УДК 004.896

П.Є. БИКОВИЙ
Тернопільський національний економічний університет

СИСТЕМА НЕЧІТКОГО ВИВОДУ ДЛЯ ОЦІНКИ РИЗИКІВ ВРАЗЛИВОСТІ СИСТЕМ БЕЗПЕКИ ПЕРИМЕТРУ ТЕРИТОРІЇ

В статті розглянуто методи оцінювання вразливості систем безпеки периметру території. Відповідні оцінки ґрунтуються на методах нечіткого виводу ризиків невиявлення порушників на множині охоронних зон, що охоплюють периметр території.

The methods estimating vulnerability of perimeter security systems are developed in the current study. Appropriate estimations are based on the fuzzy inference methods of intruder undetection risks on security zones set in territory's perimeter.

Ключові слова: периметр, вразливість, система безпеки.

Вступ

Системи безпеки та контролю доступу на сьогоднішній час стають все популярнішими [1]. Випускається велика кількість компонентів таких систем, що в свою чергу мають різні функціональні характеристики [2]. Не існує формального методу розв'язку задачі проектування системи безпеки з бажаним співвідношенням якості та ціни, тому дослідження в сфері автоматизації проектування систем безпеки периметру території є актуальними. Розв'язок такої задачі вимагає розробки міждисциплінарних методів з теорії оптимізації, комбінаторики і систем підтримки прийняття рішень.

Більшість публікацій теорії надійності із статичними та динамічними моделями (Лаплас, Баєс, Ватсон) [3] спрямовані на обчислення середнього часу напрацювання на відмову та їх частоти. Дані оцінки базуються на досвіді експлуатації систем. З іншого боку, імовірність відмови системи безпеки є значно меншою ніж її злам.

Технології обчислення надійності системи від зламування вимагає створення специфічних методів підтримки прийняття рішень. Системи нечіткого виводу є ефективним засобом для розв'язку такого типу задач в умовах слабкої визначеності функціональних характеристик сповіщувачів та різними типами порушників.

Задачею, що вимагає першочергового розв'язання, є формулювання функції мети і обмежень процесу автоматизованого проектування. Напрацювання щодо їх формулювання висвітлено в працях [4-6] де було описано технологію обробки параметрів компонентів систем безпеки, базу даних для їх зберігання та САПР проектування таких систем. В [7, 8] обговорено використання генетичних алгоритмів для оптимізації проектування систем безпеки, реалізованого в системі PSCAD. Порівняльний аналіз збіжності результатів генетичного алгоритму та алгоритму з обмеженим перебором показали перевагу генетичних алгоритмів при використанні великих за обсягом систем безпеки. Однак залишається проблема у кількісному оцінюванні значень ризику сформованих варіантів систем безпеки. Для її подолання доцільно використовувати технології підтримки прийняття рішень.

Оцінювання параметрів системи безпеки в умовах високого ступеня невизначеності її функціонування та відсутність загальної теорії, що формує методичні підвалини вивчення явищ з невизначеними факторами призводить до неможливості застосування класичних підходів теорії статистичних рішень. Тому при виборі альтернатив слід використовувати і обробляти якісну експертну інформацію. Перспективним напрямом розробки методів прийняття рішень при експертній вхідній інформації є лінгвістичний підхід на базі теорії нечітких множин і лінгвістичної змінної [9]. Основою для оцінювання систем безпеки можуть служити дані [10] щодо ймовірностей виявлення кожного виду загроз сповіщувачами (detector – англ., извещатель – рос.) різного типу. Користуючись наведеними у [10] можна розробити метод нечіткого виводу для оцінювання вразливості систем безпеки периметру території.

Мета роботи: розробка методів оцінювання вразливості систем безпеки шляхом використання методів екстремальної комбінаторики для побудови найменш вразливих систем безпеки з мінімізацією затрачених на їхнє впровадження коштів.

