

Висновки

У статті розроблено метод ідентифікації відблиску, який передбачає вибіркового розрахунок інтенсивності кольору в контрольних точках, а не у всіх точках полігону, що забезпечує суттєве зменшення обчислювальної складності процедури ідентифікації відблиску і, як наслідок, зафарбовування у цілому. Для запропонованого методу розроблено апроксимаційні формули, а також апаратне рішення.

Література

1. Романюк О. Н. Високопродуктивні методи та засоби зафарбовування тривимірних графічних об'єктів. Монографія. / О. Н. Романюк, А. В. Чорний. – Вінниця: УНІВЕСУМ-Вінниця, 2006. – 190 с.
2. Foley, Van Dam, Feiner, and Hughes Computer Graphics // Principles and Practice. Addison Wesley. – Ch. 16. – 1996. – pp. 800-870.
3. Farin G. Mathematical Principles for Scientific Computing and Visualization / G. Farin, D. Hansford. – Peters, Ltd. 2008. – 275 p.
4. Phong B.T. Illumination for computer generated images / B. T. Phong // Comm. of the ACM. – 18 (6). – June 1975. – P. 311–317.
5. Романюк О. Н. Адаптивний метод зафарбовування поверхонь / О. Н. Романюк, А. В. Чорний, А. В. Пугачова // Сборник научных трудов Национального горного университета. – 2004. – № 19, том 2. – С. 208–218.
6. Калютов А. В. Введение в фотореалистическую графику / А. В. Калютов. – СПб.: Политехника, 2006. – 118 с.
7. Pierre R. Realistic real-time rain rendering / R. Pierre, V. Jolivet, D. Ghazanfarpour // Computers & Graphics, august 2006, vol. 30, number 4, – P. 507–518.
8. Романюк О. Н. Аналітичні методи ідентифікації відблиску / О. Н. Романюк, М. Д. Обідник // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2010. – № 1. – С. 94-100.
9. Conte and C. de Boor. Elementary Numerical Analysis. An Algorithmic Approach. McGraw-Hill, New York, 1980. – p. 157.

Надійшла до редакції
7.11.2010 р.

УДК 004.896 322

**П.Є.БИКОВИЙ, Ю.Р.ПІГОВСЬКИЙ, А.О.САЧЕНКО,
А.Ф.КАРАЧКА, М.І.ЧИРКА, Г.В.САПОЖНИК, В.В.КОЧАН**

Тернопільський національний економічний університет

ОЦІНЮВАННЯ ІМОВІРНІСНИХ ХАРАКТЕРИСТИК СПОВІЩУВАЧІВ ТРИВОЖНОЇ СИГНАЛІЗАЦІЇ З ВРАХУВАННЯМ НЕВИЗНАЧЕНОГО ВПЛИВУ ЗАВАД

Розроблено метод оцінювання імовірностей хибної тривоги і неспрацювання сповіщувачів, що на відміну від існуючих враховує невизначеності оцінок інтенсивності завад і вразливості до них компонентів систем тривоної сигналізації шляхом використання нечітких множин та їх дефазифікації, дозволяючи зменшити кількість альтернативних варіантів структур системи тривоної сигналізації.

The method assessing probabilities of faulty alarm and intruder's indetection is developed. This method, in contrast to the existing, takes uncertainty of noise intensity and sensor vulnerability into account. It is based on fuzzy sets and their defuzzification allowing reducing number of alternative structures of an alarm system.

Ключові слова: системи тривоної сигналізації, нечіткі множини

Вступ

Система тривоної сигналізації (СТС) є розподіленою системою, що поєднує в мережу сповіщувачі з метою виявлення порушника, котрий намагається проникнути на підохоронний об'єкт. Сповіщувачі взаємодіють з приймально-контрольним приладом, який в свою чергу, обробляє сигнали від них та передає результат до засобів візуалізації і прийняття рішень. СТС периметру території відіграють роль першої основної захисної лінії, тому вони є важливим елементом різноманітних охоронних систем. Значне збільшення кількості СТС останнім часом стало можливе завдяки широкому застосуванню мікроелектроніки та обчислювальної техніки, зокрема мікроконтролерів, мережових технологій, безпроводного зв'язку, а також уніфікації інтерфейсів компонентів. Однак це привело також до появи на ринку великої кількості альтернативних компонентів СТС, які мають різну ціну та якість. В [1] описано систему оптимізації СТС, яка дозволяє формувати Парето-оптимальний набір структур СТС на базі заданого периметру території та бази даних допустимих компонентів СТС. При цьому критеріями оптимальності служать імовірність виявлення порушника, імовірність хибних тривог та затрати на придбання, встановлення та експлуатацію СТС. Однак отримані оптимальні структури базувались на значеннях імовірностей, які

