MATHEMATICAL AND COMPUTER MODELING

DOI 10.20535/2411-1031.2025.13.2.344709
УДК 004.056

ІГОР САМОЙЛОВ,
МИКОЛА КОНОТОПЕЦЬ,
АНТОН СТОРЧАК,
СЕРГІЙ ШОЛОХОВ

МОДЕЛЬ ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ НА БАЗІ НЕЧІТКИХ ВІДНОШЕНЬ

Сучасний етап розвитку інформаційно-комунікаційних систем характеризується їх масовим упровадженням у всі сфери суспільного життя: військову справу, державне управління, економіку, фінанси, промисловість тощо. Впровадження цифрових технологій забезпечує ефективність та швидкість обробки даних, проте одночасно підвищує залежність від кіберпростору та збільшує ризик виникнення загроз інформаційний безпеці. Задача оцінки загроз або захищеності інформаційно-комунікаційних систем на основі відомих збитків має важливе значення з кількох причин. По-перше, вона дозволяє перейти від якісного опису ризиків до кількісних оцінок, що створює підґрунтя для економічного обґрунтування рішень. По-друге, аналіз збитків дозволяє визначити пріоритетні загрози та оптимізувати ресурси на захист, орієнтуючись на найбільш критичні сценарії. По-третє, відкриває можливості для застосування сучасних математичних методів моделювання невизначеності у сфері інформаційної безпеки. Класичні методи оцінки захищеності інформаційно-комунікаційних систем базуються на обробці чітких статистичних даних про загрози та збитки. Проте на практиці інформація про ймовірність атак і масштаби збитків часто є неповною, суперечливою або подається у вигляді лінгвістичних категорій (“високий ризик загрози”, “значні збитки”). У таких умовах традиційні методи демонструють обмежену ефективність на низьку точність такої оцінки. Це зумовлює потребу у створені систем оцінки, здатних працювати з нечіткою інформацією та встановлювати причинно-наслідкові зв’язки між загрозами й можливими збитками. В статті запропонована модель оцінки захищеності інформаційно-комунікаційних систем через потенційні збитки на базі нечітких відношень II типу. Особливістю моделі є можливість оперувати з усіма типами невизначеності. Нечіткі терми загроз і збитків формалізуються інтервальними функціями належності II типу, в результаті чого міри значимості загроз і збитків визначаються інтервалами. Нечітка модель II типу будується на основі розширеного композиційного правила виведення Заде, з якого випливають дві системи рівнянь нечітких відношень. Ці системи пов’язують нижні (верхні) границі нечітких відношень і нижні (верхні) границі мір значимості загроз і збитків. Визначення значення вихідної змінної здійснюється шляхом операцій пониження типу і дефазифікації.

Ключові слова: модель, інформаційно-комунікаційна система, загроза, збиток, нечітка множина, функція належності інтервального типу, нечіткі відношення.

Постановка проблеми. Сучасний етап розвитку інформаційно-комунікаційних систем (ІКС) характеризується їх масовим упровадженням у всі сфери суспільного життя: військову справу, державне управління, економіку, фінанси, промисловість тощо. Впровадження цифрових технологій забезпечує ефективність та швидкість обробки даних, проте одночасно підвищує залежність від кіберпростору та збільшує ризик виникнення загроз інформаційний безпеці. У сучасному кіберсередовищі атаки стають більш складними та багатофазними: від кібершпигунству та фішингу до цільових атак на критичну інфраструктуру. Часто атаки

реалізуються при неповній або розмитій інформації про систему та її механізми захисту, що ускладнює їх своєчасне виявлення та оцінку. Класичні методи оцінки захищеності ІКС базуються на обробці чітких статистичних даних про загрози та збитки. Проте на практиці інформація про ймовірність атак і масштаби збитків часто є неповною, суперечливою або подається у вигляді лінгвістичних категорій (“високий ризик загрози”, “значні збитки”). У таких умовах традиційні методи демонструють обмежену ефективність на низьку точність такої оцінки [1], [2]. Це зумовлює потребу у створені систем оцінки, здатних працювати з нечіткою інформацією та встановлювати причинно-наслідкові зв’язки між загрозами й можливими збитками.

Аналіз останніх досліджень і публікацій. Під загрозою у сфері інформаційної безпеки розуміють потенційну можливість реалізації небажаного впливу на інформаційні ресурси або інфраструктуру. Наслідком реалізації загрози є збитки, що можуть мати як кількісний вимір (витрати на відновлення, зниження продуктивності), так і якісний (втрата довіри, порушення репутації). Таким чином, у системі інформаційної безпеки загроза виступає причиною, а збитки – наслідком, що може бути використано для виявлення реалізованих атак та оцінки рівня захищеності ІКС.

На сьогодні запропоновано декілька методів оцінки захищеності ІКС. Статистичні та ймовірнісні методи ґрунтуються на аналізі історичних даних для визначення частоти загроз і очікуваних збитків. Вони забезпечують строгий математичний апарат, але обмежені у випадках нових атак, для яких відсутня статистика, а також неможливості враховувати нечіткі або якісні оцінки [3]. **Методи аналізу сценаріїв (attack trees, attack graphs) моделюють послідовність дій зловмисника та можливі збитки. Вони зручні для прогнозування збитків для різних атак, однак складні у використанні для великих систем та не враховують невизначеність** [4]. Експертні методи базуються на залученні фахівців до оцінки ймовірності загроз і можливих збитків. Ефективні за відсутності статистики, але є суб’єктивними. Методи на основі нечіткої логіки дозволяють інтегрувати кількісні та якісні оцінки, працювати з неповними даними та формалізувати лінгвістичні терми. Головним обмеженням є складність побудови функцій належності та залежність від якості експертних знань [5]-[7]. Гібридні методи, що поєднують нечітку логіку з машинним навчанням забезпечують адаптивність, високу точність, здатність до самонавчання, але вимагають значних обчислювальних ресурсів та якісних навчальних вибірок [8], [9].