Формальний опис методу оцінювання вразливості систем безпеки

Оцінки вразливості системи безпеки периметру території обчислюються на основі ризиків невиявлення порушників на множині охоронних зон периметру території. Кожна зона периметру території специфічна своїм ландшафтом, сусідством з іншими зонами і об'єктами. Ця специфічність безпосередньо випливає на характер вимог, що ставляться до виявлення загроз на відповідній зоні. Крім того, кожна зона може характеризуватися різним ступенем значущості, відповідно до стратегічного значення об'єктів, що межують з цією зоною. Тому метод оцінювання вразливості систем безпеки доцільно спроектувати у вигляді дворівневої ієрархічної структури.

На першому рівні ієрархії знаходяться ступені значущості зон, на другому рівні – ризики невиявлення загроз в кожній зоні. Схематичне зображення ієрархії методу наведено на рис. 1.

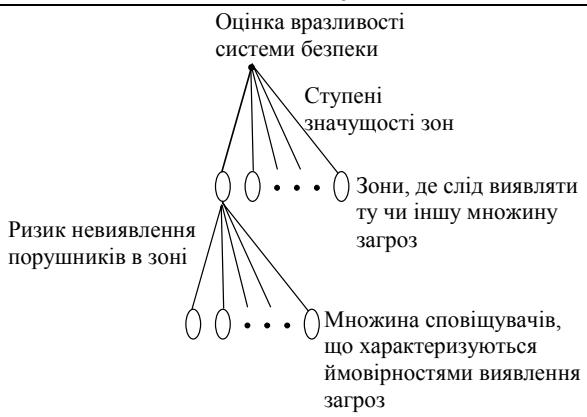


Рис. 1. Дворівнева ієрархічна структура оцінювання вразливості систем безпеки

Побудова системи нечіткого виводу на обидвох рівнях здійснюється в три етапи: означення множин входів і виходів; встановлення функцій належності для рівнів входів та виходів; формулювання набору нечітких правил виводу. Розробку методу оцінювання вразливості за описаною ієрархічною структурою слід проводити починаючи з другого рівня.

А. Другий рівень – опис ризику не виявлення порушників в зоні

На цьому рівгі входами є якісні оцінки спроможностей виявлення загроз кожного типу. Згідно з [10] виберемо множину 12-и входів якісних оцінок спроможностей виявлення порушень: дрібний крок, крок, біг, повзком, перекочуванням, стрибками, по „тунелю”, по канаві, по мості, пошкодження системи захисту, „перелаз” системи захисту, „підйом” системи захисту.

Функції належності рівнів входів вибрані однакового класу, їхня форма визначає ступінь толерантності до загрози того чи іншого виду. Всі входи описують лінгвістичну змінну „високий ризик”. Толерантність до загроз встановлюється шляхом налаштування параметру функції належності, що утворює сімейство функцій „високий ризик” різного ступеня

$$\mu = f(V)^{(1-\alpha_i)}, \tag{1}$$

де μ – значення функції належності, α_i – параметр сімейства функцій для *i*-того входу $(0 \le a_i < 1)$, $f(V)$ – базова функція належності класу Z, V – якісна оцінка спроможності виявлення загрози. Чим більше значення параметру α тим вищими є вимоги до надійності системи безпеки. Приклад сімейства функцій належності представлений на рис. 2, де значення V належить діапазону від 0 до 1.

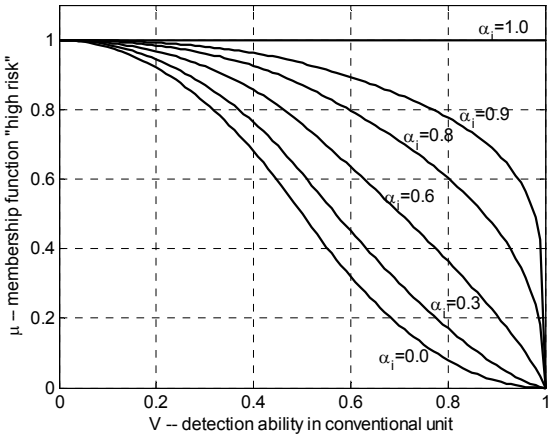


Рис. 2. Сімейство вхідних функцій належності різного рівня толерантності

Введемо поняття класу зони, що враховує специфіку охорони зони, тобто які типи загроз необхідно виявляти на ній, який ландшафт та наявність і тип межуючих з нею об’єктів. Виходом системи є детермінована оцінка ризику невиявлення порушника з врахуванням класу зони. Згідно [11, 12], клас функцій належності Z входів системи та типу S – виходів системи найкраще відповідає специфіці поставленої задачі.