враховували їх недетерміновану природу. В [2, 3] було закладено основи врахування невизначеного впливу кліматичних умов на роботу СТС. Дана стаття розвиває запропонований метод підвищення коректності виявлення оптимальних СТС за рахунок врахування умов експлуатації їх сповіщувачів.

В попередніх працях було розроблено методи оптимізації структури систем тривожної сигналізації [1] та закладено основи врахування невизначеного впливу кліматичних умов [2, 3] на її роботу.

Постановка задачі

Імовірності виявлення порушника та хибних спрацювань носять принципово недетермінований характер і, зазвичай, відомі з обмеженою точністю, оскільки виробники, якщо і надають відповідні імовірності, то не описують їх залежності від впливаючих величин. Тому врахувати їх можна тільки на базі результатів експериментальних досліджень і статистики їх експлуатації [4]. Такі результати носять в більшості не кількісний, а якісний характер, тому детермінований підхід до них принципово малопридатний. Пошук методів врахування цієї невизначеної якісної інформації є актуальною задачею.

Метод вирішення

Одним із підходів до врахування розглянутої невизначеності є методи нечіткого виводу. Врахування невизначених впливів завад та вразливості до них складових СТС ґрунтується на нечітких множинах інтенсивності завади того чи іншого виду в межах кожної ділянки периметру території. Імовірності невиявлення загроз, хибного спрацювання та безвідмовної роботи компонента j -того типу залежать від інтенсивностей електромагнітних, кліматичних та механічних завад, зокрема, описаних в [4], на i -тій ділянці та вразливості до них компонентів j -того типу. Вразливість також описується нечіткими множинами.

Згідно [4] до природно-кліматичних завад належать: сильний вітер, дощ, калюжі, сніг або туман, до механічних завад: рух малих тварин, великих тварин, птахів. Електромагнітні завади створюють розряди блискавки, повітряні та підземні високовольтні силові лінії. Проте в роботі [4] не наведено значень показників перелічених факторів, тобто відсутні об'єктивні означення фізичних величин що описують силу вітру, рівень опадів і т.п.

У випадку коли відомі лише нижні та верхні значення параметрів можна скористатися інтервальними числами [5]. Проте коли присутня незначна за об'ємом вибірка експериментальних або експертних даних, можна описати параметр одною з простих (трикутна, s-подібна, z-подібна) нечіткою функцією належності: нижня, верхня межі та найвірогідніше значення [6]. Застосування складних функцій належності необґрунтовано при малих об'ємах вибірки.

Діапазони фізичних величин, що описують інтенсивність завад, коли вони починають негативно впливати на сповіщувачі, невизначені або невідомі. Проте, за допомогою експертів можна отримати їхні оцінки у вигляді нечітких функцій і отримати наближені значення ризику невиявлення загрози як

$$\begin{aligned} r_{ij} &= r_j + \sum_{d=1}^D \text{defuz}(\tilde{E}_{id} \cap \tilde{V}_{jd}) w_d, \quad q_{ij} = q_j + \sum_{d=1}^D \text{defuz}(\tilde{E}_{id} \cap \tilde{V}'_{jd}) w'_d, \\ p_{ij} &= p_j + \sum_{d=1}^D \text{defuz}(\tilde{E}_{id} \cap \tilde{V}''_{jd}) w''_d, \end{aligned} \quad (1)$$

