УДК 004.056.5 + 004.85

к.т.н. Шевченко А.С. (ВІТІ)
к.т.н. Самойлов І.В. (ВІТІ)
Пономарьов О.А. (ВІТІ)
Науменко О.Г. (НУОУ імені Івана Черняховського)

АНАЛІЗ ЗАСТОСУВАННЯ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ У ЗАДАЧАХ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ

У статті розглядається аналіз застосування штучних нейронних мереж у прикладних задачах забезпечення виявлення та класифікації кіберзагроз. Розглянуто структуру штучних нейронних мереж, математичні основи їх роботи, основні етапи обробки даних при використанні для вирішення задач виявлення кібернетичних загроз.

Шевченко А.С., Самойлов. И.В., А.А. Пономарьов, Науменко А.Г. Анализ применения методов на основе нейронных сетей в задачах обнаружения угроз кибербезопасности. *В статье рассматривается анализ применения методов на основе искусственных нейронных сетей в прикладных задачах обеспечения выявления и классификации киберугроз. Рассмотрена структура искусственных нейронных сетей, математические основы их работы, основные этапы обработки данных при использовании для решения задач обнаружения кибернетических угроз.*

A. Shevchenko, I. Samojlov, O. Ponomarev, O. Naumenko Analysis of applying artificial neural networks in the tasks of detecting cybersecurity threats. *The article contains analysis of applying methods that basis on artificial neural networks in applied problems of detection cyber threats. Mathematical bases of artificial neural networks work and their application in the problem of detection and classification cyber threats are considered.*

Ключові слова: *штучний інтелект, штучні нейронні мережі, методи виявлення аномалій, кібербезпека.*

Вступ. Стрімкий розвиток інформаційних технологій та зріст обсягів інформації, що обертається в кіберпросторі, зробили його сучасним полем бою. Дані процеси призвели до загострення стану кібернетичної безпеки у світі.

Сучасні кіберзагрози зумовлені спробами несанкціонованого доступу (НСД), маніпуляцією, модифікацією та іншими діями над інформацією, які направлені на порушення критеріїв безпеки. Для забезпечення захисту від сучасних кіберзагроз їх необхідно ефективно виявляти. В багатьох засобах захисту інформації присутні підсистеми виявлення, які забезпечують вирізнення та ідентифікацію кіберзагроз.

Для забезпечення виявлення кіберзагроз застосовуються статистичні методи, сигнатурні методи, методи на основі виявлення аномалій. Серед даних методів, на сьогоднішній день, найбільш перспективними є методи виявлення аномалій. На відміну від статистичних та сигнатурних методів методи виявлення аномалій дозволяють виявляти нові атаки, що дозволяє більш ефективно протистояти сучасним кіберзагрозам.

Серед математичних апаратів останніми роками широко впроваджуються в кібербезпеку технології штучного інтелекту (ШІ) [1 – 3].

Головною причиною застосування технологій ШІ стало те, що дані методи дозволяють ефективно здійснювати завдання класифікації широкого класу даних, у тому числі і даних отриманих з кіберпростору.

Аналіз останніх досліджень та публікацій. На сьогоднішній день стрімко розвиваються та впроваджуються технології ШІ. Методи ШІ знайшли застосування у таких сферах як: медицина, робототехніка, автоматизація процесів, розпізнавання графічних та звукових об’єктів, аналітика та передбачення процесів, кібербезпека.

Саме для завдань забезпечення кібербезпеки використання методів ШІ є досить актуальними, основним завданням яких є навчитись виявляти та захищати від складних кіберзагроз.

Результати аналізу останніх публікацій дозволили виділити наступні математичні апарати, які відносяться до технологій ШІ [1 – 5]:

- мережі Баєса (*Bayesian Network*);
- штучні нейронні мережі (*ANN – Artificial Neural Network*);

- приховані марковські моделі (*HMM – Hidden Markov Model*);
- метод опорних векторів (*SVM – Support Vector Machine*);
- фільтри Калмана (*Kalman Filter*);
- методи „випадкового лісу” (*Random Forest*);
- методи на основі класифікації асоціативних правил (*Association Rule Classification*);
- дерева рішень (*Decision Trees*);
- кластеризація методом *k*-середніх (*K-means Clustering*);
- нечітка логіка (*Fuzzy Rule-Based*);
- метод *k*-найближчих сусідів (*k-nearest neighbor*).

Значна кількість даних методів не є новими математичними апаратами для вирішення технічних задач і розвиваються протягом не одного десятиліття. Нові сфери застосування та технології дозволили застосувати вказані математичні апарати у галузі кібербезпеки.

