© Khlaponin Yu., Kozlovskiy V., Mishchenko A. Fuzzy neural production network model for information security systems // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 3, p. 231-235.

ЗАХИСТ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ОБЛАДНАННЯ / SOFTWARE & HARDWARE ARCHITECTURE SECURITY

МОДЕЛЬ НЕЧІТКОЇ НЕЙРОННОЇ ПРОДУКЦІЙНОЇ МЕРЕЖІ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

Юрій Хлапонін, Валерій Козловський, Андрій Міщенко

Національний авіаційний університет, Україна

ХЛАПОНІН Юрій Іванович, к.т.н.

Рік та місце народження: 1963 рік, Луганська обл., Україна
Освіта: Київське вище інженерне радіотехнічне училище ППО, 1985 рік.
Посада: доцент кафедри засобів захисту інформації НАУ з 2011 року.
Наукові інтереси: інформаційна безпека, захист інформації.
Публікації: більше 50 наукових публікацій, серед яких наукові статті, авторські свідоцтва та патенти на винаходи, тези доповідей.
E-mail: yfcnz0408@ukr.net

КОЗЛОВСЬКИЙ Валерій Валерійович, д.т.н.

Рік та місце народження: 1971 рік, м. Київ, Україна.
Освіта: Київське вище військове авіаційне інженерне училище, 1992 рік,
Посада: завідувач кафедри засобів захисту інформації НАУ з 2014 року.
Наукові інтереси: селекція сигналів в умовах завад.
Публікації: більше 80 наукових публікацій, серед яких підручники, навчальні посібники, наукові статті, тези доповідей.
E-mail: vvk@zeos.net

МІЩЕНКО Андрій Віталійович, к.т.н.

Рік та місце народження: 1967 рік, м. Мінськ, Білорусь.
Освіта: Київське вище військове авіаційне інженерне училище, 1989 рік,
Національна академія оборони України, 2004 рік.
Посада: заступник генерального директора Аеропорту «Київ» з 2010 року.
Наукові інтереси: методи та засоби обробки інформації в комп'ютерних системах.
Публікації: більше 100 наукових публікацій, серед яких підручники, навчальні посібники, наукові статті, тези доповідей.
E-mail: partpravo@i.ua

Анотація. *У даній статті запропоновано модель оцінки рівня захищеності інформації на основі нечіткої нейронної продукційної мережі. Методологія якісного оцінювання рівня захищеності інформації в системі ґрунтується на результатах вимірювань та експертних оцінках, які можуть бути нечіткими і недостатньо вираженими для того, щоб бути описаними математичними залежностями. Функціонування таких систем можливо описати, використовуючи конструкції у формі нечітких правил. Нечіткі продукційні мережі за своєю структурою ідентичні багатошаровим нейронних мереж і ця властивість було застосовано авторами для побудови моделі нейромережевої системи оцінки рівня захищеності інформації. Введено поняття технологічних портретів захищеності як сукупності станів захищеності, які відповідають виявленим технічним каналам витоку інформації в певний момент часу. Запропоновано проводити ранжування технічних каналів за важливістю перед обробкою в нейромережній системі.*

Отримані результати дозволяють формалізувати напрямки подальших досліджень щодо розробки нових ефективних систем захисту інформації з використанням інтелектуальних технологій.

Ключові слова: *захист інформації, нечіткі продукційні моделі, нейрон, нейрона мережа, технологічний портрет захищеності, технічний канал витоку інформації.*

Постановка проблеми та її зв'язок з важливими науковими завданнями

На сьогоднішній день оцінювання рівня захищеності інформації визначається системою кількісних та якісних показників, які забезпечують розв'язання задачі захисту інформації на основі існуючих в державі норм та вимог [1-3].

За умови стрімких темпів розвитку інформаційних технологій, збільшення кількості загроз інформації, ступеня невизначеності їх виникнення і реалізації, а також складності систем захисту інформації та їх спеціалізованої спрямованості, набуває актуальності завдання отримання узагальненої оцінки рівня захищеності інформації на основі методології, що враховує як кількісні, так і якісні показники оцінки.

