УДК 004.056.5

В.В Погорелов

ДОСЛІДЖЕННЯ НЕЙРОМЕРЕЖЕВИХ ЗАСОБІВ РОЗПІЗНАВАННЯ КІБЕРАТАК НА МЕРЕЖЕВІ РЕСУРСИ ІНФОРМАЦІЙНИХ СИСТЕМ

Анотація. Розглянуто сучасні методи побудови систем розпізнавання кібератак, що базуються на штучних нейронних мережах. Проаналізовані параметри, що характеризують ефективність роботи та навчання данних систем, визначені типові проблеми, що виникають при застосуванні нейромережевих засобів розпізнавання сигнатур кібератак на мережеві ресурси комп'ютерних систем. Визначено переваги та недоліки використання при вирішення даного класу задач концепції глибинного навчання: глибинних мереж переконань та та згорткових нейромереж.

Ключові слова: Системи розпізнавання кібератак, штучна нейронна мережа, нейромережеві методи розпізнавання, глибинна мережа переконань, згорткова нейромережа.

Вступ. Ефективність застосування нейромережевих методів розпізнавання (НММР) кібератак на мережеві ресурси інформаційних систем (МРІС) підтверджується як статистикою застосування нейромережевих моделей (НММ), так і теоретичними дослідженнями у даній області. Тим не менш, систематичний аналіз вказує на типові проблеми, властиві для систем розпізнавання кібератак (СРК), що значно знижують їх потенціал:

- неспрацьовування та невірні спрацьовування;
- значний час розробки та нестабільність навчання;
- значний час та складність формування навчальної вибірки;
- слабка адаптація до особливостей інформаційних систем (ІС),

Потреба у вирішенні вказаних проблем зумовлює необхідність побудови цілісної методологічної бази застосування НММР при захисті МРІС від кіберзагроз, що є *метою* даного дослідження.

Кібератакою називають сукупність протиправних дій, спрямованих на порушення доступності, цілісності або конфіденційності ІС, що може включати в себе етап усунення

інформації про атаку [1-6]. Кібератаки поділяють на локальні і віддалені (за місцем виникнення) та на активні і пасивні, в залежності від того, який вплив здійснюється на функціонування ІС. Зазвичай, у публікаціях розглядаються кібератаки, що базуються на вразливості саме МРІС, та призводять до порушення функціоналу атакованого ресурсу, наприклад DOS- та DDOS-атаки [4].

Аналіз публікацій за даною темою, дає статистичну вибірку використання НММ при побудові алгоритмів СРК. У роботах [1-3, 9] показані та узагальнені методи адаптації архітектури НММ до окремих ІС, а також розглянуто перспективи оптимізації даних методів в залежності від параметрів завдання. Роботи [4, 11] присвячені особливостям застосування НММ для розпізнавання спроб підбору комбінації логін-пароль і розпізнавання DOS- та DDOS-атак. Значна кількість публікацій присвячена застосуванню у СРК нових видів НСМ [7-16]: засобам розпізнавання на базі багатошарового персептрона [7] та використанню карти Кохонена [8]. У роботах [9-16] розглядаються переваги та недоліки використання концепції глибинного навчання та переходу до СРК на основі нейромереж третього покоління. Показано, що для розпізнавання сигнатур кібератак найбільшу ефективність показують методи на основі загорткових нейромереж [10-12] та глибинних мереж переконань [15, 16].

1. Організація СРК на основі ШНМ для захисту МРІС. Для побудови узагальненої моделі СРК на базі НММ необхідно провести аналіз контрольних параметрів функціонування МРІС. При цьому важливо визначити характеристики нейромережевих моделей і методів, що можуть бути адаптовані до впровадження в СРК, зокрема доступу до бази даних сигнатур кібератак (СК), контроль функціональних параметрів МРІС та обчислювальні ресурси СРК. Розробка концептуальної моделі зумовлює використання такого параметрів, як ефективність, оперативність та ресурсоємність системи [1-3]. Ефективність вказує сукупність характеристик, які відповідають за взаємозв'язок функцій і процедур програмного комплексу, використання апартних ресурсів та послуг, оперативність відповідає часу відгуку, обробки і виконання функцій системою, а ресурсоємність визначає кількість використаних ресурсів і тривалість їх використання.

Діаграма процесу нейромережевого розпізнавання кібератак на МРІС показана на рис. 1.

