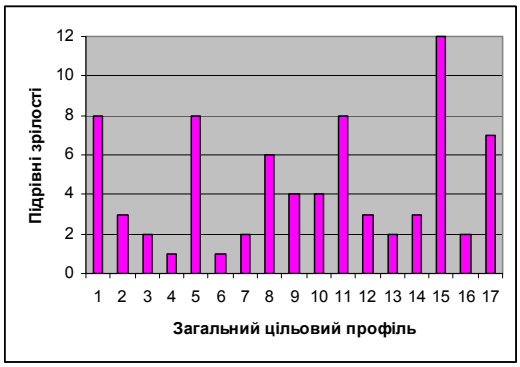

б)




г)

**Рисунок 3 – Цільові профілі зрілості**

## Висновки

В статті запропоновано методику визначення цільового профілю зрілості процесів захисту інформації. Як математична база прийняття рішення використовується метод вирішуючих матриць, для призначення коефіцієнтів значущості напрямків практичної діяльності – метод попарних порівнянь. Визначення необхідно рівня зрілості процесів захисту інформації ґрунтується на попередньому аналізі вимог безпеки до інформації, що циркулює в організації. Для вирішення задачі декомпозиції запропоновано використовувати стандарти в галузі захисту інформації. Методика може бути застосована на етапах первинного обстеження підприємства, що проводиться з метою визначення вимог безпеки під час аудиту безпеки та оцінки рівня зрілості процесів захисту інформації.

Застосування методики дозволяє визначити цільові орієнтири для роботи служби захисту інформації.

*Література:* ***1.*** *Потий А. В., Управление безопасностью информации: сущность и базовые принципы, // VIII Международная научно-практическая конференция"Безопасность информации в информационно-телекоммуникационных системах", Тезисы докладов. – К.: НИЦ "Тезис", 2005 г., 69-70 с.* ***2.*** *Потій О. В., Процесний підхід до управління безпекою інформації //VIII Международная научно-практическая конференция"Безопасность информации в информационно-телекоммуникационных системах", Тезисы докладов. – К.: НИЦ "Тезис", 2005 г., 35-36 с.* ***3****. ISO/IEC 15408, 1999: Information technology - Security techniques - Evaluation criteria for IT security.* ***4.*** *НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.* ***5.*** *FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems* ***6.*** *Bundesamt fur Sicherheit in der Informationstechnik. IT Baseline Protection Manual, 1998* ***7.*** *НД ТЗІ 2.5-004-99. Критерії захищеності інформації комп'ютерних системах від несанкціонованого доступу .* ***8.*** *НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.* ***9.*** *ISO/IEC 17779:2000 Code of practice for information securit management* ***10.*** *ISO/IEC 21827: 2002 Information technology - Systems Security Engineering - Capability Maturity Model* ***11.*** *NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems* ***12.*** *NIST SP 800-53, Recommended Security Controls for Federal Information Systems* ***13.*** *Саати Т. Принятие решений. Метод анализа иерархий. – М: Радио и связь, 1999. – 341с.*

**УДК 681.3.06**

# ПОБУДОВА ФУНКЦІЙ НАЛЕЖНОСТІ ЕКСПЕРТНИХ ОЦІНОК ДО ЗОН БАЗОВИХ ДУМОК У ПРОСТОРІ СУБ'ЄКТИВНОЇ ЛОГІКИ

***Анатолій Лєншин***
*ЗАТ „Інститут інформаційних технологій"*

*Анотація:* **Пропонується підхід до побудови функцій належності експертних оцінок щодо зрілості процесів захисту інформації до зон базових думок у просторі суб'єктивної логіки.**
*Summary:* **The approach to create membership function for expert estimations of information security process maturity to opinion base regions in the space of subjective logic are proposed**

*Ключові слова:* **Функції належності, суб'єктивна логіка, вербальні оцінки, збір знань, безпека інформації, зони базових думок.**

## Вступ

Оцінка зрілості процесів захисту інформації належить до класу задач прийняття рішень в умовах невизначеності. З метою врахування ступеню невизначеності на всіх стадіях оцінки запропоновано використовувати аналітичний апарат суб'єктивної логіки [1 – 3]. Новий підхід до визначення думок у просторі суб'єктивної логіки [4] дозволив надавати оцінки зрілості процесів захисту інформації у вербальному вигляді. В даній статті розглядаються питання побудови функцій належності вектора думки до зон базових думок з метою забезпечення можливості одержання узагальнених вербальних оцінок зрілості процесів, а також створення передумов побудови системи підтримки прийняття рішень щодо питань оцінки та управління зрілістю процесів захисту інформації.

