УДК 004.056:323.1

д.т.н. Субач І.Ю. (ВІТІ)
Фесьоха В.В. (ВІТІ)

# МОДЕЛЬ ВИЯВЛЕННЯ АНОМАЛІЙ В ІНФОРМАЦІЙНО – ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ ОРГАНІВ ВІЙСЬКОВОГО УПРАВЛІННЯ НА ОСНОВІ НЕЧІТКИХ МНОЖИН ТА НЕЧІТКОГО ЛОГІЧНОГО ВИВОДУ

*В статті запропоновано модель виявлення аномалій в інформаційних мережах органів військового управління, в основу якої покладено теорію нечітких множин та нечіткого логічного виводу.*

***Субач И.Ю., Фесёха В.В. Модель обнаружения аномалий в информационных сетях органов военного управления на основе нечеткой логики.*** *В статье предложена модель выявления аномалий в информационных сетях органов военного управления, в основу которой положена теория нечетких множеств и нечеткого логического вывода.*

***I. Subach, V. Fesokha The model of the anomalies detection in information networks of military control agencies based on fuzzy logic.*** *The article proposes a model for the detection of anomalies in the information networks of military command agencies, which is based on the theory of fuzzy sets and fuzzy logical inference.*

***Ключові слова:*** *кібернетичні вторгнення, системи запобігання вторгненням, виявлення аномалій, нечітка логіка, нечіткий шаблон нормальної поведінки.*

**Актуальність та постановка завдання в загальному вигляді.** Основним оборонним засобом інформаційно-телекомунікаційних систем та мереж (ІТСМ) від інформаційно-руйнівних впливів (втручань) у вигляді кібернетичних вторгнень (КВ) є системи виявлення та/або запобігання вторгненням (СВВ/СЗВ/СВА), основна задача яких зводиться до оперативної їх ідентифікації (встановлення відповідності між об’єктом і його ідентифікатором (унікальним атрибутом) [1]) та в ідеальному випадку ініціювання ефективного захисного сценарію щодо припинення факту порушення конфіденційності, доступності та цілісності інформаційних ресурсів, сервісів.

Практика застосування СВВ сформувала два напрямки протидії КВ: виявлення зловживань (*Misuse detection*) та виявлення аномалій (*Anomaly detection*). Перший підхід орієнтований на виявлення лише класифікованих (відомих) вторгнень на основі підходів синтаксичного порівняння відповідності структурних (сигнатур/патернів), інваріантних та кореляційних ознак виконуваного процесу (системи) з існуючою базою відомих шаблонів. Головними недоліками такого підходу є неможливість виявлення нових модифікацій КВ чи кібернетичних атак нульового дня (0-*day*) та неможливість автоматичного вводу нових шаблонів, що свідчить про їх достатньо малу ефективність. Другий підхід, навпаки, зводиться до задачі виявлення невідомих КВ на основі знаходження набору ознак, який не відповідає очікуваній поведінці об’єкта (користувача/системи) – шаблони характеристик, які не задовольняють визначеному поняттю нормальної поведінки фіксуються як аномалії [2 – 4].

Завдяки високій продуктивності та майже повній відсутності хибних спрацьовувань найбільш розвинутим та застосованим став підхід виявлення зловживань, проте його функціонал не дозволяє вирішити найбільш пріоритетні проблеми ідентифікації КВ, такі як адаптивність до них та неможливість їх визначення на початкових етапах. Саме тому пошук більш ефективних методів виявлення аномалій являється пріоритетною науковою задачею.

Це пов’язано з тим, що більшості існуючих рішень виявлення аномалій притаманний досить великий відсоток хибних спрацьовувань у зв’язку з нечітким визначенням межі між нормальною і аномальною поведінкою, складністю маркування даних для навчання моделей, пошуком взаємозв’язків і закономірностей у телеметрії мережевого трафіку, виявленням активності, подібної до навчальної вибірки, що власне є відхиленням від ідеї виявлення невідомих КВ [5].

Для вирішення даної задачі в контексті підвищення ефективності застосування СВВ до виявлення аномалій в ІТСМ цілком доцільним є застосування методів, які найбільш повно відповідають вимогам сучасності і є одночасно верифікованими, адаптивними та стійкими: експертні системи та методи на основі нечіткої логіки [2].