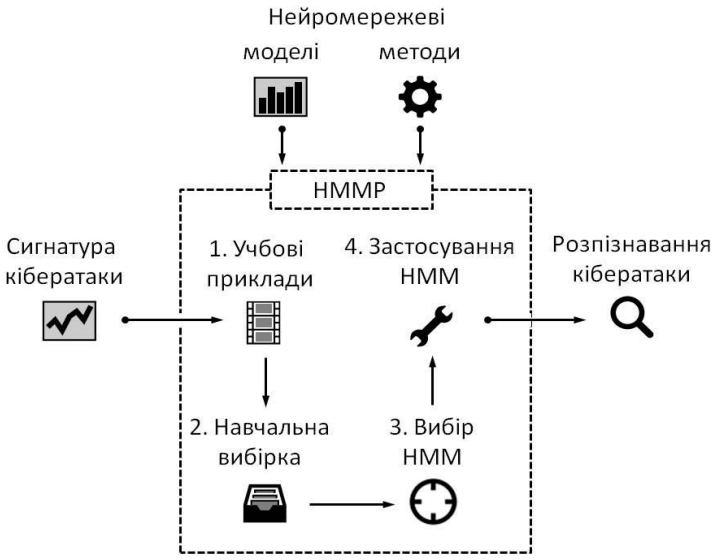

Рисунок 1 - Діаграма процесу нейромережевого розпізнавання кібератак на мережеві ресурси

Призначення компонентів блоку НММР даної діаграми полягає у (1) визначенні для кожного типу кібератак множини вихідних і вхідних параметрів, а також способу їх кодування до виду, що відповідає НММ, (2) побудові множини навчальних прикладів, що є достатньою для навчання НММ, (3) отриманні оптимальних параметрів для ефективного функціонування НММ як елементу СРК у відповідності до МРІС. Слід зауважити, що застосування у МРІС комплексу СРК на базі НСМ є ресурсоємною задачею, що подекуди може використовувати основну частину програмно-апаратних ресурсів системи. В процесі розробки СРК необхідно також враховувати недосконаліть методів та значний час формування параметрів навчальних прикладів для НММ, тому в таких схемах передбачена можливість формування навчальної вибірки за допомогою експертних даних (рис. 2).

Рисунок 2 - Діаграма взаємодії елементів СРК на базі НММ за умови наявності експертної оцінки

2. Аналіз ефективності роботи НММР у складі СРК

Ефективність роботи НММР у складі СРК, таким чином, оцінюється як ефективність процесу навчання НММ, тобто за показниками тривалості та точності роботи, а також ресурсоємності даної системи (рис. 3).

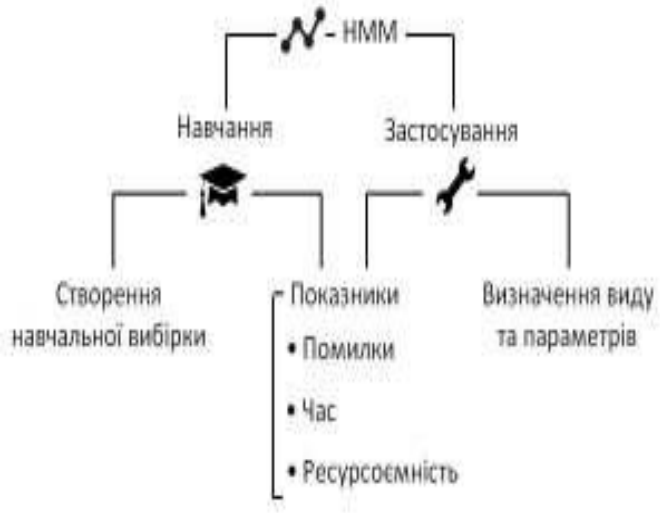

Рисунок 3 - Основні фактори, що визначають ефективність СРК на основі нейромережевих систем