де r_{ij} , q_{ij} , p_{ij} – імовірності невиявлення загроз, хибного спрацювання та безвідмовної роботи, відповідно, сповіщувачем j -того типу з врахуванням впливу завад на i -тій ділянці, де його розміщено; r_j – базова оцінка імовірності невиявлення загроз сповіщувачем j -того типу при забезпеченні придатних умов експлуатації (без завад); d – індекс завади; D – загальна кількість відомих завад; $\text{defuz}(\bullet)$ – функція дефазифікації нечіткої множини, $\text{defuz}(\bullet) \in [0;1]$; $\tilde{E}_{id}$ – нечітка множина, що описує особливості периметру території, а саме інтенсивність завади d на i -тій ділянці; $\tilde{V}_{jd}$, $\tilde{V}'_{jd}$, $\tilde{V}''_{jd}$ – нечіткі множини, що описують вразливості сповіщувачів j -того типу до завади d ; $\cap$ – оператор перетину нечітких множин; w_d , w'_d , w''_d – додатки до імовірнісних характеристик компонентів при максимальному впливі загрози d , що встановлюються експертами з врахуванням умов

$$0 \leq r_j + \sum_{d=1}^D w_d \leq 1, \quad 0 \leq q_j + \sum_{d=1}^D w'_d \leq 1, \quad 0 \leq p_j + \sum_{d=1}^D w''_d \leq 1. \quad 2$$

Враховуючи відмінність імовірнісних характеристик (1)– (2) сповіщувачів j -того типу, залежно від властивостей завад на ділянці, оцінку показників імовірності хибного спрацювання СТС можна записати так:

$$\begin{cases} Q^{sys}(\vec{N}) = \frac{1}{Z} \sum_{i=1}^Z Q_i^{zone}(\vec{N}) \xrightarrow{\vec{N}} \min, \\ R^{sys}(\vec{N}) = 1 - \left(\prod_{i=1}^Z F_i^{zone}(\vec{N}) \right) + \max_{i=1, \dots, Z} R_i^{zone}(\vec{N}) \xrightarrow{\vec{N}} \min, \\ C^{sys}(\vec{N}) = \sum_{i=1}^Z C_i^{zone}(\vec{N}) \xrightarrow{\vec{N}} \min, \end{cases} \quad (3)$$

$$Q_i^{zone}(\vec{N}) = \frac{\sum_{j=1}^{n_i} N_{ij} q_{ij}}{\sum_{j=1}^{n_i} N_{ij}}, \quad R_i^{zone}(\vec{N}) = \max_{j=1, \dots, n_i} \begin{cases} r_{ij}, & \text{if } N_{ij} > 0, \\ 0, & \text{if } N_{ij} = 0, \end{cases}$$

$$F_i^{zone}(\vec{N}) = \prod_{j=1}^{n_i} (p_{ij})^{N_{ij}}, \quad C_i^{zone}(\vec{N}) = \sum_{j=1}^{n_i} c_j N_{ij}, \quad (4)$$

де $\vec{N} = (N_{1,1}, N_{1,2}, \dots, N_{Z,n})$ – наявний набір компонентів даного варіанту СТС, $C^{sys}(\vec{N})$ – ресурсоемність придбання і монтажу компонентів СТС; $R^{sys}(\vec{N})$ – ефективність СТС; $Q^{sys}(\vec{N})$ – ресурсоемність експлуатації СТС; $N_{i,j}$ – кількість компонентів j – того типу що встановлені на i – тій охоронній ділянці; n_i – кількість типів компонентів, придатних для охорони i -тої ділянки; q_{ij} , r_{ij} та p_{ij} – імовірності хибного спрацювання, невиявлення загрози та безвідмовної роботи компонента j – того типу з врахуванням завад i – тої ділянки; c_j – вартість компонента j – того типу.

Використання формул (1)– (4) дозволяє покращити СТС шляхом врахування особливостей периметру території, що описуються множинами $\tilde{E}_{id}, \tilde{V}_{jd}$, $d = \overline{1, D}$, і суттєво зменшити Парето-оптимальну множину шляхом відсіювання СТС, що через вплив завад значно збільшують частоту хибних спрацювань.

