2 Забазпечення комп'ютерної безпеки в державних, банківських та інших інформаційних системах

УДК 004.56.021.2: 510.22 (045)

НЕЧІТКІ МОДЕЛІ СИСТЕМ ВИЯВЛЕННЯ АТАК

Віталій Бабак, Олександр Корченко, Євгенія Паціра
Національний авіаційний університет

Анотація: **Запропоновані нечіткі моделі для систем виявлення атак, заснованих на нечітких еталонах та евристичних правилах.**
Summary: **Suggested fuzzy sets for attacks discover systems are founded on the fuzzy benchmarks and heuristic rules.**
Ключові слова: **Нечіткі множини, системи виявлення атак, евристичні правила.**

I Вступ

Захист комп'ютерних систем (КС) від атак тісно пов'язаний з розробкою та використанням засобів їх виявлення. Процес ідентифікації атак можна здійснювати мануально (наприклад, систематичним аналізом даних журналізації), що безсумнівно буде пов'язано з великою рутинною роботою фахівця відповідної галузі. Часто об'єми аналізованих даних можуть збільшитись до таких меж, що експерту для їх вивчення може не вистачити 24 години на добу. В додаток до цього в процесі такого аналізу збільшується вірогідність виникнення помилок. Автоматизація процесу ідентифікації може бути реалізована за допомогою відповідних систем аналізу, методам і засобам побудови яких присвячена низка робіт [1 – 4]. Такі системи будуються на технологіях виявлення зловживань та аномалій. Перші (найбільш поширені) подібні до антивірусних систем, заснованих на сигнатурних технологіях, за якими здійснюється пошук відомих шаблонів атак, другі – ґрунтуються на виявленні ознак, що виникли в КС, і за якими приховується ворожа діяльність. Недолік систем виявлення зловживань у тому, що вони не здатні розпізнавати невідомі для них сигнатури (правила). З цих позицій системи на технологіях виявлення аномалій (які в основному ґрунтуються на профілях підозрілої діяльності) позбавлені зазначених недоліків і їх розвиток в останні роки набуває особливої актуальності.

II Постановка задачі

В роботах [1 – 5] описуються і аналізуються системи виявлення аномалій (які за своєю суттю в основному ґрунтуються на статистичних методах), а також визначаються їх недоліки, в основному пов'язані з проблемами обробки даних, що представляють нечітко визначені чинники. Математичний апарат, який дозволить уникнути зазначених в роботах недоліків при створенні технологій виявлення аномалій – це теорія нечіткості [6 – 10], ефективність використання якої була показана при побудові систем експертного оцінювання у сфері захисту інформації [11]. У цьому зв'язку за мету роботи поставлена розробка (на основі зазначеної теорії) моделей, призначених для побудови систем детектування атак на КС в умовах нечіткості.

III Модель формування нечітких еталонів

Інформація, що лягає в основу побудови нечітких моделей і систем виявлення аномалій, може бути подана у різних формах, наприклад, у вигляді різних важко пояснювальних проблем, що виникли в КС, діапазонів порогових значень, параметрів вхідного та вихідного трафіка, а також, непередбачених адрес пакетів, атрибутів, часових параметрів, запитів тощо. Типові моделі нечітких систем виявлення атак засновуються на процесах формування джерела даних, визначенні набору нечітких параметрів, побудові нечітких еталонів, формуванні поточних нечітких значень, генерації нечітких евристичних правил та визначенні на їх основі показника стану безпеки КС. Одною з важливих задач, покладених на системи виявлення атак, є визначення того, що порти КС піддаються скануванню. З цього погляду побудуємо модель формування нечітких еталонів на прикладі вирішення зазначеної задачі.

Для організації процесу формування джерела даних використаємо окремі параметри мережевого трафіка, які в подальшому будуть застосовані для визначення набору нечітких параметрів. Для цього введемо поняття віртуального каналу (ВК). Такий канал, наприклад, для Інтернет-протоколу породжується

в момент одержання адресатом (за конкретним портом) IP-пакета і після з'єднання існує деякий заданий час. Ознакою того, що створено новий ВК, служить надходження IP-пакета на порт, для якого такий канал поки не існував. Число ВК залежить від апаратних і програмних можливостей КС і має максимальне значення $max_{КВК}$. Якщо визначена кількість можливих для доступу портів в КС дорівнює 65536, то таким буде і значення $max_{КВК}$.

Будь-який ВК будемо характеризувати параметром "час життя" (ЧЖ), за яким визначається скільки каналу залишається існувати. Зазначимо, що в момент створення ВК параметру ЧЖ привласнюється значення $ЧЖ_0$, яке, наприклад, може визначатися із діапазону $ЧЖ_0 \in [1;10]$ хв. Після закінчення цього терміну канал припинить своє існування, а ЧЖ набуде значення 0. При кожному черговому проходженні цим каналом IP-пакета значення ЧЖ збільшується на ΔЧЖ, наприклад, ΔЧЖ = 100 мс. Таким чином, якщо каналом здійснюється передавання незначної кількості пакетів, то ЧЖ відносно $ЧЖ_0$ може зменшуватися дуже повільно, а при інтенсивному трафіку постійно збільшуватися, що дозволить каналу довго існувати. Якщо в певний момент часу обмін буде призупинений, то через $ЧЖ_П$ ($ЧЖ_П$ – поточне значення ЧЖ) ВК припинить своє існування.

На рис. 1 показано приклад характеристик ЧЖ (за 320 хв.) окремих ВК ($N_{ВК}$ – номер ВК; t – час з інтервалом сканування 10 хв.) одного з вузлів мережі Інтернет, які далі будуть використані для формування нечітких параметрів. Невеликі кряжі у вигляді горизонтальних ланцюжків та поодинокі підвищення на всій площині ($N_{ВК}$, t) характеризують аномалії у трафіку вузла.