Одним з перспективних шляхів формалізації експертної інформації при моделюванні причинно-наслідкових зв’язків є теорія нечітких множин [10]. Розв’язання задачі оцінки захищеності передбачає ідентифікацію залежності входи (загрози) – виходи (збитки) [11], [12]. Особливість моделювання полягає у визначенні характеру цієї залежності в умовах невизначеності. Невизначеність виникає через те, що різні люди розуміють слова (терми) по-різному, а також через неточність вхідних даних [13]. Оперувати даними типами невизначеності можливо засобами нечіткої логіки. Моделювання і мінімізація наслідків невизначеності здійснюється шляхом побудови нечітких систем ІІ типу, які спроможні оперувати з усіма типами невизначеності [14]. Для побудови таких систем використовуються функції належності ІІ типу, серед яких найбільш поширеними є функції належності інтервального типу. Носієм моделі оцінки захищеності ІКС є експертні висловлювання типу “Загроза-збиток”.

Задача оцінки загроз або захищеності ІКС на основі відомих збитків має важливе значення з кількох причин. По-перше, вона дозволяє перейти від якісного опису ризиків до кількісних оцінок, що створює підґрунтя для економічного обґрунтування рішень. По-друге, аналіз збитків дозволяє визначити пріоритетні загрози та оптимізувати ресурси на захист,

орієнтуючись на найбільш критичні сценарії. По-третє, відкриває можливості для застосування сучасних математичних методів моделювання невизначеності у сфері інформаційної безпеки.

Метою статті є побудова моделі оцінки захищеності ІКС через потенційні збитки в якій для моделювання і мінімізація наслідків невизначеності використовуються нечіткі відношення.

Виклад основного матеріалу дослідження. Нехай відомо:

– множина вхідних змінних $X = (x_1, x_2, \ldots, x_n),\ x_i \in [\underline{x_i}, \overline{x_i}],\ i = \overline{1,n};$

– множина вихідних змінних $Y = (y_1, y_2, \ldots, y_m),\ y_j \in [\underline{y_j}, \overline{y_j}],\ j = \overline{1,m};$

– множина загроз $T = (t_1, t_2, \ldots, t_n),$ де загроза $t_i,\ i = \overline{1, n},$ інтерпретується як нечіткий терм, що описує змінну x_i;

– множина збитків $L = (l_1, l_2, \ldots, l_m),$ де збиток $l_j,\ j = \overline{1, m},$ інтерпретується як нечіткий терм, що описує змінну y_j;

– відношення між загрозами і збитками $R \subseteq T \times L.$

Задача оцінки захищеності ІКС може формулюватись у формі прямого і оберненого логічного виведення. При прямому логічному виведенні необхідно визначити збитки $L^* = (l_1^*, l_2^*, \ldots, l_m^*)$ для заданого вектора вхідних змінних $X^* = (x_1^*, x_2^*, \ldots, x_n^*)$. При оберненому логічному виведенні необхідно відновити загрози $T^* = (t_1^*, t_2^*, \ldots, t_n^*)$ для заданого вектора вихідних змінних $Y^* = (y_1^*, y_2^*, \ldots, y_m^*)$ та по ним оцінити захищеність. Розв'язання останньої задачі вимагає побудови моделі на базі нечітких відношень.

На рис. 1 представлена структура нечіткої моделі оцінки захищеності ІКС ІІ типу, яка містить п'ять блоків. Блок фазифікації перетворює значення вхідних змінних в міру значимості загроз. Композиційне правило виведення Заде зв'язує міри значимості загроз і збитків за допомогою нечітких відношень. Блок пониження типу перетворює вихідні нечіткі множини ІІ типу в нечіткі множини І типу. Блок дефазифікації перетворює міри значимості збитків у значення вихідних змінних.

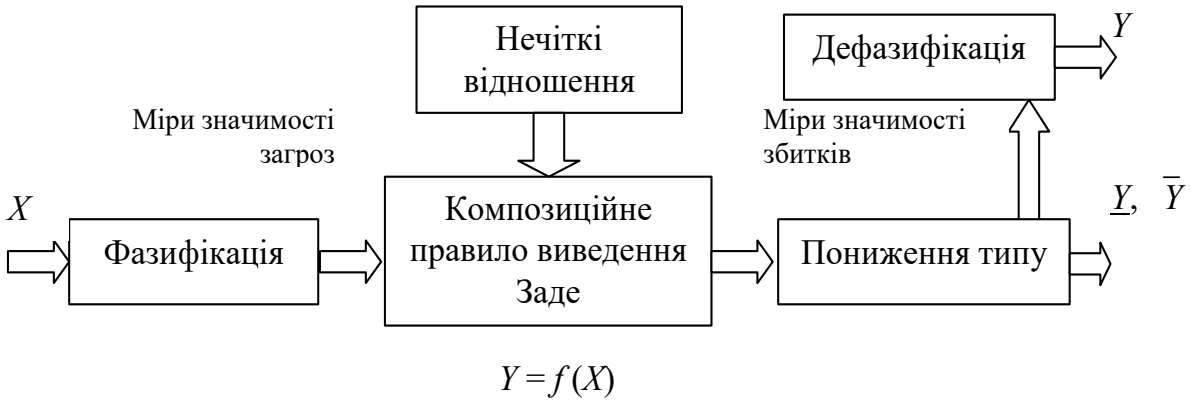

Рисунок 1 – Структура нечіткої моделі оцінки захищеності ІКС ІІ типу

Моделювання причинно-наслідкових зв'язків здійснюється шляхом інтерпретації композиційного правила виведення Заде [10]:

$$\widetilde{B} = \widetilde{A} \circ \widetilde{R}, \tag{1}$$

де $\widetilde{A}$ і $\widetilde{B}$ – нечіткі множини II типу, задані на універсальних множинах T і L:

$$\widetilde{A} = \left(\frac{\mu^{\widetilde{t}_1}}{t_1}, \frac{\mu^{\widetilde{t}_2}}{t_2}, \ldots, \frac{\mu^{\widetilde{t}_n}}{t_n} \right), \ \widetilde{B} = \left(\frac{\mu^{\widetilde{l}_1}}{l_1}, \frac{\mu^{\widetilde{l}_2}}{l_2}, \ldots, \frac{\mu^{\widetilde{l}_m}}{l_m} \right).$$

Тут $\mu^{\widetilde{t}_i}$ $(i = \overline{1, n})$ і $\mu^{\widetilde{l}_j}$ $(j = \overline{1, m})$ – міри значимості загроз t_i і збитків l_j, що визначаються як інтервальні нечіткі множини II типу, задані на універсальних множинах $a_i = [\underline{a_i}, \overline{a_i}] \subset [0,1]$ і $b_j = [\underline{b_j}, \overline{b_j}] \subset [0,1]$;

$\widetilde{R}$ – матриця нечітких відношень з елементами $\mu_{ij}^{\widetilde{R}}$, $i = \overline{1, n}$, $j = \overline{1, m}$, де $\mu_{ij}^{\widetilde{R}}$ – інтервальна нечітка множина II типу, задана на універсальній множині $r_{ij} = [\underline{r_{ij}}, \overline{r_{ij}}] \subset [0,1]$, що характеризує ступінь впливу загрози t_i на виникнення збитку l_j;

° – операція розширеної max-min композиції [13].

Із співвідношення (1) слідує система рівнянь нечітких відношень:

$$\begin{gathered}
\mu^{\widetilde{l}_1} = (\mu^{\widetilde{t}_1} \prod \mu_{11}^{\widetilde{R}}) \bigsqcup (\mu^{\widetilde{t}_2} \prod \mu_{21}^{\widetilde{R}}) \bigsqcup \ldots \bigsqcup (\mu^{\widetilde{t}_n} \prod \mu_{n1}^{\widetilde{R}}) \\
\mu^{\widetilde{l}_2} = (\mu^{\widetilde{t}_1} \prod \mu_{12}^{\widetilde{R}}) \bigsqcup (\mu^{\widetilde{t}_2} \prod \mu_{22}^{\widetilde{R}}) \bigsqcup \ldots \bigsqcup (\mu^{\widetilde{t}_n} \prod \mu_{n2}^{\widetilde{R}}) \\
\ldots \qquad \ldots \qquad \ldots \\
\mu^{\widetilde{l}_m} = (\mu^{\widetilde{t}_1} \prod \mu_{1m}^{\widetilde{R}}) \bigsqcup (\mu^{\widetilde{t}_2} \prod \mu_{2m}^{\widetilde{R}}) \bigsqcup \ldots \bigsqcup (\mu^{\widetilde{t}_n} \prod \mu_{nm}^{\widetilde{R}})
\end{gathered}$$

або

$$\mu^{\widetilde{l}_j} = \bigsqcup_{i=1,n} (\prod (\mu^{\widetilde{t}_i}, \mu_{ij}^{\widetilde{R}})), \ j = \overline{1, m}. \tag{2}$$

Враховуючи, що результатом виконання операції $\bigsqcup(\prod)$ над інтервальними множинами є інтервальна множина, область визначення якої утворена шляхом застосування операцій max (min) до границь областей визначення операндів, то система (2) переписується у вигляді двох систем

$$\begin{gathered}
\underline{b_1} = (\underline{a_1} \wedge \underline{r_{11}}) \vee (\underline{a_2} \wedge \underline{r_{21}}) \vee \ldots \vee (\underline{a_n} \wedge \underline{r_{n1}}); \\
\underline{b_2} = (\underline{a_1} \wedge \underline{r_{12}}) \vee (\underline{a_2} \wedge \underline{r_{22}}) \vee \ldots \vee (\underline{a_n} \wedge \underline{r_{n2}}); \\
\ldots \qquad \ldots \qquad \ldots \\
\underline{b_m} = (\underline{a_1} \wedge \underline{r_{1m}}) \vee (\underline{a_2} \wedge \underline{r_{2m}}) \vee \ldots \vee (\underline{a_n} \wedge \underline{r_{nm}})
\end{gathered}$$

та

$$\begin{gathered}
\overline{b_1} = (\overline{a_1} \wedge \overline{r_{11}}) \vee (\overline{a_2} \wedge \overline{r_{21}}) \vee \ldots \vee (\overline{a_n} \wedge \overline{r_{n1}}); \\
\overline{b_2} = (\overline{a_1} \wedge \overline{r_{12}}) \vee (\overline{a_2} \wedge \overline{r_{22}}) \vee \ldots \vee (\overline{a_n} \wedge \overline{r_{n2}}); \\
\ldots \qquad \ldots \qquad \ldots \\
\overline{b_m} = (\overline{a_1} \wedge \overline{r_{1m}}) \vee (\overline{a_2} \wedge \overline{r_{2m}}) \vee \ldots \vee (\overline{a_n} \wedge \overline{r_{nm}}),
\end{gathered}$$