Набір нечітких правил виводу формулюється відповідно до класу зони. Наприклад для класу зони, де потрібно виявляти крок та пошкодження системи захисту будуть використовуватись наступні правила:

IF V(“дрібний крок”) = „високий ризик Level_1”
OR V(“біг”) = „високий ризик Level_2” (2)
THEN RISK = „високий ризик”,

де $V(\cdot)$ – якісна оцінка спроможності виявлення відповідної загрози, *високий ризик Level_1* та *високий ризик Level_2* – нечіткі множини рівня ризику різних ступенів, тобто *Level_1* із $a = a_1$ та *Level_2* із $a = a_2$, *OR* – нечіткий оператор АБО, який може бути або імовірнісним або класичним.

На першому рівні (див. рис. 1.), де описано властивості зон, метод обчислює інтегральну оцінку вразливості всієї системи безпеки, що складається з багатьох зон. Цей показник розраховується на основі ризиків невиявлення загроз в кожній зоні, як було описано в попередньому підрозділі. В процедурі обчислення кожній зоні присвоюється ступінь значущості $0 \le \beta_j < 1$, де j – індекс зони, $j = \overline{1, Z}$.

Входами системи на цьому рівні є виходи попереднього рівня. Оцінка вразливості обчислюється за формулою

$$VUL = RISK_1^{\beta_1} \ OR \ RISK_2^{\beta_2} \ OR \ldots OR \ RISK_N^{\beta_N}, \tag{3}$$

де VUL - детермінована оцінка вразливості системи безпеки, $RISK_j$ – ризик невиявлення загроз в *j-тій* зоні, *OR* – нечіткий оператор АБО, який може бути або імовірнісним або класичним.

Формула (3) може бути застосована тільки в тому випадку, коли коефіцієнти β_j, $j = \overline{1, Z}$ відомі і кожна зона захищена сповіщувачами однакового типу, тобто зони є однорідними. У випадку гетерогенної зони, можна застосувати підхід заміщення кожної зони на n однорідних підзон. Нехай l_z – довжина z-тої зони, $r_{z,i}$ – довжина i-ї однорідної підзони в z – й зоні, таким чином, щоб

$$l_z \le r_{z,1} + r_{z,2} + \cdots + r_{z,n}.$$

В кожній підзоні довжиною $r_{z,j}$ встановлюється деяке число відповідних еквівалентних сповіщувачів. Кожен i-й тип сповіщувача характеризується ризиком виявлення $RISK_{z,j}$. Тому ми можемо обчислити вразливості z-ї зони з використанням однієї з наступних формул:

$$VUL_z^{(1)} = \sum_{i=1}^{n} p_{z,i} RISK_{z,i}, \tag{4}$$

$$VUL_z^{(2)} = \max_{i=1\ldots n} \begin{cases} RISK_{z,i}, if \ \rho_{z,i} > 0, \\ 0, otherwise, \end{cases}, \tag{5}$$

$$VUL_z^{(3)} = \prod_{i=1}^{n} (1 + RISK_{z,i})^{\rho_{z,i}}, \tag{6}$$

$$VUL_z^{(4)} = \prod_{i=1}^{n} (1 + \rho_{z,i})^{1+RISK_{z,i}}, \tag{7}$$

$$VUL_z^{(5)} = \max_{i=1\ldots n} (1 + RISK_i)^{\rho_i}, \tag{8}$$

де $\rho_{z,i}$ являє собою частку i-тої підзони у загальній довжині зони l_z, оскільки $\rho_{z,i} = r_{z,i} / l_z$.

Загальна вразливість системи може бути розрахована у вигляді наступної формули:

$$VUL = \sum_{z=1}^{Z} VUL_z^{(k)},$$

де $VUL_z^{(k)}$ обчислюється за будь-якою із формул (4) – (8).