## І Застосування зон базових думок для надання вербальних оцінок щодо зрілості процесів захисту інформації

В [1 – 3] запропоновано використовувати зони базових думок як інструмент для надання оцінок зрілості процесів захисту інформації. Такий підхід дозволяє надавати оцінки у вербальному вигляді, переводити їх у кількісні значення вектора думок за допомогою вдосконаленого апарату суб'єктивної логіки [5 – 6].

Розглянемо визначення зони базової думки, що наведено в [4].

*Визначення 1.* Нехай $R$ – множина всіх можливих думок експерта, а $N$ – кількість підмножин (зон), на які розбито цю множину. Тоді $R = \{r_1, r_2, ..., r_N\}$, де $r_i$ – зона базової думки, тобто сукупність точок у просторі трикутника думок, що характеризується однаковим співвідношенням головного (домінуючого) та другорядних параметрів, що дозволяє надати їй вербальний опис.

*Визначення 2.* Головний (домінуючий) параметр – один із трьох параметрів вектора думки у просторі суб'єктивної логіки, значення якого переважає загальне значення двох інших параметрів вектора думки.

*Визначення 3.* Другорядні параметри – параметри вектора думки у просторі суб'єктивної логіки, загальне значення яких менше, ніж значення третього параметра вектора думки.

Приклад. Нехай судження експерта $A$ відносно події $S$ представлено у вигляді вектора думки $w_S^A = \{b; d; u\} = \{0{,}65;\ 0{,}17;\ 0{,}18\}$, тоді оскільки $b \phi (d + u)$, параметр довіри $(b)$ – головний, а параметри недовіри $(d)$ та невизначеності $(u)$ – другорядні.

Експерт, оцінюючи зрілість процесу захисту інформації, обирає зону базової думки – вербальний опис якої, на його думку, найбільш повно відповідає поточному рівню зрілості. За кількісні значення судження експерта беруться координати, які має середня точка обраної зони базової думки у просторі суб'єктивної логіки. Для визначення середньої точки експерт повинен встановити суб'єктивні значення границь зон базових думок. Враховуючи симетричність зон у трикутнику думок, для визначення границь зон базових думок немає необхідності описувати кожну зону для кожного параметра (довіри, недовіри та невизначеності) окремо. Достатньо надати кількісну оцінку (у межах від нуля до одиниці або у відсотках) для одного випадку (табл. 1). Загальна методика визначення границь зон та середніх точок наведена в [4]. Відомо, що в зв'язку з особливостями оперативної пам'яті людини, ефективно експерт може працювати з кількістю об'єктів, що не перевищує дев'яти. З огляду на це, в цій статті пропонується здійснити укрупнення зон і зменшити кількість зон з домінуючим параметром до дев'яти.

Постановка задачі визначення чисельних значень границь має такий вигляд. Внаслідок проведення експерименту могли виникнути три події $S$, $F$, $K$. Експерту надано набір фактів, які прямо або побічно свідчать про те, яка подія відбулася. Задача визначення границь зведена до визначення найменшого відсотка фактів, якого буде достатньо для винесення суджень, що представлені у другому стовпці табл. 1.

При визначені кількісного значення необхідно враховувати такі обмеження.

1) Значення відносно судження із більшим порядковим номером не може бути більшим від значення попереднього, оскільки судження розташовані у порядку зменшення впевненості, що подія $S$ відбулася.

2) Значення, при якому експерт згоден з судженням під номером два, не може бути меншим від 0.5, бо аргументи на користь того, що відбудеться одна із трьох подій мають переважити аргументи на користь двох інших, тобто щонайменше бути більшими від половини.