Методологія якісного оцінювання рівня захищеності інформації в системі ґрунтується на результатах вимірювань та експертних оцінках, якість яких визначається кваліфікацією та підготовкою експертів, що призводять до низького рівня захищеності інформації. Експертні дані можуть бути нечіткими і недостатньо вираженими для того, щоб бути описаними математичними залежностями. Крім того, така інформація може бути різноякісною, а оцінка значень параметрів проводиться за рахунок різних шкал. Але часто функціонування таких систем можливо описати в вигляді евристичних уподобань, використовуючи конструкції в формі нечітких правил або відношень різного типу.

Формулювання цілей статті

Авторами поставлена ціль статті - запропонувати модель нейромережної системи оцінки рівня захищеності інформації, застосовуючи теорію нечітких продукційних моделей (мереж).

Результат дослідження

Інформація про систему, її параметри, входи, виходи та стан системи може бути не надійною, не чітко визначеною та слабоформалізованою.

Нечіткі продукційні моделі (Rule-Based Fuzzy Models/Systems) є найбільш загальним видом нечітких моделей, які використовуються для опису, аналізу та моделювання складних, слабо-формалізованих систем та процесів.

Найбільшого розповсюдження на теперішній час набули алгоритми нечіткої логіки Мамдані (Mamdani), Ларсена (Larsen), Цукамото (Tsukamoto), Такагі-Сугено (Takagi-Sugeno) [4].

Під нечіткою продукційною моделлю будемо розуміти узгоджену множину окремих нечітких продукційних правил виду **"ЯКЩО А, ТО В"** (де А та В – передумова (антецедент) і висновок (консеквент) даного правила в вигляді нечітких висловлювань), призначену для визначення ступеню істинності висновків нечітких продукційних правил , на основі передумов з відомим ступенем істинності відповідних правил.

Для формування простих нечітких висловлювань в передумовах і висновках нечітких продукційних правил (наприклад, **"а є А", "в є В"** в правилах виду **"ЯКЩО а є А, ТО в є В"**) необхідно задати функції приналежності відповідних нечітких множин.

Для оцінки рівня захищеності інформації можуть бути застосовані нечіткі продукційні моделі та алгоритми нечіткого висновку на їх основі.

Експерту з питань захисту інформації може бути заздалегідь заданий набір готових функцій приналежності, які покривають базову множину простору вхідних та вихідних змінних, або йому потрібно буде побудувати такі функцій приналежності. Інформація за формою представлення може озвучуватися (мовна інформація), оброблятися (інформація, що циркулює в ІТС) та зберігатися на носіях інформації (папір, магнітні та інші матеріальні носії).

Для оцінки захищеності інформації експерту необхідно враховувати всі можливі технічні канали витоку інформації, стан відповідного каналу буде відповідати стану захищеності інформації від певного виду загроз.

Незважаючи на безсумнівні переваги нечітких продукційних моделей їм притаманні і деякі недоліки:

- вхідний набір нечітких правил формулюється експертом і може виявитися неповним або таким, що має протиріччя;
- суб'єктивність в виборі виду та параметрів функцій приналежності в нечітких висловлюваннях правил;
- відсутність можливості автоматичного набуття знань.

Формально нечіткі продукційні моделі можуть бути представлені у вигляді нечітких продукційних мереж, які по своїй структурі ідентичні багатошаровим нейронним мережам, елементи кожного шару яких реалізують окремий етап нечіткого висновку в нечіткій продукційній моделі.

Для усунення вказаних вище недоліків в ряді робіт запропоновано створювати нечіткі продукційні моделі адаптивними (з корекцією в процесі та за результатами їх функціонування), а також реалізовувати різні компоненти цих моделей на основі нейромережевої технології.

Структура нейромережевої системи (НМС) оцінки рівня захищеності інформації, яка представлена на рис. 1 включає *m*-нейронних ансамблів (шарів), які визначаються кількістю станів захищеності інформації відповідно до певного виду

загроз. Стан захищеності відповідає нейронному шару, а число класів визначається параметрами, які визначаються (вимірюються) та порівнюються з нормами з метою визначення стану захищеності інформації для кожного з визначених технічних каналів витоку згідно відпрацьованої моделі загроз для інформації.

За результатом проведення обстеження та первинної інструментальної (розрахункової) оцінки захищеності для кожного можливого технічного каналу маємо бінарні матриці розміром $n \times M_l$, де M_l – загальна кількість загроз, що характеризують l-й технічний канал.