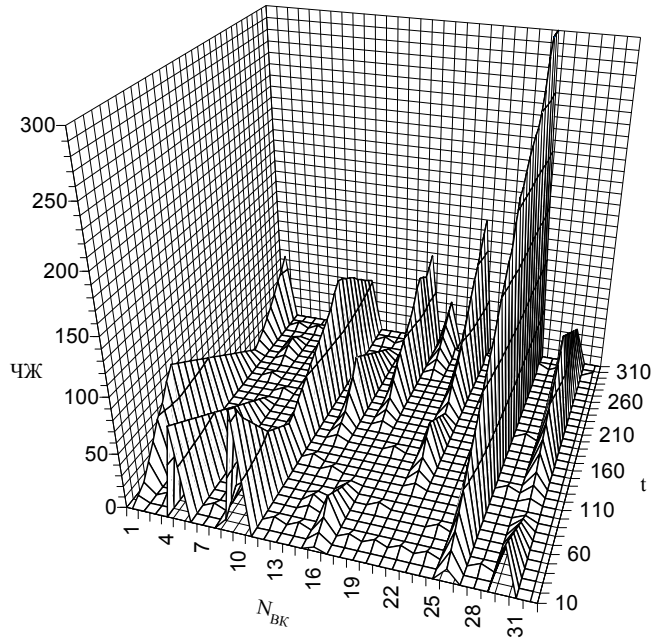

Рисунок 1 – Приклад характеристик ВК

Введемо наступну важливу характеристику – "ВІК ВК" (ВВК), тобто час, який минув з моменту його створення (народження). Отже, виходячи з властивостей ВК, чим інтенсивніший трафік, тим живучіший канал, при цьому значення ВВК постійно збільшується, а ЧЖ>>0. Далі введемо лінгвістичні змінні (ЛЗ) [6, 7, 11] "КІЛЬКІСТЬ ВІРТУАЛЬНИХ КАНАЛІВ" (**КВК**) і "ВІК ВІРТУАЛЬНОГО КАНАЛУ" (**ВВК**), які відповідно визначаються кортежами <КВК, $Т_{КВК}$, $Х_{КВК}$> і <ВВК, $Т_{ВВК}$, $Х_{ВВК}$>, для яких синтаксичне правило та семантична процедура не задані.

Тепер необхідно визначити введені ЛЗ і далі використати як еталони. Сформуємо це за такими етапами.

Для **КВК**. Етап 1 – формування базової терм-множини. Базову терм-множину задамо п'ятьма нечіткими термами $Т_{КВК} = \bigcup_{i=1}^{5} Т_{КВК_i}$ = {"дуже мала" (ДМ), "мала" (М), "середня" (С), "велика" (В), "дуже велика" (ДВ)}, які можуть бути відображені на універсальну множину $Х_{КВК} \in \{0, max_{КВК}\}$.

Множина термів $Т_{КВК}$ відображується нечіткими числами (НЧ) $\underset{\sim}{ДМ}$, $\underset{\sim}{М}$, $\underset{\sim}{С}$, $\underset{\sim}{В}$, $\underset{\sim}{ДВ}$, для яких

необхідно сформувати функцію належності (ФН) НЧ, наприклад, за допомогою методу лінгвістичних термів з використанням статистичних даних (МЛТС), вибір якого може бути обумовлений результатами досліджень в [11].

Етап 2 – формування ФН. Спираючись на МЛТС розглянемо приклад формування ФН НЧ всіх термів $T_{КВК}$ для вузла обчислювальної мережі. В емпіричній таблиці (див. табл. 1) зібрана статистика (за 24 години роботи) відносно ВК (див. рис. 1) для кожного із заданих термів, де N1, N2, N3, N4 і N5, відповідно, номера інтервалів [0; 2], [3, 8], [9; 16], [17; 64], [65; 256]. З практичної точки зору задамо $max_{КВК}$=256.

Таблиця 1 – Таблиця даних для формування $T_{КВК}$

Значення ЛЗ	Інтервал				
	N1	N2	N3	N4	N5
ДМ	3	1	0	0	0
М	1	2	1	0	0
С	0	1	3	0	0
В	0	0	2	4	1
ДВ	0	0	0	3	5

За аналогією з прикладом, описаним у [11], формуємо матрицю підказок за виразом $k_j = \bigvee_{j=1}^{5} \sum_{i=1}^{5} b_{ij}$ = {4, 4, 6, 7, 6}, де b_{ij} – елементи емпіричної таблиці. Перетворимо всі елементи матриці за виразом $c_{ij} = b_{ij} km/k_j$ ($i, j = \overline{1, 5}$), де $km = \bigvee_{j=1}^{5} k_j$ = 7, а

$$c_{ij} = \begin{matrix} 5,25 & 1,75 & 0 & 0 & 0 \\ 1,75 & 3,5 & 1,17 & 0 & 0 \\ 0 & 1,75 & 3,5 & 0 & 0 \\ 0 & 0 & 2,33 & 4 & 1,4 \\ 0 & 0 & 0 & 3 & 7. \end{matrix}$$

Далі обчислюємо ФН за виразом $\mu_{ij} = c_{ij}/cm_i$ ($i, j = \overline{1, 5}$), де $cm_i = \bigvee_{j=1}^{5} \bigvee_{i=1}^{5} c_{ij}$ = {5,25; 3,5; 3,5; 4; 7}. Обчислені значення ФН будуть такими:

$$\mu_{ij} = \begin{matrix} 1 & 0,33 & 0 & 0 & 0 \\ 0,5 & 1 & 0,5 & 0 & 0 \\ 0 & 0,33 & 1 & 0,67 & 0 \\ 0 & 0 & 0 & 1 & 0,75 \\ 0 & 0 & 0 & 0,2 & 1. \end{matrix}$$

Далі для $\bigvee_{i=1}^{5} \mu_{ij}$ відповідно знаходимо оцінні співвідношення $\bigvee_{i=1}^{5} \Delta B_i / B$ = {0,008; 0,031; 0,063; 0,25; 1} ($\Delta B/B$ – відхилення параметра $\Delta B_{КВК} \in [0, B_{КВК}]$, а $B_{КВК}$ – максимально можливе значення, яке характеризує поточні вимірювання) і отримуємо НЧ: $\underset{\sim}{ДМ}$ = {1/0,008; 0,33/0,031; 0/0,063; 0/0,25; 0/1}; $\underset{\sim}{М}$ = {0,5/0,008; 1/0,031; 0,5/0,063; 0/0,25; 0/1}; $\underset{\sim}{С}$ = {0/0,008; 0,33/0,031; 1/0,063; 0,67/0,25; 0/1}; $\underset{\sim}{В}$ = {0/0,008; 0/0,031; 0/0,063; 1/0,25; 0,75/1}; $\underset{\sim}{ДВ}$ = {0/0,008; 0/0,031; 0/0,063; 0,2/0,25; 1/1}.

