МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

**КОРЧЕНКО Анна Олександрівна**

УДК 004.056.5:004.3:004.4 (043.3)

# МЕТОДИ ІДЕНТИФІКАЦІЇ АНОМАЛЬНИХ СТАНІВ ДЛЯ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

05.13.21 – «Системи захисту інформації»

**Автореферат**

дисертації на здобуття наукового ступеня

доктора технічних наук

Київ – 2019

Дисертацією є рукопис.

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

Науковий консультант: доктор технічних наук, професор
**Терейковський Ігор Анатолійович**,
Національний технічний університет України «КПІ ім. Ігоря Сікорського»
професор кафедри системного програмування і спеціалізованих комп'ютерних систем.

Офіційні опоненти: доктор технічних наук, професор
**Грищук Руслан Валентинович**,
Житомирський військовий інститут імені С.П. Корольова, начальник кафедри захисту інформації та кібербезпеки;

доктор технічних наук, професор
**Лужецький Володимир Андрійович**,
Вінницький національний технічний університет, завідувач кафедри захисту інформації;

доктор технічних наук
**Опірський Іван Романович**,
Національний університет «Львівська політехніка», доцент кафедри захисту інформації.

Захист відбудеться «02» липня 2019 р. о $13^{\underline{00}}$ на засіданні спеціалізованої вченої ради Д 26.062.17 при Національному авіаційному університеті за адресою: 03058, м. Київ, пр. Космонавта Комарова, 1, корпус 11, ауд. 111.

З дисертацією можна ознайомитись у Науково-технічній бібліотеці Національного авіаційного університету за адресою: 03058, м. Київ, пр. Космонавта Комарова, 1.

Автореферат розісланий «___» травня 2019 р.

Учений секретар
спеціалізованої вченої ради
д.т.н., доцент С. Гнатюк

## ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

**Актуальність.** 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 на 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 відхилення 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 процеса створення відповідного статистичного профіля нормального стану ІС, а при її реконфінгурації, модифікації та інших змінах набрана статистика стає неактуальною та неповною. Необхідно також зазначити, що повні статистичні дані про систему будуть тоді, коли вона завершить своє існування в тому вигляді, у якому вона досліджувалася, але надалі не буде актуальною.

Більш ефективні в цьому відношенні є експертні підходи, що засновані на використанні знань та досвіду спеціалістів відповідної предметної області. А побудова відповідних методів, технічних рішень 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.

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.

Враховуючи викладене, тема дослідження присвячена вирішенню важливої науково-прикладної проблеми, пов'язаної з розробкою ефективних методів ідентифікації аномальних станів для СВВ, є актуальною.

Зазначена проблема обумовлюється *об'єктивним протиріччям* між постійно зростаючими витратами на моніторинг та блокування нових видів кібератак за максимально короткий час та неухильним зростанням збитків власникам РІС, що пов’язані з високою інерційністю існуючих СВВ щодо їх адаптації до виявлення аномалій, породжених реалізацією нових типів загроз. Це підтверджується відповідними регулярними публікаціями та звітами про нанесені збитки окремим підприємствам, промисловим галузям, державам та в цілому світовій економіці від реалізації нових кібератак.

Теоретичні та практичні результати, що пов'язані з процесом виявлення аномальних станів, утворених атакуючими діями на РІС, який складає об’єкт дослідження, отримані такими вітчизняними та іноземними вченими, як: О. Корченко, І. Терейковський, В. Лахно, Р. Грищук, O. Linda, J. Yao, P. Fries, D. Dasgupta та інші. Але, незважаючи на значну кількість підходів до вирішення даної проблеми, вона залишається актуальною не тільки для України, але і для всієї світової спільноти.

**Зв'язок роботи з науковими програмами, планами, темами.** Тематика дисертаційної роботи та одержані результати безпосередньо пов’язані з «Основними науковими напрямами та найважливішими проблемами фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук НАН України на 2014-2018 роки», Стратегією національної безпеки України від 26 травня 2015 року № 287/2015, Стратегією кібербезпеки України від 15 березня 2016 року №96/2016 та низкою науково-дослідних робіт (НДР). Результати досліджень відображені у звітах держбюджетних НДР «Методи та моделі виявлення уразливостей в ресурсах інформаційних систем» (2015-2017 рр.) № 25/09.01.08, «Системи мультирівневого розмежування доступу до інформаційних ресурсів», (2018-2019 рр.) № 19/14.01.05 від 01.09.2018 р., в яких здобувач був науковим керівником та відповідальним виконавцем.

**Мета та задачі дослідження.** Мета дисертаційної роботи направлена на вирішення важливої науково-прикладної проблеми, пов’язаної з виявленням нових видів кібератак за максимально короткий час шляхом розробки відповідної методології побудови систем виявлення аномальних станів, породжених реалізацією нових типів загроз, орієнтованої на створення засобів, що розширюють функціональні можливості сучасних систем виявлення вторгнень.

Для досягнення поставленої мети **розв’язуються наступні основні задачі:**

– проаналізувати сучасні методи та засоби виявлення вторгнень для вибору та розробки найбільш ефективного відповідного інструментарія;

– розробити кортежну модель формування атакуючих середовищ для відображення процесу виявлення аномального стану за заданий часовий проміжок в $m$-вимірному гетерогенному параметричному середовищі;

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

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

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

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

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

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

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

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

– розробити алгоритмічне та програмне забезпечення моделювання аномалій, породжених реалізацією різних типів кібератак і провести експериментальне дослідження для підтвердження достовірності отриманих теоретичних положень та практичних результатів.

**Об'єктом дослідження** є процес виявлення аномальних станів, утворених атакуючими діями на ресурси інформаційних систем.

**Предметом дослідження** є методи, засоби та системи виявлення аномалій, утворених атакуючими діями на ресурси інформаційних систем.

**Методи дослідження**, що використовуються в роботі, ґрунтуються на методологічному базисі теорії захисту інформації та системному аналізі новітніх теоретичних та практичних розробок, що застосовуються в галузі інформаційної безпеки для ефективного вирішення відповідних проблем кібербезпеки. Для формування кортежної моделі та її компонент використовувались методи системного аналізу, елементи теорії множин та теорії нечітких множин, моделювання та алгебра логіки. При розробці методів: формування еталонного середовища, фазифікації параметрів на еталонних підсередовищах, $\alpha$-рівневої номіналізації нечітких чисел, визначення ідентифікуючих термів, дефазифікації параметрів, формування детекційного середовища та методології побудови систем виявлення аномалій використовувалися методи та елементи нечіткої логіки, прийняття рішень, моделювання, множин, а також експертне оцінювання, аналітична геометрія та м'які обчислення. При розробці структурного рішення, алгоритмічного та програмного забезпечення системи виявлення кібератак, а також проведення експериментального дослідження застосовувались елементи теорії алгоритмів, експерименту, об'єктно-орієнтоване програмування, а також імітаційне моделювання інформаційних процесів і структур.

**Наукова новизна одержаних результатів** полягає в наступному:

– *вперше розроблена* кортежна модель формування атакуючих середовищ, 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;

– *вперше розроблений* метод формування еталонного середовища, 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;

– *вперше розроблені* методи фазифікації та дефазифікації параметрів, які на основі еталонних підсередовищ, поправкових і лінгвістичних еталонів підмножин інтервалів для формування частот зустрічальності значень фізичних параметрів в задані моменти очікуваної події та процедури визначення допоміжного терма, експертних коефіцієнтів параметрів і кібератаки, що характеризують експертні лінгвістичні оцінки, пов'язані з рівнем аномального стану в поточному середовищі дозволяють формалізувати процес перетворення значень параметрів $m$-вимірних поточних середовищ для їх подальшого застосування у виявленні аномального стану та відобразити параметри детекційного середоваща, що характеризують у числовій формі рівень упевненості експерта відносно його суджень щодо можливих кібератак;

– *вперше розроблений* метод $\alpha$-рівневої номіналізації нечітких чисел, який за рахунок побудованого механізму формування множини $\alpha$-рівней, допоміжних підмножин $\alpha$-рівневих інтервалів та міжточкових $\alpha$-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 ресурси інформаційних систем;

– *вперше розроблений* метод визначення ідентифікуючих термів, 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;

– *вперше розроблений* метод формування детекційного середовища, який на основі запропонованої кортежної моделі за рахунок механізму формування підмножин ідентифікаторів аномальності, формалізації процесу побудови вирішальних функцій та умовних детекційних виразів, дозволяє сформувати необхідну множину детекційних правил, що використовуються для визначення рівней аномальних станів, характерних впливу певних типів кібератак;

– *вперше розроблена* методологія побудови систем виявлення аномалій породжених кібератаками, яка за рахунок механізмів формування атакуючих середовищ, побудови $m_i$-вимірних параметричних еталонних та поточних підсередовищ, $\alpha$-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;

– *вперше розроблено* структурне рішення обчислювальної системи виявлення кібератак, яке за рахунок баз даних кібератак, правил та еталонів, а також модулів формування поточних значень, $\alpha$-рівневої номіналізації, дефазифікації та ідентифікуючих

термів, рівня аномальності та візуалізації дозволяє будувати засоби, які визначають рівні аномального стану, що характерні впливу певного типу кібератак і розширюють функціональні можливості сучасних систем виявлення вторгнень.

**Практичне значення отриманих результатів.** Отримані в дисертаційній роботі результати можуть бути використані для побудови програмних модулів виявлення аномальних станів, які можуть застосовуватися автономно або як розширювачі функціональних можливостей сучасних систем виявлення вторгнень.

Практична цінність роботи полягає в наступному:

– розроблене алгоритмічне та програмне забезпечення модулів, що реалізують побудову еталонних середовищ для систем виявлення кібератак;

– на основі запропонованого структурного рішення системи виявлення кібератак розроблене алгоритмічне забезпечення для реалізації відповідного програмного засобу ідентифікації аномального стану, породженого кібератаками;

– на основі запропонованого алгоритмічного забезпечення розроблено програмну модель системи для виявлення аномальних станів, породжених кібератаками, яка може використовуватися для розширення функціональні можливості сучасних систем виявлення вторгнень;

– результати дослідження впроваджені в діяльність ТОВ «Сайфер БІС», а також використовуються в навчальному процесі кафедри комп'ютеризованих систем захисту інформації Національного авіаційного університету, кафедри інформаційної безпеки, Інституту інформаційних та телекомунікаційних технологій казахського національного дослідницького технічного університета ім. К.І. Сатпаєва і кафедри інформатики та автоматики Технічно-гуманістичної академії у Бельсько-Бялій (Польща).

**Особистий внесок здобувача.** Основні положення та результати дисертаційної роботи, що виносяться на захист, отримані автором самостійно. У роботах, що написані у співавторстві, автору належать: [1-4, 6, 7, 10-15, 19-25, 27-42] – результати які отримані особисто; [5] – постановка задачі дослідження та аналіз найбільш поширених типів кібератак; [8-9] – постановка задачі дослідження та проведення аналізу методів протидії кібератакам; [16-18] – проведення аналізу методів та систем виявлення вторгнень; [26] – формування парамертів розпізнавання. З робіт, опублікованих у співавторстві, для вирішення проблеми та задач, поставлених у дисертаційному досліджені, використовуються результати отримані особисто здобувачем наукового ступеня.

**Апробація результатів дисертації.** Основні положення дисертаційної роботи доповідалися та обговорювалися на науково-технічних конференціях, семінарах, серед яких: I міжнародна науково-технічна конферентція «Проблемы информатизации» (Черкаси, 2013 р.), V науково-практична конференція «Актуальні проблеми управління інформаційною безпекою держави» (Київ, 2014 р.), 18-й Міжнародний молодіжний форум «Радиоэлектроника и молодежь в XXI веке» (Харків, 2014 р.), VII міжнародна науково-практична конференція «Інтегровані інтелектуальні робототехнічні комплекси (ІІРТК-2014)» (Київ, 2014 р.), науково-технічна конференція «Актуальні проблеми забезпечення інформаційної безпеки держави» (Київ, 2014 р.), I, II, III та IV міжнародна науково-практична конференція «Актуальні питання забезпечення кібербезпеки та захисту інформації» (Київ, 2015-2018 рр.), VI науково-практична конференція «Актуальні проблеми управління інформаційною безпекою держави» (Київ, 2015 р.), XII Міжнародна науково-технічна конференція «АВИА-2015» (Київ, 2015 р.), 7-10-а Всеукраїнська науково-практична конференція «Стан та удосконалення безпеки інформаційно-

телекомунікаційних систем (SITS`2015, SITS`2016, SITS`2017, SITS-2018)» (с. Коблево, Миколаївська обл., 2015-2017 рр.), міжнародна науково-технічна конференція «Современные информационно-телекоммуникационные технологии» (Казахстан, 2015 р.), ІІ міжнародна науково-практична конференція «Информационные и телекоммуникационные технологии: образование, наука, практика» (Алмати, 2015 р.), VI міжнародна науково-технічна конференція «ITSEC» (Київ, 2016 р.), X міжнародна науково-практична конференція «Современные информационные и коммуникационные технологии на транспорте, в промышленности и образовании (TEMPUS: CITISET)» (Дніпро, 2016 р.), 8th, 9th International Conference on (IDAACS'2015, IDAACS'2017) «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IEEE)» (Warsaw, 2015, Bucharest, 2017), VI, VII Międzynarodowa Konferencja studentow oraz doktorantow «Inżynier XXI Wieku» (Bielsku-Białej, 2016-2017), VIII Всесвітній конгрес «Авиация в XXI столетии» (Київ, 2018 р.).

**Публікації.** Базові положення дисертаційного дослідження опубліковані в 57 наукових роботах, основні 42 з яких приведені в авторефераті, в тому числі: 3 колективні монографії [1-3], 6 наукових статей в міжнародних рецензованих виданнях, що входять в бази даних Scopus та Web of Science (в періодичних [5, 6, 8, 9] та неперіодичних виданнях [4, 7]), 4 наукові статті в іноземних наукових журналах [10-13], 19 наукових статей у вітчизняних наукових журналах, які входять в інші міжнародні наукометричні бази даних [14-32], 10 матеріалів та тез доповідей міжнародних конференцій [33-42].

**Структура роботи та її обсяг.** Дисертація складається з анотації, списку скорочень, вступу, змісту, п'яти розділів, загальних висновків, додатків, списку використаних джерел до кожного розділу та має 309 сторінок основного тексту, 91 рисунок, 26 таблиць, 33 сторінки додатків. Список літератури загалом містить 241 найменування і займає 30 сторінок. Загальний обсяг роботи 405 сторінок.

## ОСНОВНА ЧАСТИНА

**В анотації та вступі** представлена загальна характеристика дисертаційної роботи, обґрунтована актуальність теми, сформульовано мету і завдання досліджень, відзначено наукову новизну та практичне значення одержаних результатів, визначено особистий внесок здобувача, наведено відомості про апробацію результатів роботи, публікації, структуру та об'єм дисертації, ключові слова.

**У першому розділі** показані результати аналізу вітчизняної та іноземної літератури за темою дисертаційної роботи.

Враховуючи результати відомих досліджень з подальшим їх узагальнюванням і відображенням щодо розширеного спектру засобів виявлення зловживань та аномалій проведено аналіз сучасних СВВ (AAFID, Snort, Prelude SIEM, NetSTAT, Shadow, ASAX, Bro, OSSEC, Cisco IPS, Arbor Networks Spectrum, InfoWatch ASAP, Symantec DeepSight Threat Management System, IPS, Tipping Poing NGIPS, Axoft invGUARD, DefensePro, KATA Platform, Suricata, Samhain та Security Onion) відносно базових характеристик, як-от «Клас кібератак», «Адаптивність», «Відкритість», «Методи виявлення», «Управління системою», «Масштабованість», «Рівень спостереження», «Реакція на кібератаку», «Захищеність» та «Підтримка ОС». Це надає можливості розробникам і користувачам обирати необхідні методи та відповідне ПЗ для захисту ІС і будувати відповідні систем безпеки.

Аналіз джерел показав, що для сучасних ІС гостро стоїть питання оперативного виявлення зловживань та аномалій. Прослідковується недосконаліть і неготовність існуючих СВВ адаптуватися в реальному режимі часу до виявлення аномалій, породжених модифікованими або раніше невідомими кібератаками. Математичний апарат нечітких множин не використовується в проаналізованих системах, але він показав свою ефективність при вирішенні такого роду завдань.

З урахуванням проведеного аналізу, визначені основні задачі та напрями наукового дослідження, що охоплюються дисертаційною роботою.

**Другий розділ** присвячений розробці кортежної моделі та методів формування еталонних середовищ для ідентифікації аномальних станів. Розроблена кортежна модель формування атакуючих середовищ (КМАС), 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, утвореному відповідним атакуючим середовищем у заданий часовий проміжок. Для формалізації процесу формування необхідних компонент вводиться множина можливих кібератак $\mathbf{CA}^{\tau_f} = \{\bigcup_{i=1}^{n} \mathbf{CA}_i^{\tau_f}\}$ $(i = \overline{1,n})$, що відображає атакуюче середовище ($\mathbf{CA}^{\tau_f}$), за визначений часовий проміжок $\tau_h$ з можливістю виявлення аномалій в момент часу $\tau_f$ ($f = \overline{1,max_\tau}$, де $max_\tau$ – максимальний номер часового проміжка $f$), де $n$ визначає кількість можливих кібератак, кожна з яких відображається узагальнювальним кортежем, елементи якого утворюють $i$-те атакуюче підсередовище

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

в якому: $CA_i$ – ідентифікатор (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 $\tau_f$ $(f = \overline{1,max_\tau})$ 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. У сукупності всі елементи підмножини $\mathbf{CA}^{\tau_f}$ визначають атакуюче середовище на РІС, стан якого фіксується часовим проміжком $\tau_f$. Сформуємо кожен компонент кортежу.