Одними з найбільш динамічних технологій ШІ є технології штучних нейронних мереж (ШНМ), які дозволяють вирішити значну кількість прикладних технічних задач [2, 4, 6, 8].

Мета. У роботі ставиться за мету провести аналіз застосування методів ШІ на основі штучних нейронних мереж для вирішення задач кібернетичної безпеки, способів застосування ШНМ та структури підсистем виявлення інцидентів порушення кібернетичних загроз.

Постановка завдання. Для досягнення мети у роботі необхідно провести аналіз технології на основі ШНМ, представити загальні математичні вирази, які використовуються в задачах виявлення та класифікації кібернетичних загроз, розглянути основні види ШНМ, які використовуються для виявлення аномальних подій та порушень кібербезпеки, визначити основні сфери застосування ШНМ в сучасних засобах забезпечення кібербезпеки.

Обмеження. В роботі обмежуємось розглядом застосування ШНМ для вирішення завдань виявлення кібернетичних атак та порушень кібернетичної безпеки. ШНМ розглядаються на прикладі багатошарового персептрона з алгоритмом зворотного розповсюдження помилки.

Викладення основного матеріалу дослідження

Сучасні кібератаки та методи НСД представляють собою ланцюг складних процесів, що досить ускладнює, а інколи й унеможливлює, процедури виявлення кіберберзагроз. Використання формальних методів на основі встановлених правил, сигнатурних методів, не дозволяють ефективно запобігти сучасним кібернетичним загрозам [2 – 3]. Сповільнене реагування на нові кібернетичні загрози призводить до значних втрат, блокування систем та компрометації великих обсягів конфіденційних даних.

Для більш ефективного виявлення загроз кібернетичної безпеки використовуються евристичні методи. Дані методи дозволяють виявляти нові загрози на основі складних алгоритмів аналізу даних. Значна кількість методів евристичного аналізу ґрунтується на методах ШІ. Одними з методів ШІ є методи, які ґрунтуються на використанні ШНМ. Нейронні мережі використовуються в задачах виявлення, класифікації та прогнозування.

ШНМ є моделлю ШІ, яка перетворює вхідні сигнали на вихідні, за допомогою нелінійних перетворень в групі штучних нейронів прихованих шарів. Суть ШІ на основі ШНМ полягає у навчанні (тренуванні) нейронної мережі на основі наданого їй зразка, або без такого, для здійснення подальшої класифікації або прогнозування на основі тренувальних даних.

В залежності від призначення, ШНМ можуть мати у своєму складі один або декілька прихованих шарів. ШНМ, які мають більше одного прихованого шару отримали назву багатошарового персептрона (*MLP – Multilayer Perceptron*) [8, 9].

Розглянемо більш детально основи роботи ШНМ на основі багатошарового персептрона з алгоритмом зворотного розповсюдження помилки.

Нейронні мережі представляють собою сукупність шарів, які складаються з нейронів. Кожна ШНМ складається з K шарів, кожний з яких складається з N нейронів. Кількість нейронів в кожному шарі може бути різною.

Структурно шари ШНМ поділяються на вхідний, вихідний та приховані. На рис. 1 представлено тришарову ШНМ з одним вхідним шаром ($k = 1$), прихованим ($k = 2$) та вихідним шаром ($k = 3$), де k – кількість шарів ШНМ, $k \in [0, K]$.