Етап 3 – формування нечітких еталонів. Для формування нечітких еталонів необхідно щоб для $\forall T_{КВК_i}$ було справедливе відношення порядку, наприклад, при i=1, $\forall X_{ДМ}$ $X_{ДМ_k} < X_{ДМ_{k+1}}$. Далі одержані $T_{КВК}$

подаються у приведеній формі $T^{e}_{КВК}$, які і будуть використовуватися як еталонні значення для **КВК**. Наведена форма для НЧ $\underset{\sim}{X}=\{\mu_1/x_1;\ \ldots;\ \mu_i/x_i;\ \ldots;\ \mu_n/x_n\}$ утворюється за такими процедурами. Процедура 1. Поглинання супортом $0/x_{min}$ і $0/x_{max}$ відповідно всіх інших супортів за умовами $x_{min} = \bigvee\limits_{U_1 \equiv \forall x:\mu=0 \& X<X_M} x$ і $x_{max} = \bigwedge\limits_{U_2 \equiv \forall x:\mu=0 \& X<X_M} x$, де $U_1 \equiv \forall x:\mu=0 \& X<X_M$, $U_2 \equiv \forall x:\mu=0 \& X<X_M$, а X_M – мода $\underset{\sim}{X}$.

Процедура 2. Якщо після процедури 1 $\exists \underset{\sim}{X}$: не має $0/x_{min}$ або $0/x_{max}$, то їх формування здійснюється згідно з виразами $x_{min} = \bigwedge\limits_{i=1}^{p} x_i$ або $x_{max} = \bigvee\limits_{i=1}^{p} x_i$, де p – кількість супортів $\underset{\sim}{X}$.

Відповідно до визначених процедур приведення утворимо всі $T^{e}_{КВК}$:

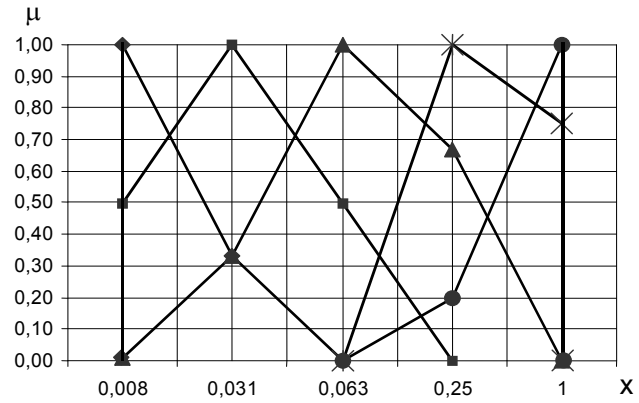

Рисунок 2 – Еталонні НЧ для КВК

$\underset{\sim}{ДМ}^{e}$ $\underset{\sim}{М}^{e}$ $\underset{\sim}{С}^{e}$ $\underset{\sim}{В}^{e}$ $\underset{\sim}{ДВ}^{e}$

$\underset{\sim}{ДМ}^{e}$ = {0/0,008; 1/0,008; 0,33/0,031; 0/0,063}; $\underset{\sim}{М}^{e}$ = {0/0,008; 0,5/0,008; 1/0,031; 0,5/0,063; 0/0,25}; $\underset{\sim}{С}^{e}$ = {0/0,008; 0,33/0,031; 1/0,063; 0,67/0,25; 0/1}; $\underset{\sim}{В}^{e}$ = {0/0,063; 1/0,25; 0,75/1; 0/1}; $\underset{\sim}{ДВ}^{e}$ = {0/0,063; 0,2/0,25; 1/1; 0/1}, графічне зображення яких наведено на рис. 2.

Для **ВВК**. Етап 1 – формування базової терм-множини. Базову терм-множину задамо трьома нечіткими термами $T_{ВВК} = \bigcup\limits_{i=1}^{3} T_{ВВК_i}$ {"молодий" (М), "середній" (СР), "старий" (СТ)}, які відображаються на універсальну множину $X_{ВВК} \in \{0, max_{ВВК}\}$. Множина термів $T_{ВВК}$ відображується НЧ $\underset{\sim}{М}$, $\underset{\sim}{СР}$, $\underset{\sim}{СТ}$ для яких сформуємо ФН. Етап 2 – формування ФН. На основі МЛТС сформуємо ФН НЧ всіх термів $T_{ВВК}$ для того ж вузла обчислювальної мережі. В емпіричній таблиці (див. табл. 2) зібрана статистика за 24 години роботи комп'ютера в мережі, де N1, N2, N3, відповідно, номера часових інтервалів (у хв.) [0;30], [30;100], [100; 250]. З практичної точки зору задамо $max_{ВВК}$=250.