Результати експериментів

В даному розділі буде обговорено експериментальні результати для верифікації запропонованої системи нечіткого виводу. Для цього вибрано множину входів, що описують можливості виявлення “дрібного кроку” та “бігу”. Функції належності для даних входів вибираються з Z - класу і вони параметризуються відповідно до заданої імовірності відповідної загрози.

Для верифікації запропонованої системи нечіткого виводу використано пакет Fuzzy Logic Toolbox системи MATLAB. Входами системи на другому рівні є загрози виявлення “дрібного кроку” та “бігу”. Виходом є детерміністична оцінка ризику невиявлення даних двох загроз в зоні. Нечіткі правила виведення описані за допомогою методу Мамдані.

На рис. 3 приведено схему системи нечіткого виводу з зображенням входів оцінок імовірностей виявлення загроз виду дрібний крок та біг, вихід – детермінована оцінка вразливості системи. Правила нечіткого виводу позначаються прямокутником всередині „Perimeter Security Vulnerability” із зазначенням методу нечіткого виводу Мамдані. Оператори нечіткої логіки вибрано наступним чином: для методу „And method” – оператор перетину, для „Or method” – оператор об’єднання, оператори „Implication” та „Aggregation” не використовуються, для методу дефазифікації – „Defuzzification” використано оператор центру ваги (centre of gravity).

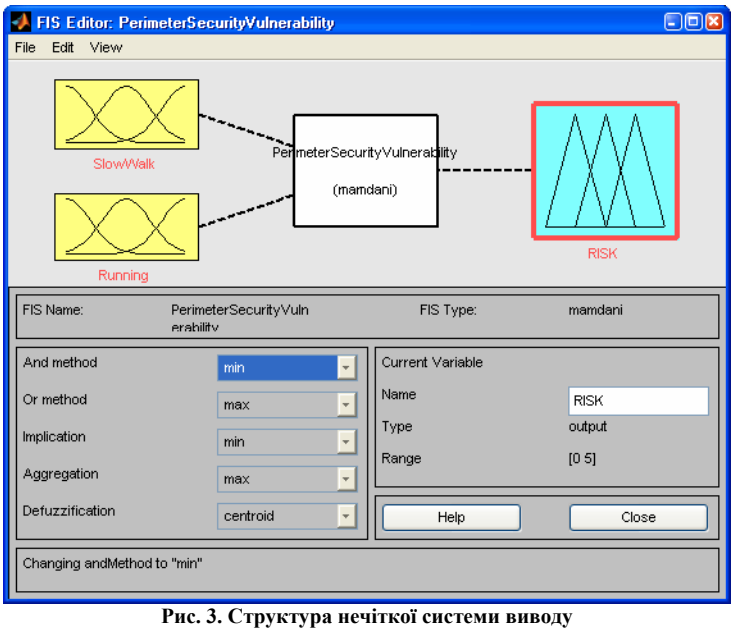


Рис. 3. Структура нечіткої системи виводу

Основними труднощами в налагодженні системи нечіткого виводу є вибір відповідних нечітких операторів, для подолання яких застосовується емпірична схема.

Класичний оператор "АБО", який є простим максимальним значенням всіх функцій належності, припускає, що при нульовій здатності виявлення для обох загроз, ризик вразливості досягає свого максимального значення 0,67. Підвищення здатності виявлення “дрібного кроку” до половини необхідної заданої імовірності та до її максимального значення не має ефекту. Такий же результат був отриманий при призначенні тих самих граничних значень для виявлення загрози “біг”. Центральні значення "0,179; 0,441" для обох здібностей виявлення загроз “дрібного кроку” та “бігу” призводить до зниження ризику вразливості до 0,623, даючи прибуток 0,047. Продовжуючи збільшення здатності виявлення загроз “дрібного кроку” та “бігу”, було знайдене граничне значення в діапазоні між 0,219 і 0,234. Це означає, що подальше підвищення здатності виявлення загроз “дрібного кроку” та “бігу” до 0,234 ніяк не впливає на значення ризику, залишаючись постійним 0,604. Збільшення оцінки здатності виявлення загрози “біг” призводить до одночасного зсуву порогу. Цей результат визначає обмежувальний фактор можливості виявлення загрози “біг”.

