+k_{b-1}+2)}^{p} = AL_{ij(\rho-1)2}^{Ip}, \\
\ldots, \\
\mu_{ijz}^{p} = AL_{ij(\rho-1)k_b}^{Ip},
\end{gathered} \tag{3.23}$$

де $z = \sum_{h=1}^{b} k_h$.

Наприклад, для $n=1$ $(i=3,$ тобто для кібератаки з ІД $CA_3 = CA_{SP} = SP),$ якщо

$$j = 3\ (P_{31} = P_{SPKOП} = KOП),\ r = 5 \text{ та якщо}$$

$$j = 6\ (P_{32} = P_{SPKПOA} = KПOA),\ r = 3 \text{ (див. п. 2.2 та [5-7])}$$

приведемо всі НЧ еталонного та поточного підсередовища ($\mathbf{T_i^e} = \mathbf{T_3^e} = \mathbf{T_{SP}^e}$ та $\mathbf{P_i^{\tau_f}} = \mathbf{P_3^{\tau_f}} = \mathbf{P_{SP}^{\tau_f}}$) до одного числа компонент шляхом їх перетворення за допомогою підмножин $\mathbf{AL_{ij}} = \mathbf{AL_{31}}$ та $\mathbf{AL_{ij}} = \mathbf{AL_{32}}$.

Крок 1. Для цього, відповідно до (3.10), множину всіх можливих номіналізованих НЧ $\mathbf{T_{ij}^{ep}} = \mathbf{T_{31}^{ep}} = \mathbf{T_{SPKOП}^{ep}}$ та $\mathbf{T_{ij}^{ep}} = \mathbf{T_{32}^{ep}} = \mathbf{T_{SPKПOA}^{ep}}$ еталонних підсередовищ ($\mathbf{T_i^e} = \mathbf{T_3^e} = \mathbf{T_{SP}^e}$) представимо у вигляді:

$$\mathbf{T}_{\mathbf{31}}^{\mathbf{ep}} = \{ \bigcup_{s=1}^{5} \underset{\sim}{T}_{ijs}^{ep} \} =$$

$$\{ \underset{\sim}{T}_{311}^{ep},\ \underset{\sim}{T}_{312}^{ep},\ \underset{\sim}{T}_{313}^{ep},\ \underset{\sim}{T}_{314}^{ep},\ \underset{\sim}{T}_{315}^{ep} \} =$$

$$\{ \underset{\sim}{T}_{SPKOP1}^{ep},\ \underset{\sim}{T}_{SPKOP2}^{ep},\ \underset{\sim}{T}_{SPKOP3}^{ep},\ \underset{\sim}{T}_{SPKOP4}^{ep},\ \underset{\sim}{T}_{SPKOP5}^{ep} \} =$$

$$\{ \underset{\sim}{OM}_{31}^{ep},\ \underset{\sim}{M}_{31}^{ep},\ \underset{\sim}{C}_{31}^{ep},\ \underset{\sim}{B}_{31}^{ep},\ \underset{\sim}{OB}_{31}^{ep} \},$$

де члени підмножини $\mathbf{T}_{\mathbf{31}}^{\mathbf{ep}}$ – $\underset{\sim}{OM}_{31}^{ep},\ \underset{\sim}{M}_{31}^{ep},\ \underset{\sim}{C}_{31}^{ep},\ \underset{\sim}{B}_{31}^{ep},\ \underset{\sim}{OB}_{31}^{ep}$ є номіналізовані НЧ еталонного підсередовища ($\mathbf{T}_{\mathbf{i}}^{\mathbf{e}} = \mathbf{T}_{\mathbf{3}}^{\mathbf{e}}$), тобто

- $\underset{\sim}{T}_{311}^{ep} = \underset{\sim}{T}_{SPKOP1}^{ep} = \underset{\sim}{OM}_{31}^{ep}$,
- $\underset{\sim}{T}_{312}^{ep} = \underset{\sim}{T}_{SPKOP2}^{ep} = \underset{\sim}{M}_{31}^{ep}$,
- $\underset{\sim}{T}_{313}^{ep} = \underset{\sim}{T}_{SPKOP3}^{ep} = \underset{\sim}{C}_{31}^{ep}$,
- $\underset{\sim}{T}_{314}^{ep} = \underset{\sim}{T}_{SPKOP4}^{ep} = \underset{\sim}{B}_{31}^{ep}$,
- $\underset{\sim}{T}_{315}^{ep} = \underset{\sim}{T}_{SPKOP5}^{ep} = \underset{\sim}{OB}_{31}^{ep}$

та

$$\mathbf{T}_{\mathbf{32}}^{\mathbf{ep}} = \{ \bigcup_{s=1}^{3} \underset{\sim}{T}_{jis}^{ep} \} = \{ \underset{\sim}{T}_{321}^{ep},\ \underset{\sim}{T}_{322}^{ep},\ \underset{\sim}{T}_{323}^{ep} \} =$$

$$\{ \underset{\sim}{T}_{SPKPOA1}^{ep},\ \underset{\sim}{T}_{SPKPOA2}^{ep},\ \underset{\sim}{T}_{SPKPOA3}^{ep} \} =$$

$$\{ \underset{\sim}{M}_{32}^{ep},\ \underset{\sim}{C}_{32}^{ep},\ \underset{\sim}{B}_{32}^{ep} \},$$

де члени підмножини $\mathbf{T}_{\mathbf{32}}^{\mathbf{ep}}$ – $\underset{\sim}{M}_{32}^{ep},\ \underset{\sim}{C}_{32}^{ep},\ \underset{\sim}{B}_{32}^{ep}$ є номіналізованими НЧ еталонного підсередовища ($\mathbf{T}_{\mathbf{i}}^{\mathbf{e}} = \mathbf{T}_{\mathbf{3}}^{\mathbf{e}}$):

- $\underset{\sim}{T}_{321}^{ep} = \underset{\sim}{T}_{SPKPOA1}^{ep} = \underset{\sim}{M}_{32}^{ep}$,
- $\underset{\sim}{T}_{322}^{ep} = \underset{\sim}{T}_{SPKPOA2}^{ep} = \underset{\sim}{C}_{32}^{ep}$,
- $\underset{\sim}{T}_{323}^{ep} = \underset{\sim}{T}_{SPKPOA3}^{ep} = \underset{\sim}{B}_{32}^{ep}$.

Далі, при $i = j = 3,\ \pi = 7,\ s = \overline{1,5},\ r = 5,\ z = 2 \cdot 7 - 1 = 13,\ g = \overline{1,13}$ сформуємо номіналізовані $\underset{\sim}{T}_{311}^{ep},\ \underset{\sim}{T}_{312}^{ep},\ \underset{\sim}{T}_{313}^{ep},\ \underset{\sim}{T}_{314}^{ep},\ \underset{\sim}{T}_{315}^{ep}$ та відповідне перетворене $\underset{\sim}{P}_{31}^{\tau_f p}$ НЧ еталонного та поточного підсередовища ($\mathbf{T}_{\mathbf{i}}^{\mathbf{e}} = \mathbf{T}_{\mathbf{3}}^{\mathbf{e}} = \mathbf{T}_{\mathbf{SP}}^{\mathbf{e}}$ та $\mathbf{P}_{\mathbf{i}}^{\boldsymbol{\tau}_{\mathbf{f}}} = \mathbf{P}_{\mathbf{3}}^{\boldsymbol{\tau}_{\mathbf{f}}} = \mathbf{P}_{\mathbf{SP}}^{\boldsymbol{\tau}_{\mathbf{f}}}$).

Для цього представимо всі НЧ еталонного підсередовища ($\mathbf{T_i^e = T_3^e}$), що відображають $P_{31} = P_{SPKOП}$, з урахуванням (3.11), в наступному вигляді:

$$\underset{\sim}{T}^{ep}_{311} = \{\bigcup_{g=1}^{13} \mu^{ep}_{311g} / x^{ep}_{311g}\} =$$

$$\{\mu^{ep}_{3111} / x^{ep}_{3111},\ \mu^{ep}_{3112} / x^{ep}_{3112},\ \mu^{ep}_{3113} / x^{ep}_{3113},\ \mu^{ep}_{3114} / x^{ep}_{3114},\ \mu^{ep}_{3115} / x^{ep}_{3115},$$
$$\mu^{ep}_{3116} / x^{ep}_{3116},\ \mu^{ep}_{3117} / x^{ep}_{3117},\ \mu^{ep}_{3118} / x^{ep}_{3118},\ \mu^{ep}_{3119} / x^{ep}_{3119},\ \mu^{ep}_{311(10)} / x^{ep}_{311(10)},$$
$$\mu^{ep}_{311(11)} / x^{ep}_{311(11)},\ \mu^{ep}_{311(12)} / x^{ep}_{311(12)},\ \mu^{ep}_{311(13)} / x^{ep}_{311(13)}\},$$

де:

- $\mu^{ep}_{3111} = \mu^{ep}_{311(13)} = AL_{311} = 0$,
- $\mu^{ep}_{3112} = \mu^{ep}_{311(12)} = AL_{312} = 0{,}2$,
- $\mu^{ep}_{3113} = \mu^{ep}_{311(11)} = AL_{313} = 0{,}3$,
- $\mu^{ep}_{3114} = \mu^{ep}_{311(10)} = AL_{314} = 0{,}4$,
- $\mu^{ep}_{3115} = \mu^{ep}_{3119} = AL_{315} = 0{,}6$,
- $\mu^{ep}_{3116} = \mu^{ep}_{3118} = AL_{316} = 0{,}7$,
- $\mu^{ep}_{3117} = \mu^{ep}_{3117} = AL_{317} = 1$,
- $\mu^{ep}_{3111} = \mu^{e}_{3111} = 0$,
- $x^{ep}_{3111} = x^{e}_{3111} = 0{,}008$;

$$\underset{\sim}{T}^{ep}_{312} = \{\bigcup_{g=1}^{13} \mu^{ep}_{312g} / x^{ep}_{312g}\} =$$

$$\{\mu^{ep}_{3121} / x^{ep}_{3121},\ \mu^{ep}_{3122} / x^{ep}_{3122},\ \mu^{ep}_{3123} / x^{ep}_{3123},\ \mu^{ep}_{3124} / x^{ep}_{3124},\ \mu^{ep}_{3125} / x^{ep}_{3125},$$
$$\mu^{ep}_{3126} / x^{ep}_{3126},\ \mu^{ep}_{3127} / x^{ep}_{3127},\ \mu^{ep}_{3128} / x^{ep}_{3128},\ \mu^{ep}_{3129} / x^{ep}_{3129},\ \mu^{ep}_{312(10)} / x^{ep}_{312(10)},$$
$$\mu^{ep}_{312(11)} / x^{ep}_{312(11)},\ \mu^{ep}_{312(12)} / x^{ep}_{312(12)},\ \mu^{ep}_{312(13)} / x^{ep}_{312(13)}\},$$

де:

- $\mu^{ep}_{3121} = \mu^{ep}_{312(13)} = AL_{311} = 0$,
- $\mu^{ep}_{3122} = \mu^{ep}_{312(12)} = AL_{312} = 0{,}2$,
- $\mu^{ep}_{3123} = \mu^{ep}_{312(11)} = AL_{313} = 0{,}3$,

- $\mu^{ep}_{3124} = \mu^{ep}_{312(10)} = AL_{314} = 0{,}4,$
- $\mu^{ep}_{3125} = \mu^{ep}_{3129} = AL_{315} = 0{,}6,$
- $\mu^{ep}_{3126} = \mu^{ep}_{3128} = AL_{316} = 0{,}7,$
- $\mu^{ep}_{3127} = \mu^{ep}_{3127} = AL_{317} = 1,$
- $\mu^{ep}_{3121} = \mu^{e}_{3121} = 0,$
- $x^{ep}_{3121} = x^{e}_{3121} = 0{,}008;$

$$\underset{\sim}{T}^{ep}_{313} = \{ \bigcup_{g=1}^{13} \mu^{ep}_{313g} / x^{ep}_{313g} \} =$$

$$\{ \mu^{ep}_{3131} / x^{ep}_{3131},\ \mu^{ep}_{3132} / x^{ep}_{3132},\ \mu^{ep}_{3133} / x^{ep}_{3133},\ \mu^{ep}_{3134} / x^{ep}_{3134},\ \mu^{ep}_{3135} / x^{ep}_{3135},$$
$$\mu^{ep}_{3136} / x^{ep}_{3136},\ \mu^{ep}_{3137} / x^{ep}_{3137},\ \mu^{ep}_{3138} / x^{ep}_{3138},\ \mu^{ep}_{3139} / x^{ep}_{3139},\ \mu^{ep}_{313(10)} / x^{ep}_{313(10)},$$
$$\mu^{ep}_{313(11)} / x^{ep}_{313(11)},\ \mu^{ep}_{313(12)} / x^{ep}_{313(12)},\ \mu^{ep}_{313(13)} / x^{ep}_{313(13)} \},$$

де:

- $\mu^{ep}_{3131} = \mu^{ep}_{313(13)} = AL_{311} = 0,$
- $\mu^{ep}_{3132} = \mu^{ep}_{313(12)} = AL_{312} = 0{,}2,$
- $\mu^{ep}_{3133} = \mu^{ep}_{313(11)} = AL_{313} = 0{,}3,$
- $\mu^{ep}_{3134} = \mu^{ep}_{313(10)} = AL_{314} = 0{,}4,$
- $\mu^{ep}_{3135} = \mu^{ep}_{3139} = AL_{315} = 0{,}6,$
- $\mu^{ep}_{3136} = \mu^{ep}_{3138} = AL_{316} = 0{,}7,$
- $\mu^{ep}_{3137} = \mu^{ep}_{3137} = AL_{317} = 1,$
- $\mu^{ep}_{3131} = \mu^{e}_{3131} = 0,$
- $x^{ep}_{3131} = x^{e}_{3131} = 0{,}008;$

$$\underset{\sim}{T}^{ep}_{314} = \{ \bigcup_{g=1}^{13} \mu^{ep}_{314g} / x^{ep}_{314g} \} =$$

$$\{ \mu^{ep}_{3141} / x^{ep}_{3141},\ \mu^{ep}_{3142} / x^{ep}_{3142},\ \mu^{ep}_{3143} / x^{ep}_{3143},\ \mu^{ep}_{3144} / x^{ep}_{3144},\ \mu^{ep}_{3145} / x^{ep}_{3145},$$
$$\mu^{ep}_{3146} / x^{ep}_{3146},\ \mu^{ep}_{3147} / x^{ep}_{3147},\ \mu^{ep}_{3148} / x^{ep}_{3148},\ \mu^{ep}_{3149} / x^{ep}_{3149},\ \mu^{ep}_{314(10)} / x^{ep}_{314(10)},$$
$$\mu^{ep}_{314(11)} / x^{ep}_{314(11)},\ \mu^{ep}_{314(12)} / x^{ep}_{314(12)},\ \mu^{ep}_{314(13)} / x^{ep}_{314(13)} \},$$

де:

- $\mu^{ep}_{3141} = \mu^{ep}_{314(13)} = AL_{311} = 0,$
- $\mu^{ep}_{3142} = \mu^{ep}_{314(12)} = AL_{312} = 0,2,$
- $\mu^{ep}_{3143} = \mu^{ep}_{314(11)} = AL_{313} = 0,3,$
- $\mu^{ep}_{3144} = \mu^{ep}_{314(10)} = AL_{314} = 0,4,$
- $\mu^{ep}_{3145} = \mu^{ep}_{3149} = AL_{315} = 0,6,$
- $\mu^{ep}_{3146} = \mu^{ep}_{3148} = AL_{316} = 0,7,$
- $\mu^{ep}_{3147} = \mu^{ep}_{3147} = AL_{317} = 1,$
- $\mu^{ep}_{3141} = \mu^{e}_{3141} = 0,$
- $x^{ep}_{3141} = x^{e}_{3141} = 0,063;$

$$\underset{\sim}{T}^{ep}_{315} = \{ \bigcup_{g=1}^{13} \mu^{ep}_{315g} \,/\, x^{ep}_{315g} \} =$$

$$\{ \mu^{ep}_{3151} / x^{ep}_{3151},\ \mu^{ep}_{3152} / x^{ep}_{3152},\ \mu^{ep}_{3153} / x^{ep}_{3153},\ \mu^{ep}_{3154} / x^{ep}_{3154},\ \mu^{ep}_{3155} / x^{ep}_{3155},$$
$$\mu^{ep}_{3156} / x^{ep}_{3156},\ \mu^{ep}_{3157} / x^{ep}_{3157},\ \mu^{ep}_{3158} / x^{ep}_{3158},\ \mu^{ep}_{3159} / x^{ep}_{3159},\ \mu^{ep}_{315(10)} / x^{ep}_{315(10)},$$
$$\mu^{ep}_{315(11)} / x^{ep}_{315(11)},\ \mu^{ep}_{315(12)} / x^{ep}_{315(12)},\ \mu^{ep}_{315(13)} / x^{ep}_{315(13)} \},$$

де:

- $\mu^{ep}_{3151} = \mu^{ep}_{315(13)} = AL_{311} = 0,$
- $\mu^{ep}_{3152} = \mu^{ep}_{315(12)} = AL_{312} = 0,2,$
- $\mu^{ep}_{3153} = \mu^{ep}_{315(11)} = AL_{313} = 0,3,$
- $\mu^{ep}_{3154} = \mu^{ep}_{315(10)} = AL_{314} = 0,4,$
- $\mu^{ep}_{3155} = \mu^{ep}_{3159} = AL_{315} = 0,6,$
- $\mu^{ep}_{3156} = \mu^{ep}_{3158} = AL_{316} = 0,7,$
- $\mu^{ep}_{3157} = \mu^{ep}_{3157} = AL_{317} = 1,$
- $\mu^{ep}_{3151} = \mu^{e}_{3151} = 0,$
- $x^{ep}_{3151} = x^{e}_{3151} = 0,25.$

Формування номіналізованого НЧ поточного підсередовища ($\mathbf{P}_{\mathbf{i}}^{\tau_f} = \mathbf{P}_{\mathbf{3}}^{\tau_f}$) здійснюється аналогічним чином з урахуванням (3.12), тобто

$$\underset{\sim}{P}_{31}^{\tau_f p} = \{ \bigcup_{g=1}^{13} \mu_{31g}^{p} / x_{31g}^{p} \} =$$

$$\{ \mu_{311}^{p} / x_{311}^{p},\ \mu_{312}^{p} / x_{312}^{p},\ \mu_{313}^{p} / x_{313}^{p},\ \mu_{314}^{p} / x_{314}^{p},\ \mu_{315}^{p} / x_{315}^{p},$$
$$\mu_{316}^{p} / x_{316}^{p},\ \mu_{317}^{p} / x_{317}^{p},\ \mu_{318}^{p} / x_{318}^{p},\ \mu_{319}^{p} / x_{319}^{p},\ \mu_{31(10)}^{p} / x_{31(10)}^{p},$$
$$\mu_{31(11)}^{p} / x_{31(11)}^{p},\ \mu_{31(12)}^{p} / x_{31(12)}^{p},\ \mu_{31(13)}^{p} / x_{31(13)}^{p} \},$$

де:

- $\mu_{311}^{p} = \mu_{31(13)}^{p} = AL_{311} = 0,$
- $\mu_{312}^{p} = \mu_{31(12)}^{p} = AL_{312} = 0,2,$
- $\mu_{313}^{p} = \mu_{31(11)}^{p} = AL_{313} = 0,3,$
- $\mu_{314}^{p} = \mu_{31(10)}^{p} = AL_{314} = 0,4,$
- $\mu_{315}^{p} = \mu_{319}^{p} = AL_{315} = 0,6,$
- $\mu_{316}^{p} = \mu_{318}^{p} = AL_{316} = 0,7,$
- $\mu_{317}^{p} = \mu_{317}^{p} = AL_{317} = 1,$
- $\mu_{311}^{p} = \mu_{311} = 0,$
- $x_{311}^{p} = x_{311} = 0,095.$

Далі, при $i = 3,\ \ j = 6,\ \ \pi = 5,\ \ s = \overline{1,3},\ \ r = 3,\ \ z = 2 \cdot 5 - 1 = 9,$ $g = \overline{1,9},$ з урахуванням (3.11), сформуємо, перетворені $\underset{\sim}{T}_{321}^{ep},\ \underset{\sim}{T}_{322}^{ep},$ $\underset{\sim}{T}_{323}^{ep}$ та відповідне номіналізоване НЧ $\underset{\sim}{P}_{32}^{\tau_f p}$ еталонного та поточного підсередовища ($\mathbf{T_i^e = T_3^e}$ та $\mathbf{P_i^{\tau_f} = P_3^{\tau_f}}$), що відображають $P_{32} = P_{SPKIOA}$ в наступному вигляді:

$$\underset{\sim}{T}_{321}^{ep} = \{ \bigcup_{g=1}^{9} \mu_{321g}^{ep} / x_{321g}^{ep} \} =$$

$$\{ \mu_{3211}^{ep} / x_{3211}^{ep},\ \mu_{3212}^{ep} / x_{3212}^{ep},\ \mu_{3213}^{ep} / x_{3213}^{ep},\ \mu_{3214}^{ep} / x_{3214}^{ep},$$
$$\mu_{3215}^{ep} / x_{3215}^{ep},\ \mu_{3216}^{ep} / x_{3216}^{ep},\ \mu_{3217}^{ep} / x_{3217}^{ep},\ \mu_{3218}^{ep} / x_{3218}^{ep},\ \mu_{3219}^{ep} / x_{3219}^{ep} \},$$

де:

- $\mu_{3211}^{ep} = \mu_{3219}^{ep} = AL_{321} = 0,$
- $\mu_{3212}^{ep} = \mu_{3218}^{ep} = AL_{322} = 0,2,$

- $\mu^{ep}_{3213} = \mu^{ep}_{3217} = AL_{323} = 0{,}5,$
- $\mu^{ep}_{3214} = \mu^{ep}_{3216} = AL_{324} = 0{,}7,$
- $\mu^{ep}_{3215} = \mu^{ep}_{3215} = AL_{325} = 1,$
- $\mu^{ep}_{3211} = \mu^{e}_{3211} = 0,$
- $x^{ep}_{3211} = x^{e}_{3211} = 0{,}01;$

$$\underset{\sim}{T}^{ep}_{322} = \{ \bigcup_{g=1}^{9} \mu^{ep}_{322g} / x^{ep}_{322g} \} =$$

$$\{ \mu^{ep}_{3221} / x^{ep}_{3221},\ \mu^{ep}_{3222} / x^{ep}_{3222},\ \mu^{ep}_{3223} / x^{ep}_{3223},\ \mu^{ep}_{3224} / x^{ep}_{3224},$$
$$\mu^{ep}_{3225} / x^{ep}_{3225},\ \mu^{ep}_{3226} / x^{ep}_{3226},\ \mu^{ep}_{3227} / x^{ep}_{3227},\ \mu^{ep}_{3228} / x^{ep}_{3228},\ \mu^{ep}_{3229} / x^{ep}_{3229} \},$$

де:

- $\mu^{ep}_{3221} = \mu^{ep}_{3229} = AL_{321} = 0,$
- $\mu^{ep}_{3222} = \mu^{ep}_{3228} = AL_{322} = 0{,}2,$
- $\mu^{ep}_{3223} = \mu^{ep}_{3227} = AL_{323} = 0{,}5,$
- $\mu^{ep}_{3224} = \mu^{ep}_{3226} = AL_{324} = 0{,}7,$
- $\mu^{ep}_{3225} = \mu^{ep}_{3225} = AL_{325} = 1,$
- $\mu^{ep}_{3221} = \mu^{e}_{3221} = 0,$
- $x^{ep}_{3221} = x^{e}_{3221} = 0{,}01;$

$$\underset{\sim}{T}^{ep}_{323} = \{ \bigcup_{g=1}^{9} \mu^{ep}_{323g} / x^{ep}_{323g} \} =$$

$$\{ \mu^{ep}_{3231} / x^{ep}_{3231},\ \mu^{ep}_{3232} / x^{ep}_{3232},\ \mu^{ep}_{3233} / x^{ep}_{3233},\ \mu^{ep}_{3234} / x^{ep}_{3234},$$
$$\mu^{ep}_{3235} / x^{ep}_{3235},\ \mu^{ep}_{3236} / x^{ep}_{3236},\ \mu^{ep}_{3237} / x^{ep}_{3237},\ \mu^{ep}_{3238} / x^{ep}_{3238},\ \mu^{ep}_{3239} / x^{ep}_{3239} \},$$

де:

- $\mu^{ep}_{3231} = \mu^{ep}_{3239} = AL_{321} = 0,$
- $\mu^{ep}_{3232} = \mu^{ep}_{3238} = AL_{322} = 0{,}2,$
- $\mu^{ep}_{3233} = \mu^{ep}_{3237} = AL_{323} = 0{,}5,$
- $\mu^{ep}_{3234} = \mu^{ep}_{3236} = AL_{324} = 0{,}7,$
- $\mu^{ep}_{3235} = \mu^{ep}_{3235} = AL_{325} = 1,$
- $\mu^{ep}_{3231} = \mu^{e}_{3231} = 0,$

- $x^{ep}_{3231} = x^{e}_{3231} = 0{,}01.$

Далі, з урахуванням (3.12), сформуємо номіналізоване НЧ поточного підсередовища ($\mathbf{P}_{\mathbf{i}}^{\boldsymbol{\tau}_{\mathbf{f}}} = \mathbf{P}_{\mathbf{3}}^{\boldsymbol{\tau}_{\mathbf{f}}}$)

$$\underset{\sim}{P}^{\tau_f p}_{32} = \{\bigcup_{g=1}^{9} \mu^{p}_{32g} \,/\, x^{p}_{32g}\} =$$

$$\{\, \mu^{p}_{321} \,/\, x^{p}_{321},\ \mu^{p}_{322} \,/\, x^{p}_{322},\ \mu^{p}_{323} \,/\, x^{p}_{323},\ \mu^{p}_{324} \,/\, x^{p}_{324},$$

$$\mu^{p}_{325} \,/\, x^{p}_{325},\ \mu^{p}_{326} \,/\, x^{p}_{326},\ \mu^{p}_{327} \,/\, x^{p}_{327},\ \mu^{p}_{328} \,/\, x^{p}_{328},\ \mu^{p}_{329} \,/\, x^{p}_{329}\,\},$$

де:

- $\mu^{p}_{321} = \mu^{p}_{329} = AL_{321} = 0,$
- $\mu^{p}_{322} = \mu^{p}_{328} = AL_{322} = 0{,}2,$
- $\mu^{p}_{323} = \mu^{p}_{327} = AL_{323} = 0{,}5,$
- $\mu^{p}_{324} = \mu^{p}_{326} = AL_{324} = 0{,}7,$
- $\mu^{p}_{325} = \mu^{p}_{325} = AL_{325} = 1,$
- $\mu^{p}_{321} = \mu_{321} = 0,$
- $x^{p}_{321} = x_{321} = 0{,}082.$

Крок 2. Отримання номіналізованих НЧ $\underset{\sim}{T}^{ep}_{ijs} = \underset{\sim}{T}^{ep}_{31s}$ еталонного підсередовища ($\mathbf{T}_{\mathbf{i}}^{\mathbf{e}} = \mathbf{T}_{\mathbf{3}}^{\mathbf{e}}$) здійснюється на основі (3.13) за допомогою підмножини α-рівневих інтервалів $\mathbf{AL}_{\mathbf{ij}}^{\mathbf{Ie}} = \mathbf{AL}_{\mathbf{31}}^{\mathbf{Ie}}$, які складаються з $r = 5$ членів та відображають $\mathbf{T}_{\mathbf{ij}}^{\mathbf{e}} = \mathbf{T}_{\mathbf{31}}^{\mathbf{e}}$, тобто

$$\mathbf{AL}_{\mathbf{31}}^{\mathbf{Ie}} = \{\bigcup_{\mathbf{s=1}}^{5} \mathbf{AL}_{\mathbf{31s}}^{\mathbf{Ie}}\} =$$

$$\{\mathbf{AL}_{\mathbf{311}}^{\mathbf{Ie}},\ \mathbf{AL}_{\mathbf{312}}^{\mathbf{Ie}},\ \mathbf{AL}_{\mathbf{313}}^{\mathbf{Ie}},\ \mathbf{AL}_{\mathbf{314}}^{\mathbf{Ie}},\ \mathbf{AL}_{\mathbf{315}}^{\mathbf{Ie}}\},$$

$$s = \overline{1,5}.$$

На основі (3.15) при $r = 5$, для $\underset{\sim}{T}^{e}_{311}$, $\underset{\sim}{T}^{e}_{312}$, $\underset{\sim}{T}^{e}_{313}$, $\underset{\sim}{T}^{e}_{314}$ та $\underset{\sim}{T}^{e}_{315}$ відповідно визначаються $r_1 = 4$, $r_2 = 5$, $r_3 = 5$, $r_4 = 5$, $r_5 = 4$ (див. приклад етапу 5 в п. 2.2) і відповідно $b = \overline{1,3}$, $b = \overline{1,4}$, $b = \overline{1,4}$, $b = \overline{1,4}$ та $b = \overline{1,3}$. При цьому (3.13) набуває вигляду:

$$\mathbf{AL}^{\mathbf{Ie}}_{\mathbf{31}} = \{\bigcup_{\mathbf{s=1}}^{\mathbf{5}} \mathbf{AL}^{\mathbf{Ie}}_{\mathbf{31s}}\} =$$

$$\{\bigcup_{\mathbf{s=1}}^{\mathbf{5}} \{\bigcup_{\mathbf{b=1}}^{\mathbf{r_S-1}} \mathbf{AL}^{\mathbf{Ie}}_{\mathbf{311b}}\}\} =$$

$$\{\mathbf{AL}^{\mathbf{Ie}}_{\mathbf{3111}},\ \mathbf{AL}^{\mathbf{Ie}}_{\mathbf{3112}},\ \mathbf{AL}^{\mathbf{Ie}}_{\mathbf{3113}}\},$$

$$\{\mathbf{AL}^{\mathbf{Ie}}_{\mathbf{3121}},\ \mathbf{AL}^{\mathbf{Ie}}_{\mathbf{3122}},\ \mathbf{AL}^{\mathbf{Ie}}_{\mathbf{3123}},\ \mathbf{AL}^{\mathbf{Ie}}_{\mathbf{3124}}\},$$

$$\{\mathbf{AL}^{\mathbf{Ie}}_{\mathbf{3131}},\ \mathbf{AL}^{\mathbf{Ie}}_{\mathbf{3132}},\ \mathbf{AL}^{\mathbf{Ie}}_{\mathbf{3133}},\ \mathbf{AL}^{\mathbf{Ie}}_{\mathbf{3134}}\},$$

$$\{\mathbf{AL}^{\mathbf{Ie}}_{\mathbf{3141}},\ \mathbf{AL}^{\mathbf{Ie}}_{\mathbf{3142}},\ \mathbf{AL}^{\mathbf{Ie}}_{\mathbf{3143}},\ \mathbf{AL}^{\mathbf{Ie}}_{\mathbf{3144}}\},$$

$$\{\mathbf{AL}^{\mathbf{Ie}}_{\mathbf{3151}},\ \mathbf{AL}^{\mathbf{Ie}}_{\mathbf{3152}},\ \mathbf{AL}^{\mathbf{Ie}}_{\mathbf{3153}}\}.$$

На основі (3.16) якщо $r_1 = 4,$ а

$$\mu^{e}_{311max} = \bigvee_{q=1}^{r_1} \mu^{e}_{311q} = \mu^{e}_{3111} \vee \mu^{e}_{3112} \vee \mu^{e}_{3113} \vee \mu^{e}_{3114} =$$

$$0 \vee 1 \vee 0{,}3 \vee 0 =$$

$$\mu^{e}_{3112} = 1$$

та з урахуванням того, що:

- $r = 1,\ r_1 = 1,\ c = \overline{1,k_1},\ k_1 = 6$ та одночасного виконання умов $\mu^{e}_{3111} < AL^{Ie}_{3111c} \le \mu^{e}_{3112}$ $(0 < AL^{Ie}_{3111c} \le 1)$ та $x^{e}_{3112} \le x^{e}_{311max}$ $(0{,}008 \le 0{,}008)$ сформуємо

$$\mathbf{AL}^{\mathbf{Ie}}_{\mathbf{3111}} = \{\bigcup_{c=1}^{k_1} AL^{Ie}_{3111c}\} =$$

$$\{\, AL^{Ie}_{31111},\ AL^{Ie}_{31112},\ AL^{Ie}_{31113},\ AL^{Ie}_{31114},\ AL^{Ie}_{31115},\ AL^{Ie}_{31116}\} =$$

$$\{\, 0{,}2;\ 0{,}3;\ 0{,}4;\ 0{,}6;\ 0{,}7;\ 1\ \};$$

- $r = 1,\ \ r_2 = 2,\ \ c = \overline{1,k_2},\ \ k_2 = 4$ та $(\mu^{e}_{3112} > AL^{Ie}_{3112c} \ge \mu^{e}_{3113}) \wedge (x^{e}_{3133} \ge x^{e}_{313max})$ (тобто $(1 > AL^{Ie}_{3112c} \ge 0{,}3) \wedge (0{,}063 \ge 0{,}008)$) сформуємо

$$\mathbf{AL}^{\mathbf{Ie}}_{\mathbf{3112}} = \{\bigcup_{c=1}^{k_2} AL^{Ie}_{3112c}\} =$$

$$\{\, AL^{Ie}_{31121},\ AL^{Ie}_{31122},\ AL^{Ie}_{31123},\ AL^{Ie}_{31124}\} =$$

$$\{\, 0{,}7;\ 0{,}6;\ 0{,}4;\ 0{,}3\ \};$$

- $r=1,\ \ r_3=3,\ \ c=\overline{1,k_3},\ \ k_3=2$ та $(\mu^e_{3113} > AL^{Ie}_{3113c} \geq \mu^e_{3114}) \wedge (x^e_{3134} \geq x^e_{313max})$ $((0,3 > AL^{Ie}_{3113c} \geq 0) \wedge (0,25 \geq 0,008))$ визначимо

$$\mathbf{AL^{Ie}_{3113}} = \{\bigcup_{c=1}^{k_3} AL^{Ie}_{3113c}\} =$$
$$\{ AL^{Ie}_{31131},\ AL^{Ie}_{31132} \} =$$
$$\{\ 0,2;\ 0\ \}.$$

Далі, при $\mu^e_{332max} = \mu^e_{3323} = 1$ та з урахуванням того, що:

- $r=2,\ \ r_1=1,\ \ c=\overline{1,k_1},\ \ k_1=4$ і $(\mu^e_{3121} < AL^{Ie}_{3121c} \leq \mu^e_{3122}) \wedge (x^e_{3122} \leq x^e_{312max})$ $((0 < AL^{Ie}_{3121c} \leq 0,6) \wedge (0,008 \leq 0,063))$ сформуємо

$$\mathbf{AL^{Ie}_{3121}} = \{\bigcup_{c=1}^{k_1} AL^{Ie}_{3121c}\} =$$
$$\{ AL^{Ie}_{31211},\ AL^{Ie}_{31212},\ AL^{Ie}_{31213},\ AL^{Ie}_{31214} \} =$$
$$\{\ 0,2;\ 0,3;\ 0,4;\ 0,6\ \};$$

- $r=2,\ \ r_2=2,\ \ c=\overline{1,k_2},\ \ k_2=2$ та $(\mu^e_{3122} < AL^{Ie}_{3122c} \leq \mu^e_{3123}) \wedge (x^e_{3123} \leq x^e_{312max})$ $((0,6 < AL^{Ie}_{3122c} \leq 1) \wedge (0,063 \leq 0,063))$ визначимо

$$\mathbf{AL^{Ie}_{3122}} = \{\bigcup_{c=1}^{k_2} AL^{Ie}_{3122c}\} =$$
$$\{ AL^{Ie}_{31221},\ AL^{Ie}_{31222} \} =$$
$$\{\ 0,7;\ 1\ \};$$

- $r=2,\ \ r_3=3,\ \ c=\overline{1,k_3},\ \ k_3=5$ та $(\mu^e_{3123} > AL^{Ie}_{3123c} \geq \mu^e_{3124}) \wedge (x^e_{3124} \geq x^e_{313max})$ $((1 > AL^{Ie}_{3123c} \geq 0,2) \wedge (0,25 \geq 0,063))$ сформуємо

$$\mathbf{AL^{Ie}_{3123}} = \{\bigcup_{c=1}^{k_3} AL^{Ie}_{3123c}\} =$$
$$\{ AL^{Ie}_{31231},\ AL^{Ie}_{31232},\ AL^{Ie}_{31233},\ AL^{Ie}_{31234},\ AL^{Ie}_{31235} \} =$$
$$\{\ 0,7;\ 0,6;\ 0,4;\ 0,3;\ 0,2\ \};$$

- $r=2,\ \ r_4=4,\ \ c=\overline{1,k_4},\ \ k_4=1$ та $(\mu^e_{3124} > AL^{Ie}_{3124\,c} \geq \mu^e_{3125}) \wedge (x^e_{3125} \geq x^e_{313max})$ $((0{,}2 > AL^{Ie}_{3124\,c} \geq 1) \wedge (0{,}5 \geq 0{,}063))$ визначимо

$$\mathbf{AL^{Ie}_{3124}} = \{\bigcup_{c=1}^{k_4} AL^{Ie}_{3124\,c}\} =$$
$$\{AL^{Ie}_{31241}\} =$$
$$\{0\}.$$

Далі, сформуємо $\mathbf{AL^{Ie}_{3131}}$, $\mathbf{AL^{Ie}_{3132}}$, $\mathbf{AL^{Ie}_{3133}}$, $\mathbf{AL^{Ie}_{3134}}$ при $\mu^e_{313max} = \mu^e_{3133} = 1$ та з урахуванням того, що:

- $r=3,\ \ r_1=1,\ \ c=\overline{1,k_1},\ \ k_1=3,\ \ (\mu^e_{3131} < AL^{Ie}_{3131\,c} \leq \mu^e_{3132}) \wedge (x^e_{3132} \leq x^e_{313max})$ $(0 < AL^{Ie}_{3131\,c} \leq 0{,}4) \wedge (0{,}063 \leq 0{,}25)$, то

$$\mathbf{AL^{Ie}_{3131}} = \{\bigcup_{c=1}^{k_1} AL^{Ie}_{3131\,c}\} =$$
$$\{AL^{Ie}_{31311},\ AL^{Ie}_{31312},\ AL^{Ie}_{31313}\} =$$
$$\{\ 0{,}2;\ 0{,}3;\ 0{,}4\ \};$$

- $r=3,\ \ r_2=2,\ \ c=\overline{1,k_2},\ \ k_2=3,\ \ (\mu^e_{3132} < AL^{Ie}_{3132\,c} \leq \mu^e_{3133}) \wedge (x^e_{3133} \leq x^e_{313max})$ $((0{,}4 < AL^{Ie}_{3132\,c} \leq 1) \wedge (0{,}25 \leq 0{,}25))$, то

$$\mathbf{AL^{Ie}_{3132}} = \{\bigcup_{c=1}^{k_2} AL^{Ie}_{3132\,c}\} =$$
$$\{AL^{Ie}_{31321},\ AL^{Ie}_{31322},\ AL^{Ie}_{31323}\} =$$
$$\{\ 0{,}6;\ 0{,}7;\ 1\ \};$$

- $r=3,\ \ r_3=3,\ \ c=\overline{1,k_3},\ \ k_3=4,\ \ (\mu^e_{3133} > AL^{Ie}_{3133\,c} \geq \mu^e_{3134}) \wedge (x^e_{3134} \geq x^e_{313max})$ $((1 > AL^{Ie}_{3133\,c} \geq 0{,}3) \wedge (0{,}5 \geq 0{,}25))$, то

$$\mathbf{AL^{Ie}_{3133}} = \{\bigcup_{c=1}^{k_3} AL^{Ie}_{3133\,c}\} =$$
$$\{AL^{Ie}_{31331},\ AL^{Ie}_{31332},\ AL^{Ie}_{31333},\ AL^{Ie}_{31334}\} =$$
$$\{\ 0{,}7;\ 0{,}6;\ 0{,}4;\ 0{,}3\ \};$$

- $r=3,\ \ r_4=4,\ \ c=\overline{1,k_4},\ \ k_4=2,\ \ (\mu^e_{3134} > AL^{Ie}_{3134\,c} \geq \mu^e_{3135}) \wedge (x^e_{3135} \geq x^e_{313max})$ $((0{,}3 > AL^{Ie}_{3134\,c} \geq 1) \wedge (1 \geq 0{,}25))$, то

$$\mathbf{AL}^{\mathbf{Ie}}_{\mathbf{3134}} = \{\bigcup_{c=1}^{k_4} AL^{Ie}_{3134c}\} =$$

$$\{AL^{Ie}_{31341},\ AL^{Ie}_{31342}\}\} =$$

$$\{\ 0{,}2;\ 0\ \}\}.$$

Формування членів підмножин $\mathbf{AL}^{\mathbf{Ie}}_{\mathbf{3141}}$, $\mathbf{AL}^{\mathbf{Ie}}_{\mathbf{3142}}$, $\mathbf{AL}^{\mathbf{Ie}}_{\mathbf{3143}}$, $\mathbf{AL}^{\mathbf{Ie}}_{\mathbf{3144}}$ при $\mu^{e}_{314max} = \mu^{e}_{3143} = 1$ та з урахуванням того, що:

- $r = 4,\quad r_1 = 1,\quad c = \overline{1,k_1},\quad k_1 = 4,\quad (\mu^{e}_{3141} < AL^{Ie}_{3141c} \le \mu^{e}_{3142}) \wedge (x^{e}_{31342} \le x^{e}_{314max})\ ((0 < AL^{Ie}_{3141c} \le 0{,}6) \wedge (0{,}25 \le 0{,}5))$, то

$$\mathbf{AL}^{\mathbf{Ie}}_{\mathbf{3141}} = \{\bigcup_{c=1}^{k_1} AL^{Ie}_{3141c}\} =$$

$$\{AL^{Ie}_{31411},\ AL^{Ie}_{31412},\ AL^{Ie}_{31413},\ AL^{Ie}_{31414}\} =$$

$$\{\ 0{,}2;\ 0{,}3;\ 0{,}4;\ 0{,}6\ \};$$

- $r = 4,\quad r_2 = 2,\quad c = \overline{1,k_2},\quad k_2 = 2,\quad (\mu^{e}_{3142} < AL^{Ie}_{3142c} \le \mu^{e}_{3143}) \wedge (x^{e}_{3143} \le x^{e}_{314max})\ ((0{,}6 < AL^{Ie}_{3142c} \le 1) \wedge (0{,}5 \le 0{,}5))$, то

$$\mathbf{AL}^{\mathbf{Ie}}_{\mathbf{3142}} = \{\bigcup_{c=1}^{k_2} AL^{Ie}_{3142c}\} =$$

$$\{AL^{Ie}_{31421},\ AL^{Ie}_{31422}\} =$$

$$\{\ 0{,}7;\ 1\ \};$$

- $r = 4,\quad r_3 = 3,\quad c = \overline{1,k_3},\quad k_3 = 1,\quad (\mu^{e}_{3143} > AL^{Ie}_{3143c} \ge \mu^{e}_{3144}) \wedge (x^{e}_{3144} \ge x^{e}_{314max})\ ((1 > AL^{Ie}_{3143c} \ge 0{,}7) \wedge (1 \ge 0{,}5))$, то

$$\mathbf{AL}^{\mathbf{Ie}}_{\mathbf{3143}} = \{\bigcup_{c=1}^{k_3} AL^{Ie}_{3143c}\} =$$

$$\{AL^{Ie}_{31431}\} =$$

$$\{0{,}7\};$$

- $r = 4,\quad r_4 = 4,\quad c = \overline{1,k_4},\quad k_4 = 5,\quad (\mu^{e}_{3144} > AL^{Ie}_{3144c} \ge \mu^{e}_{3145}) \wedge (x^{e}_{3145} \ge x^{e}_{314max})\ ((0{,}7 > AL^{Ie}_{3144c} \ge 1) \wedge (1 \ge 0{,}5))$, то

$$\mathbf{AL}^{\mathbf{Ie}}_{\mathbf{3144}} = \{\bigcup_{c=1}^{k_4} AL^{Ie}_{3144c}\} =$$

$$\{ AL^{Ie}_{31451},\ AL^{Ie}_{31452},\ AL^{Ie}_{31453},\ AL^{Ie}_{31454},\ AL^{Ie}_{31455} \} =$$
$$\{ 0{,}6;\ 0{,}4;\ 0{,}3;\ 0{,}2;\ 0 \}.$$

І, нарешті, при $\mu^{e}_{315max} = \mu^{e}_{3153} = 1$ та з урахуванням того, що:

- $r = 5,\quad r_1 = 1,\quad c = \overline{1,k_1},\quad k_1 = 4,\quad (\mu^{e}_{3151} < AL^{Ie}_{3151c} \le \mu^{e}_{3152}) \wedge (x^{e}_{3152} \le x^{e}_{315max})$ $((0 < AL^{Ie}_{3151c} \le 0{,}6) \wedge (0{,}5 \le 1))$, то

$$\mathbf{AL^{Ie}_{3151}} = \{ \bigcup_{c=1}^{k_1} AL^{Ie}_{3151c} \} =$$
$$\{ AL^{Ie}_{31511},\ AL^{Ie}_{31512},\ AL^{Ie}_{31513},\ AL^{Ie}_{31514} \} =$$
$$\{ 0{,}2;\ 0{,}3;\ 0{,}4;\ 0{,}6 \};$$

- $r = 5,\quad r_2 = 2,\quad c = \overline{1,k_2},\quad k_2 = 2,\quad (\mu^{e}_{3152} < AL^{Ie}_{3152c} \le \mu^{e}_{3153}) \wedge (x^{e}_{3153} \le x^{e}_{315max})$ $((0{,}6 < AL^{Ie}_{3152c} \le 1) \wedge (1 \le 1))$, то

$$\mathbf{AL^{Ie}_{3152}} = \{ \bigcup_{c=1}^{k_2} AL^{Ie}_{3152c} \} =$$
$$\{ AL^{Ie}_{31521},\ AL^{Ie}_{31522} \} =$$
$$\{ 0{,}7;\ 1 \};$$

- $r = 5,\quad r_3 = 3,\quad c = \overline{1,k_3},\quad k_3 = 6,\quad (\mu^{e}_{3153} > AL^{Ie}_{3153c} \ge \mu^{e}_{3154}) \wedge (x^{e}_{3154} \ge x^{e}_{315max})$ $((1 > AL^{Ie}_{3153c} \ge 1) \wedge (1 \ge 1))$, то

$$\mathbf{AL^{Ie}_{3153}} = \{ \bigcup_{c=1}^{k_3} AL^{Ie}_{3153c} \} =$$
$$\{ AL^{Ie}_{31531},\ AL^{Ie}_{31532},\ AL^{Ie}_{31533},\ AL^{Ie}_{31534},\ AL^{Ie}_{31535},\ AL^{Ie}_{31536} \} =$$
$$\{ 0{,}7;\ 0{,}6;\ 0{,}4;\ 0{,}3;\ 0{,}2;\ 0 \}.$$

На основі визначених значень представимо (3.15) у наступному вигляді:

$$\mathbf{AL^{Ie}_{31}} = \{ \bigcup_{s=1}^{r} AL^{Ie}_{311} \} = \{ \bigcup_{s=1}^{r} \{ \bigcup_{b=1}^{r_s - 1} \{ \bigcup_{c=1}^{k_b} AL^{Ie}_{31sbc} \} \} \} =$$
$$\{\{\{ AL^{Ie}_{31111},\ AL^{Ie}_{31112},\ AL^{Ie}_{31113},\ AL^{Ie}_{31114},\ AL^{Ie}_{31115},\ AL^{Ie}_{31116} \},$$
$$\{ AL^{Ie}_{31121},\ AL^{Ie}_{31122},\ AL^{Ie}_{31123},\ AL^{Ie}_{31124} \},\ \{ AL^{Ie}_{31131},\ AL^{Ie}_{31132} \}\},$$
$$\{\{ AL^{Ie}_{31211},\ AL^{Ie}_{31212},\ AL^{Ie}_{31213},\ AL^{Ie}_{31214} \},\ \{ AL^{Ie}_{31221},\ AL^{Ie}_{31222} \},$$
$$\{ AL^{Ie}_{31231},\ AL^{Ie}_{31232},\ AL^{Ie}_{31233},\ AL^{Ie}_{31234},\ AL^{Ie}_{31235} \},\ \{ AL^{Ie}_{31241} \}\},$$

$$\{\{ AL^{Ie}_{31311},\ AL^{Ie}_{31312},\ AL^{Ie}_{31313} \},\ \{ AL^{Ie}_{31321},\ AL^{Ie}_{31322},\ AL^{Ie}_{31323} \},$$
$$\{ AL^{Ie}_{31331},\ AL^{Ie}_{31332},\ AL^{Ie}_{31333},\ AL^{Ie}_{31334} \},\ \{ AL^{Ie}_{31341},\ AL^{Ie}_{31342} \}\},$$
$$\{\{ AL^{Ie}_{31411},\ AL^{Ie}_{31412},\ AL^{Ie}_{31413},\ AL^{Ie}_{31414} \},\ \{ AL^{Ie}_{31421},\ AL^{Ie}_{31422} \},$$
$$\{ AL^{Ie}_{31431} \},\ \{ AL^{Ie}_{31451},\ AL^{Ie}_{31452},\ AL^{Ie}_{31453},\ AL^{Ie}_{31454},\ AL^{Ie}_{31455} \}\},$$
$$\{\{ AL^{Ie}_{31511},\ AL^{Ie}_{31512},\ AL^{Ie}_{31513},\ AL^{Ie}_{31514} \},\ \{ AL^{Ie}_{31521},\ AL^{Ie}_{31522} \},$$
$$\{ AL^{Ie}_{31531},\ AL^{Ie}_{31532},\ AL^{Ie}_{31533},\ AL^{Ie}_{31534},\ AL^{Ie}_{31535},\ AL^{Ie}_{31536} \}\}\} =$$
$$\{\{\{ 0,2;\ 0,3;\ 0,4;\ 0,6;\ 0,7;\ 1 \},\ \{ 0,7;\ 0,6;\ 0,4;\ 0,3 \},\ \{ 0,2;\ 0 \}\},$$
$$\{\{ 0,2;\ 0,3;\ 0,4;\ 0,6 \},\ \{ 0,7;\ 1 \},\ \{ 0,7;\ 0,6;\ 0,4;\ 0,3;\ 0,2 \},\ \{ 0 \}\},$$
$$\{\{ 0,2;\ 0,3;\ 0,4 \},\ \{ 0,6;\ 0,7;\ 1 \},\ \{ 0,7;\ 0,6;\ 0,4;\ 0,3 \},\ \{ 0,2;\ 0 \}\},$$
$$\{\{ 0,2;\ 0,3;\ 0,4;\ 0,6 \},\ \{ 0,7;\ 1 \},\ \{ 0,7 \},\ \{ 0,6;\ 0,4;\ 0,3;\ 0,2;\ 0 \}\},$$
$$\{\{ 0,2;\ 0,3;\ 0,4;\ 0,6 \},\ \{ 0,7;\ 1 \},\ \{ 0,7;\ 0,6;\ 0,4;\ 0,3;\ 0,2;\ 0 \}\}\}.$$

Далі, аналогічним чином, отримання номіналізованих НЧ еталонного підсередовища ($\mathbf{T^e_i = T^e_3}$) $\underset{\sim}{T}{}^{ep}_{ijs} = \underset{\sim}{T}{}^{ep}_{32s}$ здійснюється на основі (3.13) за допомогою підмножини α-рівневих інтервалів $\mathbf{AL^{Ie}_{ij} = AL^{Ie}_{32}}$, яка складається з $r = 3$ членів і відображає $\mathbf{T^e_{ij} = T^e_{32}}$, тобто

$$\mathbf{AL^{Ie}_{32}} = \{\bigcup_{s=1}^{3} \mathbf{AL^{Ie}_{32s}}\} = \{\mathbf{AL^{Ie}_{321},\ AL^{Ie}_{322},\ AL^{Ie}_{323}}\},\ s = \overline{1,3}.$$

З урахуванням (3.15) при $r = 3$ для $\underset{\sim}{T}{}^{e}_{321}$, $\underset{\sim}{T}{}^{e}_{322}$, $\underset{\sim}{T}{}^{e}_{323}$ відповідно визначаються $r_1 = 4$, $r_2 = 5$, $r_3 = 4$ (див. п. 2.2) та $b = \overline{1,3}$, $b = \overline{1,4}$, $b = \overline{1,3}$.