Таблиця 2 – Таблиця даних для формування $T_{ВВК}$

Значення ЛЗ	Інтервал		
	N1	N2	N3
М	4	1	0
СР	2	5	1
СТ	1	2	6

Далі формуємо матрицю підказок за виразом $k_j = \bigvee_{j=1}^{3}\sum_{i=1}^{3} b_{ij}$, = {7, 8, 7} і перетворимо всі елементи матриці за виразом $c_{ij} = b_{ij}km/k_j$ ($i, j = \overline{1, 3}$), де $km = \bigvee_{j=1}^{3} k_j$ = 8, а

$$c_{ij} = \begin{matrix} 4{,}57 & 1 & 0 \\ 2{,}29 & 5 & 1{,}14 \\ 1{,}14 & 2 & 6{,}86. \end{matrix}$$

Далі знаходимо ФН $\mu_{ij} = c_{ij}/cm_i$ ($i, j = \overline{1,3}$), де $cm_i = \bigvee_{j=1}^{3}\bigvee_{i=1}^{3} c_{ij}$ = {4,57; 5; 6,86}:

$$\mu_{ij} = \begin{matrix} 1 & 0{,}2 & 0 \\ 0{,}5 & 1 & 0{,}17 \\ 0{,}25 & 0{,}4 & 1. \end{matrix}$$

Далі для $\bigvee_{i=1}^{3}\mu_{ij}$ знаходимо $\bigvee_{i=1}^{3}\Delta B_i / B$ = {0,12; 0,4; 1} (ΔB/B – відхилення параметра $\Delta B_{ВВК} \in [0, B_{ВВК}]$, де $B_{ВВК}$ – максимальне відхилення в поточному вимірюванні) і отримуємо НЧ: $\underset{\sim}{M}$ = {1/0,12; 0,5/0,4; 0,25/1}; $\underset{\sim}{CP}$ = {0,2/0,12; 1/0,4; 0,4/1}; $\underset{\sim}{CT}$ = {0/0,12; 0,17/0,4; 1/1}.

Етап 3 – формування нечітких еталонів. Для формування нечітких еталонів необхідно щоб для $\forall T_{ВВК_i}$ було справедливе відношення порядку, наприклад, при i=1, $\forall X_M$ $X_{M_k} < X_{M_{k+1}}$. Одержані $T_{ВВК}$ подамо у приведеній формі $T^e_{ВВК}$, яка для **ВВК** реалізується за процедурою 1, як у випадку з **КВК**, а процедура 2 наступна: якщо після процедури 1 не утворені $0/x_{min}$ і $0/x_{max}$, то відповідно формуємо маргінальні супорти $\mu_{X_{min}}/0$ і $\mu_{X_{max}}/1$, де $\mu_{X_{min}}$ і $\mu_{X_{max}}$ степені належності при мінімальному (X_{min}) і максимальному (X_{max}) носіях.

Тоді відповідно до цих процедур одержимо всі $T^e_{ВВК}$: $\underset{\sim}{M}^e$ = {1/0; 1/0,12; 0,5/0,4; 0,25/1}; $\underset{\sim}{CP}^e$ = {0,2/0; 0,2/0,12; 1/0,4; 0,4/1}; $\underset{\sim}{CT}^e$ = {0/0,12; 0,17/0,4; 1/1}, графічне відображення яких подано на рис. 3.

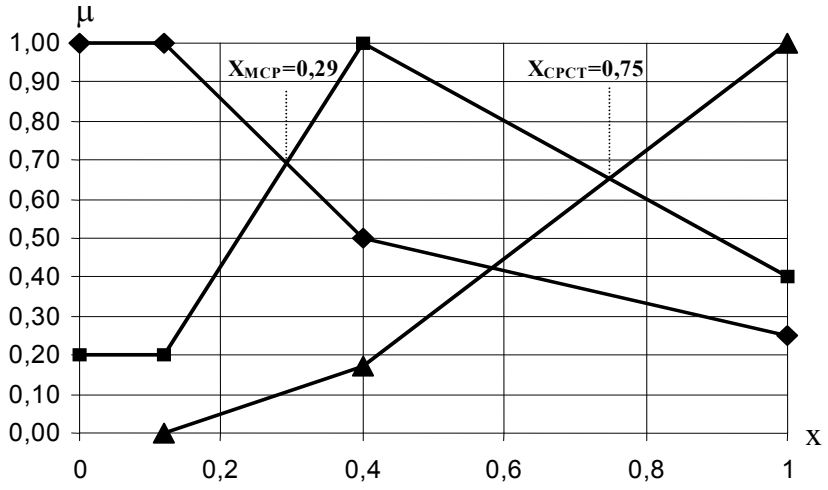

Рисунок 3 – Еталонні НЧ для ВВК

IV Модель виявлення атак на базі еталонів параметрів і евристичних правил

На основі отриманих **КВК** і **ВВК** з еталонними термами сформуємо для заданих моментів часу T=ЧЖ/max$_{ВВК}$ поточні значення **КВК** відносно **ВВК**, використовуючи побудовану на її основі кусковолінійну функцію:

$$\mu(T)=\begin{cases}1, & \text{якщо } T\in[0;X_{M1}],\ ]X_{CT3};1]\\ \text{entier}(\frac{1}{2}+10(\mu_{M1}+\frac{(\mu_{M2}-\mu_{M1})(T-X_{M1})}{X_{M2}-X_{M1}}))10^{-1}, & \text{якщо } T\in]X_{M1};X_{MCC}]\\ \text{entier}(\frac{1}{2}+10(\mu_{CPP}+\frac{(\mu_{CPP}-\mu_{CPP})(T-X_{CPP})}{X_{CPP}-X_{CPP}}))10^{-1}, & \text{якщо } T\in]X_{MCC};X_{CP2}]\\ \text{entier}(\frac{1}{2}+10(\mu_{CPP}+\frac{(\mu_{CPP}-\mu_{CPP})(T-X_{CPP})}{X_{CPP}-X_{CPP}}))10^{-1}, & \text{якщо } T\in]X_{CP2};X_{CPCT}]\\ \text{entier}(\frac{1}{2}+10(\mu_{CTT}+\frac{(\mu_{CTT}-\mu_{CTT})(T-X_{CTT})}{X_{CTT}-X_{CTT}}))10^{-1}, & \text{якщо } T\in]X_{CPCT};X_{CT3}],\end{cases} \quad (1)$$

де $X_{MCP}=\frac{K_1X_{M1}-K_2X_{CP1}+\mu_{CP1}-\mu_{M1}}{K_1-K_2}$, ($K_1=\frac{\mu_{M2}-\mu_{M1}}{X_{M2}-X_{M1}}$, $K_2=\frac{\mu_{CP2}-\mu_{CP1}}{X_{CP2}-X_{CP1}}$),

а $X_{CPCT}=\frac{K_1X_{CP2}-K_2X_{CT2}+\mu_{CT2}-\mu_{CP2}}{K_1-K_2}$, ($K_1=\frac{\mu_{CP3}-\mu_{CP2}}{X_{CP3}-X_{CP2}}$, $K_2=\frac{\mu_{CT3}-\mu_{CT2}}{X_{CT3}-X_{CT2}}$),

при цьому інтервали]0; X_{MCP}],]X_{MCP}; X_{CPCT}],] X_{CPCT}; 1] відповідно відображають поточні значення НЧ $\underset{\sim}{M}$, $\underset{\sim}{CP}$, $\underset{\sim}{CT}$.

