УДК 004.056,5.621.396

Юрій Іванович Хлапонін *(канд. техн. наук, с.н.с., доцент кафедри)*

Національний авіаційний університет, Київ

МОДЕЛЬ СИСТЕМИ ОЦІНКИ РІВНЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ НА ОСНОВІ НЕЙРОМЕРЕЖІ

В статті розглядається модель системи оцінки рівня захищеності інформації з застосуванням нейромережі. Сукупність станів захищеності, які відповідають виявленим на об'єкті інформаційної діяльності технічним каналам витоку інформації в певний момент часу, може бути представлена у вигляді динамічних систем. Середовище для нейромережевої системи (НМС) оцінки рівня захищеності інформації представлено у вигляді сукупності дискретно-подійних систем із зв'язаними дискретними технологічними станами захищеності. Запропоновано структуру нейроподібного класифікатора, що реалізує вирішальну функцію оцінки захищеності інформації.

Ключові слова: *захист інформації, нейрон, нейромережа, технологічний портрет захищеності*.

Постановка проблеми та її звязок 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 [1,2,3].

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.

Аналіз останніх досліджень та публікацій

Проблемам дослідження захищеності інформації приділяється увага в публікаціях вітчизняних та закордонних вчених. Значний вклад в рішення подібних задач внесли В.А. Хорошко, С.В. Толюпа, В.В., Домарєв [4,5,6].

Методологія якісного оцінювання рівня захищеності інформації ґрунтується на результатах вимірювань та експертних оцінках, яким притаманні принципові недоліки, що призводять до низького рівня захищеності інформації. Суть недоліків полягає у невизначеності постановки завдання і, відповідно, у складності отримуваних рішень, якість яких визначається кваліфікацією та підготовкою експертів. Інший підхід до оцінювання – кількісний, якому на сьогодні приділяється значна увага фахівців.

Формулювання цілей статті

Автором поставлена в статті ціль – запропонувати модель проблемно-орієнтованої нейромережної системи оцінки рівня захищеності інформації.

Результат дослідження

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). В залежності від форми представлення формуються технічні канали витоку інформації [4]:

радіоканали (електромагнітні випромінювання радіодіапазону);

акустичні канали (розповсюдження звукових коливань в будь-якому звукопровідному матеріалі);

електричні канали (небезпечні напруги і струми в різних струмопровідних комунікаціях);

оптичні канали (електромагнітні випромінювання в інфрачервоній, видимій і ультрафіолетовій частині спектра);

матеріально-речові канали (папір, фото, магнітні носії, відходи і т.д.).

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

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.

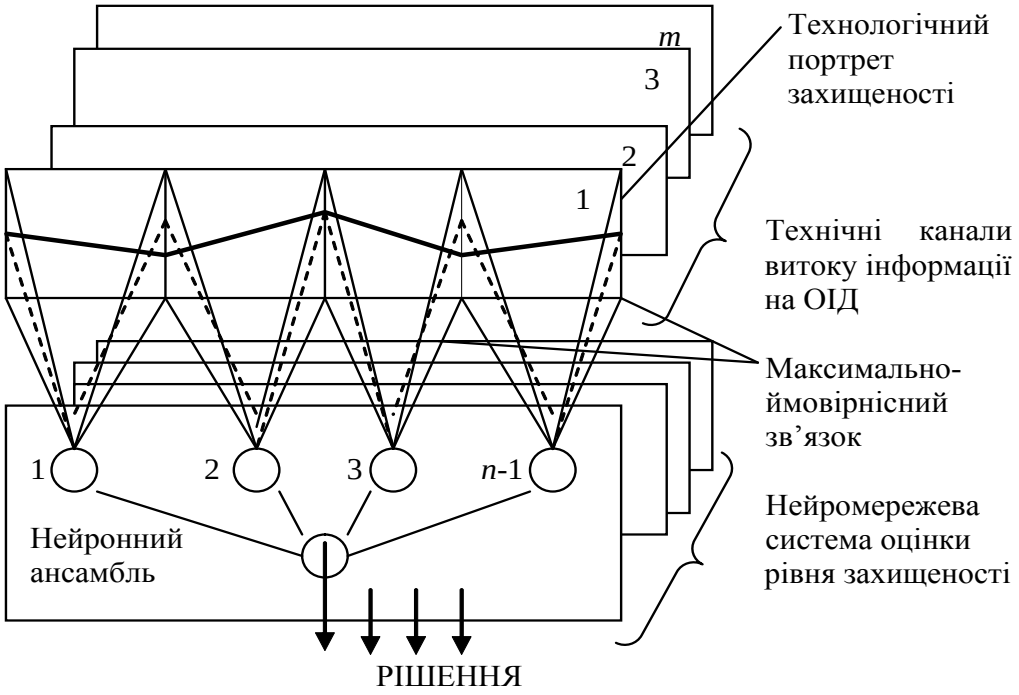

Рис. 1. Структура нейромережевої системи

В 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 $\{m_l\}_{ТКВІ}$, $l = \overline{1, L}$, 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-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 [7].