Таблиця 1- Приклад встановлення границь базових зон експертом

| № | Сутність судження | Приймаю, якщо більше ніж ... % фактів свідчать на користь того, що сталася подія S | Познач. границь |
|---|---|---|---|
| 1. | **Абсолютно** впевнений, що відбулась подія *S* | 80% (0,8) | $g1$ |
| 2. | **Граничний** випадок, коли я можу сказати, що подія S відбулась – внаслідок того, що є підстави вважати, що могли статися події *F* (та/або) *K* | 50% (0,5) | $g2$ |

*Визначення 4.* Зона з визначеним головним параметром – зона базової думки у просторі суб'єктивної логіки, в якій можна виділити головний та другорядні параметри.

*Визначення 5.* Зона припущень – зона базової думки у просторі суб'єктивної логіки, яка характеризується приблизно рівними значеннями усіх трьох параметрів, внаслідок чого неможливо визначити головний та другорядні параметри.

*Визначення 6.* Значення головного параметра середньої точки зон базових думок дорівнює середньо арифметичному значенню верхньої на нижньої границі даної зони:

$$x = \frac{верх.гр + нижн.гр}{2}. \tag{1}$$

Занотуємо, що верхня та нижня границі можуть бути відомими лише для головного параметра. Обчислення другорядних параметрів необхідно проводити таким чином. Якщо зона є такою, що вісь головного параметра поділяє її на дві симетричні області (наприклад, зона $p$ ), то другорядні параметри для середньої точки рівні.

*Визначення 7.* Значення кожного із другорядних параметрів середньої точки зони базової думки, що симетрична відносно осі головного параметру, дорівнює половині різниці максимального та середнього значення головного параметра для цієї зони.

Нехай $m$ – значення головного параметру, $t_1, t_2$ – значення другорядних параметрів, $g1$, $g2$ – значення першої та другої границі відповідно. Маємо:

$$\begin{aligned} & m \phi\phi \ (t_1 + t_2), \\ & t_1 = t_2 = (1-m)/2. \end{aligned} \tag{2}$$

Для зон $g$ та $q$ значення другорядних параметрів, застосовуючи прийняті позначення, обчислюється за формулою (3).

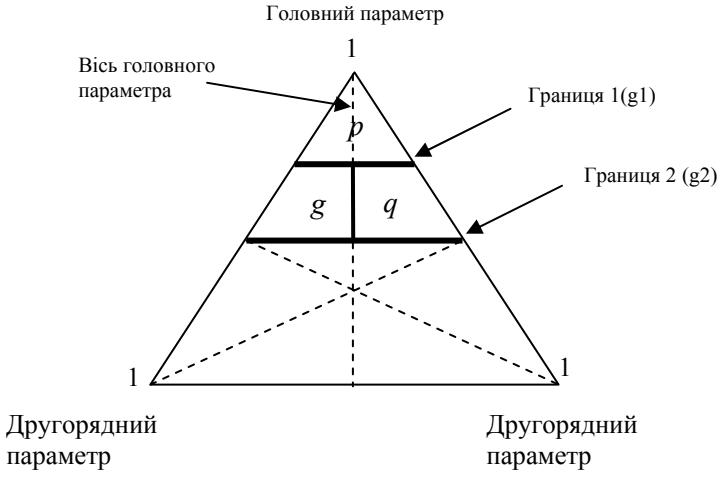



**Рисунок 1 – Границі базових зон трикутника думок**

Таким чином, застосовуючи вирази (1 – 3), можливо визначити координати середньої точки зони базової думки, при цьому даний підхід дозволяє адаптувати границі зон під кожного експерта.

Після проведення обчислення кількісних значень думок за допомогою операторів суб'єктивної логіки

визначається узагальнена зрілість процесів із захисту інформації. Результат узагальненого значення представляється у вигляді вектора думки у просторі суб'єктивної логіки. Вирішення задачі віднесення вектора думки до певної зони пропонується здійснювати за допомогою побудови функцій належності для кожної зони.

$$
\begin{aligned}
& m \ \phi \ (t_1 + t_2), \\
& t_1 \ \pi \ t_2, \\
& t_1 = \frac{\left(0 + (1-m)/2\right)}{2} = (1-m)/4, \\
& t_2 = \frac{\left((1-m) + (1-m)/2\right)}{2} = \frac{3}{4}(1-m).
\end{aligned}
\tag{3}
$$

## II Застосування функцій належності в суб'єктивній логіці. Побудова суб'єктивних функцій належності для зон базових думок

Після введення авторами поняття зон базових думок у просторі суб'єктивної логіки виникли такі задачі:

1) віднесення вектора думки до певної зони базової думки;

2) визначення ступеня належності до визначеної зони.