або

$$\begin{gathered}
\underline{b_j} = \max_{i=1,n} [\min(\underline{a_i}, \underline{r_{ij}})], \\
\overline{b_j} = \max_{i=1,n} [\min(\overline{a_i}, \overline{r_{ij}})], j = \overline{1, m}.
\end{gathered} \tag{3}$$

Для визначення мір значимості загроз пропонується використовувати функції належності $\mu^{\widetilde{t}_i}(x_i)$ вхідної змінної x_i до нечіткого терму загрози t_i. Для визначення нижніх

границь мір значимості загроз $\underline{a_i}$ використовується нижня функція належності $\underline{\mu^{\tilde{t}_i}}(x_i)$, а для визначення верхніх границь $\overline{a_i}$ – верхня функція належності $\overline{\mu^{\tilde{t}_i}}(x_i)$. Для визначення мір значимості збитків використовуються функції належності $\mu^{\tilde{l}_j}(y_j)$ вихідної змінної y_j до нечіткого терму збитку l_j. Для визначення нижніх границь мір значимості збитків $\underline{b_j}$ використовується нижня функція належності $\underline{\mu^{\tilde{l}_j}}(y_j)$, а для визначення верхніх границь $\overline{b_j}$ – верхня функція належності $\overline{\mu^{\tilde{l}_j}}(y_j)$. Для моделювання невизначеності пропонується використовувати функцію належності II типу $\mu^{\tilde{K}}(u)$, яка визначається нижньою $\underline{\mu^{\tilde{K}}}(u)$ і верхньою $\overline{\mu^{\tilde{K}}}(u)$ функціями належності I типу, які описуються співвідношеннями [13]:

$$\underline{\mu^{\tilde{K}}}(u)=\begin{cases}\mu(u,\overline{g^{\tilde{K}}},c^{\tilde{K}}),\ \text{якщо}\ u<\dfrac{\underline{g^{\tilde{K}}}+\overline{g^{\tilde{K}}}}{2}\\ \mu(u,\underline{g^{\tilde{K}}},c^{\tilde{K}}),\ \text{якщо}\ u\geq\dfrac{\underline{g^{\tilde{K}}}+\overline{g^{\tilde{K}}}}{2}\end{cases},$$

$$\overline{\mu^{\tilde{K}}}(u)=\begin{cases}\mu(u,\underline{g^{\tilde{K}}},c^{\tilde{K}}),\ \text{якщо}\ u<\underline{g^{\tilde{K}}}\\ 1,\ \text{якщо}\ \underline{g^{\tilde{K}}}\leq u\leq\overline{g^{\tilde{K}}}\\ \mu(u,\overline{g^{\tilde{K}}},c^{\tilde{K}}),\ \text{якщо}\ u>\overline{g^{\tilde{K}}}\end{cases}.\qquad(4)$$

де $g\in[\underline{g},\overline{g}]$ – координата максимуму функції, $\mu^{\tilde{K}}(g)=1$;

c – коефіцієнт концентрації-розтягнення функції (рис. 2).

Для нечіткого терму K діапазон $g\in[\underline{g},\overline{g}]$ представляє найбільш можливе значення змінної u. Функція $\mu^{\tilde{K}}(u)$ є інтервальною функцією належності, тобто вторинна функція належності $\mu^{\tilde{K}}(u^*)$ є інтервальною нечіткою множиною з областю визначення $\mu^{\tilde{K}}(u^*)=[\underline{\mu^{\tilde{K}}}(u^*),\overline{\mu^{\tilde{K}}}(u^*)]$.

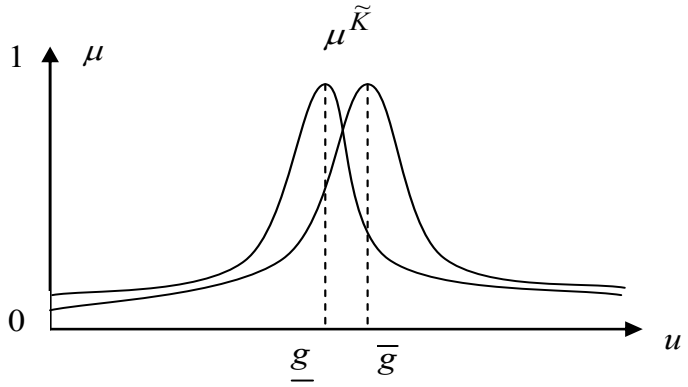

Рисунок 2 – Модель функції належності II типу

Операції над вхідними і вихідними нечіткими множинами ілюструють рис. 3 та 4.

При визначенні ступеня належності конкретного значення вхідної змінної x_i^* до нечіткого терму t_i, передбачається два випадки. В першому випадку результат вимірювання

вважається точним і в співвідношення (4) підставляються значення x_i^* (рис. 3а):

$$\mu^{\tilde{t}_1}(x_1^*) = [\underline{\mu^{\tilde{t}_1}}(x_1^*), \overline{\mu^{\tilde{t}_1}}(x_1^*)] = [\underline{a_1}, \overline{a_1}];$$
$$\mu^{\tilde{t}_2}(x_2^*) = [\underline{\mu^{\tilde{t}_2}}(x_2^*), \overline{\mu^{\tilde{t}_2}}(x_2^*)] = [\underline{a_2}, \overline{a_2}];$$
$$\dots \quad \dots \quad \dots$$
$$\mu^{\tilde{t}_n}(x_n^*) = [\underline{\mu^{\tilde{t}_n}}(x_n^*), \overline{\mu^{\tilde{t}_n}}(x_n^*)] = [\underline{a_n}, \overline{a_n}].$$