Модель визначення ефективності [1-3] базується на цільовій функції інтегральної ефективності процесу $E_{\sum}(E_{НММР}(e_В, e_П, e_Р), E_{НВ}(e_{НП}, e_{НВ}))$, де $E_{НММР}(e_В, e_П, e_Р)$ – ефективність роботи НММР, що залежить від параметрів $e_В$ відповідає за визначення оптимального НММ, $e_П$ – за пошук параметрів НММ, $e_Р$ – за ресурсоємність використання НМР, а $E_{НВ}(e_{НП}, e_{НВ})$ – ефективність створення навчальної вибірки, де $e_{НП}$ – відповідає за пошук параметрів навчальних прикладів, $e_{НВ}$ – за формування навчальної вибірки. Отже для побудови узагальненої моделі ефективності роботи СРК необхідно побудувати алгоритми визначення множини ефективних видів НММ та оцінювання ефективності виду НММ, очікування вихідного сигналу СК, а також включити параметри обчислювальних ресурсів сервера СРК і системи експертних знань, що використовується при побудові навчальної вибірки. В даному випадку ключовим фактором є ефективність навчання НММ, що залежить від часу побудови навчальної вибірки та часу, що витрачається на процес навчання $t_{\sum}(t_{НВ}, t_{ПН})$. При цьому:

 ISSN 1562-9945

$$\begin{cases} t_{\Sigma} \le t_{\text{д}}(n_i) \\ n_i \in N_{\text{д}} \end{cases}, \quad (1)$$

де $t_{\text{д}}(n_i)$ – максимальний допустимий час побудови навчальної вибірки та навчання НММ, n_i – вид НММ, а $N_{\text{д}}$ – множина допустимих видів НММ. При цьому в загальному випадку вважають, що алгоритм пошуку видів НММ має здійснювати вибірку множини ефективних видів НММ $N_{\text{е}}$ за множини всіх видів НММ N_{0}: $N_{\text{0}} \rightarrow N_{\text{д}} \rightarrow N_{\text{е}}$. Розрахунок функції ефективності кожного окремого НСМ відбувається за наступним критерієм:

$$\begin{cases} E_i = \sum_{k=1}^{K} \alpha_k R_k(n_i) \\ n_i \in N_{\text{д}} \\ i = 1..I \\ \alpha_k = 0..1 \end{cases}, \quad (2)$$

де R_k – критерій ефективності, α_k – ваговий коефіцієнт критерія ефективності, K – кількість критеріїв ефективності, I – кількість видів НММ. Слід зазначити, що функції ефективності відображають пристосованість НММ до конкретного класу задач, що дозволяє звести алгоритм обчислення оптимальних параметрів СРК до задачі пошуку максимумів цільових функцій.

3. Розробка сучасних НММР на основі концепції глибинного навчання. Концепція глибинного навчання, що базується на навчанні ознак, тобто роботі з представленням вхідних данних в межах самої НММ показала свою високу ефективність [9-16] надало змогу перейти до третього покоління штучних нейронних мереж (ШНМ). Навчання глибинних ШНМ відбувається у два етапи. Перший етап включає в себе навчання кожного шару автоасоциативної мережі за принципом «навчання без вчителя», після чого відбувається ініціалізація нейронів прихованих шарів нейронної мережі прямого поширення (НМПП), у ході якої вагові коефіцієнти нейронів кожного шару стають вхідними даними для нейронів наступного шару, що призводить для узагальнення інформації про образ (візуальне зображення чи сигнатуру кібератаки). На другому етапі відбувається процес навчання НМПП зі вчителем, що займає менший час ніж у випадку класичних ШНМ другого покоління, завдяки попередньо проведеному етапу ініціліазації.

У той час, як концепції глибинного навчання активно застосовується при росзпізнаванні образів, визначення ефективності

застосування СРК на основі глибинних ШНМ, все ж таки, є нетривіальною задачею. ШНМ третього покоління показують кращі результати за точністю та здатні працювати з принципово новими класами задач, але при цьому характеризуються викою ресурсоємністю по відношенню до завантаження програмно-апаратного комплексу та строків підготовки до навчання. Розробники повязують це з тривалістю обчислення даного типу алгоритмів та їх схильністю до перенавчання. У СРК, зазвичай, використовують НММ, що базуються на глибинній мережі переконань (ГМП), згорткових ШНМ та ШНМ на основі асоціативної пам'яті.