При цьому (3.13) приймає вигляд

$$\mathbf{AL^{Ie}_{32}} = \{\bigcup_{s=1}^{3} \mathbf{AL^{Ie}_{32s}}\} = \{\bigcup_{s=1}^{3} \{\bigcup_{b=1}^{r_s - 1} \mathbf{AL^{Ie}_{321b}}\}\} =$$
$$\mathbf{\{AL^{Ie}_{3211},\ AL^{Ie}_{3212},\ AL^{Ie}_{3213}\}},$$
$$\mathbf{\{AL^{Ie}_{3221},\ AL^{Ie}_{3222},\ AL^{Ie}_{3223},\ AL^{Ie}_{3224}\}},\ \mathbf{\{AL^{Ie}_{3231},\ AL^{Ie}_{3232},\ AL^{Ie}_{3233}\}}.$$

Аналогічно до попереднього прикладу, з урахуванням (3.16), за виразом (3.15) отримаємо

$$\mathbf{AL^{Ie}_{32}} = \{\bigcup_{s=1}^{r} AL^{Ie}_{321}\} = \{\bigcup_{s=1}^{r} \{\bigcup_{b=1}^{r_s - 1} \{\bigcup_{c=1}^{k_b} AL^{Ie}_{32sbc}\}\}\} =$$

$$\{\{\{ AL^{Ie}_{32111},\ AL^{Ie}_{32112},\ AL^{Ie}_{32113},\ AL^{Ie}_{32114} \},$$
$$\{ AL^{Ie}_{32121},\ AL^{Ie}_{32122},\ AL^{Ie}_{32123} \},\ \{ AL^{Ie}_{32131} \}\},$$
$$\{\{ AL^{Ie}_{32211},\ AL^{Ie}_{32212} \},\ \{ AL^{Ie}_{32221},\ AL^{Ie}_{32222} \},$$
$$\{ AL^{Ie}_{32231} \},\ \{ AL^{Ie}_{32241},\ AL^{Ie}_{32242},\ AL^{Ie}_{32243} \}\},$$
$$\{\{ AL^{Ie}_{32311},\ AL^{Ie}_{32312} \},\ \{ AL^{Ie}_{32321},\ AL^{Ie}_{32322} \},$$
$$\{ AL^{Ie}_{32331},\ AL^{Ie}_{32332},\ AL^{Ie}_{32333},\ AL^{Ie}_{32334} \}\}=$$
$$\{\{\{ 0{,}2;\ 0{,}5;\ 0{,}7;\ 1 \},\ \{ 0{,}7;\ 0{,}5;\ 0{,}2 \},\ \{ 1 \}\},$$
$$\{\{ 0{,}2;\ 0{,}5 \},\ \{ 0{,}7;\ 1 \},\ \{ 0{,}7 \},\ \{ 0{,}5;\ 0{,}2;\ 1 \}\},$$
$$\{\{ 0{,}2;\ 0{,}5 \},\ \{ 0{,}7;\ 1 \},\ \{ 0{,}7;\ 0{,}5;\ 0{,}2;\ 1 \}\}\}.$$

Крок 3. Формування номіналізованого НЧ $\underset{\sim}{P}{}^{\tau_f p}_{ij} = \underset{\sim}{P}{}^{\tau_f p}_{31}$ поточного підсередовища ($\mathbf{P}^{\boldsymbol{\tau_f}}_{\mathbf{i}} = \mathbf{P}^{\boldsymbol{\tau_f}}_{\mathbf{3}}$) здійснюється відповідно до (3.18) за допомогою α-рівневих інтервалів $\mathbf{AL}^{\mathbf{Ip}}_{\mathbf{31}}$ при $\rho = 5$,

$$\mu_{31max} = \bigvee_{q=1}^{\rho} \mu_{31q} = \mu_{311} \vee \mu_{312} \vee \mu_{313} \vee \mu_{314} \vee \mu_{315} =$$
$$0 \vee 0{,}4 \vee 1 \vee 0{,}2 \vee 0 =$$
$$\mu_{313} = 1$$

та з урахуванням того, що:

- $r_1 = 1,\ c = \overline{1,k_1},\ k_1 = 3$ і одночасного виконання умов $(\mu_{311} < AL^{Ip}_{311c} \le \mu_{312}) \wedge (x_{312} \le x_{31max})$ $((0 < AL^{Ip}_{311c} \le 0{,}4) \wedge (0{,}095 \le 0{,}28))$ визначимо

$$\mathbf{AL}^{\mathbf{Ip}}_{\mathbf{311}} = \{\bigcup_{c=1}^{k_1} AL^{Ip}_{311c}\} =$$
$$\{ AL^{Ip}_{3111},\ AL^{Ip}_{3112},\ AL^{Ip}_{3113} \} =$$
$$\{ 0{,}2;\ 0{,}3;\ 0{,}4 \};$$

- $r_2 = 2,\ c = \overline{1,k_2},\ k_2 = 3,\ (\mu_{312} < AL^{Ip}_{312c} \le \mu_{313}) \wedge (x_{313} \le x_{31max})$ $((0{,}4 < AL^{Ip}_{312c} \le 1) \wedge (0{,}28 \le 0{,}28))$, то

$$\mathbf{AL}^{\mathbf{Ip}}_{\mathbf{312}} = \{\bigcup_{c=1}^{k_2} AL^{Ip}_{312c}\} =$$
$$\{ AL^{Ip}_{3121},\ AL^{Ip}_{3122},\ AL^{Ip}_{3123} \} =$$

$$\{\ 0{,}6;\ 0{,}7;\ 1\ \};$$

- $r_3 = 3,\ \ c = \overline{1,k_3},\ \ k_3 = 5,\ \ (\mu_{313} > AL^{Ip}_{313c} \geq \mu_{314}) \wedge (x_{314} \geq x_{31max})$ $((1 > AL^{Ip}_{313c} \geq 0{,}2) \wedge (0{,}58 \geq 0{,}28))$, то

$$\mathbf{AL^{Ip}_{313}} = \{\bigcup_{c=1}^{k_3} AL^{Ip}_{313c}\} =$$

$$\{\ AL^{Ip}_{3131},\ AL^{Ip}_{3132},\ AL^{Ip}_{3133},\ AL^{Ip}_{3134},\ AL^{Ip}_{3135}\ \} =$$

$$\{\ 0{,}7;\ 0{,}6;\ 0{,}4;\ 0{,}3;\ 0{,}2\ \};$$

- $r_4 = 4,\ \ c = \overline{1,k_4},\ \ k_4 = 1,\ \ (\mu_{314} > AL^{Ip}_{314c} \geq \mu_{315}) \wedge (x_{315} \geq x_{31max})$ $((0{,}2 > AL^{Ip}_{314c} \geq 1) \wedge (0{,}58 \geq 0{,}28))$, то

$$\mathbf{AL^{Ip}_{314}} = \{\bigcup_{c=1}^{k_4} AL^{Ip}_{314c}\} =$$

$$\{\ AL^{Ip}_{3141}\ \} =$$

$$\{0\}.$$

З урахуванням обчислених значень, отримаємо наступний вигляд

$$\mathbf{AL^{Ip}_{31}} = \{\bigcup_{b=1}^{\rho-1}\{\bigcup_{c=1}^{k_b} AL^{Ip}_{31bc}\}\} =$$

$$\{\{\ AL^{Ip}_{3111},\ AL^{Ip}_{3112},\ AL^{Ip}_{3113}\ \},\ \{\ AL^{Ip}_{3121},\ AL^{Ip}_{3122},\ AL^{Ip}_{3123}\ \},$$

$$\{\ AL^{Ip}_{3131},\ AL^{Ip}_{3132},\ AL^{Ip}_{3133},\ AL^{Ip}_{3134},\ AL^{Ip}_{3135}\ \},\ \{\ AL^{Ip}_{3141}\ \}\} =$$

$$\{\{\ 0{,}2;\ 0{,}3;\ 0{,}4\ \},\ \{\ 0{,}6;\ 0{,}7;\ 1\ \},\ \{\ 0{,}7;\ 0{,}6;\ 0{,}4;\ 0{,}3;\ 0{,}2\ \},\ \{\ 0\ \}\}.$$

За аналогією з прикладом для $\underset{\sim}{P}^{\tau_f p}_{31}$, формування номіналізованого НЧ $\underset{\sim}{P}^{\tau_f p}_{ij} = \underset{\sim}{P}^{\tau_f p}_{32}$ поточного підсередовища ($\mathbf{P^{\tau_f}_i} = \mathbf{P^{\tau_f}_3}$) реалізується на основі (3.19), за допомогою α-рівневих інтервалів $\mathbf{AL^{Ip}_{32}}$, тобто

$$\mathbf{AL^{Ip}_{32}} = \{\bigcup_{b=1}^{\rho-1}\{\bigcup_{c=1}^{k_b} AL^{Ip}_{32bc}\}\} =$$

$$\{\{\ AL^{Ip}_{3211},\ AL^{Ip}_{3212}\ \},\ \{\ AL^{Ip}_{3221},\ AL^{Ip}_{3222}\ \},\ \{\ AL^{Ip}_{3231}\ \},$$

$$\{\ AL^{Ip}_{3241},\ AL^{Ip}_{3242},\ AL^{Ip}_{3243},\ AL^{Ip}_{3244}\ \}\} =$$

$$\{\{\ 0{,}2;\ 0{,}5\ \},\ \{\ 0{,}7;\ 1\ \},\ \{\ 0{,}7\ \},\ \{\ 0{,}5;\ 0{,}2;\ 1\ \}\}.$$

Крок 4. Обчислення значень x_{311g}^{ep} для перетворених НЧ $\underset{\sim}{T}_{311}^{ep} = \underset{\sim}{OM}_{31}^{ep}$, $\underset{\sim}{T}_{312}^{ep} = \underset{\sim}{M}_{31}^{ep}$, $\underset{\sim}{T}_{313}^{ep} = \underset{\sim}{C}_{31}^{ep}$, $\underset{\sim}{T}_{314}^{ep} = \underset{\sim}{Б}_{31}^{ep}$ та $\underset{\sim}{T}_{315}^{ep} = \underset{\sim}{OБ}_{31}^{ep}$ еталонного підсередовища ($\mathbf{T_i^e = T_3^e}$) з урахуванням (3.20) при $z = 13$, $g = \overline{2,13}$ здійснюється на основі компонентів $\mu_{ijsg}^{e} / x_{ijsg}^{e}$ (див. приклад для (2.37)), тобто $\mu_{2111}^{e} = \mu_{3111}^{e} = 0$, $\mu_{2112}^{e} = \mu_{3112}^{e} = 1$, $x_{2111}^{e} = x_{3111}^{e} = 0{,}008$, $x_{2112}^{e} = x_{3112}^{e} = 0{,}008$.

Далі, з урахуванням цих значень для $\mu_{3112}^{ep} = AL_{3112}^{Ie} = 0{,}2$ обчислимо

$$x_{3112}^{ep} = x_{3111}^{e} + \frac{(\mu_{3112}^{ep} - \mu_{3111}^{e})(x_{3112}^{e} - x_{3111}^{e})}{\mu_{3112}^{e} - \mu_{3111}^{e}} =$$

$$0{,}008 + ((0{,}2 - 0) \cdot (0{,}008 - 0{,}008)) / (1 - 0) =$$

$$0{,}008.$$

Аналогічним чином для $\mu_{3113}^{ep} = AL_{3113}^{Ie} = 0{,}3$, $\mu_{3114}^{ep} = AL_{3114}^{Ie} = 0{,}4$, $\mu_{3115}^{ep} = AL_{3115}^{Ie} = 0{,}6$, $\mu_{3116}^{ep} = AL_{3116}^{Ie} = 0{,}7$, $\mu_{3117}^{ep} = AL_{3117}^{Ie} = 1$ визначимо, що

$$x_{3113}^{ep} = x_{3114}^{ep} = x_{3115}^{ep} = x_{3116}^{ep} = x_{3117}^{ep} =$$

$$0{,}008.$$

Далі, при $\mu_{2112}^{e} = \mu_{3112}^{e} = 1$, $\mu_{2113}^{e} = \mu_{3113}^{e} = 0{,}3$, $x_{2112}^{e} = x_{3112}^{e} = 0{,}008$, $x_{2113}^{e} = x_{3113}^{e} = 0{,}063$:

- для $\mu_{3118}^{ep} = AL_{3118}^{Ie} = 0{,}7$ обчислимо

  $$x_{3118}^{ep} = 0{,}008 + ((0{,}7 - 1) \cdot (0{,}063 - 0{,}008)) / (0{,}3 - 1) =$$

  $$0{,}032;$$

- для $\mu_{3119}^{ep} = AL_{3119}^{Ie} = 0{,}6$ визначимо

  $$x_{3119}^{ep} = 0{,}008 + ((0{,}6 - 1) \cdot (0{,}063 - 0{,}008)) / (0{,}3 - 1) =$$

  $$0{,}039;$$

- для $\mu_{311(10)}^{ep} = AL_{311(10)}^{Ie} = 0{,}4$ обчислимо

  $$x_{311(10)}^{ep} = 0{,}008 + ((0{,}4 - 1) \cdot (0{,}063 - 0{,}008)) / (0{,}3 - 1) =$$

  $$0{,}055;$$

- для $\mu_{311(11)}^{ep} = AL_{311(11)}^{Ie} = 0{,}3$ визначимо

$$x^{ep}_{311(11)} = 0{,}008 + ((0{,}3-1)\cdot(0{,}063-0{,}008))/(0{,}3-1) = 0{,}063.$$

Далі, при $\mu^{e}_{2113} = \mu^{e}_{3113} = 0{,}3$, $\mu^{e}_{2114} = \mu^{e}_{3114} = 0$, $x^{e}_{2113} = x^{e}_{3113} = 0{,}063$, $x^{e}_{2114} = x^{e}_{3114} = 0{,}25$:

- для $\mu^{ep}_{311(12)} = AL^{Ie}_{311(12)} = 0{,}2$ обчислимо

$$x^{ep}_{311(12)} = 0{,}063 + ((0{,}2-0{,}3)\cdot(0{,}25-0{,}063))/(0-0{,}3) = 0{,}125;$$

- для $\mu^{ep}_{311(13)} = AL^{Ie}_{311(13)} = 0$ визначимо

$$x^{ep}_{311(13)} = 0{,}063 + ((0-0{,}3)\cdot(0{,}25-0{,}063))/(0-0{,}3) = 0,$$

а $\mu^{ep}_{3111} = \mu^{e}_{3111} = 0$, $x^{ep}_{3111} = x^{e}_{3111} = 0{,}008$.

Відповідно до (3.11) сформуємо номіналізоване НЧ еталонного підсередовища ($\mathbf{T^{e}_{i} = T^{e}_{3}}$)

$$\underset{\sim}{T}^{ep}_{311} = \underset{\sim}{OM}^{ep}_{31} =$$
$$\{0/0{,}008;\ 0{,}2/0{,}008;\ 0{,}3/0{,}008;\ 0{,}4/0{,}008;$$
$$0{,}6/0{,}008;\ 0{,}7/0{,}008;\ 1/0{,}008;\ 0{,}7/0{,}032;\ 0{,}6/0{,}039;$$
$$0{,}4/0{,}055;\ 0{,}3/0{,}063;\ 0{,}2/0{,}125;\ 0/0{,}25\}.$$

Аналогічним чином отримаємо перетворені НЧ $\underset{\sim}{T}^{ep}_{312}$, $\underset{\sim}{T}^{ep}_{313}$, $\underset{\sim}{T}^{ep}_{314}$ та $\underset{\sim}{T}^{ep}_{315}$ еталонного підсередовища ($\mathbf{T^{e}_{i} = T^{e}_{3}}$) тобто:

$$\underset{\sim}{T}^{ep}_{312} = \underset{\sim}{M}^{ep}_{31} =$$
$$\{0/0{,}008;\ 0{,}2/0{,}008;\ 0{,}3/0{,}008;\ 0{,}4/0{,}008;$$
$$0{,}6/0{,}008;\ 0{,}7/0{,}022;\ 1/0{,}063;\ 0{,}7/0{,}133;\ 0{,}6/0{,}157;$$
$$0{,}4/0{,}203;\ 0{,}3/0{,}227;\ 0{,}2/0{,}25;\ 0/0{,}5\};$$

$$\underset{\sim}{T}^{ep}_{313} = \underset{\sim}{C}^{ep}_{31} =$$
$$\{0/0{,}008;\ 0{,}2/0{,}036;\ 0{,}3/0{,}049;\ 0{,}4/0{,}063;$$
$$0{,}6/0{,}125;\ 0{,}7/0{,}157;\ 1/0{,}25;\ 0{,}7/0{,}357;\ 0{,}6/0{,}393;$$
$$0{,}4/0{,}464;\ 0{,}3/0{,}5;\ 0{,}2/0{,}667;\ 0/1\};$$

$$\underset{\sim}{T}^{ep}_{314} = \underset{\sim}{B}^{ep}_{31} =$$
$$\{0/0{,}063;\ 0{,}2/0{,}125;\ 0{,}3/0{,}157;\ 0{,}4/0{,}188;$$

$$0,6/0,25;\ 0,7/0,313;\ 1/0,5;\ 0,7/1;\ 0,6/1;$$
$$0,4/1;\ 0,3/1;\ 0,2/1;\ 0/1\};$$

$$\underset{\sim}{T}^{ep}_{315} = \underset{\sim}{ОБ}^{ep}_{31} =$$
$$\{0/0,25;\ 0,2/0,333;\ 0,3/0,375;\ 0,4/0,417;$$
$$0,6/0,5;\ 0,7/0,625;\ 1/1;\ 0,7/1;\ 0,6/1;$$
$$0,4/1;\ 0,3/1;\ 0,2/1;\ 0/1\}.$$

Обчислення значень x^{ep}_{321g} для номіналізованих НЧ $\underset{\sim}{T}^{ep}_{321} = \underset{\sim}{M}^{ep}_{32}$, $\underset{\sim}{T}^{ep}_{322} = \underset{\sim}{C}^{ep}_{32}$ та $\underset{\sim}{T}^{ep}_{323} = \underset{\sim}{Б}^{ep}_{32}$ еталонного підсередовища ($\mathbf{T}^{e}_{i} = \mathbf{T}^{e}_{3}$) з урахуванням (3.20) при $z = 9$, $g = \overline{2,9}$ здійснюється на основі компонентів $\mu^{e}_{ijsg} / x^{e}_{ijsg}$ (див. п. 2.2), тобто $\mu^{e}_{3211} = 0$, $\mu^{e}_{3212} = 1$, $x^{e}_{3211} = 0,01$, $x^{e}_{3212} = 0,01$.

Далі, з урахуванням цих значень для $\mu^{ep}_{3212} = AL^{Ie}_{3212} = 0,2$ обчислимо

$$x^{ep}_{3212} = x^{e}_{3211} + ((\mu^{ep}_{3212} - \mu^{e}_{3211}) \cdot (x^{e}_{3212} - x^{e}_{3211})) / (\mu^{e}_{3212} - \mu^{e}_{3211}) =$$
$$0,01 + ((0,2 - 0) \cdot (0,01 - 0,01)) / (1 - 0) =$$
$$0,01.$$

Аналогічним чином для $\mu^{ep}_{3213} = AL^{Ie}_{3213} = 0,5$, $\mu^{ep}_{3214} = AL^{Ie}_{3214} = 0,7$, $\mu^{ep}_{3215} = AL^{Ie}_{3215} = 1$ визначимо, що

$$x^{ep}_{3213} = x^{ep}_{3214} = x^{ep}_{3215} =$$
$$0,01.$$

Далі, при $\mu^{e}_{3212} = 1$, $\mu^{e}_{3213} = 0,2$, $x^{e}_{3212} = 0,01$, $x^{e}_{3213} = 0,1$:

- для $\mu^{ep}_{3216} = AL^{Ie}_{3216} = 0,7$ обчислимо

$$x^{ep}_{3216} = x^{e}_{3212} + ((\mu^{ep}_{3216} - \mu^{e}_{3212}) \cdot (x^{e}_{3213} - x^{e}_{3212})) / (\mu^{e}_{3213} - \mu^{e}_{3212}) =$$
$$0,01 + ((0,7 - 1) \cdot (0,1 - 0,01)) / (0,2 - 1) =$$
$$0,044;$$

- для $\mu^{ep}_{3217} = AL^{Ie}_{3217} = 0,5$ визначимо

$$x^{ep}_{3217} = x^{e}_{3212} + ((\mu^{ep}_{3217} - \mu^{e}_{3212}) \cdot (x^{e}_{3213} - x^{e}_{3212})) / (\mu^{e}_{3213} - \mu^{e}_{3212}) =$$
$$0,01 + ((0,5 - 1) \cdot (0,1 - 0,01)) / (0,2 - 1) =$$
$$0,066;$$

- для $\mu^{ep}_{3218} = AL^{Ie}_{3218} = 0,2$ обчислимо

$$x^{ep}_{3218} = x^{e}_{3212} + ((\mu^{ep}_{3218} - \mu^{e}_{3212}) \cdot (x^{e}_{3213} - x^{e}_{3212})) / (\mu^{e}_{3213} - \mu^{e}_{3212}) =$$

$$0,01+((0,2-1)\cdot(0,1-0,01))/(0,2-1)=$$
$$0,1;$$

- для $\mu^{ep}_{3219}=AL^{Ie}_{3219}=0$ визначимо

$$x^{ep}_{3219}=x^{e}_{3212}+((\mu^{ep}_{3219}-\mu^{e}_{3212})\cdot(x^{e}_{3213}-x^{e}_{3212}))/(\mu^{e}_{3213}-\mu^{e}_{3212})=$$
$$0,01+((0-1)\cdot(0,1-0,01))/(0,2-1)=$$
$$1,$$

а $\mu^{ep}_{3211}=\mu^{e}_{3211}=0,\ x^{ep}_{3211}=x^{e}_{3211}=0,01.$

Відповідно до (3.11) сформуємо перетворене НЧ еталонного підсередовища ($\mathbf{T^e_i=T^e_3}$)

$$\underset{\sim}{T}^{ep}_{321}=\underset{\sim}{M}^{ep}_{32}=\{0/0,01;\ 0,2/0,01;\ 0,5/0,01;\ 0,7/0,01;\ 1/0,1;$$
$$0,7/0,044;\ 0,5/0,066;\ 0,2/0,1;\ 0/1\}.$$

Аналогічним чином отримаємо номіналізовані НЧ еталонного підсередовища ($\mathbf{T^e_i=T^e_3}$) для $\underset{\sim}{T}^{ep}_{322}$ та $\underset{\sim}{T}^{ep}_{323}$, тобто:

$$\underset{\sim}{T}^{ep}_{322}=\underset{\sim}{C}^{ep}_{32}=\{0/0,01;\ 0,2/0,01;\ 0,5/0,01;\ 0,7/0,046;$$
$$1/0,1;\ 0,7/1;\ 0,5/1;\ 0,2/1;\ 0/1\};$$
$$\underset{\sim}{T}^{ep}_{323}=\underset{\sim}{Б}^{ep}_{32}=\{0/0,01;\ 0,2/0,046;\ 0,5/0,1;\ 0,7/0,46;$$
$$1/1;\ 0,7/1;\ 0,5/1;\ 0,2/1;\ 0/1\}.$$

Крок 5. Обчислення значень x^{p}_{31g} для перетворених НЧ $\underset{\sim}{P}^{\tau_f p}_{31}=\underset{\sim}{P}^{\tau_f p}_{SPKOП}$ поточного підсередовища ($\mathbf{P^{\tau_f}_i=P^{\tau_f}_3}$) здійснюється аналогічно до кроку 4 з урахуванням (3.22) при $z=13,\ g=\overline{2,13}$ здійснюється на основі компонентів $\mu_{ijg}\ /\ x_{ijg}$ (див. приклад етапу 3 в п. 3.1), тобто $\mu_{311}=0,\ \mu_{312}=0,4,\ x_{311}=0,095$ та $x_{312}=0,095.$

Далі, з урахуванням цього:

- для $\mu^{p}_{312}=AL^{Ip}_{312}=0,2$ обчислимо

$$x^{p}_{312}=0,095+((0,2-0)\cdot(0,095-0,095))/(0,4-0)=$$
$$0,095;$$

- для $\mu^{p}_{313}=AL^{Ip}_{313}=0,3$ визначимо

$$x^{p}_{313}=0,095+((0,3-0)\cdot(0,095-0,095))/(0,4-0)=$$
$$0,095;$$

- для $\mu_{314}^{p} = AL_{314}^{Ip} = 0,4$ обчислимо

$$x_{314}^{p} = 0,095 + ((0,4-0)\cdot(0,095-0,095))/(0,4-0) = 0,095.$$

Наступним, при $\mu_{312} = 0,4$, $\mu_{313} = 1$, $x_{312} = 0,095$ та $x_{313} = 0,28$:

- для $\mu_{315}^{p} = AL_{315}^{Ip} = 0,6$ визначимо

$$x_{315}^{p} = 0,095 + ((0,6-0,4)\cdot(0,28-0,095))/(1-0,4) = 0,157;$$

- для $\mu_{316}^{p} = AL_{316}^{Ip} = 0,7$ визначимо

$$x_{316}^{p} = 0,095 + ((0,7-0,4)\cdot(0,28-0,095))/(1-0,4) = 0,188;$$

- для $\mu_{317}^{p} = AL_{317}^{Ip} = 1$ визначимо

$$x_{317}^{p} = 0,095 + ((1-0,4)\cdot(0,28-0,095))/(1-0,4) = 0,28.$$

Далі, при $\mu_{313} = 1$, $\mu_{314} = 0,2$, $x_{313} = 0,28$ та $x_{314} = 0,58$:

- для $\mu_{318}^{p} = AL_{318}^{Ip} = 0,7$ обчислимо

$$x_{318}^{p} = 0,095 + ((0,7-1)\cdot(0,58-0,28))/(0,2-1) = 0,393;$$

- для $\mu_{319}^{p} = AL_{319}^{Ip} = 0,6$ визначимо

$$x_{319}^{p} = 0,095 + ((0,6-1)\cdot(0,58-0,28))/(0,2-1) = 0,43;$$

- для $\mu_{31(10)}^{p} = AL_{31(10)}^{Ip} = 0,4$ обчислимо

$$x_{31(10)}^{p} = 0,095 + ((0,4-1)\cdot(0,58-0,28))/(0,2-1) = 0,505;$$

- для $\mu_{31(11)}^{p} = AL_{31(11)}^{Ip} = 0,3$ визначимо

$$x_{31(11)}^{p} = 0,095 + ((0,3-1)\cdot(0,58-0,28))/(0,2-1) = 0,543;$$

- для $\mu_{31(12)}^{p} = AL_{31(12)}^{Ip} = 0,2$ обчислимо

$$x_{31(12)}^{p} = 0,095 + ((0,2-1)\cdot(0,58-0,28))/(0,2-1) = 0,58.$$

Наступним, при $\mu_{314}=0{,}2$, $\mu_{315}=0$, $x_{314}=0{,}58$ та $x_{315}=0{,}58$:

- для $\mu^{ep}_{31(13)}=AL^{Ip}_{31(13)}=0$ визначимо

$$x^{ep}_{31(13)}=0{,}58+((0-0{,}2)\cdot(0{,}58-0{,}58))/(0-0{,}2)=0{,}58,$$

а $\mu^{p}_{311}=\mu_{311}=0$, $x^{p}_{311}=x_{311}=0{,}095$.

Таким чином, номіналізоване НЧ поточного підсередовища ($\mathbf{P}^{\tau_f}_{\mathbf{i}}=\mathbf{P}^{\tau_f}_{\mathbf{3}}$) відповідно до (3.12) прийме наступний вигляд

$$\underset{\sim}{P}^{\tau_f p}_{31}=\underset{\sim}{P}^{\tau_f p}_{SPKOП}=\{0/0{,}095;\ 0{,}2/0{,}095;\ 0{,}3/0{,}095;\ 0{,}4/0{,}095;\ 0{,}6/0{,}157;\ 0{,}7/0{,}188;\ 1/0{,}28;\ 0{,}7/0{,}393;\ 0{,}6/0{,}43;\ 0{,}4/0{,}505;\ 0{,}3/0{,}543;\ 0{,}2/0{,}58;\ 0/0{,}58\}.$$

Обчислення значень x^{p}_{36g} для перетворених НЧ $\underset{\sim}{P}^{\tau_f p}_{32}=\underset{\sim}{P}^{\tau_f p}_{SPKПОА}$ поточного підсередовища ($\mathbf{P}^{\tau_f}_{\mathbf{i}}=\mathbf{P}^{\tau_f}_{\mathbf{3}}=\mathbf{P}^{\tau_f}_{\mathbf{SP}}$) здійснюється аналогічно, з урахуванням (3.22) при $z=9$ за допомогою компонентів $\mu_{ijg}\ /\ x_{ijg}$ (див. приклад етапу 3 в п. 3.1), тобто при $\mu_{321}=0$, $\mu_{322}=0{,}5$, $x_{321}=0{,}082$ та $x_{322}=0{,}082$.

Далі, з урахуванням цих значень

- для $\mu^{p}_{322}=AL^{Ip}_{322}=0{,}2$ обчислимо $x^{p}_{322}=0{,}082$;
- для $\mu^{p}_{323}=AL^{Ip}_{323}=0{,}5$ визначимо $x^{p}_{323}=0{,}082$.

При $\mu_{322}=0{,}5$, $\mu_{323}=1$, $x_{322}=0{,}082$ та $x_{323}=0{,}82$:

- для $\mu^{p}_{324}=AL^{Ip}_{324}=0{,}7$ обчислимо $x^{p}_{324}=0{,}377$;
- для $\mu^{p}_{325}=AL^{Ip}_{325}=1$ визначимо $x^{p}_{325}=0{,}82$.

Далі, при $\mu_{323}=1$, $\mu_{324}=0{,}7$, $x_{323}=0{,}82$ та $x_{324}=1$:

- для $\mu^{p}_{326}=AL^{Ip}_{326}=0{,}7$ обчислимо $x^{p}_{326}=1$.

І, нарешті, при $\mu_{324}=0{,}7$, $\mu_{325}=0$, $x_{324}=1$ та $x_{325}=1$:

- для $\mu^{p}_{327}=AL^{Ip}_{327}=0{,}5$, $\mu^{p}_{328}=AL^{Ip}_{328}=0{,}2$, $\mu^{p}_{329}=AL^{Ip}_{329}=0$ відповідно обчислимо

$x^{p}_{327}=x^{p}_{328}=x^{p}_{329}=1$, а $\mu^{p}_{321}=\mu_{321}=0$, $x^{p}_{321}=x_{321}=0{,}082$.

Таким чином, номіналізоване НЧ поточного підсередовища ($\mathbf{P}^{\tau_f}_{\mathbf{i}}=\mathbf{P}^{\tau_f}_{\mathbf{3}}=\mathbf{P}^{\tau_f}_{\mathbf{SP}}$) відповідно до (3.12) має наступний вигляд

$$\underset{\sim}{P}_{32}^{\tau_f p} = \underset{\sim}{P}_{SPKTIOA}^{\tau_f p} = \{0/0{,}082;\ 0{,}2/0{,}082;\ 0{,}5/0{,}082;\ 0{,}7/0{,}377;\ 1/0{,}82;\ 0{,}7/1;\ 0{,}5/1;\ 0{,}2/1;\ 0/1\}.$$

Формування узагальнювальних таблиць та графічна інтерпретація номіналізованих нечітких чисел еталонного та поточного підсередовища

Етап 3 – формування узагальнювальних таблиць та графічна інтерпретація номіналізованих НЧ еталонного та поточного підсередовища ($\mathbf{T}_i^e$ та $\mathbf{P}_i^{\tau_f}$). Для отримання таких таблиць всі номіналізовані $\underset{\sim}{T}_{ijs}^{ep}$ і $\underset{\sim}{P}_{ij}^{\tau_f p}$ НЧ еталонного та поточного підсередовища ($\mathbf{T}_i^e$ і $\mathbf{P}_i^{\tau_f}$) зводяться до узагальнювальних таблиць (див. табл. 3.7 та 3.8).

Таблиця 3.7

Узагальнювальна таблиця для $\underset{\sim}{T}_{ijs}^{ep}\ (s=\overline{1,r})$

$\underset{\sim}{T}_{ijs}^{ep}$	$\mu_{ijsg}^{ep}\ (g=\overline{1,z})$							
	μ_{ijs1}^{ep}	μ_{ijs2}^{ep}	…	μ_{ijsg-1}^{ep}	μ_{ijsg}^{ep}	μ_{ijsg+1}^{ep}	…	μ_{ijsz}^{ep}
	AL_{ij1}	AL_{ij2}	…	$AL_{ij\pi-1}$	$AL_{ij\pi}$	$AL_{ij\pi-1}$	…	AL_{ij1}
$\underset{\sim}{T}_{ij1}^{ep}$	x_{ij11}^{ep}	x_{ij12}^{ep}	…	x_{ij1g-1}^{ep}	x_{ij1g}^{ep}	x_{ij1g+1}^{ep}	…	x_{ij1z}^{ep}
$\underset{\sim}{T}_{ij2}^{ep}$	x_{ij21}^{ep}	x_{ij22}^{ep}	…	x_{ij2g-1}^{ep}	x_{ij2g}^{ep}	x_{ij2g+1}^{ep}	…	x_{ij2z}^{ep}
…	…	…	…	…	…	…	…	…
$\underset{\sim}{T}_{ijs}^{ep}$	x_{ijs1}^{ep}	x_{ijs2}^{ep}	…	x_{ijsg-1}^{ep}	x_{ijsg}^{ep}	x_{ijsg+1}^{ep}	…	x_{ijsz}^{ep}
…	…	…	…	…	…	…	…	…
$\underset{\sim}{T}_{ijr}^{ep}$	x_{ijr1}^{ep}	x_{ijr2}^{ep}	…	x_{ijrg-1}^{ep}	x_{ijrg}^{ep}	x_{ijrg+1}^{ep}	…	x_{ijrz}^{ep}

Таблиця 3.8

Узагальнювальна таблиця для $\underset{\sim}{P}_{ij}^{\tau_f p}$

$\underset{\sim}{P}_{ij}^{\tau_f p}$	$\mu_{ijg}^{p}\ (g=\overline{1,z})$							
	μ_{ij1}^{p}	μ_{ij2}^{p}	…	μ_{ijg-1}^{p}	μ_{ijg}^{p}	μ_{ijg+1}^{p}	…	μ_{ijz}^{p}
	AL_{ij1}	AL_{ij2}	…	$AL_{ij\pi-1}$	$AL_{ij\pi}$	$AL_{ij\pi-1}$	…	AL_{ij1}
$\underset{\sim}{P}_{ij}^{\tau_f p}$	x_{ij1}^{p}	x_{ij2}^{p}	…	x_{ijg-1}^{p}	x_{ijg}^{p}	x_{ijg+1}^{p}	…	$x_{ij\,z}^{p}$

Наприклад, для наочності відповідно до табл. 3.7 всі перетворені НЧ $\underset{\sim}{T}^{ep}_{311} = \underset{\sim}{OM}^{ep}_{31}$, $\underset{\sim}{T}^{ep}_{312} = \underset{\sim}{M}^{ep}_{31}$, $\underset{\sim}{T}^{ep}_{313} = \underset{\sim}{C}^{ep}_{31}$, $\underset{\sim}{T}^{ep}_{314} = \underset{\sim}{B}^{ep}_{31}$, $\underset{\sim}{T}^{ep}_{315} = \underset{\sim}{OB}^{ep}_{31}$ та $\underset{\sim}{T}^{ep}_{321} = \underset{\sim}{M}^{ep}_{32}$, $\underset{\sim}{T}^{ep}_{322} = \underset{\sim}{C}^{ep}_{32}$, $\underset{\sim}{T}^{ep}_{323} = \underset{\sim}{B}^{ep}_{32}$ еталонних підсередовищ ($\mathbf{T}^{e}_{i} = \mathbf{T}^{e}_{3}$) зведемо відповідно в табл. 3.9, 3.10 та 3.11.

Таблиця 3.9

Узагальнювальна таблиця для $\underset{\sim}{T}^{ep}_{31s}$ $(s=\overline{1,5})$ – $\underset{\sim}{OM}^{ep}_{31}$, $\underset{\sim}{M}^{ep}_{31}$, $\underset{\sim}{C}^{ep}_{31}$, $\underset{\sim}{B}^{ep}_{31}$, $\underset{\sim}{OB}^{ep}_{31}$

$\underset{\sim}{T}^{ep}_{31s}$	μ^{ep}_{31sg} $(g=\overline{1,7})$						
	μ^{ep}_{31s1}	μ^{ep}_{31s2}	μ^{ep}_{31s3}	μ^{ep}_{31s4}	μ^{ep}_{31s5}	μ^{ep}_{31s6}	μ^{ep}_{31s7}
	0	0,2	0,3	0,4	0,6	0,7	1
$\underset{\sim}{OM}^{ep}_{31}$	0,008	0,008	0,008	0,008	0,008	0,008	0,008
$\underset{\sim}{M}^{ep}_{31}$	0,008	0,008	0,008	0,008	0,008	0,022	0,063
$\underset{\sim}{C}^{ep}_{31}$	0,008	0,036	0,049	0,063	0,125	0,157	0,25
$\underset{\sim}{B}^{ep}_{31}$	0,063	0,125	0,157	0,188	0,25	0,313	0,5
$\underset{\sim}{OB}^{ep}_{31}$	0,25	0,333	0,375	0,417	0,5	0,625	1

Таблиця 3.10

Узагальнювальна таблиця для $\underset{\sim}{T}^{ep}_{31s}$ $(s=\overline{1,5})$ – $\underset{\sim}{OM}^{ep}_{31}$, $\underset{\sim}{M}^{ep}_{31}$, $\underset{\sim}{C}^{ep}_{31}$, $\underset{\sim}{B}^{ep}_{31}$, $\underset{\sim}{OB}^{ep}_{31}$

$\underset{\sim}{T}^{ep}_{31s}$	μ^{ep}_{31sg} $(g=\overline{8,13})$					
	μ^{ep}_{31s8}	μ^{ep}_{31s9}	$\mu^{ep}_{31s(10)}$	$\mu^{ep}_{31s(11)}$	$\mu^{ep}_{31s(12)}$	$\mu^{ep}_{31s(13)}$
	0,7	0,6	0,4	0,3	0,2	0
$\underset{\sim}{OM}^{ep}_{31}$	0,032	0,039	0,055	0,063	0,125	0,25
$\underset{\sim}{M}^{ep}_{31}$	0,133	0,157	0,203	0,227	0,25	0,5
$\underset{\sim}{C}^{ep}_{31}$	0,357	0,393	0,464	0,5	0,667	1
$\underset{\sim}{B}^{ep}_{31}$	1	1	1	1	1	1
$\underset{\sim}{OB}^{ep}_{31}$	1	1	1	1	1	1

Таблиця 3.11

Узагальнювальна таблиця для $\underset{\sim}{T}^{ep}_{32s}$ $(s=\overline{1,3})$ – $\underset{\sim}{M}^{ep}_{32}$, $\underset{\sim}{C}^{ep}_{32}$, $\underset{\sim}{Б}^{ep}_{32}$

$\underset{\sim}{T}^{ep}_{32s}$	μ^{ep}_{32sg} $(g=\overline{1,9})$								
	μ^{ep}_{32s1}	μ^{ep}_{32s2}	μ^{ep}_{32s3}	μ^{ep}_{32s4}	μ^{ep}_{32s5}	μ^{ep}_{32s6}	μ^{ep}_{32s7}	μ^{ep}_{32s8}	μ^{ep}_{32s9}
	0	0,2	0,5	0,7	1	0,7	0,5	0,2	0
$\underset{\sim}{M}^{ep}_{32}$	0,01	0,01	0,01	0,01	0,1	0,044	0,066	0,1	1
$\underset{\sim}{C}^{ep}_{32}$	0,01	0,01	0,01	0,046	0,1	1	1	1	1
$\underset{\sim}{Б}^{ep}_{32}$	0,01	0,046	0,1	0,46	1	1	1	1	1

Аналогічним чином відповідно до табл. 3.8 всі номіналізовані НЧ $\underset{\sim}{P}^{\tau_f p}_{31} = \underset{\sim}{P}^{\tau_f p}_{SPKOП}$ та $\underset{\sim}{P}^{\tau_f p}_{32} = \underset{\sim}{P}^{\tau_f p}_{SPKПОА}$ поточних підсередовищ ($\mathbf{P_i^{\tau_f} = P_{SP}^{\tau_f}}$) зведемо відповідно в табл. 3.12 та 3.13.

Таблиця 3.12

Узагальнювальна таблиця для $\underset{\sim}{P}^{p}_{SPKOП}$

$\underset{\sim}{P}^{\tau_f p}_{31}$	μ^{p}_{31g} $(g=\overline{1,13})$												
	μ^{p}_{311}	μ^{p}_{312}	μ^{p}_{313}	μ^{p}_{314}	μ^{p}_{315}	μ^{p}_{316}	μ^{p}_{317}	μ^{p}_{318}	μ^{p}_{319}	$\mu^{p}_{31(10)}$	$\mu^{p}_{31(11)}$	$\mu^{p}_{31(12)}$	$\mu^{p}_{31(13)}$
	0	0,2	0,3	0,4	0,6	0,7	1	0,7	0,6	0,4	0,3	0,2	0
$\underset{\sim}{P}^{\tau_f p}_{SPKOП}$	0,095	0,095	0,095	0,095	0,157	0,188	0,28	0,393	0,43	0,505	0,543	0,58	0,58

Таблиця 3.13

Узагальнювальна таблиця для $\underset{\sim}{P}^{p}_{SPKПОА}$

$\underset{\sim}{P}^{\tau_f p}_{32}$	μ^{p}_{32g} $(g=\overline{1,9})$								
	μ^{p}_{321}	μ^{p}_{322}	μ^{p}_{323}	μ^{p}_{324}	μ^{p}_{325}	μ^{p}_{326}	μ^{p}_{327}	μ^{p}_{328}	μ^{p}_{329}
	0	0,2	0,5	0,7	1	0,7	0,5	0,2	0
$\underset{\sim}{P}^{\tau_f p}_{SPKПОА}$	0,082	0,082	0,082	0,377	0,82	1	1	1	1

Графічна інтерпретація номіналізованих НЧ базується на побудові геометричного образу α-рівней $\mathbf{AL_{ij}}$ (див. (3.7)), а також всіх перетворених $\underset{\sim}{T}^{ep}_{ijs}$ (див. (3.11)) та $\underset{\sim}{P}^{\tau_f p}_{ij}$ (див. (3.12)) НЧ еталонного та поточного підсередовища ($\mathbf{T_i^e}$ та $\mathbf{P_i^{\tau_f}}$). Геометричне місце точок на площині визначається за допомогою ламаної, яка з'єднує точки, що відображають компоненти номіналізованих НЧ в порядку зростання їх носіїв x^{ep}_{ijsg}. Візуалізація такого НЧ представлена у вигляді ламаної —●— на рис. 3.2.

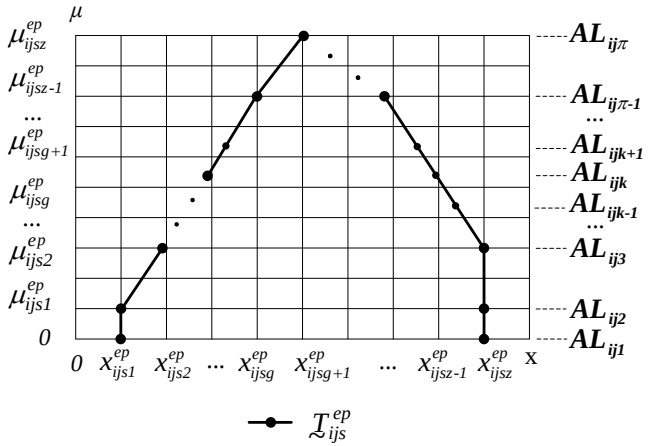

Рис. 3.2. Узагальнювальна графічна інтерпретація перетворених НЧ

Наприклад, для візуалізації перетворених $\underset{\sim}{T}^{ep}_{31s}$, $\underset{\sim}{T}^{ep}_{32s}$ і номіналізованих $\underset{\sim}{P}^{\tau_f p}_{31}$, $\underset{\sim}{P}^{\tau_f p}_{32}$ НЧ еталонних та поточних підсередовищ ($\mathbf{T_i^e = T_3^e = T_{SP}^e}$ та $\mathbf{P_i^{\tau_f} = P_3^{\tau_f} = P_{SP}^{\tau_f}}$) скористаємося сформованими значеннями (див. приклад для (3.11) та (3.12)): $\underset{\sim}{T}^{ep}_{311} = \underset{\sim}{OM}^{ep}_{31}$, $\underset{\sim}{T}^{ep}_{312} = \underset{\sim}{M}^{ep}_{31}$, $\underset{\sim}{T}^{ep}_{313} = \underset{\sim}{C}^{ep}_{31}$, $\underset{\sim}{T}^{ep}_{314} = \underset{\sim}{Б}^{ep}_{31}$, $\underset{\sim}{T}^{ep}_{315} = \underset{\sim}{OБ}^{ep}_{31}$, $\underset{\sim}{T}^{ep}_{321} = \underset{\sim}{M}^{ep}_{32}$, $\underset{\sim}{T}^{ep}_{322} = \underset{\sim}{C}^{ep}_{32}$, $\underset{\sim}{T}^{ep}_{323} = \underset{\sim}{Б}^{ep}_{32}$ та $\underset{\sim}{P}^{\tau_f p}_{SPKOП}$, $\underset{\sim}{P}^{\tau_f p}_{SPKПOA}$, а також відповідно отриманими α-рівнями підмножин $\mathbf{AL_{31}}$, $\mathbf{AL_{32}}$ (див. приклад для (3.7)). Виходячи з цього,

будується шість ламаних $\underset{\sim}{OM}^{ep}_{31}$, $\underset{\sim}{M}^{ep}_{31}$, $\underset{\sim}{C}^{ep}_{31}$, $\underset{\sim}{B}^{ep}_{31}$, $\underset{\sim}{OB}^{ep}_{31}$, $\underset{\sim}{P}^{\tau_f p}_{SPKOП}$ та чотири – $\underset{\sim}{M}^{ep}_{32}$, $\underset{\sim}{C}^{ep}_{32}$, $\underset{\sim}{B}^{ep}_{32}$, $\underset{\sim}{P}^{\tau_f p}_{SPKПОА}$, за верхніми точками перетину яких формуються нечіткі опорні двовимірні області, за якими візуально можна відобразити рівень аномального стану (див. рис. 3.3).

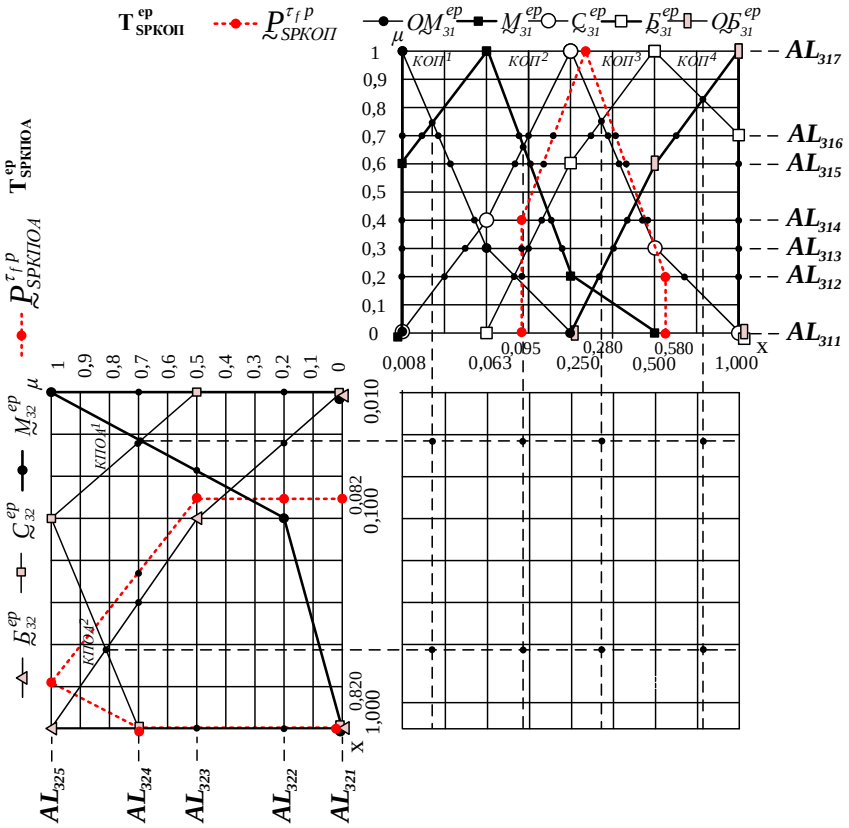

Рис. 3.3. Графічна інтерпретація перетворених $\underset{\sim}{T}^{ep}_{31s}$, $\underset{\sim}{T}^{ep}_{32s}$ та $\underset{\sim}{P}^{\tau_f p}_{31}$, $\underset{\sim}{P}^{\tau_f p}_{32}$ НЧ еталонних та поточних підсередовищ ($\mathbf{T^e_i = T^e_3 = T^e_{SP}}$ та $\mathbf{P^{\tau_f}_i = P^{\tau_f}_3 = P^{\tau_f}_{SP}}$)

Запропонований в роботі МАН НЧ [13, 15, 16] для систем виявлення вторгнень, який за рахунок побудованого механізму формування множини α-рівней, допоміжних підмножин α-рівневих інтервалів та міжточкових α-рівневих інтервалів, а також процесу номіналізації та визначення значень необхідних супортів нечітких чисел еталонних та поточних середовищ, дозволяє здійснити графічну інтерпретацію нечітких величин та визначати ідентифікуючі терми, що відображають поточні стани еталонних та поточних підсередовищ, які характерні для реалізації певних типів кібератак на РІС.

Для подальшого виявлення аномалій в ІС необхідно визначити, ідентифікуючий терм, тобто таке еталонне НЧ, яке найближче до поточного НЧ, і яке буде свідчити про рівень аномального стану в ІС.

3.3. Метод визначення ідентифікуючих термів для систем виявлення вторгнень

На основі КМАС (див. п. 2.1 та [2-4]), МФЕС (див. п. 2.2 та [5-7, 9]), МФП (див. п. 3.1 та [1, 12]) та МАН (див. п. 3.2 та [13, 15, 16]) розробимо метод визначення ідентифікуючих термів (МВІТ) [17] для СВВ. На базі такого методу (при вирішенні задач виявлення кібератак) за допомогою еталонного середовища можна здійснити пошук ідентифікуючих перетворених термів еталонного середовища, орієнтованих на обробку в детекційному середовищі для визначення рівнів аномальних станів.

Пропонується метод, базовий механізм якого ґрунтується на трьох етапах:

- формування множини ознак;
- визначення підмножин ознак;
- визначення номера ідентифікуючого терма.

Розглянемо кожний із запропонованих етапів.

Формування множини ознак

Етап 1 – формування множини ознак. Для реалізації цього етапу введемо $\mathbf{XP}_{ij}$ – множину всіх можливих характерних ознак (ХО) методів порівняння функцій належності (МПФН) та d підмножин таких ознак $\mathbf{XP}_{ij}^{c} \subseteq \mathbf{XP}_{ij}$

$$\mathbf{XP_{ij}} = \{\bigcup_{c=1}^{d} \mathbf{XP_{ij}^{c}}\} = \{\mathbf{XP_{ij}^{1}},\ \mathbf{XP_{ij}^{2}},\ \ldots,\ \mathbf{XP_{ij}^{d}}\},\quad (c = \overline{1,d}),\tag{3.24}$$

де кожний член множини $\mathbf{XP_{ij}}$ відображає можливі ХО, які сформовані за допомогою множини МПФН, тобто:

$$\mathbf{МПФН} = \{\bigcup_{c=1}^{d} МПФН_c\} = \{МПФН_1,\ МПФН_2,\ \ldots,\ МПФН_d\},\quad (c = \overline{1,d}),\tag{3.25}$$

де d – кількість використаних МПФН. Іншими словами можна сказати, що вміст кожної підмножини $\mathbf{XP_{ij}^{c}}$ формується за допомогою відповідного $МПФН_c$, $(c = \overline{1,d})$.