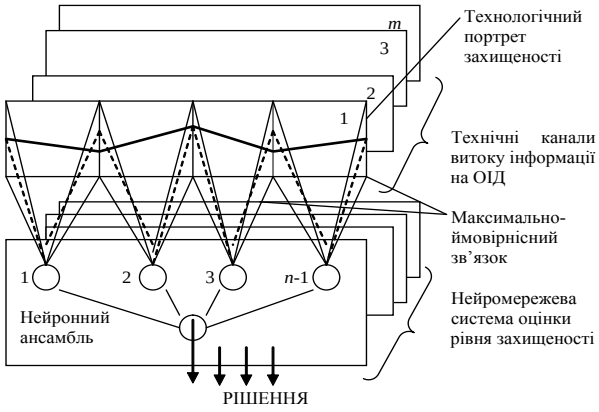

Рис. 1. Структура нейромережевої системи

У результаті маємо сукупність матриць $ТК^*_{РК}$; $ТК^*_{АЕК}$; $ТК^*_{АК}$; $ТК^*_{ВАК}$; $ТК^*_{ПЕМВН}$; $ТК^*_{ПК}$; $ТК^*_{ОК}$, які фактично визначають формальний опис ОІД.

Необхідно провести інструментальний контроль та визначити остаточний список можливих технічних каналів витоку інформації на об'єкті.

За результатами цього маємо множину $\{m_l\}_{TKBI}$, $l = \overline{1,L}$, де $L \le 7$.

Сукупність станів захищеності, які відповідають виявленим на ОІД технічним каналам витоку інформації в певний момент часу, може бути представлена у виді динамічних систем. Ці стани називаються подіями та представляються у виді технологічних портретів захищеності. Під цим терміном, що охоплює відповідні поняття фізичного, інформаційного та безпекового характеру, розуміється заняття динамічною розподіленою мережею визначеного технологічного стану чи конфігурації станів. Еволюційні зміни, що проходять між подіями, не приймаються до уваги і вважається, що динаміка системи розвивається дискретно від події до події. Така система є дискретно-подійною [5].

Середовище для нейромережевої системи (НМС) оцінки рівня захищеності інформації може бути представлено у виді сукупності дискретно-подійних систем із зв'язаними дискретними технологічними станами захищеності.

Отримуючи необхідну чисельність інструментальних вимірювань та спеціальних досліджень по кожному з технічних каналів витоку інформації, отриманих на ОІД, необхідно розробити таку процедуру обробки вимірювань, що дозволяє автоматично одержувати інформацію про технологічний стан захищеності кожного з каналів відповідно до затвердженої моделі загроз.

Результати інструментальних вимірювань та спеціальних досліджень по кожному з технічних каналів витоку інформації сприймаються сенсорною матрицею у вигляді сукупності спостережень: $X = (X_1, X_2, ..., X_i, ..., X_m)$, $i = 1,2,...,n$.

В окремому сенсорному каналі відбувається редукція вибіркового простору X, у результаті якої маємо послідовність дискретних змінних U_k, $k = 0,1,...,n\text{-}1$, які приймають значення $Z_1, Z_2,...,Z_r$.

Необхідно синтезувати структуру нейроподібного класифікатора, що реалізує вирішальну функцію $\gamma(U)$ на скороченому вибірковому просторі U [6].

Послідовність дискретних змінних U_r, $k = 0,1,...,n\text{-}1$, які приймають значення z_a, $a = 1,2,...,r$, можна апроксимувати векторами Ξ, $\Phi(0)_\mu$ та Ξ, $\Phi(k)_\mu$.

Структура найпростішої нейроподібної системи оцінки рівня захищеності - це набір M+1 ансамблів нейронних мереж першого шару. Ансамбль складається з n-нейронів, рівень збудження яких визначається як

$$Y_\mu(k) = \sum_{a=1}^{n} \Xi a(k) \Phi_a(k)_\mu,$$

де Ξ, $\Phi(0)_\mu$ та Ξ, $\Phi(k)_\mu$. – вектори, якими можна апроксимувати послідовність дискретних змінних U_r, $k = 0,1,...,n\text{-}1$, що приймають значення z_a, $a = 1,2,...,r$ [5].