Реалізація методу

Для реалізації методу введено сімейство функцій належності, форму яких вибирають методом експертних оцінок, на основі статистичних даних і результатів відповідних досліджень. Тоді задача синтезу в нечіткій постановці записується аналогічно до детермінованої за виключенням того, що формули оцінювання імовірнісних характеристик корегуються процедурою нечіткого виводу (1)– (2). Також доцільно ввести критерій мінімізації невизначеності отриманих результатів

$$f_{uncert} = \sum_{d=1}^D w(\tilde{E}_{id} \cap \tilde{V}_{jd}) \xrightarrow{\quad} \min, \quad (5)$$

де $w(\bullet)$ – функція ширини нечіткої множини, що дорівнює різниці між крайньою правою та крайньою лівою межами перетину функцій належності.

Для розв'язання задачі (3) – (5) можна скористатися методами комбінаторної оптимізації, що були використані для задачі у детермінованій постановці [1] з врахуванням (4), (5) за допомогою розробленого ГА.

Пропонована оптимізація з врахуванням (4), (5) буде генерувати множину рівноцінних Парето-оптимальних СТС. При обчисленнях функції $defuz(\dots)$ слід застосувати одну з формул дефазифікації, що повертала б точкову оцінку інтенсивності завад по ділянці. Розглянемо альтернативні підходи для виконання дефазифікації оцінок завад: за максимумом вірогідності, за центром ваги (інша назва – метод центроїду) та за верхнім межовим значенням інтенсивності завади [7, 8]

$$defuz(\tilde{E}_{id} \cap \tilde{V}_{jd}) = \begin{cases} r \mid \max_r \mu(r), & C = 1, \\ \frac{\int_{-\infty}^{\infty} r \mu(r) dr}{\int_{-\infty}^{\infty} \mu(r) dr}, & C = 2, \\ \max r, & C = 3, \end{cases} \quad (6)$$

де r – точкове значення оцінок ризику умов по ділянці, $\mu(r)$ – функція належності його нечіткої оцінки, при $C = 1$ – найвірогідніша оцінка, при $C = 2$ – оцінка за центром ваги, при $C = 3$ – оцінка за верхнім межовим значенням.

Нечітку множину інтенсивності завад на периметрі території доцільно описати функціями

належності трапецевидного класу [9] $\mu(x,a,b,c,d)$, де a,b – параметри S-сегменту, b,c – параметри інтервал-сегменту, c,d – параметри Z-сегменту. Форма функції визначає вірогідність даного значення інтенсивності завади. Точки цієї функції отримують з бази метеорологічних спостережень, їх можуть додатково уточнити експерти.

Через обмеженість експериментальних даних про вразливість сповіщувачів до кожного виду завад доцільно обрати функцію належності класу S для опису нечіткої множини вірогідності впливу заданої інтенсивності завад на сповіщувач. У цих функціях слід встановити нижню та верхню межу мінімальних і максимальних інтенсивностей завад, які впливають на роботу сповіщувача $\mu(x,a,b)$, де a,b – нижня та верхня межі функції належності, x – значення аргументу функції ($a \leq x \leq b$).

Приклад оптимізації СТС

Розглянемо приклад оптимізації СТС із нечітким виводом. Завадою виступатиме швидкість вітру. Параметри нечітких множин, що описують вірогідність швидкості вітру на периметрі підхоронного об'єкту та вразливості до нього мікрохвильових сповіщувачів визначені за даними [4]. Ілюстрації цих нечітких множин наведені на рис. 1, де множина вірогідностей швидкості вітру на ділянці $\tilde{E}_{id}$ описана трапецевидною функцією, а множина вірогідності впливу завади на роботу сповіщувача $\tilde{V}_{jd}$ позначена функцією класу S . Перетин множин $\tilde{E}_{id} \cap \tilde{V}_{jd}$ виділено заштрихованою областю – він дозволяє на основі (6) обчислити найвірогідніше значення швидкості вітру, що може негативно вплинути на функціонування сповіщувача.