ГМП мережа складається з прихованих вузлів (шарів латентних змінних), причому з'єднання наявні лише між шарами, а всередині шарів — відсутні (рис. 4). При тренуванні на навчальному наборі сигнатур кібератак ГМП навчається відбудовувати свої входи, причому шари виступають в ролі детекторів ознак на входах. При систематичному аналізі ГМП розглядають як набір обмежених машин Больцмана (ОМБ) для яких прихований шар однієї підмережі слугує видимим шаром для наступної [14-16]. Алгоритм навчання ГМП складається снаступних етапів: (1) тренування ОМБ на вхідній матриці X з метою отримання матрицю вагових коефіцієнтів, (2) перетворення матриці X за допомогою ОМБ для отримання нових даних, (3) повторення попередню процедуру для всіх шарів мережі, (4) тонке налаштування параметрів глибинної архітектури по відношенню до критерію керованого тренування (рис. 4). Спільний розподіл даної НММ для n прихованих шарів h^n може бути записаний наступним чином:

$$P(x, h^1, h^2, \ldots, h^n) = \left(\prod_{k=0}^{n-2} P(h^k \vee h^{k+1})\right) P(h^{n-1}, h^n), \qquad (3)$$

де $P(h^k \vee h^{k+1})$ — це умовний розподіл на рівні k, а $P(h^{n-1}, h^n)$ — спільний розподіл ОМБ верхнього рівня (рис. 4).

 ISSN 1562-9945

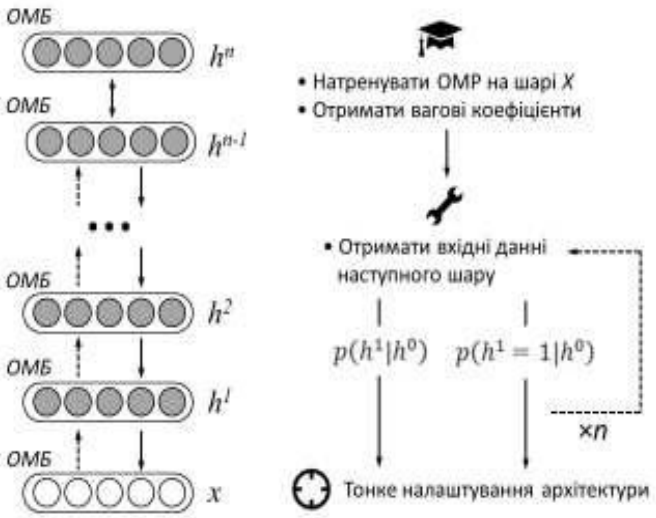

Рисунок 4 - Структура та алгоритм тренування ГМП

Перетворення матриці X відбувається шляхом вибірки $p(h^1 \vee h^0)$ або обчислення середньої активації прихованих вузлів $p(h^1 = 1 \vee h^0)$.

Згорткові ШНМ складаються з декількох шарів, за допомогою яких обробляють рецептивні поля вхідного образу (сигнатури кібератаки). Вихідні дані збірок кожного шару накладаються таким чином, щоб області перекривалися, що збільшує точність роботи нівелює вплив паралельних перенесень образу. Таким чином, для різних нейронів вихідного шару використовуються одна матриця вагових коефіцієнтів (ядром згортки). Шар отриманний в результаті операції згортки ядром згортки, показує наявність ознаки в шарі, що оброблюється, формуючи карту ознак. Далі операція субдискретізації виконує зменшення розмірності сформованих карт ознак і формує підвибірку. За рахунок цієї операції подальші обчислення прискорюються, а ШНМ стає більш інваріантною до масштабу вхідного зображення. Після обробки сигнатури кібератаки (вхідного образу) сигнал проходить шари згортки, в яких повторюються операції згортки і субдіскретізації (рис. 5). На кожному наступному шарі карти ознак зменшуються в розмірі, але збільшується кількість каналів, по яким обробляються карти ознак, що надає системі здатність розпізнавання складних ієрархій ознак.

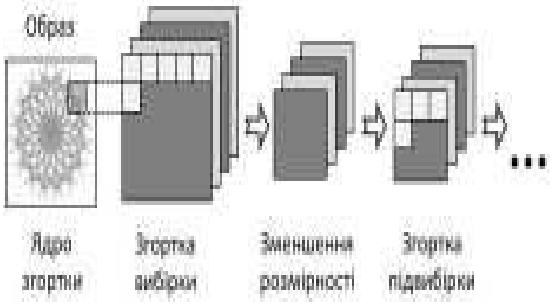

Рисунок 5 - Типова архітектура згорткової ШНМ

Основною перевагою застосування згорткових ШНМ у СРК є використання спільної ваги у згорткових шарах, що зменшує ресурсоємність і збільшує швидкодію системи. Важливо підкреслити, що згоркові ШНМ проводить тренування фільтрів по схемі «без вчителя», при цьому попередня обробка займає для данних мереж найменший час, у порівнянні з іншими ШНМ третього покоління, що суттєво зменшує собівартість підготовки СРК на базі загорткових ШНМ.