Наприклад, при $d = 8$ множина $\mathbf{XP_{ij}}$ відповідно до (3.24) приймає вигляд

$$\mathbf{XP_{ij}} = \{\bigcup_{c=1}^{8} \mathbf{XP_{ij}^{c}}\} = \{\mathbf{XP_{ij}^{1}},\ \mathbf{XP_{ij}^{2}},\ \mathbf{XP_{ij}^{3}},\ \mathbf{XP_{ij}^{4}},\ \mathbf{XP_{ij}^{5}},\ \mathbf{XP_{ij}^{6}},\ \mathbf{XP_{ij}^{7}},\ \mathbf{XP_{ij}^{8}}\},\quad (c = \overline{1,8}),$$

кожний член якої відображає всі можливі ХО, які сформовані за допомогою множини (3.25), яка складається з відомих МПФН [11, 14]. При заданому значенні d множина **МПФН** має вигляд:

$$\mathbf{МПФН} = \{\bigcup_{c=1}^{8} МПФН_c\} = \{МПФН_1,\ МПФН_2,\ МПФН_3,\ МПФН_4,\ МПФН_5,\ МПФН_6,\ МПФН_7,\ МПФН_8\} = \{ВХ,\ АРВ,\ ЦВ,\ ММ,\ БД,\ ФУП,\ УНЧ,\ УБВ\},$$

де кожний член $\mathbf{XP_{ij}^{c}}$ формується за допомогою відповідного $МПФН_c$, $(c = \overline{1,8})$, тобто $\mathbf{XP_{ij}^{1}}$ формується за допомогою узагальнювальної відстані Хеммінга (ВХ) $(МПФН_1 = ВХ)$, $\mathbf{XP_{ij}^{2}}$ – за участі

α-рівневої відстані *(МПФН$_2$=АРВ),* а $\mathbf{XP_{ij}^3}$, $\mathbf{XP_{ij}^4}$, $\mathbf{XP_{ij}^5}$, $\mathbf{XP_{ij}^6}$, $\mathbf{XP_{ij}^7}$ та $\mathbf{XP_{ij}^8}$ відповідно формуються шляхом методів центру ваги, максмінного, узагальнювальних операцій «більше або дорівнює», функції упорядкування нечітких підмножин одиничного інтервалу, упорядкування НЧ, яке характеризує неприйняття ризику та упорядкування на базі відношень, тобто: $МПФН_3 = ЦВ$, $МПФН_4 = ММ$, $МПФН_5 = БД$, $МПФН_6 = ФУП$, $МПФН_7 = УНЧ$ і $МПФН_8 = УБВ$. Ці методи частіше всього застосовуються в теорії та практиці порівняння нечітких множин [11, 14].

Визначення підмножин ознак

Етап 2 – визначення підмножин ознак. Даний етап реалізується на основі методів, які належать множині **МПФН**, за допомогою яких формуються ХО, тобто члени підмножин $\mathbf{XP_{ij}^c} \subseteq \mathbf{XP_{ij}}$:

$$\begin{gathered}\mathbf{XP_{ij}^c} = \{\bigcup_{s=1}^{r_j} XP_{ijs}^c\} = \\ \{\, XP_{ij1}^c,\ XP_{ij2}^c,\ \ldots,\ XP_{ijr_j}^c\,\}, \\ (s=\overline{1,r_j}).\end{gathered} \tag{3.26}$$

Іншими словами можна сказати, що кожний член XP_{ijs}^c $(s=\overline{1,r_j})$ підмножини $\mathbf{XP_{ij}^c}$ формується за допомогою $МПФН_c$, де відносно c визначається номер способу реалізації етапу 1.

Наприклад, при $c=1$ члени множини $\mathbf{XP_{ij}^1}$ формуються першим способом.

Спосіб 1. Використовуємо $МПФН_1 = ВХ$ із множини **МПФН** тобто

$$\begin{gathered}XP_{ijs}^1 = h\,(\underset{\sim}{T}_{ijs}^{ep},\ \underset{\sim}{P}_{ij}^{\tau_l p}) = \\ \sum_{g=1}^{z}\left|x_{ijsg}^{ep} - x_{ijg}^{p}\right| = |\,x_{ijs1}^{ep} - x_{ij1}^{p}\,| + |\,x_{ijs2}^{ep} - x_{ij2}^{p}\,| + \ldots + \\ |\,x_{ijsg}^{ep} - x_{ijg}^{p}\,| + \ldots + |\,x_{ijsz}^{ep} - x_{ijz}^{p}\,|, \\ (g=\overline{1,z}),\ (z=2\pi\text{-}1),\ (s=\overline{1,r_j}),\end{gathered} \tag{3.27}$$

де x_{ijsg}^{ep} та x_{ijg}^{p} – відповідно супорти (носії) перетвореного $\underset{\sim}{T}_{ijs}^{ep}$ і $\underset{\sim}{P}_{ij}^{\tau_f p}$ НЧ еталонного та поточного середовища ($\mathbf{T^e}$ та $\mathbf{P^{\tau_f}}$), z – кількість компонент в $\underset{\sim}{T}_{ijs}^{ep}$ та $\underset{\sim}{P}_{ij}^{\tau_f p}$ (див. (3.11) та (3.12), [13]).

Розглянемо приклад реалізації першим способом етапу 2 для $n=1$ ($i=3$ тобто для кібератаки з ІД $CA_3 = CA_{SP} = SP$) при

$$j=1 \ (P_{31} = P_{SPKOП} = KOП),$$

$$r_1 = 5, \ g = \overline{1,13},$$

$$\underset{\sim}{T}_{ijs}^{ep} = \underset{\sim}{T}_{31s}^{ep}, \ \underset{\sim}{P}_{ij}^{p} = \underset{\sim}{P}_{31}^{\tau_f p} = \underset{\sim}{P}_{SPKOП}^{\tau_f p}$$

та якщо

$$j=2 \ (P_{32} = P_{SPKПОА} = KПОА),$$

$$r_2 = 3, \ g = \overline{1,9},$$

$$\underset{\sim}{T}_{ijs}^{ep} = \underset{\sim}{T}_{32s}^{ep}, \ \underset{\sim}{P}_{ij}^{p} = \underset{\sim}{P}_{32}^{\tau_f p} = \underset{\sim}{P}_{SPKПОА}^{\tau_f p}.$$

Підмножину всіх можливих відстаней $\mathbf{XP_{ij}^1} = \mathbf{XP_{31}^1}$ та $\mathbf{XP_{ij}^1} = \mathbf{XP_{32}^1}$ (див. (3.26)) обчислимо за допомогою (3.27) тобто:

$$\mathbf{XP_{31}^1} = \{\bigcup_{s=1}^{5} XP_{31s}^1\} =$$

$$\{XP_{311}^1, \ XP_{312}^1, \ XP_{313}^1, \ XP_{314}^1, \ XP_{315}^1\} =$$

$$\{h(\underset{\sim}{T}_{311}^{ep}, \ \underset{\sim}{P}_{31}^{\tau_f p}), \ h(\underset{\sim}{T}_{312}^{ep}, \ \underset{\sim}{P}_{31}^{\tau_f p}), \ h(\underset{\sim}{T}_{313}^{ep}, \ \underset{\sim}{P}_{31}^{\tau_f p}),$$

$$h(\underset{\sim}{T}_{314}^{ep}, \ \underset{\sim}{P}_{31}^{\tau_f p}), \ h(\underset{\sim}{T}_{315}^{ep}, \ \underset{\sim}{P}_{31}^{\tau_f p})\} =$$

$$\{(\left|x_{3111}^{ep} - x_{311}^{p}\right| + \left|x_{3112}^{ep} - x_{312}^{p}\right| + \left|x_{3113}^{ep} - x_{313}^{p}\right| + \left|x_{3114}^{ep} - x_{314}^{p}\right| + \left|x_{3115}^{ep} - x_{315}^{p}\right| +$$

$$\left|x_{3116}^{ep} - x_{316}^{p}\right| + \left|x_{3117}^{ep} - x_{317}^{p}\right| + \left|x_{3118}^{ep} - x_{318}^{p}\right| + \left|x_{3119}^{ep} - x_{319}^{p}\right| +$$

$$\left|x_{311(10)}^{ep} - x_{31(10)}^{p}\right| + \left|x_{311(11)}^{ep} - x_{31(11)}^{p}\right| + \left|x_{311(12)}^{ep} - x_{31(12)}^{p}\right| + \left|x_{311(13)}^{ep} - x_{31(13)}^{p}\right|),$$

$$(\left|x_{3121}^{ep} - x_{311}^{p}\right| + \left|x_{3122}^{ep} - x_{312}^{p}\right| + \left|x_{3123}^{ep} - x_{313}^{p}\right| + \left|x_{3124}^{ep} - x_{314}^{p}\right| + \left|x_{3125}^{ep} - x_{315}^{p}\right| +$$

$$\left|x_{3126}^{ep} - x_{316}^{p}\right| + \left|x_{3127}^{ep} - x_{317}^{p}\right| + \left|x_{3128}^{ep} - x_{318}^{p}\right| + \left|x_{3129}^{ep} - x_{319}^{p}\right| +$$

$$\left|x_{312(10)}^{ep} - x_{31(10)}^{p}\right| + \left|x_{312(11)}^{ep} - x_{31(11)}^{p}\right| + \left|x_{312(12)}^{ep} - x_{31(12)}^{p}\right| + \left|x_{312(13)}^{ep} - x_{31(13)}^{p}\right|),$$

$$(\left|x_{3131}^{ep} - x_{311}^{p}\right| + \left|x_{3132}^{ep} - x_{312}^{p}\right| + \left|x_{3133}^{ep} - x_{313}^{p}\right| + \left|x_{3134}^{ep} - x_{314}^{p}\right| + \left|x_{3135}^{ep} - x_{315}^{p}\right| +$$

$$\left|x^{ep}_{3136}-x^{p}_{316}\right|+\left|x^{ep}_{3137}-x^{p}_{317}\right|+\left|x^{ep}_{3138}-x^{p}_{318}\right|+\left|x^{ep}_{3139}-x^{p}_{319}\right|+$$
$$\left|x^{ep}_{313(10)}-x^{p}_{31(10)}\right|+\left|x^{ep}_{313(11)}-x^{p}_{31(11)}\right|+\left|x^{ep}_{313(12)}-x^{p}_{31(12)}\right|+\left|x^{ep}_{313(13)}-x^{p}_{31(13)}\right|\ ),$$
$$(\ \left|x^{ep}_{3141}-x^{p}_{311}\right|+\left|x^{ep}_{3142}-x^{p}_{312}\right|+\left|x^{ep}_{3143}-x^{p}_{313}\right|+\left|x^{ep}_{3144}-x^{p}_{314}\right|+\left|x^{ep}_{3145}-x^{p}_{315}\right|+$$
$$\left|x^{ep}_{3146}-x^{p}_{316}\right|+\left|x^{ep}_{3147}-x^{p}_{317}\right|+\left|x^{ep}_{3148}-x^{p}_{318}\right|+\left|x^{ep}_{3149}-x^{p}_{319}\right|+$$
$$\left|x^{ep}_{314(10)}-x^{p}_{31(10)}\right|+\left|x^{ep}_{314(11)}-x^{p}_{31(11)}\right|+\left|x^{ep}_{314(12)}-x^{p}_{31(12)}\right|+\left|x^{ep}_{314(13)}-x^{p}_{31(13)}\right|\ ),$$
$$(\ \left|x^{ep}_{3151}-x^{p}_{311}\right|+\left|x^{ep}_{3152}-x^{p}_{312}\right|+\left|x^{ep}_{3153}-x^{p}_{313}\right|+\left|x^{ep}_{3154}-x^{p}_{314}\right|+\left|x^{ep}_{3155}-x^{p}_{315}\right|+$$
$$\left|x^{ep}_{3156}-x^{p}_{316}\right|+\left|x^{ep}_{3157}-x^{p}_{317}\right|+\left|x^{ep}_{3158}-x^{p}_{318}\right|+\left|x^{ep}_{3159}-x^{p}_{319}\right|+$$
$$\left|x^{ep}_{315(10)}-x^{p}_{31(10)}\right|+\left|x^{ep}_{315(11)}-x^{p}_{31(11)}\right|+\left|x^{ep}_{315(12)}-x^{p}_{31(12)}\right|+\left|x^{ep}_{315(13)}-x^{p}_{31(13)}\right|\ )\}=$$

{(|0,008–0,095|+|0,008–0,095|+|0,008–0,095|+|0,008–0,095|+|0,008–0,157|+|0,008–0,188|+|0,008–0,28|+|0,032–0,393|+|0,039–0,43|+|0,055–0,505|+|0,063–0,543|+|0,125–0,58|+|0,25–0,58|),
(0,008–0,095|+|0,008–0,095|+|0,008–0,095|+|0,008–0,095|+|0,008–0,157|+|0,022–0,188|+|0,063–0,28|+|0,133–0,393|+|0,157–0,43|+|0,203–0,505|+|0,227–0,543|+|0,25–0,58|+|0,5–0,58|),
(0,008–0,095|+|0,036–0,095|+|0,049–0,095|+|0,063–0,095|+|0,125–0,157|+|0,157–0,188|+|0,25–0,28|+|0,357–0,393|+|0,393–0,43|+|0,464–0,505|+|0,5–0,543|+|0,667–0,58|+|1–0,58|),
(0,063–0,095|+|0,125–0,095|+|0,157–0,095|+|0,188–0,095|+|0,25–0,157|+|0,313–0,188|+|0,5–0,28|+|1–0,393|+|1–0,43|+|1–0,505|+|1–0,543|+|1–0,58|+|1–0,58|),
(0,25–0,095|+|0,333–0,095|+|0,375–0,095|+|0,417–0,095|+|0,5–0,157|+|0,625–0,188|+|1–0,28|+|1–0,393|+|1–0,43|+|1–0,505|+|1–0,543|+|1–0,58|+|1–0,58|)}=

(0,087+0,087+0,087+0,087+0,149+0,18+0,272+0,361+0,391+0,45+0,48+0,455+0,33),
(0,087+0,087+0,087+0,087+0,149+0,166+0,217+0,26+0,273+0,302+0,316+0,33+0,08),
(0,087+0,059+0,046+0,032+0,032+0,031+0,03+0,036+0,037+0,041+0,043+0,087+0,42),
(0,032+0,03+0,062+0,093+0,093+0,125+0,22+0,607+0,57+0,495+0,457+0,42+0,42),
(0,155+0,238+0,28+0,322+0,343+0,437+0,72+0,607+0,57+0,495+0,457+0,42+0,42)=

$$\{\ 3{,}416;\ 2{,}441;\ 0{,}981;\ 3{,}624;\ 5{,}464\ \}$$

та

$$\mathbf{XP^1_{32}} = \{\bigcup_{s=1}^{3} XP^1_{32s}\} =$$

$$\{\ XP^1_{321},\ XP^1_{322},\ XP^1_{323}\} =$$

$$\{\ h\ (\underset{\sim}{T}^{ep}_{321},\ \underset{\sim}{P}^{\tau_f p}_{32}),\ h\ (\underset{\sim}{T}^{ep}_{322},\ \underset{\sim}{P}^{\tau_f p}_{32}),\ h\ (\underset{\sim}{T}^{ep}_{323},\ \underset{\sim}{P}^{\tau_f p}_{32})\} =$$

$$\{(\ \left|x^{ep}_{3211} - x^{p}_{321}\right| + \left|x^{ep}_{3212} - x^{p}_{322}\right| + \left|x^{ep}_{3213} - x^{p}_{323}\right| + \left|x^{ep}_{3214} - x^{p}_{324}\right| + \left|x^{ep}_{3215} - x^{p}_{325}\right| +$$

$$\left|x^{ep}_{3216} - x^{p}_{326}\right| + \left|x^{ep}_{3217} - x^{p}_{327}\right| + \left|x^{ep}_{3218} - x^{p}_{328}\right| + \left|x^{ep}_{3219} - x^{p}_{329}\right|),$$

$$(\ \left|x^{ep}_{3221} - x^{p}_{321}\right| + \left|x^{ep}_{3222} - x^{p}_{322}\right| + \left|x^{ep}_{3223} - x^{p}_{323}\right| + \left|x^{ep}_{3224} - x^{p}_{324}\right| + \left|x^{ep}_{3225} - x^{p}_{325}\right| +$$

$$\left|x^{ep}_{3226} - x^{p}_{326}\right| + \left|x^{ep}_{3227} - x^{p}_{327}\right| + \left|x^{ep}_{3228} - x^{p}_{328}\right| + \left|x^{ep}_{3229} - x^{p}_{329}\right|),$$

$$(\ \left|x^{ep}_{3231} - x^{p}_{321}\right| + \left|x^{ep}_{3232} - x^{p}_{322}\right| + \left|x^{ep}_{3233} - x^{p}_{323}\right| + \left|x^{ep}_{3234} - x^{p}_{324}\right| + \left|x^{ep}_{3235} - x^{p}_{325}\right| +$$

$$\left|x^{ep}_{3236} - x^{p}_{326}\right| + \left|x^{ep}_{3237} - x^{p}_{327}\right| + \left|x^{ep}_{3238} - x^{p}_{328}\right| + \left|x^{ep}_{3239} - x^{p}_{329}\right|\ )\} =$$

$$\{(\ 0{,}01–0{,}082|+|0{,}01–0{,}082|+|0{,}01–0{,}082|+|0{,}01–0{,}377|+|0{,}1–$$

$$0{,}82|+|0{,}044–1|+|0{,}066–1|+|0{,}1–1|+|1–1|),$$

$$(|0{,}01–0{,}082|+|0{,}01–0{,}082|+|0{,}01–0{,}082|+|0{,}046–0{,}377|+|0{,}1–$$

$$0{,}82|+|1–1|+|1–1|+|1–1|+|1–1|),$$

$$(|0{,}01–0{,}082|+|0{,}046–0{,}082|+|0{,}01–0{,}082|+|0{,}46–0{,}377|+|1–0{,}82|+|1–$$

$$1|+|1–1|+|1–1|+|1–1|\ )\} =$$

$$\{(\ 0{,}072+0{,}072+0{,}072+0{,}367+0{,}72+0{,}956+0{,}934+0{,}9+0),$$

$$(0{,}072+0{,}072+0{,}072+0{,}331+0{,}72+0+0+0+0),$$

$$(0{,}072+0{,}036+0{,}072+0{,}083+0{,}18+0+0+0+0\ )\} =$$

$$\{\ 4{,}093;\ 1{,}267;\ 0{,}443\ \}.$$

Таким чином:

$$\mathbf{XP^1_{31}} = \{\ 3{,}416;\ 2{,}441;\ 0{,}981;\ 3{,}624;\ 5{,}464\ \}\ \text{і}$$

$$\mathbf{XP^1_{32}} = \{\ 4{,}093;\ 1{,}267;\ 0{,}443\ \}. \qquad (3.28)$$

Визначення номера ідентифікуючого терма

Етап 3 – визначення номера ідентифікуючого терма. Для реалізації цього етапу введемо множину всіх номерів ідентифікуючих термів **NUM** та підмножину таких номерів $\mathbf{NUM_i}$

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\mathbf{NUM_i}\}=\{\mathbf{NUM_1},\ \mathbf{NUM_2},\ \ldots,\ \mathbf{NUM_n}\},\quad (i=\overline{1,n}),\tag{3.29}$$

де $\mathbf{NUM_i} \subseteq \mathbf{NUM}$ визначимо як:

$$\mathbf{NUM_i}=\{\bigcup_{j=1}^{m_i} NUM_{ij}\}=\{NUM_{i1},\ NUM_{i2},\ \ldots,\ NUM_{im_i}\},\quad (j=\overline{1,m_i}),\tag{3.30}$$

а m_i – кількість номерів ідентифікуючих термів, які використовуються для виявлення *i*-ї кібератаки. З урахуванням (3.30) формулу (3.29) запишемо в наступному вигляді:

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\mathbf{NUM_i}\}=\{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i} NUM_{ij}\}\}=\{\{NUM_{11},\ NUM_{12},\ \ldots,\ NUM_{1m_1}\},\ \{NUM_{21},\ NUM_{22},\ \ldots,\ NUM_{2m_2}\},\ \ldots,\ \{NUM_{n1},\ NUM_{n2},\ \ldots,\ NUM_{nm_n}\},\quad (i=\overline{1,n},\ \ j=\overline{1,m_i}).\tag{3.31}$$

Далі, виконання цього етапу здійснюється за допомогою функції пошуку ідентифікуючої ХО та її номеру, тобто такої ідентифікуючої ознаки $IX^{c}_{ijNUM_{ij}}$, відповідно до якої певній функції (тип якої визначається значенням змінної c) буде присвоєно одне із значень XP^{c}_{ijs}, $(s=\overline{1,r_j})$. Очевидно, що при цьому $NUM_{ij}=s$. Фактично, за номером (поточним значенням s) ідентифікуючої ХО в (3.26) можна визначити відповідний ідентифікуючий терм в підмножині $\mathbf{T^e_{ij}}$ (див. (2.35), [5]).

Таким чином, пошук $IX^{c}_{ijNUM_{ij}} = XP^{c}_{ijs}$ здійснюється за допомогою узгодженої з МПФН функції $\mathbf{F^c\ (XP^c_{ij})}$, тобто:

$$IX^{c}_{ijNUM_{ij}} = F^{c}(\bigcup_{s=1}^{r_j} XP^{c}_{ijs}) =$$
$$F^{c}_{ij}(\, XP^{c}_{ij1},\ XP^{c}_{ij2},\ \ldots,\ XP^{c}_{ijr_j}\,), \qquad (3.32)$$
$$(\, s = \overline{1,r_j}\,),$$

де за значенням змінної c визначається номер способу реалізації етапу 3, який також пов'язаний з номером способу, за допомогою якого реалізується етап 2.

Наприклад, при $c = 1$ здійснюється перший спосіб пошуку номеру ідентифікуючого терму, який пов'язаний з $МПФН_1 = ВХ$ та складається з наступних кроків.

Спосіб 1. Крок 1. Визначення $IX^{1}_{ijNUM_{ij}}$ здійснюється шляхом узгодженої з ВХ функції F^{1} $\mathbf{(XP^{1}_{ij})}$, яка виконує пошук мінімального значення із членів підмножини $\mathbf{XP^{c}_{ij}}$ відповідно до наступного виразу:

$$IX^{1}_{ijNUM_{ij}} = F^{1}(\bigcup_{s=1}^{r_j} XP^{1}_{ijs}) =$$
$$F^{1}_{ij}\,(\, XP^{1}_{ij1},\ XP^{1}_{ij2},\ \ldots,\ XP^{1}_{ijr_j}\,)$$
або
$$IX^{1}_{ijNUM_{ij}} = \bigwedge_{s=1}^{r_j} XP^{1}_{ijs} = XP^{1}_{ij1} \wedge XP^{1}_{ij2} \wedge \ldots \wedge XP^{1}_{ijr_j}, \qquad (3.33)$$
$$(\, s = \overline{1,r_j}\,).$$

Крок 2. Визначення ідентифікуючого терму в $\mathbf{T^{e}_{ij}}$ (див. (2.35)) здійснюється на основі того, що $IX^{1}_{ijNUM_{ij}} = XP^{1}_{ijs}$, а значення NUM_{ij} буде еквівалентно s. Відповідно до цього, у підмножині $\mathbf{T^{e}_{ij}}$ знаходиться терм, у якого значення $s = NUM_{ij}$ і який приймаємо за ідентифікуючий.

Розглянемо приклад реалізації етапу 3 першим способом для $n = 1$ $(i = 3$ тобто для кібератаки з ІД $CA_3 = CA_{SP} = SP)$ при
$$j = 1\ \ (P_{31} = P_{SPKOP} = KOP),$$

$$r_1 = 5,\ \ XP^1_{ijs} = XP^1_{31s}$$

та якщо

$$j = 2\ \ (P_{32} = P_{SPKPOA} = KPOA),$$

$$r_2 = 3,\ \ XP^1_{ijs} = XP^1_{32s}$$ (див. (3.26)).

Спосіб 1. Крок 1. Визначення $IX^1_{31NUM_{31}}$ та $IX^1_{32NUM_{32}}$ здійснюється за допомогою функції F^1 $\mathbf{(XP^1_{31})}$ і F^1 $\mathbf{(XP^1_{32})}$, яка здійснює пошук мінімального значення із членів підмножини $\mathbf{XP^1_{31}}$ та $\mathbf{XP^1_{32}}$ (див. (3.31)) відповідно до (3.32) і (3.33) тобто:

$$IX^1_{31NUM_{31}} = \bigwedge_{s=1}^{5} XP^1_{31s} =$$

$$XP^1_{311} \wedge XP^1_{312} \wedge XP^1_{313} \wedge XP^1_{314} \wedge XP^1_{315} =$$

$$3{,}416 \wedge 2{,}441 \wedge 0{,}981 \wedge 3{,}624 \wedge 5{,}464 =$$

$$XP^1_{313} = 0{,}981$$ та

$$IX^1_{32NUM_{32}} = \bigwedge_{s=1}^{3} XP^1_{32s} =$$

$$XP^1_{321} \wedge XP^1_{322} \wedge XP^1_{323} =$$

$$4{,}093 \wedge 1{,}267 \wedge 0{,}443 =$$

$$XP^1_{323} = 0{,}443.$$

Крок 2. Визначення ідентифікуючого терму в $\mathbf{T^e_{31}}$ здійснюється на основі того, що $IX^1_{31NUM_{31}} = XP^1_{31s} = XP^1_{313}$, а $NUM_{31} = s = 3.$ Виходячи з цього, ідентифікуючим буде терм $\underset{\sim}{T}^e_{313}$ (див. приклад для (2.35)), у якого значення $s = 3,$ яке відповідає номеру мінімального значення ідентифікуючої ХО.

Аналогічна величина визначається в $\mathbf{T^e_{32}}$ на основі того, що $IX^1_{32NUM_{32}} = XP^1_{32s} = XP^1_{323}$ та $NUM_{32} = s = 3.$ Отже, ідентифікуючим буде терм $\underset{\sim}{T}^e_{323}$ (див. приклад для (2.35)).

Виходячи з обчислень видно, що ідентифікуючим в $\mathbf{T^e_{31}}$ буде терм $\underset{\sim}{T}^e_{313} = \underset{\sim}{C}^e_{31}$ (див. приклад для (2.35)), а відповідне йому перетворене

еталонне $\underset{\sim}{T}^{ep}_{313} = \underset{\sim}{T}^{ep}_{SPKOП3} = \underset{\sim}{C}^{ep}_{31}$ (див. приклад етапу 2 для (3.10)). Фактично, обчислення показують, що $XP^{1}_{313} = 0{,}981$, отже перетворене НЧ $\underset{\sim}{P}^{\tau_f p}_{31} = \underset{\sim}{P}^{\tau_f p}_{SPKOП}$ поточного підсередовища ($\mathbf{P_i^{\tau_f}} = \mathbf{P_3^{\tau_f}} = \mathbf{P_{SP}^{\tau_f}}$) найближче розташоване до перетвореного НЧ $\underset{\sim}{T}^{ep}_{313} = \underset{\sim}{C}^{ep}_{31}$ еталонного підсередовища ($\mathbf{T_i^e} = \mathbf{T_3^e} = \mathbf{T_{SP}^e}$). А оскільки $\underset{\sim}{P}^{\tau_f p}_{SPKOП}$ та $\underset{\sim}{C}^{ep}_{31}$ є відображенням $\underset{\sim}{P}^{\tau_f p}_{SPKOП}$ та $\underset{\sim}{C}^{e}_{31}$, то $\underset{\sim}{P}^{\tau_f p}_{SPKOП}$ найближче розташоване до НЧ $\underset{\sim}{C}^{e}_{31}$ еталонного підсередовища ($\mathbf{T_i^e} = \mathbf{T_3^e} = \mathbf{T_{SP}^e}$).

Аналогічно, ідентифікуючим в $\mathbf{T_{32}^e}$ є значення $\underset{\sim}{T}^{e}_{323} = \underset{\sim}{Б}^{e}_{32}$ (див. приклад для (2.35)) та, при цьому, $\underset{\sim}{T}^{ep}_{323} = \underset{\sim}{T}^{ep}_{SPKПОА3} = \underset{\sim}{Б}^{ep}_{32}$ (див. приклад етапу 2 для (3.10)). Також, враховуючи, що $XP^{1}_{323} = 0{,}443$, то перетворене НЧ $\underset{\sim}{P}^{\tau_f p}_{32} = \underset{\sim}{P}^{\tau_f p}_{SPKПОА}$ поточного підсередовища ($\mathbf{P_i^{\tau_f}} = \mathbf{P_3^{\tau_f}} = \mathbf{P_{SP}^{\tau_f}}$) найближче до перетвореного НЧ $\underset{\sim}{T}^{ep}_{323} = \underset{\sim}{Б}^{ep}_{32}$ еталонного підсередовища ($\mathbf{T_i^e} = \mathbf{T_3^e} = \mathbf{T_{SP}^e}$). І, отже, якщо $\underset{\sim}{P}^{\tau_f p}_{SPKПОА}$ та $\underset{\sim}{Б}^{ep}_{32}$ є відображенням $\underset{\sim}{P}^{\tau_f p}_{SPKПОА}$ та $\underset{\sim}{Б}^{e}_{32}$, то $\underset{\sim}{P}^{\tau_f p}_{SPKПОА}$ є найближчим до $\underset{\sim}{Б}^{e}_{32}$.

Для візуалізації отриманих результатів можна здійснити графічну інтерпретацію еталонних нечітких термів $\underset{\sim}{T}^{e}_{31s}$ та $\underset{\sim}{T}^{e}_{32s}$. За їх допомогою, аналогічно п. 3.1 та [1], будуються п’ять нечітких опорних двовимірних областей (див. рис. 3.4), які характеризують можливі рівні аномального стану відносно лінгвістичних еталонів $\mathbf{T_{31}^e} = \mathbf{T_{SPKOП}^e}$ та $\mathbf{T_{32}^e} = \mathbf{T_{SPKПОА}^e}$ еталонних підсередовищ $\mathbf{T_i^e} = \mathbf{T_3^e} = \mathbf{T_{SP}^e}$, які позначаються одним із текстових значень – Н, БНВ, БВН, В, П (див. п. 3.1).

За допомогою цих еталонів здійснюємо пошук нечітких термів, які найближчі до відповідних значень параметрів $\underset{\sim}{P}^{\tau_f}_{SPKOП}$ та $\underset{\sim}{P}^{\tau_f}_{SPKПОА}$ поточних підсередовищ $\mathbf{P_i^{\tau_f}} = \mathbf{P_3^{\tau_f}} = \mathbf{P_{SP}^{\tau_f}}$.

За аналогією з опорними областями також можна візуалізувати так званий нечіткий поточний блок (див. заштриховану прямокутну область на рис. 3.4), який утворений шляхом перетину $\underset{\sim}{P}^{\tau_f}_{SPKOП}$ та

$\tilde{P}^{\tau_f}_{SPKПОА}$. За допомогою цього блоку здійснюється графічна інтерпретація поточного аномального стану.

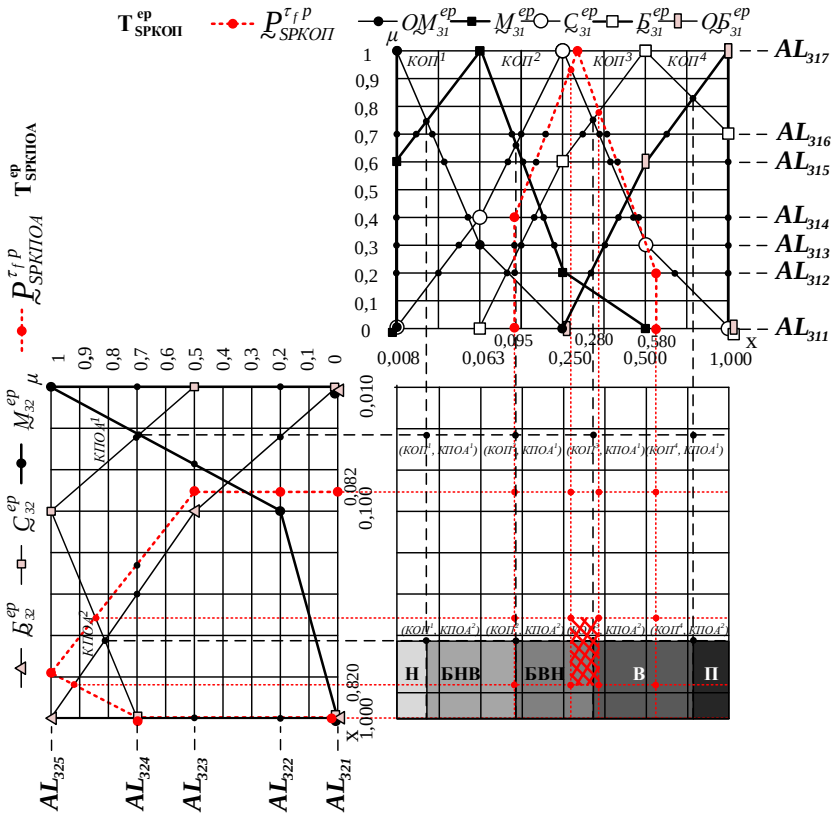

Рис. 3.4. Графічна інтерпретація нечіткого поточного блоку, за допомогою якого визначається рівень аномального стану, що породжений кібератакою з ІД $CA_3 = CA_{SP} = SP$

Таким чином, запропонований МВІТ [17, 18], який за рахунок базового механізму, що реалізує формування елементів множини характерних ознак та використання узгодженої функції, дозволяє за

допомогою еталонного середовища здійснити пошук ідентифікуючих перетворених еталонних термів, орієнтованих на обробку в детекційному середовищі для визначення рівней аномальних станів.

Далі, для наступного виявлення аномалій в ІС потрібне детекційне середовище, що включає необхідний набір базових детекційних правил, які будуть свідчити про рівень аномального стану в ІС.

СПИСОК ЛІТЕРАТУРИ ДО РОЗДІЛУ 3

1. А. Корченко, «Метод фаззификации параметров на лингвистических эталонах для систем выявления кибератак», *Безпека інформації*, Т.20, №1, С. 21-28, 2014.

2. А. Корченко, «Кортежная модель формирования набора базовых компонент для выявления кибератак», *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, В.2 (28), С. 29-36, 2014.

3. A. Korchenko, K. Warwas, A. Kłos-Witkowska, «The Tupel Model of Basic Components' Set Formation for Cyberattacks», in *Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2015 IEEE 8th International Conference on*, 2015, pp. 478-483.

4. А. Корченко, «Модель базових компонент для виявлення кібератак на ресурси інформаційних систем», *Актуальні проблеми управління інформаційною безпекою держави: VI наук.-практ. конф.*, Київ, 2015, С. 274-275.

5. А. Корченко, «Метод формирования лингвистических эталонов для систем выявления вторжений», *Захист інформації*, Т.16, №1, С. 5-12, 2014.

6. А. Корченко, «Формирование лингвистических эталонов на основе кортежной модели для систем выявления вторжений», *Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS`2015): 7-та Всеук. наук.-практ. конф.*, с. Коблево Миколаївської обл., 2015, С. 43-46.

7. B. Akhemetov, A. Korchenko, S. Akhmetova, N. Zhumangalieva, «Improved method for the formation of linguistic standards for of intrusion detection systems», *Journal of Theoretical and Applied Information Technology*, vol. 87, no. 2, pp. 221-232, 2016.

8. M. Karpinski, A. Korchenko, P. Vikulov, R. Kochan, «The Etalon Models of Linguistic Variables for Sniffing-Attack Detection», in *Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2017 IEEE 9th International Conference on*, 2017, pp. 258-264.

9. Anna Korchenko, «Formation of linguistic standards for of intrusion detection systems», *Безопасность в авиации и космические технологии: VIII Всемирный конгресс «Авиация в XXI столетии»,* Киев, 2018, С. 3.2.1.-3.2.6.

10. Б.С. Ахметов, Р.Б. Абдрахманов, А.А. Корченко, Н.К. Жумангалиева, «Базовые модели эталонных величин для систем обнаружения вторжений», *Вестник Международного Казахско-Турецкого университета. им. А.Ясави*, №5-6 (97-98), С. 15-26, 2015.

11. Б. Ахметов, А. Корченко, Н. Жумангалиева «Использование методов нечетких множеств в системах обнаружения вторжений», *Інформаційна безпека,* №1, №2, С. 42-55, 2014.

12. Н. Карпинский, А. Корченко, С. Казмирчук, «Фаззификация параметров в кортежной модели для выявления кибератак», *Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS`2016): 8-та Всеук. наук.-практ. конф.*, с. Коблево Миколаївської обл., 2016, С. 39-42.

13. А. Корченко, «Метод α-уровневой номинализации нечетких чисел для систем обнаружения вторжений», *Захист інформації,* Т.16, №4, С. 292-304, 2014.

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

15. Н. Карпинский, А. Корченко, П. Викулов, Н. Жумангалиева, «Номинализация нечетких величин для систем выявления аномалий», *Современные информационные и коммуникационные технологии на транспорте, в промышленности и образовании (TEMPUS: CITISET): X междунар. науч.-практ. конф.*, Днипро, 2016, С. 51-52.

16. M. Karpinski, A. Korchenko, P. Vikulov, «Method of α-leveled nominalization of fuzzy numbers for intrusion detection systems», in *Inżynier XXI Wieku: VI Międzynarodowa Konferencja studentow oraz doktorantow, 02.12.2016: monografia,* 1st ed., Bielsko – Biała (Poland): Akademia Techniczno-Humanistyczna w Bielsku-Białej, 2016, pp. 155-164.

17. А. Корченко, «Метод определения идентифицирующих термов для систем обнаружения вторжений», *Безпека інформації*, Т.20, №3, С. 217-223, 2014.

18. А. Корченко, «Метод определения идентифицирующих термов для систем выявления кибератак», *Актуальні питання забезпечення кібернетичної безпеки та захист інформації: наук.-практ. конф.*, Київ, 2015, С. 64-67.

РОЗДІЛ 4. МЕТОДИ ВИЯВЛЕННЯ АНОМАЛЬНИХ СТАНІВ ПОРОДЖЕНИХ КІБЕРАТАКАМИ

4.1. Метод дефазифікації параметрів детекційного середовища

На основі КМАС (див. п. 2.1 і [1-3]) та МВІТ (див. п. 3.3 і [4, 5]) розробимо метод дефазифікації параметрів детекційного середовища (МДП) для СВВ. Він дозволить отримати числові оцінки, що характеризують лінгвістичні величини відносно суджень експерта.

Базовий механізм МДП ґрунтується на трьох етапах:

- визначення допоміжного терма;
- визначення експертних коефіцієнтів параметрів;
- визначення експертного коефіцієнта кібератаки.

Розглянемо кожний із запропонованих етапів.

Визначення допоміжного терма

Етап 1 – визначення допоміжного терма. Для реалізації цього етапу необхідно визначити допоміжний терм, який слідує за ідентифікуючим, тобто наступний за близькістю розташування до поточного значення $\underset{\sim}{P}_{ij}^{\tau_f p}$.

Далі, за допомогою функції пошуку ідентифікуючої ХО (див. етап 2 та 3 в п. 3.3), тобто ознаки $IX^{c}_{ijNUM_{ij}}$, якій відповідно до функції, наприклад, F^{1} $\mathbf{(XP^{1}_{ij})}$ (тип якої визначається за ХО з підмножини $\mathbf{XP^{c}_{ij}}$) буде здійснено пошук додаткового терма, що слідує за ідентифікуючим XP^{1}_{ijs}.

Базуючись на (3.29) введемо множину всіх номерів допоміжних термів $\mathbf{NUM'}$ та підмножини таких номерів $\mathbf{NUM'_i}$

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{NUM'_i}\} = \{\mathbf{NUM'_1}\ ,\ \mathbf{NUM'_2}\ ,\ \ldots,\ \mathbf{NUM'_n}\},\quad (i=\overline{1,n}), \tag{4.1}$$

де $\mathbf{NUM'_i} \subseteq \mathbf{NUM'}$ визначимо як:

$$\mathbf{NUM'_i} = \{\bigcup_{j=1}^{m_i} NUM'_{ij}\} = \{NUM'_{i1},\ NUM'_{i2},\ \ldots,\ NUM'_{im_i}\},\ (j=\overline{1,m_i}), \tag{4.2}$$

а m_i – кількість номерів допоміжних термів.

Далі, кожне NUM'_{ij} представимо у вигляді

$$NUM'_{ij} = \begin{cases} s-1, \text{ якщо } (s=r_j) \vee (XP^1_{ijs-1} \le XP^1_{ijs+1}) \\ s+1, \text{ якщо } (s=1) \vee (XP^1_{ijs-1} > XP^1_{ijs+1}) \end{cases}. \tag{4.3}$$

Наприклад, якщо $i=3$ (тобто для кібератаки з ІД $CA_3 = CA_{SP} = SP$), $m_3 = 2$ ($P_{31} = P_{SPKOП} = КОП$ та $P_{32} = P_{SPKПОА} = КПОА$), $r_1 = 5$, $r_2 = 3$, то (4.3) з урахуванням (3.33) та прикладу етапа 3 в п. 3.3 і рис. 3.4 (для $\mathbf{T^e_{31}}$ і $\mathbf{T^e_{32}}$ ідентифікуючими будуть терми $\underset{\sim}{T}^e_{313}$ та $\underset{\sim}{T}^e_{323}$) можна записати як:

$$NUM'_{31} = \begin{cases} 3-1, \text{ якщо } (3=5) \vee (XP^1_{312} \le XP^1_{314}) \\ 3+1, \text{ якщо } (3=1) \vee (XP^1_{312} > XP^1_{314}) \end{cases}$$

або

$$NUM'_{31} = \begin{cases} 3-1, \text{ якщо } (3=5) \vee (2{,}441 \le 3{,}624) \\ 3+1, \text{ якщо } (3=1) \vee (2{,}441 > 3{,}624) \end{cases}.$$

Очевидно, що в наведеному прикладі відповідно до (4.3) для NUM'_{31} виконується перша умова, тобто $NUM'_{31} = 2$. Виходячи з цього, наступним за ідентифікуючим для $\mathbf{T^e_{31}}$ буде слідувати терм з $XP^1_{312} = 2{,}441$, тобто це $\underset{\sim}{T}^e_{312}$, який і є допоміжним.

Далі, за аналогією, визначимо

$$NUM'_{32} = \begin{cases} 3-1, \text{ якщо } (3=3) \vee (XP^1_{322} \le 0) \\ 3+1, \text{ якщо } (3=1) \vee (XP^1_{322} > 0) \end{cases}$$

або

$$NUM'_{32} = \begin{cases} 3-1, \text{ якщо } (3=3) \vee (1{,}267 \le 0) \\ 3+1, \text{ якщо } (3=1) \vee (1{,}267 > 0) \end{cases}.$$

У цьому випадку, відповідно до (4.3) також виконується перша умова, тобто $NUM'_{32} = 2$ і допоміжним для $\mathbf{T^e_{32}}$ буде терм з $XP^1_{322} = 1{,}267$, тобто $\underset{\sim}{T}^e_{322}$.

Визначення експертних коефіцієнтів параметрів

Етап 2 – визначення експертних коефіцієнтів параметрів. Для реалізації цього етапу введемо множину експертних коефіцієнтів **EC** (expert coefficient) та підмножини таких коефіцієнтів $\mathbf{EC_i}$

$$\begin{gathered}\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\mathbf{EC_i}\} = \\ \{\mathbf{EC_1}, \mathbf{EC_2}, \ldots, \mathbf{EC_n}\}, \\ (i = \overline{1,n}),\end{gathered} \tag{4.4}$$

де $\mathbf{EC_i} \subseteq \mathbf{EC}$ визначимо як:

$$\begin{gathered}\mathbf{EC_i} = \{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}}\mathbf{EC_{ij}}\} = \\ \{EC_{ij}^{min}, EC_{ij}^{max}\}, \\ (j = \overline{1,m_i}),\end{gathered} \tag{4.5}$$

при цьому $\mathbf{EC_i} \in \{EC_{ij}^{min}, EC_{ij}^{max}\}$, а EC_{ij}^{min} і EC_{ij}^{max} відповідно є мінімальними і максимальними елементами $(EC_{ij}^{min} \le EC_{ij}^{max})$ підмножини $\mathbf{EC_i}$, які в числовій формі характеризують рівень впевненості експерта щодо сформованих значень поточних величин відносно лінгвістичних еталонів. Можна також зазначити, що експертний коефіцієнт EC_{ij}^{max} характеризує рівень упевненості експерта відносно ідентифікуючого терма і за певною аналогією його можна порівняти з вірогідністю сформованих поточних значень параметрів відносно їх еталонів.

Наприклад, якщо $i = 3$ (тобто для кібератаки з ІД $CA_3 = CA_{SP} = SP$), $m_3 = 2$ ($P_{31} = P_{SPKOП} = КОП$ та $P_{32} = P_{SPKПОА} = КПОА$), $r_1 = 5$, $r_2 = 3$ і з використанням ідентифікуючої ознаки $IX^1_{ijNUM_{ij}} = XP^1_{ijs}$ (див.

(3.33) в п. 3.3)) та визначеними (на етапі 1 з урахуванням (4.3)) допоміжними термами XP^1_{312} і XP^1_{322} розрахуємо нормуючі коефіцієнти за формулою

$$k_{ij} = 1/(IX^1_{ijNUM_{ij}} + IX^1_{ijNUM'_{ij}}), \quad (i=\overline{1,n},\ j=\overline{1,m_i}). \tag{4.6}$$

Далі, для наведеного прикладу отримаємо

$$k_{31} = 1/(XP^1_{313} + XP^1_{312}) = 1/(0{,}981 + 2{,}441) = 0{,}292,$$

а також

$$k_{32} = 1/(XP^1_{323} + XP^1_{322}) = 1/(0{,}443 + 1{,}267) = 0{,}585.$$

З урахуванням (4.6) запишемо (4.5) у наступному вигляді

$$EC^{max}_{ij} = 1 - k_{ij} \cdot IX^1_{ijNUM_{ij}} \text{ та } EC^{min}_{ij} = 1 - k_{ij} \cdot IX^1_{ijNUM_{ij}}, \quad (i=\overline{1,n},\ j=\overline{1,m_i}). \tag{4.7}$$

На основі (4.7) обчислимо конкретні значення EC^{max}_{31}, EC^{min}_{31} та EC^{max}_{32}, EC^{min}_{32} відповідно, тобто

$$EC^{min}_{31} = 1 - k_{31} \cdot XP^1_{312},\ EC^{max}_{31} = 1 - k_{31} \cdot XP^1_{313},$$

$EC^{min}_{31} = 1 - 0{,}292 \cdot 2{,}441 = 0{,}287$, $EC^{max}_{31} = 1 - 0{,}292 \cdot 0{,}981 = 0{,}713$ та

$$EC^{min}_{32} = 1 - k_{32} \cdot XP^1_{322},\ EC^{max}_{32} = 1 - k_{32} \cdot XP^1_{323},$$

$EC^{min}_{32} = 1 - 0{,}585 \cdot 1{,}267 = 0{,}259$, $EC^{max}_{32} = 1 - 0{,}585 \cdot 0{,}443 = 0{,}741.$

Зазначимо, що $EC^{max}_{31} = 0{,}713$ та $EC^{max}_{32} = 0{,}741$ будуть відображати рівень упевненості експерта, щодо значень сформованих поточних величин $\underset{\sim}{P}^{\tau_f p}_{31}$ і $\underset{\sim}{P}^{\tau_f p}_{32}$ відносно їх еталонних термів, що відповідно входять в $\mathbf{T^e_{31}}$ і $\mathbf{T^e_{32}}$.

Визначення експертного коефіцієнта кібератаки

Етап 3 – визначення експертного коефіцієнта кібератаки. Для реалізації цього етапу введемо множину експертних коефіцієнтів кібератак $\mathbf{EC^{CA}}$ (expert coefficients of cyberattacks) та підмножину таких коефіцієнтів $\mathbf{EC^{CA}_i}$

$$\mathbf{EC_i^{CA}} = \{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}} \mathbf{EC_i^{CA}}\} = \{EC_1^{CA},\ EC_2^{CA},\ ...,\ EC_n^{CA}\},\ (i=\overline{1,n}), \tag{4.8}$$

де $\mathbf{EC_i} \subseteq \mathbf{EC}$, а також визначимо, що

$$EC_i^{CA} = \frac{1}{m_i}\sum_{j=1}^{m_i} EC_{ij}^{max}. \tag{4.9}$$

Наприклад, якщо $i=3$ (тобто для кібератаки з ІД $CA_3 = CA_{SP} = SP$), $m_3 = 2$ ($P_{31} = P_{SPKOП} = KOП$ та $P_{32} = P_{SPKПОА} = KПОА$), то з використанням (4.9) розрахуємо

$$EC_3^{CA} = (EC_{31}^{max} + EC_{32}^{max})/2 = (0{,}713 + 0{,}741)/2 = 0{,}727.$$

Таким чином формується вся підмножина $\mathbf{EC^{CA}}$, члени якої є дефазифікованими (числовими) значеннями, що характеризують лінгвістичні оцінки експертів щодо рівня аномального стану в поточному середовищі ($\mathbf{P^{\tau_f}}$) і може характеризувати рівень упевненості експерта або бути використаним за аналог вірогідності відносно його суджень щодо можливих кібератак. Отримані коефіцієнти можна застосувати для формування умовних виразів з підмножини $\mathbf{DR_{3\ 13}}$ детекційного підсередовища ($\mathbf{DR_{SP}}$) (див. приклад в п. 4.2), наприклад, для виявлення спуфінгу: «Якщо поточний параметр «Кількість одночасних підключень до сервера» в момент часу τ_f найближчий до еталону «Середнє» (з експертним коефіцієнтом $0{,}713$) і поточний параметр «Кількість пакетів з однаковою адресою відправника та одержувача» в момент часу τ_f найближчий до еталону «Велике» (з експертним коефіцієнтом $0{,}741$), то рівень аномального стану породженого спуфінгом буде «Більш високим ніж низьким» (з експертним коефіцієнтом кібератаки $0{,}727$)», що з урахуванням (4.33) можна записати, як

$$if\ (E(NUM_{SPKOП},3)\big|_{0{,}713} \wedge E(NUM_{SPKПОА},3)\big|_{0{,}741})\ then\ "БВН"\big|_{0{,}727}.$$

Таким чином, запропонований МДП, який за рахунок визначення допоміжного терму, експертних коефіцієнтів параметрів та кібератак, дозволяє отримати числові значення, що конкретизують лінгвістичні оцінювання експертів щодо рівня аномального стану, породженого певним атакуючим середовищем.

Далі, для наступного виявлення аномалій в ІС потрібно визначити необхідний набір базових детекційних правил, що створюють необхідне детекційне середовище, яке буде визначати рівень аномального стану в ІС.

4.2. Метод формування детекційного середовища для систем виявлення вторгнень

На основі запропонованої КМАС (див. п. 2.1 та [1-3]) і методів МФЕС (див. п. 2.2 та [6-9]) і МДП (див. п. 4.1), а також з урахуванням [10, 11] для побудови підмножин базових детекційних правил $\mathbf{DR}_i$ (див. вираз (2.19) в п. 2.1 та [1]), розробимо відповідний метод формування базових детекційних середовищ (МФДС) [12] для систем виявлення вторгнень, що орієнтовані на функціонування в нечітких умовах. Цей метод довзолить формалізувати процес отримання множини правил, які використовуються для виявлення *i*-ї кібератаки на основі параметричних підсередовищ різної розмірності [1-3]. За допомогою МФДС (при вирішення задач виявлення кібератак) можна ефективно детектувати рівень аномального стану, що характерний визначеному типу атак відносно конкретного гетерогенного середовища оточення в заданий проміжок часу.

Запропонований МФДС базується на трьох етапах:

- формування підмножин ідентифікаторів аномальності;
- формування вирішальних функцій;
- формування умовних виразів детекційного середовища.