Перша задача може бути вирішена простим порівнянням значень параметрів вектора думки. Тобто визначенням домінуючого параметру, порівнянням його значущості з другорядними параметрами, а також порівнянням взаємної значущості другорядних параметрів. На основі проведених порівнянь за таблицею обирається зона базової думки, до якої належить вектор думки. Розв'язання другої задачі потребує розробки аналітичного виразу або побудови функції, за допомогою якої після віднесення вектора думки до певної базової зони можна було б визначити ступінь належності до цієї зони. Проведений аналіз [7 – 11] показав, що подібні задачі вирішуються в теорії нечітких множин за допомогою використання функції належності (ФН).

Таблиця 2 – Порівняння призначення ФН в теорії нечітких множин та суб'єктивній логіці

| № | Призначення ФН | |
|---|---|---|
| | в теорії нечітких множин | в суб'єктивній логіці |
| 1 | віднесення елемента до певної нечіткої множини, що описується лінгвістичною змінною | віднесення вектора думки до певної зони базової думки, що має вербальний опис |
| 2 | визначення ступеня належності елемента до визначеної нечіткої множини | визначення ступеня належності до визначеної зони базової думки |

В теорії нечітких множин залежно від задачі, для рішення якої використовується нечітка множина, розглядають такі ступені належності: ступінь належності визначеному поняттю, імовірність, можливість, корисність, істинність, правдоподібність, значення функції тощо. Для кожної трактовки розроблено свої методи побудови ФН. У ряді моделей м'яких обчислень ФН задаються в параметричному вигляді. Найпоширенішими в теорії нечітких множин є трикутникові, трапецієподібні, гауссівські та дзвоноподібні функції належності.

Трапецієподібні ФН задаються чотирма параметрами (*a, b, c, d*):

$$
\begin{aligned}
& m(x) = 0, x \le a \\
& m(x) = \frac{(x-a)}{(b-a)}, a < x \le b \\
& m(x) = 1, \ b < x \le c \\
& m(x) = \frac{(d-x)}{(d-c)}, c < x \le d \\
& m(x) = 0, \ d < x
\end{aligned}
$$

Трикутникові ФН задаються трьома параметрами (*a, b, c*):

$$m(x) = 0, x \le a$$

$$m(x) = \frac{(x-a)}{(b-a)}, a < x \le b$$

$$m(x) = \frac{(c-x)}{(c-b)}, b < x \le c$$

$$m(x) = 0,\ c < x$$

Гауссівські ФН задаються двома параметрами $(c,s)$: $m(x) = e^{\frac{-0,5(x-c)^2}{s^2}}$

Д звоноподібні ФН задаються трьома параметрами $(a,b,c)$: $m(x) = \frac{1}{1+\left(\frac{x-c}{a}\right)^{2b}}$

В традиційній теорії суб'єктивної логіки ФН не використовуються, але внаслідок адаптації до задач проведення оцінки зрілості процесів захисту інформації було поставлено задачу розробки ФН із врахуванням досвіду побудови подібних функцій у теорії нечітких множин.

Для позначення відношення цих функцій до суб'єктивної логіки пропонується назвати їх функції належності до зон базових думок у просторі суб'єктивної логіки або коротше суб'єктивні функції належності (СФН). Суб'єктивність цих функцій підтверджується також їх залежністю від границь, що визначаються відповідно до особистих міркувань експерта або групи експертів.

*Визначення 8.* Суб'єктивна функція належності – функція, яка для довільного вектора думки, залежно від визначених експертом границь, визначає, до якої зони базових думок та з якою мірою впевненості він належить.