Апарат нечітких множин дозволяє вести математичну обробку формалізованої якісної інформації, а результати обробки можуть бути представлені в математичній формі. Переваги методології експертних систем дозволять зберігати важкоформалізуємий досвід експертів у формі моделі, а також накопичувати та систематизувати його. Поряд з цим, вибір апарату нечітких множин та нечіткої логіки не обмежується лише цим, оскільки для наявності лінгвістичної невизначеності, обумовленої присутністю людського фактора, вербального опису досліджуваних об'єктів та складності маркування даних для навчання моделей, найбільш придатними є методи нечіткого моделювання.

Вибір рішення в умовах невизначеності виникає в тому випадку, коли з кожним прийнятим рішенням пов'язана деяка множина можливих результатів. Тому використання апарату нечітких множин та нечіткої логіки при розробці бази знань та механізмів виведення експертної системи дозволить формалізувати процедуру оцінки стану ІТСМ на базі фрагментарної і часто неточної інформації.

У зв'язку з цим задача підвищення ефективності застосування СВВ на основі розробки та впровадження нових моделей виявлення аномалій на основі теорії нечітких множин та нечіткої логіки є актуальною.

**Аналіз останніх досліджень і публікацій** [2 – 9] показав, що гібридизація підходів математичного апарату нечіткої логіки та експертних систем отримала досить широке застосування не тільки в області автоматизації технологічних процесів, медицини, менеджменту, електроенергетики, а й в предметній області кібернетичного захисту в руслі виявлення кібернетичних вторгнень та дозволив досягнути більше 90 % спрацьовувань системи на них. Проте, запропоновані рішення в роботах [6 – 9] базуються на специфічному формулюванні проблематики (виявленням активності, подібної до навчальної вибірки) та обмеженні природи аналізованих даних (мають суттєві обмеження в руслі дослідження об'єму мережевого трафіка та категорій вже класифікованих КВ (відмова в обслуговуванні, атаки на користувача з найвищими привілеями, зондування мережі)), що не дозволяє охопити усієї множини проблемної області виявлення аномалій.

У зв'язку з цим, виникає завдання розробки моделі виявлення аномалій на основі нечітких множин та нечіткого логічного виводу, яка на відміну від існуючих моделей дозволить вирішити розглянуту проблематику для найбільш ефективного детектування аномалій у ІТСМ.

**Метою статті є** побудова моделі виявлення аномалій в інформаційно-телекомунікаційних мережах органів військового управління на основі нечітких множин та нечіткого логічного виводу.

Для формулювання та вирішення задачі нечіткої ідентифікації аномалій в ІТСМ, пропонуємо підхід, який висвітлений у [10 – 12], згідно якого процес прийняття рішення про факт наявності/відсутності аномалій (вихідний параметр $y$) на основі вищеописаних кількісних (якісних) інформативних ознак (вхідні параметри $\{x_1,...,x_i,...,x_n\}$) за умови наявності причинно-наслідкової залежності:

$$y = f_y\{x_1,...,x_i,...,x_n\}, i = \overline{1,n} \quad (1)$$

зводиться до задачі знаходження виразу:

$$X^* = (x_1^*, x_2^*,..., x_n^*) \to y = d_j \in D = (d_1^*, d_2^*,..., d_m^*), i = \overline{1,n},\ j = \overline{1,m} \quad (2)$$

В якості досліджуваного об'єкта в умовах функціонування ІТСМ, для якого буде визначатись поняття аномального стану на основі аналізу сукупності деяких параметрів може виступати як телеметрія мережевого трафіка, *log (pcap)*-файли СВВ так і їх комбінація.

Для встановлення залежності (1) між аналізованим трафіком та результатом аналізу, вхідні і вихідну змінні розглядаємо як лінгвістичні [12], що задані в наступних універсальних множинах для кількісних параметрів:

$$X_i = \underline{x_i}, x_i\ , i = 1, n \quad (3)$$

$$Y = \underline{y}, \overline{y} \quad (4)$$

де $X_i$ – множина всіх можливих параметрів досліджуваного мережевого трафіка, $Y$ – множина усіх можливих рішень щодо наявності аномалій в ІТСМ, $\underline{x}_i$ $\overline{x}_i$ та $\underline{y}, \overline{y}$ – нижні (верхні) границі значень вхідних та вихідної змінної

якісних параметрів:

$$X_i = v_i^1, v_i^2, \ldots, v_i^{q_i}, i = 1, n \quad (5)$$

$$Y = y^1, y^2, \ldots, y^{q_m} \quad (6)$$

де $v_i^1$ $v_i^{q_i}$ та $y^1$ $y^{q_m}$ – бальна оцінка, що відповідає мінімальному (максимальному) значенню $x_i/y$, де $q_i, i = 1, n$ та $q_m$ – потужності множин (5) и (6).