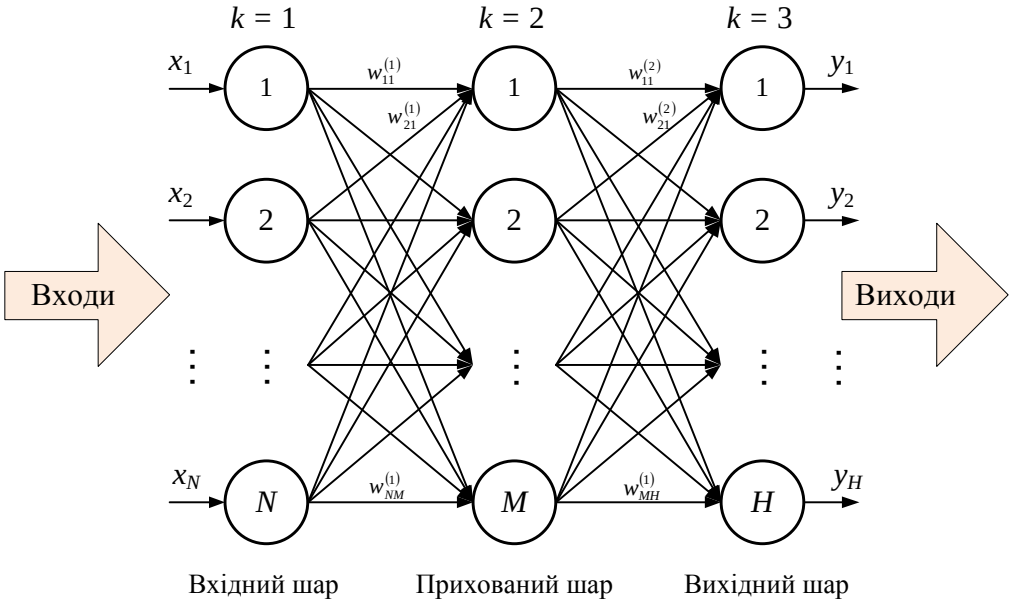

Рис. 1. Структура штучної нейронної мережі

Кожний з нейронів кожного шару з'єднаний з кожним нейроном наступного шару. Дані ШНМ є повнозв'язними. Кожне з'єднання має власну вагу w. На вхід кожного шару подаються вхідні сигнали x, на виході нейрону маємо вихідні сигнали y.

Для навчання ШНМ на початковому етапі генеруються малі значення випадкових величин вагових коефіцієнтів w для кожного зв'язку між нейронами шарів. Представляються вектор вхідних даних $X_q = (x_1, x_2, \ldots, x_N)_q$ та вихідний вектор навчальних зразків даних $D_q = (d_1, d_2, \ldots, d_H)_q$, де X_q – вектор вхідних, даних які поступають на вхід ШНМ, D_q – вектор навчальних зразків даних, які використовуються в процесі навчання ШНМ, x_N – елемент вхідних даних, d_H – елемент навчальних зразків, N – кількість входів (нейронів) у вхідному шарі, H – кількість виходів (нейронів) у вихідному шарі, q – номер зразка в навчальній виборці.

У ШНМ сигнали розповсюджуються у прямому напрямку від входу до виходу за усіма з'єднувальними лініями. Вхідні сигнали з першого шару подають на прихований шар без перетворень. На кожний нейрон прихованого шару подається сигнал від кожного нейрона попереднього шару [9]:

$$S_j = \sum_{i=1}^{I} x_i \cdot w_{ij} , \qquad (1)$$

де S_j – зважена сума сигналів j-го нейрона; x_i – вхідний сигнал від i-го нейрона першого (вхідного) шару; w_{ij} – величина вагового коефіцієнта між i-м нейроном вхідного шару та i-м нейроном прихованого шару; n – порядковий номер нейрона вхідного шару, $n \in [1, N]$; i – порядковий номер нейрона прихованого шару, $i \in [1, I]$.

В основі ШНМ лежать принципи роботи біологічних нейронів. Штучний нейрон може знаходитись у двох станах: збудженому та незбудженому. Для переходу нейрона у збуджений стан на його вхід повинен податись такий рівень сигналу, який би його активував. В якості функції активації в штучних нейронах використовуються порогові та лінійні функції, гіперболічний тангенс, логістична функція, сигмоідна функція [9]:

$$F(S) = \frac{1}{1 - e^{-S}}, \tag{2}$$

радіально-базисна активаційна функція:

$$F(S) = e^{-\frac{\|X-C\|^2}{2\sigma^2}}, \tag{3}$$

де X – вхідний вектор активаційної функції; C – центр активаційної функції; σ – параметр кривої Гауса.

З виходіа нейронів прихованого шару отримуємо результати застосування сигмоідної функції (2) до зваженої суми сигналів j-го нейрона S_j (1). Результуюча функція вихідних сигналів має наступний вигляд [9]:

$$y_j^{(k)} = F\left(\sum_{j=0}^{J} w_{ij}^{(k)} x_i^{(k-1)}\right), \tag{4}$$

де $y_j^{(k)}$ – вихідний сигнал з j-го нейрона k-го шару ШНМ, $x_i^{(k-1)}$ – вхідний сигнал від i-го нейрона шару k-1; $w_{ij}^{(k)}$ – величина вагового коефіцієнта між i-м нейроном k-1 шару та j-м нейроном k-го шару; i – порядковий номер нейрона вхідного шару, $i \in [1, I]$; j – порядковий номер нейрона прихованого шару, $j \in [1, J]$.