Далі відповідно до ЧЖ $N_{ВК}$ (див. рис. 1) за формулою (1) визначимо μ(t) і занесемо їх в таблицю степенів належності, значення яких при деяких фіксованих t показані в табл. 3.

На основі повних даних, частина яких відображена в табл. 3, визначимо частоти зустрічальності поточних значень μ(t) для формування термів M, CP і CT при конкретних фіксованих μ (див. рис. 1) і одержані значення цих частот інтегруємо в таблиці. Оскільки для даної моделі використовуються величини терма M, то будемо використовувати тільки його дані (див. табл. 4).

Таблиця 3 – Степені належності при t ∈ {10, 30, 60, 190, 300, 320}

t	μ(t) для $N_{ВК}$ ∈ {1,32}																														
	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*	*17*	*18*	*19*	*20*	*21*	*22*	*23*	*24*	*25*	*26*	*27*	*28*	*29*	*30*	*31*	*32*
10					*0,8*				**1,0**	*1,0*						**1,0**										**1,0**				**0,9**		
30	**1,0**		**1,0**		*0,7*		**1,0**		**1,0**	*0,9*		**1,0**		**1,0**		**1,0**		**1,0**		**1,0**		**1,0**		**1,0**		**1,0**		**1,0**		**1,0**		
60	**0,9**				**0,8**				**1,0**	**0,8**				**1,0**		**1,0**								**1,0**		**0,8**				**1,0**		
190	**1,0**					**1,0**			**1,0**	**0,7**			**0,9**			**1,0**					**1,0**					0,7		**1,0**		**0,8**		
300	**0,9**		1,0		**1,0**		**1,0**		**1,0**	**0,8**		**1,0**		**1,0**		*0,7*		**1,0**	**1,0**		*1,0*	**1,0**		**1,0**		1,0	**1,0**		**1,0**	**0,9**		
320	**0,3**									**0,2**								**0,2**												**0,1**		

Примітка: значення μ(t) відображені напівжирним, курсивом та звичайним шрифтом відповідно відносяться до M, CP та CT ВК.

Таблиця 4 – Частоти зустрічальності значень μ(t) для терма М при заданих μ

μ	Частоти зустрічальності при фіксованих t ∈ {10; 320}																															
	10	*20*	*30*	*40*	*50*	*60*	*70*	*80*	*90*	*100*	*110*	*120*	*130*	*140*	*150*	*160*	*170*	*180*	*190*	*200*	*210*	*220*	*230*	*240*	*250*	*260*	*270*	*280*	*290*	*300*	*310*	*320*
0,7				1	1		1	1			1								1	1					1	1			1			
0,8					1	3	2					1	1	1		1	1	2	1					1	2	1	1	1		1	2	2
0,9	1	1		1	1	1	1	2	2	1			1	1	2	2	2		1	1	1	1	2	1					1	2	1	1
1,0	3	4	14	4	5	5	5	3	3	4	5	5	3	6	5	4	5	5	6	3	4	3	2	3	3	4	4	4	2	12	1	1

Далі зведемо повні сумарні дані частот зустрічальності значень μ(t) при фіксованих μ для термів М, СР і СТ (див. табл. 5).

На основі даних, представлених у табл. 5, використання апроксимаційних умов [11] і функцій для формування ЛЗ [8] та приведення відповідно до оцінного співвідношення ΔВ/В шляхом ділення на $\max_{КВК}$, можемо сформувати поточні НЧ за виразами:

КВК($\underset{\sim}{M}$) = {CON ($\Omega((\overset{4}{\underset{i=1}{Y}}\mu_{Mi}/x_{Mi})/\max_{КВК})$)} = {CON (Ω(($\mu_{M1}/x_{M1}$; μ_{M2}/x_{M2}; μ_{M3}/x_{M3}; μ_{M4}/x_{M4})/$\max_{КВК}$))} = {CON (Ω((0,7/10; 0,8/25; 0,9/31; 1,0/140)/$\max_{КВК}$))} = {0,49/0,039; 0,64/0,098; 0,8/0,121; 1,0/0,547}; КВК($\underset{\sim}{CP}$) = {CON ($\Omega((\overset{4}{\underset{i=1}{Y}}\mu_{CPi}/x_{CPi})/\max_{КВК})$)} = {CON (Ω(($\mu_{CP1}/x_{CP1}$; μ_{CP2}/x_{CP2}; μ_{CP3}/x_{CP3}; μ_{CP4}/x_{CP4}; μ_{CP5}/x_{CP5})/$\max_{КВК}$))} = {CON (Ω ((0,6/1; 0,7/10; 0,8/17; 0,9/11; 1,0/7)/$\max_{КВК}$))} = {0,36/0,004; 1,0/0,027; 0,81/0,043; 0,64/0,066}; КВК($\underset{\sim}{CT}$) = {CON ($\Omega((\overset{4}{\underset{i=1}{Y}}\mu_{CTi}/x_{CTi})/\max_{КВК})$)} = {CON (Ω(($\mu_{CT1}/x_{CT1}$; μ_{CT2}/x_{CT2}; μ_{CT3}/x_{CT3}; μ_{CT4}/x_{CT4})/$\max_{КВК}$))} = {CON (Ω ((0,7/1; 0,8/3; 0,9/4; 1,0/6)/$\max_{КВК}$))} = {0,49/0,004; 0,64/0,012; 0,81/0,016; 1,0/0,023}, де Ω – оператор формування НЧ на основі множин порядку і апроксимації відповідно до умов Ω_1 або Ω_2 (див. метод ЛАЛМ [11]). Графік поточних НЧ подано на рис. 4.