Кожен нейрон здійснює кодування процесу, що визначається за, так званим, методом мічених ліній, при якому певним значенням процесу надаються у відповідність визначені (мічені) лінії $Z_1, Z_2,...,Z_a,...,Z_k$ і отже, певному значенню параметра процесу відповідає один максимально збуджений синаптичний зв'язок $\Xi_a(k) = 1$.

На відміну від типового нейрона, синаптичні зв'язки якого рівнозначні, у нейрона, що здійснює кодування методом мічених ліній, синаптичні зв'язки мають пріоритет. Синаптичному входу з великим номером відповідає більше значення параметра процесу. Ще одна відмінність полягає у тому, що у k-й момент часу збуджується тільки один синаптичний зв'язок і, тим самим, значно спрощується задача введення й управління порогом Θ, за допомогою вагової функції w. Дійсно

$$Y_\mu(k) = \sum_{a=1}^{r} \Xi a(k) \Phi_a(k)_\mu - \Theta_a(k)_\mu.$$

Для кожного технічного каналу із множини $\{m_l\}_{TKBI}$ визначити треба його важливість [8].

Незважаючи на різницю у кількості загроз згідно з [5], які визначають кожен можливий технічний канал, ця кількість не визначає ступінь небезпеки самого технічного каналу. Тому для визначення коефіцієнтів важливості раціонально використати співвідношення між загальною кількістю загроз конкретного каналу та кількістю загроз, які прийняли значення "1" за результатами експертного опитування.

Тоді формула для визначення коефіцієнтів важливості кожного технічного каналу у списку має такий вид:

$$л_l = \frac{M_l^1}{M_l}, \quad l = \overline{1, L},$$

де M_l^1 - кількість загроз l-го технічного каналу, які прийняли значення "1" за результатами експертного опитування; M_l – загальна кількість загроз, що характеризують l-й технічний канал.

Таким чином, формується множина значень важливості кожного можливого технічного каналу витоку інформації - $\{\lambda_l\}_{\text{ТКВІ}}$, $l = \overline{1, L}$. Синаптичному входу з більшим номером відповідає значення параметра технічного каналу з більшим рейтингом.

Необхідно провести ранжування технічних каналів за важливістю та сформувати остаточний перелік можливих технічних каналів витоку інформації на ОІД:

$$\{\text{m}_l\}^*_{\text{ТКВІ}}, \; l = \overline{1, L}, \text{ де } L \le 8.$$

Висновки

При рішенні задач, пов'язаних із оцінкою рівня захищеності інформації, необхідно попередньо оцінити ступінь відповідності прийнятих сигналів (технологічних портретів захищеності – результатів інструментальних вимірювань та спеціальних досліджень по кожному з технічних каналів витоку інформації) еталонним, тобто, визначити критерій ухвалення рішення. Кількісну міру відповідності доводиться вибирати по-різному, у відповідності від характеру проведених досліджень. Так, прийняття рішення щодо захищеності від витоку інформації, наприклад, акустичним, віброакустичним, акустоелектричним каналами приймається після порівняння на відповідність нормам, які викладені нормативних документах системи технічного захисту в Україні. Розроблено таку процедуру обробки вимірювань, що дозволяє автоматично одержувати інформацію про стан захищеності кожного з каналів відповідно до затвердженої моделі загроз.

Практичне значення отриманих результатів дослідження

Запропоновані підходи дозволяють формалізувати напрямки подальших досліджень щодо розробки нових ефективних систем захисту інформації з використанням інтелектуальних технологій.

Відмінність її від існуючих систем оцінки рівня захищеності полягає у тому, що нейромережева структура орієнтована на рішення конкретної задачі – створення та проведення атестації об'єкта інформаційної діяльності або створення комплексної системи захисту інформації в ІТС. Вимога проблемної орієнтації нейромережі (НМ) призводить до реалізації принципу адекватності її структури та зовнішнього середовища, тобто можливості гнучкої структурної і функціональної перебудови. Цим обумовлюється найважливіша властивість НМ – адаптивність до змін середовища функціонування ІТС, що досить актуально при складності структури сучасних ІТС. Початкова структуризація нейромережі повинна проводитися методами формального синтезу, за допомогою яких визначається оптимальна структура, що включає кількість нейронних шарів і нейронних ансамблів, кількість нейроподібних елементів в кожному шарі, наявність детермінованих зв'язків між ними і початкові вагові коефіцієнти.