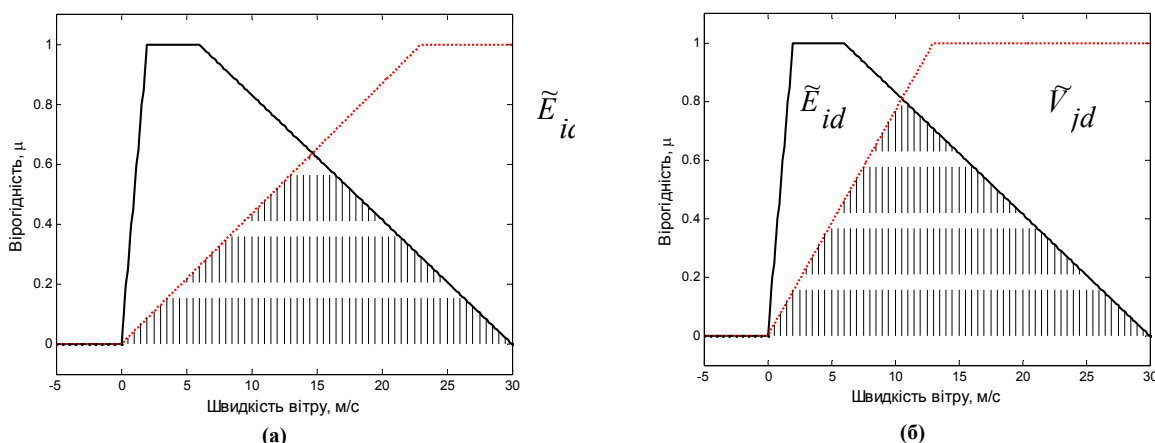


Рис. 1. Ілюстрація нечітких функцій швидкості вітру та вразливості до нього сповіщувачів двох типів: (а) та (б)

Врахування невизначеності оцінок інтенсивностей завад і вразливості до них компонентів СТС, дає змогу виявити напрямки покращення СТС за рахунок врахування особливостей периметру території.

Розглянемо вплив завад нечітко визначеного типу та інтенсивності на результати оптимізації СТС охорони периметру острова Ayers [10]. Врахування їх впливу здійснимо за допомогою розробленого методу нечіткого виводу. Імовірнісні характеристики сповіщувачів, що використовуються під час розробки СТС, параметри сповіщувачів та нечіткі функції вразливості наведені в таблиці 1.

Таблиця 1

Характеристики сповіщувачів

Тип спові- щува-ча, j	Область дії, м	Ймовірність функціону- вання p_j	Ймовірність хибної тривоги q_j	Ймовірність невиявлення r_j	Параметри вразливості, м/с, $\mu(x,a,b)$	Варті- сть, дол. США
1	200	0.999	0.25	0.02	[0 23.0]	450
2	100	0.999	0.25	0.11	[0 23.0]	300
3	75	0.999	0.03	0.14	[0 21.5]	250
4	75	0.999	0.25	0.15	[0 23.0]	186
5	50	0.999	0.25	0.15	[0 25.0]	200
6	50	0.999	0.25	0.20	[0 13.0]	150

Характеристики інтенсивності впливу завади “сильний вітер” описуються трапецевидною нечіткою функцією $\mu(x,a,b,c,d)$ із параметрами $a=0$ $b=2$ $c=6$ $d=30$. Зображення нечітких множин, що

характеризують перший та шостий сповіщувачі з таблиці 1 та їх перетин з нечіткою множиною “сильний вітер” наведено на рис. 1. Згідно (1)- (2), скореговані значення імовірностей хибного спрацювання з врахуванням впливів завад складають: $q_1 = 0.7357$, $q_2 = 0.7357$, $q_3 = 0.7800$, $q_4 = 0.7357$, $q_5 = 0.7955$, $q_6 = 1.0000$. Їх отримано шляхом дефазифікації перетинів нечітких множин вразливості кожного сповіщувача з множиною “сильний вітер” методом центроїда ($C=2$), див (6), і встановленням значення $w_d = 1 - \max_j q_j = 0.75$. Значення $q_6 = 1.0000$ свідчить про те, що компонент 6-того типу в умовах даного

впливу завад не придатний для використання. Це є результатом корегування оптимальних СТС, тобто СТС, що містять в своєму складі даний компонент в будь-якій кількості є не оптимальні.

Оптимізація з нечітким виводом, що враховує вплив “сильного вітру” на сповіщувачі, скорочує обсяг Парето-оптимальних структур до 8 варіантів СТС, що складає приблизно 5 % від початкової множини 178 варіантів (див. табл. 2).