В другому випадку результати вимірювання спотворені шумом з відомим середнім відхиленням. Тоді значення вхідної змінної задається у вигляді функції належності μ_i^* з параметрами (x_i^*, c_i^*). В цьому випадку нижня і верхня границі ступеня належності конкретного значення вхідної змінної x_i^* до нечіткого терму t_i визначаються за формулами (рис. 3б):

$$\begin{aligned} \underline{\mu^{\tilde{t}_1}}(x_1^*) &= \sup[\min(\mu_i^*(x_i^*), \underline{\mu^{\tilde{t}_1}}(x_1^*))], \\ \overline{\mu^{\tilde{t}_1}}(x_1^*) &= \sup[\min(\mu_i^*(x_i^*), \overline{\mu^{\tilde{t}_1}}(x_1^*))]. \end{aligned} \quad (5)$$

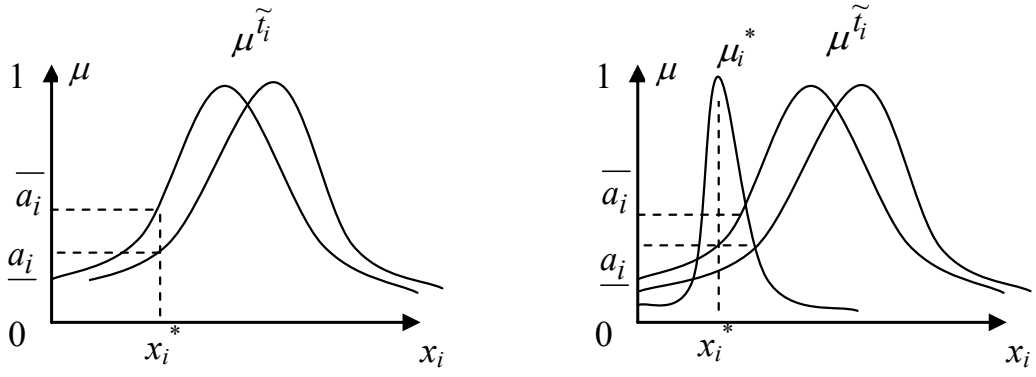

Рисунок 3 – Формування мір значимості загроз
а) при точних вхідних даних, б) якщо вхідні дані спотворені шумом

Міри значимості збитків дозволяють сформувати вихідні нечіткі множини $\tilde{W}_j(y_j)$. Функція належності нечіткої множини $\tilde{W}_j$ формується на основі співвідношення (рис. 4):

$$\mu^{\tilde{W}_j}(y) = \prod(b_j, \mu^{\tilde{l}_j}(y)), \quad (6)$$

де нижня і верхня функції належності вихідної нечіткої множини $\tilde{W}_j$ визначаються за формулами:

$$\begin{aligned} \underline{\mu^{\tilde{W}_j}}(y_j) &= \min(\underline{b_j}(X), \underline{\mu^{\tilde{l}_j}}(y_j)), \\ \overline{\mu^{\tilde{W}_j}}(y_j) &= \min(\overline{b_j}(X), \overline{\mu^{\tilde{l}_j}}(y_j)). \end{aligned} \quad (7)$$

Для отримання кількісних значень вихідних змінних y_j, що відповідають нечітким множинам (6) необхідно виконати операцію пониження типу і дефазифікації [13]. Результатом виконання операції пониження типу є значення центроїду вихідної нечіткої множини $\tilde{W}_j(y_j)$,

що представляє собою інтервальну нечітку множину I типу y_j^{DR} з областю визначення $y_j^{DR} = [y_j^l, y_j^r]$. Для знаходження центроїду діапазон $[\underline{y_j}, \overline{y_j}]$ змінення змінної y_j дискретизується на N точок. Відповідно операція пониження типу виконується за формулами:

$$y_j^l(X) = \frac{\sum_{k=1}^{N} y_j^k h_k^l}{\sum_{k=1}^{L(X)} \mu^{\overline{W_j}}(X) + \sum_{k=L(X)+1}^{N} \mu^{\underline{W_j}}(X)}, \quad h_k^l = \begin{cases} \mu^{\overline{W_j}}(X), \text{ якщо } k \le L(X) \\ \mu^{\underline{W_j}}(X), \text{ якщо } k > L(X) \end{cases}$$

$$y_j^r(X) = \frac{\sum_{k=1}^{N} y_j^k h_k^r}{\sum_{k=1}^{R(X)} \mu^{\underline{W_j}}(X) + \sum_{k=R(X)+1}^{N} \mu^{\overline{W_j}}(X)}, \quad h_k^r = \begin{cases} \mu^{\underline{W_j}}(X), \text{ якщо } k \le R(X) \\ \mu^{\overline{W_j}}(X), \text{ якщо } k > R(X) \end{cases} \tag{8}$$