Новизна отриманих результатів

Науковою новизною результатів цього дослідження є:

– запропоновано моделювання системи оцінки рівня захищеності інформації на основі нечіткої нейронної продукційної мережі.

– введено поняття технологічних портретів захищеності як сукупності станів захищеності, які відповідають виявленим на ОІД технічним каналам витоку інформації в певний момент часу.

– запропоновано проводити ранжування технічних каналів за важливістю перед обробкою в нейромережній системі.

Література

[1] Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».

[2] НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

[3] НД ТЗІ 2.7-009-09. Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.

[4] Борисов В.В., Круглов В.В., Федулов А.С. Нечеткие модели и сети мережі. — 2 изд. / М. : Горячая линия-Телеком, 2012. — 284 с.

[5] Кривуца В.Г., Беркман Л.Н., Толюпа С.В. Інфокомунікаційні мережі нового покоління / За ред. В.Г. Кривуци. — К. : ДУІКТ, 2012. — 288 с.

[6] Корольов А.П., Толюпа С.В., Тхоржевський І.В. Необхідність побудови нейромережевих систем технічного діагностування радіоелектронної техніки // Зб. наук. праць КВІУЗ. — К. : 2001. — № 3. — С. 51-60.

[7] Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации / Под ред. В.А. Хорошко. — К.: Арий, 2010. — Т. 1. Несанкционированное получение информации. — 464 с.

[8] Хлапонін Ю.І. Модель системи оцінки рівня захищеності інформації на основі нейромережі // Сучасні інформаційні технології в сфері безпеки та оборони. — 2014. — № 1. — С. 96-100.

УДК 004.056.55 (045)

© Khlaponin Yu., Kozlovskiy V., Mishchenko A. Fuzzy neural production network model for information security systems // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 3, p. 231-235.

Хлапонин Ю.И., Козловский В.В., Мищенко А.В. Модель нечеткой нейронной продукционной сети в системах защиты информации

Аннотация. *В данной статье предложена модель оценки уровня защищенности информации на основе нечеткой нейронной продукционной сети. Методология качественного оценивания уровня защищенности информации в системе основывается на результатах измерений и экспертных оценках, которые могут быть нечеткими и недостаточно выраженными для того, чтобы быть описанными математическими зависимостями. Функционирование таких систем возможно описать, используя конструкции в форме нечетких правил. Нечеткие продукционные сети по своей структуре идентичны многослойным нейронным сетям и это свойство было применено авторами для построения модели нейросетевой системы оценки уровня защищенности информации. Введено понятие технологических портретов защищенности как совокупности состояний защищенности. Предложено проводить ранжирование технических каналов по важности перед обработкой в нейросетевой системе. Полученные результаты позволяют формализовать направления дальнейших исследований по разработке новых эффективных систем защиты информации с использованием интеллектуальных технологий.*

Ключевые слова: *защита информации, нечеткие продукционные модели, нейрон, нейронная сеть, технологический портрет защищенности, технический канал утечки информации.*

Khlaponin Yu., Kozlovskiy V., Mishchenko A. Fuzzy neural production network model for information security systems

Abstract. *In this paper authors propose a model assessing the level of data protection based on fuzzy neural network of production. Methodology of qualitative evaluation of the level of data protection in the system based on the results of measurements and expert assessments that can be vague and insufficiently severe to be described mathematically dependencies. Such systems may be described using the structure in the form of fuzzy rules. Fuzzy production network structure identical multilayer neural networks, and this property was used by the authors to construct a model of neural network system of assessing the level of data protection. The concept of technology as a set of portraits of security protection states is introduced. It is proposed to conduct technical channels ranking in importance before processing in neural network system. The obtained results allow to formalize the directions for further research to develop new and effective information security systems with intelligent technologies.*

Key words: *information security, fuzzy production models, neuron, neural network, technology portrait of security, technical channel of information leakage.*

Отримано *16 вересня 2014 року*, затверджено редколегією *2 жовтня 2014 року*