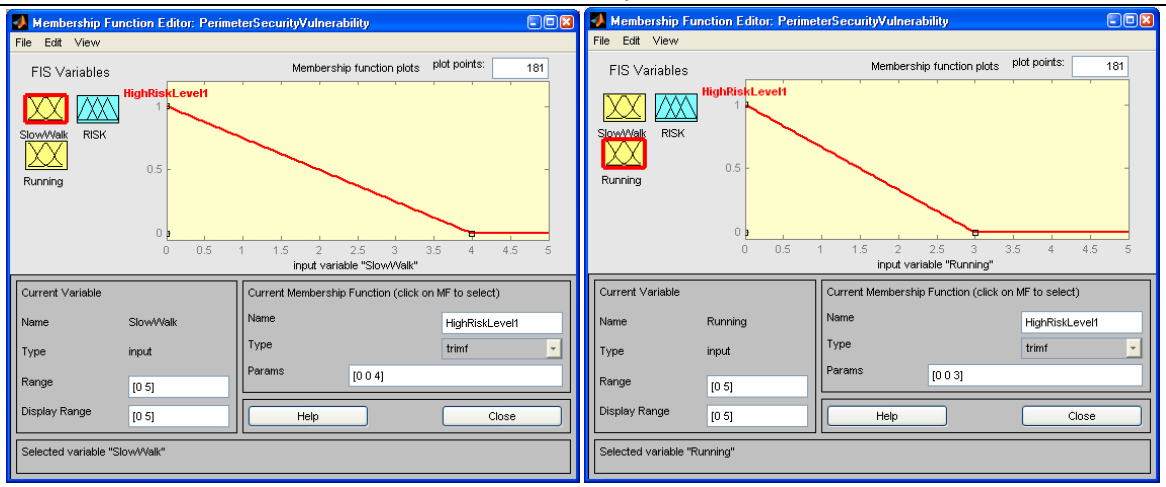
Оскільки імовірнісне "АБО" $Y = A + B - AB$ не має такого порогового ефекту, можна зробити висновок, що імовірнісне "АБО" доречніший для визначення ризику вразливості, через кращу чутливість до змін у значеннях здатності виявлення.

Нечіткі значення вхідних та вихідної лінгвістичних змінних, що описують ризик невиявлення загроз та вразливості системи функціями класу Z представлені на наступних рисунках. Зокрема представлено нечіткі функцій для лінгвістичної змінної "HighRiskLevel1" для загрози “дрібний крок”, та змінна "HighRiskLevel1" для загрози “біг”. Змінна "HighVulnerability" для виведення оцінки вразливості системи класу S. Всі ці функції представлені на рис. 4 та 5.

Інтерфейс пакету Fuzzy Logic Toolbox дозволяє оцінювати вразливість для детермінованих значень імовірностей виявлення загроз що дає змогу прогнозувати вразливість системи безпеки при різних характеристиках параметрів сповіщувачів з яких вона складається.

Оцінка вразливості для вектора значень імовірностей виявлення дозволяє досліджувати нечітку систему виводу для цілого ряду різних імовірностей виявлення загроз. Зокрема, такий аналіз представлений у вигляді поверхні графа на рис. 6 для загроз “дрібний крок” та “біг”. Граф описує ризики невиявлення на j-тій зоні залежно від здібностей (імовірностей) виявлення загроз “дрібний крок” та “біг”.

Інтерфейс пакету Fuzzy Logic Toolbox дозволяє оцінювати вразливість для детермінованих значень ймовірностей виявлення загроз, що дає змогу прогнозувати вразливість системи безпеки при різних характеристиках параметрів сповіщувачів з яких вона складається.