В даній таблиці наведено характеристики СТС без врахування невизначеного впливу завади “сильний вітер”. В таблиці 3 наведено результуючу Парето-множину СТС, де враховано вплив завади та вразливостей до неї сповіщувачів. Порівнюючи таблиці 2 і 3 можна побачити, що СТС з однаковим складом сповіщувачів залежно від врахування завад мають різний показник імовірності хибного спрацювання, наприклад у стрічках 1 і 2 таблиць 2 і 3.

Таблиця 2

Опис множини Парето-оптимальних СТС без врахування впливу завад

№	К-сть сповіщувачів відповідного типу						Q^{sys}	R^{sys}	C^{sys}
	Тип 1	Тип 2	Тип 3	Тип 4	Тип 5	Тип 6			
1	10	5	0	0	0	0	0.250	0.125	6000.000
2	10	1	0	4	0	0	0.250	0.165	5544.000
3	9	1	2	4	0	0	0.209	0.166	5594.000
...									
176	7	1	11	0	0	0	0.126	0.159	6200.000
177	9	0	8	0	0	0	0.140	0.157	6050.000
178	6	2	12	0	0	0	0.113	0.160	6300.000

Таблиця 3

Опис множини Парето-оптимальних СТС з врахуванням завади “сильний вітер”

№	К-сть сповіщувачів відповідного типу						Q^{sys}	R^{sys}	C^{sys}
	Тип 1	Тип 2	Тип 3	Тип 4	Тип 5	Тип 6			
1	10	5	0	0	0	0	0.736	0.125	6000.000
2	10	1	0	4	0	0	0.736	0.165	5544.000
3	9	1	0	6	0	0	0.736	0.166	5466.000
4	9	1	0	4	0	2	0.763	0.216	5394.000
5	8	0	0	10	0	0	0.736	0.168	5460.000
6	8	0	0	8	0	2	0.763	0.218	5388.000
7	15	0	0	0	0	0	0.736	0.035	6750.000
8	10	1	4	0	0	0	0.749	0.155	5800.000

Висновок

Розроблено метод оцінювання функціональних характеристик СТС, що враховує невизначеності оцінок інтенсивності завад і вразливості до них компонентів СТС. Це дало змогу скоротити обсяг Парето-оптимальних структур до 8 варіантів СТС, що складає приблизно 5 % від початкової множини 178 варіантів.

Література

1. Bykovyy P. Genetic Algorithm Implementation for Perimeter Security Systems CAD / P.Bykovyy, V.Kochan, A.Sachenko, G.Markowsky // 4-th IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'07). – Dortmund, 2007. – P. 634-638.
2. Биковий П.Є. Багатокритеріальний синтез систем безпеки периметру території в умовах невизначеного впливу завад / П.Є. Биковий, Ю.Р. Піговський // Труды XI міжнародної науково-практичної конференції «Сучасні інформаційні та електронні технології». – Одеса, 2010. – Т.1. – С. 88.
3. Биковий П.Є. Система нечіткого виводу для оцінки ризиків вразливості систем безпеки периметру території / П.Є. Биковий // Вісник Хмельницького національного університету. Технічні науки. 2010. – № 2 (146). – С. 174-180.
4. Звездинский С.С. Классификации, особенности и информационно-измерительные модели средств обнаружения / С.С. Звездинский, В.А. Иванов, В.А. Рудниченко // Специальная техника. – 2007, – № 6. – С. 26-33.
5. Алефельд Г. Введение в интервальные вычисления / Г. Алефельд, Ю. Херцбергер. – М.: Мир,

1987. – 356 с.

6. Рутковская Д., Пилинский М., Рутковский Л. Нейронные сети, генетические алгоритмы и нечеткие системы / Рутковская Д., Пилинский М., Рутковский Л.; Пер. с польск. И.Д. Рудинского. – М.: Горячая линия – Телеком, 2006. – 452 с.

7. Ротштейн А. П. Нечеткий многокритериальный анализ вариантов с применением парных сравнений / А. П. Ротштейн, С. Д. Штовба // Известия РАН. Теория и системы управления. – 2001. – № 3. – С.150–154.