**Формування** ідентифікаторів $CA_i$ 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 $n = 5$,

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

$$\{\mathbf{CA}^{\tau_f}_{\mathbf{SNF}},\ \mathbf{CA}^{\tau_f}_{\mathbf{DS}},\ \mathbf{CA}^{\tau_f}_{\mathbf{SP}},\ \mathbf{CA}^{\tau_f}_{\mathbf{ESP}},\ \mathbf{CA}^{\tau_f}_{\mathbf{SN}}\} = \{\mathbf{SNF}^{\tau_f},\ \mathbf{DS}^{\tau_f},\ \mathbf{SP}^{\tau_f},\ \mathbf{ESP}^{\tau_f},\ \mathbf{SN}^{\tau_f}\},$$

де, наприклад, $\mathbf{CA}^{\tau_f}_{\mathbf{3}} = \mathbf{CA}^{\tau_f}_{\mathbf{SP}} = \mathbf{SP}^{\tau_f}$, відображає стан атакуючого середовища ($\mathbf{CA}^{\tau_f}$) (SP-середовища) в момент часу $\tau_f$ та за відповідним аномальним станом визначає кібератаку з ім'ям «Спуфінг (SP)», якій відповідно буде присвоєний ІД $CA_3=CA_{SP}=SP$.

**Формування** підмножини можливих параметрів $\mathbf{P}_i$ здійснюється на основі множини всіх можливих параметрів $\mathbf{P}$ та визначається як

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

при цьому $(j=\overline{1,m_i})$, $m_i$ означає кількість параметрів, за допомогою яких здійснюється виявлення аномального стану, породженого кібератакою з ІД $CA_i$. Конкретні значення членів підмножини $\mathbf{P}_i$ визначають $m_i$-вимірне параметричне підсередовище ($\mathbf{P_i}$), що використовується для виявлення кібератаки з ІД $CA_i$.

Наприклад, при $n=5$, $m_1=m_2=m_4=3$ та $m_3=m_5=2$ визначимо необхідні параметри для виявлення відповідних кібератак та отримаємо

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{5}}\mathbf{P_i}\} = \{\bigcup_{i=1}^{5}\{\bigcup_{j=1}^{m_i}P_{ij}\}\} = \{\{P_{11},\ P_{12},\ P_{13}\},\ \{P_{21},\ P_{22},\ P_{23}\},\ \{P_{31},\ P_{32}\},\ \{P_{41},\ P_{42},\ P_{43}\},$$

$$\{P_{51},\ P_{52}\}\} = \{\{P_{SNFKBП},\ P_{SNFCOП},\ P_{SNFTП}\},\ \{P_{DSKOП},\ P_{DSCO3},\ P_{DS3M3}\},\ \{P_{SPKOП},\ P_{SPKПOA}\},$$

$$\{P_{ESPKCБ},\ P_{ESPKCT},\ P_{ESPKCC}\},\ \{P_{SNKBK},\ P_{SNBBK}\}\} = \{\{КВП,\ СОП,\ ТП\},$$

$$\{КОП,\ СО3,\ ЗМЗ\},\ \{КОП,\ КПОА\},\ \{КСБ,\ КСТ,\ КСС\},\ \{КВК,\ ВВК\}\},$$

де, наприклад, $P_{31}=P_{SPKOП}=КОП$ та $P_{32}=P_{SPKПOA}=КПОА$ є параметрами, що визначають 2-вимірне параметричне підсередовище ($\mathbf{P_i=P_3=P_{SP}}$ – КОП-КПОА-підсередовище) і відповідно відображають «КОП» та «КПОА», за допомогою яких здійснюється виявлення кібератаки з ІД $CA_{SP}$ або *SP*-атаки;

**Формування** підмножини можливих нечітких еталонів $\mathbf{T}^{\mathbf{e}}_{\mathbf{i}}$ здійснюється на основі множини всіх можливих еталонів $\mathbf{T}^{\mathbf{e}}$, що відображають характерні стани відповідних параметрів з $\mathbf{P}_i$ в $m_i$-вимірному параметричному підсередовищі ($\mathbf{P_i}$) тобто

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\mathbf{T}^{\mathbf{e}}_{\mathbf{i}}\} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}}\mathbf{T}^{\mathbf{e}}_{\mathbf{ij}}\}\} = \{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\{\bigcup_{s=1}^{r_j}\underset{\sim}{T}^{e}_{ijs}\}\}\} =$$

$$\{\{\underset{\sim}{T}^{e}_{i11},\ \underset{\sim}{T}^{e}_{i12},\ldots,\ \underset{\sim}{T}^{e}_{i1r_i}\},\{\underset{\sim}{T}^{e}_{i21},\ \underset{\sim}{T}^{e}_{i22},\ldots,\ \underset{\sim}{T}^{e}_{i2r_2}\},\ldots,\{\underset{\sim}{T}^{e}_{im_i1},\ \underset{\sim}{T}^{e}_{im_i2},\ldots,\ \underset{\sim}{T}^{e}_{im_ir_{m_i}}\}\},\ldots,$$

$$\{\{\underset{\sim}{T}^{e}_{n11},\ \underset{\sim}{T}^{e}_{n12},\ldots,\ \underset{\sim}{T}^{e}_{n1r_1}\},\{\underset{\sim}{T}^{e}_{n21},\ \underset{\sim}{T}^{e}_{n22},\ldots,\ \underset{\sim}{T}^{e}_{n2r_2}\},\ldots,\{\underset{\sim}{T}^{e}_{nm_n1},\ \underset{\sim}{T}^{e}_{nm_n2},\ldots,\ \underset{\sim}{T}^{e}_{nm_nr_{m_n}}\}\}\},$$

при цьому $\mathbf{T}^{\mathbf{e}}_{\mathbf{ij}}$ $(j=\overline{1,m_i})$ – підмножина лінгвістичних еталонів, яка відображає характерні судження експерта відносно аномальності стану параметра $P_{ij}$, а $\underset{\sim}{T}^{e}_{ijs}$ $(s=\overline{1,r_j})$ – еталоні нечіткі числа (НЧ), $r_j$ – кількість членів в $\mathbf{T}^{\mathbf{e}}_{\mathbf{ij}}$. Сукупність конкретних величин

всіх членів підмножини $\mathbf{T_i^e}$ складають еталонне підсередовище ($\mathbf{T_i^e}$), яке орієнтоване на виявлення кібератаки з ІД $CA_i$.

Наприклад, при $n=5$ ($\mathbf{CA_1^{\tau_f} = CA_{SNF}^{\tau_f}}$ ($m_1=3$, $r_1=5$, $r_2=3$, $r_3=4$), $\mathbf{CA_2^{\tau_f}}$ = $\mathbf{CA_{DS}^{\tau_f}}$ ($m_2=3$, $r_1=5$, $r_2=r_3=3$), $\mathbf{CA_3^{\tau_f}} = \mathbf{CA_{SP}^{\tau_f}}$ ($m_3=2$, $r_1=5$, $r_2=3$), $\mathbf{CA_4^{\tau_f} = CA_{ESP}^{\tau_f}}$ ($m_4=3$, $r_1=4$, $r_2=r_3=3$) та $\mathbf{CA_5^{\tau_f} = CA_{SN}^{\tau_f}}$ ($m_5=2$, $r_1=5$, $r_2=3$)) визначимо

$$\{\bigcup_{\mathbf{i=1}}^{5}\mathbf{T_i^e}\} = \{\bigcup_{\mathbf{i=1}}^{5}\{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}}\mathbf{T_{ij}^e}\}\} = \{\bigcup_{i=1}^{5}\{\bigcup_{j=1}^{m_i}\{\bigcup_{s=1}^{r_j}\widetilde{T}_{ijs}^e\}\}\} =$$

$$\{\{\{\widetilde{T}^e_{SNFKBП1},\ \dots,\ \widetilde{T}^e_{SNFKBП5}\},\ \{\widetilde{T}^e_{SNFCOП1},\ \dots,\ \widetilde{T}^e_{SNFCOП3}\},\ \{\widetilde{T}^e_{SNFTП1},\ \dots,\ \widetilde{T}^e_{SNFTП4}\}\},$$

$$\{\{\widetilde{T}^e_{DSKOП1},\ \dots,\ \widetilde{T}^e_{DSKOП5}\},\ \{\widetilde{T}^e_{DSCO31},\ \dots,\ \widetilde{T}^e_{DSCO33}\},\ \{\widetilde{T}^e_{DS3M31},\ \dots,\ \widetilde{T}^e_{DS3M33}\}\},$$

$$\{\{\widetilde{T}^e_{SPKOП1},\ \dots,\ \widetilde{T}^e_{SPKOП5}\},\ \{\widetilde{T}^e_{SPKПOA1},\ \dots,\ \widetilde{T}^e_{SPKПOA3}\}\},$$

$$\{\{\widetilde{T}^e_{ESPKCБ1},\ \dots,\ \widetilde{T}^e_{ESPKCБ4}\},\ \{\widetilde{T}^e_{ESPKCT1},\ \dots,\ \widetilde{T}^e_{ESPKCT3}\},\ \{\widetilde{T}^e_{ESPKCC1},\ \dots,\ \widetilde{T}^e_{ESPKCC3}\}\},$$

$$\{\{\widetilde{T}^e_{SNKBK1},\ \dots,\ \widetilde{T}^e_{SNKBK5}\},\ \{\widetilde{T}^e_{SNBBK1},\ \dots,\ \widetilde{T}^e_{SNBBK3}\}\}\} =$$

$$\{\{\{\widetilde{QM}^e_{SNFKBП},\ \dots,\ \widetilde{QБ}^e_{SNFKBП}\},\ \{\widetilde{H}^e_{SNFCOП},\ \dots,\ \widetilde{B}^e_{SNFCOП}\},\ \{\widetilde{H}^e_{SNFTП},\ \dots,\ \widetilde{QB}^e_{SNFTП}\}\},$$

$$\{\{\widetilde{QM}^e_{DSKOП},\ \dots,\ \widetilde{QБ}^e_{DSKOП}\},\ \{\widetilde{H}^e_{DSCO3},\ \dots,\ \widetilde{B}^e_{DSCO3}\},\ \{\widetilde{M}^e_{DS3M3},\ \dots,\ \widetilde{Б}^e_{DS3M3}\}\},$$

$$\{\{\widetilde{QM}^e_{SPKOП},\ \widetilde{M}^e_{SPKOП},\ \widetilde{C}^e_{SPKOП},\ \widetilde{Б}^e_{SPKOП},\ \widetilde{QБ}^e_{SPKOП}\},\ \{\widetilde{M}^e_{SPKПOA},\ \widetilde{C}^e_{SPKПOA},\ \widetilde{Б}^e_{SPKПOA}\}\},$$

$$\{\{\widetilde{M}^e_{ESPKCБ},\ \dots,\ \widetilde{QБ}^e_{ESPKCБ}\},\ \{\widetilde{H}^e_{ESPKCT},\ \dots,\ \widetilde{B}^e_{ESPKCT}\},\ \{\widetilde{H}^e_{ESPKCC},\ \dots,\ \widetilde{B}^e_{ESPKCC}\}\},$$

$$\{\{\widetilde{QM}^e_{SNKBK},\ \dots,\ \widetilde{QБ}^e_{SNKBK}\},\ \{\widetilde{M}^e_{SNBBK},\ \dots,\ \widetilde{CT}^e_{SNBBK}\}\}\},$$

де, наприклад, $\widetilde{T}^e_{SPKOП1} = \widetilde{QM}^e_{SPKOП}$, …, $\widetilde{T}^e_{SPKOП5} = \widetilde{QБ}^e_{SPKOП}$ та $\widetilde{T}^e_{SPKПOA1} = \widetilde{M}^e_{SPKПOA}$, …, $\widetilde{T}^e_{SPKПOA3} = \widetilde{Б}^e_{SPKПOA}$ – є компонентами лінгвістичних еталонів, які відображають параметри $P_{SPKOП} = KOП$, $P_{SPKПOA} = KПOA$ та в сукупності визначають еталонне КОП-КПОА-підсередовище ($\mathbf{T_i^e = T_3^e = T_{SP}^e}$), за допомогою якого здійснюється виявлення кібератаки з ІД $CA_{SP}$ або *SP*-атаки.

**Формування** підмножини поточних значень нечітких параметрів $\mathbf{P_i^{\tau_f}}$ здійснюється за допомогою $\mathbf{T_i^e}$ в момент часу $\tau_f$. Тут отримаємо

$$\mathbf{P_i^{\tau_f}} = \{\bigcup_{j=1}^{m_i}\widetilde{P}_{ij}^{\tau_f}\} = \{\widetilde{P}_{i1}^{\tau_f},\ \dots,\ \widetilde{P}_{im_i}^{\tau_f}\},$$

де ($j=\overline{1,m_i}$), $m_i$ – кількість нечітких поточних параметрів, за станом аномальності яких здійснюється виявлення кібератак з ІД $CA_i$. Значення підмножини $\mathbf{P_i^{\tau_f}}$ визначають поточне підсередовище ($\mathbf{P_i^{\tau_f}}$) в загальному гетерогенному параметричному середовищі (**P**), породженого кібератакою з ІД $CA_i$ в момент часу $\tau_f$. Наприклад, при $n=1$ ($\mathbf{CA_{SP}^{\tau_f}}$ = $\mathbf{SP^{\tau_f}}$), $i=3$, $m_3=2$ визначимо $P_3^{\tau_f} = \{\bigcup_{j=1}^{2}\widetilde{P}_{3j}^{\tau_f}\} = \{\widetilde{P}_{SPKOП}^{\tau_f},\ \widetilde{P}_{SPKПOA}^{\tau_f}\}$, де, наприклад, $\widetilde{P}_{SPKOП}^{\tau_f}$ та $\widetilde{P}_{SPKПOA}^{\tau_f}$ – є нечіткими поточними значеннями, які відображають параметри

$P_{SPKOП} = KOП$ та $P_{SPKПОА} = KПОА$, тобто конкретні значення яких в сукупності складають поточне КОП-КПОА-підсередовище ( $\mathbf{P_i^{\tau_f} = P_3^{\tau_f} = P_{SP}^{\tau_f}}$ ), що використовується для виявлення аномального стану в *2*-вимірному параметричному підсередовищі ($\mathbf{P_i=P_3=P_{SP}}$), що породжено *SP*-атакою.

**Формування** підмножини базових детекційних правил $\mathbf{DR_i}$, що використовуються для виявлення *i*-ї кібератаки здійснюється на основі виразу

$$\{\bigcup_{i=1}^{n}\mathbf{DR_i}\}=\{\bigcup_{i=1}^{n}\{\bigcup_{a=1}^{w_i}\mathbf{DR_{ia}}\}\}=\{\{\mathbf{DR_{11}},\ \mathbf{DR_{12}},\ldots,\ \mathbf{DR_{1w_1}}\},\ \ldots,\ \{\mathbf{DR_{n1}},\ \mathbf{DR_{n2}},\ldots,\ \mathbf{DR_{nw_n}}\},$$

де $(i=\overline{1,n},\ a=\overline{1,w_i})$, $w_i$ – кількість базових детекційних правил, $\mathbf{DR_i}$ – множина всіх можливих правил утворюючих детекційне підсередовище ($\mathbf{DR_i}$), що використовується для виявлення кібератаки з ІД $CA_i$ в атакуючому середовищі ( $\mathbf{CA^{\tau_f}}$ ).

Наприклад, при $n=5$ ( $\mathbf{CA_{SNF}^{\tau_f}}$, $\mathbf{CA_{DS}^{\tau_f}}$, $\mathbf{CA_{SP}^{\tau_f}}$, $\mathbf{CA_{ESP}^{\tau_f}}$ та $\mathbf{CA_{SN}^{\tau_f}}$ ) та $w_1 = w_2 = w_3 = w_4 = w_5 = 5$ визначимо $\{\bigcup_{i=1}^{5}\mathbf{DR_i}\}=\{\mathbf{DR_1},...,\mathbf{DR_5}\}=\{\bigcup_{i=1}^{5}\{\bigcup_{a=1}^{w_i}\mathbf{DR_{ia}}\}\}=\{\{\mathbf{DR_{11}},\ldots,\mathbf{DR_{15}}\},$

$\{\mathbf{DR_{21}},\ \ldots,\ \mathbf{DR_{25}}\},\ \{\mathbf{DR_{31}},\ \ldots,\ \mathbf{DR_{35}}\},\ \{\mathbf{DR_{41}},\ \ldots,\ \mathbf{DR_{45}}\},\ \{\mathbf{DR_{51}},\ \ldots,\ \mathbf{DR_{55}}\}\}$,

де в сукупності всі елементи відповідних підмножин $\{\mathbf{DR_1},\ \ldots,\ \mathbf{DR_5}\}$ визначають детекційні середовища (**DR**), що містять безпосередні базові детекційні правила, які відповідно використовуються для виявлення *SNF*-, *DS*-, *SP*-, *ESP*- та *SN*-атак.

Таким чином, сформовані всі компоненти кортежу, що дозволяють визначати $m_i$-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 $n=1$ ( $m_3 = 2$, $r_1 = 5$, $r_2 = 3$ та $w_3 = 5$ ) на основі узагальнювального кортежу можна сформувати його часткове відображення в $\mathbf{CA_{SP}^{\tau_f}} = \mathbf{SP^{\tau_f}}$, тобто

$\mathbf{CA_3^{\tau_f}} = < CA_{SP},\ \mathbf{P_3},\ \mathbf{T_3^e},\ \mathbf{P_3^{\tau_f}},\ \mathbf{DR_3} >$ і отримаємо $\mathbf{CA_{SP}^{\tau_f}} = < CA_{SP},\ \{P_{SPKOП},\ P_{SPKПОА}\},$

$\{\{\underset{\sim}{T}^e_{SPKOП1},\ \underset{\sim}{T}^e_{SPKOП2},\ \underset{\sim}{T}^e_{SPKOП3},\ \underset{\sim}{T}^e_{SPKOП4},\ \underset{\sim}{T}^e_{SPKOП5}\},\ \{\underset{\sim}{T}^e_{SPKПОА1},\ \underset{\sim}{T}^e_{SPKПОА2},\ \underset{\sim}{T}^e_{SPKПОА3}\}\},$

$\{\underset{\sim}{P}^{\tau_f}_{SPKOП},\ \underset{\sim}{P}^{\tau_f}_{SPKПОА}\},\ \{\mathbf{DR_{31}},\ \mathbf{DR_{32}},\ \mathbf{DR_{33}},\ \mathbf{DR_{34}},\ \mathbf{DR_{35}}\} >$

За допомогою сформованого кортежу визначається стан аномальності в *m*-вимірному гетерогенному параметричному середовищі (**P**), яке утворюється не тільки атакуючим SP-середовищем ( $\mathbf{CA^{\tau_f}}$ ) в момент часу $\tau_f$, але і середовищами з іншими класами кібератак, для яких можна сформувати подібні кортежі.