За результатами нелінійної обробки вектора вхідних сигналів X_q на виході ШНМ отримуємо вектор вихідних сигналів $Y_q = (y_1, y_2, \ldots, y_H)_q$. Отриманий вектор вихідних сигналів Y_q, для навченої ШНМ, повинен дорівнювати значенням вектора навчальних зразків D_q. В іншому разі ШНМ повинна бути навчена до зазначеного результату. Суть навчання ШНМ полягає в корегуванні вагових коефіцієнтів нейронної мережі, до того стану поки значення зразків навчання та вихідних сигналів не будуть рівними ($Y_q = D_q$).

Основними властивостями ШНМ, які використовуються в системах захисту інформації та кібернетичної безпеки, є можливість ідентифікувати різноманітні атаки, виявляти аномальні події та зловживання в системах та мережах, здійснювати прогнозування поведінки та процесів систем.

Розглянемо прикладне застосування ШНМ в задачах виявлення кіберзагроз. Використання ШНМ в системах виявлення та розпізнавання інцидентів кібернетичної безпеки передбачає реалізацію наступних етапів [4, 6]: збір даних, попередня обробка даних, побудова, тренування та тестування мережі, класифікація загроз (рис. 2).

Збір даних здійснюється за допомогою спеціальних програмних засобів (сніферів), з використанням протоколів збору даних (*NetFlow*, *IPFIX*, *sFlow* та інших) та протоколів збору журналів подій та логів (*Syslog*). Дані від сніферу поступають у вигляді мережних пакетів *IP*, у інших варіантах пакетами зі службовою інформацією у відповідності до протоколу.

Рис. 2. Процес обробки даних та виявлення інцидентів кібернетичної безпеки з використанням штучної нейронної мережі

Вказані вхідні дані не можуть використовуватись ШНМ для виконання класифікації. Первинні вхідні дані потребують обробки. Під час первинної обробки з пакетів витягуються дані, які в подальшому використовуються для обробки ШНМ. До таких вхідних даних відносяться: дані відповідно до бази записів мережних з'єднань *KDD* 99; данні заголовків *IP* пакетів, *TCP* та *UDP* сегментів: *IP* адреси, номери портів, типи протоколів, флаги тощо. Крім того, для приведення до виду, прийнятного для обробки ШНМ ці дані зазнають нормалізації та стискання в залежності від потреби.

Наступним етапом є класифікація загроз. По суті шляхом класифікації загроз здійснюється виявлення та розпізнавання аномальних подій. Процедура класифікації здійснюється безпосередньо за допомогою ШНМ.

Але, будь-яка ШНМ не може здійснювати та розпізнавати кібернетичні загрози без попереднього навчання. Класичні методи на основі ШНМ поділяються на методи навчання з вчителем, навчання без вчителя та навчання з підкріпленням. Для вирішення завдань ідентифікації кібернетичних загроз, як правило, використовуються перші два методи навчання [2].

На сьогоднішній день в задачах забезпечення кібербезпеки використовують різнотипні ШНМ. Для виявлення кібернетичних атак та зловживань в комп'ютерних мережах більш широко використовуються наступні ШНМ [2 – 4, 6, 10 – 13]:

- зі зворотнім розповсюдженням (*BP – Back-propagation*);
- з радіально-базисною функцією (*RBF – Radial Basis Function*);
- з самоорганізуємі карти (*SOM – Self-Organizing Map*).

ШНМ зі зворотнім розповсюдженням помилки на сьогоднішній день найбільш класичний варіант застосування нейронних мереж. Дані мережі дозволяють корегувати ваги з'єднань між нейронами шляхом визначення величини помилки між бажаним значенням виходу та реальним. Найбільше застосування ці ШНМ знайшли в системах виявлення вторгнень [3, 6, 10].

На відміну від класичних ШНМ зі зворотнім розповсюдженням помилки ШНМ з *RBF* мають кращу апроксимаційну здатність, добрі класифікаційні властивості та більшу швидкість навчання. ШНМ з *RBF*, як і попередній клас ШНМ використовуються в системах виявлення вторгнень для вирішення задачах розпізнавання кібернетичних загроз [2, 3, 6].

Методи з використанням ШНМ з самоорганізуємими картами є реалізацією методу навчання без вчителя. *SOM* перетворюють вхід довільної розмірності в низькорозмірні дискретні карти за допомогою методу навчання без вчителя Конохена [2, 7]. Вихідний шар ШНМ складається з нейронів які організовані, зазвичай, у двовимірний простір. ШНМ з SOM використовуються в системах виявлення вторгнень та анти-*DDOS* системах, варіанти їх реалізації представлені в роботах [2, 13].