8. Runkler T. A. Extended defuzzification methods and their properties / T. A. Runkler // IEEE Transactions. – 1996. – P. 694–700.

9. Алиев Р. А. Управление производством при нечеткой исходной информации / Алиев Р.А., Церковский А.Э., Мамедова Г.А. – М.: Энергоатомиздат, 1991. – 240 с.

10. U.S. Civilian Research and Development Foundation grant CRDF FSTM UM2-5012-TE-03 "Design of Distributed Sensor Network for Ayers Island Security Using Value Analysis Technology", 2003-2005.

Надійшла до редакції
3.10.2010 р.

УДК 004.89

М.П. КОМАР, Д.І. БОДНАР, А.О. САЧЕНКО

Тернопільський національний економічний університет

ІНТЕЛЕКТУАЛІЗОВАНА ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ВІЯВЛЕННЯ КОМП'ЮТЕРНИХ АТАК

Розроблено інтелектуалізовану інформаційну технологію як сукупність нейромережових методів, алгоритмів та програмних засобів для виявлення комп'ютерних хакерських атак, основним елементом якої є нейромережовий детектор. Наведено архітектуру та алгоритми навчання і функціонування нейромережових детекторів. Представлені результати експериментальних досліджень.

Intelligent information technology as a complex of neuronetwork methods and algorithms and software are proposed to detect network hacker attacks on computer systems. A key component of such system is a neuronetwork detector, and its architecture, training and functioning algorithms are developed there. The experimental results are presented as well.

Ключові слова: нейромережовий метод, інтелектуалізована інформаційна технологія, комп'ютерні атаки, нейромережовий детектор, алгоритми навчання і функціонування, виявлення вторгнень.

Вступ

На сьогоднішній день склалася ситуація, коли найбільш поширені методи сигнатурного аналізу для виявлення вторгнень [1-3], або методи статистичного аналізу для виявлення аномалій [1-3] не здатні на належному рівні забезпечити інформаційну безпеку. Комп'ютерні системи безперервно піддаються різного роду загрозам, наприклад у вигляді вторгнень (атак) і користувач не може бути впевнений у захищеності важливої інформації, оскільки кіберзлочинці продовжують удосконалювати і розвивати методи і засоби організації комп'ютерних атак.

Основним недоліком існуючих систем захисту від мережових атак, заснованих на традиційних методах, є їх нездатність виявляти нові або невідомі атаки, які характеризуються відсутністю записів у системі про них [4,5]. Відомі системи виявлення вторгнень також погано пристосовані до роботи в реальному режимі часу, що знижує їх ефективність використання в системах захисту. Ситуація, що склалася стимулює пошук і розробку нових підходів, спрямованих на підвищення рівня захищеності комп'ютерних систем від шкідливих впливів.

Одним із перспективних напрямів є застосування штучних нейронних мереж (ШНМ), які мають на меті моделювання біологічної нейронної мережі для досягнення таких властивостей систем як здатність до навчання, самоорганізації та адаптації [9,10]. Ідея застосування ШНМ для виявлення вторгнень на комп'ютерні системи в стислій формі описана в [6,11]. Нижче наведені результати подальших досліджень в цьому напрямку.

Архітектура та алгоритм навчання нейромережового детектора для виявлення мережових атак

Нейромережовий детектор на основі багатошарової нейронної мережі з одним прихованим шаром нейронів Кохонена [7] містить перший шар нейронних елементів, призначений для розподілу вхідних сигналів на нейрони шару Кохонена. Вхідними сигналами є параметри мережного з'єднання. Виділяють 41 параметр (атрибут) мережного з'єднання, які характеризують мережовий трафік і містять інформацію про час з'єднання, тип протоколу, кількість переданих байт, кількість виникнення помилок під час з'єднання і т.д [8]. Кількість нейронних елементів розподільного шару дорівнює кількості атрибутів мережного трафіку $n = 41$.

Другий шар ШНМ складається з нейронів Кохонена. Шар Кохонена відіграє ключову роль в класифікації даних і здійснює кластеризацію вхідного простору образів, в результаті чого утворюються