Схожість ФН в теорії нечітких множин та функцій належності до зон базових думок у просторі суб'єктивної логіки обумовлюється не лише схожим призначенням (табл. 2), але і тим, що за своєю суттю простір думок суб'єктивної логіки є чіткою множиною, аналогом якої є універсальна множина у теорії нечітких множин. Продовжуючи аналогію, слід зазначити тотожність понять „зона базової думки" та „нечітка множина", оскільки зона базової думки є множиною векторів думок. Належність до цієї множини визначається за допомогою границь, що суб'єктивно призначаються експертом. Слід також зазначити, що зона базової думки, як і будь-яка нечітка множина, має вербальний опис чи, як її ще називають, лінгвістичну змінну. Вищезазначені передумови підтверджують можливість розробки СФН для кожної зони базової думки.

Складність побудови СФН експертної оцінки до зони базових думок полягає в тому, що оцінка представляється в вигляді вектора думки $\omega = \{b,d,u\}$ і отже СФН має залежати від трьох параметрів та може бути задана таким чином: $(b,d,u,g1,g2)$. Побудова подібної функції можлива в чотиривимірному просторі, або з урахуванням умови нормування

$$b + d + u = 1 \tag{4}$$

у більш звичному тривимірному. Але навіть тривимірне відображення не є наочним. Значно корисніше в контексті зручності було б використовувати функцію, що будується у звичайному двовимірному вигляді, тобто значення змінної/значення СФН для цієї змінної. Для побудови такої функції необхідно виразити співвідношення параметрів вектора думки за допомогою однієї змінної. Цю задачу може бути розв'язано завдяки тому факту, що параметри вектора думки почергово відіграють роль головного та другорядних параметрів, а, отже, зони базових думок є симетричними відносно центра трикутника думок. Таким чином, введемо до розгляду змінну $\eta$, яка відображає значення головного параметра вектора думки та співвідношення другорядних параметрів:

$$\eta = \begin{cases} m,\ t_1\ \phi = t_2 \\ -m,\ t_1\ \pi\ t_2 \end{cases} \tag{5}$$

де $m$ – головний (домінуючий) параметр, $t_1$ та $t_2$ – другорядні параметри.

Як видно з (5), змінна має однакове (за модулем) значення для зон з однаковим головним параметром, але знак залежить від співвідношення другорядних параметрів.

Визначимо властивості суб'єктивних функцій належності.

1) Безперервність. Властивість безперервності полягає у можливості обчислення значення СФН для будь-якого значення вхідного параметра, обчисленого за рівнянням (5). Властивість обумовлюється необхідністю можливості визначення ступеня належності до зони базової думки для довільної точки з простору суб'єктивної логіки.

2) Визначеність на проміжку $[-1;\ 1]$. Властивість обумовлена областю можливих значень вхідного параметра (змінна $\eta$), модуль якого не може бути більшим одиниці внаслідок рівняння (4).

3) Область значень $[0;\ 1]$. Ця властивість є подібною до властивості ФН у теорії нечітких множин. Якщо точка належить до зони базової думки із 100% суб'єктивною імовірністю, то відповідна СФН має одиничне значення. Якщо точка є такою, що із 100% суб'єктивною імовірністю не належить до зони базової думки, то відповідна СФН має нульове значення.

4) СФН, визначені для зон базових думок для одного домінуючого параметра та різних співвідношень другорядних, є взаємно симетричними відносно осі значень.

5) Суб'єктивні функції належності до зон базових думок з визначеним головним параметром мають нульове значення, для всіх точок, в яких модуль вхідного параметра (змінна $\eta$) менше від $0{,}5$, тобто граничного випадку, при якому можливо визначити домінуючий параметр.

6) Суб'єктивні функції належності до зони припущень мають нульове значення, для всіх точок, в яких модуль вхідного параметра (змінна $\eta$) більше, ніж нижня границя $g2$.

7) Значення суб'єктивної функції належності до зони базової думки із визначеним головним параметром є не меншим від значення нижньої границі для цієї зони. Ця властивість обумовлена тим, що визначення границь зон базових думок здійснюється на основі впевненості в істинності домінуючого параметра.