На сьогоднішній час багато вендорів – розробників засобів захисту інформації та забезпечення кібербезпеки заявляють про використання методів штучного інтелекту у власних продуктах. Методи та математичний апарат, на якому ґрунтуються дані розробки, здебільшого не розкриваються. До основних засобів, які використовують методи на основі ШНМ відносяться: системи антивірусного захисту, системи виявлення та запобігання вторгненням (*IDS/IPS*), системи попередження втрати даних (*DLP*), системи управління інформаційною

безпекою та подіями (*SIEM*), анти-*DDOS* системи, системи розслідування порушень кібернетичнох безпеки та інші системи [2, 3, 5, 6, 10 – 14]. Основною їх особливістю є те, що в даних системах ШНМ застосовуються в задачах інтелектуального пошуку загроз кібернетичної безпеки.

Висновки. Сучасні методи виявлення на сигнатур, асоціативних правил не дозволяють виявляти нові загрози даних про які немає в базі даних загроз. Основним недоліком методів евристичного аналізу є значна кількість хибних спрацювань та пропуску загроз. Використання методів ШІ на основі ШНМ в засобах захисту інформації та кібербезпеки дозволить вирішити завдання інтелектуального виявлення кібернетичних загроз нульового дня. На сьогоднішній день основними проблемами для застосування методів на основі ШНМ є вибір структури ШНМ, функцій активації, методів навчання ШНМ та зразків навчальних даних. Пріоритетним напрямком є розвиток методів навчання без вчителя, що дозволить навчати ШНМ без втручання експерта, що дозволить усунути недолік, який пов'язаний з залежністю від зразків навчальних даних.

Напрямками подальшого дослідження є реалізація ШНМ та здійснення напівнатурного експерименту з виявлення аномальної поведінки з даних, отриманих за *NetFlow* протоколом.

ЛІТЕРАТУРА

1. Гудфеллоу Я., Бенджио И., Курвилль А. Глубокое обучение / пер. с анг. А.А. Слинкина. 2-е изд., испр. М.: ДМК Пресс, 2018. 652 с.

2. Leslie F. Sikos. AI in Cybersecurity. New York : Springer, 2018. 205 p.

3. Sumeet Dua, Xian Du. Data Mining and Machine Learning in Cybersecurity. Boston: CRC Press, 2011. 256 p.

4. Шелухин О.И., Сакалема Д.Ж., Филипова А.С. Обнаружение вторжений в компьютерные сети (сетевые аномалии): уч. пос. для вуз. / под ред. проф. О.И. Шелухина. М. : Горячая линия-Телеком, 2016. 220 с.

5. Roman V. Yampolskiy, M. S. Spellchecker. Artificial Intelligence Safety and Cybersecurity: a Timeline of AI Failures, NY, Cornell University, 2017. – 123 – 128 p.

6. P. Ganesh Kumar, D. Devaraj. Intrusion detection using artificial neural network with reduced input features. *ICTACT Journal on Soft Computing*. 2010. Vol. 01. Issue 01. P. 30 – 36.

7. Christopher M. Bishop. Pattern Recognition and Machine Learning. New York : Springer Science +Business Media. 2006. 758 p.

8. Рашид Т. Создаем нейронную сеть / пер. с англ. СПб.: ООО „Альфа-книга", 2017. 272 с.

9. Ясницкий Л.Н. Интелектуальные системы: учебник. М.: Лаборатория знания, 2016. 221 с.

10. Bhutada S., Bhutada P. Applications of Artificial Intelligence in Cyber Security. *International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)*. 2018. Vol 5. Issue 4. P. 214 – 219.

11. Arockia Panimalar, Giri Pai, Salman Khan. Artificial Intelligence Techniques for Cyber Security. *International Research Journal of Engineering and Technology (IRJET)*. 2018. Vol. 05 Issue 03. P. 122 – 124.

12. Mohammad Amini, Jalal Rezaeenoor, Esmaeil Hadavandi. Effective Intrusion Detection with a Neural Network Ensemble Using Fuzzy Clustering and Stacking Combination Method. *Journal of Computing and Security*. 2014. Vol. 1. Number 4. P. 293 – 305.

13. RasoolAbdulkader A. Alfantookh. DoS Attacks Intelligent Detection using Neural Networks. J. *King Saud Univ. Comp. & Info. Sci.* 2005.Vol. 18. P. 27 – 45.

14. Федорченко А. В., Левшун Д. С., Чечулин А. А., Котенко И. В., Анализ методов корреляции событий безопасности в SIEM-системах. Часть 2, Тр. СПИИРАН, 2016, выпуск 49, 208 – 225.