Послідовність дискретних змінних U_r, k = 0,1,...,n-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-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

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

або

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

При $\Theta_a(k)_\mu=0$ структура системи, що розпізнає, є квазілінійною, а при $\Theta_a(k)_\mu\rangle 0$ вона має нелінійні граничні властивості.

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

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:

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

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 - $\{\lambda_l\}_{TKBI}$, $l=\overline{1,L}$. 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:

$\{m_l\}^*_{TKBI}$, $l=\overline{1,L}$, де $L\le 8$.

Висновки з даного дослідження

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.

Практичне значення отриманих результатів

Запропонована модель проблемно-орієнтованої нейромережної системи оцінки рівня захищеності інформації.

Відмінність її від існуючих систем оцінки рівня захищеності заключається в 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. Найголовнішою відмінністю є те, що рішення задач оцінки рівня захищеності відбувається в масштабі часі, близькому до реального. Ця вимога досягається шляхом реалізації принципу паралельності обробки інформації, що приводить до різкого підвищення швидкодії НМ.

Новизна результату

Науковою новизною результату дослідження є:

вперше запропоновано моделювання системи оцінки рівня захищеності інформації на основі нейромережі.

вперше 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.

рішення задачі оцінки рівня захищеності відбувається в масштабі часі, близькому до реального. Це досягається шляхом реалізації принципу паралельності обробки інформації в нейромережі.

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. Ленков С.В.** Методы и средства защиты информации / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко // Под ред. В.А. Хорошко. – К.: Арий, 2010. – Том I. Несанкционированное получение информации. – 464 с. **5. Толюпа С.В.** Дослідження функціонування інфокомунікаційних мереж нового покоління на основі інтелектуальних технологій. Автореферат дисертації на здобуття наукового ступеня доктора технічних наук. **6. Домарев В.В.** Безопасность информационных технологий: Методология создания систем защиты. К.: ООО «Тид «ДС». 2001. 688 с. **7. Корольов А.П.,** Необхідність побудови нейромережових систем технічного діагностування радіоелектронної техніки / А.П. Корольов, С.В. Толюпа, І.В. Тхоржевський // Зб. наук. праць КВІУЗ. – К., 2001. – № 3. - С. 51-60.

МОДЕЛЬ СИСТЕМЫ ОЦЕНКИ УРОВНЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ НА ОСНОВЕ НЕЙРОСЕТИ

Юрий Иванович Хлапонин ***(канд. техн. наук, с.н.с., доцент кафедры)***

Национальный авиационный университет, Киев

В статье рассматривается модель системы оценки уровня защищенности информации с применением нейросети. Совокупность состояний защищенности, которые соответствуют выявленным на объекте информационной деятельности техническим каналам утечки информации в определенный момент времени, может быть представлена в виде динамических систем. Среда для нейросетевой системы (НМС) оценки уровня защищенности информации может быть представлено в виде совокупности дискретно − событийных систем со связанными дискретными технологическими состояниями защищенности. Предложена структура нейроподобного классификатора, реализущего решающую функцию оценки защищенности информации.

Ключевые слова: *защита информации, нейрон, нейросеть, технологический портрет защищенности.*

THE MODEL OF EVALUATION SYSTEM OF INFORMATION SECURITY LEVEL BASED ON NEURAL NETWORK

Yurii Khlaponin ***(Candidate of Technical Sciences, Senior Research Fellow, Associate Professor of a Department)***

National Aviation University, Kyiv

The article deals with model evaluation system level of data protection with the use of neural networks . The aggregate of security, which correspond to the object of information activities identified technical channels of information leakage at a given time can be represented as dynamical systems. Environment for neural network system (NNS) assess the level of data protection can be represented as a set of discrete – event systems with discrete bound states of technological security. The structure of neural classifier that implements the decision function estimation of information security.

Key words: *information security, neuron, neural network, technology portrait protection.*