Таблиця 5 – Сумарні частоти зустрічальності для М, СР і СТ

μ	Частоти μ(t)		
	М (X_M)	СР (X_{CP})	СТ (X_{CT})
0,6	–	1	–
0,7	10	10	1
0,8	25	17	3
0,9	31	11	4
1,0	140	7	6

Отримані НЧ за допомогою функції упорядкування нечітких підмножин одиничного інтервалу (ФУП) [11] порівнюємо з еталонними $\underset{\sim}{ДМ}^e$, $\underset{\sim}{M}^e$, $\underset{\sim}{C}^e$, $\underset{\sim}{B}^e$ і $\underset{\sim}{ДВ}^e$ (рис. 2) для визначення до якого з них отримане НЧ найближче.

Для використання ФУП еталони і вищезазначене поточне НЧ КВК($\underset{\sim}{M}$) подамо у α-рівневому вигляді, при цьому необхідно задати крок дискретизації α (наприклад, k=0,1) і за аналогією з (1) і обмеженням за α_{min} апроксимуємо всі $T^e_{КВК}$ до значень, що мають мінімальну кількість точок перетину.

Апроксимацію будемо здійснювати за формулою $\underset{\sim}{X}^{eA} = \{\underset{\forall\mu(x)\ge\alpha_{min}}{Y}\mu(x)/x\}$, де $\alpha_{min} = \alpha_{ДММ} \vee \alpha_{МС} \vee \alpha_{СВ} \vee \alpha_{ВДВ} = 0{,}71 \vee 0{,}71 \vee 0{,}75 \vee 0{,}81 = 0{,}81$, де: $\alpha_{ДММ}$ =

$$\text{entier}\left(\frac{1}{2}+10\left(\frac{K_1\mu_{ДМ2}-K_2\mu_{M2}+x_{M2}-x_{ДМ2}}{K_1-K_2}\right)\right)10^{-1},\ \text{при}\ K_1=\frac{x_{ДМ3}-x_{ДМ2}}{\mu_{ДМ3}-\mu_{ДМ2}}\ \text{і}\ K_2=\frac{x_{M3}-x_{M2}}{\mu_{M3}-\mu_{M2}};$$

$$\alpha_{MC}=\text{entier}\left(\frac{1}{2}+10\left(\frac{K_1\mu_{M2}-K_2\mu_{C2}+x_{C2}-x_{M2}}{K_1-K_2}\right)\right)10^{-1},\ \text{при}\ K_1=\frac{x_{M4}-x_{M3}}{\mu_{M4}-\mu_{M3}}\ \text{і}\ K_2=\frac{x_{C3}-x_{C2}}{\mu_{C3}-\mu_{C2}};$$

$$\alpha_{CB}=\text{entier}\left(\frac{1}{2}+10\left(\frac{K_1\mu_{C3}-K_2\mu_{B1}+x_{B1}-\mu_{C3}}{K_1-K_2}\right)\right)10^{-1},\ \text{при}\ K_1=\frac{x_{C4}-x_{C3}}{\mu_{C4}-\mu_{C3}}\ \text{і}\ K_2=\frac{x_{B2}-x_{B1}}{\mu_{B2}-\mu_{B1}};$$

$$\alpha_{ВДВ}=\text{entier}\left(\frac{1}{2}+10*\left(\frac{K_1\mu_{B2}-K_2\mu_{ДВ2}+x_{ДВ2}-x_{B2}}{K_1-K_2}\right)\right)10^{-1},\ \text{при}\ K_1=\frac{x_{B3}-x_{B2}}{\mu_{B3}-\mu_{B2}}\ \text{і}$$

$$K_2=\frac{x_{ДВ3}-x_{ДВ2}}{\mu_{ДВ3}-\mu_{ДВ2}}.$$

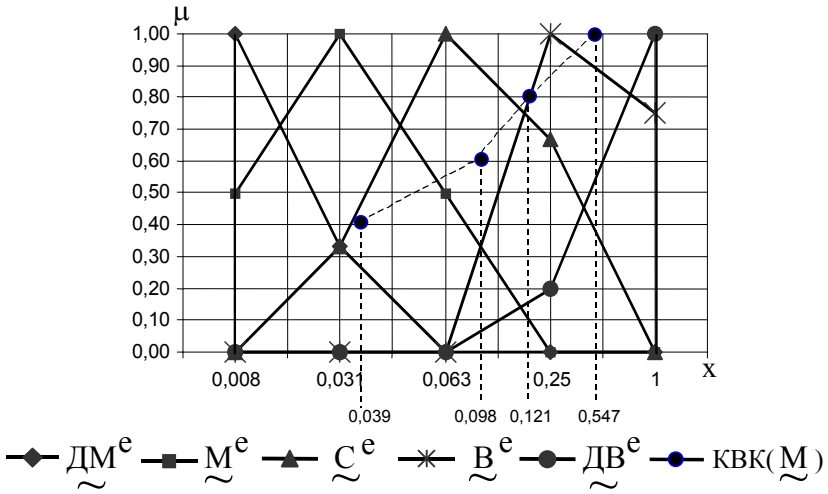

Рисунок 4 – Поточне КВК($\underset{\sim}{M}$) і еталонні НЧ для КВК

За допомогою цієї процедури, а також відповідно до набору евристичних правил, визначаємо стан системи щодо можливого процесу сканування. Якщо отримане поточне НЧ найбільш близьке до $\underset{\sim}{B}^e$ або $\underset{\sim}{ДВ}^e$, то виходячи з властивостей ВК можна зробити висновок, що можливість сканування портів висока.