На основі КМАС розроблено метод формування еталонних середовищ (МФЕС), який за рахунок використання множини ІД лінгвістичних оцінок та ІД 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, дозволить формалізувати процес отримання еталонних значень фіксованих параметрів заданих груп лінгвістичних змінних, що характеризує конкретне еталонне підсередовище. Метод МФЕС реалізується в 6 основних етапів.

**Етап 1 – визначення підмножини ІД лінгвістичних оцінок.** Будується підмножина ІД лінгвістичних оцінок

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

де $\mathbf{LE_{ij}}$ $(j=\overline{1,m_i})$ – підмножина ІД суджень експерта відносно значень параметрів $P_{ij}$, а $LE_{ijk}$ $(k=\overline{1,r_j})$ – $k$-й ідентифікатор лінгвістичної оцінки експерта відносно стану $j$-го параметра при $i$-й атаці на РІС, а $r_j$ – кількість ІД в $\mathbf{LE_{ij}}$. Наприклад, при $n=3$ (для кібератак з ІД $CA_{SN}$, $CA_{DS}$, $CA_{SP}$), $m_1=m_3=2$, $m_2=3$, $r_1=5$, $r_2=r_3=3$

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

$$\{\{\{LE_{SNKBK1},\ldots,LE_{SNKBK5}\},\{LE_{SNBBK1},\ldots,LE_{SNBBK3}\}\},\{\{LE_{DS\,KOП1},\ldots,LE_{DS\,KOП5}\},$$

$$\{LE_{DSCO31},\ldots,LE_{DSCO33}\},\{LE_{DS3M31},\ldots,LE_{DS3M33}\}\},\{\{LE_{SP\,KOП1},\ldots,LE_{SP\,KOП5}\},$$

$$\{LE_{SPKПOA1},\ldots,LE_{SPKПOA3}\}\}\}=$$

$$\{\{\{"ОМ",\ldots,"ОБ"\},\{"МЛ",\ldots,"СТ"\}\},\{\{"ОМ",\ldots,"ОБ"\},\{"Н",\ldots,"В"\},$$

$$\{"М",\ldots,"Б"\}\},\{\{"ОМ",\ldots,"ОБ"\},\{"М",\ldots,"Б"\}\}\}.$$

**Етап 2 – формування базової матриці частот.** З урахуванням сформованих підмножин ІД інтервалів $\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\mathbf{N_i}\}=\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}}\mathbf{N_{ij}}\}\}=\{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\{\bigcup_{k=1}^{r_j}N_{ijk}\}\}\}$, ($\mathbf{N_{ij}}$ $(j=\overline{1,m_i})$ – підмножина ІД інтервалів, на області визначення яких експерт здійснює лінгвістичне оцінювання відносно значень параметрів $P_{ij}$, а $N_{ijk}$ $(k=\overline{1,r_j})$ – ІД $k$-го інтервалу, що використовується для формування на ньому частот зустрічальності оцінок експерта за поточним станом $j$-го параметра відносно $i$-ї атаки на РІС, $r_j$ – кількість ІД фіксованих інтервалів) та $\mathbf{LE_{ij}}$ формується узагальнювальна таблиця оцінок, вміст якої ґрунтується на поточному фіксуванні суджень (оцінок) експерта, з використанням якої будується базова матриця частот $F_{ij}=\|f_{ijsq}\|$, $(s,q=\overline{1,r_j})$.

**Етап 3 – формування похідної матриці частот.** Створюється вектор сум за відповідними стовпцями матриці частот $VS_{ij}=\left\|\bigcup_{q=1}^{r_j}\sum_{s=1}^{r_j}f_{ijsq}\right\|$ серед членів $VS_{ij}$ знаходимо максимальне значення $vsm_{ij}=\bigvee_{q=1}^{r_j}vs_{ijq}$, що використовується для формування похідної матриці частот $F'_{ij}=\|f'_{ijsq}\|=(vsm_{ij}/vs_{ijq})\|f_{ijsq}\|$.

**Етап 4 – побудова нечітких термів.** Побудуємо підмножини нечітких термів

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\mathbf{T_i}\}=\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}}\mathbf{T_{ij}}\}\}=\{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\{\bigcup_{s=1}^{r_j}T_{jjs}\}\}\}=$$

$\{\{\{\underset{\sim}{T}_{i11},\ldots,\underset{\sim}{T}_{i1r_1}\},\ldots,\{\underset{\sim}{T}_{im_i1},\ldots,\underset{\sim}{T}_{im_ir_{m_i}}\}\},\ldots,\{\{\underset{\sim}{T}_{n11},\ldots,\underset{\sim}{T}_{n1r_1}\},\ldots,\{\underset{\sim}{T}_{nm_n1},\ldots,\underset{\sim}{T}_{nm_nr_{m_n}}\}\}\}$,

де $\mathbf{T_{ij}}$ $(j=\overline{1,m_i})$ – підмножина нечітких термів відносно значень параметрів $P_{ij}$, а $\underset{\sim}{T}_{ijs}$ $(s=\overline{1,r_j})$ – нечіткі терми, $r_j$ – кількість членів в $\mathbf{T_{ij}}$. Далі, для формування значень компонент $\underset{\sim}{T}_{ijs}$ за елементами $F_{ij}^{'}$ будується вектор максимумів $FM_{ij}=\left\| fm_{ijq} \right\|=$ $\left\| \bigcup_{q=1}^{r_j} \bigvee_{s=1}^{r_j} f_{ijsq}^{'} \right\|$ та формується матриця функцій належності (ФН) $M_{ij}=\left\| \mu_{ijsq} \right\|$, кожний елемент якої обчислюється за виразом $\mu_{ijsq}=f_{ijsq}^{'}/fm_{ijs}$. З урахуванням цього визначаються набори нечітких термів (чисел) $\underset{\sim}{T}_{ijs}=\{\bigcup_{q=1}^{r_j}\mu_{ijsq}/x_{ijsq}\}=\{\mu_{ijs1}/x_{ijs1},\mu_{ijs2}/x_{ijs2},\ldots,$ $\mu_{ijsr_j}/x_{ijsr_j}\}$, НЧ $\underset{\sim}{T}_{ijs}$ відповідно є інтерпретацією лінгвістичних висловлювань експертів $LE_{ijk}$).

**Етап 5 – побудова НЧ еталонного середовища ($T^e$).** Базується на підмножині нечітких еталонів $\mathbf{T_{ij}^e}$ сформованих в кортежній моделі та НЧ з $\mathbf{T_{ij}}$ і реалізується за допомогою кроків: Крок 1. Перетворення нечітких термів, 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. В кожному $\underset{\sim}{T}_{ijs}$ здійснюється поглинання компонент $0/x_{ijs}^{min}$, $0/x_{ijs}^{max}$ та визначається набір проміжних термів $\underset{\sim}{T}_{ijs}^{'}$ з урахуванням яких формується $\underset{\sim}{T}_{ijs}^{e}=\{\bigcup_{q=1}^{r_{js}}\mu_{ijsq}^{e}/x_{ijsq}^{e}\}=$ $\{\mu_{ijs1}^{e}/x_{ijs1}^{e},\mu_{ijs2}^{e}/x_{ijs2}^{e},\ldots,\mu_{ijsr_{js}-1}^{e}/x_{ijsr_{js}-1}^{e},\mu_{ijsr_{js}}^{e}/x_{ijsr_{js}}^{e}\}$ $(q=\overline{1,r_{js}})$.

**Етап 6 – візуалізація еталонних підсередовищ.** Побудова геометричного образу НЧ еталонних підсередовищ ($\mathbf{T_i^e}$), що належать підмножині $\mathbf{T_{ij}^e}$.

Геометричне місце точок на площині визначаються за допомогою ламаної з'єднуючої точки, що відображають компоненти НЧ $\underset{\sim}{T}_{ijs}^{e}$ в порядку зростання їх супортів $x_{ijsq}^{e}$. Візуалізація одного типового еталонного терму представлена у вигляді ламаної ⟵● на рис. 1. Також, базуючись на МФЕС розроблено метод формування еталонного підсередовища для виявлення сніфінг-атак та метод побудови еталонів лінгвістичних змінних для систем виявлення email-спуфінг-атак.

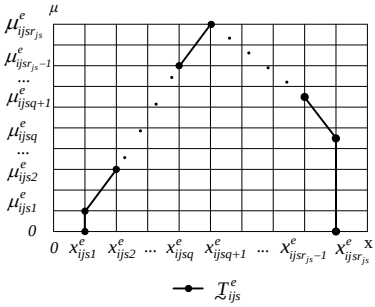


Рис. 1. НЧ $\underset{\sim}{T}_{ijs}^{e}$ еталонного підсередовища ($\mathbf{T_i^e}$)

Використання розробленої КМАС та МФЕС дозволить сформувати набір часткових кортежів, що відображають процес виявлення аномального стану в *m*-вимірному гетерогенному параметричному середовищі, що утворене відповідним атакуючим середовищем в заданий часовий проміжок та формалізувати процес отримання еталонних значень фіксованих параметрів заданих груп лінгвістичних змінних, що характеризують конкретне еталонне підсередовище.

**Третій розділ** присвячений розробці базових методів формування поточного середовища що складаються з методів: фазифікації параметрів, номіналізації НЧ, визначення ідентифікуючих термів. Метод фазифікації параметрів на еталонних підсередовищах (МФП), який за рахунок введених множин сенсорів, лічильників 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 параметрів *m*-вимірних поточних середовищ для їх подальшого застосування у виявленні аномального стану. Основу методу складають три базові етапи.

**Етап 1 – формування частот зустрічальності параметрів.** Вводяться підмножини сенсорів $\mathbf{S_{ij}}$, що використовуються для контролю поточного стану фізичних параметрів, які відображаються шляхом $\mathbf{P_i^{\tau_i}}$ в $\mathbf{CA_i^{\tau_i}}$.

$$\mathbf{S_{ij}} = \{\bigcup_{k=1}^{r_j} S_{ijk}(t_\eta)\} = \{S_{ij1}(t_\eta),\ S_{ij2}(t_\eta),\ \ldots,\ S_{ijr_j}(t_\eta)\},$$

$$(i=\overline{1,n},\ j=\overline{1,m_i},\ k=\overline{1,r_j}),$$

де, $S_{ijk}(t_\eta)$ – сенсор $N_{ijk}$-го інтервалу, який відображає значення $P_{ij}(t_\eta)$ в момент $t_\eta$, а $r_j$ – кількість сенсорів. Сенсор $S_{ijk}(t_\eta)$ є бінарною функцією $S_{ijk}(t_\eta) = \begin{cases} 1, при P_{ij}(t_\eta) \in N_{ijk} \\ 0, при P_{ij}(t_\eta) \notin N_{ijk}. \end{cases}$ Введемо підмножини лічильників сенсорів $\mathbf{CS_{ij}}$, які на основі даних сенсорів $S_{ijk}(t_\eta)$, формують частоти зустрічальності $P_{ij}(t_\eta)$ на кожному з інтервалів $N_{ijk}$ за допомогою $\mathbf{CS_{ij}} = \{\bigcup_{k=1}^{r_j} CS_{ijk}\} = \{\bigcup_{k=1}^{r_j}\sum_{\eta=1}^{\eta_{max}} S_{ijk}(t_\eta)\}$, де $CS_{ijk}$ – лічильник сенсора $S_{ijk}(t_\eta)$, а $\eta_{max}$ відповідає загальній кількості можливих $t_\eta$.

Зазначені частоти зустрічальності, що відображені лічильниками $CS_{ijk}$ представимо у вигляді таблиці 1, тобто кожний $CS_{ijk}$ лічильник відповідає за контроль стану відповідного параметра на інтервалі $N_{ijk}$.

Типова таблиця для $\mathbf{CS_{ij}}$ Таблиця 1

| Лічильник сенсора | $\mathbf{N_{ij}}$ $(k=\overline{1,r_j})$ | | | |
|---|---|---|---|---|
| | $N_{ij1}$ | $N_{ij2}$ | … | $N_{ijr_j}$ |
| $CS_{ij}$ | $CS_{ij1}$ | $CS_{ij2}$ | … | $CS_{ijr_j}$ |

**Етап 2 – формування поправкових еталонів.** Введемо підмножини поправкових еталонів $\mathbf{T_{ij}^E}$ (базуючись на $\mathbf{T_{ij}^e}$):

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

де $\underset{\sim}{T}^{E}_{ijs}$ $(s=\overline{1,r_j})$ – поправкові еталонні НЧ. Ці числа формуються на основі перетворення відповідних НЧ з підмножини $\mathbf{T^e_{ij}}$ за допомогою лічильників сенсорів із $\mathbf{CS_{ij}}$, відповідно до $\{\bigcup_{s=1}^{r_j}\underset{\sim}{T}^{E}_{ijs}\}=\{\bigcup_{s=1}^{r_j}(\underset{\sim}{T}^{e}_{ijs}\cdot CS_{ijs})\}=\{\underset{\sim}{T}^{e}_{ij1}\cdot CS_{ij1}, \underset{\sim}{T}^{e}_{ij2}\cdot CS_{ij2},\ldots, \underset{\sim}{T}^{e}_{ijr_j}\cdot CS_{ijr_j}\}$.

**Етап 3 – формування нечітких параметрів поточного середовища ( $\mathbf{P^{\tau_f}}$ ).** Реалізація цього етапу здійснюється відповідно до наступного виразу

$$\underset{\sim}{P}^{\tau_f}_{ij}=(\sum_{s=1}^{r_j}\underset{\sim}{T}^{E}_{ijs})/\eta_{max}=(\underset{\sim}{T}^{E}_{ij1}\overset{\sim}{+}\ldots\overset{\sim}{+}\underset{\sim}{T}^{E}_{ijr_j})/\eta_{max},$$

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

Маючи узагальнювальні описи процесу фазифікації поточних параметрів та еталонних середовищ ($\mathbf{T^e}$) для еквівалентного перетворення відповідних НЧ необхідно їх привести до однієї множини визначених $\alpha$-рівнів.

Розроблений метод $\alpha$-рівневої номіналізації НЧ (МАН), який за рахунок побудованого механізму формування множини $\alpha$-рівней, допоміжних підмножин $\alpha$-рівневих та міжточкових $\alpha$-рівневих інтервалів, а також процесу номіналізації та визначення значень необхідних супортів НЧ еталонних та поточних середовищ, дозволяє здійснити графічну інтерпретацію нечітких величин та визначати ідентифікуючі терми, що відображають поточні стани еталонних та поточних підсередовищ. Основу запропонованого методу складають три базові етапи.

**Етап 1 – формування $\alpha$-рівней.** Вводиться підмножина $\alpha$-рівней

$$\mathbf{AL_{ij}}=\{\bigcup_{k=1}^{\pi}AL_{ijk}\}=\{AL_{ij1}, AL_{ij2},\ldots, AL_{ij\pi}\}\ (k=\overline{1,\pi}),$$

що використовуються для перетворення НЧ, які відображають $\mathbf{P_{ij}}$, де $\pi$ – кількість членів у множині $\mathbf{AL_{ij}}$, а $AL_{ijk}$ – $k$-й член множини $\mathbf{AL_{ij}}$, що відповідає $k$-му $\alpha$-рівню. Всі члени множини $\mathbf{AL_{ij}}$ формуються за формулою $\mathbf{AL_{ij}}=\{\bigcup_{s=1}^{r}\{\bigcup_{q=1}^{r_s}\mu^{e}_{ijsq}\}\}$ та представляються у вигляді виразу $\mathbf{AL_{ij}}=\{\bigcup_{k=1}^{\pi}AL_{ijk}\}=\{\bigcup_{s=1}^{r}\{\bigcup_{q=1}^{r_s}\mu^{e}_{ijsq}\}\}$.

Наприклад, при $i=3$ $(CA_3=CA_{SP})$, $j=1$ $(P_{31}=P_{SPKOП})$, $r=5$, $s=\overline{1,5}$, $r_1=4$, $r_2=5$, $r_3=5$, $r_4=5$ та $r_5=4$ і при значенні $\mu^{e}_{31sq}$, що відповідає $\mu^{e}_{21sq}$, то підмножина $\mathbf{AL_{31}}$ приймає вигляд

$$\mathbf{AL_{31}}=\{\bigcup_{k=1}^{\pi}AL_{31k}\}=\{\bigcup_{s=1}^{r}\{\bigcup_{q=1}^{r_s}\mu^{e}_{31sq}\}\}=$$

$$\{\{\mu^{e}_{3111},\ldots,\mu^{e}_{3114}\},\{\mu^{e}_{3121},\ldots,\mu^{e}_{3125}\},\{\mu^{e}_{3131},\ldots,\mu^{e}_{3135}\},\{\mu^{e}_{3141},\ldots,\mu^{e}_{3145}\},\{\mu^{e}_{3151},\ldots,\mu^{e}_{3154}\}\}=$$

$$\{\{0;\ 1;\ 0{,}3;\ 0\},\ \{0;0{,}6;\ 1;0{,}2;0\},\ \{0;0{,}4;1;0{,}3;0\},\ \{0;0{,}6;1;0{,}7;0\},\{0;0{,}6;1;0\}\}=$$
$$\{0;0{,}2;0{,}3;0{,}4;\ 0{,}6;0{,}7;1\}.$$

В процесі формування членів $\mathbf{AL_{31}}$ визначається їх кількість, тобто $\pi = 7$, відповідно $\mathbf{AL_{31}} = \{\bigcup_{k=1}^{\pi} AL_{31k}\} = \{AL_{311}, \ldots, AL_{317}\} = \{AL_{SPKOП1}, \ldots, AL_{SPKOП7}\} = \{0;\ 0{,}2;\ 0{,}3;\ 0{,}4;\ 0{,}6;\ 0{,}7;\ 1\}$, де $AL_{311} = AL_{SPKOП1} = 0, \ldots, AL_{317} = AL_{SPKOП7} = 1$.

**Етап 2 – еквівалентне перетворення НЧ.** Приведемо всі НЧ еталонних та поточних середовищ ( $\mathbf{T^e}$ та $\mathbf{P^{\tau_f}}$ ) до номінального (одного для всіх) числа компонент за допомогою підмножин $\mathbf{AL_{ij}}$ (5 кроків).

Крок 1. Введемо множину всіх можливих перетворених або номіналізованих (приведених до $z$) НЧ еталонних середовищ ($\mathbf{T^e}$)

$$\mathbf{T_{ij}^{ep}} = \{\bigcup_{s=1}^{r} \underset{\sim}{T}_{ijs}^{ep}\} = \{\underset{\sim}{T}_{ij1}^{ep},\ \underset{\sim}{T}_{ij2}^{ep}, \ldots,\ \underset{\sim}{T}_{ijr}^{ep}\}$$

та отримане на їх основі перетворене $\underset{\sim}{P}_{ij}^{\tau_f p}$ $(s = \overline{1,r})$ НЧ поточних середовищ ( $\mathbf{P^{\tau_f}}$ ).

Сформуємо перетворене $\underset{\sim}{T}_{ijs}^{ep}$, $\underset{\sim}{P}_{ij}^{\tau_f p}$ НЧ еталонного та поточного середовища ( $\mathbf{T^e}$ та $\mathbf{P^{\tau_f}}$ ) $\underset{\sim}{T}_{ijs}^{ep} = \{\bigcup_{g=1}^{z} \mu_{ijsg}^{ep} / x_{ijsg}^{ep}\} = \{\mu_{ijs1}^{ep} / x_{ijs1}^{ep}, \ldots, \mu_{ijsz}^{ep} / x_{ijsz}^{ep}\}$, $(g = \overline{1,z})$, $(z = 2\pi\text{-}1)$ та

$$\underset{\sim}{P}_{ij}^{\tau_f p} = \{\bigcup_{g=1}^{z} \mu_{ijg}^{p} / x_{ijg}^{p}\} = \{\mu_{ij1}^{p} / x_{ij1}^{p},\ \mu_{ij2}^{p} / x_{ij2}^{p}, \ldots, \mu_{ijz}^{p} / x_{ijz}^{p}\},\ (g = \overline{1,z}),\ (z = 2\pi\text{-}1),$$

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 $\mu_{ijg}^{p} = \mu_{ij(z-g+1)}^{p} = AL_{ijg}$, $\mu_{ij1}^{p} = \mu_{ij1}$, $x_{ij1}^{p} = x_{ij1}$, $z$ – кількість компонент в $\underset{\sim}{P}_{ij}^{\tau_f p}$.

Число компонент всіх НЧ однакове та визначається параметром $z$, який назвемо номінальним числом компонент.

Крок 2. Номіналізація (перетворення до $z$) НЧ $\underset{\sim}{T}_{ijs}^{ep}$ еталонного середовища ($\mathbf{T^e}$) здійснюється за допомогою введення підмножини $\alpha$-рівневих інтервалів $\mathbf{AL_{ij}^{Ie}}$

$$\mathbf{AL_{ij}^{Ie}} = \{\bigcup_{s=1}^{r} \mathbf{AL_{ijs}^{Ie}}\} = \{\mathbf{AL_{ij1}^{Ie}}, \ldots, \mathbf{AL_{ijr}^{Ie}}\},\ \text{де}\ \mathbf{AL_{ijs}^{Ie}} = \{\bigcup_{b=1}^{r_s-1} \mathbf{AL_{ijsb}^{Ie}}\} = \{\mathbf{AL_{ijs1}^{Ie}}, \ldots, \mathbf{AL_{ijsr_s-1}^{Ie}}\},$$

а $\mathbf{AL_{ijs}^{Ie}} \subseteq \mathbf{AL_{ij}^{Ie}}$ та $r_s$ $(s = \overline{1,r})$ визнає кількість компонент в $\underset{\sim}{T}_{ijs}^{e}$, з урахуванням цього

$$\mathbf{AL_{ij}^{Ie}} = \{\bigcup_{s=1}^{r} \mathbf{AL_{ijs}^{Ie}}\} = \{\bigcup_{s=1}^{r} \{\bigcup_{b=1}^{r_s-1} \mathbf{AL_{ijsb}^{Ie}}\}\} =$$

$$\{\{\mathbf{AL_{ij11}^{Ie}},\ \mathbf{AL_{ij12}^{Ie}}, \ldots, \mathbf{AL_{ij1\,r_1-1}^{Ie}}\},\ \{\mathbf{AL_{ij21}^{Ie}},\ \mathbf{AL_{ij22}^{Ie}}, \ldots, \mathbf{AL_{ij2\,r_2-1}^{Ie}}\}, \ldots,$$
$$\{\mathbf{AL_{ijs1}^{Ie}},\ \mathbf{AL_{ijs2}^{Ie}}, \ldots, \mathbf{AL_{ijr\,r_r-1}^{Ie}}\}\},$$

$\mathbf{AL_{ijsb}^{Ie}} \subseteq \mathbf{AL_{ijs}^{Ie}}$ – підмножина міжточкових $\alpha$-рівневих інтервалів, представляється як

$$\mathbf{AL^{Ie}_{ijsb}} = \{\bigcup_{c=1}^{k_b} AL^{Ie}_{ijsbc}\} = \{AL^{Ie}_{ijsb1},\ AL^{Ie}_{ijsb2},\ \ldots,\ AL^{Ie}_{ijsbk_b}\},\ (b=\overline{1,r_s-1}),$$

де $k_b$ – кількість членів в $\mathbf{AL^{Ie}_{ijsb}}$, значення кожного з яких знаходиться на інтервалі між двома точками $\mu^e_{ijsq}$ та $\mu^e_{ijsq+1}$, тобто для всіх $\mathbf{AL^{Ie}_{ijsb}}$ виконується умова:

$$\begin{cases} \mu^e_{ijsq} < AL^{Ie}_{ijsbc} \le \mu^e_{ijsq+1},\ при\ x^e_{ijsq+1} \le x^e_{ijsmax} \\ \mu^e_{ijsq} > AL^{Ie}_{ijsbc} \ge \mu^e_{ijsq+1},\ при\ x^e_{ijsq+1} \ge x^e_{ijsmax} \end{cases} (c=\overline{1,k_b}),\ (q=\overline{1,r_s}),$$

де $x^e_{ijsmax}$ – носій НЧ $\underset{\sim}{T}^e_{ijs}$, значення ФН якого визначається $\mu^e_{ijsmax} = \bigvee_{q=1}^{r_s} \mu^e_{ijsq}$. При супорті $x^e_{ijsmax}$ в НЧ $\underset{\sim}{T}^e_{ijs}$, міститься максимальне значення ФН $\mu^e_{ijsmax}$ тобто існує компонент $\mu^e_{ijsmax} / x^e_{ijsmax}$.

Далі, з урахуванням $\mathbf{AL^{Ie}_{ijsb}}$ представимо $\mathbf{AL^{Ie}_{ij}}$ в наступному вигляді:

$$\mathbf{AL^{Ie}_{ij}} = \{\bigcup_{s=1}^{r} AL^{Ie}_{ijs}\} = \{\bigcup_{s=1}^{r}\{\bigcup_{b=1}^{r_s-1}\{\bigcup_{c=1}^{k_b} AL^{Ie}_{ijsbc}\}\}\} =$$

$$\{\{\{AL^{Ie}_{ij111},\ AL^{Ie}_{ij112},\ \ldots,\ AL^{Ie}_{ij11k_1}\},\ \ldots,\ \{AL^{Ie}_{ij1(r_1-1)1},\ AL^{Ie}_{ij1(r_1-1)2},\ \ldots,\ AL^{Ie}_{ij1(r_1-1)k_{r_1-1}}\}\},\ldots,$$

$$\{\{AL^{Ie}_{ijr11},\ AL^{Ie}_{ijr12},\ \ldots,\ AL^{Ie}_{ijr1k_1}\},\ \ldots,\ \{AL^{Ie}_{ijr(r_r-1)1},\ AL^{Ie}_{ijr(r_r-1)2},\ \ldots,\ AL^{Ie}_{ijr(r_r-1)k_{r_r-1}}\}\}\}.$$

Крок 3. Формування перетвореного (номіналізованого) $\underset{\sim}{P}^{\tau_f p}_{ij}$ НЧ поточного середовища ($\mathbf{P^{\tau_f}}$) за аналогією з $\mathbf{AL^{Ie}_{ijsb}}$ здійснюється за допомогою множини міжточкових $\alpha$-рівневих інтервалів $\mathbf{AL^{Ip}_{ijb}} = \{\bigcup_{c=1}^{k_b} AL^{Ip}_{ijbc}\} = \{AL^{Ip}_{ijb1},\ AL^{Ip}_{ijb2},\ \ldots,\ AL^{Ip}_{ijbk_b}\},\ (b=\overline{1,\rho-1}),$

де $\rho$ – кількість компонент в $\underset{\sim}{P}^{\tau_f p}_{ij}$ НЧ поточного середовища ($\mathbf{P^{\tau_f}}$), $k_b$ – кількість членів в підмножині $\mathbf{AL^{Ip}_{ijb}}$, значення кожного з яких знаходиться між двома точками $\mu_{ijq}$ та $\mu_{ijq+1}$, тобто для всіх членів $\mathbf{AL^{Ip}_{ijb}}$ виконується умова:

$$\begin{cases} \mu_{ijq} < AL^{Ip}_{ijbc} \le \mu_{ijq+1},\ при\ x_{ijq+1} \le x_{ijmax} \\ \mu_{ijq} > AL^{Ip}_{ijbc} \ge \mu_{ijq+1},\ при\ x_{ijq+1} \ge x_{ijmax} \end{cases} (c=\overline{1,k_b}),\ (q=\overline{1,\rho}),$$

де $x_{ijmax}$ – носій НЧ $\underset{\sim}{P}^{\tau_f}_{ij}$, значення ФН якого визначається за $\mu_{ijmax} = \bigvee_{q=1}^{\rho} \mu_{ijq}$, тобто супорт $x_{ijmax}$ в НЧ $\underset{\sim}{P}^{\tau_f}_{ij}$ містить максимальне значення ФН $\mu_{ijmax}$.

Далі, за аналогією з $\mathbf{AL^{Ie}_{ij}}$ та з урахуванням $\mathbf{AL^{Ip}_{ijb}}$, сформуємо

$$\mathbf{AL^{Ip}_{ij}} = \{\bigcup_{b=1}^{\rho-1}\{\bigcup_{c=1}^{k_b} AL^{Ip}_{ijbc}\}\} = \{\{AL^{Ip}_{ij11},\ \ldots,\ AL^{Ip}_{ij1k_1}\},\ \ldots,\ \{AL^{Ip}_{ij(\rho-1)1},\ \ldots,\ AL^{Ip}_{ij(\rho-1)k_{\rho-1}}\}\}.$$

Крок 4. Обчислення значень $x^{ep}_{ijsg}$, $(g=\overline{1,z})$ для номіналізованих НЧ еталонного середовища ($\mathbf{T^e}$) здійснюється за допомогою $x^{ep}_{ijsg}=x^{e}_{ijsq}+((\mu^{ep}_{ijsg}-\mu^{e}_{ijsq})(x^{e}_{ijsq+1}-x^{e}_{ijsq}))/(\mu^{e}_{ijsq+1}-\mu^{e}_{ijsq})$, $(g=\overline{2,z})$, при цьому $\mu^{ep}_{ijs1}=\mu^{e}_{ijs1}$, $x^{ep}_{ijs1}=x^{e}_{ijs1}$, а $\mu^{ep}_{ijs1}=AL^{Ie}_{ijs11}$, $\mu^{ep}_{ijs2}=AL^{Ie}_{ijs12}$, …, $\mu^{ep}_{ijsk_1}=AL^{Ie}_{ijs1k_1}$,…, $\mu^{ep}_{ijs(k_1+k_2+k_3+...+k_{b-1}+1)}=AL^{Ie}_{ijr(r_s-1)1}$, $\mu^{ep}_{ijs(k_1+k_2+k_3+...+k_{b-1}+2)}=AL^{Ie}_{ijr(r_s-1)2}$,…,$\mu^{ep}_{ijsz}=AL^{Ie}_{ijr(r_s-1)k_b}$, де $z=\sum_{h=1}^{b}k_h$. Крок 5. Обчислення значень $x^{p}_{ijg}$, $(g=\overline{1,z})$ для номіналізованих НЧ поточного середовища ($\mathbf{P^{\tau_f}}$) здійснюється відповідно до кроку 4 за виразом $x^{p}_{ijg}=x_{ijq}+((\mu^{p}_{ijg}-\mu_{ijq})(x_{ijq+1}-x_{ijq}))/(\mu_{ijq+1}-\mu_{ijq})$, $(g=\overline{2,z})$, при цьому $\mu^{p}_{ij1}=\mu_{ij1}$, $x^{p}_{ij1}=x_{ij1}$, а $\mu^{p}_{ij1}=AL^{Ip}_{ij11}$, $\mu^{p}_{ij2}=AL^{Ip}_{ij12}$, …, $\mu^{p}_{ijk_1}=AL^{Ip}_{ij1k_1}$, …, $\mu^{p}_{ij(k_1+k_2+k_3+...+k_{b-1}+1)}=AL^{Ip}_{ij(\rho-1)1}$, $\mu^{p}_{ij(k_1+k_2+k_3+...+k_{b-1}+2)}=AL^{Ip}_{ij(\rho-1)2}$,...,$AL^{Ip}_{ij(\rho-1)k_b}$, де $z=\sum_{h=1}^{b}k_h$.

**Етап 3 – формування узагальнювальних таблиць та графічна інтерпретація номіналізованих НЧ еталонних та поточних підсередовищ.** Всі номіналізовані $\underset{\sim}{T}^{ep}_{ijs}$ та $\underset{\sim}{P}^{\tau_f p}_{ij}$ НЧ еталонного та поточного підсередовища ($\mathbf{T^e_i}$ та $\mathbf{P^{\tau_f}_i}$) зводяться до узагальнювальних таблиць 2-3. Графічна інтерпретація номіналізованих НЧ базується на побудові геометричного образу $\alpha$-рівней $\mathbf{AL_{ij}}$, а також всіх $\underset{\sim}{T}^{ep}_{ijs}$, $\underset{\sim}{P}^{\tau_f p}_{ij}$ НЧ.

Узагальнювальна таблиця для $\underset{\sim}{T}^{ep}_{ijs}$ Таблиця 2

| | $\mu^{ep}_{ijsg}$ $(g=\overline{1,z})$ | | | | | | |
|---|---|---|---|---|---|---|---|
| $\underset{\sim}{T}^{ep}_{ijs}$ | $\mu^{ep}_{ijs1}$ | .. | $\mu^{ep}_{ijsg-1}$ | $\mu^{ep}_{ijsg}$ | $\mu^{ep}_{ijsg+1}$ | .. | $\mu^{ep}_{ijsz}$ |
| | $AL_{ij1}$ | .. | $AL_{ij\pi-1}$ | $AL_{ij\pi}$ | $AL_{ij\pi-1}$ | .. | $AL_{ij1}$ |
| $\underset{\sim}{T}^{ep}_{ij1}$ | $x^{ep}_{ij11}$ | .. | $x^{ep}_{ij1g-1}$ | $x^{ep}_{ij1g}$ | $x^{ep}_{ij1g+1}$ | .. | $x^{ep}_{ij1z}$ |
| … | … | .. | … | … | … | .. | … |
| $\underset{\sim}{T}^{ep}_{ijr}$ | $x^{ep}_{ijr1}$ | .. | $x^{ep}_{ijrg-1}$ | $x^{ep}_{ijrg}$ | $x^{ep}_{ijrg+1}$ | .. | $x^{ep}_{ijrz}$ |

Узагальнювальна таблиця для $\underset{\sim}{P}^{\tau_f p}_{ij}$ Таблиця 3

| | $\mu^{p}_{ijg}$ $(g=\overline{1,z})$ | | | | | | |
|---|---|---|---|---|---|---|---|
| $\underset{\sim}{P}^{\tau_f p}_{ij}$ | $\mu^{p}_{ij1}$ | .. | $\mu^{p}_{ijg-1}$ | $\mu^{p}_{ijg}$ | $\mu^{p}_{ijg+1}$ | .. | $\mu^{p}_{ijz}$ |
| | $AL_{ij1}$ | .. | $AL_{ij\pi-1}$ | $AL_{ij\pi}$ | $AL_{ij\pi-1}$ | .. | $AL_{ij1}$ |
| $\underset{\sim}{P}^{\tau_f p}_{ij}$ | $x^{p}_{ij1}$ | .. | $x^{p}_{ijg-1}$ | $x^{p}_{ijg}$ | $x^{p}_{ijg+1}$ | .. | $x^{p}_{ij\,z}$ |

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. 2.

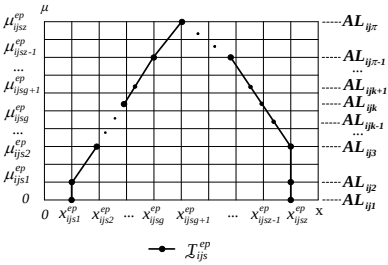


Рис. 2. Узагальнювальна графічна інтерпретація перетворених НЧ

Для подальшого виявлення аномалій в ІС необхідно визначити, ідентифікуючий терм, тобто таке еталонне НЧ, яке найближче знаходиться до поточного НЧ, і яке буде свідчити про рівень аномального стану в ІС.

Для цього розроблено метод визначення ідентифікуючих термів (МВІТ), 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. Базовий механізм МІДТ базується на трьох етапах.

**Етап 1 – формування множини ознак.** Для знаходження ідентифікуючого терму введемо множину характерних ознак (ХО) $\mathbf{XP_{ij}}$ методів порівняння ФН (МПФН)

$$\mathbf{XP_{ij}} = \{\bigcup_{\mathbf{c=1}}^{\mathbf{d}} \mathbf{XP_{ij}^{c}}\} = \{\mathbf{XP_{ij}^{1}}, \mathbf{XP_{ij}^{2}}, \ldots, \mathbf{XP_{ij}^{d}}\}, \ (c = \overline{1,d}),$$

а $d$ – підмножина ознак, а кожний член множини $\mathbf{XP_{ij}}$ відображає можливі ХО, які сформовані за допомогою множини МПФН, тобто $\mathbf{МПФН} = \{\bigcup_{c=1}^{d} МПФН_c\} = \{МПФН_1, МПФН_2, \ldots, МПФН_d\}$, де фактично $d$ – кількість використаних МПФН. Вміст кожної підмножини $\mathbf{XP_{ij}^{c}}$ формується за допомогою відповідного $МПФН_c$. Наприклад, при $d = 8$ множина $\mathbf{XP_{ij}}$ приймає вигляд $\mathbf{XP_{ij}} = \{\bigcup_{\mathbf{c=1}}^{\mathbf{8}} \mathbf{XP_{ij}^{c}}\} = \{\mathbf{XP_{ij}^{1}, \ldots, XP_{ij}^{8}}\}$. Кількість підмножин ХО пов'язано з кількістю використаних МПФН: $\mathbf{МСФП} = \{\bigcup_{c=1}^{8} МПФН_c\} = \{МПФН_1, \ldots, МПФН_8\} = \{BX, \ldots, MM\}$, де кожний член $\mathbf{XP_{ij}^{c}}$ формується за допомогою відповідного $МПФН_c$.

**Етап 2 – визначення підмножини ознак.** Етап пов'язаний з формуванням членів підмножин ХО: $\mathbf{XP_{ij}^{c}} = \{\bigcup_{s=1}^{r_j} XP_{ijs}^{c}\} = \{XP_{ij1}^{c}, XP_{ij2}^{c}, \ldots, XP_{ijr_j}^{c}\}$, $(s = \overline{1,r_j})$, де кожний член $XP_{ijs}^{c}$ підмножини $\mathbf{XP_{ij}^{c}}$ формується за допомогою $МПФН_c$, а відносно $c$ визначається номер способу реалізації етапу 1.

Наприклад, при $c = 1$ члени підмножини $\mathbf{XP_{ij}^{1}}$ формуються першим способом.

Спосіб 1. Використовуємо $МПФН_1 = BX$ із множини $\mathbf{МСФП}$, тобто

$$XP_{ijs}^{1} = h\ (\underset{\sim}{T}_{ijs}^{ep}, \underset{\sim}{P}_{ij}^{\tau_f p}) = \sum_{g=1}^{z} \left| x_{ijsg}^{ep} - x_{ijg}^{p} \right| = | x_{ijs1}^{ep} - x_{ij1}^{p} | + | x_{ijs2}^{ep} - x_{ij2}^{p} | + \ldots + | x_{ijsz}^{ep} - x_{ijz}^{p} |,$$

де $x_{ijsg}^{ep}$ та $x_{ijg}^{p}$ – супорти (носії) перетвореного $\underset{\sim}{T}_{ijs}^{ep}$ та $\underset{\sim}{P}_{ij}^{\tau_f p}$ НЧ, $z$ – кількість компонент в $\underset{\sim}{T}_{ijs}^{ep}$ та $\underset{\sim}{P}_{ij}^{\tau_f p}$, $(g = \overline{1,z})$, $(z = 2\pi\text{-}1)$.

Наприклад (етап 2, спосіб 1), для $i = 3$ $(CA_3 = CA_{SP})$ і якщо $j = 1$ $(P_{31} = P_{SPKOП})$, $r_1 = 5$, $g = \overline{1,13}$, $\underset{\sim}{T}_{ijs}^{ep} = \underset{\sim}{T}_{31s}^{ep}$, $\underset{\sim}{P}_{31}^{\tau_f p} = \underset{\sim}{P}_{SPKOП}^{\tau_f p}$ та $j = 2$ $(P_{32} = P_{SPKПОА})$, $r_2 = 3$, $g = \overline{1,9}$, $\underset{\sim}{T}_{ijs}^{ep} = \underset{\sim}{T}_{32s}^{ep}$, $\underset{\sim}{P}_{32}^{\tau_f p} = \underset{\sim}{P}_{SPKПОА}^{\tau_f p}$, то отримаємо підмножину можливих $\mathbf{XP_{31}^{1}} = \{\bigcup_{s=1}^{5} XP_{31s}^{1}\} = \{XP_{311}^{1}, \ldots, XP_{315}^{1}\} = \{h\ (\underset{\sim}{T}_{311}^{ep}, \underset{\sim}{P}_{31}^{\tau_f p}), \ldots, h\ (\underset{\sim}{T}_{315}^{ep}, \underset{\sim}{P}_{31}^{\tau_f p})\} = \{3{,}119;\ 2{,}441;\ 0{,}981;$

*3,624; 5,464 }* та $\mathbf{XP^1_{32}} = \{\bigcup_{s=1}^{3} XP^1_{32s}\} = \{XP^1_{321}, ..., XP^1_{323}\} = \{h(\underset{\sim}{T}^{ep}_{321}, \underset{\sim}{P}^{\tau_f p}_{32}), ..., h(\underset{\sim}{T}^{ep}_{323}, \underset{\sim}{P}^{\tau_f p}_{32})\} =$ *{4,093;1,267;0,443}*.

**Етап 3 – визначення номеру ідентифікуючого терму.** Введемо підмножину номерів ІД термів $\mathbf{NUM_i}$,

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{NUM_i}\} = \{\bigcup_{i=1}^{n} \{\bigcup_{j=1}^{m_i} NUM_{ij}\}\} =$$

$$\{\{NUM_{11}, \ldots, NUM_{1m_1}\}, \ldots, \{NUM_{n1}, \ldots, NUM_{nm_n}\},$$

де $m_i$ – кількість номерів ІД термів, $(i = \overline{1,n},\ j = \overline{1,m_i})$. Далі, виконання цього етапу здійснюється за допомогою функції пошуку ІД ХО та її номеру, тобто такої ІД ознаки $IX^c_{ijNUM_{ij}}$, відповідно до якої певній функції (визначається за $c$) буде присвоєно одне із значень $XP^c_{ijs}$ $(s = \overline{1,r_j})$. При цьому $NUM_{ij} = s$. Фактично за номером (поточним значенням $s$) ІД ХО можливо визначити відповідний ІД терм в підмножині $\mathbf{T^e_{ij}}$. Таким чином, пошук $IX^c_{ijNUM_{ij}} = XP^c_{ijs}$ здійснюється за допомогою узгодженої з МПФН $F^c$ $\mathbf{(XP^c_{ij})}$, тобто: $IX^c_{ijNUM_{ij}} = F^c(\bigcup_{s=1}^{r_j} XP^c_{ijs}) = F^c_{ij}\ (XP^c_{ij1},\ XP^c_{ij2}, \ldots,\ XP^c_{ijr_j})$, $(s = \overline{1,r_j})$, а за $c$ визначається номер способу реалізації етапу 3 (який також пов'язаний з номером способу реалізації етапу 2). Наприклад, при $c = 1$ застосовується перший спосіб пошуку номера ІД терма, який пов'язаний з $МПФН_1 = BX$ та складається з наступних кроків.

Спосіб 1. Крок 1. Визначення ІД ознаки $IX^1_{ijNUM_{ij}}$ здійснюється за допомогою узгодженої з ВХ функції $F^1$ $\mathbf{(XP^1_{ij})}$, що виконує пошук мінімального значення з членів підмножини $\mathbf{XP^c_{ij}}$ відповідно до виразу: $IX^1_{ijNUM_{ij}} = F^1(\bigcup_{s=1}^{r_j} XP^1_{ijs}) = F^1_{ij}\ (XP^1_{ij1}, \ldots,\ XP^1_{ijr_j})$ або $IX^1_{ijNUM_{ij}} = \bigwedge_{s=1}^{r_j} XP^1_{ijs} = XP^1_{ij1} \wedge \ldots \wedge XP^1_{ijr_j}$, $(s = \overline{1,r_j})$. Крок 2. Визначення ІД терма в $\mathbf{T^e_{ij}}$ 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.

Приклад, етапу 3 (спосіб 1) для $i = 3$ $(CA_3 = CA_{SP})$ при $j = 1$ $(P_{31} = P_{SPKOII})$, $r_1 = 5$, $XP^1_{ijs} = XP^1_{31s}$ та якщо $j = 2$ $(P_{32} = P_{SPKIIOA})$, $r_2 = 3$, $XP^1_{ijs} = XP^1_{32s}$.

Наприклад, Крок 1. Визначення $IX^1_{31NUM_{31}}$ і $IX^1_{32NUM_{32}}$ здійснюється за допомогою функції $F^1$ $\mathbf{(XP^1_{31})}$ та $F^1$ $\mathbf{(XP^1_{32})}$, яка здійснює пошук мінімального значення

$IX^{1}_{31NUM_{31}}=\bigwedge_{s=1}^{5} XP^{1}_{31s}=XP^{1}_{311}\wedge...\wedge XP^{1}_{315}=3{,}119\wedge 2{,}441\wedge 0{,}981\wedge 3{,}624\wedge 5{,}464=XP^{1}_{313}=$

$0{,}981$ та $IX^{1}_{32NUM_{32}}=\bigwedge_{s=1}^{3} XP^{1}_{32s}=XP^{1}_{321}\wedge...\wedge XP^{1}_{323}=4{,}093\wedge 1{,}267\wedge 0{,}443=XP^{1}_{323}=0{,}443.$

Крок 2. Визначення ІД терму в $\mathbf{T^{e}_{31}}$ здійснюється на основі того, що $IX^{1}_{31NUM_{31}}=XP^{1}_{31s}=XP^{1}_{313}$, а $NUM_{31}=s=3$. Тоді ІД буде терм $\underset{\sim}{T}^{e}_{313}$, у якого значення $s=3$, яке відповідає номеру мінімального значення ІД 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 ІД буде терм $\underset{\sim}{T}^{e}_{323}$. А ІД в $\mathbf{T^{e}_{31}}$ буде терм $\underset{\sim}{T}^{e}_{313}=\underset{\sim}{C}^{e}_{31}$, а відповідне йому перетворене еталонне $\underset{\sim}{T}^{ep}_{313}=\underset{\sim}{C}^{ep}_{SPKOII3}=\underset{\sim}{C}^{ep}_{31}$. Обчислення показують, що $XP^{1}_{313}=0{,}981$, відповідно перетворене НЧ $\underset{\sim}{P}^{\tau_f p}_{31}=\underset{\sim}{P}^{\tau_f p}_{SPKOII}$ поточного підсередовища ($\mathbf{P_i^{\tau_f}=P_3^{\tau_f}=P_{SP}^{\tau_f}}$) найближче розташоване до перетвореного НЧ $\underset{\sim}{T}^{ep}_{313}=\underset{\sim}{C}^{ep}_{31}$ еталонного підсередовища ($\mathbf{T_i^{e}=T_3^{e}=T_{SP}^{e}}$). А оскільки $\underset{\sim}{P}^{\tau_f p}_{SPKOII}$ та $\underset{\sim}{C}^{ep}_{31}$ є відображенням $\underset{\sim}{P}^{\tau_f p}_{SPKOII}$ та $\underset{\sim}{C}^{e}_{31}$, то $\underset{\sim}{P}^{\tau_f p}_{SPKOII}$ найближче розташоване до НЧ $\underset{\sim}{C}^{e}_{31}$ еталонного підсередовища ($\mathbf{T_i^{e}=T_3^{e}=T_{SP}^{e}}$). Аналогічно, ІД в $\mathbf{T^{e}_{32}}$ є значення $\underset{\sim}{T}^{e}_{323}=\underset{\sim}{E}^{e}_{32}$ та $XP^{1}_{323}=0{,}443$, то перетворене НЧ $\underset{\sim}{P}^{\tau_f p}_{32}=\underset{\sim}{P}^{\tau_f p}_{SPKIIOA}$ поточного підсередовища ($\mathbf{P_i^{\tau_f}=P_3^{\tau_f}=P_{SP}^{\tau_f}}$) найближче до перетвореного НЧ $\underset{\sim}{T}^{ep}_{323}=\underset{\sim}{E}^{ep}_{32}$ еталонного підсередовища ($\mathbf{T_i^{e}=T_3^{e}=T_{SP}^{e}}$). І відповідно, $\underset{\sim}{P}^{\tau_f p}_{SPKIIOA}$ є найближчим до $\underset{\sim}{E}^{e}_{32}$.

Використання МФП, МАН, МВІТ дозволило формалізувати процес перетворення в нечітку форму поточних значень параметрів *m*-вимірних поточних середовищ, визначати ідентифікуючі терми, що відображають стан еталонних та поточних підсередовищ та за допомогою еталонного середовища здійснити пошук ідентифікуючих перетворених еталонних термів, для визначення рівней аномальних станів.

**Четвертий розділ** присвячений розробці методів: дефазифікації параметрів, формування детекційного середовища та методології побудови систем виявлення аномалій.

Розроблено метод дефазифікації параметрів детекційного середовища, який за рахунок процедури визначення допоміжного терма, експертних коефіцієнтів (ЕК) параметрів та ЕК кібератаки, що характеризують експертні лінгвістичні оцінки, пов'язані з рівнем аномального стану в поточному середовищі, дозволяє у числовій формі відобразити рівень упевненості експерта відносно його суджень щодо можливих кібератак. Базовий механізм МДП ґрунтується на трьох етапах:

**Етап 1 – визначення допоміжного терма.** Визначається допоміжний терм, який слідує за ідентифікуючим, тобто наступний за близькістю розташування до поточного значення $\underset{\sim}{P}^{\tau_f p}_{j}$. Далі, за допомогою функції пошуку ідентифікуючої ХО, тобто ознаки $IX^{c}_{ijNUM_{ij}}$, якій відповідно до функції, наприклад, $F^{1}$ $\mathbf{(XP^{1}_{ij})}$ буде здійснено пошук додаткового терма, що слідує за ідентифікуючим $XP^{1}_{ijs}$. Введемо підмножину всіх номерів

допоміжних термів $\mathbf{NUM'_i} = \{\bigcup_{j=1}^{m_i} NUM'_{ij}\} = \{NUM'_{i1},\ NUM'_{i2},\ ...,\ NUM'_{im_i}\},\ (j = \overline{1,m_i})$,

де $m_i$ – кількість номерів допоміжних термів, а кожне $NUM'_{ij}$ представимо у вигляді

$NUM'_{ij} = \begin{cases} s-1,\ якщо\ (s = r_j) \vee (XP^1_{ijs-1} \le XP^1_{ijs+1}) \\ s+1,\ якщо\ (s = 1) \vee (XP^1_{ijs-1} > XP^1_{ijs+1}) \end{cases}$. Наприклад, якщо $i = 3$ (для кібератаки з ІД $CA_3 = CA_{SP} = SP$), $m_3 = 2$, $r_1 = 5$, $r_2 = 3$, то для $NUM'_{31}$ і $NUM'_{32}$ виконується перша умова, тобто $NUM'_{31} = 2$ і $NUM'_{32} = 2$. 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, а для $\mathbf{T^e_{32}}$ буде терм з $XP^1_{322} = 1{,}267$, тобто $\underset{\sim}{T}^e_{322}$.

**Етап 2 – визначення ЕК параметрів.** Введемо підмножину ЕК

$$\mathbf{EC_i} = \{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}} \mathbf{EC_{ij}}\} = \{EC^{min}_{ij}, EC^{max}_{ij}\},\ (j = \overline{1,m_i}),$$

при цьому $\mathbf{EC_i} \in \{EC^{min}_{ij}, EC^{max}_{ij}\}$, а $EC^{min}_{ij}$ і $EC^{max}_{ij}$ відповідно є мінімальними і максимальними елементами $(EC^{min}_{ij} \le EC^{max}_{ij})$ підмножини $\mathbf{EC_i}$.

Наприклад, якщо $i = 3$ $(CA_3 = CA_{SP} = SP)$, $m_3 = 2$, $r_1 = 5$, $r_2 = 3$ та з використанням ідентифікуючої ознаки $IX^1_{ijNUM_{ij}} = XP^1_{ijs}$ і допоміжними термами $XP^1_{312}$ та $XP^1_{322}$ розрахуємо нормуючі коефіцієнти за виразом $k_{ij} = 1/(IX^1_{ijNUM_{ij}} + IX^1_{ijNUM'_{ij}})$ та отримаємо $k_{31} = 0{,}292$ і $k_{32} = 0{,}585$. Далі, за виразом $EC^{max}_{ij} = 1 - k_{ij} \cdot IX^1_{ijNUM_{ij}}$ та $EC^{min}_{ij} = 1 - k_{ij} \cdot IX^1_{ijNUM_{ij}}$ обчислимо значення $EC^{max}_{31} = 0{,}713$ та $EC^{max}_{32} = 0{,}741$ які будуть відображати рівень упевненості експерта (в числовій формі), щодо значень сформованих поточних величин $\underset{\sim}{P}^{\tau_f\, p}_{\partial 1}$ і $\underset{\sim}{P}^{\tau_f\, p}_{\partial 2}$ відносно їх еталонних термів, що відповідно входять в $\mathbf{T^e_{31}}$ і $\mathbf{T^e_{32}}$.

**Етап 3 – визначення ЕК кібератаки.** Введемо підмножину ЕК кібератак

$$\mathbf{EC^{CA}_i} = \{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}} \mathbf{EC^{CA}_i}\} = \{EC^{CA}_1, EC^{CA}_2, ..., EC^{CA}_n\},\ (i = \overline{1,n}),\ \text{де}\ EC^{CA}_i = \frac{1}{m_i}\sum_{j=1}^{m_i} EC^{max}_{ij}.$$

Наприклад, якщо $i = 3$ $(CA_3 = CA_{SP} = SP)$, $m_3 = 2$, а $EC^{CA}_3 = 0{,}727$, то це є дефазифікованим (числовим) значенням, що характеризує лінгвістичну оцінку експерта 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 вирішальних правилах.