Висновки. Штучні нейронні мережі показали себе ефективним інструментом розпізнавання кібератак на мережеві ресурси інформаційних систем. Практика досліджень у цій галузі вказує на переваги застосування нейромереж третього покоління, зокрема глибинної мережі переконань та загорткової нейромережі. При розробці адекватної математичної моделі нейромережевих систем розпізнавання сигнатур кібератак важливо враховувати параметри ефективності, оперативності та ресурсоємності системи. Зазначені функції слід віднести до цільових функцій, що відображають пристосованість нейромережевої моделі розпізнавання до конкретного класу задач. За їх допомогою алгоритм обчислення оптимальних параметрів системи може бути зведений до математичної задачі пошуку максимумів функцій.

ЛІТЕРАТУРА

1. Бурячок В.П. Завдання, форми та способи ведення воєн у кібернетичному просторі / В. Л. Бурячок, Г. М. Гулак, В.О. Хорошко // Наука і оборона . – 2011. – №3. – С. 35-43.

2. Гірницька Д.А. Визначення коефіцієнтів важливості для експертного оцінювання у галузі інформаційної безпеки / Д.А. Горніцька, В.В. Волянська, А.О. Корченко // Захист інформації. – 2012. – Том 14, №1 (54). – С. 108-121.

3. Гнатюк С. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. / С. Гнатюк // Безпека інформації. – 2013. – Том 9, №2. – С. 118 – 129.

4. Емельянова Ю.Г. Нейросетевая технология обнаружения сетевых атак на информационные ресурсы / Ю.Г. Емельянова, А.А. Талалаев, И.П. Тищенко,

В.П. Фраленко // Программные системы: теория и приложения. – 2011. – №3(7). – С. 3–15.

5. Терейковський І. Нейронні мережі в засобах захисту комп'ютерної інформації / І. Терейковський. – К. : ПоліграфКонсалтинг. – 2007. – 209 с.

6. Корченко А.А. Модель эвристических правил на логико-лингвистических связках для обнаружения аномалий в компьютерных системах / А.А. Корченко //Захист інформації – 2012. – № 4. – С. 109-115.

7. Терейковський І.А. Вдосконалення алгоритму навчання багатошарового персептрону призначеного для розпізнавання мережевих атак / І.А. Терейковський // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні — 2012. — Випуск 2 (24). — С. 65-70.

8. Bezobrazov S., Golovko V. Neural Networks for Artificial Immune Systems: LVQ for Detectors Construction // IDAACS'2007: proceedings of the 4 IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications. – Dortmund, 2010. – P. 180-184.

9. Y. Mo, T. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopol, "Cyber-physical security of a smart grid infrastructure," Proceedings of the IEEE, vol. 100, no. 1, pp. 195-209, January 2012.

10. Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 3, pp. 717 - 729, March 2014.

11. L. L. an M. Esmalifalak, Q. Ding, V. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," IEEE Transactions on Smart Grid, vol. 5, pp. 612 - 621, March 2014.

12. Y. Liu, L. Yan, J. Ren, and D. Su, "Research on efficient detection methods for false data injection in smart grid," in International Conference on Wireless Communication and Sensor Network (WCSN), Wuhan, China, December 2014, pp. 188 - 192.

13. Z. Hu, Y. Wang, X. Tian, X. Yang, D. Meng, and R. Fan, "False data injection attacks identification for smart grids," in Third International Conference on Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE), Beirut, Lebanon, April - May 2015, pp. 139 - 143.

14. H. Lee, R. Grosse, R. Ranganath, and A. Ng, "Unsupervised learning of hierarchical representations with convolutional deep belief networks," Communications of the ACM, vol. 54, no. 10, pp. 95 - 103, October 2011.

15. Y. Yan, X. Yin, S. Li, M. Yang, and H. Hao, "Learning document semantic representation with hybrid deep belief network," Computational Intelligence and Neuroscience, vol. 2015, pp. 1 - 9, 2015.

16. Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," ACM Transactions on Information and System Security, p. to appear, 2011.