Для оцінки лінгвістичних змінних $x_i, i = \overline{1, n}$ та $y$ використовуються якісні терми з наступних терм-множин:

$A_i = a_i^1, a_i^2, \ldots, a_i^{l_i}$ – терм-множина $x_i, i = \overline{1, n}$,

$D = d_1, d_2, \ldots, d_m$ – терм-множина $y$, де $a_i^p$ – $p$-й лінгвістичний терм $x_i, p = \overline{1, l_i}, i = \overline{1, n}$; $d_j$ – $j$-й лінгвістичний терм $y$;

$m$ – кількість можливих значень змінної $y$ у встановленій області її значень.

Оскільки лінгвістичні терми $a_i^p \in A_i$, $d_j \in D$, $p = \overline{1, l_i}, i = \overline{1, n}$, $j = \overline{1, m}$ можливо представити як нечіткі множини $a_i^p$ і $d_j$ на основі досвіду у [11,12], що задані на універсальних множинах $U_i$ і $Y$ та визначаються виразами (3) – (4), то у випадку наявності кількісних $x_i, i = \overline{1, n}$ та $y$ вони будуть визначатися співвідношеннями:

$$a_i^p = \int_{x_i}^{\overline{x}_i} \mu^{a_i^p}(x_i) / x_i \quad (7)$$

$$d_j = \int_{\underline{y}}^{\overline{y}} \mu^{d_j}(y) / y \quad (8)$$

де $\mu^{a_i^p}(x_i)$ – функція приналежності значення $x_i \in \left[\underline{x}_i, \overline{x}_i\right]$ терму $a_i^p \in A_i, p = \overline{1, l_i}, i = \overline{1, n}$;

$\mu^{d_j}(y)$ – функція приналежності значення вихідної змінної $y \in \left[\underline{y}, \overline{y}\right]$ терму $d_j \in D, j = \overline{1, m}$.

У випадку наявності якісних $x_i, i = \overline{1, n}$ та $y$ нечіткі множини $a_i^p$ і $d_j$ будуть визначатися співвідношеннями:

$$a_i^p = \sum_{k=1}^{q_i} \mu^{a_i^p} \; v_i^k \; / v_i^k \quad (9)$$

$$d_j = \sum_{r=1}^{q_m} \mu^{d_j} \; y^r \; / y^r \quad (10)$$

де $\mu^{a_i^p} \; v_i^k$ – ступінь приналежності елемента $v_i^k \in U_i$ терму $a_i^p \in A_i$, $p = \overline{1, l_i}, i = \overline{1, n}$, $k = \overline{1, q_i}$; $\mu^{d_j} \; y^r$ – ступінь приналежності елемента $y^r \in Y$ терму $d_j \in D, j = \overline{1, m}$.

Лінгвістична оцінка всіх (вхідних/вихідної) змінних і необхідних для їх формалізації функцій приналежності є першим етапом побудови нечіткої моделі ідентифікації аномалій ІТСМ, оскільки дозволяє визначити тільки показник їх належності терму відповідної терм-множини.