Сформуємо відповідно до п'ятого етапу типової моделі набір нечітких евристичних правил:

Якщо КВК $\underset{\sim}{M}$ *ближче до* $\underset{\sim}{ДМ}^e$, *то можливість сканування Н* (правило 1);

Якщо КВК $\underset{\sim}{M}$ *ближче до* $\underset{\sim}{M}^e$, *то можливість сканування БНВ* (правило 2);

Якщо КВК $\underset{\sim}{M}$ *ближче до* $\underset{\sim}{C}^e$, *то можливість сканування БВН* (правило 3);

Якщо КВК $\underset{\sim}{M}$ *ближче до* $\underset{\sim}{B}^e$, *то можливість сканування В* (правило 4);

Якщо КВК $\underset{\sim}{M}$ *ближче до* $\underset{\sim}{ДВ}^e$, *то можливість сканування В* (правило 5), де Н – низька, БНВ – більш низька, ніж висока, БВН – більше висока ніж низька, В – висока.

Далі, відповідно до шостого етапу типової моделі системи виявлення атак, необхідно визначити можливості сканування портів. Для цього скориставшись одержаними еталонними і поточними даними, а

також знайденим α_{min}, проведемо обчислення відповідно до сформованих правил та ФУП. Подамо НЧ $\underset{\sim}{ДМ}^{e}$, $\underset{\sim}{М}^{e}$, $\underset{\sim}{С}^{e}$, $\underset{\sim}{В}^{e}$, $\underset{\sim}{ДВ}^{e}$ та КВК ($\underset{\sim}{М}$) у α-рівневому вигляді: $\underset{\sim}{ДМ}^{e}$ = {0,2/0,008; 0,4/0,008; 0,6/0,008; 0,8/0,008; 1/0,008; 0,8/0,015; 0,6/0,022; 0,4/0,029; 0,2/0,044}; $\underset{\sim}{М}^{e}$ = {0,2/0,008; 0,4/0,008; 0,6/0,013; 0,8/0,022; 1/0,031; 0,8/0,044; 0,6/0,057; 0,4/0,1; 0,2/0,175}; $\underset{\sim}{С}^{e}$ = {0,2/0,022; 0,4/0,034; 0,6/0,044; 0,8/0,053; 1/0,063; 0,8/0,176; 0,6/0,328; 0,4/0,52; 0,2/0,776}; $\underset{\sim}{В}^{e}$ = {0,2/0,1; 0,4/0,1; 0,6/0,175; 0,8/0,213; 1/0,25; 0,8/0,85; 0,6/1; 0,4/1; 0,2/1}; $\underset{\sim}{ДВ}^{e}$ = {0,2/0,25; 0,4/0,438; 0,6/0,625; 0,8/0,813; 1/1; 0,8/1; 0,6/1; 0,4/1; 0,2/1}; КВК $\underset{\sim}{М}$ = {0,2/0,039; 0,4/0,039; 0,6/0,098; 0,8/0,121; 1/0,547; 0,8/0,547; 0,6/0,547; 0,4/0,547; 0,2/0,547} і апроксимуємо їх: $\underset{\sim}{ДМ}^{eA}$ = {0,8/0,008; 0,9/0,008; 1/0,008; 0,9/0,011; 0,8/0,015}; $\underset{\sim}{М}^{eA}$ = {0,8/0,022; 0,9/0,026; 1/0,031; 0,9/0,037; 0,8/0,044}; $\underset{\sim}{С}^{eA}$ = {0,8/0,053; 0,9/0,058; 1/0,063; 0,9/0,126; 0,8/0,188}; $\underset{\sim}{В}^{eA}$ = {0,8/0,212; 0,9/0,231; 1/0,25; 0,9/0,55; 0,8/0,85}; $\underset{\sim}{ДВ}^{eA}$ = {0,8/0,812; 0,9/0,906; 1/1; 0,9/1; 0,8/1}; КВК ($\underset{\sim}{М}^{A}$) = {0,8/0,121; 0,9/0,334; 1/0,547; 1/0,547; 1/0,547}.

Далі з урахуванням α_{min} розіб'ємо $\underset{\sim}{ДМ}^{eA}$ на рівневі множини: перший рівень – $\underset{\sim}{ДМ}^{eA}_{\alpha 1}$ = {0,008; 0,008; 0,008; 0,011; 0,015}, при $0 < \alpha \le 0{,}8$; другий рівень – $\underset{\sim}{ДМ}^{eA}_{\alpha 1}$ = {0,008; 0,008; 0,011; 0,015}, при $0{,}8 < \alpha \le 0{,}9$; третій рівень – $\underset{\sim}{ДМ}^{eA}_{\alpha 3}$ = {0,008; 0,011; 0,015}, при $0{,}9 < \alpha \le 1$ і знайдемо середні значення [11] на кожному рівні: $M_1 \approx 0{,}0100$; $M_2 \approx 0{,}0105$; $M_3 \approx 0{,}0113$ та функцію упорядкування $F(\underset{\sim}{ДМ}^{eA})$

$$= \int\limits_{\substack{0\\(\alpha=\overline{1,3})}}^{1} M(ДМ_{\alpha}^{e_A})\,d\alpha = \int\limits_{0}^{0,8} M_1\,d\alpha + \int\limits_{0,8}^{0,9} M_2\,d\alpha + \int\limits_{0,9}^{1} M_3\,d\alpha = \int\limits_{0}^{0,8} 0{,}0100\,d\alpha + \int\limits_{0,8}^{0,9} 0{,}0105\,d\alpha + \int\limits_{0,9}^{1} 0{,}0113\,d\alpha$$

$= 0{,}0102.$

Аналогічні операції виконаємо для $\underset{\sim}{М}^{eA}$, $\underset{\sim}{С}^{eA}$, $\underset{\sim}{В}^{eA}$, $\underset{\sim}{ДВ}^{eA}$ та КВК($\underset{\sim}{М}^{A}$) і відповідно отримаємо значення функції упорядкування: $F(\underset{\sim}{М}^{eA}_{\alpha}) = \int\limits_{\substack{0\\(\alpha=\overline{1,3})}}^{1} M(М_{\alpha}^{e_A})\,d\alpha = \int\limits_{0}^{0,8} 0{,}026\,d\alpha + \int\limits_{0,8}^{0,9} 0{,}003\,d\alpha + \int\limits_{0,9}^{1} 0{,}004\,d\alpha = 0{,}033$;