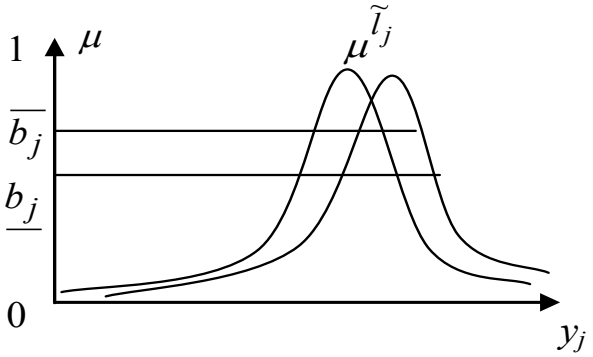

Рисунок 4 – Формування вихідної нечіткої множини

Операція дефазифікації зводиться до знаходження середнього значення:

$$y_j = \frac{y_j^l + y_j^r}{2}. \tag{9}$$

Співвідношення (1)-(9) визначають залежність $Y = f_{\tilde{R}}(X)$ у вигляді:

$$y_1 = f_1^{\text{II}}(X, \tilde{R}, C_X, \underline{G_{\tilde{T}}}, \overline{G_{\tilde{T}}}, C_{\tilde{T}}, \underline{g^{\tilde{l}_1}}, \overline{g^{\tilde{l}_1}}, c^{\tilde{l}_1});$$

$$y_2 = f_2^{\text{II}}(X, \tilde{R}, C_X, \underline{G_{\tilde{T}}}, \overline{G_{\tilde{T}}}, C_{\tilde{T}}, \underline{g^{\tilde{l}_2}}, \overline{g^{\tilde{l}_2}}, c^{\tilde{l}_2});$$

$$\dots \qquad \dots \qquad \dots$$

$$y_m = f_m^{\text{II}}(X, \tilde{R}, C_X, \underline{G_{\tilde{T}}}, \overline{G_{\tilde{T}}}, C_{\tilde{T}}, \underline{g^{\tilde{l}_m}}, \overline{g^{\tilde{l}_m}}, c^{\tilde{l}_m})$$

або

$$Y = f_R^{\text{II}}(X, \tilde{R}, C_X, \underline{G_{\tilde{T}}}, \overline{G_{\tilde{T}}}, C_{\tilde{T}}, \underline{G_{\tilde{L}}}, \overline{G_{\tilde{L}}}, C_{\tilde{L}}), \tag{10}$$

де $X = (x_1, x_2, \dots, x_n)$ – вектор вхідних змінних;

$\tilde{R} = \{[r_{ij}, \overline{r_{ij}}]\}$ – матриця інтервальних нечітких відношень II типу;

$C_X = (c_1^*, c_2^*, \dots, c_n^*)$ – вектор параметрів концентрації функцій належності, що моделюють неточність вхідних даних;

$\underline{G_{\tilde{T}}} = (\underline{g^{\tilde{l}_1}}, \underline{g^{\tilde{l}_2}}, \dots, \underline{g^{\tilde{l}_n}})$, $\overline{G_{\tilde{T}}} = (\overline{g^{\tilde{l}_1}}, \overline{g^{\tilde{l}_2}}, \dots, \overline{g^{\tilde{l}_n}})$, $C_{\tilde{T}} = (c^{\tilde{l}_1}, c^{\tilde{l}_2}, \dots, c^{\tilde{l}_n})$ – вектори параметрів

нижніх і верхніх функцій належності вхідних змінних до термів загроз $t_1, t_2, \ldots, t_n$;

$\underline{G_{\tilde{L}}} = (\underline{g^{\tilde{l}_1}}, \underline{g^{\tilde{l}_2}}, \ldots, \underline{g^{\tilde{l}_m}})$, $\overline{G_{\tilde{L}}} = (\overline{g^{\tilde{l}_1}}, \overline{g^{\tilde{l}_2}}, \ldots, \overline{g^{\tilde{l}_m}})$, $C_{\tilde{L}} = (c^{\tilde{l}_1}, c^{\tilde{l}_2}, \ldots, c^{\tilde{l}_m})$ – вектори параметрів нижніх і верхніх функцій належності вихідних змінних до термів збитків $l_1, l_2, \ldots, l_m$;

f_R^{II} – оператор зв'язку "входи-виходи" для нечіткої системи II типу, що відповідає співвідношенням (1)-(9).

Побудована модель оцінки захищеності ІКС на базі нечітких відношень II типу (10) оперує з невизначеністю шляхом використання інтервальних функції належності нечітких термів загроз і збитків, а також використовує функції належності I типу, які дозволяють моделювати неточність вхідних даних.

Висновки. Таким чином побудована модель оцінки захищеності ІКС через потенційні збитки на базі нечітких відношень II типу (10), які спроможні оперувати з усіма типами невизначеності. Нечіткі терми загроз і збитків формалізуються інтервальними функціями належності II типу, в результаті чого міри значимості загроз і збитків визначаються інтервалами. Нечітка модель II типу будується на основі розширеного композиційного правила виведення Заде, з якого випливають дві системи рівнянь нечітких відношень. Ці системи пов'язують нижні (верхні) границі нечітких відношень і нижні (верхні) границі мір значимості загроз і збитків. Визначення значення вихідної змінної здійснюється шляхом операцій пониження типу і дефазифікації.

Перспективним напрямком подальших досліджень є розгляд методів побудова нечітких відношень які враховують як невизначеність у функціях належності нечітких термів, так і розбіжностей у висновках експертів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] N.R. Pokhrel, and C.P. Tsokos, "Cybersecurity: A stochastic predictive model to determine overall network security risk using Markovian process", *Journal of Information Security*, vol. 8, no. 2, pp. 91-105, Apr. 2017. doi: https://doi.org/10.4236/jis.2017.82007.

[2] О.А. Ревнюк, Н.В. Загорода, та О.С. Улічев, "Адаптивна методологія розрахунку кількісного показника стану захищеності вебзастосунків", *Центральноукраїнський науковий вісник. Технічні науки*, вип. 10 (41), ч. II, с. 3-10, 2024. doi: https://doi.org/10.32515/2664-262X.2024.10(41).2.3-10.