Опишемо кожний з визначених етапів.

Формування підмножин ідентифікаторів аномальності

Етап 1 – формування підмножин ідентифікаторів аномальності. Побудова підмножини $\mathbf{IA}_i$ здійснюється на основі множини всіх можливих ІД аномальності $\mathbf{IA}$, що представлені як

$$\mathbf{IA} = \{\bigcup_{o=1}^{\xi} IA_o\} = \{IA_1, IA_2, ..., AI_\xi\}, \quad (o = \overline{1,\xi}), \tag{4.10}$$

та за допомогою яких (у лінгвістичній формі) можна віборазити можливі рівні аномального стану в *m*-вимірному гетерогенному параметричному середовищі (**P**), яке може бути утворено кібератакою з ІД CA_i (див. п. 2.1 та [1]), а ξ – кількість ІД аномальності.

Наприклад, при $\xi = 9$ відповідно до (4.10) множину **IA** можна представити наступним чином:

$$\mathbf{IA} = \{\bigcup_{o=1}^{9} IA_o\} = \{IA_1, IA_2, ..., AI_9\} = \tag{4.11}$$

$$\{IA_Н, IA_{БНВ}, IA_{НС}, IA_С, IA_{ВС}, IA_{ББН}, IA_В, IA_П, IA_Г\} =$$

$$\{"Н", "БНВ", "НС", "С", "ВС", "ББН", "В", "П", "Г"\},$$

де:

- $IA_1 = IA_Н = "Н"$,
- $IA_2 = IA_{БНВ} = "БНВ"$,
- $IA_3 = IA_{НС} = "НС"$,
- $IA_4 = IA_С = "С"$,
- $IA_5 = IA_{ВС} = "ВС"$,
- $IA_6 = IA_{ББН} = "ББН"$,
- $IA_7 = IA_В = "В"$,
- $IA_8 = IA_П = "П"$,
- $IA_9 = IA_Г = "Г"$

відповідно є ІД аномальності, за допомогою яких в лінгвістичних формах:

- «НИЗЬКИЙ» або «НИЗКИЙ (Н)» (при $o = 1$),
- «БІЛЬШ НИЗЬКИЙ НІЖ ВИСОКИЙ» або «БОЛЬШЕ НИЗКИЙ ЧЕМ ВЫСОКИЙ (БНВ)» (при $o = 2$),
- «НИЖЧЕ СЕРЕДНЬОГО» або «НИЖЕ СРЕДНЕГО (НС)» (при $o = 3$),

- «СЕРЕДНІЙ» або «СРЕДНИЙ (С)» (при $o = 4$),
- «ВИЩЕ СЕРЕДНЬОГО» або «ВЫШЕ СРЕДНЕГО (ВС)» (при $o = 5$),
- «БІЛЬШ ВИСОКИЙ НІЖ НИЗЬКИЙ» або «БОЛЬШЕ ВЫСОКИЙ ЧЕМ НИЗКИЙ (БВН)» (при $o = 6$),
- «ВИСОКИЙ» або «ВЫСОКИЙ (В)» (при $o = 7$),
- «МЕЖЕВИЙ» або «ПРЕДЕЛЬНЫЙ (П)» (при $o = 8$),
- «ГРАНИЧНИЙ» або «ГРАНИЧНЫЙ (Г)» (при $o = 9$),

можна відобразити можливі рівні аномальності.

Далі, сформуємо підмножини ІД аномальності для підмножини правил $\mathbf{DR_i}$, що входять в детекційне середовище ($\mathbf{DR}$) (див. п. 2.1) тобто:

$$\begin{gathered}\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{IA_i}\} = \\ \{\mathbf{IA_1}, \mathbf{IA_2}, \ldots, \mathbf{IA_n}\}, \\ (i = \overline{1,n}),\end{gathered} \tag{4.12}$$

де $\mathbf{IA_i} \subseteq \mathbf{IA}$ визначимо як:

$$\begin{gathered}\mathbf{IA_i} = \{\bigcup_{u=1}^{v_i} IA_{iu}\} = \\ \{IA_{i1}, IA_{i2}, ..., IA_{iv_i}\}, \\ (u = \overline{1,v_i}),\end{gathered} \tag{4.13}$$

при цьому v_i показує кількість ІД аномальності, шляхом яких в лінгвістичній формі можна відобразити можливі рівні аномальності, породжені кібератакою з ІД CA_i. Таким чином, вираз (4.12) з урахуванням (4.13) представимо у наступному вигляді:

$$\begin{gathered}\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{IA_i}\} = \{\bigcup_{i=1}^{n} \{\bigcup_{u=1}^{v_i} IA_{iu}\}\} = \\ \{\{IA_{11}, IA_{12}, ..., IA_{1v_1}\}, \\ \{IA_{21}, IA_{22}, ..., IA_{2v_2}\}, \\ \ldots,\end{gathered} \tag{4.14}$$

$$\{ IA_{n1}, IA_{n2}, ..., AI_{nv_n} \}\}.$$

Наприклад, при $n = 3$ (тобто для кібератак з ІД $CA_1 = CA_{SN} = SN$, $CA_2 = CA_{DS} = DS$ і $CA_3 = CA_{SP} = SP$), $v_1 = v_2 = v_3 = 5$ і на основі (4.10) визначимо необхідні ІД для відображення відповідного рівня аномальності. Тоді вираз (4.14) з урахуванням (4.11) буде мати наступний вигляд:

$$\begin{gathered}
\{\bigcup_{\mathbf{i=1}}^{\mathbf{3}} \mathbf{IA_i}\} = \{\bigcup_{i=1}^{3}\{\bigcup_{u=1}^{v_i} IA_{iu}\}\} = \\
\{\{ IA_{11}, IA_{12}, IA_{13}, IA_{14}, IA_{15} \}, \\
\{ IA_{21}, IA_{22}, IA_{23}, IA_{24}, IA_{25} \}, \\
\{ IA_{31}, IA_{32}, IA_{33}, IA_{34}, IA_{35} \}\} = \\
\{\{ IA_{SNH}, IA_{SNБНВ}, IA_{SNББН}, IA_{SNB}, IA_{SNП} \}, \\
\{ IA_{DSH}, IA_{DSБНВ}, IA_{DSББН}, IA_{DSB}, IA_{DSП} \}, \\
\{ IA_{SPH}, IA_{SPБНВ}, IA_{SPББН}, IA_{SPB}, IA_{SPП} \}\} = \\
\{\{"Н", "БНВ", "ББН", "В", "П"\}, \\
\{"Н", "БНВ", "ББН", "В", "П"\}, \\
\{"Н", "БНВ", "ББН", "В", "П"\}\},
\end{gathered} \tag{4.15}$$

де:

- $IA_{11} = IA_{SNH} = "Н"$,
- $IA_{12} = IA_{SNБНВ} = "БНВ"$,
- $IA_{13} = IA_{SNББН} = "ББН"$,
- $IA_{14} = IA_{SNB} = "В"$,
- $IA_{15} = IA_{SNП} = "П"$ відповідно є ІД таких станів аномальності в атакуючому середовищі ($\mathbf{CA}^{\tau_f}$), які відображають різну ступінь упевненості експерта щодо дії кібератаки з ІД $CA_1 = CA_{SN}$ (див. п. 2.1);
- $IA_{21} = IA_{DSH} = "Н"$,
- $IA_{22} = IA_{DSБНВ} = "БНВ"$,
- $IA_{23} = IA_{DSББН} = "ББН"$,
- $IA_{24} = IA_{DSB} = "В"$,

- $IA_{25} = IA_{DSП} = "П"$ відповідно є ІД таких станів аномальності в атакуючому середовищі ($\mathbf{CA}^{\tau_f}$), які відображають різну ступінь упевненості експерта щодо дії кібератаки з ІД $CA_2 = CA_{DS}$;
- $IA_{31} = IA_{SPH} = "Н"$,
- $IA_{32} = IA_{SPБНВ} = "БНВ"$,
- $IA_{33} = IA_{SPББН} = "ББН"$,
- $IA_{34} = IA_{SPB} = "В"$,
- $IA_{35} = IA_{SPП} = "П"$ відповідно є ІД таких станів аномальності в атакуючому середовищі ($\mathbf{CA}^{\tau_f}$), які відображають різну ступінь упевненості експерта щодо дії кібератаки з ІД $CA_3 = CA_{SP}$.

Формування вирішальних функцій

Етап 2 – формування вирішальних функцій. Для реалізації цього етапу введемо множину всіх аргументів вирішальних функцій $\mathbf{AF}$ та підмножину таких аргументів $\mathbf{AF_i}$

$$\{\bigcup_{i=1}^{n} \mathbf{AF_i}\} = \{\mathbf{AF_1}, \mathbf{AF_2}, \ldots, \mathbf{AF_n}\}, \quad (i = \overline{1,n}), \tag{4.16}$$

де $\mathbf{AF_i} \subseteq \mathbf{AF}$, визначимо як:

$$\mathbf{AF_i} = \{\bigtimes_{a=1}^{w_i} \mathbf{AF_{ia}}\} = \{\mathbf{AF_{i1}} \times \mathbf{AF_{i2}} \times \ldots \times \mathbf{AF_{iw_i}}\}, \quad (a = \overline{1,w_i}), \tag{4.17}$$

при цьому w_i – кількість підмножин аргументів вирішальних функцій, які використовуються для виявлення *i*-ї кібератаки, а символ × позначає прямий добуток множин. З урахуванням (4.17) формулу (4.16) запишемо у наступному вигляді:

$$\{\bigcup_{i=1}^{n}\mathbf{AF_i}\} = \{\bigcup_{i=1}^{n}\{\times_{a=1}^{w_i}\mathbf{AF_{ia}}\}\} =$$
$$\{\{\mathbf{AF_{11}},\ \mathbf{AF_{12}}, ...,\ \mathbf{AF_{1w_1}}\}\times$$
$$\{\mathbf{AF_{21}},\ \mathbf{AF_{22}}, \ldots,\ \mathbf{AF_{2w_2}}\}\times \qquad (4.18)$$
$$\ldots\times$$
$$\{\mathbf{AF_{n1}},\ \mathbf{AF_{n2}}, \ldots,\ \mathbf{AF_{nw_n}}\},$$
$$(i=\overline{1,n},\ a=\overline{1,w_i}).$$

Підмножину $\mathbf{AF_{ia}} \subseteq \mathbf{AF_i}$ визначимо як:

$$\mathbf{AF_{ia}} = \{\bigcup_{s=1}^{r_j} AF_{ias}\} =$$
$$\{AF_{ia1},\ AF_{ia2},\ ...,\ AF_{iar_j}\}, \qquad (4.19)$$
$$(s=\overline{1,r_j}),$$

де r_j – кількість членів в $\mathbf{AF_{ia}}$ (що відображає кількість членів в $\mathbf{T_{ij}^e}$ (див. (2.13)).

Тоді, вираз (4.18) з урахуванням (4.19) приймає наступний вигляд:

$$\{\bigcup_{i=1}^{n}\mathbf{AF_i}\} = \{\bigcup_{i=1}^{n}\{\times_{a=1}^{w_i}\mathbf{AF_{ia}}\}\} =$$
$$\{\bigcup_{i=1}^{n}\{\times_{a=1}^{w_i}\{\bigcup_{s=1}^{r_j} AF_{ias}\}\}\} =$$
$$\{\{\{AF_{111},\ AF_{112},\ ...,\ AF_{11r_j}\}\times\{AF_{121},\ AF_{122},\ ...,\ AF_{12r_j}\}\times...$$
$$\times\{AF_{1w_1 1},\ AF_{1w_1 2},\ ...,\ AF_{1w_1 r_j}\}\}, \qquad (4.20)$$
$$\{\{AF_{211},\ AF_{212},\ ...,\ AF_{21r_j}\}\times\{AF_{221},\ AF_{222},\ ...,\ AF_{22r_j}\}\times...$$
$$\times\{AF_{2w_2 1},\ AF_{2w_2 2},\ ...,\ AF_{2w_2 r_j}\}\},\ \mathbf{...},$$
$$\{\{AF_{n11},\ AF_{n12},\ ...,\ AF_{n1r_j}\}\times\{AF_{n21},\ AF_{n22},\ ...,\ AF_{n2r_j}\}\times...$$
$$\times\{AF_{nw_n 1},\ AF_{nw_n 2},\ ...,\ AF_{nw_n r_j}\}\}\} =$$

$$\{\{\langle AF_{111}, AF_{121}, ..., AF_{1w_1 1}\rangle, \langle AF_{111}, AF_{121}, ..., AF_{1w_1 2}\rangle, ...,$$
$$\langle AF_{111}, AF_{121}, ..., AF_{1w_1 r_1}\rangle,$$
$$\langle AF_{111}, AF_{122}, ..., AF_{1w_1 1}\rangle, \langle AF_{111}, AF_{122}, ..., AF_{1w_1 2}\rangle,$$
$$..., \langle AF_{111}, AF_{122}, ..., AF_{1w_1 r_1}\rangle, ...,$$
$$\langle AF_{111}, AF_{12r_2}, ..., AF_{1w_1 1}\rangle, \langle AF_{111}, AF_{12r_2}, ..., AF_{1w_1 2}\rangle,$$
$$..., \langle AF_{111}, AF_{12r_2}, ..., AF_{1w_1 r_1}\rangle,$$
$$\langle AF_{112}, AF_{121}, ..., AF_{1w_1 1}\rangle, \langle AF_{112}, AF_{121}, ..., AF_{1w_1 2}\rangle,$$
$$..., \langle AF_{112}, AF_{121}, ..., AF_{1w_1 r_1}\rangle,$$
$$\langle AF_{112}, AF_{122}, ..., AF_{1w_1 1}\rangle, \langle AF_{112}, AF_{122}, ..., AF_{1w_1 2}\rangle,$$
$$..., \langle AF_{112}, AF_{122}, ..., AF_{1w_1 r_1}\rangle, ...,$$
$$\langle AF_{112}, AF_{12r_2}, ..., AF_{1w_1 1}\rangle, \langle AF_{112}, AF_{12r_2}, ..., AF_{1w_1 2}\rangle,$$
$$..., \langle AF_{112}, AF_{12r_2}, ..., AF_{1w_1 r_1}\rangle, ...,$$
$$\langle AF_{11r_1}, AF_{121}, ..., AF_{1w_1 1}\rangle, \langle AF_{11r_1}, AF_{121}, ..., AF_{1w_1 2}\rangle,$$
$$..., \langle AF_{11r_1}, AF_{121}, ..., AF_{1w_1 r_1}\rangle,$$
$$\langle AF_{11r_1}, AF_{122}, ..., AF_{1w_1 1}\rangle, \langle AF_{11r_1}, AF_{122}, ..., AF_{1w_1 2}\rangle,$$
$$..., \langle AF_{11r_1}, AF_{122}, ..., AF_{1w_1 r_1}\rangle, ...,$$
$$\langle AF_{11r_1}, AF_{12r_2}, ..., AF_{1w_1 1}\rangle, \langle AF_{11r_1}, AF_{12r_2}, ..., AF_{1w_1 2}\rangle,$$
$$..., \langle AF_{11r_1}, AF_{12r_2}, ..., AF_{1w_1 r_1}\rangle\},$$
$$...,$$

$$\{\langle AF_{n11},\ AF_{n21},\ ...,\ AF_{nw_n1}\rangle, \langle AF_{n11},\ AF_{n21},\ ...,\ AF_{nw_n2}\rangle,$$
$$...,$$
$$\langle AF_{n11},\ AF_{n21},\ ...,\ AF_{nw_nr_j}\rangle,$$
$$\langle AF_{n11},\ AF_{n22},\ ...,\ AF_{nw_n1}\rangle, \langle AF_{n11},\ AF_{n22},\ ...,\ AF_{nw_n2}\rangle,$$
$$...,$$
$$\langle AF_{n11},\ AF_{n22},\ ...,\ AF_{nw_nr_j}\rangle,\ ...,$$
$$\langle AF_{n11},\ AF_{n2r_2},\ ...,\ AF_{nw_n1}\rangle, \langle AF_{n11},\ AF_{n2r_2},\ ...,\ AF_{nw_n2}\rangle,$$
$$...,$$
$$\langle AF_{n11},\ AF_{n2r_2},\ ...,\ AF_{nw_nr_j}\rangle,$$
$$\langle AF_{n12},\ AF_{n21},\ ...,\ AF_{nw_n1}\rangle, \langle AF_{n12},\ AF_{n21},\ ...,\ AF_{nw_n2}\rangle,$$
$$...,$$
$$\langle AF_{n12},\ AF_{n21},\ ...,\ AF_{nw_nr_j}\rangle,$$
$$\langle AF_{n12},\ AF_{n22},\ ...,\ AF_{nw_n1}\rangle, \langle AF_{n12},\ AF_{n22},\ ...,\ AF_{nw_n2}\rangle,$$
$$...,$$
$$\langle AF_{n12},\ AF_{n22},\ ...,\ AF_{nw_nr_j}\rangle,\ ...,$$
$$\langle AF_{n12},\ AF_{n2r_2},\ ...,\ AF_{nw_n1}\rangle, \langle AF_{n12},\ AF_{n2r_2},\ ...,\ AF_{nw_n2}\rangle,$$
$$...,$$
$$\langle AF_{n12},\ AF_{n2r_2},\ ...,\ AF_{nw_nr_j}\rangle,\ ...,$$
$$\langle AF_{n1r_1},\ AF_{n21},\ ...,\ AF_{nw_n1}\rangle, \langle AF_{n1r_1},\ AF_{n21},\ ...,\ AF_{nw_n2}\rangle,$$
$$...,$$
$$\langle AF_{n1r_1},\ AF_{n21},\ ...,\ AF_{nw_nr_j}\rangle,$$
$$\langle AF_{n1r_1},\ AF_{n22},\ ...,\ AF_{nw_n1}\rangle, \langle AF_{n1r_1},\ AF_{n22},\ ...,\ AF_{nw_n2}\rangle,$$
$$...,$$
$$\langle AF_{n1r_1},\ AF_{n22},\ ...,\ AF_{nw_nr_j}\rangle,\ ...,$$
$$\langle AF_{n1r_1}, AF_{n2r_2},\ ...,\ AF_{nw_n1}\rangle, \langle AF_{n1r_1}, AF_{n2r_2},\ ...,\ AF_{nw_n2}\rangle,$$
$$...,$$
$$\langle AF_{n1r_1}, AF_{n2r_2},\ ...,\ AF_{nw_nr_j}\rangle\}\}=$$
$$\{\{\langle \mathbf{SAF_{11}}\rangle, \langle \mathbf{SAF_{12}}\rangle, ..., \langle \mathbf{SAF_{1w_1}}\rangle\}, ...,$$

$$\{\langle \mathbf{SAF_{i1}} \rangle, \langle \mathbf{SAF_{i2}} \rangle, \ldots, \langle \mathbf{SAF_{iw_i}} \rangle\},$$

$$\ldots,$$

$$\{\langle \mathbf{SAF_{n1}} \rangle, \langle \mathbf{SAF_{n2}} \rangle, \ldots, \langle \mathbf{SAF_{nw_n}} \rangle\}\},$$

де для наочності використовуються кутові дужки "⟨" та "⟩", які виокремлюють підмножини аргументів вирішальних функцій ($\mathbf{SAF_{ia}}$), що відображають значення термів $\mathbf{T_{ij}^{ep}}$.

З урахуванням (4.20) визначимо, що для виявлення *i*-ї кібератаки загальна кількість підмножин аргументів обчислюється за формулою

$$w_i = \prod_{j=1}^{m_i} r_j, \quad (j = \overline{1, m_i}). \tag{4.21}$$

Тоді, (4.20) з урахуванням (4.21) можна записати у наступному вигляді

$$\{\bigcup_{i=1}^{n} \mathbf{AF_i}\} = \{\bigcup_{i=1}^{n} \{\bigcup_{a=1}^{w_i} \langle \mathbf{SAF_{ia}} \rangle\}\}, \quad (a = \overline{1, w_i}). \tag{4.22}$$

Далі, введемо множину всіх бінарних вирішальних функцій **SF** та підмножину таких функцій $\mathbf{SF_i}$

$$\{\bigcup_{i=1}^{n} \mathbf{SF_i}\} = \{\mathbf{SF_1}, \mathbf{SF_2}, \ldots, \mathbf{SF_n}\}, \quad (i = \overline{1, n}), \tag{4.23}$$

де $\mathbf{SF_i} \subseteq \mathbf{SF}$, $(i = \overline{1, n})$ визначимо, як

$$\mathbf{SF_i} = \{\bigcup_{a=1}^{w_i} SF_{ia}\} = \{SF_{i1}, SF_{i2}, \ldots, SF_{iw_i}\}, \text{ а} \tag{4.24}$$

$$SF_{ia} = SF_{ia}(\mathbf{SAF_{ia}}). \tag{4.25}$$

Зазначимо, що функція SF_{ia} визначає взаємозв'язки в $\mathbf{SAF_{ia}}$, які формуються, наприклад, за участю експерта у вигляді логічних ланцюжків (заснованих на диз'юнкціях та кон'юнкціях) для наступної

побудови детекційних виразів, орієнтованих на виявлення *i*-ї кібератаки.

Експерт для отримання конкретної множини бінарних функцій, що виявляє *i*-ту кібератаку, створює відповідний шаблон, який визначає взаємозв'язки в $\mathbf{SAF_{ia}}$.

Наприклад, якщо

$$\mathbf{SAF_{ia}} = \langle\, AF_{111},\, AF_{112},\, AF_{113} \,\rangle,$$

а шаблони мають вигляд

$$\langle\, AF \wedge AF \wedge AF \,\rangle$$

або

$$\langle\, AF \wedge (AF \vee AF) \,\rangle,$$

то відповідно

$$SF_{11} = AF_{111} \wedge AF_{112} \wedge AF_{113}$$

або

$$SF_{11} = AF_{111} \wedge (AF_{112} \vee AF_{113}).$$

Конкретні значення елементів підмножини $\mathbf{AF_i}$ $(i = \overline{1,n})$ формуються на основі бінарної функції еквівалентності $E(x,\, y)$, яка приймає значення 1 тільки при рівності x та y, тобто:

$$E(x,\, y) = \begin{cases} 1, \text{ якщо } x = y \\ 0, \text{ якщо } x \neq y. \end{cases} \qquad (4.26)$$

Виходячи з цього визначимо, що $AF_{ias} = E\,(NUM_{ia},\, s)$, а за аргументи в $E(x,\, y)$ використовуються індекси нечітких термів $\mathbf{T_{ij}^{ep}}$ та $\mathbf{P_i^{\tau_f p}}$.

Розглянемо приклад формування вирішальних функцій при $n = 3,\ \ i = \overline{1,3}$ ($\mathbf{CA_1^{\tau_f}} = \mathbf{CA_{SN}^{\tau_f}} = \mathbf{SN^{\tau_f}}$, $\mathbf{CA_2^{\tau_f}} = \mathbf{CA_{DS}^{\tau_f}} = \mathbf{DS^{\tau_f}}$ та $\mathbf{CA_3^{\tau_f}} = \mathbf{CA_{SP}^{\tau_f}} = \mathbf{SP^{\tau_f}}$), $m_1 = m_3 = 2,\ \ m_2 = 3,\ \ r_1 = 5,\ \ r_2 = r_3 = 3$ (див. приклад для (2.15)).

Відповідно до (4.21)

$$w_1 = \prod_{j=1}^{m_1} r_j = r_1 \cdot r_2 = 5 \cdot 3 = 15,$$

$$w_2 = \prod_{j=1}^{m_2} r_j = r_1 \cdot r_2 \cdot r_3 = 5 \cdot 3 \cdot 3 = 45,$$

$$w_3 = \prod_{j=1}^{m_3} r_j = r_1 \cdot r_2 = 5 \cdot 3 = 15,$$

а (4.20) можна визначити як:

$$\{\bigcup_{\mathbf{i=1}}^{3} \mathbf{AF_i}\} = \{\mathbf{AF_1}\ ,\ \mathbf{AF_2}\ ,\ \mathbf{AF_3}\} =$$

$$\{\bigcup_{\mathbf{i=1}}^{3} \{\bigtimes_{\mathbf{a=1}}^{\mathbf{w_i}} \mathbf{AF_{ia}}\}\} = \{\bigcup_{i=1}^{3} \{\bigtimes_{a=1}^{w_i} \{\bigcup_{s=1}^{r_j} AF_{ias}\}\}\} =$$

$$\{\{\{ AF_{111}, AF_{112}, AF_{113}, AF_{114}, AF_{115} \} \times \{ AF_{121}, AF_{122}, AF_{123} \}\},$$
$$\{\{ AF_{211}, AF_{212}, AF_{213}, AF_{214}, AF_{215} \} \times$$
$$\{ AF_{221}, AF_{222}, AF_{223} \} \times \{ AF_{231}, AF_{232}, AF_{233} \}\},$$
$$\{\{ AF_{311}, AF_{312}, AF_{313}, AF_{314}, AF_{315} \} \times \{ AF_{321}, AF_{322}, AF_{323} \}\}\} =$$
$$\{\langle AF_{111}, AF_{121} \rangle, \langle AF_{112}, AF_{121} \rangle, \langle AF_{113}, AF_{121} \rangle,$$
$$\langle AF_{114}, AF_{121} \rangle, \langle AF_{115}, AF_{121} \rangle, \ ...,$$
$$\langle AF_{111}, AF_{123} \rangle, \langle AF_{112}, AF_{123} \rangle, \langle AF_{113}, AF_{123} \rangle,$$
$$\langle AF_{114}, AF_{123} \rangle, \langle AF_{115}, AF_{123} \rangle\},$$
$$\{\langle AF_{211}, AF_{221}, AF_{231} \rangle, \langle AF_{212}, AF_{221}, AF_{231} \rangle, \qquad (4.27)$$
$$\langle SF_{213}, AF_{221}, AF_{231} \rangle,$$
$$\langle AF_{214}, AF_{221}, AF_{231} \rangle, \langle AF_{215}, AF_{221}, AF_{231} \rangle \ ...,$$
$$\langle AF_{211}, AF_{223}, AF_{233} \rangle, \langle AF_{212}, AF_{223}, AF_{233} \rangle,$$
$$\langle AF_{213}, AF_{223}, AF_{233} \rangle,$$
$$\langle AF_{214}, AF_{223}, AF_{233} \rangle, \langle AF_{215}, AF_{223}, AF_{233} \rangle\},$$
$$\{\langle AF_{311}, AF_{321} \rangle, \langle AF_{312}, AF_{321} \rangle, \langle AF_{313}, AF_{321} \rangle,$$
$$\langle AF_{314}, AF_{321} \rangle, \langle AF_{315}, AF_{321} \rangle, \ ...,$$
$$\langle AF_{311}, AF_{323} \rangle, \langle AF_{312}, AF_{323} \rangle, \langle AF_{313}, AF_{323} \rangle,$$
$$\langle AF_{314}, AF_{323} \rangle, \langle AF_{315}, AF_{323} \rangle\} =$$
$$\{\{\langle \mathbf{SAF_{11}} \rangle, \langle \mathbf{SAF_{12}} \rangle, \ldots, \langle \mathbf{SAF_{1\ 15}} \rangle\},$$
$$\{\langle \mathbf{SAF_{21}} \rangle, \langle \mathbf{SAF_{22}} \rangle, \ldots, \langle \mathbf{SAF_{2\ 45}} \rangle\},$$
$$\{\langle \mathbf{SAF_{31}} \rangle, \langle \mathbf{SAF_{32}} \rangle, \ldots, \langle \mathbf{SAF_{3\ 15}} \rangle\}\}.$$

У п. 2.1 визначено, що для виявлення кібератак «Сканування портів (SN)» ($\mathbf{CA}_{\mathbf{1}}^{\boldsymbol{\tau}_{\mathbf{f}}} = \mathbf{CA}_{\mathbf{SN}}^{\boldsymbol{\tau}_{\mathbf{f}}} = \mathbf{SN}^{\boldsymbol{\tau}_{\mathbf{f}}}$) та «Спуфінг (SP)» ($\mathbf{CA}_{\mathbf{3}}^{\boldsymbol{\tau}_{\mathbf{f}}} = \mathbf{CA}_{\mathbf{SP}}^{\boldsymbol{\tau}_{\mathbf{f}}} = \mathbf{SP}^{\boldsymbol{\tau}_{\mathbf{f}}}$) необхідно одночасно використовувати два параметри, які визначають *2*-вимірне параметричне підсередовище ($\mathbf{P_i} = \mathbf{P_1} = \mathbf{P_{SN}}$ та $\mathbf{P_i} = \mathbf{P_3} = \mathbf{P_{SP}}$) (КВК-ВВК-підсередовище та КОП-КПОА-підсередовище), а для кібератаки «Відмова в обслуговуванні (DS)» ($\mathbf{CA}_{\mathbf{2}}^{\boldsymbol{\tau}_{\mathbf{f}}} = \mathbf{CA}_{\mathbf{DS}}^{\boldsymbol{\tau}_{\mathbf{f}}} = \mathbf{DS}^{\boldsymbol{\tau}_{\mathbf{f}}}$) – три параметри, які визначають *3*-вимірне параметричне підсередовище ($\mathbf{P_i} = \mathbf{P_2} = \mathbf{P_{DS}}$) (КОП-СОЗ-ЗМЗ-підсередовище) (див. (2.9)).

Експерт для отримання контретної множини функцій, які виявляють SN та SP створює шаблон $\langle\ AF \wedge AF\ \rangle$, а для DS – $\langle\ AF \wedge (AF \vee AF)\ \rangle$.

Далі, відповідно до сформованих шаблонів, а також (4.24) та (4.27) визначимо:

$$\mathbf{SF_1} = \{\bigcup_{a=1}^{w_1} SF_{1a}\} =$$

$$\{(E(NUM_{11}, 1) \wedge E(NUM_{12}, 1)),$$
$$(E(NUM_{11}, 2) \wedge E(NUM_{12}, 1)),$$
$$(E(NUM_{11}, 3) \wedge E(NUM_{12}, 1)),$$
$$(E(NUM_{11}, 4) \wedge E(NUM_{12}, 1)),$$
$$(E(NUM_{11}, 5) \wedge E(NUM_{12}, 1))\},$$
$$\{(E(NUM_{11}, 1) \wedge E(NUM_{12}, 2)),$$
$$(E(NUM_{11}, 2) \wedge E(NUM_{12}, 2)),$$
$$(E(NUM_{11}, 3) \wedge E(NUM_{12}, 2)),$$
$$(E(NUM_{11}, 4) \wedge E(NUM_{12}, 2)),$$
$$(E(NUM_{11}, 5) \wedge E(NUM_{12}, 2))\},$$
$$\{(E(NUM_{11}, 1) \wedge E(NUM_{12}, 3)),$$
$$(E(NUM_{11}, 2) \wedge E(NUM_{12}, 3)),$$
$$(E(NUM_{11}, 3) \wedge E(NUM_{12}, 3)),$$
$$(E(NUM_{11}, 4) \wedge E(NUM_{12}, 3)),$$

$(E\,(NUM_{11},\,5)\wedge E\,(NUM_{12},\,3))\},$

$$\mathbf{SF_2} = \{\bigcup_{a=1}^{w_2} SF_{2a}\,\} =$$

$\{(E\,(NUM_{21},\,1)\wedge(E\,(NUM_{22},\,1)\vee E\,(NUM_{23},\,1))),$
$(E\,(NUM_{21},\,2)\wedge(E\,(NUM_{22},\,1)\vee E\,(NUM_{23},\,1))),$
$(E\,(NUM_{21},\,3)\wedge(E\,(NUM_{22},\,1)\vee E\,(NUM_{23},\,1))),$
$(E\,(NUM_{21},\,4)\wedge(E\,(NUM_{22},\,1)\vee E\,(NUM_{23},\,1))),$
$(E\,(NUM_{21},\,5)\wedge(E\,(NUM_{22},\,1)\vee E\,(NUM_{23},\,1)))\},$
$\{(E\,(NUM_{21},\,1)\wedge(E\,(NUM_{22},\,1)\vee E\,(NUM_{23},\,2))),$
$(E\,(NUM_{21},\,2)\wedge(E\,(NUM_{22},\,1)\vee E\,(NUM_{23},\,2))),$
$(E\,(NUM_{21},\,3)\wedge(E\,(NUM_{22},\,1)\vee E\,(NUM_{23},\,2))),$
$(E\,(NUM_{21},\,4)\wedge(E\,(NUM_{22},\,1)\vee E\,(NUM_{23},\,2))),$
$(E\,(NUM_{21},\,5)\wedge(E\,(NUM_{22},\,1)\vee E\,(NUM_{23},\,2)))\},$
$\{(E\,(NUM_{21},\,1)\wedge(E\,(NUM_{22},\,1)\vee E\,(NUM_{23},\,3))),$
$(E\,(NUM_{21},\,2)\wedge(E\,(NUM_{22},\,1)\vee E\,(NUM_{23},\,3))),$
$(E\,(NUM_{21},\,3)\wedge(E\,(NUM_{22},\,1)\vee E\,(NUM_{23},\,3))),$
$(E\,(NUM_{21},\,4)\wedge(E\,(NUM_{22},\,1)\vee E\,(NUM_{23},\,3))),$
$(E\,(NUM_{21},\,5)\wedge(E\,(NUM_{22},\,1)\vee E\,(NUM_{23},\,3)))\},$
$\{(E\,(NUM_{21},\,1)\wedge(E\,(NUM_{22},\,2)\vee E\,(NUM_{23},\,1))),$
$(E\,(NUM_{21},\,2)\wedge(E\,(NUM_{22},\,2)\vee E\,(NUM_{23},\,1))),$
$(E\,(NUM_{21},\,3)\wedge(E\,(NUM_{22},\,2)\vee E\,(NUM_{23},\,1))),$
$(E\,(NUM_{21},\,4)\wedge(E\,(NUM_{22},\,2)\vee E\,(NUM_{23},\,1))),$
$(E\,(NUM_{21},\,5)\wedge(E\,(NUM_{22},\,2)\vee E\,(NUM_{23},\,1)))\},$
$\{(E\,(NUM_{21},\,1)\wedge(E\,(NUM_{22},\,2)\vee E\,(NUM_{23},\,2))),$
$(E\,(NUM_{21},\,2)\wedge(E\,(NUM_{22},\,2)\vee E\,(NUM_{23},\,2))),$
$(E\,(NUM_{21},\,3)\wedge(E\,(NUM_{22},\,2)\vee E\,(NUM_{23},\,2))),$
$(E\,(NUM_{21},\,4)\wedge(E\,(NUM_{22},\,2)\vee E\,(NUM_{23},\,2))),$
$(E\,(NUM_{21},\,5)\wedge(E\,(NUM_{22},\,2)\vee E\,(NUM_{23},\,2)))\}),$

$\{(E(NUM_{21}, 1) \wedge (E(NUM_{22}, 2) \vee E(NUM_{23}, 3))),$
$(E(NUM_{21}, 2) \wedge (E(NUM_{22}, 2) \vee E(NUM_{23}, 3))),$
$(E(NUM_{21}, 3) \wedge (E(NUM_{22}, 2) \vee E(NUM_{23}, 3))),$
$(E(NUM_{21}, 4) \wedge (E(NUM_{22}, 2) \vee E(NUM_{23}, 3))),$
$(E(NUM_{21}, 5) \wedge (E(NUM_{22}, 2) \vee E(NUM_{23}, 3)))\},$
$\{(E(NUM_{21}, 1) \wedge (E(NUM_{22}, 3) \vee E(NUM_{23}, 1))),$
$(E(NUM_{21}, 2) \wedge (E(NUM_{22}, 3) \vee E(NUM_{23}, 1))),$
$(E(NUM_{21}, 3) \wedge (E(NUM_{22}, 3) \vee E(NUM_{23}, 1))),$
$(E(NUM_{21}, 4) \wedge (E(NUM_{22}, 3) \vee E(NUM_{23}, 1))),$
$(E(NUM_{21}, 5) \wedge (E(NUM_{22}, 3) \vee E(NUM_{23}, 1)))\},$
$\{(E(NUM_{21}, 1) \wedge (E(NUM_{22}, 3) \vee E(NUM_{23}, 2))),$
$(E(NUM_{21}, 2) \wedge (E(NUM_{22}, 3) \vee E(NUM_{23}, 2))),$
$(E(NUM_{21}, 3) \wedge (E(NUM_{22}, 3) \vee E(NUM_{23}, 2))),$
$(E(NUM_{21}, 4) \wedge (E(NUM_{22}, 3) \vee E(NUM_{23}, 2))),$
$(E(NUM_{21}, 5) \wedge (E(NUM_{22}, 3) \vee E(NUM_{23}, 2)))\},$
$\{(E(NUM_{21}, 1) \wedge (E(NUM_{22}, 3) \vee E(NUM_{23}, 3))),$
$(E(NUM_{21}, 2) \wedge (E(NUM_{22}, 3) \vee E(NUM_{23}, 3))),$
$(E(NUM_{21}, 3) \wedge (E(NUM_{22}, 3) \vee E(NUM_{23}, 3))),$
$(E(NUM_{21}, 4) \wedge (E(NUM_{22}, 3) \vee E(NUM_{23}, 3))),$
$(E(NUM_{21}, 5) \wedge (E(NUM_{22}, 3) \vee E(NUM_{23}, 3)))\},$

$$\mathbf{SF_3} = \{\bigcup_{a=1}^{w_3} SF_{3a}\} =$$

$\{(E(NUM_{31}, 1) \wedge E(NUM_{32}, 1)),$
$(E(NUM_{31}, 2) \wedge E(NUM_{32}, 1)),$
$(E(NUM_{31}, 3) \wedge E(NUM_{32}, 1)),$
$(E(NUM_{31}, 4) \wedge E(NUM_{32}, 1)),$
$(E(NUM_{31}, 5) \wedge E(NUM_{32}, 1))\},$

$\{(E\,(NUM_{31},\,1)\wedge E\,(NUM_{32},\,2)),$

$(E\,(NUM_{31},\,2)\wedge E\,(NUM_{32},\,2)),$

$(E\,(NUM_{31},\,3)\wedge E\,(NUM_{32},\,2)),$

$(E\,(NUM_{31},\,4)\wedge E\,(NUM_{32},\,2)),$

$(E\,(NUM_{31},\,5)\wedge E\,(NUM_{32},\,2))\},$

$\{(E\,(NUM_{31},\,1)\wedge E\,(NUM_{32},\,3)),$

$(E\,(NUM_{31},\,2)\wedge E\,(NUM_{32},\,3)),$

$(E\,(NUM_{31},\,3)\wedge E\,(NUM_{32},\,3)),$

$(E\,(NUM_{31},\,4)\wedge E\,(NUM_{32},\,3)),$

$(E\,(NUM_{31},\,5)\wedge E\,(NUM_{32},\,3))\}.$

На рис. 4.1 представлено експертний розподіл всіх можливих рівнів аномальності, породженої атакуючим середовищем ($\mathbf{CA}^{\tau_t}$) та відображеної ідентифікаторами атакуючих дій за допомогою різних значень параметрів КОП-КПОА-підсередовища ($\mathbf{P_i = P_3}$).

З графічної інтерпретації (рис. 4.1) видно, що найбільш значимими для виявлення кібератаки SN є опорні блоки з ідентифікаторами БВН, В та П.

Виходячи з цього приклад конкретних розрахунків представимо тільки для вирішальних функцій $(SF_{3\,11},\ ...,\ SF_{3\,15})$ з $\mathbf{SF_3}$, тобто

$$\begin{aligned}
SF_{3\,11} &= (E\,(NUM_{31},\,1)\wedge E\,(NUM_{32},\,3)),\\
SF_{3\,12} &= (E\,(NUM_{31},\,2)\wedge E\,(NUM_{32},\,3)),\\
SF_{3\,13} &= (E\,(NUM_{31},\,3)\wedge E\,(NUM_{32},\,3)),\\
SF_{3\,14} &= (E\,(NUM_{31},\,4)\wedge E\,(NUM_{32},\,3)),\\
SF_{3\,15} &= (E\,(NUM_{31},\,5)\wedge E\,(NUM_{32},\,3)).
\end{aligned} \qquad (4.28)$$

Відмітимо, якщо $j=1,\ r_1=5,\ NUM_{31}=3$ та $s=\overline{1,5}$ то

$$\mathbf{T}^{\mathbf{e}}_{\mathbf{31}} = \{\bigcup_{s=1}^{5} \underset{\sim}{T}^{ep}_{31s}\} = \{\underset{\sim}{T}^{ep}_{311},\ \underset{\sim}{T}^{ep}_{312},\ \underset{\sim}{T}^{ep}_{313},\ \underset{\sim}{T}^{ep}_{314},\ \underset{\sim}{T}^{ep}_{315}\} =$$

$$\{\underset{\sim}{OM}^{ep}_{31},\ \underset{\sim}{M}^{ep}_{31},\ \underset{\sim}{C}^{ep}_{31},\ \underset{\sim}{Б}^{ep}_{31},\ \underset{\sim}{OБ}^{ep}_{31}\}\ \text{(див. (2.50))}.$$

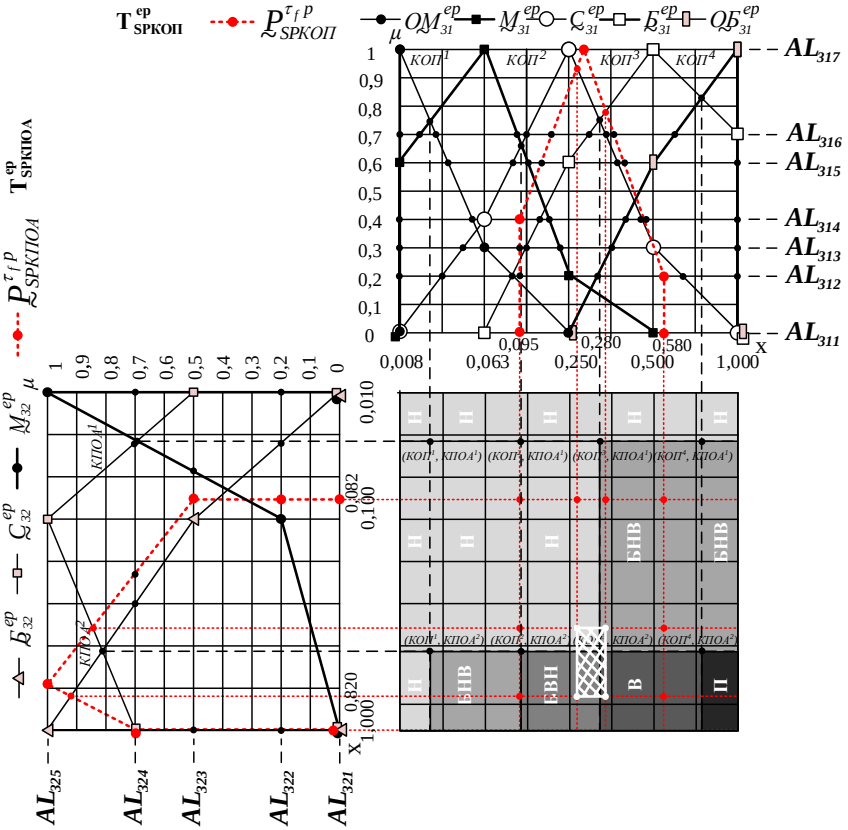

Рис. 4.1. Графічна інтерпретація експертного розподілу ідентифікаторів атакуючих дій (відображених двовимірними опорними областями Н, БНВ, БВН, В, П) та фазифікованих значень поточних параметрів $\underset{\sim}{P}^{\tau_f}_{31}$ і $\underset{\sim}{P}^{\tau_f}_{32}$ відносно лінгвістичних еталонів $\mathbf{T}^{ep}_{31}$ і $\mathbf{T}^{ep}_{32}$ відповідно

Функція еквівалентності E відповідно до (4.26) приймає значення

$$E(NUM_{31},\ 1) = E(NUM_{31},\ 2) =$$

$$E(NUM_{31},\ 4) = E(NUM_{31},\ 5) = 0$$

оскільки $NUM_{31} = 3 \neq 1 \neq 2 \neq 4 \neq 5.$

Це виходить з того, що

$$\underset{\sim}{T}^{ep}_{313} \neq \underset{\sim}{T}^{ep}_{311} \neq \underset{\sim}{T}^{ep}_{312} \neq \underset{\sim}{T}^{ep}_{314} \neq \underset{\sim}{T}^{ep}_{315},\ \text{тобто}$$

$$\underset{\sim}{C}^{ep}_{31} \neq \underset{\sim}{OM}^{ep}_{31} \neq \underset{\sim}{M}^{ep}_{31} \neq \underset{\sim}{B}^{ep}_{31} \neq \underset{\sim}{OB}^{ep}_{31}.$$

Також, $E(NUM_{31},\ 3)=1$ оскільки $NUM_{31}=3,$ з цього випливає, що $\underset{\sim}{T}^{ep}_{313}=\underset{\sim}{T}^{ep}_{313}$, тобто $\underset{\sim}{C}^{ep}_{31}=\underset{\sim}{C}^{ep}_{31}$.

Аналогічним чином для

$$\mathbf{T}^{\mathbf{e}}_{\mathbf{32}}=\{\bigcup_{s=1}^{3}\underset{\sim}{T}^{ep}_{32s}\}=\{\underset{\sim}{T}^{ep}_{321},\ \underset{\sim}{T}^{ep}_{322},\ \underset{\sim}{T}^{ep}_{323}\}=$$

$$\{\underset{\sim}{M}^{ep}_{32},\ \underset{\sim}{C}^{ep}_{32},\ \underset{\sim}{B}^{ep}_{32}\}$$

при $j=2,\ r_2=3,\ NUM_{32}=3,\ s=\overline{1,3}$ (див. (2.50)), а функція еквівалентності E відповідно до (4.26) приймає значення

$$E(NUM_{32},\ 1)=E(NUM_{32},\ 2)=0$$

оскільки $NUM_{32}=3\neq 1\neq 2.$

Це виходить з того, що

$$\underset{\sim}{T}^{ep}_{323} \neq \underset{\sim}{T}^{ep}_{321} \neq \underset{\sim}{T}^{ep}_{322},\ \text{тобто}\ \underset{\sim}{B}^{ep}_{32} \neq \underset{\sim}{M}^{ep}_{32} \neq \underset{\sim}{C}^{ep}_{32},$$

а $E(NUM_{32},\ 3)=1$ оскільки $NUM_{32}=3,$ і далі випливає, що $\underset{\sim}{T}^{ep}_{323}=\underset{\sim}{T}^{ep}_{323}$, тобто $\underset{\sim}{B}^{ep}_{32}=\underset{\sim}{B}^{ep}_{32}$.

Таким чином:

$$\begin{aligned}
&SF_{3\,11}=(E\,(NUM_{31},\ 1)\wedge E\,(NUM_{32},\ 3))=(1\wedge 0)=0,\\
&SF_{3\,12}=(E\,(NUM_{31},\ 2)\wedge E\,(NUM_{32},\ 3))=(1\wedge 0)=0,\\
&SF_{3\,13}=(E\,(NUM_{31},\ 3)\wedge E\,(NUM_{32},\ 3))=(1\wedge 0)=0,\\
&SF_{3\,14}=(E\,(NUM_{31},\ 4)\wedge E\,(NUM_{32},\ 3))=(1\wedge 0)=0,\\
&SF_{3\,15}=(E\,(NUM_{31},\ 5)\wedge E\,(NUM_{32},\ 3))=(1\wedge 0)=0.
\end{aligned} \qquad (4.29)$$

Формування умовних виразів детекційного середовища

Етап 3 – формування умовних виразів детекційного середовища. Умовні детекційні вирази, які відображають сформовані базові правила для виявлення *i*-ї кібератаки (див. вираз (2.19) в п. 2.1, [1]) представимо у наступному вигляді:

$$\mathbf{DR_i} = \{\bigcup_{\mathbf{a=1}}^{\mathbf{w_i}} \mathbf{DR_{ia}}\} = \{\mathbf{DR_{i1}}, \mathbf{DR_{i2}}, \ldots, \mathbf{DR_{iw_i}}\} =$$

$$\{ \mathbf{DR_{i1}} \Rightarrow \{ if\ SF_{i1}\ then\ \{\bigcup_{u=1}^{v_i} IA_{iu}\}\},\ \mathbf{DR_{i2}}$$

$$\Rightarrow \{ if\ SF_{i2}\ then\ \{\bigcup_{u=1}^{v_i} IA_{iu}\}\}, \qquad (4.30)$$

$$\ldots,$$

$$\mathbf{DR_{iw_i}} \Rightarrow \{ if\ SF_{ia}\ then\ \{\bigcup_{u=1}^{v_i} IA_{iu}\}\}\},$$

$$(a = \overline{1, w_i},\ u = \overline{1, v_i}).$$

Зазначимо, що формально кожна SF_{ia} може бути пов'язана з v_i-ю кількістю ідентифікаторів аномальності та, таким чином, кожне базове правило може породжуватись v_i кількістю детекційних виразів, тобто:

$$\mathbf{DR_i} = \{\mathbf{DR_{i1}}, \mathbf{DR_{i2}}, \ldots, \mathbf{DR_{iw_i}}\} =$$

$$\{ \mathbf{DR_{i1}} \Rightarrow \{ if\ SF_{i1}\ then\ IA_{i1},\ if\ SF_{i1}\ then\ IA_{i2}, \ldots,$$
$$if\ SF_{i1}\ then\ IA_{iv_i}\},$$

$$\mathbf{DR_{i2}} \Rightarrow \{ if\ SF_{i2}\ then\ IA_{i1},\ if\ SF_{i2}\ then\ IA_{i2}, \ldots,$$
$$if\ SF_{i2}\ then\ IA_{iv_i}\},$$

$$\ldots, \qquad (4.31)$$

$$\mathbf{DR_{iw_i}} \Rightarrow \{ if\ SF_{iw_i}\ then\ IA_{i1},\ if\ SF_{iw_i}\ then\ IA_{i2}, \ldots,$$
$$if\ SF_{iw_i}\ then\ IA_{iv_i}\}\}$$

або

$$\mathbf{DR_i} = \{\bigcup_{a=1}^{w_i} \{\bigcup_{u=1}^{v_i} if\ SF_{ia}\ then\ IA_{iu}\}\},$$

$$(a = \overline{1, w_i},\ u = \overline{1, v_i}).$$

Очевидно, що можлива кількість умовних детекційних виразів для виявлення *i*-ї кібератаки визначається за формулою

$$CDR_i = w_i \cdot v_i, \qquad (4.32)$$

а їх кількість для виявлення n атак обчислюється за виразом

$$CDR = \sum_{i=1}^{n} CDR_i .$$

Слід зазначити, що із загальної кількості можливих детекційних виразів не всі є визначальними (тобто впливають на процес виявлення вторгнення) для виявлення *i*-ї кібератаки, що також випливає з рис. 4.1 та (4.29) (тут визначальними будуть $\mathbf{DR}_{3\,11}$, $\mathbf{DR}_{3\,12}$,…, $\mathbf{DR}_{3\,15}$).