Для реалізації наступного етапу варто представити знання експерта кібернетичної безпеки з нечіткої бази правил у вигляді композиційної таблиці:

*Таблиця* 1

**Композиційна таблиця знань нечіткої бази правил СВВ**

| Номер вхідної комбінації | Вхідні змінні (телеметрія мережевого трафіка) | | | | Вихідна змінна $y$ (нечіткий висновок виявлення аномалії) |
|---|---|---|---|---|---|
| | $x_1$ | $x_2$ | …$x_1$… | $x_n$ | |
| 11<br>12<br>…<br>$1k_1$ | $a_1^{11}$<br>$a_1^{12}$<br>…<br>$a_1^{1k_1}$ | $a_2^{11}$<br>$a_2^{12}$<br>…<br>$a_2^{1k_1}$ | … $a_i^{11}$ …<br>… $a_i^{12}$ …<br>… … …<br>… $a_i^{1k_1}$ … | $a_n^{11}$<br>$a_n^{12}$<br>…<br>$a_n^{1k_1}$ | $d_1$ |
| … | … | … | … | … | … |
| $j1$<br>$j2$<br>…<br>$jk_j$ | $a_1^{j1}$<br>$a_1^{j2}$<br>…<br>$a_1^{jk_j}$ | $a_2^{j1}$<br>$a_2^{j2}$<br>…<br>$a_2^{jk_j}$ | … $a_i^{j1}$ …<br>… $a_i^{j2}$ …<br>… … …<br>… $a_i^{jk_j}$ … | $a_n^{j1}$<br>$a_n^{j2}$<br>…<br>$a_n^{jk_j}$ | $d_j$ |
| … | … | … | … | … | … |
| $m1$<br>$m2$<br>…<br>$mk_m$ | $a_1^{m1}$<br>$a_1^{m2}$<br>…<br>$a_1^{mk_m}$ | $a_2^{m1}$<br>$a_2^{m2}$<br>…<br>$a_2^{mk_m}$ | … $a_i^{m1}$ …<br>… $a_i^{m2}$ …<br>… … …<br>… $a_i^{mk_m}$ … | $a_n^{m1}$<br>$a_n^{m2}$<br>…<br>$a_n^{mk_m}$ | $d_m$ |

де $x$ – вхідна лінгвістична змінна, що відповідає певному параметру мережевого трафіка (наприклад, рівень відхилення трафіка від шаблону нормальної поведінки), $a$ – нечіткий терм змінної $x$ (наприклад, “високий рівень”), $d$ – терм нечіткого логічного рішення для лінгвістичної вихідної змінної $y$ на основі $x$, нечітких термів для кожного досліджуваного параметра мережевого трафіка, які відповідають значенню $d_j$ результативної змінної $y$; $m$ – потужність множини значень $y$.

Таким чином, шукане відношення (1) формалізується у вигляді системи нечітких логічних тверджень типу „ЯКЩО-ТО, ІНАКШЕ”, побудованої на базі таблиці 1:

ЯКЩО ( $x_1 = a_1^{11}$ ) І ( $x_2 = a_2^{11}$ ) І…І ( $x_n = a_n^{11}$ ) АБО
( $x_1 = a_1^{12}$ ) І ( $x_2 = a_2^{12}$ ) І…І ( $x_n = a_n^{12}$ ) АБО
( $x_1 = a_1^{1k_1}$ ) І ( $x_2 = a_2^{1k_1}$ ) І…І ( $x_n = a_n^{1k_1}$ ) ТО
$y = d_1$ , ІНАКШЕ
ЯКЩО ( $x_1 = a_1^{21}$ ) І ( $x_2 = a_2^{21}$ ) І…І ( $x_n = a_n^{21}$ ) АБО
( $x_1 = a_1^{22}$ ) І ( $x_2 = a_2^{22}$ ) І…І ( $x_n = a_n^{22}$ ) АБО
( $x_1 = a_1^{2k_2}$ ) І ( $x_2 = a_2^{2k_2}$ ) І…І ( $x_n = a_n^{2k_2}$ ) ТО
$y = d_2$ , ІНАКШЕ
ЯКЩО ( $x_1 = a_1^{m1}$ ) І ( $x_2 = a_2^{m1}$ ) І…І ( $x_n = a_n^{m1}$ ) АБО
( $x_1 = a_1^{m2}$ ) І ( $x_2 = a_2^{m2}$ ) І…І ( $x_n = a_n^{m2}$ ) АБО
( $x_1 = a_1^{mk_m}$ ) І ( $x_2 = a_2^{mk_m}$ ) І…І ( $x_n = a_n^{mk_m}$ ) ТО
$y = d_m$.