а. **б.**

Рис. 4. Представлення нечіткої функції лінгвістичної змінної „Високий ризик першого рівня” для загрози “дрібного кроку” – (а) та “бігу” – (б)

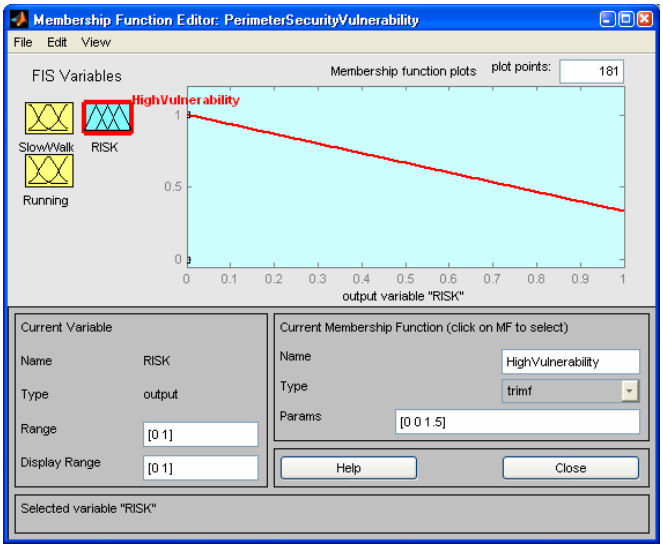


Рис. 5. Представлення нечіткої функції лінгвістичної змінної „Висока Вразливість” для вихідної оцінки вразливості системи

Оцінка вразливості для вектора значень ймовірностей виявлення дозволяє досліджувати нечітку систему виводу для цілого ряду різних ймовірностей виявлення загроз. Зокрема, такий аналіз представлений у вигляді поверхні графа на рис. 6 для загроз «дрібний крок» та «біг». Граф описує ризики не виявлення на *j*-й зоні залежно від здібностей (ймовірностей) виявлення загроз «дрібний крок» та «біг».

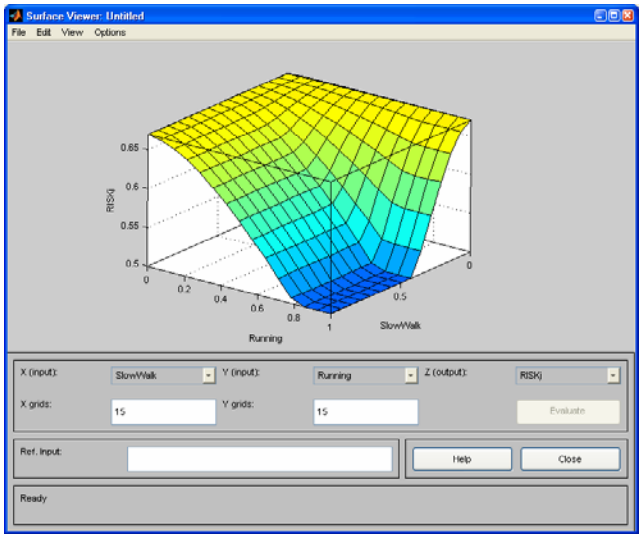


Рис. 6. Поверхня графа імовірностей виявлення

Розроблена система нечіткого виводу поряд з раніше розробленим багатокритеріальним генетичним алгоритмом [7] була використана для автоматизованого проектування системи безпеки. Як приклад, розглянуто процес проектування системи безпеки для трикутного периметру, кожна зона якого має довжину l_1=19100 м, l_2=22100 м, l_3=9000 м.

Визначено, що для охорони можуть використовуватись два альтернативних сповіщувачі: "Бар'єр-300" [13] або "SPEC-5-125" [14]. Сповіщувач "Бар'єр-300" є радіо хвилевим пристроєм із зоною виявлення 300 м., ризик $RISK_{3,1}$=0.443, ціна 811 доларів США в той час як сповіщувач "SPEC-5-125", котрий є інфрачервоним пристроєм із дальністю зони виявлення 125 м., ризик $RISK_{3,2}$=0.445, ціна 271 доларів США. Всі проходи генетичного алгоритму отримували одну і ту саму вхідну популяцію сповіщувачів. Час обчислення кожного проходу був приблизно пів хвилини. Незважаючи на те, що кожен запуск багатокритеріального генетичного алгоритму повертає популяцію Парето-оптимальних результатів, відзначимо лише один результат який має найвищу збіжність в популяції. Результати проектування системи безпеки із застосуванням цільових функцій (4) – (8) приведені в таблиці 1, де стовпці "B" і "S" відповідають за кількість сповіщувачів "Бар'єр-300" і "SPEC-5-125", які використовуються в розробленій системі безпеки.