З урахуванням цього, розглянемо приклад реалізації етапу 3 при $i = 3$ $(CA_3 = CA_{SP} = SP)$, $j = \overline{1,2}$ $(P_{31} = P_{SPKOП} = KOП,\ P_{32} = P_{SPKПОА} = KПОА)$, $u_3 = 5,\ w_3 = 15.$

Тоді, загальну кількість правил визначимо за формулою (4.32), тобто

$$CDR_3 = w_3 \cdot v_3 = 15 \cdot 5 = 75,$$

а вираз (4.31) буде мати наступний вигляд:

$$\begin{gathered}
\mathbf{DR_3} = \{ \ldots ,\ \mathbf{DR}_{3\,11} \Rightarrow \{ if\ SF_{3\,11}\ then\ IA_{31}, \\
if\ SF_{3\,11}\ then\ IA_{32},\ if\ SF_{3\,11}\ then\ IA_{33}, \\
if\ SF_{3\,11}\ then\ IA_{34},\ if\ SF_{3\,11}\ then\ IA_{35} \}, \\
\mathbf{DR}_{3\,12} \Rightarrow \{ if\ SF_{3\,12}\ then\ IA_{31}, \\
if\ SF_{3\,12}\ then\ IA_{32},\ if\ SF_{3\,12}\ then\ IA_{33}, \\
if\ SF_{3\,12}\ then\ IA_{34},\ if\ SF_{3\,12}\ then\ IA_{35} \}, \\
\mathbf{DR}_{3\,13} \Rightarrow \{ if\ SF_{3\,13}\ then\ IA_{31}, \\
if\ SF_{3\,13}\ then\ IA_{32},\ if\ SF_{3\,13}\ then\ IA_{33}, \\
if\ SF_{3\,13}\ then\ IA_{34},\ if\ SF_{3\,13}\ then\ IA_{35} \}, \\
\mathbf{DR}_{3\,14} \Rightarrow \{ if\ SF_{3\,14}\ then\ IA_{31}, \\
if\ SF_{3\,14}\ then\ IA_{32},\ if\ SF_{3\,14}\ then\ IA_{33}, \\
if\ SF_{3\,14}\ then\ IA_{34},\ if\ SF_{3\,14}\ then\ IA_{35} \},
\end{gathered} \tag{4.33}$$

$$\mathbf{DR}_{3\ 15} \Rightarrow \{ if\ SF_{3\ 15}\ then\ IA_{31},$$
$$if\ SF_{3\ 15}\ then\ IA_{32},\ if\ SF_{3\ 15}\ then\ IA_{33},$$
$$if\ SF_{3\ 15}\ then\ IA_{34},\ if\ SF_{3\ 15}\ then\ IA_{35}\ \}\}.$$

Відповідно до заданих у прикладі вхідних даних, а також з урахуванням виразу (4.29) та графічної візуалізації (див. рис. 4.1) видно, що визначальною є вирішальна функція $SF_{3\ 13}$, яка входить у підмножину детекційних виразів $\mathbf{DR}_{3\ 13}$, тобто:

$$\mathbf{DR}_{3\ 13} \Rightarrow \{ if\ SF_{3\ 13}\ then\ IA_{31},$$
$$if\ SF_{3\ 13}\ then\ IA_{32},\ if\ SF_{3\ 13}\ then\ IA_{33},$$
$$if\ SF_{3\ 13}\ then\ IA_{34},\ if\ SF_{3\ 13}\ then\ IA_{35}\ \} =$$
$$\{ if\ (E(NUM_{31},\ 1) \wedge E(NUM_{32},\ 3))\ then\ IA_{31},$$
$$if\ (E(NUM_{31},\ 2) \wedge E(NUM_{32},\ 3))\ then\ IA_{32},$$
$$if\ (E(NUM_{31},\ 3) \wedge E(NUM_{32},\ 3))\ then\ IA_{33},$$
$$if\ (E(NUM_{31},\ 4) \wedge E(NUM_{32},\ 3))\ then\ IA_{34},$$
$$if\ (E(NUM_{31},\ 5) \wedge E(NUM_{32},\ 3))\ then\ IA_{35}\ \} =$$
$$\{ if\ (E(NUM_{SPKOP},\ 1) \wedge E(NUM_{SPKPOA},\ 3))\ then\ "Н",$$
$$if\ (E(NUM_{SPKOP},\ 2) \wedge E(NUM_{SPKPOA},\ 3))\ then\ "БНВ",$$
$$if\ (E(NUM_{SPKOP},\ 3) \wedge E(NUM_{SPKPOA},\ 3))\ then\ "БВН",$$
$$if\ (E(NUM_{SPKOP},\ 4) \wedge E(NUM_{SPKPOA},\ 3))\ then\ "В",$$
$$if\ (E(NUM_{SPKOP},\ 5) \wedge E(NUM_{SPKPOA},\ 3))\ then\ "П"\}.$$

Після перевірки всіх правил в $\mathbf{DR}_{3\ 13}$ визначимо, що ідентифікація аномального стану здійснюється за допомогою умовного виразу

$$if\ (E(NUM_{SPKOP},\ 3) \wedge E(NUM_{SPKPOA},\ 3))\ then\ "БВН" =$$
$$if\ (1 \wedge 1)\ then\ "БВН".$$

На рис. 4.1 графічно показаний поточний блок (у вигляді заштрихованої прямокутної області, яка утворена за допомогою $\underset{\sim}{P}_{31}^{\tau_f}$, $\underset{\sim}{P}_{32}^{\tau_f}$), який інтерпретує аномалію у *2*-вимірному параметричному КОП-КПОА-підсередовищі ($\mathbf{P_i} = \mathbf{P_3} = \mathbf{P_{SP}}$), породжену відповідним

атакуючим SP-середовищем ($\mathbf{CA}^{\tau_f}$) в момент часу τ_f (оскільки атакуюче середовище відображається тільки однією атакою).

Тут, навіть при візуальному порівнянні, можна визначити, що отриманий поточний блок найближче всього розташований до нечіткої опорної двовимірної області з ідентифікатором *"БВН"*.

З використанням отриманих у п. 4.1 відповідно до формул (4.7) та (4.9) експертних коефіцієнтів параметрів (EC_{31}^{max}, EC_{32}^{max}) і кібератаки (EC_3^{CA}) зазначимо умовний вираз з підмножини $\mathbf{DR}_{3\ 13}$ детекційного підсередовища ($\mathbf{DR}_{\mathbf{SP}}$) для виявлення спуфінгу: «Якщо поточний параметр «Кількість одночасних підключень до сервера» в момент часу τ_f найближчий до еталону «Середнє» (з експертним коефіцієнтом $0{,}713$) і поточний параметр «Кількість пакетів з однаковою адресою відправника та одержувача» в момент часу τ_f найближчий до еталону «Велике» (з експертним коефіцієнтом $0{,}741$), то рівень аномального стану, породженого спуфінгом буде «Більш високим ніж низьким» (з експертним коефіцієнтом кібератаки $0{,}727$)». З урахуванням (4.33) можна застосувати еквівалентний запис:

$$if\ \left(E\left(NUM_{SPKOП},3\right)\Big|_{0,713} \wedge E\left(NUM_{SPKПОА},3\right)\Big|_{0,741}\right) then$$
$$"БВН"\Big|_{0,727}.$$

Аналогічним чином, при різних початкових даних визначаються інші типи кібератак, що породжують певні аномалії в інформаційних системах.

Таким чином, запропоновано МФДС [12, 13], який на основі базової кортежної моделі (див. п. 2.1 і [1]) та за рахунок механізму формування підмножин ідентифікаторів аномальності, формалізації процесу побудови вирішальних функцій і умовних детекційних виразів, дозволяє сформувати необхідну множину детекційних правил, що використовуються для визначення рівней аномальних станів, характерних впливу певних типів кібератак.

На основі запропонованих методів можна розробляти СВВ для побудови яких необхідна відповідна методологія.

4.3. Методологія побудови систем виявлення аномалій, породжених кібератаками

На основі запропонованої КМАС (див. п. 2.1 та [1-3]) і методів МФЕС (див. п. 2.2 та [6-9]), МФП (див. п. 3.1 і [14, 15]), МАН (див. п. 3.2 та [16, 17]), МВІТ (див. п. 3.3 і [4, 5]), МДП (див. п. 4.1) та МФДС (див. п. 4.2 та [12, 13]), а також з урахуванням [18-30] і їх розвитком в [31] пропонується методологія побудови систем виявлення аномалій породжених кібератаками (МПСВ) [32] для розширення можливостей систем виявлення вторгнень, що функціонують в слабоформалізованному нечіткому середовищі оточення. За допомогою такої методології (при вирішенні задач виявлення кібератак) можна ефективно будувати системи, які детектують рівень аномального стану, характерного для впливу певного типу кібератак щодо конкретного гетерогенного параметричного середовища оточення в заданий часовий проміжок.

Базовий механізм МПСВ (див. рис. 4.2), яка орієнтована на вирішення задач виявлення кібератак в ІС, базується на семи етапах:

- формування атакуючих середовищ;
- побудова m_i-вимірного параметричного підсередовища;
- формування m_i-вимірних еталонних підсередовищ;
- формування m_i-вимірних поточних підсередовищ;
- α-рівнева номіналізація еталонних і поточних підсередовищ;
- дефазифікація та визначення ідентифікуючих термів;
- формування детекційних середовищ.

Опишемо кожен з них.

Формування атакуючих середовищ

Етап 1 – формування атакуючих середовищ. Ідентифікатори кібератак використовуються для однозначного визначення конкретної кібератаки (із усієї можливої множини) шляхом присвоєння її імені конкретному ІД. Кожний ІД $CA_i \ \ (i=\overline{1,n})$ визначається на основі того, що кожний елемент множини $\mathbf{CA}^{\tau_1}$ пов'язаний з певною кібератакою, яку ідентифікують за відповідним їй ім'ям.

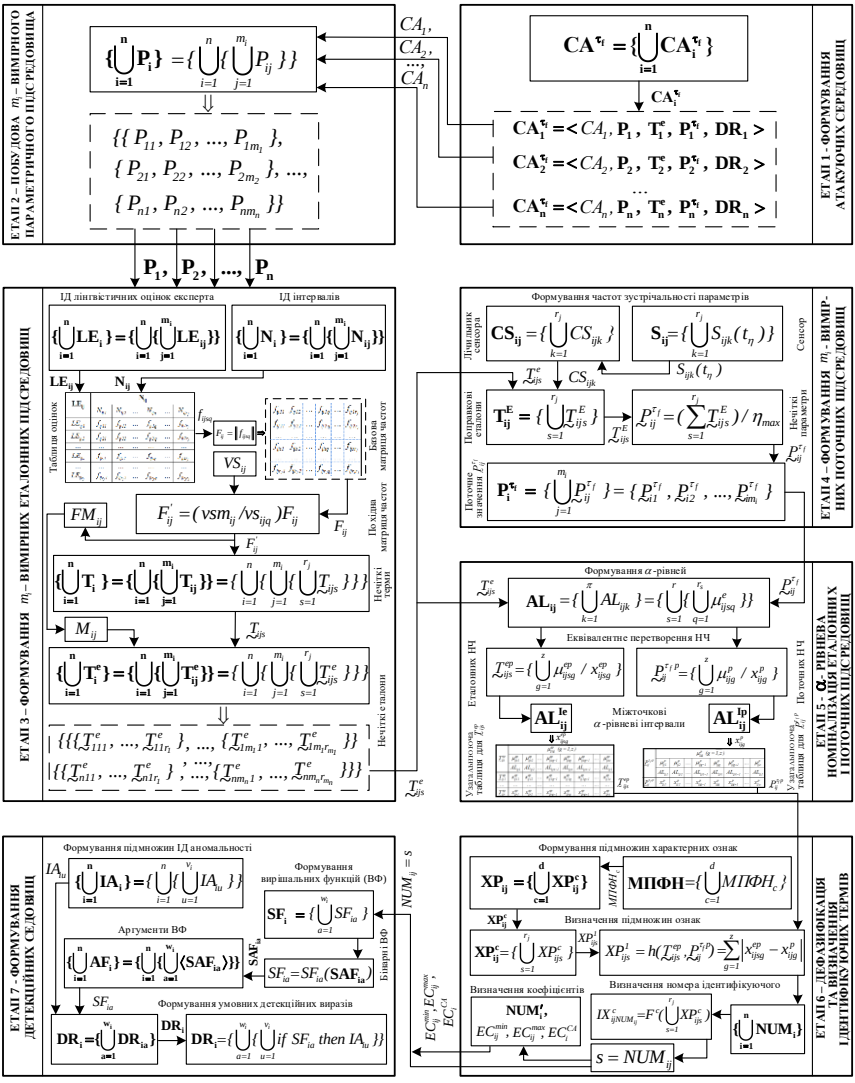

Рис. 4.2. Схема відображення методології побудови систем виявлення аномалій, породжених кібератаками

Перший етап використовується для формування множин

$$\mathbf{CA}^{\tau_f} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{CA}_\mathbf{i}^{\tau_f}\} \text{ (див. (2.1), [1])}$$

за часовий проміжок τ_f, кожна з яких відображається узагальнювальним кортежем

$$\mathbf{CA}_\mathbf{i}^{\tau_f} = < CA_i, \ \mathbf{P_i}, \ \mathbf{T_i^e}, \ \mathbf{P_i^{\tau_f}}, \ \mathbf{DR_i} > \text{(див. (2.2))},$$

елементи якого утворюють *i*-е атакуюче підсередовище ($\mathbf{CA}_\mathbf{i}^{\tau_f}$).

Побудова m_i-вимірного параметричного підсередовища

Етап 2 – побудова m_i-вимірного параметричного підсередовища. Підмножини параметрів $\mathbf{P_i}$ (див. (2.8)) необхідні для побудови нечітких (лінгвістичних) еталонів. Тут, для побудови підмножини $\mathbf{P_i}$ на основі множини всіх можливих параметрів $\mathbf{P}$ (див. (2.4)), які характеризують стан середовища оточення, за значеннями яких можна виявити аномальний стан, породжений впливом кібератаки з ІД CA_i (див. етап 1).

Таким чином, формується

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{P_i}\} = \{\bigcup_{i=1}^{n} \{\bigcup_{j=1}^{m_i} P_{ij}\}\},$$

$$(\overline{j = 1, m_i}),$$

де конкретні значення членів підмножини $\mathbf{P_i}$ визначають m_i-вимірне параметричне підсередовище ($\mathbf{P_i}$), що використовується для виявлення CA_i-атаки.

Формування m_i-вимірних еталонних підсередовищ

Етап 3 – формування m_i-вимірних еталонних підсередовищ. Підмножини нечітких (лінгвістичних) еталонів $\mathbf{T_i^e}$ (див. (2.14)), які необхідні для відображення певних (фіксованих) станів відповідних параметрів із підмножини $\mathbf{P_i}$ у m_i-вимірному параметричному підсередовищі ($\mathbf{P_i}$).

На даному етапі здійснюється формування підмножин можливих нечітких (лінгвістичних) еталонів $\mathbf{T_i^e}$, що відображають характерні

судження експерта відносно аномальності стану відповідних параметрів P_{ij} з підмножини $\mathbf{P_i}$ (див. етап 2) в заданому середовищі оточення.

Для цього, формуємо підмножини ІД лінгвістичних оцінок (суджень) експерта

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\mathbf{LE_i}\} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}}\mathbf{LE_{ij}}\}\} =$$

$$\{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\{\bigcup_{k=1}^{r_j} LE_{ijk}\}\}\},$$

$$(k=\overline{1,r_j})$$

(див. (2.30), [6]) та підмножини ІД інтервалів

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\mathbf{N_i}\} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}}\mathbf{N_{ij}}\}\} = \{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\{\bigcup_{k=1}^{r_j} N_{ijk}\}\}\}$$

(див. (2.35)), які відповідно необхідні для побудови базової матриці частот F_{ij} (див. (2.36)).

Далі з використанням $\mathbf{LE_{ij}}$, $\mathbf{N_{ij}}$ та F_{ij}, за допомогою вектора сум VS_{ij} (див. (2.38)) будується похідна матриця частот $F_{ij}^{'} = (vsm_{ij}/vs_{ijq})F_{ij}$ (див. (2.40)).

З урахуванням матриці $F_{ij}^{'}$ формуються підмножини нечітких термів

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\mathbf{T_i}\} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}}\mathbf{T_{ij}}\}\} =$$

$$\{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\{\bigcup_{s=1}^{r_j}\underset{\sim}{T}_{ijs}\}\}\},$$

$$(s=\overline{1,r_j})$$

(див. (2.45)), а також з використанням вектора максимумів FM_{ij} (див. (2.46)) і матриці функцій належності M_{ij} (див. (2.47)) визначаються набори нечітких термів (чисел) $\underset{\sim}{T}_{ijs}$ (див. (2.48)). Відповідно

до $\underset{\sim}{T}_{ijs}$ та наборів проміжних термів $\underset{\sim}{T}'_{ijs}$ (див. (2.51)) отримаємо підмножини можливих нечітких (лінгвістичних) еталонів

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{T}_{\mathbf{i}}^{\mathbf{e}}\} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}} \mathbf{T}_{\mathbf{ij}}^{\mathbf{e}}\}\} =$$

$$\{\bigcup_{i=1}^{n} \{\bigcup_{j=1}^{m_i} \{\bigcup_{s=1}^{r_j} \underset{\sim}{T}_{jis}^{e}\}\}\}$$

(див. (2.14)), де сукупність конкретних значень всіх членів підмножини $\mathbf{T}_{\mathbf{i}}^{\mathbf{e}}$ визначають m_i-вимірне еталонне підсередовище ($\mathbf{T}_{\mathbf{i}}^{\mathbf{e}}$), орієнтоване на виявлення кібератаки з ІД CA_i (див. етап 1).

Формування m_i-вимірних поточних підсередовищ

Етап 4 – формування m_i-вимірних поточних підсередовищ. Підмножини поточних значень нечітких параметрів $\mathbf{P}_{\mathbf{i}}^{\boldsymbol{\tau}_{\mathbf{f}}}$ (див. (2.16)) необхідні для формування поточних значень змінних в нечіткій формі, за допомогою яких формалізуються параметри, характерні для конкретного середовища оточення при вирішенні задач виявлення кібератак.

Етап орієнтований на побудову підмножин всіх можливих поточних значень нечітких параметрів, що утворюють m_i-вимірне параметричне підсередовище ($\mathbf{P}_{\mathbf{i}}$), сформоване за допомогою $\mathbf{T}_{\mathbf{i}}^{\mathbf{e}}$ (див. етап 3) в заданий момент часу τ_f за його визначений проміжок, тривалість якого $\tau_h = \tau_f - \tau_{f-1}$, $(f = \overline{1, max_\tau})$.

Для цього, з урахуванням підмножини всіх можливих сенсорів

$$\mathbf{S}_{\mathbf{ij}} = \{\bigcup_{k=1}^{r_j} S_{ijk}(t_\eta)\}$$

(див. (3.1), [14]), використаних для контроля поточного стану фізичних параметрів, що відображаються за допомогою $\mathbf{P}_{\mathbf{i}}^{\boldsymbol{\tau}_{\mathbf{f}}}$ в $\mathbf{CA}_{\mathbf{i}}^{\boldsymbol{\tau}_{\mathbf{f}}}$ (див. (2.2) та (2.16)) і підмножини всіх можливих лічильників сенсорів

$$\mathbf{CS}_{\mathbf{ij}} = \{\bigcup_{k=1}^{r_j} CS_{ijk}\} =$$

$$\{\bigcup_{k=1}^{r_j}\sum_{\eta=1}^{\eta_{max}} S_{ijk}(t_\eta)\}$$

(див. (3.3)) формуються частоти зустрічальності фізичних параметрів (див. етап 1 в п. 3.1).

Далі, з використанням поправкових еталонів

$$\mathbf{T_{ij}^{E}} = \{\bigcup_{s=1}^{r_j} \underset{\sim}{T}_{ijs}^{E}\}$$

(див. (3.4)) і нечітких параметрів

$$\underset{\sim}{P}_{ij}^{\tau_f} = (\sum_{s=1}^{r_j} \underset{\sim}{T}_{ijs}^{E}) / \eta_{max}$$

(див. (3.6)) формуються підмножини поточних величин

$$\mathbf{P_i^{\tau_f}} = \{\bigcup_{j=1}^{m_i} \underset{\sim}{P}_{ij}^{\tau_f}\} \text{ (див. (2.16))},$$

а сукупність конкретних значень всіх членів підмножини $\mathbf{P_i^{\tau_f}}$ визначає m_i-вимірне поточне підсередовище ($\mathbf{P_i^{\tau_f}}$), яке використовується для виявлення аномального стану в загальному гетерогенному параметричному середовищі ($\mathbf{P}$), породженого кібератакою з ІД CA_i (див. етап 1) в момент часу τ_f.

α-рівнева номіналізація еталонних і поточних підсередовищ

Етап 5 – α-рівнева номіналізація еталонних і поточних підсередовищ. Номіналізація НЧ необхідна для зведення до одного числа компонент НЧ еталонних та поточних підсередовищ ($\mathbf{T_i^e}$ та $\mathbf{P_i^{\tau_f}}$), обчислених на основі об'єднаних значень їх α-рівней.

Перетворення сформованих підмножин можливих нечітких (лінгвістичних) еталонів $\mathbf{T_i^e}$ (див. етап 3) та поточних значень нечітких параметрів $\mathbf{P_i^{\tau_f}}$ (див. етап 4) вимагає чіткої формалізації процесу формування α-рівневих інтервалів для відповідного еквівалентного перетворення НЧ еталонних та поточних підсередовищ ($\mathbf{T_i^e}$ та $\mathbf{P_i^{\tau_f}}$).

Це дасть можливість визначати ідентифікуючі терми, які відображають аномальність поточного стану середовища ($\mathbf{P}^{\tau_f}$) оточення при вирішенні задач виявлення атак в інформаційних системах.

Для цього (див. (3.9), [16]), за допомогою підмножин всіх можливих значень

$$\mathbf{AL_{ij}} = \{\bigcup_{k=1}^{\pi} AL_{ijk}\} =$$

$$\{\bigcup_{s=1}^{r}\{\bigcup_{q=1}^{r_s} \mu^{e}_{ijsq}\}\}$$

(які використовуються для перетворення НЧ, що відображають $\mathbf{P_i}$ з базової терм-множини $\mathbf{T_i}$), формуються α-рівні (див. етап 1 в п. 3.2).

Далі, з використанням множини всіх можливих перетворених (номіназолізованих) НЧ

$$\mathbf{T^{ep}_{ij}} = \{\bigcup_{s=1}^{r} \underset{\sim}{T}^{ep}_{ijs}\}$$

еталонних підсередовищ ($\mathbf{T^e_i}$) (див. (3.10)) і отриманого на їх основі перетвореного НЧ $\underset{\sim}{P}^{\tau_f p}_{ij}$ поточного підсередовища ($\mathbf{P}^{\tau_f}$),

тобто: $\underset{\sim}{T}^{ep}_{ijs} = \{\bigcup_{g=1}^{z} \mu^{ep}_{ijsg} \;/\; x^{ep}_{ijsg}\}$ та

$$\underset{\sim}{P}^{\tau_f p}_{ij} = \{\bigcup_{g=1}^{z} \mu^{p}_{ijg} \;/\; x^{p}_{ijg}\}$$

(див. (3.11) та (3.12)), а також підмножини α-рівневих інтервалів

$$\mathbf{AL^{Ie}_{ij}} = \{\bigcup_{s=1}^{r} AL^{Ie}_{ijs}\} =$$

$$\{\bigcup_{s=1}^{r}\{\bigcup_{b=1}^{r_s-1}\{\bigcup_{c=1}^{k_b} AL^{Ie}_{ijsbc}\}\}\}$$

(див. (3.17)), здійснюється номіналізація НЧ $\underset{\sim}{T}^{ep}_{ijs}$ еталонних підсередовищ ($\mathbf{T^e_i}$).

Далі, за рахунок підмножини міжточкових α-рівневих інтервалів

$$\mathbf{AL_{ij}^{Ip}} = \{\bigcup_{b=1}^{\rho-1}\{\bigcup_{c=1}^{k_b} AL_{ijbc}^{Ip}\}\}$$

(див. (3.19)), за аналогією з номіналізацією НЧ $\underset{\sim}{T}_{ijs}^{ep}$ еталонних підсередовищ ($\mathbf{T_i^e}$), формуються перетворені (номіналізовані) НЧ $\underset{\sim}{P}_{ij}^{\tau_f p}$ поточного підсередовища ($\mathbf{P_i^{\tau_f}}$). Виходячи з цього, знаходяться значення x_{ijsg}^{ep} та x_{ijg}^{p} для $\underset{\sim}{T}_{ijs}^{ep}$ та $\underset{\sim}{P}_{ij}^{\tau_f p}$.

Таким чином, здійснюється еквівалентне перетворення НЧ (див. етап 2 в п. 3.2), яке реалізується за рахунок зведення всіх НЧ еталонних та поточних підсередовищ ($\mathbf{T_i^e}$ та $\mathbf{P_i^{\tau_f}}$) до номінального (одного для всіх) числа компонент.

Далі, з урахуванням всіх перетворених НЧ $\underset{\sim}{T}_{ijs}^{ep}$ та $\underset{\sim}{P}_{ij}^{\tau_f p}$ еталонних та поточних підсередовищ ($\mathbf{T_i^e}$ та $\mathbf{P_i^{\tau_f}}$) будуються узагальнювальні таблиці, а також виконується графічна інтерпретація відповідних НЧ (див. етап 3 в п. 3.2).

Дефазифікація та визначення ідентифікуючих термів

Етап 6 – дефазифікація та визначення ідентифікуючих термів. Етап орієнтований на пошук в заданій лінгвістичній змінній ідентифікуючого еталонного терму, за яким за допомогою базових детекційних виразів та отриманих числових оцінок, які інтерпретують лінгвістичні параметри, можна визначити рівень аномального стану, характерного для певного типу атак.

Для цього, на базі

$$\mathbf{МПФН} = \{\bigcup_{c=1}^{d} МПФН_c\}$$

(див. (3.25), [4]) формуються підмножини всіх можливих ХО

$$\mathbf{XP_{ij}} = \{\bigcup_{\mathbf{c=1}}^{\mathbf{d}} \mathbf{XP_{ij}^c}\}$$

(див. (3.24)).

Далі, на основі сформованих ХО

$$\mathbf{XP_{ij}^c} = \{\bigcup_{s=1}^{r_j} XP_{ijs}^c\}$$

(див. (3.26)) і за значенням c визначається номер методу із множини **МПФН**, який використовується для визначення конкретної ХО.

Наприклад, якщо $c = 1,$ то ХО формується на основі відстані Хеммінга

$$XP^1_{ijs} = h\,(\underset{\sim}{T}^{ep}_{ijs},\ \underset{\sim}{P}^{\tau_f p}_{ij}) =$$

$$\sum_{g=1}^{z} \left| x^{ep}_{ijsg} - x^{p}_{ijg} \right|$$

(див. (3.27)). Таким чином, можна визначити всі можливі для використання підмножини ознак (див. етап 2 в п. 3.3).

Далі, за допомогою підмножини всіх номерів ідентифікуючих термів

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{NUM_i}\} = \{\bigcup_{i=1}^{n} \{\bigcup_{j=1}^{m_i} NUM_{ij}\}\}$$

(див. (3.31)), а також з урахуванням функції пошуку ідентифікуючої ХО та її номера

$$IX^{\,c}_{ijNUM_{ij}} = F^c(\bigcup_{s=1}^{r_j} XP^c_{ijs})$$

(див. (3.32)) здійснюється пошук в підмножині $\mathbf{T^e_{ij}}$ такого терму, у якого значення $s = NUM_{ij}$, яке і приймається ідентифікуючим. Іншими словами, визначається номер ідентифікуючого терму (див. етап 3 в п. 3.3).

Далі, необхідно визначити який терм після ідентифікуючого найбільш близько розташований до поточного значення $\underset{\sim}{P}^{\tau_f p}_{ij}$.

Для цього, формуються підмножини всіх номерів допоміжних термів

$$\mathbf{NUM'_i} = \{\bigcup_{j=1}^{m_i} NUM'_{ij}\}$$

(див. (4.2)), де кожне NUM'_{ij} відповідно до (4.3) приймає вигляд

$$NUM'_{ij} = \begin{cases} s-1, \ якщо\ (s = r_j) \vee (XP^1_{ijs-1} \le XP^1_{ijs+1}) \\ s+1, \ якщо\ (s = 1) \vee (XP^1_{ijs-1} > XP^1_{ijs+1}) \end{cases}$$

і далі, знаходяться допоміжні терми.

Наступним, формуються підмножини експертних коефіцієнтів параметрів

$$\mathbf{EC_i} = \{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}} \mathbf{EC_{ij}}\} = \{\, EC_{ij}^{min},\ EC_{ij}^{max} \,\}$$

(див. (4.5)) при цьому EC_{ij}^{min} і EC_{ij}^{max} відповідно є мінімальними і максимальними елементами $(\, EC_{ij}^{min} \le EC_{ij}^{max} \,)$ підмножини $\mathbf{EC_i}$, які характеризують рівень впевненості експерта щодо значень поточних величин.

Далі, визначається експертний коефіцієнт кібератаки EC_i^{CA} (див. (4.9)).

Формування детекційних середовищ

Етап 7 – формування детекційних середовищ. Формування детекційного середовища ($\mathbf{DR}$) засновується на побудові підмножини базових детекційних правил $\mathbf{DR_i}$ (див. п. 2.1 і 4.2 та [1, 12]), яке необхідне для виявлення *i*-ї кібератаки на основі параметричних підсередовищ ($\mathbf{P_i}$) різних розмірностей (п. 2.1).

Для цього, формуються підмножини всіх можливих ІД аномальності

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{IA_i}\} = \{\bigcup_{i=1}^{n} \{\bigcup_{u=1}^{v_i} IA_{iu}\}\}$$

(див. (4.14)), за допомогою яких (у лінгвістичній формі) можна відобразити можливі рівні аномального стану в *m*-вимірному гетерогенному параметричному середовищі ($\mathbf{P}$), породженому кібератакою з ідентифікатором CA_i (див. етап 1) для підмножини правил $\mathbf{DR_i}$.

Далі, на основі підмножини всіх побудованих бінарних вирішальних функцій

$$\mathbf{SF_i} = \{\bigcup_{a=1}^{w_i} SF_{ia}\},$$

$$(\, SF_{ia} = SF_{ia}(\ \mathbf{SAF_{ia}}\ ))$$

(див. (4.24) та (4.25)), формуються підмножини всіх аргументів вирішальних функцій

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{AF_i}\} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \{\bigcup_{\mathbf{a=1}}^{\mathbf{w_i}} \langle \mathbf{SAF_{ia}} \rangle\}\}$$

(див. (4.22)).

Далі, кожне базове правило може породити v_i детекційних виразів

$$\mathbf{DR_i} = \{\bigcup_{a=1}^{w_i} \{\bigcup_{u=1}^{v_i} if \;\; SF_{ia} \;\; then \;\; IA_{iu}\}\}$$

(див. (4.31)), а також, з урахуванням SF_{ia} та IA_{iu}, формуються підмножини умовних детекційних виразів

$$\mathbf{DR_i} = \{\bigcup_{\mathbf{a=1}}^{\mathbf{w_i}} \mathbf{DR_{ia}}\}$$

(див. (4.30)), які відображають сформовані базові правила для виявлення *i*-ї кібератаки або CA_i-атаки.

Таким чином, розроблена МПСВ [31, 32], яка за рахунок механізмів формування атакуючих середовищ, побудови m_i-вимірних параметричних еталонних та поточних підсередовищ, α-рівневої номіналізації еталонних та поточних підсередовищ, процесу дефазифікації та визначення ідентифікуючих термів і формування детекційних середовищ, дозволяє будувати системи, що використовуються для визначення рівня аномального стану в *m*-вимірному гетерогенному параметричному середовищі;

СПИСОК ЛІТЕРАТУРИ ДО РОЗДІЛУ 4

1. А. Корченко, «Кортежная модель формирования набора базовых компонент для выявления кибератак», *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, В.2 (28), С. 29-36, 2014.

2. A. Korchenko, K. Warwas, A. Kłos-Witkowska, «The Tupel Model of Basic Components' Set Formation for Cyberattacks», in *Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2015 IEEE 8th International Conference on*, 2015, pp. 478-483.

3. А. Корченко, «Модель базових компонент для виявлення кібератак на ресурси інформаційних систем», *Актуальні проблеми управління інформаційною безпекою держави: VI наук.-практ. конф.*, Київ, 2015, С. 274-275.

4. А. Корченко, «Метод определения идентифицирующих термов для систем обнаружения вторжений», *Безпека інформації*, Т.20, №3, С. 217-223, 2014.

5. А. Корченко, «Метод определения идентифицирующих термов для систем выявления кибератак», *Актуальні питання забезпечення кібернетичної безпеки та захист інформації: наук.-практ. конф.*, Київ, 2015, С. 64-67.

6. А. Корченко, «Метод формирования лингвистических эталонов для систем выявления вторжений», *Захист інформації*, Т.16, №1, С. 5-12, 2014.

7. А. Корченко, «Формирование лингвистических эталонов на основе кортежной модели для систем выявления вторжений», *Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS`2015): 7-та Всеук. наук.-практ. конф.*, с. Коблево Миколаївської обл., 2015, С. 43-46.

8. B. Akhemetov, A. Korchenko, S. Akhmetova, N. Zhumangalieva, «Improved method for the formation of linguistic standards for of intrusion detection systems», *Journal of Theoretical and Applied Information Technology*, vol. 87, no. 2, pp. 221-232, 2016.

9. Anna Korchenko, «Formation of linguistic standards for of intrusion detection systems», *Безопасность в авиации и космические технологии: VIII Всемирный конгресс «Авиация в XXI столетии»*, Киев, 2018, С. 3.2.1.-3.2.6.

10. А. Корченко, «Формирование эвристических правил для систем обнаружения вторжений», *Актуальні проблеми забезпечення інформаційної безпеки держави : наук.-техн. конф.*, Київ, 2014, С. 23-24.

11. Б.С. Ахметов, А.А. Корченко, Н.К. Жумангалиева, «Модель решающих правил для обнаружения аномалий в информационных системах», *Известия Национальной Академии наук Республики Казахстан. Серия физико-математическая*, №4 (308), С. 91-100, 2016.

12. Н. Карпинский, А. Корченко, С. Ахметова, «Метод формирования базовых детекционных правил для систем обнаружения», *Захист інформації*, Т.17, №4, С. 312-324, 2015.

13. Н. Карпинский, А. Корченко, С. Ахметова, Н. Жумангалиева, «Метод построения условных детекционных выражений для систем обнаружения кибератак», *Актуальні питання забезпечення кібернетичної безпеки та захист інформації: ІІ міжнар. наук.-практ. конф.*, Київ, 2016, С. 65-69.

14. А. Корченко, «Метод фаззификации параметров на лингвистических эталонах для систем выявления кибератак», *Безпека інформації*, Т.20, №1, С. 21-28, 2014.

15. Н. Карпинский, А. Корченко, С. Казмирчук, «Фаззификация параметров в кортежной модели для выявления кибератак», *Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS`2016): 8-та Всеук. наук.-практ. конф.*, с. Коблево Миколаївської обл., 2016, С. 39-42.

16. А. Корченко, «Метод α-уровневой номинализации нечетких чисел для систем обнаружения вторжений», *Захист інформації*, Т.16, №4, С. 292-304, 2014.

17. Н. Карпинский, А. Корченко, П. Викулов, Н. Жумангалиева, «Номинализация нечетких величин для систем выявления аномалий», *Современные информационные и коммуникационные технологии на транспорте, в промышленности и образовании (TEMPUS: CITISET): X междунар. науч.-практ. конф.*, Днипро, 2016, С. 51-52.

18. А. Корченко «Модели систем выявления аномалий, порожденных кибератаками», *Эвристические алгоритмы и распределенные вычисления в прикладных задачах: Коллективная монография*, Выпуск 2, Под ред. Б.Ф. Мельникова, Ульяновск, 2013, С. 56-86.

19. Б.С. Ахметов, А.А. Корченко, Н.К. Жумангалиева, «Технология выявления аномального состояния для систем обнаружения

вторжений», *Вестник Казахского национального университета. Серия математика, механика, информатика*, №1 (88), С. 106-113, 2016.

20. А. Корченко, «Метод выявления аномалий, порожденных кибератаками в компьютерных сетях», *Проблемы информатизации: I междунар. науч.-техн. конф.*, Черкасы, 2013, С. 25.

21. Терейковский И.А., Терейковская Л.А., Корченко А.О., Ахметов Б.Б., Алібієва Ж.М., «Нейросетевое распознавание рукописных символов в системе биометрической аутентификации», *Інформаційні технології в економіці і природокористуванні*, №2, С. 29-44, 2017.

22. А. Корченко, С. Ахметова, «Классификация систем обнаружения вторжений», *Інформаційна безпека*, №1, №2, С. 168-175, 2014.

23. Б. Ахметов, А. Корченко, С. Ахметова, Н. Жумангалиева, «Использование методов экспертного оценивания в системах обнаружения вторжений», *Інформаційна безпека*, №3, №4, С. 34-43, 2014.

24. С. Казмірчук, А. Корченко, Т. Паращук, «Аналіз систем виявлення вторгнень», Захист інформації, Т.20, №4, С. 259-276, 2018.

25. І. Терейковський, А. Корченко, Т. Паращук, Є. Педченко, «Аналіз відкритих систем виявлення вторгнень», Безпека інформації. Т.24, №3, С. 201-216, 2018.

26. А. Корченко, С. Ахметова, «Базовые признаки классификации систем обнаружения вторжений», *Современные информационно-телекоммуникационные технологии: междунар. науч.-тех. конф.,* Казахстан, ГУТ, 2015, С. 24-26.

27. Б. Ахметов, А. Корченко, Н. Жумангалиева, «Анализ методов нечетких множеств для построения систем обнаружения вторжений», *Современные информационно-телекоммуникационные технологии»: междунар. науч.-тех. конф.* Казахстан, ГУТ, 2015, С. 38-40.

28. Б. Ахметов, А. Корченко, С. Ахметова, Н. Жумангалиева, «Анализ методов экспертного оценивания для систем обнаружения», *Информационные и телекоммуникационные технологии: образование, наука, практика: II междунар. науч.-практич. конф.*, Алматы, II том, 2015, С. 28-31.

29. К. Ануфрієнко, А. Корченко, «Напрямки застосування прогнозування у галузі управління уразливостями програмного забезпечення», *ITSEC : VI міжнар. наук.-техн.конф*., Київ, 2016, С.126.

30. А. Корченко, В. Щербина, Т. Паращук, «Аналіз програмних засобів виявлення вторгнень», *Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS-2018) : X Всеук. наук.-практ. конф.,* с. Коблево Миколаївської обл., 2018, С. 48-49.

31. А. Корченко, Б. Ахметов, В. Щербина, П. Викулов, «Структурно-аналитическая модель методологии построения систем выявления вторжений», *Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS`2017): 9-та Всеук. наук.-практ. конф.*, с. Коблево Миколаївської обл., 2017, С. 42-44.

32. А. Корченко, В. Щербина, Н. Вишневская, «Методология построения систем выявления аномалий порожденных кибератаками», *Захист інформації*, Т.18, №1, С. 30-38, 2016.

РОЗДІЛ 5. ЗАСОБИ РОЗШИРЕННЯ ФУНКЦІОНАЛЬНИХ МОЖЛИВОСТЕЙ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

5.1. Система виявлення кібератак

На базі МПСВ породжених кібератаками (див. п. 4.3 і [1, 2]), в основу якої закладена КМАС (див. п. 2.1 та [3-5]) і методи МФЕС (див. п. 2.2-2.4 та [6-12]), МФП (див. п. 3.1 і [13, 14]), МАН (див. п. 3.2 та [15-17]), МВІТ (див. п. 3.3 та [18, 19]), МДП (див. п. 4.1) і МФДС (див. п. 4.2 та [20, 21]), а також з урахуванням [22-27] та проведеного в [28-30] аналізу побудуємо систему виявлення кібератак (СВК) [31]. Вона дозволить ефективно детектувати в слабоформалізованому нечітко визначеному середовищі аномальний стан за заданий проміжок часу.

Структурне рішення СВК відображено на рис. 5.1. Воно містить узгоджені за параметрами:

- бази даних кібератак (БДК);
- бази даних правил (БДП);
- бази даних еталонів (БДЕ);

а також модулі:

- формування поточних значень (МФПЗ);
- α-рівневої номіналізації (МАРН);
- дефазифікації та ідентифікуючих термів (МДІТ);
- рівня аномальності (МРА);
- візуалізації (МВ).

База БДК містить множину ІД кібератак

$$CA_i,\ (i=\overline{1,n})$$

(див. (2.2), [3]), за допомогою яких здійснюється однозначне визначення атаки в процесі присвоєння її імені конкретному ІД (див. етап 1 в п. 4.3 та [1]).

База БДП складається з бінарних вирішальних функцій

$$SF_{ia},\ (i=\overline{1,n},\ a=\overline{1,w_i})$$

(див. (4.24), [20]) та ІД аномальності

$$IA_{iu},\ (i=\overline{1,n},\ u=\overline{1,v_i})$$

(див. (4.14)), що входять в множини базових правил

$$\mathbf{DR_i}\ \ (i=\overline{1,n})$$

(див. (4.30)), які необхідні для виявлення *i*-ї кібератаки за допомогою параметричних підсередовищ ($\mathbf{P_i}$) різної розмірності (див. етап 7 в п. 4.3).

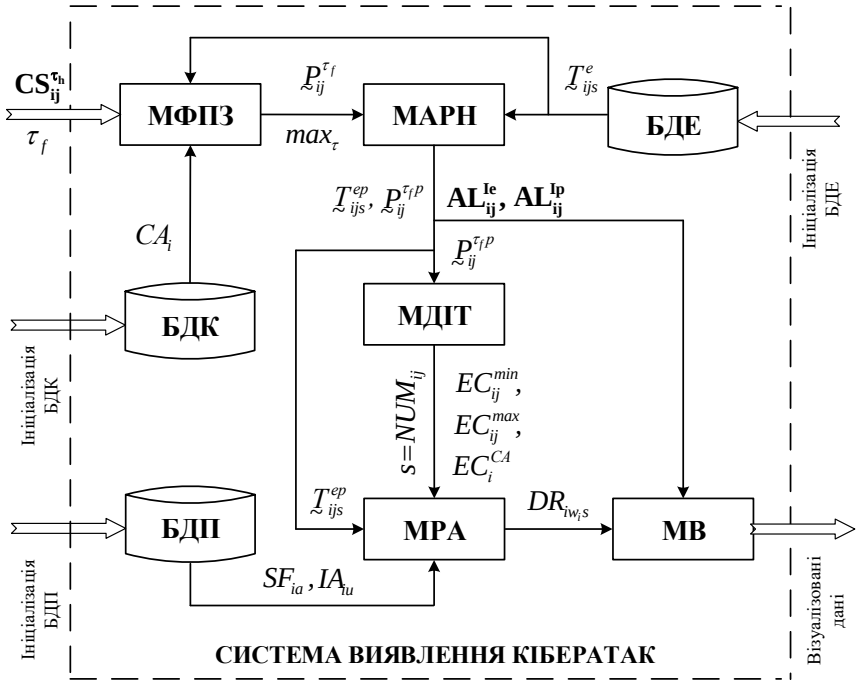

Рис. 5.1. Структурна схема СВК

База БДЕ містить множину лінгвістичних еталонів

$$\underset{\sim}{T}^{e}_{ijs},\ (i=\overline{1,n},\ \ j=\overline{1,m_i},\ \ s=\overline{1,r_j})$$

(див. (2.52), [6]), призначених для відображення стану множин відповідних параметрів

$$\mathbf{P_i},\ (i=\overline{1,n})$$

у визначеному середовищі оточення, що направлені на виявлення кібератаки з ІД CA_i (див. етап 3 в п. 4.3).

Модуль МФПЗ призначений для формування всіх можливих поточних значень нечітких параметрів

$$\underset{\sim}{P}_{ij}^{\tau_f},\ (i=\overline{1,n},\ \ j=\overline{1,m_i})$$

(див. етап 2 в п. 4.3), одержаних за допомогою

$$\mathbf{T_i^e},\ (i=\overline{1,n})$$

у визначений момент часу τ_f за його заданий проміжок, тривалість якого $\tau_h=\tau_f-\tau_{f-1}$ $(f=\overline{1,max_\tau})$ (див. п. 2.1).

Модуль МАРН здійснює еквівалентне перетворення НЧ за допомогою зведення всіх еталонних $\underset{\sim}{T}_{ijs}^{e}$ та поточних $\underset{\sim}{P}_{ij}^{\tau_f},\ (i=\overline{1,n},\ j=\overline{1,m_i},\ s=\overline{1,r_j})$ величин до номінального (одного для всіх) числа компонент на основі підмножин α-рівневих інтервалів $\mathbf{AL_{ij}^{Ie}}$ та міжточкових α-рівневих інтервалів $\mathbf{AL_{ij}^{Ip}}$ (див. етап 5 в п. 4.3).

Модуль МДІТ орієнтований на пошук, відповідно до заданої лінгвістичної змінної, ідентифікуючого еталонного терма (тобто його номера, а $s=NUM_{ij}$), за яким із допомогою детекційних виразів та отриманих числових оцінок $(EC_{ij}^{min},\ EC_{ij}^{max},\ EC_i^{CA})$, які інтерпретують лінгвістичні параметри можна визначити рівень аномального стану, що характерний для визначеного типу кібератак (див. етап 6 в п. 4.3).

Модуль МРА необхідний для формування DR_{iw_is} на основі ідентифікуючого еталонного терма (використання NUM_{ij}), еталонного перетвореного НЧ $\underset{\sim}{T}_{ijs}^{ep}$, а також ідентифікаторів аномальності IA_{iu} та бінарних вирішальних функцій SF_{ia}, за допомогою обробки підмножин умовних детекційних виразів

$$\mathbf{DR_i}=\{\bigcup_{a=1}^{w_i}\{\bigcup_{u=1}^{v_i} if\ \ SF_{ia}\ \ then\ \ IA_{iu}\}\},$$

$$(i=\overline{1,n},\ a=\overline{1,w_i},\ u=\overline{1,v_i}),$$

що відображають сформовані базові правила для виявлення *i*-ї кібератаки з використанням параметричних підсередовищ ($\mathbf{P_i}$) різної розмірності (див. етап 7 в п. 4.3).

Модуль МВ використовується для графічної інтерпретації полі-параметричного мультирозмірного середовища (див. п. 2.1), розподілу ідентифікаторів атакуючих дій та фазифікованих значень поточних параметрів $\underset{\sim}{P}_{ij}^{\tau_f p}$ відносно лінгвістичних еталонів $\mathbf{T}_{\mathbf{ij}}^{\mathbf{ep}}$ у вигляді визначеної області, яка характеризує атаки, а також відображення умовного виразу ($DR_{iw_i s}$) базового детекційного правила, відповідно до якого було здійснено виявлення кібератак.

Система СВК (побудова якої здійснюється відповідно до відомої методології (див. п. 4.3) за допомогою 7 етапів) відповідно до алгоритму, який представлений на рис. 5.2, функціонує наступним чином.

Умовно роботу СВК можна представити двома процесами:

1) процес ініціалізації БД;

2) процес виявлення кібератак (див. рис. 5.2).

Процес ініціалізації БД пов'язаний з наповненням (модифікацією) БДК, БДП та БДЕ (див. відповідно вершини 1-3, 8; 1, 2-8; та 1, 2, 9-12 на рис. 5.2).

За необхідністю, на етапі функціонування СВК, вказані БД можуть піддаватися модифікації.

Процес виявлення кібератак CA_i здійснюється за заданий часовий проміжок τ_h в кожний момент часу τ_f ($f = \overline{1, max_\tau}$, де max_τ – максимальний номер часового проміжку f) (див. вершину 13 на рис. 5.2) на основі множини значень лічильників сенсорів $\mathbf{CS}_{\mathbf{ij}}$ (див. (3.3) та вершини 14-16), показники яких залежать від τ_h ($\mathbf{CS}_{\mathbf{ij}}^{\boldsymbol{\tau}_\mathbf{h}}$), а також НЧ $\underset{\sim}{T}_{ijs}^{e}$ еталонного підсередовища ($\mathbf{T}_{\mathbf{i}}^{\mathbf{e}}$), які передаються із БДЕ та надходять в модуль МФПЗ, де формуються поточні значення нечітких параметрів $\underset{\sim}{P}_{ij}^{\tau_f}$ та визначається max_τ (див. вершини 17-20).

Далі, з БДЕ та МФПЗ відповідно НЧ $\underset{\sim}{T}_{ijs}^{e}$ і $\underset{\sim}{P}_{ij}^{\tau_f}$ еталонного та поточного підсередовищ ($\mathbf{T}_{\mathbf{i}}^{\mathbf{e}}$ та $\mathbf{P}_{\mathbf{i}}^{\boldsymbol{\tau}_\mathbf{f}}$) надходять в МАРН, де здійснюється їх α-рівнева номіналізація (див. рис. 5.2 вершини 21-24).

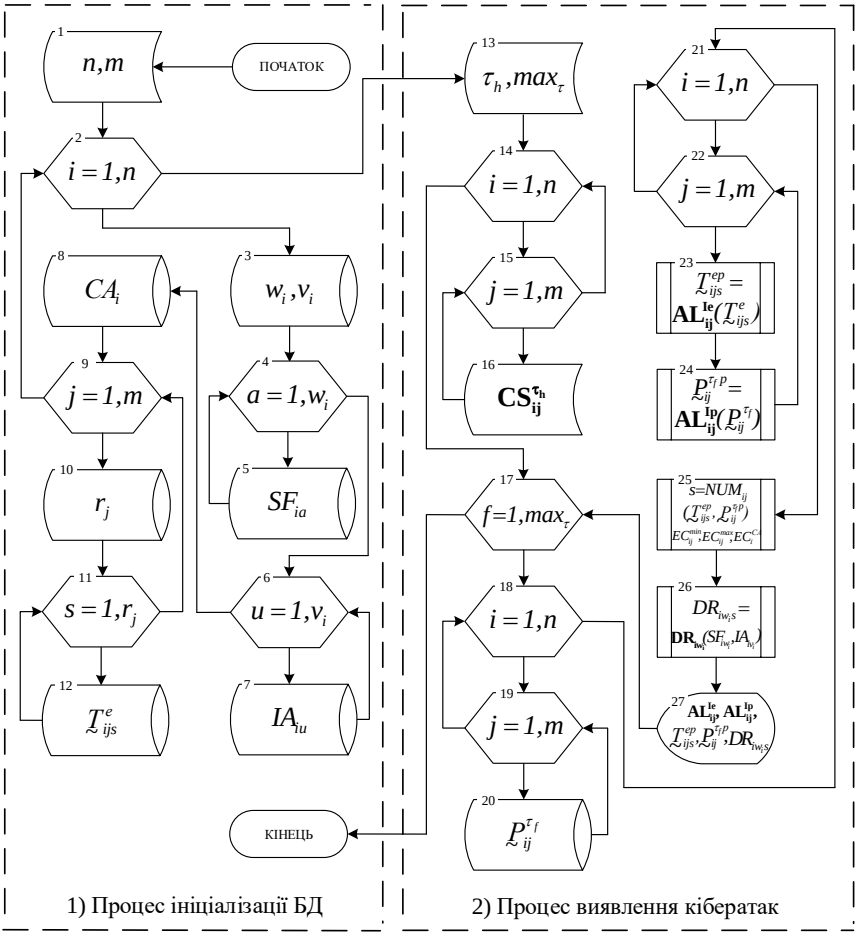

Рис. 5.2. Алгоритм роботи СВК

У результаті цього, з МАРН на вхід МДІТ надходять перетворені НЧ $\underset{\sim}{T}^{ep}_{ijs}$ та $\underset{\sim}{P}^{\tau_f p}_{ij}$, де визначаються ідентифікуючі терми (у яких $s = NUM_{ij}$). На їх основі отримуємо числові оцінки у вигляді експертних коефіцієнтів параметрів і кібератак (EC^{min}_{ij}, EC^{max}_{ij} і

EC_i^{CA}), які інтерпретують лінгвістичні параметри і в сукупності відображають аномальність поточного стану середовища оточення, породженого визначеними кібератаками (див. вершину 25 на рис. 5.2).

Далі, на основі отриманих в МАРН ідентифікуючих термів $\underset{\sim}{T}_{ijs}^{ep}$ та термів, для яких $s = NUM_{ij}$, що надійшли з МДІТ, а також бінарних вирішальних функцій SF_{ia} (див. (4.24)) та ідентифікаторів аномальності IA_{iu} (див. (4.14)), які надходять з БДП, в МРА формуються підмножини базових правил $\mathbf{DR_i}$ (див. (4.30)), за допомогою яких визначається умовний вираз $DR_{iw_i s}$, за яким здійснюється виявлення *i*-ї кібератаки (див. вершину 26 на рис. 5.2).