[3] M. Alali, N. Almakhadmen, and M. Mafarja, "Improving risk assessment model of cyber security using fuzzy logic inference system", Procedia Computer Science, vol. 141, pp. 436-443, 2018. doi: https://doi.org/10.1016/j.cose.2017.09.011.

[4] N.K. N. Dang, M. Lopuhaä-Zwakenberg, and M. Stoelinga, "Fuzzy quantitative attack tree analysis" in *Proc 27th Inter. Conf. Fundamental Approaches to Software Engineering (FASE 2024)*, Luxembourg City, Luxembourg, 2024, pp. 210-231. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-031-57259-3_10?utm_source=chatgpt.com. Accessed on: May 10, 2025.

[5] S. Kerimkhulle, Z. Dildebayeva, A. Tokhmetov, A. Amirova, J. Tussupov, U. Makhazhanova, A. Adalbek, R. Taberkhan, A. Zakirova, and A. Salykbayeva, "Fuzzy logic and its application in the assessment of information security risk of industrial internet of things", *Symmetry*, vol. 15, art. 1958, 29 p., 2023. doi: https://doi.org/10.3390/sym15101958.

[6] A.A. Tubis, S. Werbińska-Wojciechowska, M. Góralczyk, A. Wróblewski, and B. Ziętek, "Cyber-attacks risk analysis method for different levels", *Sensors (Basel). 2020 Dec 16;*

20 (24):7210. doi: https://doi.org/10.3390/s20247210.

[7] І. Субач, та В. Кубрак, "Модель ідентифікації кіберінцидентів SIEM-системою для захисту інформаційно-комунікаційних систем", *Кібербезпека: освіта, наука, техніка*, № 4 (20), с. 81-92, 2023. doi: https://doi.org/10.28925/2663-4023.2023.20.8192.

[8] P. Cheimonidis, and K. Rantos, "Dynamic risk assessment in cybersecurity: A systematic review", *Future Internet*, vol. 15, art. 324, 25 p., 2023. doi: https://doi.org/10.3390/fi15100324.

[9] O. Kozlenko, "An example of fuzzy ontology usage for risk assessment and attack impact", in *Proc. 2024 IEEE Int. Conf. on Advanced Trends in Information Theory (ATIT)*, Kyiv, Ukraine, 2024, pp. 123-127. doi: https://doi.org/10.20535/tacs.2664-29132024.1.312677.

[10] L.A. Zadeh, "The Concept of a Linguistic Variable and Its Application to Approximate Reasoning-I", *Information Sciences*, no. 8, pp. 199-249, 1975. doi: http://dx.doi.org/10.1016/0020-0255(75)90036-5.

[11] А.П. Ротштейн, *Интеллектуальные технологии идентификации: нечеткие множества, генетические алгоритмы, нейронные сети*. Винница, Україна: УНІВЕРСУМ-Вінниця, 1999.

[12] Б.М. Герасимов, В.М. Локазюк, О.Г. Оксіюк, та О.В. Поморова, *Інтелектуальні системи підтримки прийняття рішень*. Київ, Україна: Європейський університет, 2007.

[13] J Mendel, *Uncertain Rule-Based Fuzzy Logic Systems*: *Introduction and New Direction*. Prentice-Hall, Englewood Cliffs, NJ, USA, 2001.

[14] О. П. Ротштейн, та Г. Б. Ракитянська, "Діагностика на базі багатовимірних нечітких відношень в умовах невизначеності", *Системні дослідження та інформаційні технології*, № 2, с. 97-111, 2015.

Стаття надійшла до редакції 10.08.2025.

REFERENCE

[1] N.R. Pokhrel, and C.P. Tsokos, "Cybersecurity: A stochastic predictive model to determine overall network security risk using Markovian process", *Journal of Information Security*, vol. 8, no. 2, pp. 91-105, Apr. 2017. doi: https://doi.org/10.4236/jis.2017.82007.

[2] O.A. Revnyuk, N.V. Zagorod, and O.S. Ulichev, "Adaptive methodology for calculating the quantitative indicator of the security status of web applications", *Central Ukrainian Scientific Bulletin. Technical Sciences*, iss. 10 (41), part. II, pp. 3-102024. doi: https://doi.org/10.32515/2664-262X.2024.10(41).2.3-10.

[3] M. Alali, N. Almakhadmen, and M. Mafarja, "Improving risk assessment model of cyber security using fuzzy logic inference system", Procedia Computer Science, vol. 141, pp. 436-443, 2018. doi: https://doi.org/10.1016/j.cose.2017.09.011.

[4] N.K. N. Dang, M. Lopuhaä-Zwakenberg, and M. Stoelinga, "Fuzzy quantitative attack tree analysis" in *Proc 27th Inter. Conf. Fundamental Approaches to Software Engineering (FASE 2024)*, Luxembourg City, Luxembourg, 2024, pp. 210-231. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-031-57259-3_10?utm_source=chatgpt.com. Accessed on: May 10, 2025.

[5] S. Kerimkhulle, Z. Dildebayeva, A. Tokhmetov, A. Amirova, J. Tussupov, U. Makhazhanova, A. Adalbek, R. Taberkhan, A. Zakirova, and A. Salykbayeva, "Fuzzy logic and its application in the assessment of information security risk of industrial internet of things", *Symmetry*, vol. 15, art. 1958, 29 p., 2023. doi: https://doi.org/10.3390/sym15101958.