З використанням операцій $\cup$ (АБО) $\cap$ (І) система логічних висловлювань приводиться до наступного вигляду:

$$\bigcup_{p=1}^{k_j}\left[\bigcap_{i=1}^{n} x_i = a_i^{jp}\right] \to y = d_j,\ j = \overline{1,m} \tag{11}$$

Таким чином, шукане відношення (1), що встановлює взаємозв'язок між параметрами мережевої телеметрії, яка збирається інтелектуальним мережевим обладнанням та висновком про наявність аномалії, формалізовано у вигляді системи нечітких логічних висловлювань (11), побудованих на даній матриці знань.

Для розрахунку значення функцій приналежності різних рішень при фіксованих значеннях вхідних змінних, зв'язок між функціями приналежності вхідного параметра $x_i$ та вектора $x_1^*, x_2^*, \ldots, x_n^*$ рішенню $y$ може бути представлений у вигляді наступних рівнянь:

$$\begin{aligned}
\mu^{d_1}\ x_1, x_2, \ldots, x_n &= \mu^{11}(x_1) \wedge \mu^{11}(x_2) \wedge \ldots \wedge \mu^{11}(x_n) \vee \\
&\vee \mu^{12}(x_1) \wedge \mu^{12}(x_2) \wedge \ldots \wedge \mu^{12}(x_n) \vee \ldots \\
&\ldots \vee \mu^{1k_1}(x_1) \wedge \mu^{1k_1}(x_2) \wedge \ldots \wedge \mu^{1k_1}(x_n), \\
\mu^{d_2}\ x_1, x_2, \ldots, x_n &= \mu^{21}(x_1) \wedge \mu^{21}(x_2) \wedge \ldots \wedge \mu^{21}(x_n) \vee \\
&\vee \mu^{22}(x_1) \wedge \mu^{22}(x_2) \wedge \ldots \wedge \mu^{22}(x_n) \vee \ldots \\
&\ldots \vee \mu^{2k_2}(x_1) \wedge \mu^{2k_2}(x_2) \wedge \ldots \wedge \mu^{2k_2}(x_n), \\
\mu^{d_m}\ x_1, x_2, \ldots, x_n &= \mu^{m1}(x_1) \wedge \mu^{m1}(x_2) \wedge \ldots \wedge \mu^{m1}(x_n) \vee \\
&\vee \mu^{m2}(x_1) \wedge \mu^{m2}(x_2) \wedge \ldots \wedge \mu^{m2}(x_n) \vee \ldots \\
&\ldots \vee \mu^{mk_m}(x_1) \wedge \mu^{mk_m}(x_2) \wedge \ldots \wedge \mu^{mk_m}(x_n),
\end{aligned} \tag{12}$$

де $\wedge$ – логічне І, $\vee$ – логічне АБО.

Нечіткі логічні рівняння отримано шляхом заміни в них лінгвістичних термів відповідними функціями приналежності, а операції $\bigcap$ та $\bigcup$ – на $\wedge$ та $\vee$. В загальному вигляді система нечітких логічних висловлювань про рішення виглядає наступним чином:

$$\mu^{d_j}\ x_1, x_2, \ldots, x_n = \bigvee_{p=1}^{k_j}\left[\bigwedge_{i=1}^{n} \mu^{jp}(x_i)\right],\ j = \overline{1,m} \tag{13}$$

Таким чином, на основі (13) в якості прийнятого рішення обирається результат з найбільшим значенням функції приналежності.

В якості прикладу аномалії в ІТСМ розглянемо КВ, метою якого є виведення з ладу мережевої служби сервера для унеможливлення надання ним певного сервісу користувачам. Для цього зловмисником на адресу вузла-жертви надсилається велика кількість пакетів з метою переповнення каналу обслуговування.

Задача ідентифікації аномалії у контексті викладеного полягає в тому, щоб на основі (13) множині характерних ознак даного шкідливого програмного забезпечення (ПЗ), що спостерігаються в системі, засобами математичного апарату нечіткої логіки аналітично поставити у відповідність рішення щодо її виявлення. Для формалізації знань експертів по даному КВ опишемо лінгвістичні змінні, кожна з яких характеризує одну з компонент вектора параметрів вхідних змінних на основі класичної схеми застосування функцій приналежності *Z,S* – подібного (початок/кінець діапазону значень) – (14), трикутного та трапецеїдального (проміжні значення діапазону значень) – (15) вигляду:

*count_packages* – час надходження (кількість в секунду) пакетів, {"Н – низька [100,400]", "С – середня [350,550,800]", "В – велика [700,1000]"} на універсумі [0,1000];

*percent_ip* – відсоток зовнішніх *ip*-адес, {"Н – низький [0,25]", "нС – нижче середнього [20,30,40]", "С – середній [40,45,55,65]", "вС – вище середнього [60,70,80]", "В – високий [80,100]"} на універсумі [0,100];

*percent_bad_packages* – відсоток пакетів з пошкодженими заголовками, {"Н – низький [0,25]", "нС – нижче середнього [20,30,40]", "С – середній [40,45,55,65]", "вС – вище середнього [60,70,80]", "В – високий [80,100]"} на універсумі [0,100];

та результату (прийнятого рішення):

$d_1$ – нормальний стан мережевої служби сервера.

$d_2$ – програмний (апаратний) збій мережевої служби сервера.

$d_3$ – аномалія, що відповідає ознакам розглянутого КВ.

$$\mu^{a_i^p}(x)=\begin{cases}1, x\le a\\ \dfrac{x-a}{b-a}, a<x<b\\ 0, x\ge b\end{cases}\qquad \mu^{a_i^p}(x)=\begin{cases}0, x\le a\\ \dfrac{x-a}{b-a}, a<x<b\\ 1, x\ge b\end{cases} \tag{14}$$

$$\mu^{a_i^p}(x)=\begin{cases}0, x\le a\\ \dfrac{x-a}{b-a}, a\le x<b\\ \dfrac{c-x}{c-b}, b\le x\le c\\ 0, c\le x\end{cases}\qquad \mu^{a_i^p}(x)=\begin{cases}\dfrac{x-a}{b-a}, a\le x<b\\ 1, b\le x<c\\ \dfrac{d-x}{d-c}, c\le x\le d\\ 0, x\notin(a,d)\end{cases} \tag{15}$$

Нечіткий шаблон опису допустимого стан мережевої служби сервера на основі вищевказаних показників для описаних рішень експертами в галузі кібернетичної безпеки складається з наступних правил, представлених таблиці 2:

*Таблиця* 2

**Визначені термів для кожної терм-множини**

| Лінгвістичні змінні | | | Висновок |
|---|---|---|---|
| *count_packages* | *percent_ip* | *percent_bad_packages* | *y* |
| *H* | *B* | *H* | $d_1$ |
| *C* | *B* | *H* | |
| *B* | *H* | *B* | $d_2$ |
| *B* | *H* | *B* | |
| *B* | *B* | *H* | $d_3$ |
| *B* | *H* | *B* | |

Функції приналежності для деякого фіксованого вектора значень вхідних змінних: $X^*$ = < *count_packages*, percent_ip*, percent_bad_packages** >=< 901, 93, 19> представлено у зведеній таблиці 3:

*Таблиця* 3

**Результати обчислень ступеню приналежності вхідного вектора**

| | $x_i^*$ | $\mu^H(x_i^*)$ | $\mu^{нС}(x_i^*)$ | $\mu^C(x_i^*)$ | $\mu^{вС}(x_i^*)$ | $\mu^B(x_i^*)$ |
|---|---|---|---|---|---|---|
| *count_packages* | 901 | 0 | | 0 | | 0.67 |
| *percent_ip* | 93 | 0 | 0 | 0 | 0 | 0.65 |
| *percent_bad_packages* | 19 | 0.76 | 0 | 0 | 0 | 0 |

З метою визначення максимальної відповідності досліджуваних ознак мережевої служби сервера (досліджуваного вектора) до шаблону нормальної поведінки системи обчислюємо багатомірні функції приналежності на основі (13) для всіх значень висновку $y$ ,а логічні операції кон'юнкції та диз'юнкції замінюємо на нечіткі кон'юнкцію та диз'юнкцію на основі максимінного підходу:

$$\mu(a)\wedge\mu(b)=\min[\mu(a),\mu(b)],$$
$$\mu(a)\vee\mu(b)=\max[\mu(a),\mu(b)].$$

$\mu^{d_1}\ X^*\ =(0\wedge 0.65\wedge 0.76)\vee(0\wedge 0.65\wedge 0.76)=0.$ $\mu^{d_2}\ X^*\ =(0.67\wedge 0\wedge 0)\vee(0.67\wedge 0\wedge 0)=0.$

$\mu^{d_3}\ X^*\ =(0.67\wedge 0.65\wedge 0.76)\vee(0.67\wedge 0\wedge 0)=0.65.$

Шуканим результатом проведених розрахунків буде значення $d_j$, функція приналежності якого максимальна, тобто $\mu^{d_3}$, що відповідає ознакам розглянутого КВ.