На основі підмножини α-рівневих інтервалів $\mathbf{AL_{ij}^{Ie}}$, міжточкових α-рівневих інтервалів $\mathbf{AL_{ij}^{Ip}}$, а також всіх перетворених $\underset{\sim}{T}_{ijs}^{ep}$ і $\underset{\sim}{P}_{ij}^{\tau_f p}$, що надійшли з МАРН та умовного виразу $DR_{iw_i s}$, який надійшов з МРА, в МВ графічно інтерпретуються ідентифікатори атакуючих дій (що відображаються за допомогою багатовимірних (наприклад, двовимірних або тривимірних) опорних областей, наприклад, Н, БНВ, БВН, В, П [22]) та фазифіковані значення поточних параметрів $\underset{\sim}{P}_{ij}^{\tau_f p}$ відносно лінгвістичних еталонів $\mathbf{T_{ij}^{ep}}$ відповідно (див. вершину 27 на рис. 5.2).

Таким чином, запропонована СВК [31, 32], яка за рахунок баз даних кібератак, правил та еталонів, а також модулів формування поточних значень, α-рівневої номіналізації, дефазифікації та ідентифікуючих термів, рівня аномальності та візуалізації дозволяє будувати засоби, що розширюють функціональні можливості сучасних СВВ, за допомогою визначення рівня аномального стану, характерного впливу певного типу кібератак в слабоформалізованому нечіткому середовищі оточення.

Далі, для наступного виявлення кібератак необхідно розробити алгоритмічне та програмне забезпечення формування еталонів параметрів для систем виявлення аномалій.

5.2. Алгоритмічне та програмне забезпечення формування еталонів параметрів для систем виявлення кібератак

Відповідно до запропонованого структурного рішення СВК (див. п. 5.1 та [31, 32]), яке базується на МПСВ (див. п. 4.3 і [1, 2]), в основу якої закладена КМАС (див. п. 2.1 та [3-5]), а також методи МФЕС (див. п. 2.2 і [6-12]) та МФДС (див. п. 4.2 і [20, 21]) побудуємо і проведемо експериментальне дослідження алгоритмічного та програмного забезпечення формування еталонів параметрів для систем виявлення аномалій [33].

Таке забезпечення функціонує на основі базового алгоритму System_level_Click (рис. 5.3), що поєднує низку наступних зумовлених процесів (процедур):

- Coordinate_axes
  (конструювання координатної сітки для μ і x);
- Convert_List
  (ініціалізація величин на основі БДК і БДЕ (див. п. 5.1 та [31]) та МФПЗ. Відповідно до структури СВК (див. п. 5.1) визначаються координати еталонних $\underset{\sim}{I}^{e}_{ijs}$ та поточних $\underset{\sim}{P}^{\tau_f}_{ij}$ НЧ в m_i-вимірному параметричному підсередовищі ($\mathbf{P_i}$) (рис. 5.3));
- Graph_Build
  (графічне формування параметрів, наприклад, $P_{31} = P_{SPKOП} = KOП$ і $P_{32} = P_{SPKПOA} = KПOA$ та їх відображення на об'єкті Canvas відповідно до етапу 3 (див. п. 4.3 та [1]));
- Crossing
  (реалізуються процедури IntersectionPoint і GetPoint та здійснюється відображення поточного стану системи відповідно до базових правил $\mathbf{DR_i}$ в детекційному середовищі ($\mathbf{DR}$) (див. етап 5-7 в п. 4.3));
- Rect_Area
  (будуються двовимірні опорні області (див. етап 5 в п. 4.3) відповідно до заданих правил, які надходять з БДП (див. п.

5.1), що формуються на основі $\mathbf{DR_i}$ $(i=\overline{1,n})$ та використовуються для виявлення *i*-ї кібератаки на основі параметричних підсередовищ ($\mathbf{P_i}$) різної розмірності);

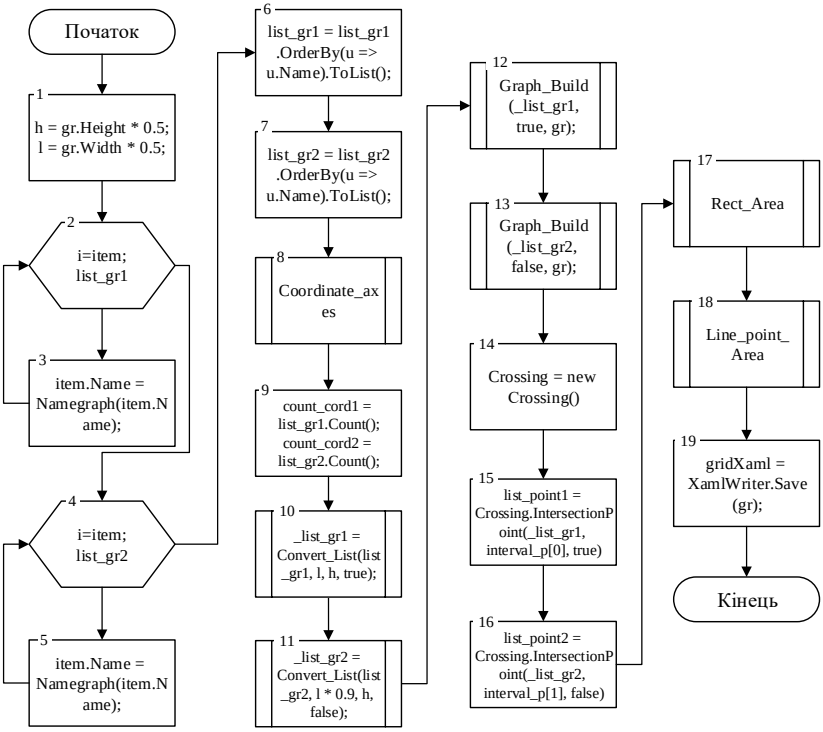

Рис. 5.3. Базовий алгоритм System_level_Click

- Line_point_Area
  (відповідно до етапу 5 (див. п. 4.3) будуються і відображаються спільні точки ліній проектування еталонних $\underset{\sim}{T}^{e}_{ijs}$ і поточних $\underset{\sim}{P}^{\tau_f}_{ij}$ НЧ, наприклад, для параметрів $P_{31}=P_{SPKOP}=KOP$ і $P_{32}=P_{SPKPOA}=KPOA$ в *2*-вимірному параметричному підсередовищі ($\mathbf{P_i=P_3=P_{SP}}$)).

Розглянемо принцип роботи головного алгоритму System_level_Click (рис. 5.3), який інтегрує зазначені процедури для побудови повного переліку графічних компонентів необхідних для ефективного виявлення аномального стану в інформаційних системах.

На початку обчислювального процесу (рис. 5.3, вершина 1) відбувається ініціалізація необхідних консольних характеристик.

Далі (рис. 5.3, вершина 2-3 та 4-5), відповідно, отримуємо в циклах початкові дані з БДЕ [31], наприклад, для параметрів КОП та КПОА. Наступним (рис. 5.3, вершина 6-7) формуються множини порядку параметрів відповідно до (2.14) та (2.16).

Наступним (рис. 5.3, вершина 8), реалізується зумовлений процес (клас Coordinate_axes), відповідно до якого виконується процедура Main_coordinate_axes (рис. 5.4), що здійснює послідовну обробку трьох підпрограм градуювання:

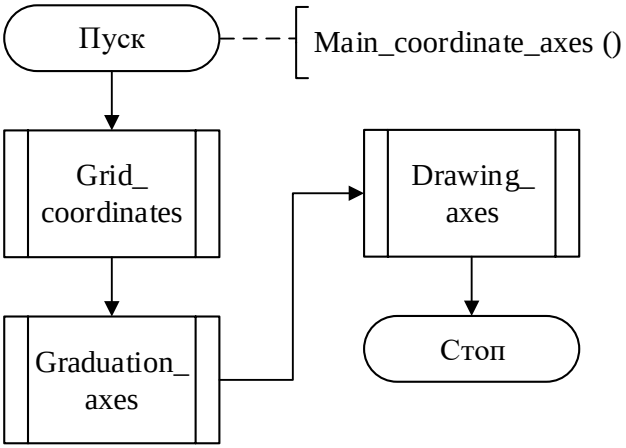

Рис. 5.4. Алгоритм Main_coordinate_axes

- Grid_coordinates
  (відповідає за побудову масштабованої координатної сітки);
- Graduation_axes
  (відповідає за маркування осей μ і x, інтервали градуювання в масштабованій області);

- Drawing_axes
  (відповідає за побудову осей для відображення необхідних параметрів, наприклад, $P_{31} = P_{SPKOП} = КОП$ і $P_{32} = P_{SPKПОА} = КПОА$ в *2*-вимірному параметричному підсередовищі ($\mathbf{P_i = P_3 = P_{SP}}$) (див. п. 2.2).

Далі (рис. 5.3, вершина 9), відповідно до структури СВК (див. п. 5.1) визначається кількість даних (count_cord1 і count_cord2) у БДЕ для кожного з параметрів, наприклад, $P_{31} = P_{SPKOП} = КОП$ і $P_{32} = P_{SPKПОА} = КПОА$.

На наступному етапі (рис. 5.3, вершини 10 та 11) викликається процедура Convert_List (рис. 5.5), яка дозволяє отримувати дані з таблиць за визначеними параметрами (відповідно до етапу 3 п. 4.3), наприклад, КОП та КПОА, які конвертуються в форму необхідну для побудови графічних зображень заданих параметрів, наприклад, $P_{31} = P_{SPKOП} = КОП$ і $P_{32} = P_{SPKПОА} = КПОА$ в *2*-вимірному параметричному підсередовищі ($\mathbf{P_i = P_3 = P_{SP}}$).

Процес конвертування даних складається з двох етапів.

Перший, відповідно до етапу 4 (див. п. 4.3) визначає інтервал, якому належить вершина графічного зображення поточного НЧ $\underset{\sim}{P}_{ij}^{\tau_f}$ в m_i-вимірному поточному підсередовищі ($\mathbf{P_i^{\tau_f}}$).

Це необхідно для пошуку спільних точок графічних зображень еталонних $\underset{\sim}{T}_{ijs}^{e}$ та поточного $\underset{\sim}{P}_{ij}^{\tau_f}$ НЧ, оскільки зазначені точки повинні лежати в одних межах з вершиною $\underset{\sim}{P}_{ij}^{\tau_f}$ будь-якого з параметрів.

Другий – конвертує еталонні $\underset{\sim}{T}_{ijs}^{e}$ та поточні $\underset{\sim}{P}_{ij}^{\tau_f}$ НЧ (які знаходяться в БДЕ та МФПЗ (див. п. 5.1)) у значення, що відповідають системі координат Canvas. Зазначена процедура повертає список конвертованих значень НЧ та меж, де можуть знаходитись спільні точки графічного зображення поточного стану (див. етап 4 в п. 4.3), наприклад, для параметрів $P_{31} = P_{SPKOП} = КОП$ і $P_{32} = P_{SPKПОА} = КПОА$.

Отриманні дані необхідні для побудови проекцій та спільних точок графічних зображень за заданими параметрами КПОА і КОП.

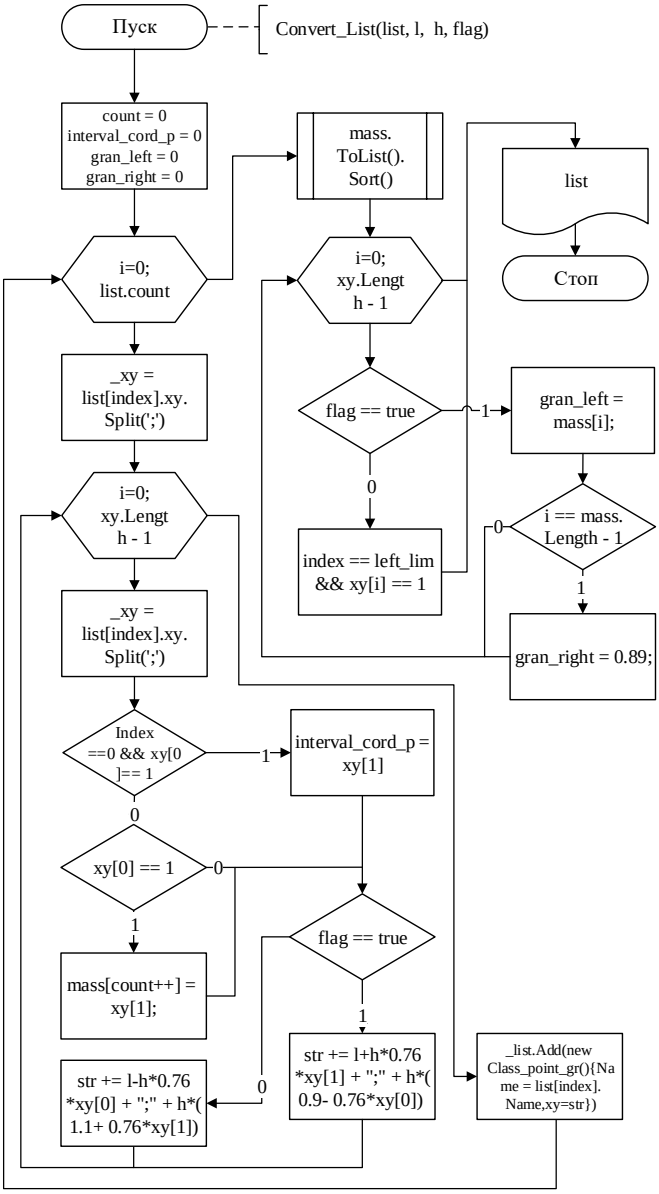

Рис. 5.5. Алгоритм реалізації Convert_List

Далі (рис. 5.3, вершини 12-13), викликається процедура Graph_ Build (рис. 5.6), що на підставі БДЕ та МФПЗ (див. п. 5.1) дозволяє будувати графічні зображення еталонних $\underset{\sim}{T}^{e}_{ijs}$ та поточних $\underset{\sim}{P}^{\tau_f}_{ij}$ НЧ.

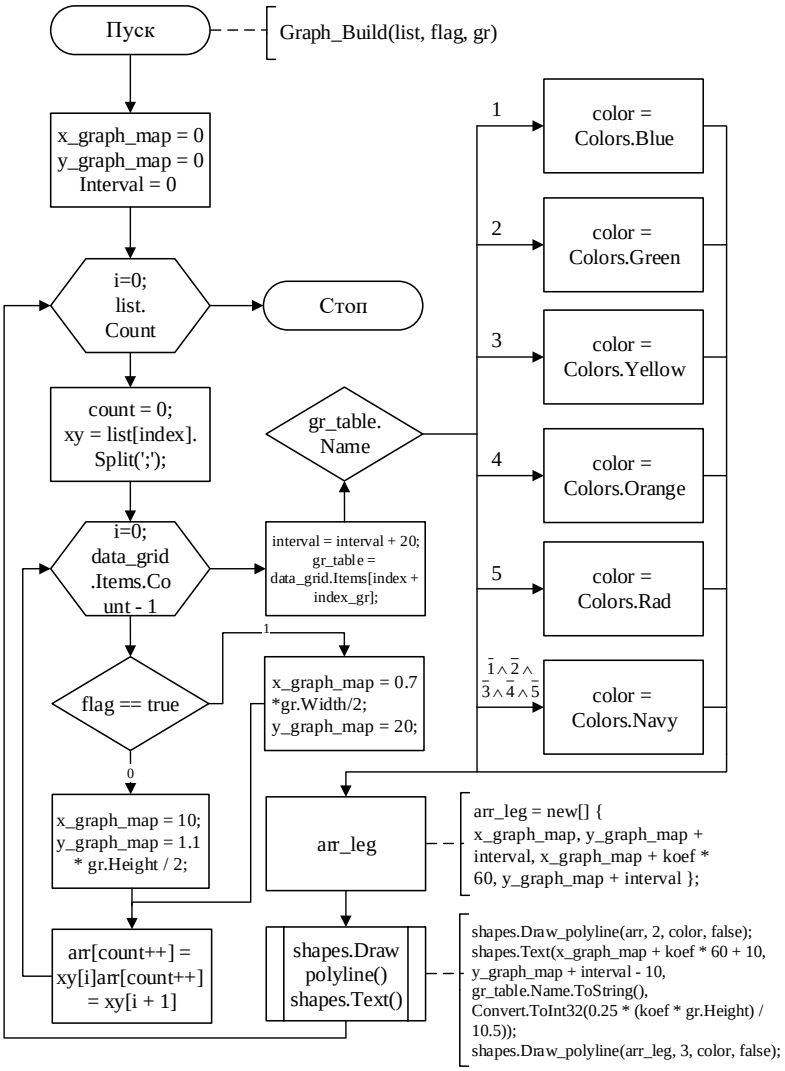

Рис. 5.6. Алгоритм реалізації Graph_Build

Після проведення процесу конвертування даних з БДЕ вони передаються в підпрограму Graph_Build, яка при виклику отримує список конвертованих даних у вигляді індексу для отримання кольору та зміни графічного об'єкта Canvas для побудови базових значень.

Використовуючи Main_figures створюється об'єкт класу shapes в тілі Graph_Build і далі за допомогою shapes викликається Draw_polyline та дані зі списку записуються в масив. Також визначаються варіації кольорів та типів ліній.

Виконання в циклі зазначеної послідовності дій пов'язане з побудовою графічних зображень та їх легенд (наприклад, «Р», «ОМ», «М», «С», «Б» та «ОБ» для параметрів $P_{31} = P_{SPKOП} = КОП$ і $P_{32} = P_{SPKПОА} = КПОА$ (див. рис. 5.7 та 5.8) в *2*-вимірному параметричному підсередовищі ($\mathbf{P_i = P_3 = P_{SP}}$) (див. п. 2.2)).

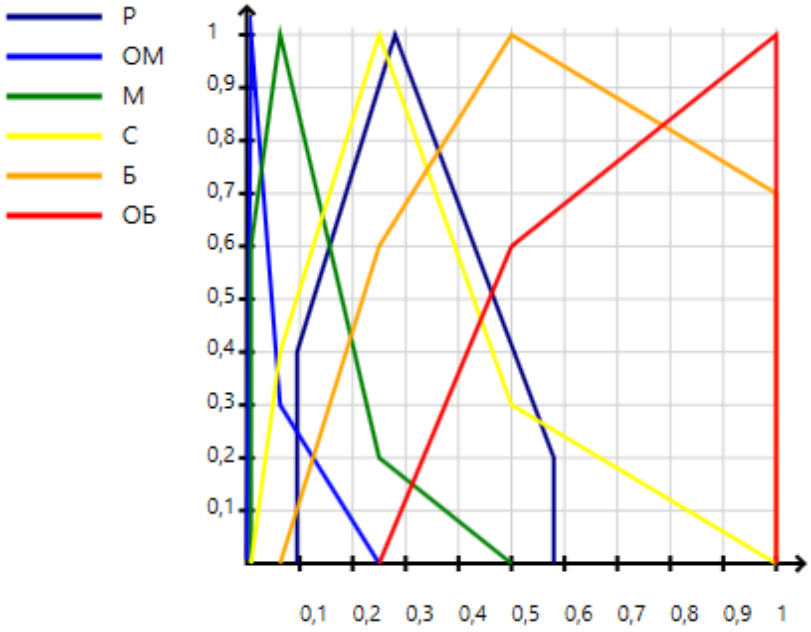

Рис. 5.7. Результат роботи процедури Graph_Build
для параметра КОП

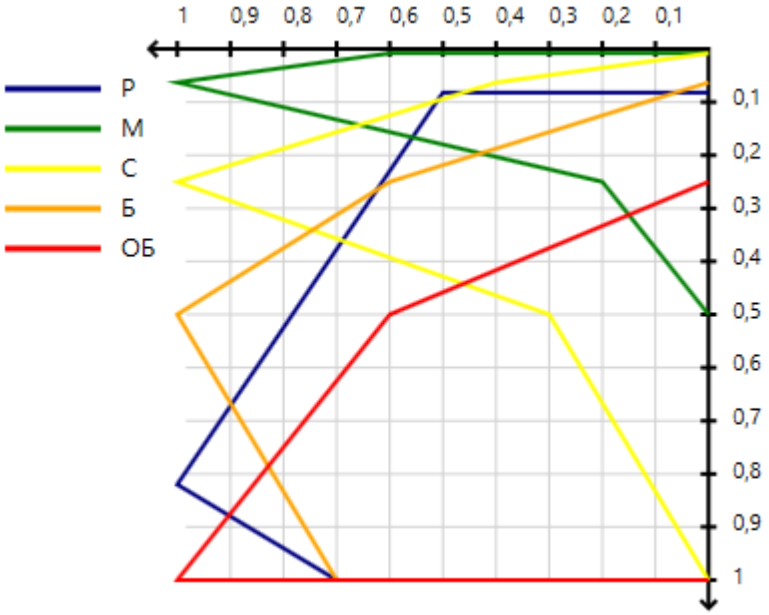

Рис. 5.8. Результат роботи процедури Graph_Build
для параметра КПОА

На наступному етапі (рис. 5.3, вершина 14) створюється об'єкт класу Crossing і викликається процедура IntersectionPoint та формується список координат спільних точок, необхідних для відображення поточного стану системи.

Отримавши список та ідентифікатори еталонних НЧ за допомогою Convert_List (рис. 5.3, вершини 10-11), визначаються параметри ідентифікації опорних областей за допомогою Draw_main_rect.

Слід зазначити, що клас Crossing складається з двох процедур:

- IntersectionPoint (рис. 5.9);
- GetPoint (рис. 5.10).

Перша процедура IntersectionPoint дозволяє отримати спільні точки графічних зображень $\underset{\sim}{T}^{e}_{ijs}$ та $\underset{\sim}{P}^{\tau_f}_{ij}$ (окремо для кожного з параметрів), а також для $\underset{\sim}{T}^{e}_{ijs}$ з суміжними еталонними НЧ (див. етап 5 та 6 в п. 4.3).

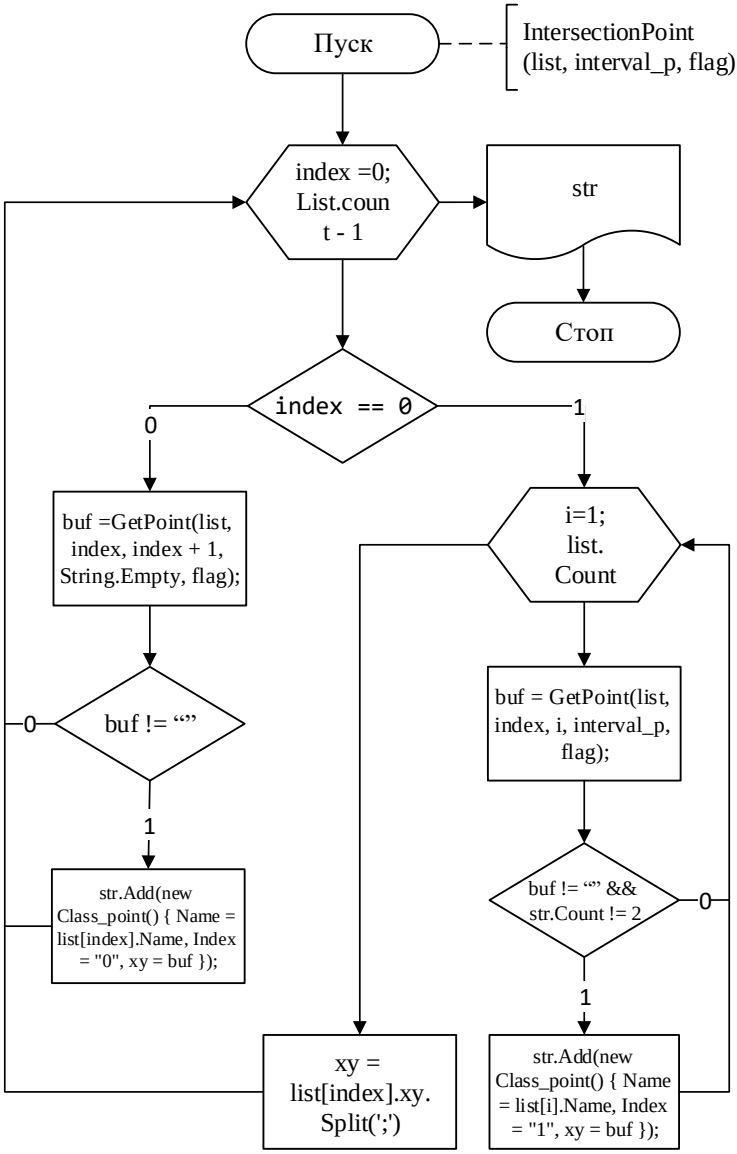

Рис. 5.9. Алгоритм реалізації процедури IntersectionPoint

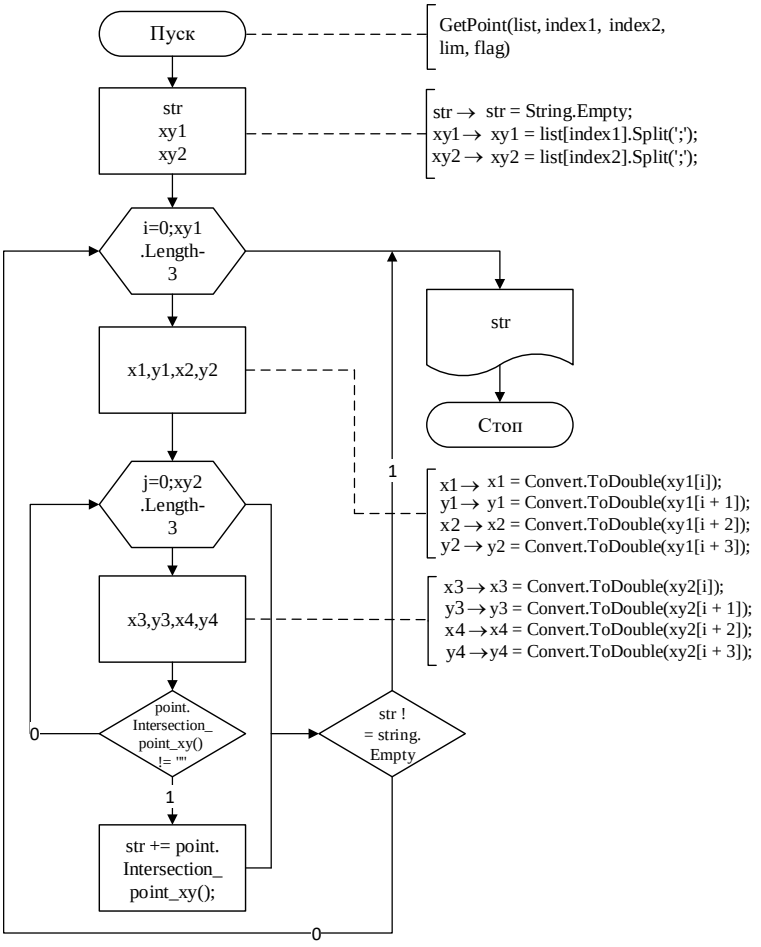

Рис. 5.10. Алгоритм реалізації процедури GetPoint

Друга процедура GetPoint (див. етап 5 та 6 в п. 4.3) відповідає за отримання координат вищезазначених точок, тобто, наприклад, пара значень $(\mu_1; x_1)$ та $(\mu_2; x_2)$, які характеризують складову першого графічного зображення і пара значень $(\mu_3; x_3)$ та $(\mu_4; x_4)$ – другого.

Далі, обчислюються всі можливі значення для обраної складової першого графічного зображення відносно всіх можливих складових

другого. Обчислення здійснюється за допомогою Intersection_point, яка визначає спільні точки складових для заданих координат і повертає до GetPoint.

Наступним (рис. 5.3, вершини 15-16), реалізується клас Intersection_point (відповідно до функціоналу МАРН і МДІТ – див. структуру СВК в п. 5.1), що складається з двох процедур Intersection_point (рис. 5.11) та Intersection_point_xy (рис. 5.12).

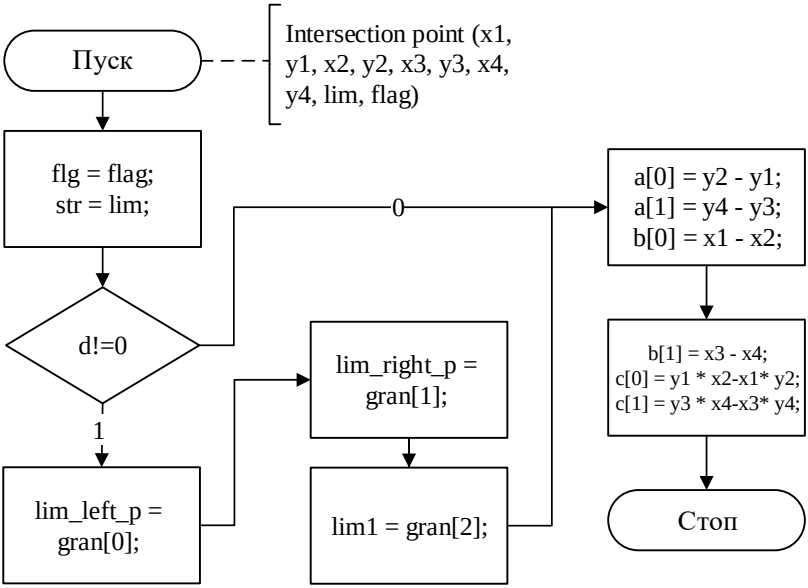

Рис. 5.11. Алгоритм реалізації процедури Intersection_point

У свою чергу, перша є конструктором, що отримує дані з GetPoint (рис. 5.10) та визначає коефіцієнти при μ і x, які передаються в другу – Intersection_point_xy, де розраховуються спільні точки і повертаються в GetPoint.

На наступному етапі (рис. 5.3, вершина 17) викликається процедура Rect_Area (відповідно до функціоналу БДП і МРА – див. структуру СВК в п. 5.1) (рис. 5.13), що відповідає за побудову базових двовимірних областей та областей поточного стану (див. етап 7 в п. 4.3) і послідовно активує Draw_main_rect (рис. 5.14) та Draw_Rect.

Процедура Draw_main_rect відповідає за побудову двовимірних опорних областей з урахуванням правил $\mathbf{DR_i}$, на основі яких буде визначатися рівень аномального стану системи.

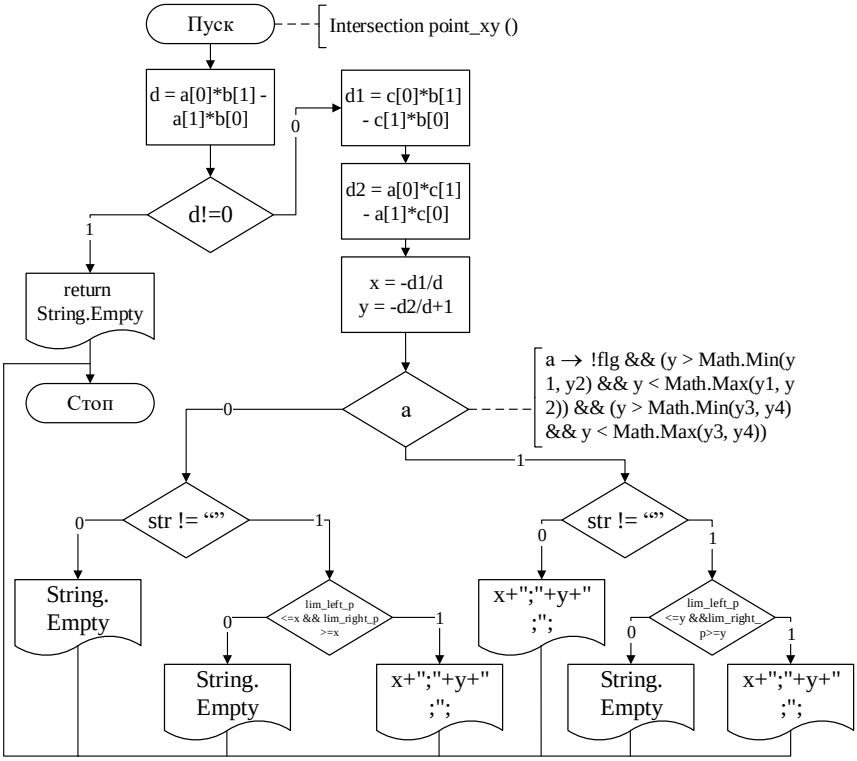

Рис. 5.12. Алгоритм реалізації процедури Intersection_point_xy

Залежно від отриманих даних щодо візуалізації, наприклад, параметрів $P_{31} = P_{SPKOP} = KOP$ і $P_{32} = P_{SPKPOA} = KPOA$ та на основі спільних точок графічних зображень еталонних $\underset{\sim}{T}^{e}_{ijs}$ НЧ та проекцій лінійних компонент, побудованих за допомогою класу Draw_main_ object, отримаємо необхідні опорні області. Їх генерація здійснюється за вище визначеними правилами, тому на графічному зобра-

женні генеруються кольорові області, які відображають рівень аномального стану системи в детекційному середовищі (**DR**) відповідно до $\mathbf{DR_i}$ (див. етап 7 в п. 4.3).

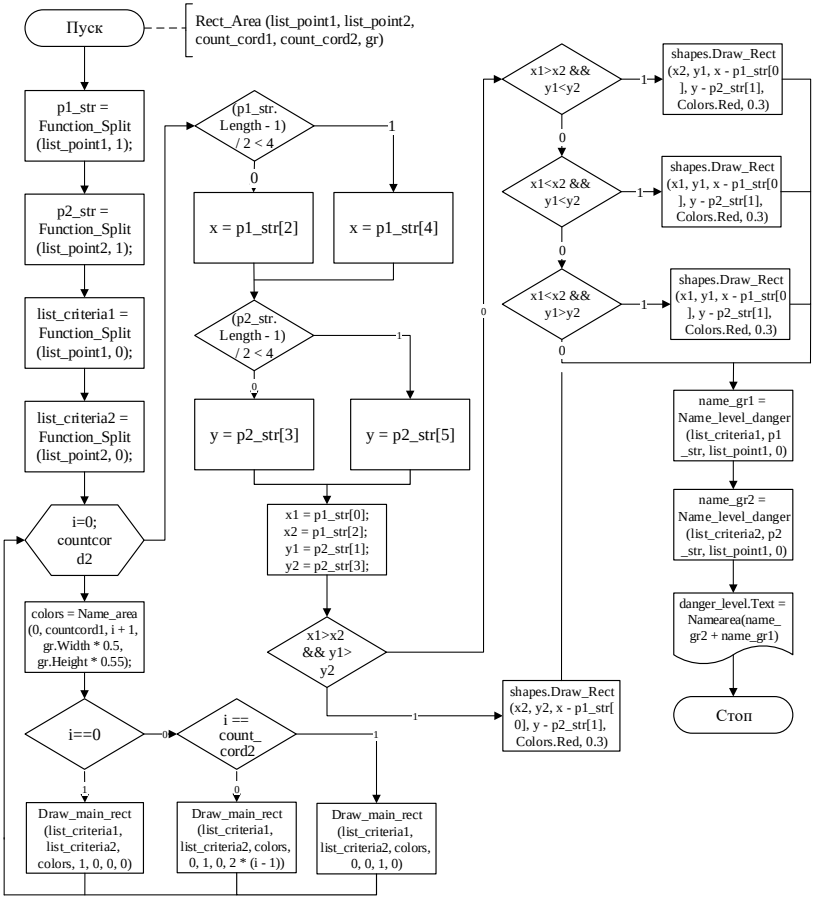

Рис. 5.13. Алгоритм реалізації процедури Rect_Area

Далі (рис. 5.3, вершина 18), викликається підпрограма Line_ point_Area (відповідно до функціоналу МВ – див. структуру СВК в

п. 5.1) (рис. 5.15) і на графічному об’єкті Canvas за допомогою класу Draw_main_object, викликаючи його процедури:

- Draw_main_point (рис. 5.16);
- Draw_main_line (рис. 5.17),

будуються проекції лінійних компонент та спільні точки, як на початкових графічних зображеннях, так і на кінцевому зображенні поточного стану.

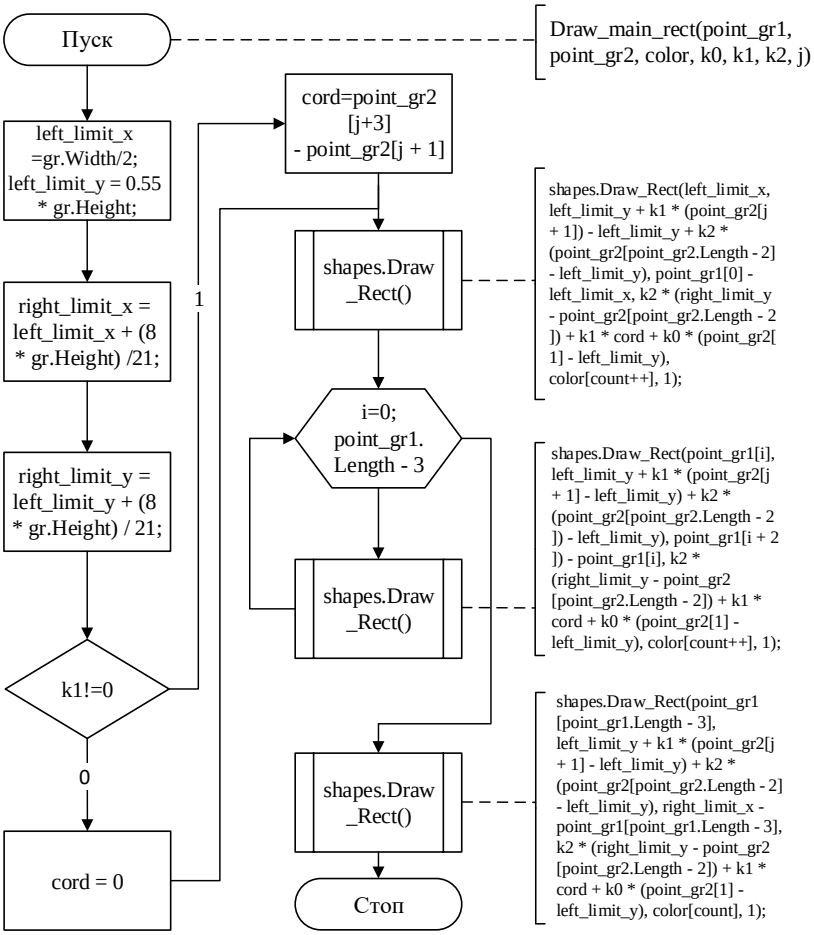

Рис. 5.14. Алгоритм реалізації процедури Draw_main_rect

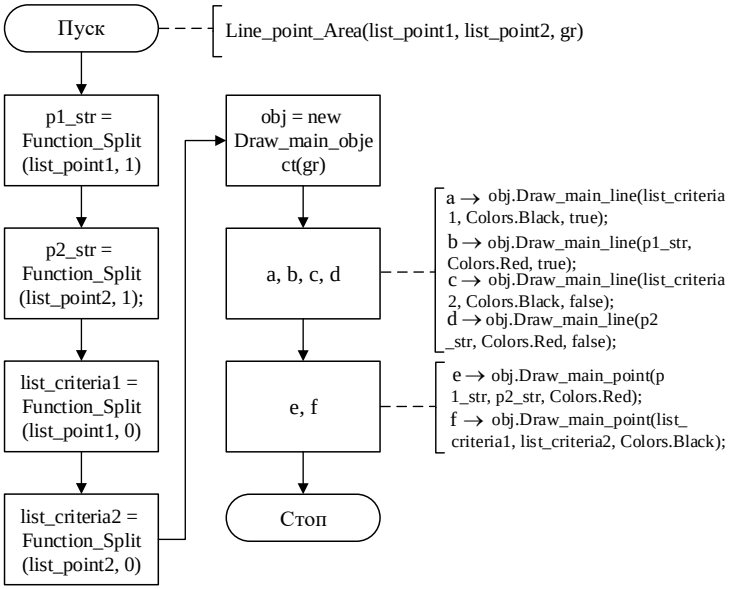

Рис. 5.15. Алгоритм реалізації процедури Line_point_Area

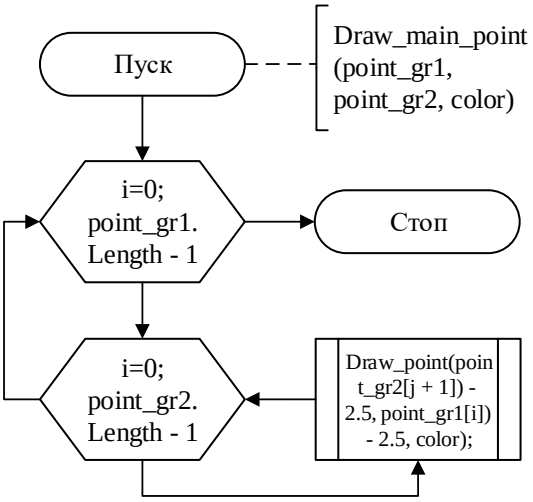

Рис. 5.16. Алгоритм реалізації процедури Draw_main_point

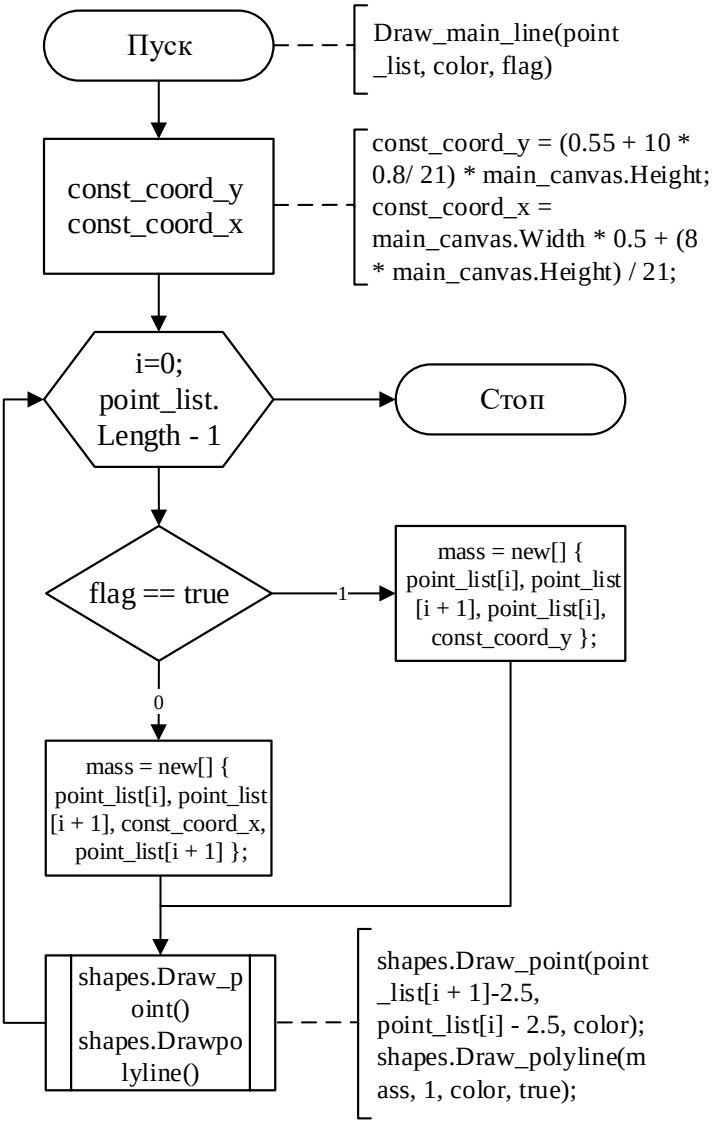

Рис. 5.17. Алгоритм реалізації процедури Draw_main_line

Приклад реалізації роботи цих двох процедур наведений на рис. 5.18.

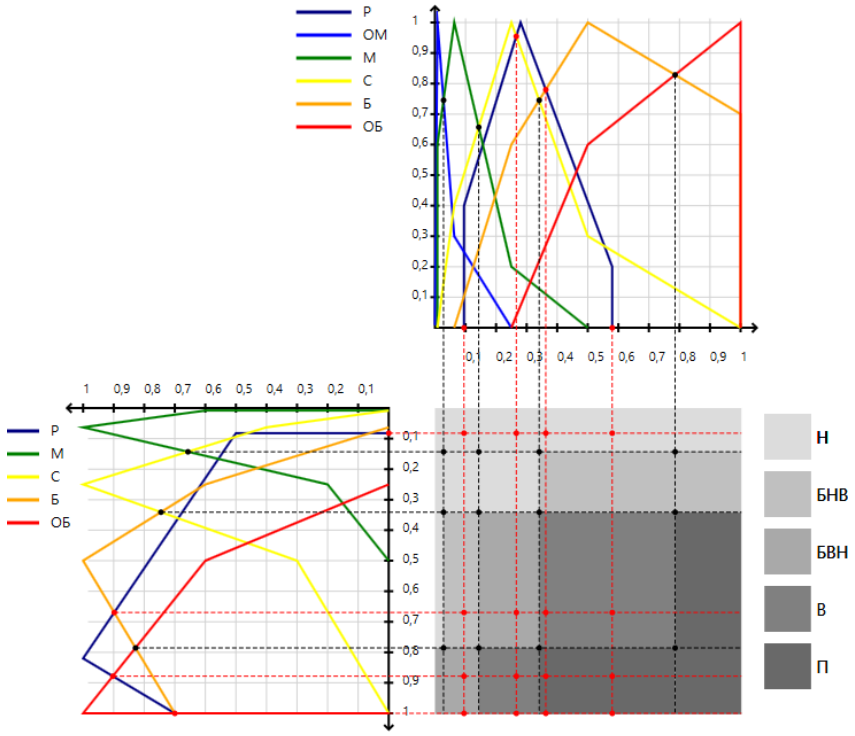

Рис. 5.18. Приклад побудови опорних областей відповідно до Draw_main_rect

Також, при побудові графічних елементів в алгоритмі System_level_Click (рис. 5.3) використовуються додаткові складові, наприклад, клас Main_figures включає в себе процедури: Draw_polyline (рис. 5.19); Draw_point; Draw_Rect (рис. 5.20),
які відповідно формують лінійні компоненти з різними вхідними характеристиками точок на графічному об’єкті Canvas і прямокутні компоненти.

Після отримання всіх даних System_level_Click здійснює побудову області поточного стану (відповідно до функціоналу МВ – див. структуру СВК в п. 5.1), що дозволяє візуально оцінити аномальний стан в системі для прийняття необхідного рішення.

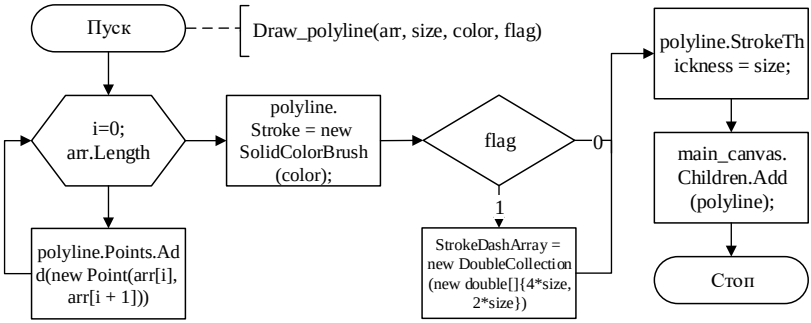

Рис. 5.19. Алгоритм реалізації процедури Draw_polyline

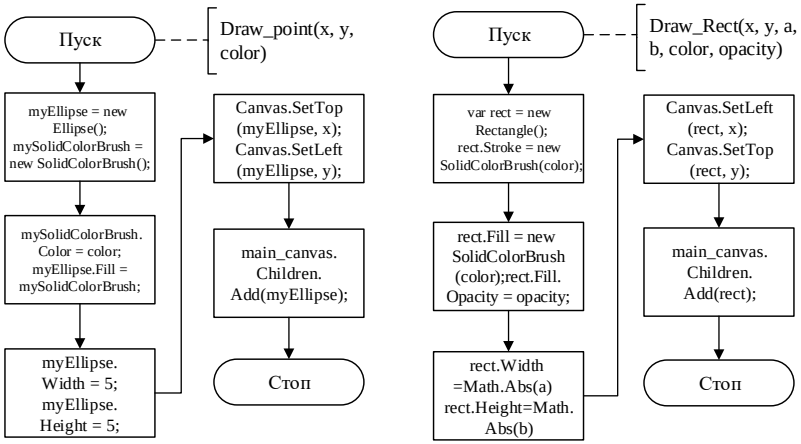

Рис. 5.20. Алгоритми реалізації процедур Draw_point і Draw_Rect

Фактично, процедура генерує поточний блок, наприклад, у вигляді червоної прямокутної області, утвореної за допомогою $\underset{\sim}{P}_{31}^{\tau_f}$ і $\underset{\sim}{P}_{32}^{\tau_f}$, що інтерпретує аномалію в *2*-вимірному параметричному КОП-КПОА-підсередовищі ($\mathbf{P_i = P_3 = P_{SP}}$), породжену відповідним атакуючим SP-середовищем ($\mathbf{CA}^{\tau_f}$) в момент часу τ_f (див. п. 4.2).

Приклад роботи ПЗ формування еталонів параметрів з різними експериментальними даними наведений на рис. 5.21 і рис. 5.22.

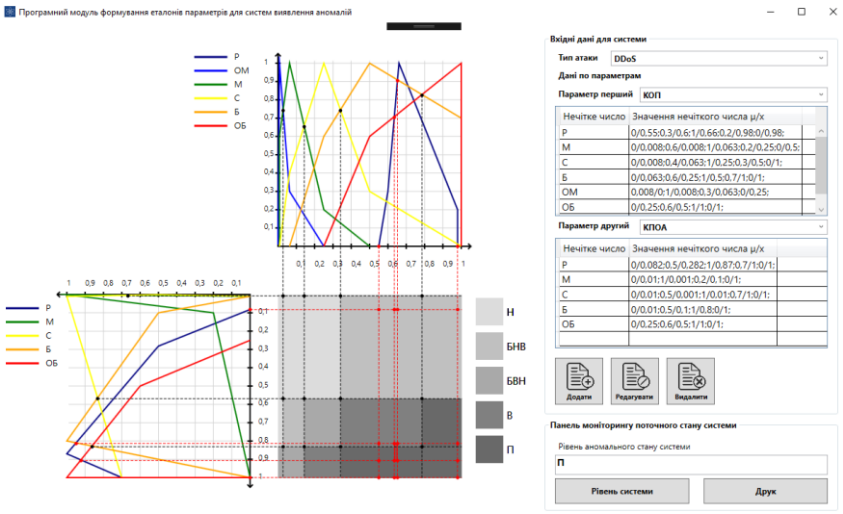

Рис. 5.21. Приклад роботи ПЗ формування еталонів параметрів (визначення першого поточного стану системи)

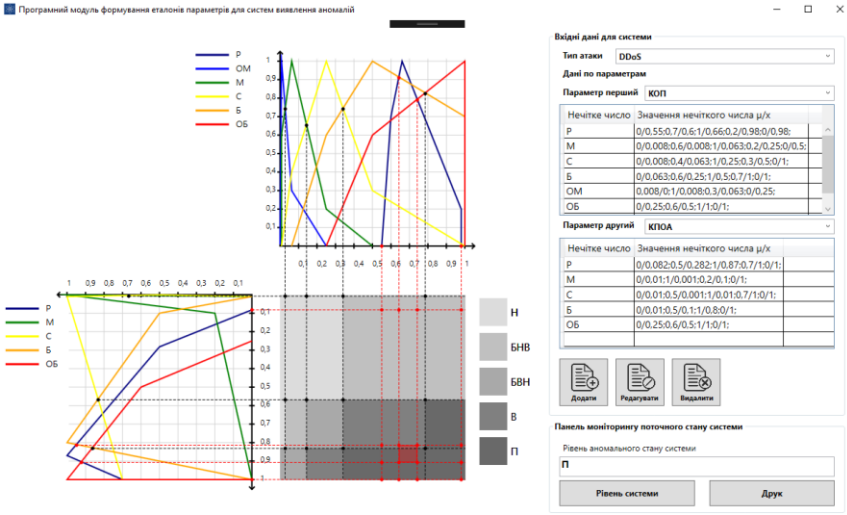

Рис. 5.22. Приклад роботи ПЗ формування еталонів параметрів (визначення другого поточного стану системи)

На заключному етапі (рис. 5.3, вершина 19) використовуються класи PrintPreviewWindow та Print, що відповідають за створення файлу звіту та його попереднього перегляду.

Тобто, користувач за необхідністю у момент часу τ_f може ініціалізувати режим друку, що приведе до створення у буферній пам'яті файлу попереднього перегляду (рис. 5.23), який можна роздрукувати (рис. 5.24) або зберегти у форматі pdf (рис. 5.25).