Метод формування детекційного середовища (МФДС), який на основі запропонованої кортежної моделі за рахунок механізму формування підмножин ідентифікаторів аномальності, формалізації процесу побудови вирішальних функцій та умовних детекційних виразів, дозволяє сформувати необхідну множину детекційних правил, що використовуються для визначення рівней аномальних станів, характерних впливу певних типів кібератак. Запропонований МФДС базується на трьох етапах.

**Етап 1 – формування підмножин ІД аномальності.** Введемо підмножину ІД $\mathbf{IA_i}$ аномальності

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\mathbf{IA_i}\}=\{\bigcup_{i=1}^{n}\{\bigcup_{u=1}^{v_i}IA_{iu}\}\}=$$

$$\{\{IA_{11}, IA_{12}, ..., IA_{1v_1}\}, \{IA_{21}, IA_{22}, ..., IA_{2v_2}\}, \ldots,$$

$$\{IA_{n1}, IA_{n2}, ..., AI_{nv_n}\}\ \ (i=\overline{1,n}),\ (u=\overline{1,v_i}),$$

де $v_i$ – кількість ІД аномальності, за допомогою яких в лінгвістичних формах можна відобразити можливі рівні аномальності, утворені кібератакою з ІД $CA_i$. Наприклад, при $n=3$ ($CA_1=CA_{SN}$, $CA_2=CA_{DS}$, $CA_3=CA_{SP}$) та $v_1=v_2=v_3=5$ визначимо

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{3}}\mathbf{IA_i}\}=\{\bigcup_{i=1}^{3}\{\bigcup_{u=1}^{v_i}IA_{iu}\}\}=\{\{IA_{11}, ..., IA_{15}\}, \{IA_{21}, ..., IA_{25}\}, \{IA_{31}, ..., IA_{35}\}\}=$$

$$\{\{IA_{SNH}, ..., IA_{SNII}\}, \{IA_{DSH}, ..., IA_{DSII}\}, \{IA_{SPH}, IA_{SPБHB}, IA_{SPБBH}, IA_{SPB}, IA_{SPII}\}\}=$$

$$\{\{"Н",...,"П"\}, \{"Н",...,"П"\}, \{"Н","БНВ","БВН","В","П"\}\}.$$

де, наприклад, $IA_{31}=IA_{SPH}="Н"$, …, $IA_{35}=IA_{SPII}="П"$ відповідно є ІД таких станів аномальності в атакуючому середовищі ($\mathbf{CA^{\tau_f}}$), які відображають різну ступінь упевненості експерта відносно дії кібератаки з ІД $CA_3=CA_{SP}$.

**Етап 2 – формування вирішальних функцій (ВФ).**

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\mathbf{AF_i}\}=\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\{\bigtimes_{\mathbf{a=1}}^{\mathbf{w_i}}\mathbf{AF_{ia}}\}\}=\{\bigcup_{i=1}^{n}\{\bigtimes_{a=1}^{w_i}\{\bigcup_{s=1}^{r_j}AF_{ias}\}\}\}=$$

$$\{\{\{AF_{111}, AF_{112}, ..., AF_{11r_j}\}\times...\times\{AF_{1w_i1}, AF_{1w_i2}, ..., AF_{1w_ir_j}\}\}, \ldots,$$

$$\{\{AF_{n11}, AF_{n12}, ..., AF_{n1r_j}\}\times...\times\{AF_{nw_n1}, AF_{nw_n2}, ..., AF_{nw_nr_j}\}\}\}=$$

$$\{\{\langle\mathbf{SAF_{11}}\rangle, \langle\mathbf{SAF_{12}}\rangle, \ldots, \langle\mathbf{SAF_{1w_1}}\rangle\}, \ldots, \{\langle\mathbf{SAF_{n1}}\rangle, \langle\mathbf{SAF_{n2}}\rangle, \ldots, \langle\mathbf{SAF_{nw_n}}\rangle\}\},$$

де $\mathbf{AF_i}$ – аргумент ВФ, $w_i$ – кількість підмножин аргументів ВФ, а символ $\times$ позначає прямий добуток множин, $r_j$ – кількість членів в $\mathbf{AF_{ia}}$ (що відображає кількість членів в $\mathbf{T_{ij}^e}$), $(a=\overline{1,w_i})$, $(s=\overline{1,r_j})$. Для виявлення $CA_i$ кількість підмножин аргументів є $w_i=\prod_{j=1}^{m_i}r_j$, $(j=\overline{1,m_i})$, а підмножиною ІД аномальності є $\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\mathbf{AF_i}\}=\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\{\bigcup_{\mathbf{a=1}}^{\mathbf{w_i}}\langle\mathbf{SAF_{ia}}\rangle\}\}$, $(a=\overline{1,w_i})$. Далі, введемо підмножину всіх бінарних ВФ: $\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\mathbf{SF_i}\}=\{\mathbf{SF_1}, \ldots, \mathbf{SF_n}\}$,

$$\mathbf{SF_i}=\{\bigcup_{a=1}^{w_i}SF_{ia}\}=\{SF_{i1}, \ldots, SF_{iw_i}\},\ SF_{ia}=SF_{ia}(\ \mathbf{SAF_{ia}}\ ).$$

Функція $SF_{ia}$ визначає взаємозв'язки в $\mathbf{SAF_{ia}}$, які формуються, наприклад, за участю експерта у вигляді логічних ланцюгів. Експерт для отримання визначеної множини бінарних функцій, створює шаблон, що 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 $SF_{11} = AF_{111} \wedge (AF_{112} \vee AF_{113})$. Визначені значення елементів підмножини $\mathbf{AF_i}$ формуються на основі бінарної функції еквівалентності $E(x,\, y) = \begin{cases} 1, \text{ при } x = y \\ 0, \text{ при } x \neq y. \end{cases}$

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 $\mathbf{P_i^{\tau_i p}}$.

Наприклад, формування ВФ, при $n = 3$, для $\mathbf{CA_{SN}^{\tau_i}}$, $\mathbf{CA_{DS}^{\tau_i}}$, $\mathbf{CA_{SP}^{\tau_i}}$, та $w_1 = r_1 \cdot r_2 = 5 \cdot 3 = 15$, $w_2 = r_1 \cdot r_2 \cdot r_3 = 5 \cdot 3 \cdot 3 = 45$, $w_3 = r_1 \cdot r_2 = 5 \cdot 3 = 15$ визначимо

$$\{\bigcup_{i=1}^{3} \mathbf{AF_i}\} = \{\mathbf{AF_1},\ \mathbf{AF_2},\ \mathbf{AF_3}\} = \{\bigcup_{i=1}^{3} \{\bigtimes_{a=1}^{w_i} \mathbf{AF_{ia}}\}\} =$$

$$\{\bigcup_{i=1}^{3} \{\bigtimes_{a=1}^{w_i} \{\bigcup_{s=1}^{r_j} AF_{ias}\}\}\} = \{\{\{AF_{111}, ..., AF_{115}\} \times \{AF_{121}, ..., AF_{123}\}\}, \{\{AF_{211}, ..., AF_{215}\} \times$$

$$\{AF_{221}, ..., AF_{223}\} \times \{AF_{231}, ..., AF_{233}\}\}, \{\{AF_{311}, ..., AF_{315}\} \times \{AF_{321}, ..., AF_{323}\}\}\} =$$

$$\{\{\langle \mathbf{SAF_{11}} \rangle, \ldots, \langle \mathbf{SAF_{1\,15}} \rangle\},\ \{\langle \mathbf{SAF_{21}} \rangle, \ldots, \langle \mathbf{SAF_{2\,45}} \rangle\},\ \{\langle \mathbf{SAF_{31}} \rangle, \ldots, \langle \mathbf{SAF_{3\,15}} \rangle\}\}.$$

Експерт для отримання конкретної множини бінарних функцій, які виявляють SN та SP створює шаблон $\langle AF \wedge AF \rangle$, а для DS – $\langle AF \wedge (AF \vee AF) \rangle$, далі наприклад, визначимо для SP

$$\mathbf{SF_3} = \{\bigcup_{a=1}^{w_3} SF_{3a}\} =$$

$$\{(E(NUM_{31}, 1) \wedge E(NUM_{32}, 1)), \ldots, (E(NUM_{31}, 5) \wedge E(NUM_{32}, 1))\},$$

$$\{(E(NUM_{31}, 1) \wedge E(NUM_{32}, 2)), \ldots, (E(NUM_{31}, 5) \wedge E(NUM_{32}, 2))\},$$

$$\{(E(NUM_{31}, 1) \wedge E(NUM_{32}, 3)), \ldots, (E(NUM_{31}, 5) \wedge E(NUM_{32}, 3))\}.$$

Найбільш значимими є опорні блоки з ІД БВН, В та П. З урахуванням з цього приклад конкретних розрахунків представимо для ВФ $(SF_{3\,11}, ..., SF_{3\,15})$ з $\mathbf{SF_3}$ та отримаємо визначальну ВФ $SF_{3\,13} = (E(NUM_{31}, 3) \wedge E(NUM_{32}, 3)) = (1 \wedge 1) = 1$.

**Етап 3 – формування умовних виразів детекційного середовища (DR).** Умовні вирази, які відображають сформовані базові правила представимо у вигляді

$$\mathbf{DR_i} = \{\bigcup_{a=1}^{w_i} \mathbf{DR_{ia}}\} = \{\mathbf{DR_{i1}},\ \mathbf{DR_{i2}}, \ldots,\ \mathbf{DR_{iw_i}}\} =$$

$$\{\ \mathbf{DR_{i1}} \Rightarrow \{if\ SF_{i1}\ then\ \{\bigcup_{u=1}^{v_i} IA_{iu}\}\},\ \ldots,$$

$$\mathbf{DR_{iw_i}} \Rightarrow \{if\ SF_{ia}\ then\ \{\bigcup_{u=1}^{v_i} IA_{iu}\}\}\},\ (a = \overline{1, w_i},\ u = \overline{1, v_i}).$$

Кожна бінарна ВФ $SF_{ia}$ може бути пов'язан з $v_i$-ю кількістю ІД аномальності та, таким чином, кожне базове правило може породжуватись $v_i$ кількістю виразів, тобто:

$$\mathbf{DR_i} = \{\mathbf{DR_{i1}}, \mathbf{DR_{i2}}, \ldots, \mathbf{DR_{iw_i}}\} =$$

$$\{\ \mathbf{DR_{i1}} \Rightarrow \{if\ SF_{i1}\ then\ IA_{i1}, if\ SF_{i1}\ then\ IA_{i2}, ..., if\ SF_{i1}\ then\ IA_{iv_i}\}, \ldots,$$

$$\mathbf{DR_{iw_i}} \Rightarrow \{if\ SF_{iw_i}\ then\ IA_{i1}, if\ SF_{iw_i}\ then\ IA_{i2}, ..., if\ SF_{iw_i}\ then\ IA_{iv_i}\}\}.$$

Кількість умовних виразів $CDR_i = w_i \cdot v_i$, а для виявлення $n$ атак $CDR = \sum_{i=1}^{n} CDR_i$.

Із загальної кількості можливих детекційних виразів не всі впливають на процес виявлення вторгнень, в цьому випадку визначальними будуть $\mathbf{DR_{3\,11}}, \mathbf{DR_{3\,12}}, \ldots, \mathbf{DR_{3\,15}}$.

Визначальною є ВФ $SF_{3\,13}$ (із етапу 2), яка входить в підмножину $\mathbf{DR_{3\ 13}}$, тобто:

$$\mathbf{DR_{3\ 13}} \Rightarrow \{if\ SF_{3\,13}\ then\ IA_{31}, \ \ldots,\ if\ SF_{3\,13}\ then\ IA_{35}\} =$$

$$\{if\ \ (E(NUM_{SPKOП}, 1) \wedge E(NUM_{SPKПОА}, 3))\ then\ "Н",$$

$$if\ \ (E(NUM_{SPKOП}, 2) \wedge E(NUM_{SPKПОА}, 3))\ then\ "БНВ",$$

$$if\ \ (E(NUM_{SPKOП}, 3) \wedge E(NUM_{SPKПОА}, 3))\ then\ "БВН",$$

$$if\ \ (E(NUM_{SPKOП}, 4) \wedge E(NUM_{SPKПОА}, 3))\ then\ "В",$$

$$if\ \ (E(NUM_{SPKOП}, 5) \wedge E(NUM_{SPKПОА}, 3))\ then\ "П"\}.$$

Після перевірки всіх виразів в $\mathbf{DR_{3\ 13}}$ визначимо, що ідентифікація аномального стану здійснюється за допомогою умовного виразу

$$if\ \ (E(NUM_{SPKOП}, 3) \wedge E(NUM_{SPKПОА}, 3))\ then\ "БВН" = if\ \ (1 \wedge 1)\ then\ "БВН".$$

Показаний поточний блок (заштрихована прямокутна область, яка утворена за допомогою $\underset{\sim}{P}_{31}^{\tau_f}$, $\underset{\sim}{P}_{32}^{\tau_f}$) (рис. 3), який інтерпретує аномалію у 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 $\tau_f$. Поточний блок ближче всього розташований до нечіткої опорної двомірної області з ІД *"БВН"*, а з використанням ЕК параметрів ($EC_{31}^{max}$, $EC_{32}^{max}$) та кібератаки ($EC_3^{CA}$) зазначимо умовний вираз з підмножини $\mathbf{DR_{3\,13}}$ детекційного підсередовища ($\mathbf{DR_{SP}}$) для виявлення спуфінгу: «Якщо поточний параметр «Кількість одночасних підключень до сервера» в момент часу $\tau_f$ найближчий до еталону «Середнє» (з ЕК $0{,}713$) і поточний параметр «Кількість пакетів з однаковою адресою відправника та одержувача» в момент часу $\tau_f$ найближчий до еталону «Велике» (з ЕК $0{,}741$), то рівень аномального стану, породженого спуфінгом буде «Більш високим ніж низьким» (з ЕК кібератаки $0{,}727$)». Також, можна застосувати еквівалентний запис: $if\ \ (E(NUM_{SPKOП}, 3)\big|_{0{,}713} \wedge E$

$(NUM_{SPKIIOA},\ 3)\big|_{0,741})$ *then* "БВН"$\big|_{0,727}$. Аналогічним чином, при різних початкових вхідних даних визначаються інші типи кібератак.

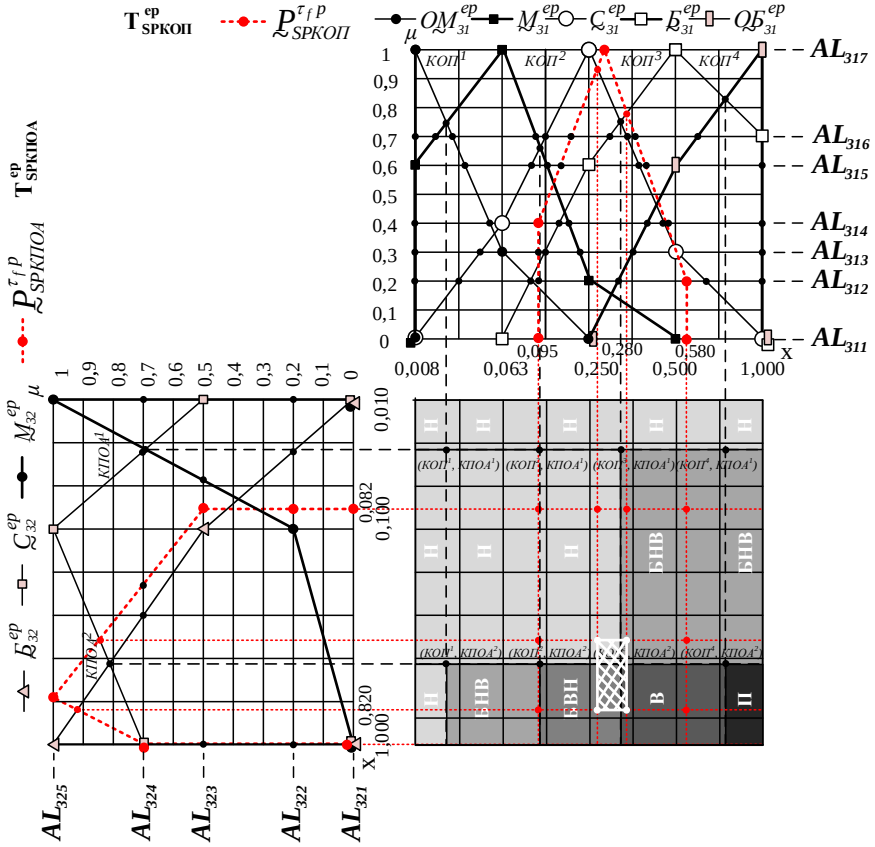


Рис. 3. Графічна інтерпретація експертного розподілу ідентифікаторів атакуючих дій (відображених двовимірними опорними областями Н, БНВ, БВН, В, П) та фазифікованих значень поточних параметрів $\tilde{P}^{\tau_f}_{31}$ і $\tilde{P}^{\tau_f}_{32}$ відносно лінгвістичних еталонів $\mathbf{T}^{ep}_{31}$ і $\mathbf{T}^{ep}_{32}$ відповідно

На основі КМАС та методів МФЕС, МФП, МАН, МВІТ, МДП і МФДС розроблена методологія побудови систем виявлення аномалій (МПСВ) породжених кібератаками (рис. 4), яка за рахунок механізмів формування атакуючих середовищ, побудови $m_i$-вимірних параметричних еталонних та поточних підсередовищ, $\alpha$-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.

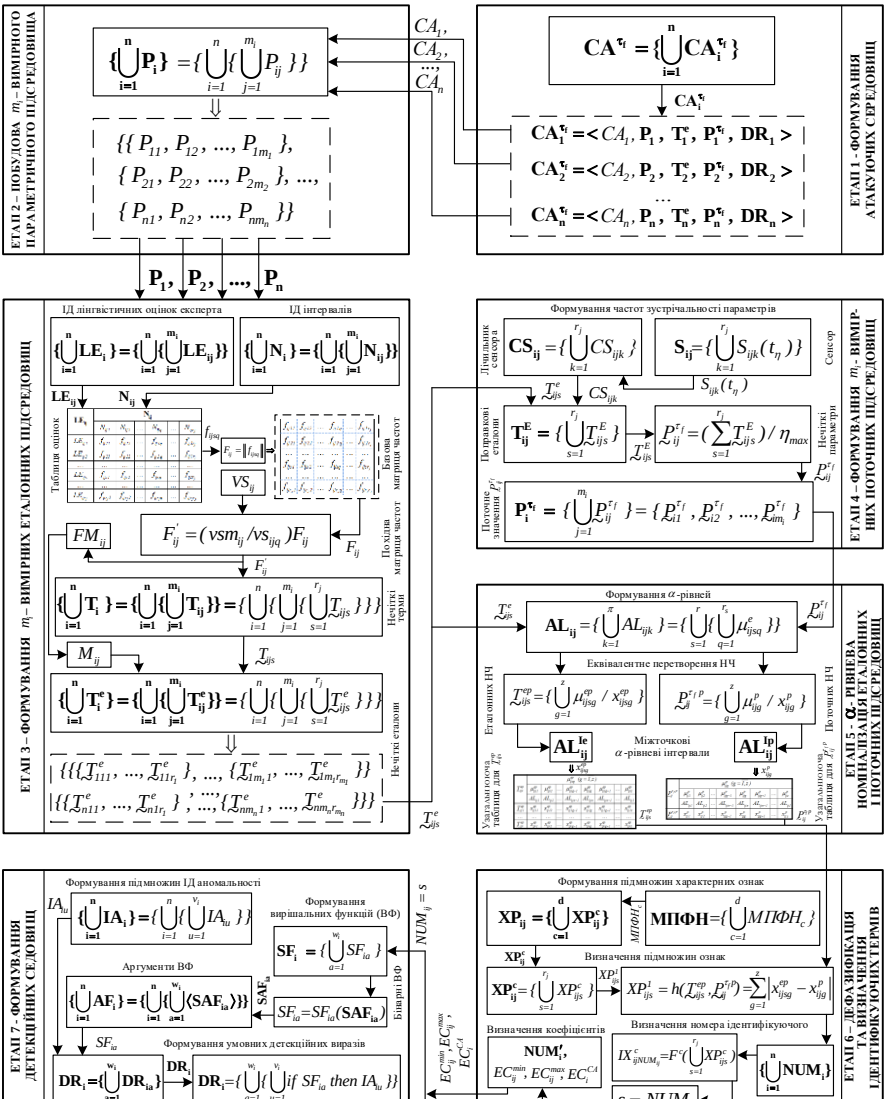


Рис. 4. Схема відображення методології побудови систем виявлення аномалій, породжених кібератаками

Базовий механізм запропонованої методології базується на семи етапах: етап 1 – формування атакуючих середовищ ( $\mathbf{CA}^{\tau_f}$ ); етап 2 – побудова $m_i$-вимірного параметричного підсередовища ($\mathbf{P_i}$); етап 3 – формування $m_i$-вимірних еталонних підсередовищ

( $\mathbf{T_i^e}$ ); етап 4 – формування $m_i$-вимірних поточних підсередовищ ( $\mathbf{P_i^{\tau_f}}$ ); етап 5 – $\alpha$-рівнева номіналізація еталонних і поточних підсередовищ ( $\mathbf{T_i^e}$ та $\mathbf{P_i^{\tau_f}}$ ); етап 6 – дефазифікація та визначення ідентифікуючих термів; етап 7 – формування детекційних середовищ (**DR**). 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.

**П'ятий розділ** присвячений розробці засобів розширення функціональних можливостей СВВ. На основі запропонованої методології розроблено структурне рішення обчислювальної системи виявлення кібератак (СВК), яке за рахунок баз даних кібератак, правил та еталонів, а також модулів формування поточних значень, $\alpha$-рівневої номіналізації, дефазифікації та ідентифікуючих термів, рівня аномальності та візуалізації дозволяє будувати засоби, які визначають рівні аномального стану, що характерні впливу певного типу кібератак і розширюють функціональні можливості сучасних СВВ.

Структурне рішення СВК відображено на рис. 5. Воно містить узгоджені за параметрами: бази даних кібератак (БДК); бази даних правил (БДП); бази даних еталонів (БДЕ), а також модулі формування поточних значень (МФПЗ), $\alpha$-рівневої номіналізації (МАРН), дефазифікації та ідентифікуючих термів (МДІТ), рівня аномальності (МРА) та візуалізації (МВ).

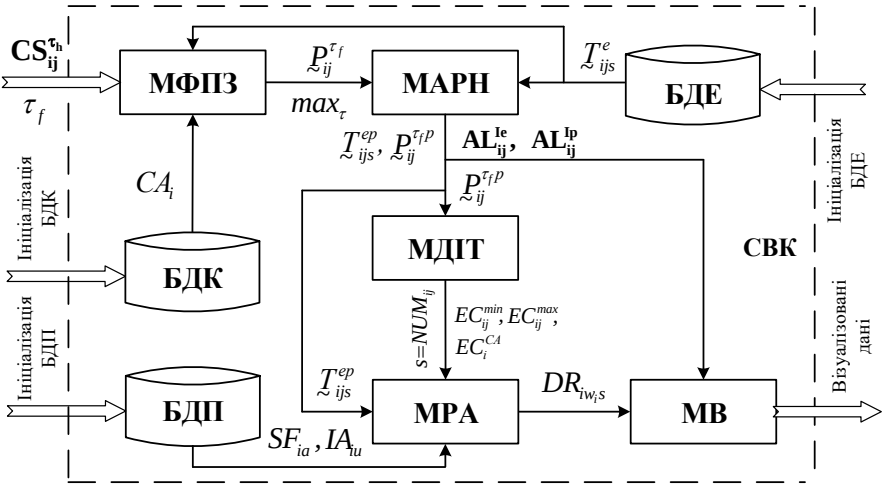


Рис. 5. Структурна схема СВК

База БДК містить множину ІД кібератак $CA_i$, за допомогою яких здійснюється однозначне виявлення атаки в процесі присвоєння її імені конкретному ІД. База БДП складається з бінарних вирішальних функцій $SF_{ia}$ та ІД аномальності $IA_{iu}$, що входять в множину базових правил $\mathbf{DR_i}$, які необхідні для виявлення $i$-ї кібератаки за допомогою параметричних підсередовищ ($\mathbf{P_i}$) різної розмірності. База БДЕ містить множину лінгвістичних еталонів $\underset{\sim}{T}_{ijs}^{e}$ призначених для відображення стану множини відповідних па-

раметрів $\mathbf{P_i}$ у визначеному середовищі оточення, що направлені на виявлення кібератаки з ІД $CA_i$. Модуль МФПЗ призначений для формування всіх можливих поточних значень нечітких параметрів $\underset{\sim}{P}_{ij}^{\tau_f}$, одержаних за допомогою $\mathbf{T_i^e}$ у визначений момент часу $\tau_f$ за заданий проміжок. Модуль МАРН здійснює еквівалентне перетворення НЧ за допомогою зведення всіх еталонних $\underset{\sim}{T}_{ijs}^{e}$ та поточних $\underset{\sim}{P}_{ij}^{\tau_f}$ до номінального числа компонент на основі підмножин α-рівневих інтервалів $\mathbf{AL_{ij}^{Ie}}$ та міжточкових α-рівневих інтервалів $\mathbf{AL_{ij}^{Ip}}$. 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. Модуль МРА необхідний для формування $DR_{iw_i s}$ на основі ідентифікуючого еталонного терму (використання $NUM_{ij}$), еталонного перетвореного НЧ $\underset{\sim}{T}_{ijs}^{ep}$, а також ІД аномальності $IA_{iu}$ та бінарних вирішальних функцій $SF_{ia}$, за допомогою обробки підмножин умовних детекційних виразів $\mathbf{DR_i} = \{\bigcup_{a=1}^{w_i}\{\bigcup_{u=1}^{v_i} if\ SF_{ia}\ then\ IA_{iu}\}\}$, які відображають сформовані базові правила для виявлення *i*-ї кібератаки з використанням параметричних підсередовищ ($\mathbf{P_i}$) різної розмірності. Модуль МВ використовується для графічної інтерпретації поліпараметричного мультирозмірного середовища, розподілу ІД атакуючих дій та фазифікованих значень поточних параметрів $\underset{\sim}{P}_{ij}^{\tau_f p}$ відносно лінгвістичних еталонів $\mathbf{T_{ij}^{ep}}$ у вигляді області, яка характеризує атаки, а також відображення умовного виразу $DR_{iw_i s}$ базового детекційного правила, відповідно до якого було здійснено виявлення кібератак. На базі запропонованої методології та структурованого рішення відповідної обчислювальної системи розроблено алгоритмічне забезпечення для реалізації відповідного ПЗ виявлення кібератак.

Система СВК відповідно до алгоритму (рис. 6) функціонує наступним чином. Умовно роботу СВК можна представити двома процесами: 1) процес ініціалізації БД; 2) процес виявлення кібератак. Процес ініціалізації БД зв'язаний з наповненням (модифікацією) БДК, БДП та БДЕ. За необхідністю, на етапі функціонування СВК, зазначені БД можуть піддаватися модифікації. Процес виявлення кібератак $CA_i$ здійснюється за заданий часовий проміжок $\tau_h$ в кожний момент часу $\tau_f$ ($f = \overline{1,max_\tau}$, де $max_\tau$ – максимальний номер часового проміжку $f$) на основі множини значень лічильників сенсорів $\mathbf{CS_{ij}}$, показники яких залежать від $\tau_h$ ($CS_{ij}^{\tau_h}$), а також НЧ $\underset{\sim}{T}_{ijs}^{e}$ еталонного підсередовища ($\mathbf{T_i^e}$), які передаються з БДЕ та надходять в модуль МФПЗ, де формуються поточні значення нечітких параметрів $\underset{\sim}{P}_{ij}^{\tau_f}$ та визначається $max_\tau$.

Далі, з БДЕ та МФПЗ відповідно НЧ $\underset{\sim}{T}^{e}_{ijs}$ і $\underset{\sim}{P}^{\tau_f}_{ij}$ еталонного та поточного підсередовища ($\mathbf{T_i^e}$ та $\mathbf{P_i^{\tau_f}}$) надходять в МАРН, де здійснюється їх $\alpha$-рівнева номіналізації. 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 ЕК параметрів і кібератак ($EC_{ij}^{min}$, $EC_{ij}^{max}$ і $EC_i^{CA}$), які інтерпретують лінгвістичні параметри і в сукупності відображають аномальність поточного ($\mathbf{P^{\tau_f}}$) стану середовища оточення, породженого визначеними кібератаками.

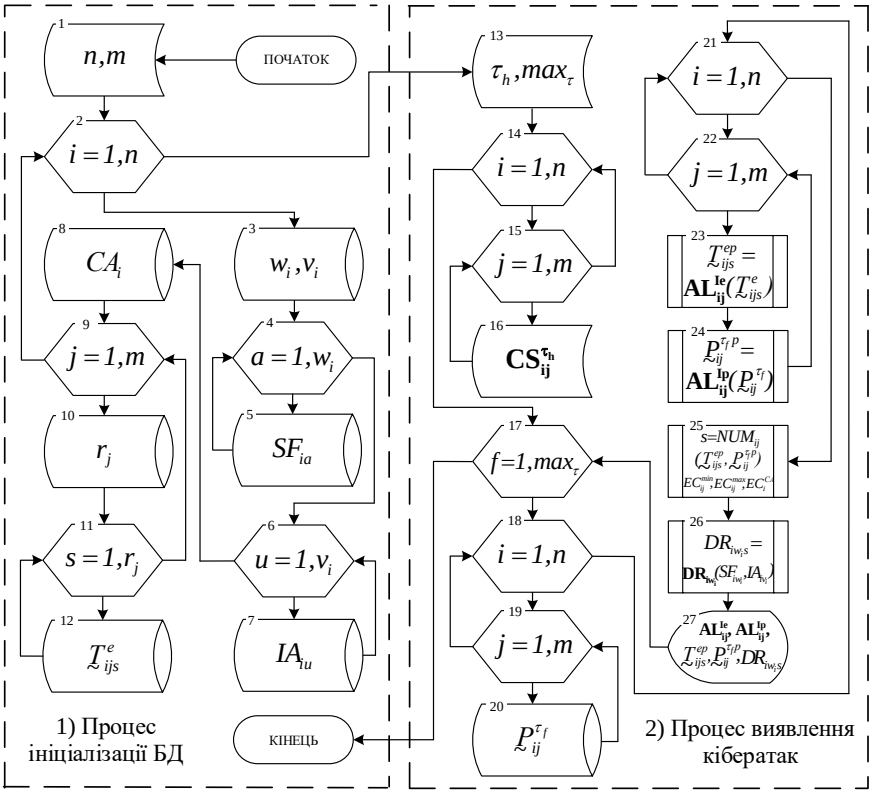


Рис. 6. Алгоритм роботи СВК

Далі, на основі отриманих в МАРН ідентифікуючих термів $\underset{\sim}{T}^{ep}_{ijs}$ та термів, для яких $s=NUM_{ij}$, що надійшли з МДІТ, а також бінарних функцій $SF_{ia}$ та ІД аномальності $IA_{iu}$, які надходять з БДП, в МРА формуються підмножини базових правил $\mathbf{DR_i}$, за допомогою яких визначається умовний вираз $DR_{iw_i s}$, за яким здійснюється виявлення

*i*-ї кібератаки. На основі підмножини $\alpha$-рівневих інтервалів $\mathbf{AL}_{\mathbf{ij}}^{\mathbf{Ie}}$, міжточкових $\alpha$-рівневих інтервалів $\mathbf{AL}_{\mathbf{ij}}^{\mathbf{Ip}}$, а також всіх перетворених $\underset{\sim}{T}_{ijs}^{ep}$ та $\underset{\sim}{P}_{ij}^{\tau_f p}$, що надійшли з МАРН та умовного виразу $DR_{iw_i s}$, який надійшов з МРА, в МВ графічно інтерпретуються ІД атакуючих дій (що відображаються за допомогою багатовимірних (наприклад, двовимірних або тривимірних) опорних областей, наприклад, Н, БНВ, БВН, В, П) та фазифіковані значення поточних параметрів $\underset{\sim}{P}_{ij}^{\tau_f p}$ відносно лінгвістичних еталонів $\mathbf{T}_{\mathbf{ij}}^{\mathbf{ep}}$ відповідно.

З урахуванням запропонованого алгоритмічного забезпечення розроблено програмну модель системи, яка може функціонувати в наступних режимах (див. рис. 7-9): формування поточного середовища ( $\mathbf{P}^{\tau_f}$ ); формування еталонного середовища ($\mathbf{T}^{\mathbf{e}}$); формування атакуючого середовища ( $\mathbf{CA}^{\tau_f}$ ); виявлення аномального стану.

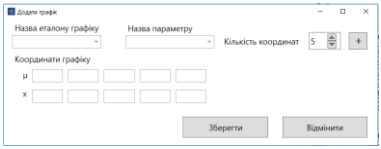


Рис. 7. Вікно ініціалізації еталонних середовищ

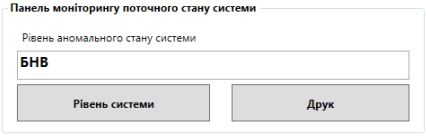


Рис. 8. Вікно ідентифікації аномального стану

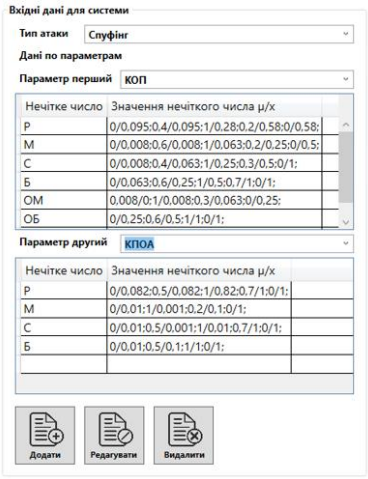


Рис. 9. Вікно відображення НЧ для поточних та еталонних середовищ

На рис. 10 представлена графічна інтерпретація аномального стану, утвореного атакуючим SP-седовищем ( $\mathbf{CA}^{\tau_f}$ ) в момент часу $\tau_f$. Тут, на основі поточного блоку за допомогою умовного виразу (з підмножини $\mathbf{DR}_{\mathbf{3\,13}}$ детекційного підсередовища $\mathbf{DR}_{\mathbf{SP}}$), який можна інтерпретувати як: «Якщо поточний параметр «Кількість одночасних підключень до сервера» в момент часу $\tau_f$ найближчий до еталону «Середнє» (з ЕК *0,713* ) і поточний параметр «Кількість пакетів з однаковою адресою відправника та одержувача» в момент часу $\tau_f$ найближчий до еталону «Велике» (з ЕК *0,741),* то рівень аномального стану, породженого спуфінгом буде «Більш високим ніж низьким» (з ЕК кібератаки *0,727)*», здійснюється виявлення аномального стану в момент часу $\tau_f$. Також, умовний вираз можна записати як

$$if \quad (E\,(NUM_{SPKOП},\ 3)\big|_{0,713} \wedge E\,(NUM_{SPKПОА},\ 3)\big|_{0,741})\ \ then\ \ "БВН"\big|_{0,727},$$

з якого видно що, для виявлення кібератаки був застосований умовний вираз з ІД аномальності «БВН». За результатами експерименту можна зробити висновок, що у всіх випадках 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.

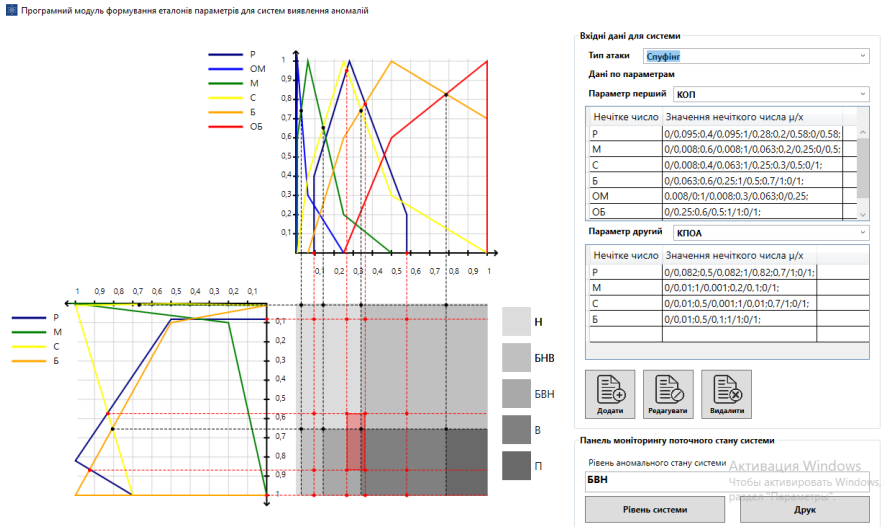


Рис. 10. Графічне відображення аномального стану, утвореного атакуючим SP-середовищем ( $\mathbf{CA}^{\tau_f}$ ) в момент часу $\tau_f$ .

Експериментальне дослідження здійснювалось за допомогою розробленої віртуальної мережі, де проведене моделювання 2000 атак (з достатньо високим рівнем впливу на файл-сервер), кожна з яких була виявлена за допомогою певного умовного виразу сформованого детекційного середовища, яке у розглянутому випадку складається з одного підсередовища (**$DR_3$=$DR_{SP}$**). Результати проведеного експерименту інтегровано в табл. 4.

Таблиця 4

Результати моделювання впливів атакуючого SP-середовища

| Підмножина детекційних виразів | Задіяний ІД аномальності | Середнє значення ЕК кібератаки | Кількість кібератак | Відсоток виявлених кібератак |
|---|---|---|---|---|
| **$DR_{3\,13}$** | ББН | 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 ББН, В та П, що входять у підмножини детекційних виразів **$DR_{3\,13}$**, **$DR_{3\,14}$** та **$DR_{3\,15}$**, на кожне з яких відповідно припало 32,35%, 45,5% та 22,15% реалізованих загроз на файл-сервер.

Проведені експериментальні дослідження підтвердили достовірність основних теоретичних положень, практичних розробок та висновків наукової роботи.

У **додатках** містяться акти впровадження результатів дисертаційної роботи та лістинг (початковий код) програмної моделі системи.

## ВИСНОВКИ

У ході виконання дисертаційної роботи вирішена актуальна науково-прикладна проблема, яка пов'язана з розробкою ефективного методологічного забезпечення процесу виявлення аномалій, породжених кібератаками на ресурси інформаційних систем. Зазначена проблема обумовлюється 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, породжених реалізацією нових типів загроз РІС. Отримані наукові результати мають фундаментальне теоретичне та практичне значення у сфері безпеки інформації та можуть бути використані при розробці відповідних систем захисту інформації.

У ході розв'язання поставлених задач були отримані наступні результати:

1. 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.

2. 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.

3. 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.

4. 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.

5. Розроблений метод $\alpha$-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.

6. 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.

7. Розроблений метод дефазифікації параметрів детекційного середовища, який дозволив у числовій формі характеризувати рівень упевненості експерта відносно його суджень щодо можливих кібератак.

8. 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.

9. Запропонована методологія побудови систем виявлення аномалій, породжених кібератаками, яка використовується для визначення рівня аномального стану в *m*-вимірному гетерогенному параметричному середовищі.

10. 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.

11. 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.

12. Експериментальне дослідження програмної моделі системи, а також впровадження та успішне практичне використання відповідних розробок підтвердило достовірність теоретичних положень та гіпотез, практичних розробок і висновків дисертаційної роботи.

## ПУБЛІКАЦІЇ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. 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.

2. 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.

3. 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.

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. 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.

6. 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.

7. 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.

8. 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.

9. 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.

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.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.

12. 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.

13. 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.

14. А. Корченко, «Система формирования нечетких эталонов сетевых параметров», *Захист інформації*. Т.15, №3, С. 240-246, 2013.

15. А. Корченко, «Система формирования эвристических правил для оценивания сетевой активности», *Захист інформації*, Т.15, №4, С. 353-359, 2013.

16. Б. Ахметов, А. Корченко, Н. Жумангалиева «Использование методов нечетких множеств в системах обнаружения вторжений», *Інформаційна безпека*, №1, №2, С. 42-55, 2014.

17. А. Корченко, С. Ахметова, «Классификация систем обнаружения вторжений», *Інформаційна безпека*, №1, №2, С. 168-175, 2014.

18. Б. Ахметов, А. Корченко, С. Ахметова, Н. Жумангалиева, «Использование методов экспертного оценивания в системах обнаружения вторжений», *Інформаційна безпека*, №3, №4, С. 34-43, 2014.

19. А. Корченко, «Метод формирования лингвистических эталонов для систем выявления вторжений», *Захист інформації*, Т.16, №1, С. 5-12, 2014.

20. А. Корченко, «Метод фаззификации параметров на лингвистических эталонах для систем выявления кибератак», *Безпека інформації*, Т.20, №1, С. 21-28, 2014.

21. А. Корченко, «Метод $\alpha$-уровневой номинализации нечетких чисел для систем обнаружения вторжений», *Захист інформації*, Т.16, №4, С. 292-304, 2014.

22. А. Корченко, «Метод определения идентифицирующих термов для систем обнаружения вторжений», *Безпека інформації*, Т.20, №3, С. 217-223, 2014.

23. 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.

24. Н. Карпинский, А. Корченко, С. Ахметова, «Метод формирования базовых детекционных правил для систем обнаружения», *Захист інформації*, Т.17, №4, С. 312-324, 2015.

25. А. Корченко, В. Щербина, Н. Вишневская, «Методология построения систем выявления аномалий порожденных кибератаками», *Захист інформації*, Т.18, №1, С. 30-38, 2016.

26. 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.

27. 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.

28. И. Терейковский, А. Корченко, «Система выявления кибератак», *Безпека інформації*, Т.23, №3, С. 176-180, 2017.

29. 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.

30. ПЗ 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.

31. С. Казмірчук, А. Корченко, Т. Паращук, «Аналіз систем виявлення вторгнень», *Захист інформації*, Т.20, №4, С. 259-276, 2018.

32. І. Терейковський, А. Корченко, Т. Паращук, Є. Педченко, «Аналіз відкритих систем виявлення вторгнень», *Безпека інформації*, Т.24, №3, С. 201-216, 2018.

33. 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.

34. 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.

35. 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.

36. 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.

37. 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.

38. 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.

39. 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.

40. 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.

41. 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.

42. 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.

## АНОТАЦІЯ

**Корченко А. О. Методи ідентифікації аномальних станів для систем виявлення вторгнень.** – Рукопис.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації». – Національний авіаційний університет, Київ, 2019.

Дисертаційна робота присвячена вирішенню актуальної науково-прикладної проблеми, яка пов'язана з розробкою методів ідентифікації аномальних станів для систем виявлення вторгнень (СВВ). В роботі проведено аналіз сучасних СВВ відносно базових характеристик, як-от «Клас кібератак», «Адаптивність», «Відкритість», «Методи виявлення», «Управління системою», «Масштабованість», «Рівень спостереження», «Реакція на кібератаку», «Захищеність» та «Підтримка ОС». Це надає можливості розробникам і користувачам обирати необхідні методи та відповідне програмне забезпечення (ПЗ) для захисту інформаційних систем (ІС) і будувати відповідні системи безпеки. На основі цього, 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. Також 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. Запропоновані методи фазифікації та дефазифікації параметрів, які дозволили формалізувати процес перетворення значень параметрів *m*-вимірних поточних середовищ для їх подальшого застосування у виявленні аномального стану та відобразити параметри детекційного середоваща, що характеризують у числовій формі рівень упевненості експерта відносно його суджень щодо можливих кібератак. 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 ІС. 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 формування детекційного середовища для побудови необхідної множини детекційних правил, що використовуються при визначенні поточного рівня аномального стану, характерного дії визначеного типу кібератак в *m*-вимірному гетерогенному параметричному середовищі. На підставі запропонованих методів і моделі розроблено методологію 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 СВВ. Також, на базі запропонованої методології та відповідного структурного рішення розроблено алгоритмічне забезпечення та програмна модель системи, яка може використовуватися автономно або бути розширювачем функціональних можливостей сучасних СВВ. Проведені експериментальні дослідження підтвердили достовірність теоретичних положень та практичних розробок дисертаційного дослідження.

**Ключові слова:** атаки, кібератаки, аномалії, лінгвістичні змінні, нечіткі множини, нечіткі числа, виявлення кібератак, виявлення аномалій, системи виявлення вторгнень, системи виявлення аномалій, системи виявлення атак, системи виявлення кібератак.

## АННОТАЦИЯ

**Корченко А.А. Методы идентификации аномальных состояний для систем обнаружения вторжений.** – Рукопись.

Диссертация на соискание ученой степени доктора технических наук по специальности 05.13.21 – «Системы защиты информации». – Национальный авиационный университет, Киев, 2019.

Диссертация посвящена решению актуальной научно-прикладной проблемы, которая связана с разработкой методов идентификации аномальных состояний для систем обнаружения вторжений (СОВ). В работе проведен анализ современных СОВ относительно базовых характеристик, таких как «Класс кибератак», «Адаптивность», «Открытость», «Методы выявления», «Управление системой», «Масштабируемость», «Уровень наблюдения», «Реакция на кибератаку», «Защищенность» и «Поддержка ОС». Это дает возможности разработчикам и пользователям выбирать необходимые методы и соответствующее программное обеспечение (ПО) для защиты информационных систем (ИС) и строить соответствующие системы безопасности. На основе этого разработано кортежную модель формирования атакующих сред, которая позволяет сформировать набор частных кортежей, для симуляции процесса выявления аномального состояния в *m*-мерной гетерогенной параметрической среде, порожденной соответствующей атакующей средой в заданный временной промежуток. Также, разработан метод формирования эталонов для формализации процесса получения эталонных сред, содержащих множества значений фиксированных параметров заданных групп лингвистических переменных, характеризующих конкретную эталонную подсреду. Предложенны методы фаззификации и дефаззификации параметров, которые позволили формализовать процесс преобразования значений параметров *m*-мерных текущих сред для их дальнейшего применения при выявлении аномального состояния и отразить параметры детекционной среды, характеризующие в числовой форме уровень уверенности эксперта относи-

тельно его суждений о возможных кибератак. Разработан метод α-уровневой номинализации нечетких чисел, который позволил осуществить графическую интерпретацию нечетких величин и определение идентифицирующих термов, отражающих в заданный момент времени значение эталонных и текущих подсред, которые характерны для реализации определенных типов кибератак на ресурсы ИС. Предложен метод определения идентифицирующих термов, для поиска в заданных лингвистических переменных, идентифицирующих преобразованных эталонных термов, по которым с помощью детекционных выражений определяются уровни аномальных состояний. Разработан метод формирования детекционной среды для построения необходимого множества детекционных правил, используемых при определении текущего уровня аномального состояния, характерного воздействию определенного типа кибератак в *m*-мерной гетерогенной параметрической среде. На основе предложенных методов и модели разработана методология построения систем обнаружения аномалий, порожденных кибератаками, которая используется для определения уровня аномального состояния в *m*-мерной гетерогенной параметрической среде. Разработано структурное решение вычислительной системы обнаружения кибератак, что позволяет с помощью определения уровня аномального состояния, характерного воздействию определенного типа кибератак, расширить функциональные возможности современных СОВ. Также, на базе предложенной методологии и соответствующего структурного решения разработано алгоритмическое обеспечение и программная модель системы, которая может использоваться автономно или в качестве расширителя функциональных возможностей современных СОВ. Проведенные экспериментальные исследования подтвердили достоверность теоретических положений и практических разработок диссертационного исследования.

**Ключевые слова:** атаки, кибератаки, аномалии, лингвистические переменные, нечеткие множества, нечеткие числа, выявления кибератак, выявление аномалий, системы обнаружения вторжений, системы обнаружения аномалий, системы обнаружения атак, системы обнаружения кибератак.

## ABSTRACT

**A. Korchenko. Methods for identifying abnormal states for intrusion detection systems. –** Manuscript.

Thesis for a Doctor of Technical Science degree in specialty 05.13.21 – «Information security systems». – National Aviation University, Kyiv, 2019.

The functionality of modern intrusion detection and blocking systems depends to a great extent on their capabilities to detect new cyberattacks in real time. Systems for countering cyberattacks are well developed, but their effective operation requires appropriate information that is supposed to be helpful in detecting attack actions. As a rule, such data is formed post facto and requires certain time. So, detection and blocking of new cyberattacks are characterized by the conflict between the readiness of cyberattack counteraction systems to immediately respond to an intrusion and the lack of readiness of detection tools to appropriately inform the counteraction functional. In order to deal with this problem, it is necessary to design specific tools that would enable enlarged functional capabilities of modern intrusion detection systems through the a priori formation of information about anomalous states in information systems caused by certain cyberattack types. For this purpose, the most effective approach consists in using the expert knowledge, which, as a rule, is represented in the form of the expert's judgments about the parameters abnormality level caused by the effect of new types

of threats. The dissertation deals with a pressing applied scientific problem related to detection of new kinds of cyberattacks within the shortest possible time by designing an appropriate methodology of creating systems for detecting anomalous states caused by new types of threats. The methodology is supposed to focus on creation of tools that would enlarge the functionality of modern intrusion detection systems.

Taking into account some publicized studies with their further generalization and display with regard to an expanded range of tools for detecting abuses and anomalies, modern intrusion detection systems have been analyzed in relation to such basic characteristics as «Class of cyberattacks», «Adaptability», «Openness», «Detection methods», «System management», «Scalability», «Observation level», «Reaction to cyberattacks», «Security» and «OS Support». This enables developers and users to choose necessary techniques and appropriate software to protect information systems and create appropriate security systems. The analysis of the sources shows that early detection of abuses and anomalies is an urgent problem of modern information systems. The existing systems show their imperfection and unavailability to adapt in real time to detect anomalies caused by modified or unknown threats. The mathematics of fuzzy sets is not used in the systems that have been analyzed although it shows its effectiveness in solving this kind of problems. On this basis, a tuple model for the formation of attacking media has been designed, which, by formalizing the process of creation of $m_i$-dimensional parametric, attacking, reference, current and detecting sub-environments, makes it possible to form a set of partial tuples to simulate the process of detecting anomalous states in an $m$-dimensional heterogeneous parametric environment created by the appropriate attacking environment at a given time interval. Also, a method of reference environment formation has been designed, which, by using a set of identifiers of linguistic estimates and identifiers of intervals, basic and derived frequency matrices, by formal representation of expert reasoning regarding the description of the current state of parameters with respect to the cyberattack, by forming the occurrence of expert estimates and fuzzy terms subsets within the specified frequency intervals, makes it possible to formalize the process of obtaining the reference values of the fixed parameters of the specified groups of linguistic variables, which characterizes a specific reference sub-environment. A method of parameter phasing in reference sub-environments is suggested, which, by introducing sets of sensors, sensor counters and correction references as well as by using sets of linguistic references and those of the appropriate subsets of intervals in order to form the frequencies of occurrence of physical parameter values at the specified moments of the expected event, makes it possible to formalize the process of transformation of the current values of the $m$-dimensional current environment parameters into a fuzzy form for their further application in detecting anomalous states. A method of $\alpha$-level nominalization of fuzzy numbers has been designed, which, due to the constructed mechanism of creation of a set of $\alpha$-levels, auxiliary subsets of $\alpha$-level intervals and inter-point $\alpha$-level intervals as well as due to the nominalization process and determination of the values of the necessary supports of the fuzzy numbers of the reference and current environments, allows graphical interpretation of fuzzy quantities and determination of identifying terms that represent the current states of the reference and current environments that are characteristic of realization of certain types of cyber-attacks on information resources. A method for determination of the identifying terms is suggested, which, due to the basic mechanism that forms elements of the set of characteristic features and uses the agreed function, makes it possible, due to the reference environment, searching the transformed identifying reference terms focusing on processing in the detecting environment in order to determine the levels of anomalous states. A method for dephasing the detecting environment parameters has been designed,

which, by defining the auxiliary term, the expert coefficients of parameters and the expert cyberattack coefficient, which characterize the expert linguistic estimates associated with the anomalous state level in the current environment, allows numerical representation of the expert's confidence in his judgments about possible cyberattacks. A method of detecting environment formation has been designed, which, on the basis of the suggested tuple model and due to the mechanism of formation of subsets of abnormality parameters as well as due to formalization of the process of building decision functions and conditional detecting expressions, makes it possible to create the necessary set of detecting rules that are used to determine the levels of anomalous states characteristic of the action of a certain type of cyberattack. Based on the proposed methods and model, a methodology has been designed for constructing systems that detect anomalies generated by cyber-attacks, which, due to the mechanisms of attacking environments formation, those of creation of $m_i$-dimensional parametric reference and current sub-environments, those of $\alpha$-level nominalization of reference and current sub-environments, those of determination of identifying terms and formation of detecting environments, enables creating systems that are used to determine the level of an anomalous state in an $m$-dimensional heterogeneous parametric environment. A structure of a cyberattack detection system has been designed, which, due to the databases of cyberattacks, rules and references as well as current values formation module, $\alpha$-level nominalization, identifying terms, anomaly level and visualization, allows creating tools that would determine the anomalous state levels characteristic of the action of a certain type of cyberattack and enlarge the functionality of modern intrusion detection systems. Also, on the basis of the proposed methodology and the corresponding structural solution, an algorithmic support and a software model of a system for detecting anomalous states created by cyberattacks are designed. The model can be used either autonomously or to expand the functionality of modern intrusion detection systems. The conducted experiments confirmed the reliability of the theoretical principles and practical developments of the dissertation. The results of the study have been adopted by the Saifer BIS Ltd Company. They are also used in the educational process at the Department of Data Protection Computerized Systems of the National Aviation University, at the Information Security Department of the Institute of Information and Telecommunications Technologies of K.I. Satbayev Kazakh National Research Technical University and at the Department of Computer Science and Automatics of the University (Technical-Humanistic Academy) of Bielsko-Biała, Poland.

**Key words:** attacks, cyber-attacks, anomalies, linguistic variables, fuzzy sets, fuzzy numbers, detection of cyber-attacks, detection of anomalies, intrusion detection systems, anomaly detection systems, attack detection systems, cyberattack detection systems.