Таблиця 1

Оцінка вразливості різних компонентів системи безпеки

	Зона 1		Зона 2		Зона 3		*VUL*	Вартість
	B	S	B	S	B	S		
VUL_1	2	148	0	177	30	0	1.33	113910
VUL_2	0	153	0	177	30	0	1.33	113641
VUL_3	17	112	7	160	0	72	4.33	112564
VUL_4	0	153	0	177	0	72	8.17	108794
VUL_5	3	146	27	112	15	36	3.89	116065

Таблиця 2 дає можливість порівняння результатів генетичного алгоритму з використанням різних нормованих функцій. Кожен рядок таблиці, позначених буквами "GA target" означає, що генетичному алгоритму був наданий відповідний VUL_n в якості цільової функції, а в колонках були використані ті ж функції в якості нормованих функцій. Аналізуючи таблицю II можна побачити результат не тільки у своїй власній нормі, а й у всіх протилежних нормах.

Таблиця 2

Оцінка вразливостей за форулами (4)- (8)

		Нормовані функції →				
		VUL_1	VUL_2	VUL_3	VUL_4	VUL_5
GA target ←	VUL_1	1.333	1.333	4.334	8.226	4.317
	VUL_2	1.334	1.333	4.334	8.169	4.334
	VUL_3	1.334	1.335	4.334	8.730	4.150
	VUL_4	1.336	1.335	4.336	8.173	4.336
	VUL_5	1.334	1.335	4.335	9.231	3.886

Можна очікувати, що мінімальний елемент в кожному стовпці має бути в діагональному положенні, тобто кожен результат має бути кращим у своїй власній нормі. Це правило порушується для VUL_4, оскільки надання генетичному алгоритму значення мети VUL_2 призводить до кращого значення 8,169 в нормі. Тому VUL_4 має погані властивості збіжності через малі зміни значення *VUL* для різних конструкцій системи.

Проект системи безпеки для VUL_4 є найдешевшим. Інші проекти дорожчі, зокрема, результат для VUL_5 є найдорожчим через використання 45-ти (3+27+15) елементів "Бар'єр-300". Він з'явився як результат вкрай високої чутливості до ризиків невиявлення в VUL_5. Проекти для VUL_1-VUL_3 дещо дешевші та кращі за інші через велику кількість надійних компонентів "Бар'єр-300". Зазначивши, що результати VUL_2 і VUL_3 мають однакові вразливості в нормах VUL_1 і VUL_3, але другий проект дешевший, можна зробити висновок, що детермінована оцінка вразливості системи безпеки VUL_3 володіє найкращими властивостями збіжності.

Висновки

Розроблено метод оцінювання вразливості системи безпеки периметру території з врахуванням неповної інформації про характеристики сповіщувачів та охоронних зон. Метод реалізовано з використанням теорії нечітких множин, дворівневої ієрархії оцінювання загроз за зонами та системи в цілому. Для отримання якісних оцінок спроможностей виявлення порушника, що використовуються при обчисленні вразливості системи, використано дані інших дослідників.

Розроблений метод використано в генетичному алгоритмі автоматизованого проектування систем безпеки. Генетичний алгоритм був оснащений різними співвідношеннями для оцінювання вразливості гетерогенних систем. Отримані результати порівняно за допомогою властивостей збіжності на множині нормованих функцій, що дозволило виробити рекомендації щодо адекватного вибору співвідношень оцінювання вразливості гетерогенних систем в конкретних умовах. Використання розроблених методів

можливе в задачах екстремальної комбінаторики для побудови найменш вразливих систем безпеки з мінімізацією коштів, затрачених на їх побудову.