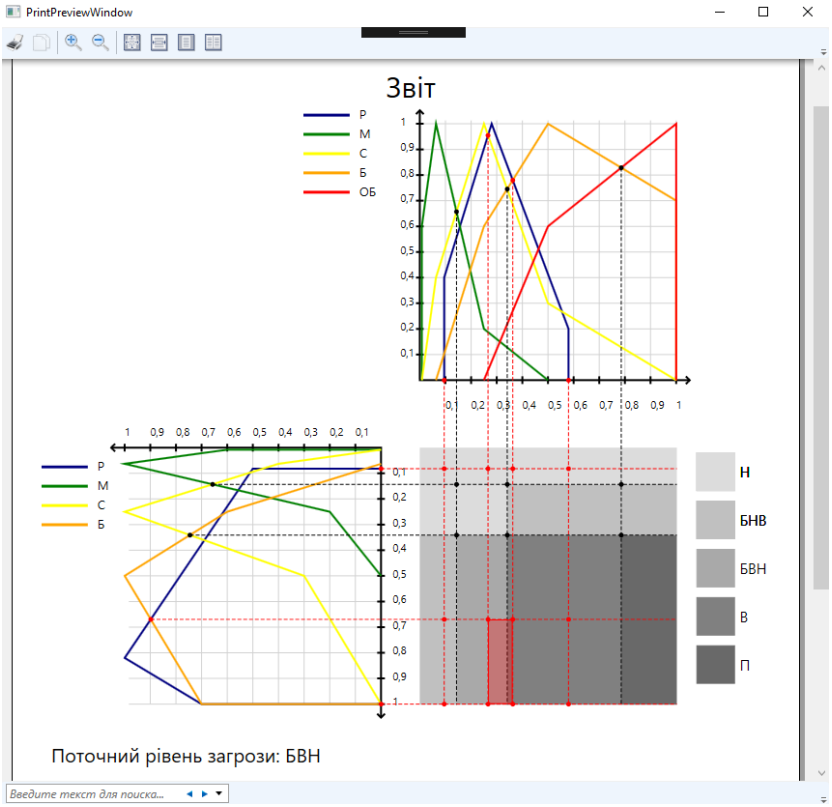

Рис. 5.23. Режим попереднього перегляду звіту

Друк ініціюється кнопкою «Рівень системи», у результаті чого графічний об'єкт Canvas конвертується в Xaml файл, а решта тексту,

заголовок звіту і правило, що спрацювало (відповідно до функціоналу МВ – див. структуру СВК в п. 5.1), генеруються за допомогою стандартного класу FixedDocument, який дозволяє зручно розміщати текст в звіті.

Файл звіту передається у буферну пам'ять, після чого його можна переглядати, змінювати налаштування друку тощо.

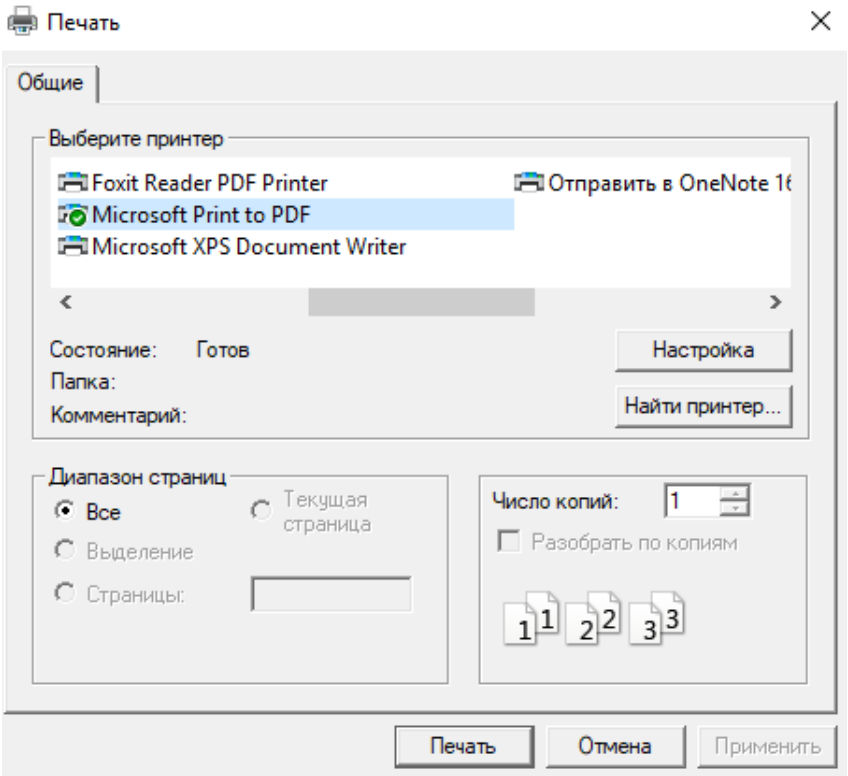

Рис. 5.24. Вікно вибору варіанту друку документа

У звіті формується відображення рівня аномального стану системи (у тому числі в момент часу τ_f).

Також, у розробленому ПЗ використовується модуль Child Window, який відповідає за створення та редагування $\mathcal{T}_{ijs}^{e}$ і $\mathcal{P}_{ij}^{\tau_f}$

(див. п. 2.2). Він представлений окремим вікном програми із базовим інтерфейсом для виконання сформованих вище задач. Дані в БДЕ за допомогою функціоналу цього модуля можна модифікувати та переглядати.

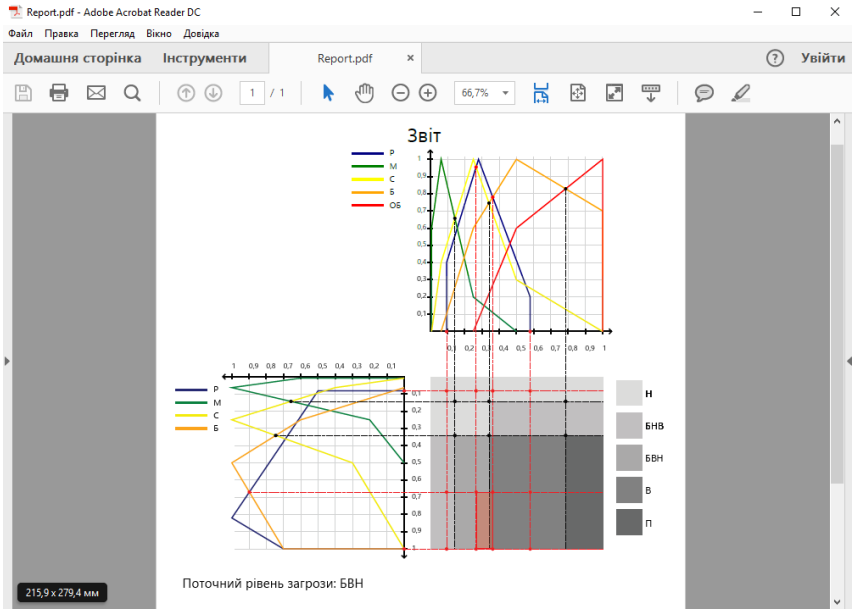

Рис. 5.25. Приклад друку звіту у форматі pdf

Аналогічна процедура реалізується при активізації кнопок:

- додати;
- редагувати;
- видалити.

Додавання запису (рис. 5.26).

За допомогою функціоналу вікна «Додати графік» є можливість доповнити такі дані як:

- назва графічного зображення еталонного та поточного НЧ (обирається за допомогою ComboBox і списку назв),
- кількість та ініціалізація значень їх координат (за допомогою «+» реалізується додавання/вилучення нової пари координат).

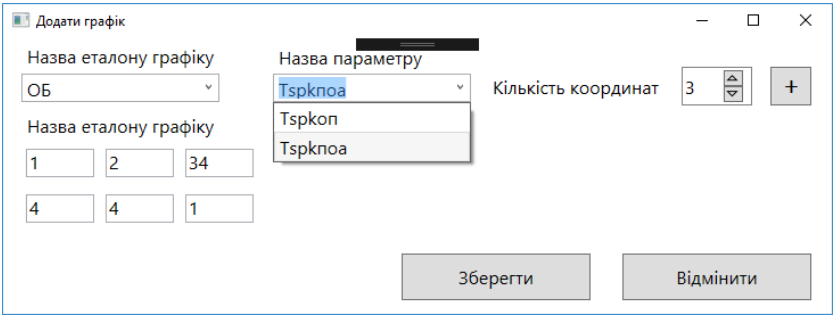

Рис. 5.26. Вікно додавання запису еталонних значень

Редагування існуючого запису (рис. 5.27).

Процес редагування подібний процесу додавання, оскільки базис роботи цих процедур схожий. Тому, після використання в головному вікні кнопки «Редагувати» з'являється відповідне вікно, де за допомогою функціоналу «Редагування даних графіка» є можливість його модифікації.

Вилучення даних (рис. 5.28).

При обранні необхідного рядка запису для вилучення використовується функціональна клавіша «Видалити», в результаті чого відбувається вилучення даних з БДЕ і її автоматичне оновлення.

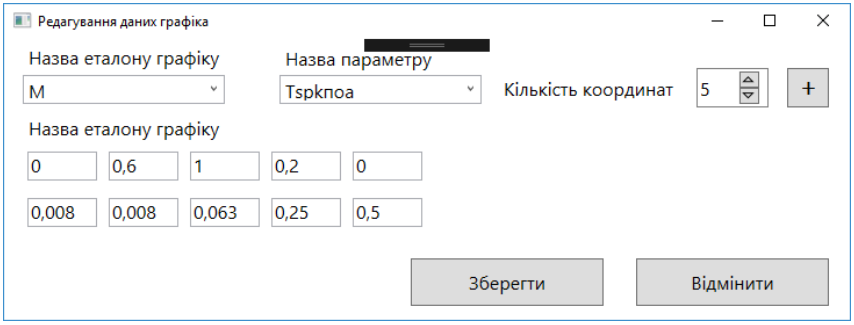

Рис. 5.27. Вікно редагування запису

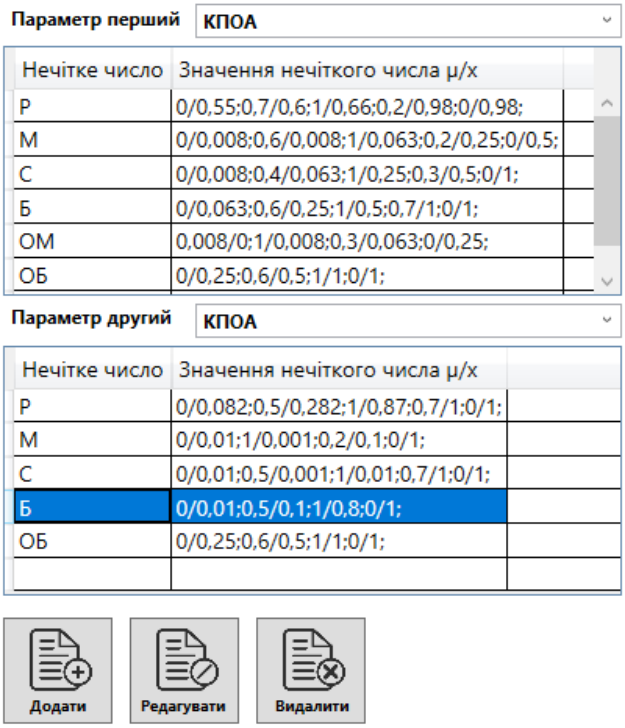

Рис. 5.28. Маркування рядка необхідного запису та його вилучення

Експериментальне дослідження та практичне використання запропонованого ПЗ підтвердило сформовані теоретичні положення, які стали основою розробленого алгоритмічного забезпечення.

Таким чином, запропоноване ПЗ [33, 34], яке за рахунок базового алгоритму та низки розроблених процедур (конструювання координатної сітки; ініціалізації величин на основі набору баз даних та модулів; графічного формування параметрів; пошуку спільних точок відповідно базових правил та графічної інтерпретації результату) дозволяє автоматизувати процес формування еталонів параметрів для сучасних систем виявлення атак та відображати результати детектування аномального стану у заданий проміжок часу. Також відповідне ПЗ може використовуватись автономно або, як розширювач функціональних можливостей сучасних СВВ.

5.3. Верифікація програмного модуля системи виявлення кібератак

Відповідно до запропонованого структурного рішення СВК (див. п. 5.1 та [31, 32]), яке базується на МПСВ (див. п. 4.3 і [1, 2]) та з урахуванням [33-35], здійснимо верифікацію програмної моделі СВК (див. п. 5.2 і [33, 34]) з метою підтвердження достовірності теоретичних положень наукових досліджень, проведених у роботі. Для цього розробимо структуру віртуальної мережі (рис. 5.29), за допомогою якої проведемо моделювання різних типів загроз РІС.

Така мережа складається з файл-сервера (ФС) (192.245.23.1), СВК і шести клієнтів (К) – К1 (192.245.23.2), К2 (192.245.23.3), К3 (192.245.23.4), К4 (192.245.23.5), К5 (192.245.23.6) та К6 (192.245.23.7).

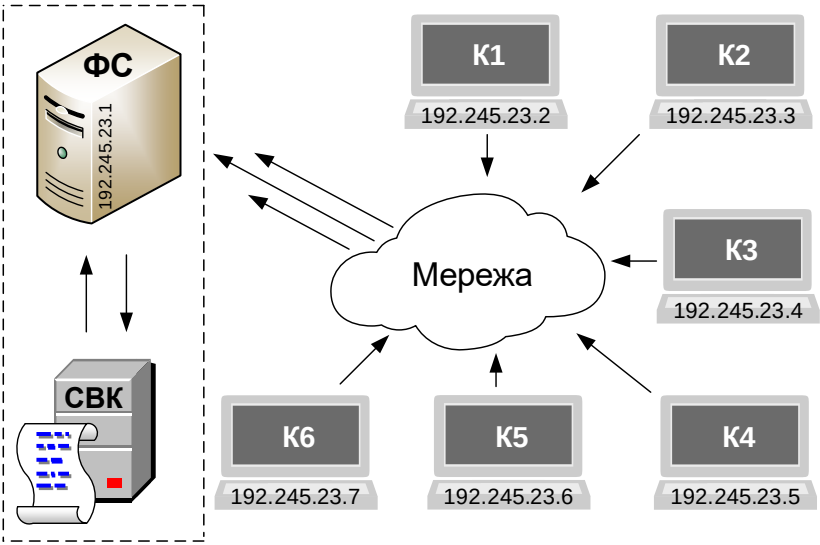

Рис. 5.29. Структура віртуальної мережі для моделювання атак

Для реалізації атак за допомогою віртуальної мережі розроблено клієнт серверний застосунок, що емулює роботу системи в режимі реального часу. Так, у вікні на рис. 5.30 відображено приклад приймання запитів від клієнтів і перевірка значення параметру КПОА, а

в момент підключення (відключення) нового клієнта здійснюється процес отримання значення параметру КОП (інтервал між запитами складає 50 мс.).

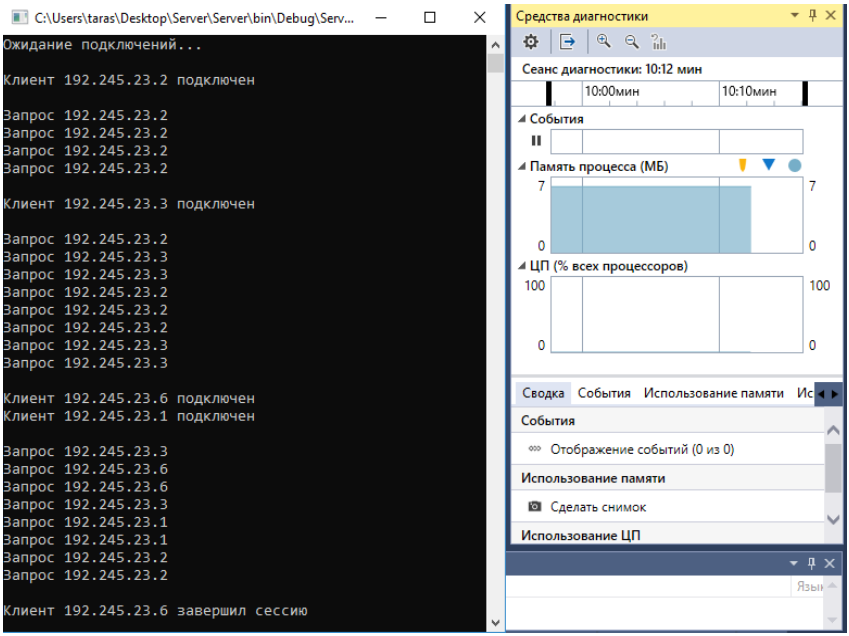

Рис. 5.30. Відображення процесів, пов'язаних із функціонуванням ФС у віртуальній мережі

Для прикладу, сформуємо значення величин $\underset{\sim}{P}^{\tau_f}_{SPKOП}$ та $\underset{\sim}{P}^{\tau_f}_{SPKПОА}$ поточного підсередовища ($\mathbf{P}_i^{\tau_f} = \mathbf{P}_3^{\tau_f}$) атакуючого середовища ($\mathbf{CA}^{\tau_f}$), які несуть мінімальну загрозу для ФС:

$$\underset{\sim}{P}^{\tau_f}_{SPKOП} = \{0/0{,}030;\ 0{,}4/0{,}030;\ 1/0{,}05;\ 0{,}2/0{,}07;\ 0/0{,}07\};$$

$$\underset{\sim}{P}^{\tau_f}_{SPKПОА} = \{0/0{,}030;\ 0{,}5/0{,}030;\ 1/0{,}05;\ 0{,}7/0{,}150;\ 0/0{,}150\}.$$

Далі, відповідно до номіналізованих НЧ еталонного підсередовища ($\mathbf{T}_i^e = \mathbf{T}_3^e = \mathbf{T}_{SP}^e$), визначених в п. 3.2, здійснимо формування номіналізованого НЧ поточного підсередовища ($\mathbf{P}_i^{\tau_f} = \mathbf{P}_3^{\tau_f}$) з урахуванням (3.12), тобто

$$\underset{\sim}{P}_{31}^{\tau_f p} = \{ \bigcup_{g=1}^{13} \mu_{31g}^{p} / x_{31g}^{p} \} =$$

$$\{ \mu_{311}^{p} / x_{311}^{p},\ \mu_{312}^{p} / x_{312}^{p},\ \mu_{313}^{p} / x_{313}^{p},\ \mu_{314}^{p} / x_{314}^{p},\ \mu_{315}^{p} / x_{315}^{p},$$
$$\mu_{316}^{p} / x_{316}^{p},\ \mu_{317}^{p} / x_{317}^{p},\ \mu_{318}^{p} / x_{318}^{p},\ \mu_{319}^{p} / x_{319}^{p},\ \mu_{31(10)}^{p} / x_{31(10)}^{p},$$
$$\mu_{31(11)}^{p} / x_{31(11)}^{p},\ \mu_{31(12)}^{p} / x_{31(12)}^{p},\ \mu_{31(13)}^{p} / x_{31(13)}^{p} \},$$

де:

- $\mu_{311}^{p} = \mu_{31(13)}^{p} = AL_{311} = 0,$
- $\mu_{312}^{p} = \mu_{31(12)}^{p} = AL_{312} = 0,2,$
- $\mu_{313}^{p} = \mu_{31(11)}^{p} = AL_{313} = 0,3,$
- $\mu_{314}^{p} = \mu_{31(10)}^{p} = AL_{314} = 0,4,$
- $\mu_{315}^{p} = \mu_{319}^{p} = AL_{315} = 0,6,$
- $\mu_{316}^{p} = \mu_{318}^{p} = AL_{316} = 0,7,$
- $\mu_{317}^{p} = \mu_{317}^{p} = AL_{317} = 1,$
- $\mu_{311}^{p} = \mu_{311} = 0,$
- $x_{311}^{p} = x_{311} = 0,030$ та

$$\underset{\sim}{P}_{32}^{\tau_f p} = \{ \bigcup_{g=1}^{9} \mu_{32g}^{p} / x_{32g}^{p} \} =$$

$$\{ \mu_{321}^{p} / x_{321}^{p},\ \mu_{322}^{p} / x_{322}^{p},\ \mu_{323}^{p} / x_{323}^{p},\ \mu_{324}^{p} / x_{324}^{p},$$
$$\mu_{325}^{p} / x_{325}^{p},\ \mu_{326}^{p} / x_{326}^{p},\ \mu_{327}^{p} / x_{327}^{p},\ \mu_{328}^{p} / x_{328}^{p},\ \mu_{329}^{p} / x_{329}^{p} \},$$

де:

- $\mu_{321}^{p} = \mu_{329}^{p} = AL_{321} = 0,$
- $\mu_{322}^{p} = \mu_{328}^{p} = AL_{322} = 0,2,$
- $\mu_{323}^{p} = \mu_{327}^{p} = AL_{323} = 0,5,$
- $\mu_{324}^{p} = \mu_{326}^{p} = AL_{324} = 0,7,$
- $\mu_{325}^{p} = \mu_{325}^{p} = AL_{325} = 1,$
- $\mu_{321}^{p} = \mu_{321} = 0,$
- $x_{321}^{p} = x_{321} = 0,030.$

Далі, формування номіналізованого НЧ $\underset{\sim}{P}_{ij}^{\tau_f p} = \underset{\sim}{P}_{31}^{\tau_f p}$ поточного підсередовища ($\mathbf{P_i^{\tau_f} = P_3^{\tau_f}}$) здійснюється відповідно до (3.18) за допомогою α-рівневих інтервалів $\mathbf{AL_{31}^{Ip}}$ (див. п. 3.2) при $\rho = 5$, а

$$\mu_{31max} = \bigvee_{q=1}^{\rho} \mu_{31q} = \mu_{311} \vee \mu_{312} \vee \mu_{313} \vee \mu_{314} \vee \mu_{315} =$$

$$0 \vee 0{,}4 \vee 1 \vee 0{,}2 \vee 0 = \mu_{313} = 1$$

та якщо:

- $r_1 = 1,\ c = \overline{1,k_1},\ k_1 = 3$ і $(\mu_{311} < AL_{311c}^{Ip} \le \mu_{312}) \wedge (x_{312} \le x_{31max})$ $((0 < AL_{311c}^{Ip} \le 0{,}4) \wedge (0{,}030 \le 0{,}05))$, то

$$\mathbf{AL_{311}^{Ip}} = \{\bigcup_{c=1}^{k_1} AL_{311c}^{Ip}\} = \{AL_{3111}^{Ip},\ AL_{3112}^{Ip},\ AL_{3113}^{Ip}\} = \{0{,}2;\ 0{,}3;\ 0{,}4\};$$

- $r_2 = 2,\ c = \overline{1,k_2},\ k_2 = 3,\ (\mu_{312} < AL_{312c}^{Ip} \le \mu_{313}) \wedge (x_{313} \le x_{31max})$ $((0{,}4 < AL_{312c}^{Ip} \le 1) \wedge (0{,}05 \le 0{,}05))$, то

$$\mathbf{AL_{312}^{Ip}} = \{\bigcup_{c=1}^{k_2} AL_{312c}^{Ip}\} = \{AL_{3121}^{Ip},\ AL_{3122}^{Ip},\ AL_{3123}^{Ip}\} = \{0{,}6;\ 0{,}7;\ 1\};$$

- $r_3 = 3,\ c = \overline{1,k_3},\ k_3 = 5,\ (\mu_{313} > AL_{313c}^{Ip} \ge \mu_{314}) \wedge (x_{314} \ge x_{31max})$ $((1 > AL_{313c}^{Ip} \ge 0{,}2) \wedge (0{,}07 \ge 0{,}05))$, то

$$\mathbf{AL_{313}^{Ip}} = \{\bigcup_{c=1}^{k_3} AL_{313c}^{Ip}\} = \{AL_{3131}^{Ip},\ AL_{3132}^{Ip},\ AL_{3133}^{Ip},\ AL_{3134}^{Ip},\ AL_{3135}^{Ip}\} =$$

$$\{0{,}7;\ 0{,}6;\ 0{,}4;\ 0{,}3;\ 0{,}2\};$$

- $r_4 = 4,\ c = \overline{1,k_4},\ k_4 = 1,\ (\mu_{314} > AL_{314c}^{Ip} \ge \mu_{315}) \wedge (x_{315} \ge x_{31max})$ $((0{,}2 > AL_{314c}^{Ip} \ge 1) \wedge (0{,}07 \ge 0{,}05))$, то

$$\mathbf{AL_{314}^{Ip}} = \{\bigcup_{c=1}^{k_4} AL_{314c}^{Ip}\} = \{AL_{3141}^{Ip}\} = \{0\}.$$

З урахуванням обчислених значень, отримаємо наступний вигляд

$$\mathbf{AL_{31}^{Ip}} = \{\bigcup_{b=1}^{\rho-1}\{\bigcup_{c=1}^{k_b} AL_{31bc}^{Ip}\}\} =$$

$$\{\{AL_{3111}^{Ip},\ AL_{3112}^{Ip},\ AL_{3113}^{Ip}\},\ \{AL_{3121}^{Ip},\ AL_{3122}^{Ip},\ AL_{3123}^{Ip}\},$$

$$\{ AL^{Ip}_{3131},\ AL^{Ip}_{3132},\ AL^{Ip}_{3133},\ AL^{Ip}_{3134},\ AL^{Ip}_{3135} \},\ \{ AL^{Ip}_{3141} \}\} =$$
$$\{\{ 0{,}2;\ 0{,}3;\ 0{,}4 \},\ \{ 0{,}6;\ 0{,}7;\ 1 \},\ \{ 0{,}7;\ 0{,}6;\ 0{,}4;\ 0{,}3;\ 0{,}2 \},\ \{ 0 \}\}.$$

За аналогією з прикладом, для $\underset{\sim}{P}^{\tau_f p}_{31}$ формування номіналізованого НЧ $\underset{\sim}{P}^{\tau_f p}_{ij} = \underset{\sim}{P}^{\tau_f p}_{32}$ поточного підсередовища ($\mathbf{P}^{\boldsymbol{\tau_f}}_{\mathbf{i}} = \mathbf{P}^{\boldsymbol{\tau_f}}_{\mathbf{3}}$) реалізується на основі (3.19) за допомогою α-рівневих інтервалів $\mathbf{AL}^{\mathbf{Ip}}_{\mathbf{32}}$ (див. п. 3.2), тобто

$$\mathbf{AL}^{\mathbf{Ip}}_{\mathbf{32}} = \{ \bigcup_{b=1}^{\rho-1} \{ \bigcup_{c=1}^{k_b} AL^{Ip}_{32bc} \}\} =$$
$$\{\{ AL^{Ip}_{3211},\ AL^{Ip}_{3212} \},\ \{ AL^{Ip}_{3221},\ AL^{Ip}_{3222} \},\ \{ AL^{Ip}_{3231} \},$$
$$\{ AL^{Ip}_{3241},\ AL^{Ip}_{3242},\ AL^{Ip}_{3243},\ AL^{Ip}_{3244} \}\} =$$
$$\{\{ 0{,}2;\ 0{,}5 \},\ \{ 0{,}7;\ 1 \},\ \{ 0{,}7 \},\ \{ 0{,}5;\ 0{,}2;\ 1 \}\}.$$

Обчислення значень x^{p}_{31g} для перетворених НЧ $\underset{\sim}{P}^{\tau_f p}_{31} = \underset{\sim}{P}^{\tau_f p}_{SPKOП}$ поточного підсередовища ($\mathbf{P}^{\boldsymbol{\tau_f}}_{\mathbf{i}} = \mathbf{P}^{\boldsymbol{\tau_f}}_{\mathbf{3}}$) здійснюється аналогічно до кроку 4 (див. п. 3.2) з урахуванням (3.22) при $z = 13,\ g = \overline{2,13}$ на основі компонентів μ_{ijg} / x_{ijg} (див. приклад етапу 3 в п. 3.1), тобто $\mu_{311} = 0,\ \mu_{312} = 0{,}4,\ x_{311} = 0{,}03$ та $x_{312} = 0{,}03$.

Далі, з урахуванням цього:

- якщо $\mu^{p}_{312} = AL^{Ip}_{312} = 0{,}2$, то
  $x^{p}_{312} = 0{,}03 + ((0{,}2 - 0) \cdot (0{,}03 - 0{,}03)) / (0{,}4 - 0) = 0{,}03$;
- якщо $\mu^{p}_{313} = AL^{Ip}_{313} = 0{,}3$, то
  $x^{p}_{313} = 0{,}03 + ((0{,}3 - 0) \cdot (0{,}03 - 0{,}03)) / (0{,}4 - 0) = 0{,}03$;
- якщо $\mu^{p}_{314} = AL^{Ip}_{314} = 0{,}4$, то
  $x^{p}_{314} = 0{,}03 + ((0{,}4 - 0) \cdot (0{,}03 - 0{,}03)) / (0{,}4 - 0) = 0{,}03$.

Наступним, при $\mu_{312} = 0{,}4,\ \mu_{313} = 1,\ x_{312} = 0{,}03$ та $x_{313} = 0{,}05$:

- якщо $\mu^{p}_{315} = AL^{Ip}_{315} = 0{,}6$, то
  $x^{p}_{315} = 0{,}03 + ((0{,}6 - 0{,}4) \cdot (0{,}05 - 0{,}03)) / (1 - 0{,}4) = 0{,}037$;
- якщо $\mu^{p}_{316} = AL^{Ip}_{316} = 0{,}7$, то

$x^{p}_{316}=0,03+((0,7-0,4)\cdot(0,05-0,03))/(1-0,4)=0,04$;

- якщо $\mu^{p}_{317}=AL^{Ip}_{317}=1$, то

$x^{p}_{317}=0,03+((1-0,4)\cdot(0,05-0,03))/(1-0,4)=0,05$.

Далі, при $\mu_{313}=1$, $\mu_{314}=0,2$, $x_{313}=0,05$ та $x_{314}=0,07$ обчислимо:

- якщо $\mu^{p}_{318}=AL^{Ip}_{318}=0,7$, то

$x^{p}_{318}=0,03+((0,7-1)\cdot(0,07-0,05))/(0,2-1)=0,038$;

- якщо $\mu^{p}_{319}=AL^{Ip}_{319}=0,6$, то

$x^{p}_{319}=0,03+((0,6-1)\cdot(0,07-0,05))/(0,2-1)=0,04$;

- якщо $\mu^{p}_{31(10)}=AL^{Ip}_{31(10)}=0,4$, то

$x^{p}_{31(10)}=0,03+((0,4-1)\cdot(0,07-0,05))/(0,2-1)=0,045$;

- якщо $\mu^{p}_{31(11)}=AL^{Ip}_{31(11)}=0,3$, то

$x^{p}_{31(11)}=0,03+((0,3-1)\cdot(0,07-0,05))/(0,2-1)=0,048$;

- якщо $\mu^{p}_{31(12)}=AL^{Ip}_{31(12)}=0,2$, то

$x^{p}_{31(12)}=0,03+((0,2-1)\cdot(0,07-0,05))/(0,2-1)=0,05$.

Наступним, при $\mu_{314}=0,2$, $\mu_{315}=0$, $x_{314}=0,07$ та $x_{315}=0,07$ для $\mu^{ep}_{31(13)}=AL^{Ip}_{31(13)}=0$ визначимо

$x^{ep}_{31(13)}=0,07+((0-0,2)\cdot(0,07-0,07))/(0-0,2)=0,07$,

а $\mu^{p}_{311}=\mu_{311}=0$, $x^{p}_{311}=x_{311}=0,03$.

Таким чином, номіналізоване НЧ поточного підсередовища ($\mathbf{P}^{\tau_f}_{i}=\mathbf{P}^{\tau_f}_{3}$) відповідно до (3.12) прийме наступний вигляд:

$\underset{\sim}{P}^{\tau_f p}_{31}=\underset{\sim}{P}^{\tau_f p}_{SPKOП}=\{0/0,03;\ 0,2/0,03;\ 0,3/0,03;\ 0,4/0,03;\ 0,6/0,037;\ 0,7/0,04;$
$1/0,05;\ 0,7/0,038;\ 0,6/0,04;\ 0,4/0,045;\ 0,3/0,048;\ 0,2/0,05;\ 0/0,07\}$.

Обчислення значень x^{p}_{36g} для перетворених НЧ $\underset{\sim}{P}^{\tau_f p}_{32}=\underset{\sim}{P}^{\tau_f p}_{SPKПОА}$ поточного підсередовища ($\mathbf{P}^{\tau_f}_{i}=\mathbf{P}^{\tau_f}_{3}=\mathbf{P}^{\tau_f}_{SP}$) здійснюється аналогічно, з урахуванням (3.22) при $z=9$, за допомогою компонентів μ_{ijg}/x_{ijg} (див. приклад етапу 3 в п. 3.1), тобто при $\mu_{321}=0$, $\mu_{322}=0,5$, $x_{321}=0,03$ та $x_{322}=0,03$.

Далі, з урахуванням цих значень:

- якщо $\mu^{p}_{322} = AL^{Ip}_{322} = 0{,}2$, то $x^{p}_{322} = 0{,}03$;
- якщо $\mu^{p}_{323} = AL^{Ip}_{323} = 0{,}5$, то $x^{p}_{323} = 0{,}03$.

При $\mu_{322} = 0{,}5$, $\mu_{323} = 1$, $x_{322} = 0{,}03$ та $x_{323} = 0{,}05$:

- якщо $\mu^{p}_{324} = AL^{Ip}_{324} = 0{,}7$, то $x^{p}_{324} = 0{,}038$;
- якщо $\mu^{p}_{325} = AL^{Ip}_{325} = 1$, то $x^{p}_{325} = 0{,}05$.

Далі, при $\mu_{323} = 1$, $\mu_{324} = 0{,}7$, $x_{323} = 0{,}05$ та $x_{324} = 0{,}15$ для $\mu^{p}_{326} = AL^{Ip}_{326} = 0{,}7$ обчислимо $x^{p}_{326} = 0{,}15$.

І, нарешті, при $\mu_{324} = 0{,}7$, $\mu_{325} = 0$, $x_{324} = 0{,}15$ та $x_{325} = 0{,}15$ для $\mu^{p}_{327} = AL^{Ip}_{327} = 0{,}5$, $\mu^{p}_{328} = AL^{Ip}_{328} = 0{,}2$, $\mu^{p}_{329} = AL^{Ip}_{329} = 0$ відповідно обчислимо $x^{p}_{327} = x^{p}_{328} = x^{p}_{329} = 0{,}15$, а $\mu^{p}_{321} = \mu_{321} = 0$, $x^{p}_{321} = x_{321} = 0{,}03$.

Таким чином, номіналізоване НЧ поточного підсередовища ($\mathbf{P}^{\tau_f}_{\mathbf{i}} = \mathbf{P}^{\tau_f}_{\mathbf{3}} = \mathbf{P}^{\tau_f}_{\mathbf{SP}}$) відповідно до (3.12) має вигляд

$$\underset{\sim}{P}^{\tau_f p}_{32} = \underset{\sim}{P}^{\tau_f p}_{SPKПОА} = \{0/0{,}03;\ 0{,}2/0{,}03;\ 0{,}5/0{,}03;\ 0{,}7/0{,}378;$$
$$1/0{,}05;\ 0{,}7/0{,}15;\ 0{,}5/0{,}15;\ 0{,}2/0{,}15;\ 0/0{,}15\}.$$

Зведемо отримані дані до узагальнювальних табл. 5.1-5.2

Таблиця 5.1

Узагальнювальна таблиця для $\underset{\sim}{P}^{p}_{SPKOП}$

$\underset{\sim}{P}^{\tau_f p}_{31}$	$\mu^{p}_{31g}\ (g = \overline{1,13})$												
	μ^{p}_{311}	μ^{p}_{312}	μ^{p}_{313}	μ^{p}_{314}	μ^{p}_{315}	μ^{p}_{316}	μ^{p}_{317}	μ^{p}_{318}	μ^{p}_{319}	$\mu^{p}_{31(10)}$	$\mu^{p}_{31(11)}$	$\mu^{p}_{31(12)}$	$\mu^{p}_{31(13)}$
	0	0,2	0,3	0,4	0,6	0,7	1	0,7	0,6	0,4	0,3	0,2	0
$\underset{\sim}{P}^{\tau_f p}_{SPKOП}$	0,03	0,03	0,03	0,03	0,037	0,04	0,05	0,038	0,04	0,045	0,048	0,05	0,07

Таблиця 5.2

Узагальнювальна таблиця для $\underset{\sim}{P}^{p}_{SPKПОА}$

$\underset{\sim}{P}^{\tau_f p}_{32}$	$\mu^{p}_{32g}\ (g = \overline{1,9})$								
	μ^{p}_{321}	μ^{p}_{322}	μ^{p}_{323}	μ^{p}_{324}	μ^{p}_{325}	μ^{p}_{326}	μ^{p}_{327}	μ^{p}_{328}	μ^{p}_{329}
	0	0,2	0,5	0,7	1	0,7	0,5	0,2	0
$\underset{\sim}{P}^{\tau_f p}_{SPKПОА}$	0,03	0,03	0,03	0,038	0,05	0,15	0,15	0,15	0,15

Наступним, відповідно до п. 3.3, сформуємо ХО:

$$\mathbf{XP^1_{31}} = \{\bigcup_{s=1}^{5} XP^1_{31s}\} = \{ XP^1_{311},\ XP^1_{312},\ XP^1_{313},\ XP^1_{314},\ XP^1_{315}\} =$$

$$\{ h(\underset{\sim}{T}^{ep}_{311},\ \underset{\sim}{P}^{\tau_f p}_{31}),\ h(\underset{\sim}{T}^{ep}_{312},\ \underset{\sim}{P}^{\tau_f p}_{31}),\ h(\underset{\sim}{T}^{ep}_{313},\ \underset{\sim}{P}^{\tau_f p}_{31}),$$

$$h(\underset{\sim}{T}^{ep}_{314},\ \underset{\sim}{P}^{\tau_f p}_{31}),\ h(\underset{\sim}{T}^{ep}_{315},\ \underset{\sim}{P}^{\tau_f p}_{31})\} =$$

$$\{0{,}478;\ 1{,}327;\ 3{,}575;\ 7{,}058;\ 8{,}962\};$$

$$\mathbf{XP^1_{32}} = \{\bigcup_{s=1}^{3} XP^1_{32s}\} = \{ XP^1_{321},\ XP^1_{322},\ XP^1_{323}\} =$$

$$\{ h(\underset{\sim}{T}^{ep}_{321},\ \underset{\sim}{P}^{\tau_f p}_{32}),\ h(\underset{\sim}{T}^{ep}_{322},\ \underset{\sim}{P}^{\tau_f p}_{32}),\ h(\underset{\sim}{T}^{ep}_{323},\ \underset{\sim}{P}^{\tau_f p}_{32})\} =$$

$$\{1{,}228;\ 3{,}518;\ 4{,}878\}.$$

Далі, визначення $IX^1_{31NUM_{31}}$ та $IX^1_{32NUM_{32}}$ здійснюється за допомогою функції F^1 $\mathbf{(XP^1_{31})}$ і F^1 $\mathbf{(XP^1_{32})}$, яка реалізує пошук мінімального значення із членів підмножини $\mathbf{XP^1_{31}}$ та $\mathbf{XP^1_{32}}$ (див. (3.31)) відповідно до (3.32) і (3.33), тобто:

$$IX^1_{31NUM_{31}} = \bigwedge_{s=1}^{5} XP^1_{31s} = XP^1_{311} \wedge XP^1_{312} \wedge XP^1_{313} \wedge XP^1_{314} \wedge XP^1_{315} =$$

$$0{,}478 \wedge 1{,}327 \wedge 3{,}575 \wedge 7{,}058 \wedge 8{,}962 =$$

$$XP^1_{311} = 0{,}478;$$

$$IX^1_{32NUM_{32}} = \bigwedge_{s=1}^{3} XP^1_{32s} = XP^1_{321} \wedge XP^1_{322} \wedge XP^1_{323} =$$

$$1{,}228 \wedge 3{,}518 \wedge 4{,}878 =$$

$$XP^1_{321} = 1{,}228.$$

Виходячи з обчислень видно, що ідентифікуючим в $\mathbf{T^e_{31}}$ буде терм $\underset{\sim}{T}^e_{311} = \underset{\sim}{OM}^e_{31}$ (див. приклад для (2.35)), а відповідне йому перетворене еталонне є $\underset{\sim}{T}^{ep}_{311} = \underset{\sim}{T}^{ep}_{SPKOП\,1} = \underset{\sim}{OM}^{ep}_{31}$ (див. приклад етапу 2 для (3.10)). Фактично, обчислення показують, що $XP^1_{311} = 0{,}478$, отже перетворене НЧ $\underset{\sim}{P}^{\tau_f p}_{31} = \underset{\sim}{P}^{\tau_f p}_{SPKOП}$ поточного підсередовища ($\mathbf{P^{\tau_f}_i = P^{\tau_f}_3 = P^{\tau_f}_{SP}}$) найбільш близько розташоване до перетвореного НЧ $\underset{\sim}{T}^{ep}_{311} = \underset{\sim}{OM}^{ep}_{31}$ еталонного підсередовища ($\mathbf{T^e_i = T^e_3 = T^e_{SP}}$). А оскільки $\underset{\sim}{P}^{\tau_f p}_{SPKOП}$

та $\underset{\sim}{OM}^{ep}_{31}$ є відображенням $\underset{\sim}{P}^{\tau_f p}_{SPKOП}$ та $\underset{\sim}{OM}^{e}_{31}$, то НЧ $\underset{\sim}{P}^{\tau_f p}_{SPKOП}$ найближче розташоване до НЧ $\underset{\sim}{OM}^{e}_{31}$ еталонного підсередовища ($\mathbf{T^e_i = T^e_3 = T^e_{SP}}$).

Аналогічно, ідентифікуючим в $\mathbf{T^e_{32}}$ є значення $\underset{\sim}{T}^{e}_{321} = \underset{\sim}{M}^{e}_{32}$ (див. приклад для (2.35)) та, при цьому, $\underset{\sim}{T}^{ep}_{321} = \underset{\sim}{T}^{ep}_{SPKПОА\,1} = \underset{\sim}{M}^{ep}_{32}$ (див. приклад етапу 2 для (3.10)). Також, враховуючи, що $XP^1_{321} = 1{,}228$, то перетворене НЧ $\underset{\sim}{P}^{\tau_f p}_{32} = \underset{\sim}{P}^{\tau_f p}_{SPKПОА}$ поточного підсередовища ($\mathbf{P^{\tau_f}_i = P^{\tau_f}_3 = P^{\tau_f}_{SP}}$) найближче до перетвореного НЧ $\underset{\sim}{T}^{ep}_{321} = \underset{\sim}{M}^{ep}_{32}$ еталонного підсередовища ($\mathbf{T^e_i = T^e_3 = T^e_{SP}}$). І, отже, якщо $\underset{\sim}{P}^{\tau_f p}_{SPKПОА}$ та $\underset{\sim}{M}^{ep}_{32}$ є відображенням $\underset{\sim}{P}^{\tau_f p}_{SPKПОА}$ та $\underset{\sim}{M}^{e}_{32}$, то $\underset{\sim}{P}^{\tau_f p}_{SPKПОА}$ є найближчим до $\underset{\sim}{M}^{e}_{32}$.

Відповідно до (4.3) наступним за ідентифікуючим для $\mathbf{T^e_{31}}$ буде слідувати терм з $XP^1_{312} = 1{,}327$, тобто це $\underset{\sim}{T}^{e}_{312}$, який і є допоміжним, а для $\mathbf{T^e_{32}}$ – буде терм з $XP^1_{322} = 3{,}518$, тобто $\underset{\sim}{T}^{e}_{322}$.

Далі, з урахуванням (4.6) та допоміжних термів XP^1_{312} і XP^1_{322} розрахуємо нормуючі коефіцієнти

$$k_{31} = 1/(XP^1_{311} + XP^1_{312}) = 1/(0{,}478 + 1{,}327) = 0{,}554,$$

а також

$$k_{32} = 1/(XP^1_{321} + XP^1_{322}) = 1/(1{,}228 + 3{,}518) = 0{,}211.$$

На основі (4.7) обчислимо експертні коефіцієнти параметрів ($P_{31} = P_{SPKOП} = KOП$ та $P_{32} = P_{SPKПОА} = KПОА$)

$$EC^{min}_{31} = 1 - k_{31} \cdot XP^1_{312},$$

$$EC^{max}_{31} = 1 - k_{31} \cdot XP^1_{311},$$

$$EC^{min}_{31} = 1 - 0{,}554 \cdot 1{,}327 = 0{,}265,$$

$$EC^{max}_{31} = 1 - 0{,}554 \cdot 0{,}478 = 0{,}735$$ та

$$EC^{min}_{32} = 1 - k_{32} \cdot XP^1_{322},$$

$$EC^{max}_{32} = 1 - k_{32} \cdot XP^1_{321},$$

$$EC^{min}_{32} = 1 - 0{,}211 \cdot 3{,}518 = 0{,}258,$$

$$EC_{32}^{max} = 1 - 0{,}211 \cdot 1{,}228 = 0{,}741.$$

Зазначимо, що $EC_{31}^{max} = 0{,}735$ та $EC_{32}^{max} = 0{,}741$ будуть відображати рівень упевненості експерта щодо значень сформованих поточних величин $\underset{\sim}{P}_{31}^{\tau_f p}$ і $\underset{\sim}{P}_{32}^{\tau_f p}$ відносно їх еталонних термів, що, відповідно, входять до $\mathbf{T}_{31}^{e}$ і $\mathbf{T}_{32}^{e}$.

З урахуванням (4.9) розрахуємо експертний коефіцієнт кібератаки ($\mathbf{CA}_{3}^{\tau_f} = \mathbf{CA}_{SP}^{\tau_f} = \mathbf{SP}^{\tau_f}$):

$$EC_{3}^{CA} = (EC_{31}^{max} + EC_{32}^{max}) / 2 = (0{,}735 + 0{,}741) / 2 = 0{,}738.$$

З використанням (4.33) та отриманих експертних коефіцієнтів параметрів $(EC_{31}^{max},\ EC_{32}^{max})$ і кібератаки (EC_{3}^{CA}) визначимо умовний вираз з підмножини $\mathbf{DR}_{3\ 13}$ (див. приклад в п. 4.2) детекційного підсередовища ($\mathbf{DR}_{SP}$) для виявлення спуфінгу, який буквально можна інтерпретувати, як: «Якщо поточний параметр «Кількість одночасних підключень до сервера» в момент часу τ_f найближчий до значення еталону «Дуже мале» (з експертним коефіцієнтом $0{,}735$) і поточний параметр «Кількість пакетів з однаковою адресою відправника та одержувача» в момент часу τ_f найближчий до значення еталону «Мале» (з експертним коефіцієнтом $0{,}741$), то рівень аномального стану, породженого спуфінгом буде «Низьким» (з експертним коефіцієнтом кібератаки $0{,}738$)», а з урахуванням (4.33) можна застосувати еквівалентний запис:

$$if\ \ (E(NUM_{SPKOП},\ 1)\big|_{0{,}735} \wedge E(NUM_{SPKПОА},\ 1)\big|_{0{,}741})$$
$$then\ \ "H"\big|_{0{,}738}.$$

Як бачимо, для виявлення спуфінгу із підмножини $\mathbf{DR}_{3\ 13}$ був застосований умовний вираз з ІД аномальності «Н».

На рис. 5.31 графічно показаний поточний блок (у вигляді заштрихованої прямокутної області, яка утворена за допомогою $\underset{\sim}{P}_{31}^{\tau_f}$ і $\underset{\sim}{P}_{32}^{\tau_f}$) з ІД аномальності «Н», який інтерпретує аномалію у *2*-вимірному параметричному КОП-КПОА-підсередовищі ($\mathbf{P_i} = \mathbf{P_3} = \mathbf{P_{SP}}$),

породжену відповідним атакуючим SP-середовищем ($\mathbf{CA}^{\tau_f}$) в момент часу τ_f. Відповідно до наведеного прикладу видно, що при мінімальному рівні загроз програмна модель СВК ідентифікує аномальний стан, що може бути породжений спуфінгом, як «Низький». Це відповідає адекватній реакції СВК на мінімальний вплив загроз РІС.