$F(\underset{\sim}{С}^{eA}) = \int\limits_{\substack{0\\(\alpha=\overline{1,3})}}^{1} M(С_{\alpha}^{e_A})\,d\alpha = \int\limits_{0}^{0,8} 0{,}078\,d\alpha + \int\limits_{0,8}^{0,9} 0{,}011\,d\alpha + \int\limits_{0,9}^{1} 0{,}013\,d\alpha = 0{,}102$;

$F(\underset{\sim}{В}^{eA}) = \int\limits_{\substack{0\\(\alpha=\overline{1,3})}}^{1} M(В_{\alpha}^{e_A})\,d\alpha = \int\limits_{0}^{0,8} 0{,}335\,d\alpha + \int\limits_{0,8}^{0,9} 0{,}047\,d\alpha + \int\limits_{0,9}^{1} 0{,}055\,d\alpha = 0{,}437$; $F(\underset{\sim}{ДВ}^{eA})$

$$= \int\limits_{\substack{0\\(\alpha=\overline{1,3})}}^{1} M(ВД_{\alpha}^{e_A})\,d\alpha = \int\limits_{0}^{0,8} 0{,}755\,d\alpha + \int\limits_{0,8}^{0,9} 0{,}098\,d\alpha + \int\limits_{0,9}^{1} 0{,}100\,d\alpha = 0{,}953;\quad F(КВК(\underset{\sim}{М}^{A}))$$

$$= \int_{\substack{0 \\ (\alpha=1,3)}}^{1} M(КВК(M_{\alpha}^{e_A}))\,d\alpha = \int_{0}^{0,8} 0{,}335\,d\alpha + \int_{0,8}^{0,9} 0{,}049\,d\alpha + \int_{0,9}^{1} 0{,}055\,d\alpha = 0{,}439.$$

З розрахунків ФУП видно, що $F(\underset{\sim}{B}^{eA}) < F(КВК(\underset{\sim}{M}^{A})) < F(\underset{\sim}{ДВ}^{eA})$. Отже поточне КВК ($\underset{\sim}{M}^{A}$) знаходиться між $\underset{\sim}{B}^{eA}$ і $\underset{\sim}{ДВ}^{eA}$, але, відповідно до розрахунків, ближче до $\underset{\sim}{B}^{eA}$. Отже, результат застосування побудованих нечітких евристичних правил показує, що можливість сканування портів на заданий момент часу – висока.

V Висновки

Описані моделі можуть використовуватися в загальній концепції побудови моделей і технологій систем ідентифікації атак як додатковий засіб, що дозволяє виявляти аномалії у відповідному середовищі, які створюються, наприклад, в результаті дії різних складних механізмів, закладених у сучасних скануючих утилітах.

Література: ***1.*** *Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа . – СПб: Наука и техника, 2004. – 384 с.* ***2.*** *Коул Э. Руководство по защите от хакеров: Пер. с англ. – М.: Издательский дом "Вильямс", 2002. – 640 с.* ***3.*** *Зима В. М., Молдовян А. А., Молдовян Н. А. Безопасность глобальных сетевых технологий. – 2-е изд. – СПб.: БХВ-Петербург, 2003. – 368 с.* ***4.*** *Лукацкий А. В. Обнаружение атак. – СПб.: БВХ–Петербург, 2001. – 624 с.* ***5.*** *Бэнкс М. Психи и маньяки в Интернете. – Пер. с англ. – СПб: Символ-Плюс, 1998. – 320 с.* ***6.*** *Модели принятия решений на основе лингвистической переменной / А. Н. Борисов, А. В. Алексеев, О. А. Крумберг и др. – Рига: Зинатне, 1982. – 256 с.* ***7.*** *Обработка нечеткой информации в системах принятия решений / А. Н. Борисов, А. В. Алексеев, Г. В. Меркурьева и др. – М.: Радио и связь, 1989. – 304 с.* ***8.*** *Заде Л. Понятие лингвистической переменной и его применение к принятию приближенных решений. – М.: Мир, 1976. – 166 с.* ***9.*** *Вероятность и математическая статистика. Энциклопедия / Под ред. Прохорова Ю. В. - М.: БРЭ, 1999. – 910 с.* ***10.*** *Кофман А. Введение в теорию нечетких множеств.- М.: Радио и связь, 1982. – 432 с.* ***11.*** *Корченко О. Г. Системи захисту інформації: Монографія – К.: НАУ, 2004. – 264 с.*

УДК 681.3.06

МЕТОДИКА ВИЗНАЧЕННЯ ЦІЛЬОВОГО ПРОФІЛЮ ЗРІЛОСТІ ПРОЦЕСІВ ЗАХИСТУ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ МЕТОДУ ВИРІШУЮЧИХ МАТРИЦЬ

Олександр Потій, Анатолій Лєншин
Харківський національний університет радіоелектроніки

Анотація: **Пропонується методика визначення цільового профілю зрілості з урахуванням вимог до конфіденційності, цілісності та доступності критичних інформаційних ресурсів.**
Summary: **The approach to designate purpose maturity profile according with integrity, confidentiality and availability requirements to critical informational assets are proposed.**
Ключові слова: **Модель зрілості процесів захисту інформації, безпека інформації, попарні порівняння.**

Вступ

Сучасні підходи до захисту інформації потребують застосування комплексних рішень завдань захисту інформації. Одним із елементів таких рішень є управління зрілістю процесів захисту інформації. Завдання управління потребує прийняття рішень та здійснення коректуючих впливів. Прийняття рішень (наприклад, начальником служби захисту інформації) можливо за таких умов:

- наявні альтернативи;
- визначені цілі;
- визначені обмеження на реалізацію поставлених цілей.

Тобто якщо немає альтернатив – немає об’єкту відносно якого потрібно приймати рішення, якщо