Єдиним обмеженням при побудові СФН є вимога мати вищеперераховані властивості. Наведемо приклад параметричного завдання СФН ($\mu_i(\eta),\ i=\overline{1,9}$, де $i$ – порядковий номер зони) для зон з домінуючим параметром:

$$\mu_i(\eta)=\begin{cases} 0, \quad 0\le|\eta|\le 0{,}5 \\ \dfrac{(|\eta|-0{,}5)grN(i)}{(grN(i)-0{,}5)},\ 0{,}5<|\eta|\le grN(i),\ grN(i)>0{,}5 \\ \dfrac{(|\eta|-grN(i))(grV(i)-grN(i))}{(S-grN(i))}+grN(i),\ grN(i)<|\eta|\le S,\quad grV(i)>grN(i) \\ 1,\quad S<|\eta|\le grV(i) \\ 0,\ |\eta|>grV(i) \end{cases} \tag{6}$$

де $S=\dfrac{grN(i)+grV(i)}{2}$, а $grN(i)$ та $grV(i)$ позначають відповідно нижню та верхню границю зони з $i$ - тим порядковим номером.

Для зони припущень СФН може мати такий вигляд:

$$\mu_{10}(\eta)=\begin{cases} \dfrac{2}{\sqrt{2\pi}}e^{-2p^2},\ 0\le|\eta|\le 0{,}5 \\ \left(\dfrac{g2-|\eta|}{g2-0{,}5}\right)g2,\ 0{,}5<|\eta|\le g2 \\ 0,\ |\eta|\ge g2 \end{cases} \tag{7}$$

*Визначення 9.* Родина СФН – набір СФН, в якому кожній зоні базової думки відповідає своя СФН.

Побудуємо графічне представлення родини СФН до зон базових думок згідно з (6) – (7).

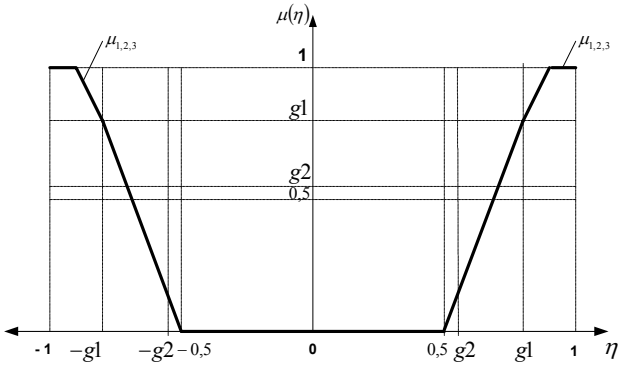



**Рисунок 2 – Вид СФН для зон базових думок з абсолютною перевагою домінуючого параметру**

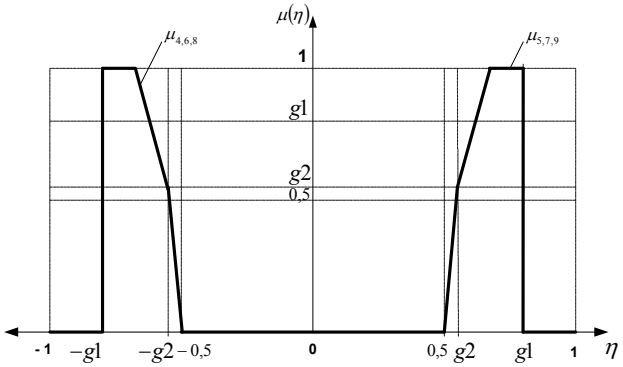



**Рисунок 3 – Вид СФН для зон базових думок з перевагою домінуючого параметру**

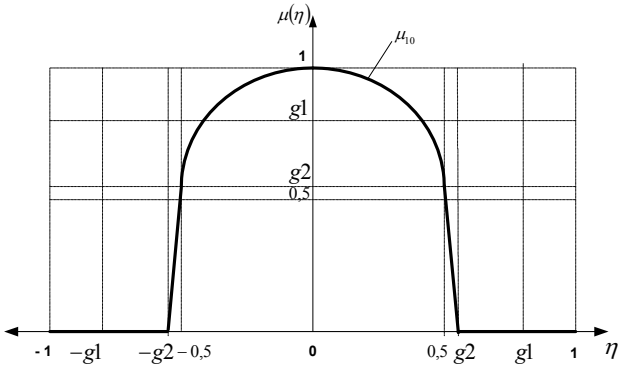



**Рисунок 4 – Вид СФН для зони припущень**

Згідно з визначенням 8 СФН має задовольняти таким вимогам:

- забезпечувати можливість визначення, до якої зони базової думки належить довільний вектор думки;
- забезпечувати можливість визначення ступеню належності довільного вектора думки до зони базової думки.

З метою виконання цих вимог побудуємо СФН для всіх зон базових думок. Приклади СФН, розрахованих для зон базових думок з домінуючим параметром $\mu_i(\eta),\ i=\overline{1,9}$ та зони припущень $\mu_{10}(\eta)$, наведено на рис. 5, а – в.

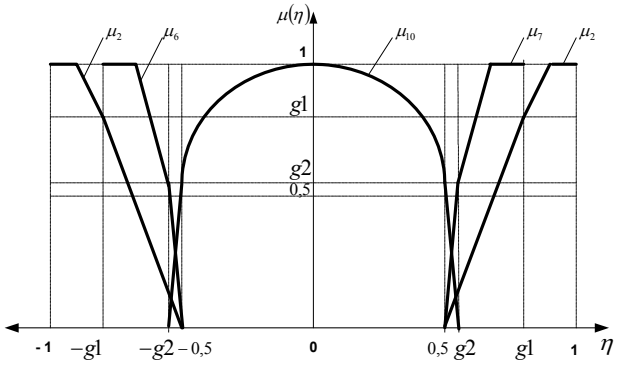



**Рисунок 5, а – СФН для (** $m = b \quad t_1 = d \quad t_2 = u$ **)**

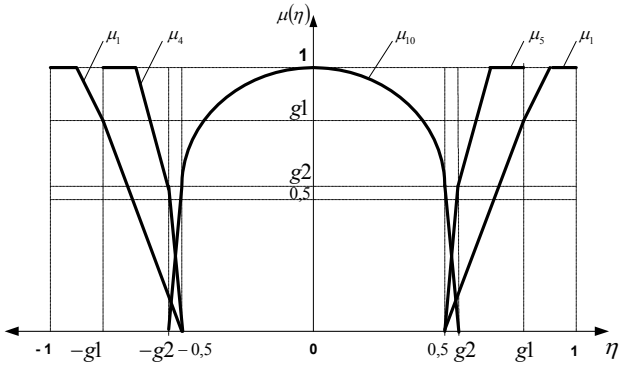



**Рисунок 5, б – СФН для (** $m = d \quad t_1 = b \quad t_2 = u$ **)**

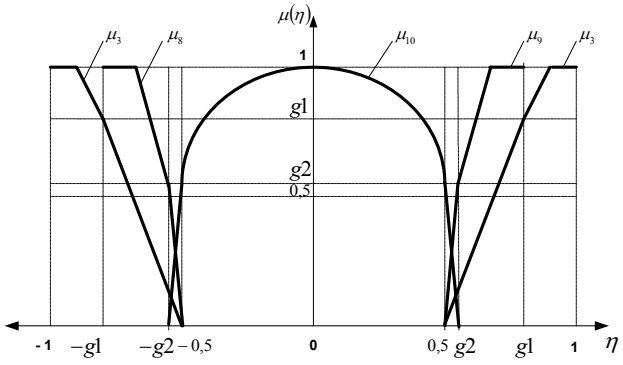



**Рисунок 5, в – СФН для (** $m = u \quad t_1 = d \quad t_2 = b$ **)**

Таким чином, віднесення вектора думки до певної зони базової думки та визначення ступеню належності до визначеної зони здійснюється за таким алгоритмом:

1) обчислити значення змінної $\eta$ за допомогою (5);
2) визначити значення СФН $\mu_i(\eta), i = \overline{1,9}$ за допомогою формули (6) та значення $\mu_{10}(\eta)$ за формулою (7) або використовуючи графічне представлення СФН;
3) визначити зону, для якої значення СФН $\mu_i(\eta), i = \overline{1,10}$ є максимальним:

$$\mu_{\max}(\eta) = \max_{i=1,10}(\mu_i(\eta)); \tag{8}$$

4) Зона, якій відповідає СФН $\mu_{\max}(\eta)$, і є зоною базової думки, до якої відноситься вектор думки, а значення $\mu_{\max}(\eta)$ є ступенем належності до цієї зони.