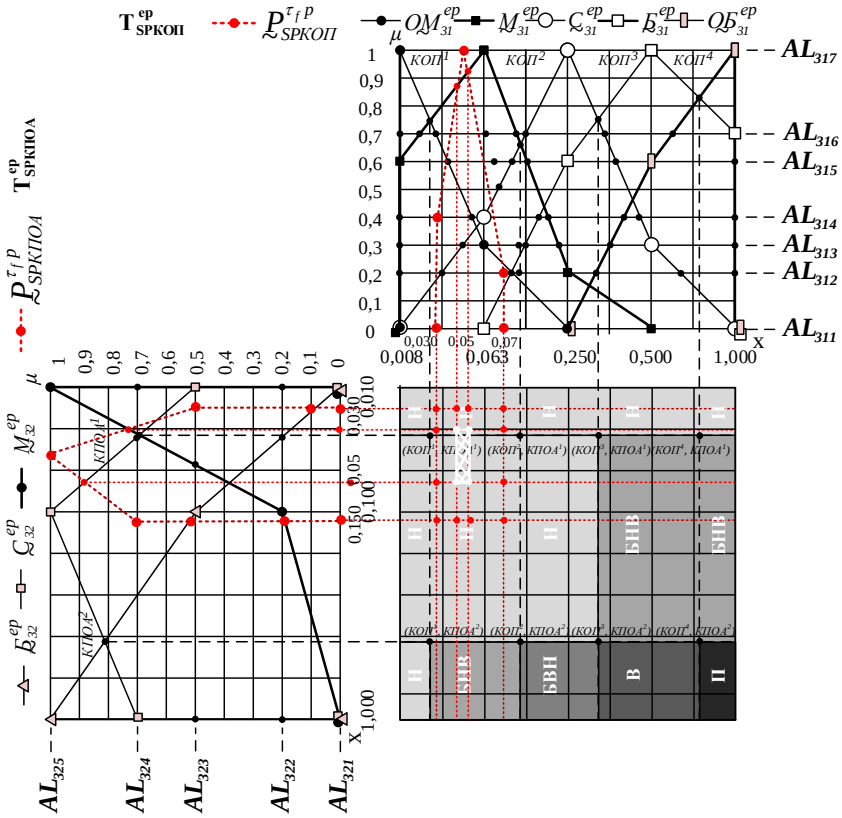

Рис. 5.31. Графічна інтерпретація поточного блоку відносно фазифікованих значень $\underset{\sim}{P}_{31}^{\tau_f}$ і $\underset{\sim}{P}_{32}^{\tau_f}$ з ІД «Н», який інтерпретує аномалію у КОП-КПОА-підсередовищі, породжену SP-середовищем

Розглянемо наступний приклад, для якого сформуємо значення величин $\underset{\sim}{P}^{\tau_f}_{SPKOP}$ та $\underset{\sim}{P}^{\tau_f}_{SPKPOA}$ поточного підсередовища ($\mathbf{P_i^{\tau_f} = P_3^{\tau_f}}$) атакуючого середовища ($\mathbf{CA^{\tau_f}}$), що несе незначну (дещо вищого мінімального рівня) загрозу ФС:

$$\underset{\sim}{P}^{\tau_f}_{SPKOP} = \{0/0{,}2;\ 0{,}4/0{,}2;\ 1/0{,}42;\ 0{,}2/0{,}75;\ 0/0{,}75\};$$

$$\underset{\sim}{P}^{\tau_f}_{SPKPOA} = \{0/0{,}05;\ 0{,}5/0{,}05;\ 1/0{,}3;\ 0{,}7/0{,}5;\ 0/0{,}5\}.$$

Далі, відповідно до номіналізованих НЧ еталонного підсередовища ($\mathbf{T_i^e = T_3^e = T_{SP}^e}$), визначених в п. 3.2, здійснимо формування номіналізованого НЧ поточного підсередовища ($\mathbf{P_i^{\tau_f} = P_3^{\tau_f}}$) з урахуванням (3.12), тобто

$$\underset{\sim}{P}^{\tau_f p}_{31} = \{\bigcup_{g=1}^{13} \mu^p_{31g} / x^p_{31g}\} =$$

$$\{\mu^p_{311} / x^p_{311},\ \mu^p_{312} / x^p_{312},\ \mu^p_{313} / x^p_{313},\ \mu^p_{314} / x^p_{314},\ \mu^p_{315} / x^p_{315},$$
$$\mu^p_{316} / x^p_{316},\ \mu^p_{317} / x^p_{317},\ \mu^p_{318} / x^p_{318},\ \mu^p_{319} / x^p_{319},\ \mu^p_{31(10)} / x^p_{31(10)},$$
$$\mu^p_{31(11)} / x^p_{31(11)},\ \mu^p_{31(12)} / x^p_{31(12)},\ \mu^p_{31(13)} / x^p_{31(13)}\},$$

де:

- $\mu^p_{311} = \mu^p_{31(13)} = AL_{311} = 0$,
- $\mu^p_{312} = \mu^p_{31(12)} = AL_{312} = 0{,}2$,
- $\mu^p_{313} = \mu^p_{31(11)} = AL_{313} = 0{,}3$,
- $\mu^p_{314} = \mu^p_{31(10)} = AL_{314} = 0{,}4$,
- $\mu^p_{315} = \mu^p_{319} = AL_{315} = 0{,}6$,
- $\mu^p_{316} = \mu^p_{318} = AL_{316} = 0{,}7$,
- $\mu^p_{317} = \mu^p_{317} = AL_{317} = 1$,
- $\mu^p_{311} = \mu_{311} = 0$,
- $x^p_{311} = x_{311} = 0{,}2$.

$$\underset{\sim}{P}^{\tau_f p}_{32} = \{\bigcup_{g=1}^{9} \mu^p_{32g} / x^p_{32g}\} =$$

$$\{\mu^p_{321}/x^p_{321},\ \mu^p_{322}/x^p_{322},\ \mu^p_{323}/x^p_{323},\ \mu^p_{324}/x^p_{324},$$
$$\mu^p_{325}/x^p_{325},\ \mu^p_{326}/x^p_{326},\ \mu^p_{327}/x^p_{327},\ \mu^p_{328}/x^p_{328},\ \mu^p_{329}/x^p_{329}\},$$

де:

- $\mu^p_{321}=\mu^p_{329}=AL_{321}=0,$
- $\mu^p_{322}=\mu^p_{328}=AL_{322}=0{,}2,$
- $\mu^p_{323}=\mu^p_{327}=AL_{323}=0{,}5,$
- $\mu^p_{324}=\mu^p_{326}=AL_{324}=0{,}7,$
- $\mu^p_{325}=\mu^p_{325}=AL_{325}=1,$
- $\mu^p_{321}=\mu_{321}=0,$
- $x^p_{321}=x_{321}=0{,}05.$

Далі, формування номіналізованого НЧ $\underset{\sim}{P}^{\tau_f p}_{ij}=\underset{\sim}{P}^{\tau_f p}_{31}$ поточного підсередовища ($\mathbf{P^{\tau_f}_i=P^{\tau_f}_3}$) здійснюється відповідно до (3.18) за допомогою α--рівневих інтервалів $\mathbf{AL^{Ip}_{31}}$ (див. п. 3.2) при $\rho=5$ і

$$\mu_{31max}=\bigvee_{q=1}^{\rho}\mu_{31q}=\mu_{311}\vee\mu_{312}\vee\mu_{313}\vee\mu_{314}\vee\mu_{315}=$$
$$0\vee 0{,}4\vee 1\vee 0{,}2\vee 0=\mu_{313}=1$$

та якщо:

- $r_1=1,\ c=\overline{1,k_1},\ k_1=3$ і $(\mu_{311}<AL^{Ip}_{311c}\le\mu_{312})\wedge(x_{312}\le x_{31max})$ $((0<AL^{Ip}_{311c}\le 0{,}4)\wedge(0{,}2\le 0{,}42))$, то

$$\mathbf{AL^{Ip}_{311}}=\{\bigcup_{c=1}^{k_1}AL^{Ip}_{311c}\}=\{AL^{Ip}_{3111},\ AL^{Ip}_{3112},\ AL^{Ip}_{3113}\}=\{0{,}2;\ 0{,}3;\ 0{,}4\};$$

- $r_2=2,\ c=\overline{1,k_2},\ k_2=3,\ (\mu_{312}<AL^{Ip}_{312c}\le\mu_{313})\wedge(x_{313}\le x_{31max})$ $((0{,}4<AL^{Ip}_{312c}\le 1)\wedge,(0{,}42\le 0{,}42))$, то

$$\mathbf{AL^{Ip}_{312}}=\{\bigcup_{c=1}^{k_2}AL^{Ip}_{312c}\}=\{AL^{Ip}_{3121},\ AL^{Ip}_{3122},\ AL^{Ip}_{3123}\}=\{0{,}6;\ 0{,}7;\ 1\};$$

- $r_3=3,\ c=\overline{1,k_3},\ k_3=5,\ (\mu_{313}>AL^{Ip}_{313c}\ge\mu_{314})\wedge(x_{314}\ge x_{31max})$ $((1>AL^{Ip}_{313c}\ge 0{,}2)\wedge(0{,}75\ge 0{,}42))$, то

$$\mathbf{AL^{Ip}_{313}} = \{\bigcup_{c=1}^{k_3} AL^{Ip}_{313c}\} = \{ AL^{Ip}_{3131},\ AL^{Ip}_{3132},\ AL^{Ip}_{3133},\ AL^{Ip}_{3134},\ AL^{Ip}_{3135} \} =$$

$$\{ 0{,}7;\ 0{,}6;\ 0{,}4;\ 0{,}3;\ 0{,}2 \};$$

- $r_4 = 4,\ c = \overline{1,k_4},\ k_4 = 1,\ (\mu_{314} > AL^{Ip}_{314c} \geq \mu_{315}) \wedge (x_{315} \geq x_{31max})$ $((0{,}2 > AL^{Ip}_{314c} \geq 1) \wedge (0{,}75 \geq 0{,}42))$, то

$$\mathbf{AL^{Ip}_{314}} = \{\bigcup_{c=1}^{k_4} AL^{Ip}_{314c}\} = \{ AL^{Ip}_{3141} \} = \{0\}.$$

З урахуванням обчислених значень, отримаємо наступний вигляд

$$\mathbf{AL^{Ip}_{31}} = \{\bigcup_{b=1}^{\rho-1} \{\bigcup_{c=1}^{k_b} AL^{Ip}_{31bc}\}\} =$$

$$\{\{ AL^{Ip}_{3111},\ AL^{Ip}_{3112},\ AL^{Ip}_{3113} \},\ \{ AL^{Ip}_{3121},\ AL^{Ip}_{3122},\ AL^{Ip}_{3123} \},$$
$$\{ AL^{Ip}_{3131},\ AL^{Ip}_{3132},\ AL^{Ip}_{3133},\ AL^{Ip}_{3134},\ AL^{Ip}_{3135} \},\ \{ AL^{Ip}_{3141} \}\} =$$
$$\{\{ 0{,}2;\ 0{,}3;\ 0{,}4 \},\ \{ 0{,}6;\ 0{,}7;\ 1 \},$$
$$\{ 0{,}7;\ 0{,}6;\ 0{,}4;\ 0{,}3;\ 0{,}2 \},\ \{ 0 \}\}.$$

За аналогією з прикладом для $\underset{\sim}{P}^{\tau_f p}_{31}$, формування номіналізованого НЧ $\underset{\sim}{P}^{\tau_f p}_{ij} = \underset{\sim}{P}^{\tau_f p}_{32}$ поточного підсередовища ($\mathbf{P^{\tau_f}_i} = \mathbf{P^{\tau_f}_3}$) реалізується на основі (3.19) за допомогою α-рівневих інтервалів $\mathbf{AL^{Ip}_{32}}$ (див. п. 3.2), тобто

$$\mathbf{AL^{Ip}_{32}} = \{\bigcup_{b=1}^{\rho-1} \{\bigcup_{c=1}^{k_b} AL^{Ip}_{32bc}\}\} =$$

$$\{\{ AL^{Ip}_{3211},\ AL^{Ip}_{3212} \},\ \{ AL^{Ip}_{3221},\ AL^{Ip}_{3222} \},\ \{ AL^{Ip}_{3231} \},$$
$$\{ AL^{Ip}_{3241},\ AL^{Ip}_{3242},\ AL^{Ip}_{3243},\ AL^{Ip}_{3244} \}\} =$$
$$\{\{ 0{,}2;\ 0{,}5 \},\ \{ 0{,}7;\ 1 \},\ \{ 0{,}7 \},\ \{ 0{,}5;\ 0{,}2;\ 1 \}\}.$$

Обчислення значень x^p_{31g} для перетворених НЧ $\underset{\sim}{P}^{\tau_f p}_{31} = \underset{\sim}{P}^{\tau_f p}_{SPKOP}$ поточного підсередовища ($\mathbf{P^{\tau_f}_i} = \mathbf{P^{\tau_f}_3}$) здійснюється аналогічно до кроку 4 (див. п. 3.2) з урахуванням (3.22) при $z = 13,\ g = \overline{2,13}$ на основі компонентів μ_{ijg} / x_{ijg} (див. приклад етапу 3 в п. 3.1), тобто $\mu_{311} = 0,\ \mu_{312} = 0{,}4,\ x_{311} = 0{,}2$ та $x_{312} = 0{,}2$.

Далі, з урахуванням цього:

- якщо $\mu^{p}_{312} = AL^{Ip}_{312} = 0{,}2$, то
$$x^{p}_{312} = 0{,}2 + ((0{,}2 - 0) \cdot (0{,}2 - 0{,}2)) / (0{,}4 - 0) = 0{,}2;$$
- якщо $\mu^{p}_{313} = AL^{Ip}_{313} = 0{,}3$, то
$$x^{p}_{313} = 0{,}2 + ((0{,}3 - 0) \cdot (0{,}2 - 0{,}2)) / (0{,}4 - 0) = 0{,}2;$$
- якщо $\mu^{p}_{314} = AL^{Ip}_{314} = 0{,}4$, то
$$x^{p}_{314} = 0{,}2 + ((0{,}4 - 0) \cdot (0{,}2 - 0{,}2)) / (0{,}4 - 0) = 0{,}2.$$

Наступним, при $\mu_{312} = 0{,}4$, $\mu_{313} = 1$, $x_{312} = 0{,}2$ та $x_{313} = 0{,}42$:

- якщо $\mu^{p}_{315} = AL^{Ip}_{315} = 0{,}6$, то
$$x^{p}_{315} = 0{,}2 + ((0{,}6 - 0{,}4) \cdot (0{,}42 - 0{,}2)) / (1 - 0{,}4) = 0{,}27;$$
- якщо $\mu^{p}_{316} = AL^{Ip}_{316} = 0{,}7$, то
$$x^{p}_{316} = 0{,}2 + ((0{,}7 - 0{,}4) \cdot (0{,}42 - 0{,}2)) / (1 - 0{,}4) = 0{,}31;$$
- якщо $\mu^{p}_{317} = AL^{Ip}_{317} = 1$, то
$$x^{p}_{317} = 0{,}2 + ((1 - 0{,}4) \cdot (0{,}42 - 0{,}2)) / (1 - 0{,}4) = 0{,}42.$$

Далі, при $\mu_{313} = 1$, $\mu_{314} = 0{,}2$, $x_{313} = 0{,}42$ та $x_{314} = 0{,}75$:

- якщо $\mu^{p}_{318} = AL^{Ip}_{318} = 0{,}7$, то
$$x^{p}_{318} = 0{,}2 + ((0{,}7 - 1) \cdot (0{,}75 - 0{,}42)) / (0{,}2 - 1) = 0{,}324;$$
- якщо $\mu^{p}_{319} = AL^{Ip}_{319} = 0{,}6$, то
$$x^{p}_{319} = 0{,}2 + ((0{,}6 - 1) \cdot (0{,}75 - 0{,}42)) / (0{,}2 - 1) = 0{,}365;$$
- якщо $\mu^{p}_{31(10)} = AL^{Ip}_{31(10)} = 0{,}4$ то
$$x^{p}_{31(10)} = 0{,}2 + ((0{,}4 - 1) \cdot (0{,}75 - 0{,}42)) / (0{,}2 - 1) = 0{,}448;$$
- якщо $\mu^{p}_{31(11)} = AL^{Ip}_{31(11)} = 0{,}3$, то
$$x^{p}_{31(11)} = 0{,}2 + ((0{,}3 - 1) \cdot (0{,}75 - 0{,}42)) / (0{,}2 - 1) = 0{,}489;$$
- якщо $\mu^{p}_{31(12)} = AL^{Ip}_{31(12)} = 0{,}2$, то
$$x^{p}_{31(12)} = 0{,}2 + ((0{,}2 - 1) \cdot (0{,}75 - 0{,}42)) / (0{,}2 - 1) = 0{,}53.$$

Наступним, при $\mu_{314} = 0{,}2$, $\mu_{315} = 0$, $x_{314} = 0{,}75$ та $x_{315} = 0{,}75$ для $\mu^{ep}_{31(13)} = AL^{Ip}_{31(13)} = 0$ визначимо

$$x^{ep}_{31(13)} = 0,75 + ((0-0,2)\cdot(0,75-0,75))/(0-0,2) = 0,75,$$

а $\mu^{p}_{311} = \mu_{311} = 0,\ x^{p}_{311} = x_{311} = 0,2.$

Таким чином, номіналізоване НЧ поточного підсередовища ($\mathbf{P}^{\tau_f}_{\mathbf{i}} = \mathbf{P}^{\tau_f}_{\mathbf{3}}$) відповідно до (3.12) приймає вигляд:

$$\underset{\sim}{P}^{\tau_f p}_{31} = \underset{\sim}{P}^{\tau_f p}_{SPKOII} = \{0/0,2;\ 0,2/0,2;\ 0,3/0,2;\ 0,4/0,2;$$
$$0,6/0,27;\ 0,7/0,31;\ 1/0,42;\ 0,7/0,324;\ 0,6/0,365;\ 0,4/0,448;$$
$$0,3/0,489;\ 0,2/0,53;\ 0/0,75\}.$$

Обчислення значень x^{p}_{36g} для перетворених НЧ $\underset{\sim}{P}^{\tau_f p}_{32} = \underset{\sim}{P}^{\tau_f p}_{SPKIIOA}$ поточного підсередовища ($\mathbf{P}^{\tau_f}_{\mathbf{i}} = \mathbf{P}^{\tau_f}_{\mathbf{3}} = \mathbf{P}^{\tau_f}_{\mathbf{SP}}$) здійснюється аналогічно, з урахуванням (3.22), при $z = 9$ за допомогою компонентів μ_{ijg} / x_{ijg} (див. приклад етапу 3 в п. 3.1), тобто

при $\mu_{321} = 0,\ \mu_{322} = 0,5,\ x_{321} = 0,05$ та $x_{322} = 0,05$.

Далі, з урахуванням цих значень:

- якщо $\mu^{p}_{322} = AL^{Ip}_{322} = 0,2$, то $x^{p}_{322} = 0,05$;
- якщо $\mu^{p}_{323} = AL^{Ip}_{323} = 0,5$, то $x^{p}_{323} = 0,05$.

При $\mu_{322} = 0,5,\ \mu_{323} = 1,\ x_{322} = 0,05$ та $x_{323} = 0,3$:

- якщо $\mu^{p}_{324} = AL^{Ip}_{324} = 0,7$, то $x^{p}_{324} = 0,15$;
- якщо $\mu^{p}_{325} = AL^{Ip}_{325} = 1$, то $x^{p}_{325} = 0,3$.

Наступним, при $\mu_{323} = 1,\ \mu_{324} = 0,7,\ x_{323} = 0,3$ та $x_{324} = 0,5$ для $\mu^{p}_{326} = AL^{Ip}_{326} = 0,7$ обчислимо $x^{p}_{326} = 0,5$

І, нарешті, при $\mu_{324} = 0,7,\ \mu_{325} = 0,\ x_{324} = 0,5$ та $x_{325} = 0,5$ для $\mu^{p}_{327} = AL^{Ip}_{327} = 0,5,\ \mu^{p}_{328} = AL^{Ip}_{328} = 0,2,\ \mu^{p}_{329} = AL^{Ip}_{329} = 0$ відповідно обчислимо $x^{p}_{327} = x^{p}_{328} = x^{p}_{329} = 0,5$, а $\mu^{p}_{321} = \mu_{321} = 0,\ x^{p}_{321} = x_{321} = 0,05$.

Таким чином, номіналізоване НЧ поточного підсередовища ($\mathbf{P}^{\tau_f}_{\mathbf{i}} = \mathbf{P}^{\tau_f}_{\mathbf{3}} = \mathbf{P}^{\tau_f}_{\mathbf{SP}}$) відповідно до (3.12) має вигляд

$$\underset{\sim}{P}^{\tau_f p}_{32} = \underset{\sim}{P}^{\tau_f p}_{SPKIIOA} = \{0/0,05;\ 0,2/0,05;\ 0,5/0,05;\ 0,7/0,15;$$
$$1/0,3;\ 0,7/0,5;\ 0,5/0,5;\ 0,2/0,5;\ 0/0,5\}.$$

Зведемо отримані дані до узагальнювальних табл. 5.3-5.4

Таблиця 5.3

Узагальнювальна таблиця для $\underset{\sim}{P}^{p}_{SPKOП}$

$\underset{\sim}{P}^{\tau_f p}_{31}$	$\mu^{p}_{31g}\ (g=\overline{1,13})$												
	μ^{p}_{311}	μ^{p}_{312}	μ^{p}_{313}	μ^{p}_{314}	μ^{p}_{315}	μ^{p}_{316}	μ^{p}_{317}	μ^{p}_{318}	μ^{p}_{319}	$\mu^{p}_{31(10)}$	$\mu^{p}_{31(11)}$	$\mu^{p}_{31(12)}$	$\mu^{p}_{31(13)}$
	0	0,2	0,3	0,4	0,6	0,7	1	0,7	0,6	0,4	0,3	0,2	0
$\underset{\sim}{P}^{\tau_f p}_{SPKOП}$	*0,2*	*0,2*	*0,2*	*0,2*	*0,27*	*0,31*	*0,42*	*0,324*	*0,365*	*0,448*	*0,489*	*0,53*	*0,75*

Таблиця 5.4

Узагальнювальна таблиця для $\underset{\sim}{P}^{p}_{SPKПOA}$

$\underset{\sim}{P}^{\tau_f p}_{32}$	$\mu^{p}_{32g}\ (g=\overline{1,9})$								
	μ^{p}_{321}	μ^{p}_{322}	μ^{p}_{323}	μ^{p}_{324}	μ^{p}_{325}	μ^{p}_{326}	μ^{p}_{327}	μ^{p}_{328}	μ^{p}_{329}
	0	0,2	0,5	0,7	1	0,7	0,5	0,2	0
$\underset{\sim}{P}^{\tau_f p}_{SPKПOA}$	*0,05*	*0,05*	*0,05*	*0,15*	*0,3*	*0,5*	*0,5*	*0,5*	*0,5*

Далі, відповідно до п. 3.3, сформуємо ХО:

$$\mathbf{XP^{1}_{31}} = \{\bigcup_{s=1}^{5} XP^{1}_{31s}\} = \{XP^{1}_{311},\ XP^{1}_{312},\ XP^{1}_{313},\ XP^{1}_{314},\ XP^{1}_{315}\} =$$

$$\{h(\underset{\sim}{T}^{ep}_{311},\ \underset{\sim}{P}^{\tau_f p}_{31}),\ h(\underset{\sim}{T}^{ep}_{312},\ \underset{\sim}{P}^{\tau_f p}_{31}),\ h(\underset{\sim}{T}^{ep}_{313},\ \underset{\sim}{P}^{\tau_f p}_{31}),$$

$$h(\underset{\sim}{T}^{ep}_{314},\ \underset{\sim}{P}^{\tau_f p}_{31}),\ h(\underset{\sim}{T}^{ep}_{315},\ \underset{\sim}{P}^{\tau_f p}_{31})\} =$$

$$\{4{,}086;\ 3{,}111;\ 1{,}587;\ 3{,}464;\ 4{,}794\};$$

$$\mathbf{XP^{1}_{32}} = \{\bigcup_{s=1}^{3} XP^{1}_{32s}\} = \{XP^{1}_{321},\ XP^{1}_{322},\ XP^{1}_{323}\} =$$

$$\{h(\underset{\sim}{T}^{ep}_{321},\ \underset{\sim}{P}^{\tau_f p}_{32}),\ h(\underset{\sim}{T}^{ep}_{322},\ \underset{\sim}{P}^{\tau_f p}_{32}),\ h(\underset{\sim}{T}^{ep}_{323},\ \underset{\sim}{P}^{\tau_f p}_{32})\} =$$

$$\{2{,}25;\ 2{,}424;\ 3{,}104\}.$$

Далі, визначення $IX^{1}_{31NUM_{31}}$ та $IX^{1}_{32NUM_{32}}$ здійснюється за допомогою функції $F^{1}(\mathbf{XP^{1}_{31}})$ і $F^{1}(\mathbf{XP^{1}_{32}})$, яка реалізує пошук мінімального значення із членів підмножини $\mathbf{XP^{1}_{31}}$ та $\mathbf{XP^{1}_{32}}$ (див. (3.31)) відповідно до (3.32) і (3.33), тобто:

$$IX^{1}_{31NUM_{31}} = \bigwedge_{s=1}^{5} XP^{1}_{31s} =$$

$$XP^{1}_{311} \wedge XP^{1}_{312} \wedge XP^{1}_{313} \wedge XP^{1}_{314} \wedge XP^{1}_{315} =$$
$$4{,}086 \wedge 3{,}111 \wedge 1{,}587 \wedge 3{,}464 \wedge 4{,}794 =$$
$$XP^{1}_{313} = 1{,}587;$$

$$IX^{1}_{32\,NUM_{32}} = \bigwedge_{s=1}^{3} XP^{1}_{32s} =$$
$$XP^{1}_{321} \wedge XP^{1}_{322} \wedge XP^{1}_{323} =$$
$$2{,}25 \wedge 2{,}424 \wedge 3{,}104 =$$
$$XP^{1}_{321} = 2{,}25.$$

Виходячи з обчислень видно, що ідентифікуючим в $\mathbf{T^{e}_{31}}$ буде терм $\underset{\sim}{T}^{e}_{313} = \underset{\sim}{C}^{e}_{31}$ (див. приклад для (2.35)), а відповідне йому перетворене еталонне є $\underset{\sim}{T}^{ep}_{313} = \underset{\sim}{T}^{ep}_{SPKOП3} = \underset{\sim}{C}^{ep}_{31}$ (див. приклад етапу 2 для (3.10)). Фактично, обчислення показують, що $XP^{1}_{313} = 1{,}587$, отже перетворене НЧ $\underset{\sim}{P}^{\tau_f p}_{31} = \underset{\sim}{P}^{\tau_f p}_{SPKOП}$ поточного підсередовища ($\mathbf{P^{\tau_f}_{i} = P^{\tau_f}_{3} = P^{\tau_f}_{SP}}$) найближче розташоване до перетвореного НЧ $\underset{\sim}{T}^{ep}_{313} = \underset{\sim}{C}^{ep}_{31}$ еталонного підсередовища ($\mathbf{T^{e}_{i} = T^{e}_{3} = T^{e}_{SP}}$). А, оскільки, $\underset{\sim}{P}^{\tau_f p}_{SPKOП}$ та $\underset{\sim}{C}^{ep}_{31}$ є відображенням $\underset{\sim}{P}^{\tau_f p}_{SPKOП}$ та $\underset{\sim}{C}^{e}_{31}$, то $\underset{\sim}{P}^{\tau_f p}_{SPKOП}$ найближче розташоване до НЧ $\underset{\sim}{C}^{e}_{31}$ еталонного підсередовища ($\mathbf{T^{e}_{i} = T^{e}_{3} = T^{e}_{SP}}$).

Аналогічно, ідентифікуючим в $\mathbf{T^{e}_{32}}$ є значення $\underset{\sim}{T}^{e}_{321} = \underset{\sim}{M}^{e}_{32}$ (див. приклад для (2.35)) та, при цьому, $\underset{\sim}{T}^{ep}_{321} = \underset{\sim}{T}^{ep}_{SPKПОА\,1} = \underset{\sim}{M}^{ep}_{32}$ (див. приклад етапу 2 для (3.10)). Також, враховуючи, що $XP^{1}_{321} = 2{,}25$, то перетворене НЧ $\underset{\sim}{P}^{\tau_f p}_{32} = \underset{\sim}{P}^{\tau_f p}_{SPKПОА}$ поточного підсередовища ($\mathbf{P^{\tau_f}_{i} = P^{\tau_f}_{3} = P^{\tau_f}_{SP}}$) найближче до перетвореного НЧ $\underset{\sim}{T}^{ep}_{321} = \underset{\sim}{M}^{ep}_{32}$ еталонного підсередовища ($\mathbf{T^{e}_{i} = T^{e}_{3} = T^{e}_{SP}}$). І, отже, якщо $\underset{\sim}{P}^{\tau_f p}_{SPKПОА}$ та $\underset{\sim}{M}^{ep}_{32}$ є відображенням $\underset{\sim}{P}^{\tau_f p}_{SPKПОА}$ та $\underset{\sim}{M}^{e}_{32}$, то $\underset{\sim}{P}^{\tau_f p}_{SPKПОА}$ є найближчим до $\underset{\sim}{M}^{e}_{32}$.

Відповідно до (4.3) наступним за ідентифікуючим для $\mathbf{T^{e}_{31}}$ буде слідувати терм з $XP^{1}_{312} = 3{,}111$, тобто це $\underset{\sim}{T}^{e}_{312}$, який і є допоміжним, а для $\mathbf{T^{e}_{32}}$ – терм з $XP^{1}_{322} = 2{,}424$, тобто $\underset{\sim}{T}^{e}_{322}$.

Далі, з урахуванням (4.6) та допоміжних термів XP^1_{312} і XP^1_{322} розрахуємо нормуючі коефіцієнти:

$$k_{31} = 1/(XP^1_{313} + XP^1_{312}) = 1/(1{,}587 + 3{,}111) = 0{,}213;$$

$$k_{32} = 1/(XP^1_{321} + XP^1_{322}) = 1/(2{,}25 + 2{,}424) = 0{,}214.$$

На основі (4.7) обчислимо експертні коефіцієнти параметрів ($P_{31} = P_{SPKOP} = KOP$ та $P_{32} = P_{SPKPOA} = KPOA$)

$$EC^{min}_{31} = 1 - k_{31} \cdot XP^1_{312},$$

$$EC^{max}_{31} = 1 - k_{31} \cdot XP^1_{313},$$ тобто

$$EC^{min}_{31} = 1 - 0{,}213 \cdot 3{,}111 = 0{,}338,$$

$$EC^{max}_{31} = 1 - 0{,}213 \cdot 1{,}587 = 0{,}662$$ та

$$EC^{min}_{32} = 1 - k_{32} \cdot XP^1_{322},$$

$$EC^{max}_{32} = 1 - k_{32} \cdot XP^1_{321},$$ тобто

$$EC^{min}_{32} = 1 - 0{,}214 \cdot 2{,}424 = 0{,}482,$$

$$EC^{max}_{32} = 1 - 0{,}214 \cdot 2{,}25 = 0{,}518.$$

Зазначимо, що $EC^{max}_{31} = 0{,}662$ та $EC^{max}_{32} = 0{,}518$ будуть відображати рівень упевненості експерта щодо значень сформованих поточних величин $\underset{\sim}{P}^{\tau_f p}_{31}$ і $\underset{\sim}{P}^{\tau_f p}_{32}$ відносно їх еталонних термів, що, відповідно, входять до $\mathbf{T^e_{31}}$ і $\mathbf{T^e_{32}}$.

З урахуванням (4.9) розрахуємо експертний коефіцієнт кібератаки ($\mathbf{CA^{\tau_f}_3 = CA^{\tau_f}_{SP} = SP^{\tau_f}}$):

$$EC^{CA}_3 = (EC^{max}_{31} + EC^{max}_{32})/2 = (0{,}662 + 0{,}518)/2 = 0{,}59.$$

З використанням (4.33) та отриманих експертних коефіцієнтів параметрів (EC^{max}_{31}, EC^{max}_{32}) і кібератаки (EC^{CA}_3) визначимо умовний вираз з підмножини $\mathbf{DR_{3\ 13}}$ (див. приклад в п. 4.2) детекційного підсередовища ($\mathbf{DR_{SP}}$) для виявлення спуфінгу, що інтерпретується, як: «Якщо поточний параметр «Кількість одночасних підключень до

сервера» в момент часу τ_f найближчий до значення еталону «Середнє» (з експертним коефіцієнтом $0{,}662$) і поточний параметр «Кількість пакетів з однаковою адресою відправника та одержувача» в момент часу τ_f найближчий до значення еталону «Мале» (з експертним коефіцієнтом $0{,}518$), то рівень аномального стану, породженого спуфінгом буде «Більш низький ніж високий» (з експертним коефіцієнтом кібератаки $0{,}59$)», що з урахуванням (4.33) можна записати, як

$$if\ \ (E(NUM_{SPKOП},\ 3)\big|_{0{,}662} \wedge E(NUM_{SPKПОА},\ 1)\big|_{0{,}518})$$
$$then\ \ "БНВ"\big|_{0{,}59}.$$

Із застосованого еквівалентного представлення видно, що для виявлення кібератаки із підмножини $\mathbf{DR}_{3\ 13}$ був застосований умовний вираз з ІД аномальності «БНВ».

На рис. 5.32 графічно показаний поточний блок (у вигляді заштрихованої прямокутної області, яка утворена за допомогою $\underset{\sim}{P}_{31}^{\tau_f}$, $\underset{\sim}{P}_{32}^{\tau_f}$) з ІД аномальності «БНВ», який інтерпретує аномалію у *2*-вимірному параметричному КОП-КПОА-підсередовищі ($\mathbf{P_i}=\mathbf{P_3}=\mathbf{P_{SP}}$), породжену відповідним атакуючим SP-середовищем ($\mathbf{CA}^{\tau_f}$) в момент часу τ_f.

Відповідно до наведеного прикладу видно, що при незначному (дещо вищого мінімального) рівні загроз програмна модель СВК ідентифікує аномальний стан, що може бути породжений кібератакою, як «Більш низький ніж високий». Це відповідає (з урахуванням експертних коефіцієнтів та коефіцієнта кібератаки) адекватній реакції СВК на незначний вплив загроз на РІС.

У наступному прикладі скористаємось сформованими значеннями величин $\underset{\sim}{P}_{SPKOП}^{\tau_f}$ та $\underset{\sim}{P}_{SPKПОА}^{\tau_f}$ поточного підсередовища ($\mathbf{P_i^{\tau_f}} = \mathbf{P_3^{\tau_f}}$) (див. п. 3.2), що несе високий рівень загроз ФС:

$$\underset{\sim}{P}_{SPKOП}^{\tau_f} = \{0/0{,}095;\ 0{,}4/0{,}095;\ 1/0{,}28;\ 0{,}2/0{,}58;\ 0/0{,}58\};$$
$$\underset{\sim}{P}_{SPKПОА}^{\tau_f} = \{0/0{,}082;\ 0{,}5/0{,}082;\ 1/0{,}82;\ 0{,}7/1;\ 0/1\}.$$

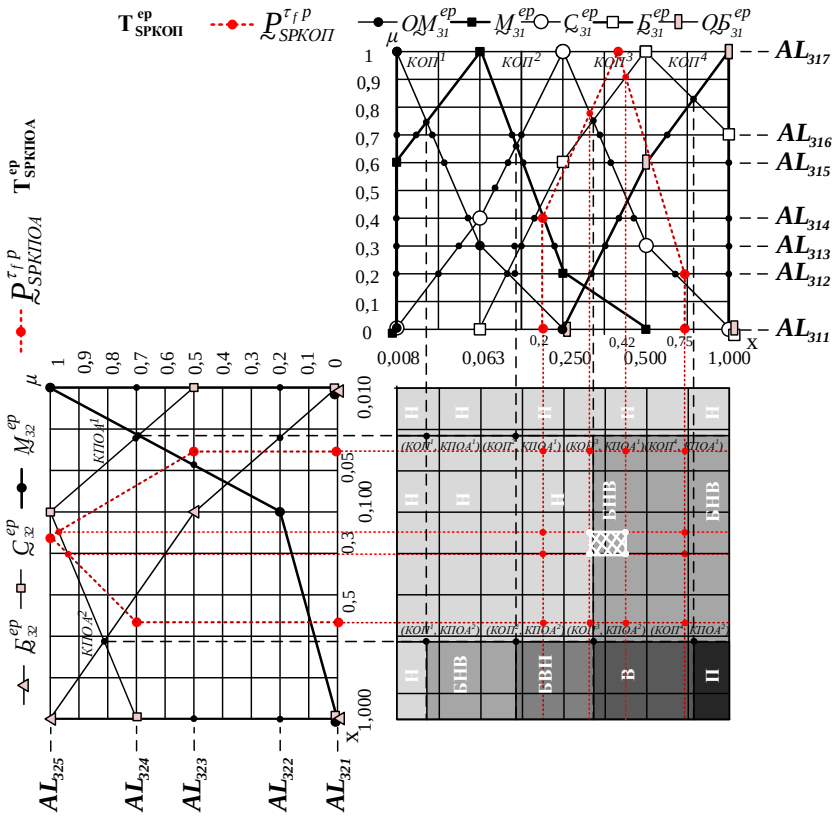

Рис. 5.32. Графічна інтерпретація поточного блоку відносно фазифікованих значень $\underset{\sim}{P}_{31}^{\tau_f}$ і $\underset{\sim}{P}_{32}^{\tau_f}$ з ІД «БНВ», який інтерпретує аномалію у КОП-КПОА-підсередовищі, породжену SP-середовищем

З урахуванням (4.33) та отриманих експертних коефіцієнтів параметрів (EC_{31}^{max}, EC_{32}^{max}) і кібератаки (EC_3^{CA}) зазначимо умовний вираз з підмножини $\mathbf{DR}_{3\ 13}$ (див. приклад в п. 4.2) детекційного підсередовища ($\mathbf{DR}_{SP}$) для виявлення спуфінгу: «Якщо поточний параметр «Кількість одночасних підключень до сервера» в момент часу

τ_f найближчий до значення еталону «Середнє» (з експертним коефіцієнтом $0{,}713$) і поточний параметр «Кількість пакетів з однаковою адресою відправника та одержувача» в момент часу τ_f найближчий до значення еталону «Велике» (з експертним коефіцієнтом $0{,}741$), то рівень аномального стану, породженого спуфінгом буде «Більш високим ніж низьким» (з експертним коефіцієнтом кібератаки $0{,}727$)». З урахуванням (4.33) можна застосувати еквівалентний запис:

$$if \ \ (E\,(NUM_{SPKOП},\ 3)\big|_{0{,}713} \wedge E\,(NUM_{SPKПОА},\ 3)\big|_{0{,}741})$$
$$then \ "БВН"\big|_{0{,}727}\ .$$

Як бачимо, для виявлення кібератаки із підмножини $\mathbf{DR_{3\ 13}}$ був застосований умовний вираз з ІД аномальності «БВН».

На рис. 5.33 графічно показаний поточний блок (у вигляді заштрихованої прямокутної області, яка утворена за допомогою $\underset{\sim}{P}_{31}^{\tau_f}$, $\underset{\sim}{P}_{32}^{\tau_f}$) з ІД аномальності «БВН», який інтерпретує аномалію у КОП-КПОА-підсередовищі ($\mathbf{P_i{=}P_3{=}P_{SP}}$), породжену відповідним атакуючим SP-середовищем ($\mathbf{CA^{\tau_f}}$) в момент часу τ_f.

Відповідно до представленого прикладу видно, що при високому рівні загроз СВК ідентифікує аномальний стан, який може бути породжений кібератакою, як «Більш високим ніж низьким». Це відповідає адекватній реакції програмної моделі СВК високому рівню впливу кібератак на РІС.

За результатами експерименту можна зробити висновок, що у всіх випадках модель СВК адекватно реагує на впливи атакуючого середовища. На основі такого типу програмних розробок можна удосконалювати сучасні СВВ за рахунок додаткової можливості динамічного (у режимі реального часу) контролю стану безпеки ІС відносно реалізованих кібератак та рівнів впливу різних типів загроз на РІС. Це, також, підтверджується наступними експериментальними даними, що адекватно відображають впливи атакуючого середовища.

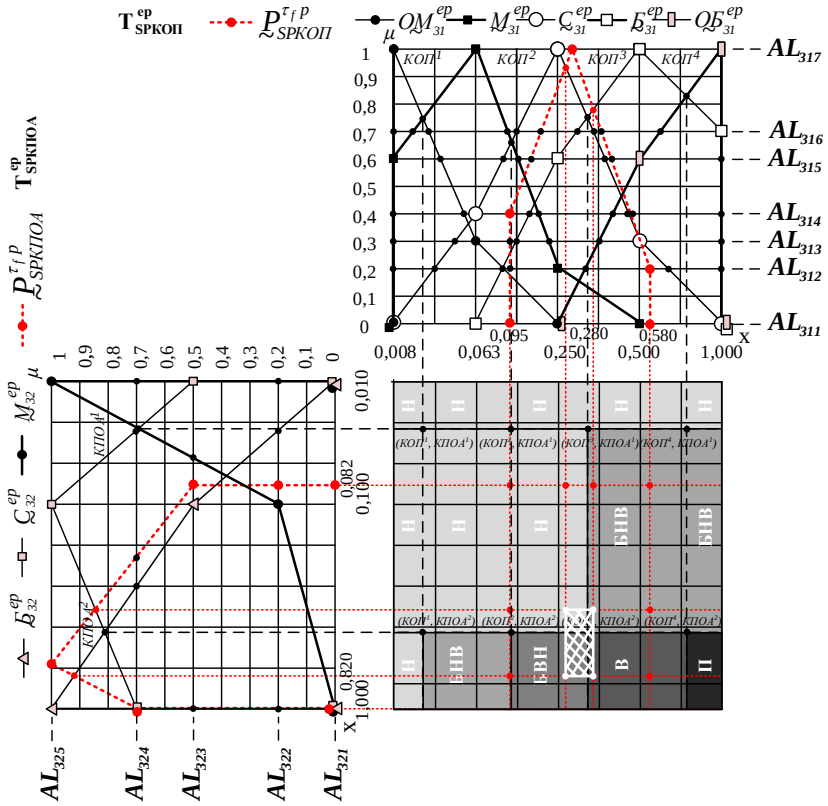

Рис. 5.33. Графічна інтерпретація поточного блоку відносно фазифікованих значень $\underset{\sim}{P}^{\tau_f}_{31}$ і $\underset{\sim}{P}^{\tau_f}_{32}$ з ІД «БВН», який інтерпретує аномалію у КОП-КПОА-підсередовищі, породжену SP-середовищем

Експериментальне дослідження здійснювалось за допомогою розробленої віртуальної мережі (див. рис. 5.29), де проведене моделювання 2000 атак (з достатньо високим рівнем впливу на ФС), кожна з яких була виявлена за допомогою певного умовного виразу сформованого детекційного середовища, яке у розглянутому випадку складається з одного підсередовища ($\mathbf{DR_3=DR_{SP}}$). Результати проведеного експерименту інтегровано в табл. 5.1.

Таблиця 5.1

Результати моделювання впливів атакуючого SP-середовища

Підмножина детекційних виразів	Задіяний ІД аномальності	Середнє значення ЕК кібератаки	Кількість кібератак	Відсоток виявлених кібератак
$DR_{3\,13}$	БВН	0,652	647	32,35%
$DR_{3\,14}$	В	0,785	910	45,5%
$DR_{3\,15}$	П	0,715	443	22,15%

Як видно з таблиці, вся множина модельованих кібератак була відповідно виявлена умовними виразами SP-середовища з ІД аномальності БВН, В та П, що входять у підмножини детекційних виразів $\mathbf{DR_{3\,13}}$, $\mathbf{DR_{3\,14}}$ та $\mathbf{DR_{3\,15}}$, на кожне з яких відповідно припало 32,35%, 45,5% та 22,15% реалізованих загроз на ФС.

Проведені експериментальні дослідження підтвердили достовірність основних теоретичних положень, практичних розробок та висновків наукової роботи.

СПИСОК ЛІТЕРАТУРИ ДО РОЗДІЛУ 5

1. А. Корченко, В. Щербина, Н. Вишневская, «Методология построения систем выявления аномалий порожденных кибератаками», *Захист інформації*, Т.18, №1, С. 30-38, 2016.

2. А. Корченко, Б. Ахметов, В. Щербина, П. Викулов, «Структурно-аналитическая модель методологии построения систем выявления вторжений», *Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS`2017): 9-та Всеук. наук.-практ. конф.*, с. Коблево Миколаївської обл., 2017, С. 42-44.

3. А. Корченко, «Кортежная модель формирования набора базовых компонент для выявления кибератак», *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, В.2 (28), С. 29-36, 2014.

4. A. Korchenko, K. Warwas, A. Kłos-Witkowska, «The Tupel Model of Basic Components' Set Formation for Cyberattacks», in *Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2015 IEEE 8th International Conference on*, 2015, pp. 478-483.

5. А. Корченко, «Модель базових компонент для виявлення кібератак на ресурси інформаційних систем», *Актуальні проблеми управління інформаційною безпекою держави: VI наук.-практ. конф.*, Київ, 2015, С. 274-275.

6. А. Корченко, «Метод формирования лингвистических эталонов для систем выявления вторжений», *Захист інформації*, Т.16, №1, С. 5-12, 2014.

7. B. Akhemetov, A. Korchenko, S. Akhmetova, N. Zhumangalieva, «Improved method for the formation of linguistic standards for of intrusion detection systems», *Journal of Theoretical and Applied Information Technology*, vol. 87, no. 2, pp. 221-232, 2016.

8. И. Терейковский, А. Корченко, П. Викулов, А. Шаховал, «Модели эталонов лингвистических переменных для обнаружения сниффинг-атак», *Захист інформації*, Т.19, №3, С. 228-242, 2017.

9. І. Терейковський, А. Корченко, П. Вікулов, І. Ірейфідж, «Моделі еталонів лінгвістичних змінних для систем виявлення email-спуфінг-атак», *Безпека інформації*. Т.24, №2, С. 99-109, 2018.

10. А. Корченко, Н. Жумангалиева, П. Викулов, «Построение лингвистических эталонов для выявления сниффинг атак», *Актуальні питання забезпечення кібернетичної безпеки та захист інформації: ІІІ міжнар. наук.-практ. конф.*, Київ, 2017, С. 93-97.

11. А. Корченко, «Формирование лингвистических эталонов на основе кортежной модели для систем выявления вторжений», *Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS`2015): 7-та Всеук. наук.-практ. конф.*, с. Коблево Миколаївської обл., 2015, С. 43-46.

12. M. Karpinski, A. Korchenko, P. Vikulov, R. Kochan, «The Etalon Models of Linguistic Variables for Sniffing-Attack Detection», in *Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2017 IEEE 9th International Conference on*, 2017, pp. 258-264.

13. А. Корченко, «Метод фаззификации параметров на лингвистических эталонах для систем выявления кибератак», *Безпека інформації*, Т.20, №1, С. 21-28, 2014.

14. Н. Карпинский, А. Корченко, С. Казмирчук, «Фаззификация параметров в кортежной модели для выявления кибератак», *Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS`2016): 8-та Всеук. наук.-практ. конф.*, с. Коблево Миколаївської обл., 2016, С. 39-42.

15. А. Корченко, «Метод α-уровневой номинализации нечетких чисел для систем обнаружения вторжений», *Захист інформації*, Т.16, №4, С. 292-304, 2014.

16. Н. Карпинский, А. Корченко, П. Викулов, Н. Жумангалиева, «Номинализация нечетких величин для систем выявления аномалий», *Современные информационные и коммуникационные технологии на транспорте, в промышленности и образовании (TEMPUS: CITISET): X междунар. науч.-практ. конф.*, Днипро, 2016, С. 51-52.

17. M. Karpinski, A. Korchenko, P. Vikulov, «Method of α-leveled nominalization of fuzzy numbers for intrusion detection systems», in *Inżynier XXI Wieku: VI Międzynarodowa Konferencja studentow oraz doktorantow, 02.12.2016: monografia*, 1st ed., Bielsko – Biała (Poland): Akademia Techniczno-Humanistyczna w Bielsku-Białej, 2016, pp. 155-164.

18. А. Корченко, «Метод определения идентифицирующих термов для систем обнаружения вторжений», *Безпека інформації,* Т.20, №3, С. 217-223, 2014.

19. А. Корченко, «Метод определения идентифицирующих термов для систем выявления кибератак», *Актуальні питання забезпечення кібернетичної безпеки та захист інформації: наук.-практ. конф.*, Київ, 2015, С. 64-67.

20. Н. Карпинский, А. Корченко, С. Ахметова, «Метод формирования базовых детекционных правил для систем обнаружения», *Захист інформації*, Т.17, №4, С. 312-324, 2015.

21. Н. Карпинский, А. Корченко, С. Ахметова, Н. Жумангалиева, «Метод построения условных детекционных выражений для систем обнаружения кибератак», *Актуальні питання забезпечення кібернетичної безпеки та захист інформації: ІІ міжнар. наук.-практ. конф.*, Київ, 2016, С. 65-69.

22. A. Korchenko, Z. Alimseitova, N. Zhumangaliyeva, «A system for identifying anomaly state in informational systems», in *Inżynier XXI Wieku: VII Międzynarodowa Konferencja studentow oraz doktorantow, 08.12.2017: monografia,* 1st ed., Vol.2., Bielsko – Biała (Poland): Akademia Techniczno-Humanistyczna w Bielsku-Białej, 2017, pp. 39-48.

23. M. Al Hadidi, Y. Ibrahim, V. Lakhno, A. Korchenko, A, Tereshchuk, A. Pereverzev, «Intelligent systems for monitoring and recognition of cyber attacks on information and communication systems of transport», *International Review on Computers and Software (IRECOS),* vol. 11, no. 2, pp. 1167-1177, 2016.

24. А. Корченко, «Система формирования нечетких эталонов сетевых параметров», *Захист інформації.* Т.15, №3, С. 240-246, 2013.

25. А. Корченко, «Система формирования эвристических правил для оценивания сетевой активности», *Захист інформації*, Т.15, №4, С. 353-359, 2013.

26. А. Корченко, «Система принятия решений для выявления аномального состояния», *Управление знаниями и конкурентная разведка : 18-й междунар. молод. форум «Радиоэлектроника и молодежь в XXI веке»*, Харьков, 2014, Т. 9, С. 81-82.

27. А. Корченко, «Система формирования эталонов параметров для выявления подозрительной активности», *Інтегровані інтелектуальні робототехнічні комплекси (ІПРТК-2014) : VII міжнар. наук.-практ. конф.*, Київ, 2014, С. 354-355.

28. «Базовые признаки классификации систем обнаружения вторжений», *Современные информационно-телекоммуникационные технологии: междунар. науч.-тех. конф.,* Казахстан, ГУТ, 2015, С. 24-26.

29. С. Казмірчук, А. Корченко, Т. Паращук, «Аналіз систем виявлення вторгнень», Захист інформації, Т.20, №4, С. 259-276, 2018.

30. І. Терейковський, А. Корченко, Т. Паращук, Є. Педченко, «Аналіз відкритих систем виявлення вторгнень», Безпека інформації. Т.24, №3, С. 201-216, 2018.

31. И. Терейковский, А. Корченко, «Система выявления кибератак», *Безпека інформації*, Т.23, №3, С. 176-180, 2017.

32. А. Корченко, С. Казмирчук, В. Щербина, П. Викулов, «Расширитель функциональных возможностей для систем обнаружения вторжений», *Актуальні питання забезпечення кібернетичної безпеки та захист інформації: IV міжнар. наук.-практ. конф.*, Київ, 2018, С. 78-80.

33. А. Корченко, О. Заріцький, Т. Паращук, В. Бичков, «Програмне забезпечення формування еталонів параметрів для систем виявлення кібератак», *Захист інформації*. Т.20, №3, С. 133-148, 2018.

34. Програмний модуль формування еталонів параметрів для систем виявлення аномалій. *Комп'ютерна програма* / Т. Паращук, А. Корченко – К. – Свідоцтво про реєстрацію авторського права на твір №74016 від 02.10.2017.

35. А.О. Корченко, Є.В. Іванченко, В.В. Погорелов, «Оцінювання ефективності експертної системи виявлення вторгнень на базі нечіткої логіки», *Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки*, Т.30 (69), №1, С. 66-72, 2019.

ВИСНОВКИ

Проведений аналіз сучасних методів та засобів виявлення кібератак, який показав їх обмежені можливості відносно функціоналу, що дозволяє таким системам здійснити в режимі реального часу необхідну адаптацію (під зміни атакуючого середовища) до виявлення аномалій, породжених модифікованими або раніше невідомими кібератаками та, таким чином, дозволив визначити задачі дослідження, які орієнтовані на побудову ефективних систем виявлення вторгнень.

Розроблено кортежну модель формування атакуючих середовищ, яка дозволяє сформувати набір часткових кортежів, для симуляції процесу виявлення аномального стану в m-вимірному гетерогенному параметричному середовищі, утвореного відповідним атакуючим середовищем у заданий часовий проміжок.

Розроблений метод формування еталонів, для формалізації процесу отримання еталонних середовищ, які містять множини значень фіксованих параметрів заданих груп лінгвістичних змінних, що характеризують конкретне еталонне підсередовище.

Запропонований метод фазифікації параметрів на еталонних підсередовищах, який дозволив формалізувати процес перетворення в нечітку форму поточних значень параметрів m-вимірних поточних середовищах для їх подальшого застосування у виявленні аномального стану.

Розроблений метод α-рівневої номіналізації нечітких чисел, який дозволив здійснити графічну інтерпретацію нечітких величин та визначення ідентифікуючих термів, що відображають у заданий момент часу значення еталонних та поточних підсередовищ, які характерні для реалізації певних типів кібератак на ресурси інформаційних систем.

Запропонований метод визначення ідентифікуючих термів, для пошуку в заданих лінгвістичних змінних, ідентифікуючих перетворених еталонних термів, за якими за допомогою детекційних виразів, визначаються рівні аномальних станів.

Розроблений метод дефазифікації параметрів детекційного середовища, який дозволив у числовій формі характеризувати рівень упевненості експерта відносно його суджень щодо можливих кібератак.

Розроблений метод формування детекційного середовища для побудови необхідної множини детекційних правил, що використовуються при визначенні поточного рівня аномального стану, характерного дії визначеного типу атак. Використання даного методу при побудові систем виявлення вторгнень також дозволить розширити їх функціональні можливості щодо виявлення кібератак в m-вимірному гетерогенному параметричному середовищі.

Запропонована методологія побудови систем виявлення аномалій, породжених кібератаками, яка використовується для визначення рівня аномального стану в m-вимірному гетерогенному параметричному середовищі.

Розроблено структурне рішення обчислювальної системи виявлення кібератак, що дозволяє за допомогою визначення рівня аномального стану, характерного впливу певного типу кібератак, розширити функціональні можливості сучасних систем виявлення вторгнень.

На базі запропонованої методології та структурного рішення розроблено, алгоритмічне забезпечення та відповідна програмна модель системи, яка може використовуватися автономно або бути розширювачем функціональних можливостей сучасних систем виявлення вторгнень.

Експериментальне дослідження програмної моделі системи, а також впровадження та успішне практичне використання відповідних розробок підтвердило достовірність теоретичних положень та гіпотез, практичних розробок і висновків наукової роботи.

Монографія

КОРЧЕНКО Анна Олександрівна

МЕТОДИ ІДЕНТИФІКАЦІЇ АНОМАЛЬНИХ СТАНІВ ДЛЯ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Редактор А.О. Корченко
Коректор А.О. Корченко
Комп'ютерна верстка М.В. Коломієць

Підписано до друку 22.02.2019. Формат 60х84/16
Ум. друк. арк. 22,5. Папір офсетний.
Надруковано в Україні.
Тираж 300 прим.

Видавець і виготовлювач ТОВ «ЦП «КОМПРИНТ»
03150, Київ, вул. Предславинська, 28
Свідоцтво про внесення до Державного реєстру
суб'єкта видавничої справи ДК № 4131 від 04.08.2011 р.