Розглянутий приклад демонструє можливості застосування запропонованої в статті моделі для виявлення аномалій в роботі інформаційно-телекомунікаційної системи її адміністратором безпеки.

**Висновки:** Таким чином, отримала подальшого розвитку модель виявлення аномалій в роботі інформаційно-телекомунікаційних систем органів військового управління, яка ґрунтується на застосуванні математичного апарату теорії нечітких множин та нечіткого логічного виводу та, на відміну від відомих, дозволяє обробляти кількісні та якісні дані про параметри функціонування системи для ідентифікації на ранніх стадіях більш широкого кола несанкціонованих кібернетичних втручань в її роботу. Перспективними напрямками подальших наукових досліджень є удосконалення запропонованої моделі шляхом застосування ваг до нечітких правил бази знань, що характеризуватимуть впевненість експерта з кібернетичної безпеки у кожному обраному для прийняття рішення правилі та розробці методики застосування запропонованої моделі ідентифікації кібернетичних атак на інформаційно-телекомунікаційні мережі органів військового управління.

ЛІТЕРАТУРА

1. ТЗІ 1.1-003–99. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу – Київ: ДСТСЗІ СБУ, 1999. – 38 с.

2. Субач І.Ю. Аналіз існуючих рішень запобігання вторгненням в інформаційно-телекомунікаційні мережі, відкритих на основі загальнодоступних ліцензій / І. Ю. Субач, В. В. Фесьоха, Н. О. Фесьоха. // Збірник наукових праць ІСЗЗІ. – 2017. – № 5 (1).

3. Басараб М.А. Обнаружение аномалий в информационных процессах на основе мультифрактального анализа / М.А. Басараб, И.С. Строганов. // Вопросы кибербезопасности. – 2014. – №4 (5). – С. 30 – 40.

4. Kumar, V. Parallel and distributed computing for cybersecurity / V. Kumar //IEEE Distributed Systems Online. – 2005. – Vol. 6, №. 10.

5. Браницкий А. А. Анализ и классификация методов обнаружения сетевых атак / А. А. Браницкий, И. В. Котенко. // Труды СПИИРАН. – 2016. – №45. – С. 207 – 244.

6. Shanmugavadivu R. Network intrusion detection system using fuzzy logic / R. Shanmugavadivu, N. Nagarajan. // Indian Journal of Computer Science and Engineering (IJCSE), ISSN : 0976-5166. – 2011. – Vol. 2, №1. – С. 101 – 111.

7. Anomaly Detection Using Cooperative Fuzzy Logic Controller / [A. Feizollah, S. Shamshirband, N. Anuar та ін.]. // Communications in Computer and Information Science. – 2013.

8. Ажмухамедов И. М. Определение аномалий объема сетевого трафика на основе апарата нечетких множеств / И. М. Ажмухамедов, А.Н. Марьянков. // Вестник АГТУ. – 2011. – № 1 (51).

9. Слеповичев И.И. Обнаружение DDoS атак нечеткой нейронной сетью / [И.И. Слеповичев, П.В. Ирматов, М.С. Комарова]. // Известия Саратовского университета. Математика. Механика. Информатика. – 2009. – №3.

10. Ротштейн А. П. Медицинская диагностика на нечеткой логике / А. П. Ротштейн. – Винница: Континент– ПРИМ, 1996. – 132 с.

11. Мітюшкін Ю. І. Soft Computing: ідентифікація закономірностей нечіткими базами знань / Ю. І. Мітюшкін, Б. І. Мокін, О. П. Ротштейн // Монографія. – Вінниця: УНІВЕРСУМ-Вінниця. – 2002. – 145 с.

12. Заде Л. Понятие лингвистической переменной и его применение к принятию приближенных решений / Л. Заде. – М.: Мир, 1976. – 167 с.