## Висновки

Проведення аудиту безпеки інформації потребує нормативно-правового, методичного, математичного та програмного забезпечення. В статті розглянуто питання застосування зон базових думок для надання вербальних оцінок щодо зрілості процесів захисту інформації на основі існуючих стандартів в галузі захисту інформації. Наведено методику визначення границь та значень середніх точок для зон базових думок.

В статті наведено такі нові наукові результати:

- на основі виявленої подібності задач, що вирішуються в теорії нечітких множин та суб'єктивної логіки вперше обґрунтовано можливість побудови СФН вектора думки до зони базової думки для суб'єктивної логіки. Таким чином аналітичний апарат суб'єктивної логіки набув подальшого теоретичного розвитку щодо вирішення задач оцінки зрілості процесів захисту інформації;
- надано визначення СФН та сформульовані задачі побудови СФН;
- вперше визначено перелік властивостей, які повинні мати усі суб'єктивні функції належності;
- згідно з визначеними властивостями СФН, в параметричному вигляді задано родину СФН та побудовано їх графічне представлення для кожної зони базової думки у просторі суб'єктивної логіки;
- визначено алгоритм віднесення вектора думки до зони базової думки та визначення ступеню належності вектора думки до зон базових думок.

Практичне значення одержаних результатів полягає в створенні передумов для формування вербального опису обчислених узагальнених оцінок зрілості процесів захисту інформації та для розробки системи підтримки прийняття рішень начальника служби безпеки інформації щодо зрілості процесів захисту інформації.

*Література: **1**. Леншин А. В. Применение аппарата субъективной логики для оценки безопасности банковских ИТ-систем // Актуальні проблеми та перспективи розвитку фінансово-кредитної системи України: Збірник наукових статей. Харків: Фінарт, 2002, с. 410 – 412 **2**. Потий А. В., Леншин А. В. Оценка защищенности информационно-телекоммуникационных систем с использованием математического аппарата субъективной логики //7-я Научно - практическая конференция «Безопасность информации в информационно – телекоммуникационных системах», Киев. 2004 р. **3**. Потій О. В., Лєншин А. В. Основні положення математичного апарату суб'єктивної логіки та його застосування для оцінки рівня зрілості систем забезпечення безпеки інформації //Радиотехника. Тематический выпуск "Информационная безопасность", вып. 141, Харьков, 2005 г., с. 144-160. **4**. Потій О.В., Лєншин А.В. Методика визначення думок експертів відносно зрілості безпеки інформації із застосуванням математичного апарату суб'єктивної логіки //Науково-технічний збірник „Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 9, Київ, 2004 р., с. 38-47. **5.** A. Jøsang., S. J. Knapskog. A Metric for Trusted Systems. In Reinhard Posh, editor, Proceedings of the 15th IFIP/SEC International Information Security Conference. IFIP, 1998 **6**. A. Jøsang. A Logic for Uncertain Probabilities. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 9(3):279–311, June 2001. **7.** Беллман Р., Заде Л. Принятие решений в расплывчатых условиях.- В кн.: Вопросы анализа и процедуры принятия решений.- М.:Мир, 1976. - С. 172-215. **8.** Заде Л. А. Основы нового подхода к анализу сложных систем и процессов принятия решений.- В кн.: Математика сегодня.- М.:Знание, 1974, с. 5-49. **9.** Hong T.-P., Lee C.-Y. Induction of rules and membership functions from training examples. - Fuzzy Sets and Systems, 84, 1996, 33 - 47. **10.** Берштейн Л. С., Целых А. Н., Тимошенко Р. П. Об использовании интервальной функции принадлежности нечеткого множества. Известия высших учебных заведения. Северо - Кавказский регион. Технические науки. Ростов – на – Дону: изд-во Ростовского госуниверситета, №1, 1999г., . с.3-8. **11.** Кофман А. Введение в теорию нечетких множеств. М: Радио и связь, 1982, 432с.*

**УДК 681.3.06**

# КРИТЕРИИ И ПОКАЗАТЕЛИ ОЦЕНКИ КРИПТОПРОТОКОЛОВ. МАТЕМАТИЧЕСКИЙ АППАРАТ СРАВНЕНИЯ ПРОТОКОЛОВ

***Дмитрий Балагура***

*Харьковский национальный университет радиоэлектроники*

*Аннотация:* **Предлагаются критерии оценки криптографических протоколов. Вводятся условные и**