[6] A.A. Tubis, S. Werbińska-Wojciechowska, M. Góralczyk, A. Wróblewski, and B. Ziętek, "Cyber-attacks risk analysis method for different levels", *Sensors (Basel). 2020 Dec 16;*

20 (24):7210. doi: https://doi.org/10.3390/s20247210.
[7] I. Subach, and V. Kubrak, "A model for identifying cyber incidents using a SIEM system for protecting information and communication systems", *Cybersecurity: Education, Science, Technology*, iss. 4 (20), pp. 81-92, 2023. doi: https://doi.org/10.28925/2663-4023.2023.20.8192.
[8] P. Cheimonidis, and K. Rantos, "Dynamic risk assessment in cybersecurity: A systematic review", *Future Internet*, vol. 15, art. 324, 25 p., 2023. doi: https://doi.org/10.3390/fi15100324.
[9] O. Kozlenko, "An example of fuzzy ontology usage for risk assessment and attack impact", in *Proc. 2024 IEEE Int. Conf. on Advanced Trends in Information Theory (ATIT)*, Kyiv, Ukraine, 2024, pp. 123-127. doi: https://doi.org/10.20535/tacs.2664-29132024.1.312677.
[10] L.A. Zadeh, "The Concept of a Linguistic Variable and Its Application to Approximate Reasoning-I", *Information Sciences*, no. 8, pp. 199-249, 1975. doi: http://dx.doi.org/10.1016/0020-0255(75)90036-5.
[11] A.P. Rotshteyn, *Intelligent Identification Technologies: Fuzzy Sets, Genetic Algorithms*, Neural Networks. Vinnytsia, Ukraine: UNIVERSUM-Vinnytsia, 1999.
[12] B.M. Gerasimov, V.M. Lokaziuk, O.G. Oksiyuk, and O.V. Pomorova, *Intelligent Decision Support Systems*. Kyiv, Ukraine: European University, 2007.
[13] J Mendel, *Uncertain Rule-Based Fuzzy Logic Systems*: *Introduction and New Direction*. Prentice-Hall, Englewood Cliffs, NJ, USA, 2001.
[14] O.P. Rotshtein, and G.B. Rakytyanska, "Diagnostics based on multidimensional fuzzy relations under conditions of uncertainty", *Systems Research and Information Technologies*, no. 2, pp. 97-111, 2015.

IGOR SAMOILOV,
MIKOLA KONOTOPETS,
ANTON STORCHAK,
SERHII SHOLOKHOV

MODEL OF ASSESSMENT OF THE SECURITY OF INFORMATION AND COMMUNICATION SYSTEMS BASED ON FUZZY VISIONS

The current stage of development of information and communication systems is characterized by their massive advances in all spheres of everyday life: military law, government, economics, finance, industry, etc. The advancement of digital technologies will ensure the efficiency and speed of data processing, while simultaneously increasing the risk of threats to information security in the cyberspace. The task of assessing the threat or the security of information and communication systems based on known intelligence is important for several reasons. First of all, it allows you to go from a clear description of the risks to comprehensive estimates, which creates a basis for an economical solution. In another way, the analysis of traffic jams allows you to identify priority threats and optimize defense resources, focusing on the most critical scenarios. Thirdly, it reveals the possibility of using current mathematical methods for modeling non-significance in the field of information security. Classic methods for assessing the security of information and communication systems are based on the collection of clear statistical data about the threats and attacks. However, in practice, information about the severity of attacks and the scale of traffic attacks is often inconsistent, overly sensitive, or presented in what appears to be linguistic categories ("high risk of threat", "significant losses"). In such minds, traditional methods demonstrate limited effectiveness due to the low accuracy of such assessments. This necessitates the need to create assessment systems that effectively deal with fuzzy information and establish cause-and-effect relationships between threats and potential losses.

The article proposes a model for assessing the security of information and communication systems through potential losses based on type II fuzzy relations. A special feature of the model is the ability to deal with types of non-significance in a comprehensive manner. Fuzzy terms of threats and losses are formalized by interval functions of type II reliability, as a result of which the world significance of threats and losses is determined at intervals. The type II fuzzy model will be based on the extended compositional rule of Zadeh's derivation, from which two systems of fuzzy relations are combined. These systems link the lower (upper) boundaries of fuzzy relationships and the lower (upper) boundaries of the world of significance of threats and losses. The value of the output variable is determined by type reduction and defuzzification operations.

Keywords: model, information and communication system, threat, loss, fuzzy multiplier, interval-type membership function, fuzzy relation.

Самойлов Ігор Володимирович, кандидат технічних наук, доцент, доцент кафедри безпеки державних інформаційних ресурсів, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0002-8251-9257, samoilov1966igor@gmail.com.

Конотопець Микола Миколайович, кандидат технічних наук, доцент, доцент кафедри безпеки державних інформаційних ресурсів, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0002-6963-1877, egorvetrovsky99@gmail.com.

Сторчак Антон Сергійович, кандидат технічних наук, доцент, доцент кафедри безпеки державних інформаційних ресурсів, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0002-5267-3122, storchakanton@gmail.com.

Шолохов Сергій Миколайович, кандидат технічних наук, доцент, доцент кафедри спеціальних телекомунікаційних систем, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0003-2222-8842, kit.docent71@gmail.com.

Samoilov Igor, candidate of technical sciences, associate professor, associate professor of the department of security of state information resources, Institute of special communication and information protection at the National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

Konotopets Mykola, candidate of technical sciences, associate professor, associate professor of the department of security of state information resources, Institute of special communication and information protection at the National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

Storchak Anton, candidate of technical sciences, associate professor, associate professor of the department of security of state information resources, Institute of special communication and information protection at the National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

Sholokhov Serhii, candidate of technical sciences, associate professor, associate professor of the electronic communications academic department, Institute of special communications and information protection at the National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.