Подяки

Робота виконується за підтримки Міністерства освіти і науки України та Ради з наукових і технологічних досліджень Турецької Республіки (TUBITAK) в рамках міжнародного українсько-турецького науково-технічного проекту № М/47-2008 "Розробка методів проектування та оптимізації систем виявлення порушників безпеки".

Література

1. Магауенов Р.Г. Системы охранной сигнализации: основы теории и принципы построения: Учебное пособие. 2-е изд., перераб. и. доп. – М.: Горячая линия – Телеком, 2008. – 496 с.

2. Perimeter Security Sensor Technologies Handbook / Electronic Security Systems Engineering Division, North Charleson, South Carolina, 1997. – p. 107, (URL http://www.nlectc.org/perimetr/Hb-Word.doc).

3. Ernest J. Henley, Hiromitsu Kumamoto. Reliability Engineering and Risk Assessment. – Prentice-Hall, Inc., Englewood Cliffs, 1981. – 566 p.

4. Bykovyy P., Development of the knowledge base of perimeter security systems // Proceedings of the 2nd International IEEE Conference "Intelligent Systems. – Varna (Bulgaria). – June 22 – 24, 2004. – vol. 3. – P. 54-57.

5. Turchenko I., Turchenko V., Kochan V., Bykovyy P., Sachenko A., Markowsky G., Database design for CAD system optimising distributed sensor networks for perimeter security // Proceedings of the 8th IASTED International Conference Software Engineering and Applications. – November 9-11, 2004. – MIT, Cambridge, MA (USA). – P. 59-64.

6. Bykovyy P., Kochan V., Sachenko A., Markowsky G., A CAD system that optimizes distributed sensor networks for perimeter security // Proceedings of the Second IEEE International Conference on Technologies for Homeland Security and Safety. – Istanbul (Turkey). – October 9-13, 2006. – P. 271-276.

7. Bykovyy P., Kochan V., Sachenko A., Markowsky G., Genetic algorithm implementation for perimeter security systems CAD // 4-th IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'07). – Dortmund (Germany). – 6-8 September, 2007. – P. 634-638.

8. Bykovyy P., Pigovsky Y., Kochan V., Sachenko A., Markowsky G., Aksoy S., Genetic algorithm implementation for distributed security systems optimization // IEEE International Conference on Computational Intelligence for Measurement Systems and Applications (CIMSA 2008). – Istanbul (Turkey). – 14-16 July 2008. – P. 120-124.

9. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты. – К.: ООО "ТИД "ДС", 2002. – 688 с.

10. Звежинский С. С., Иванов В. А., Рудниченко В. А. Классификации, особенности и информационно-измерительные модели средств обнаружения // "Специальная техника". – № 6. – 2007. – С. 26-33.

11. Алиев Р. А., Церковный А. Э., Мамедова Г. А. Управление производством при нечеткой исходной информации. – Москва.: Энергоатомиздат, 1991. – 240 с.

12. Rutkowska D. Neuro-Fuzzy Architectures and Hybrid Learning. – Physica-Verlag, 2002, – 308 p.

13. "Barrier-300" – характеристики сповіщувача // www.centers.ru/catalog/perimeter/russia/umirs/barier_300.htm

14. "SPEC-5" – характеристики сповіщувача //http://spec.ru/product_about.php?p_s=1&&prod=sp5

Надійшла 4.2.2010 р.

УДК 389:638.011.54

В.Т. КОНДРАТОВ

Институт кибернетики им. В.М.Глушкова НАН Украины

ОСНОВЫ (МИНИ-)ТЕОРИИ МЕТРОЛОГИЧЕСКОЙ ЭФФЕКТИВНОСТИ

В настоящей статье изложены основы мини-теории метрологической эффективности, изучающей и характеризующей качество целенаправленной метрологической деятельности человека и ее результатов на разных уровнях познания сущности свойств, процессов, объектов и систем.

In present article bases of the mini-theory of the metrological efficiency studying and characterising quality of purposeful metrological activity of the person and its results at different levels of knowledge of essence of properties, processes, objects and systems are stated.

Ключевые слова: метрологическая эффективность.

Введение

На сегодняшний день известны различные виды деятельности человека и коллективов людей: