УДК 681.3.06

Олександр Григорович Корченко
Доктор технічних наук, професор, завідувач кафедри безпеки інформаційних технологій
Ігор Анатолійович Терейковський
Кандидат технічних наук, доцент, докторант кафедри безпеки інформаційних технологій
Світлана Володимирівна Казмірчук
Кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій

Національний авіаційний університет, Київ

ВЕРИФІКАЦІЯ НЕЙРОМЕРЕЖЕВИХ МЕТОДІВ РОЗПІЗНАВАННЯ КІБЕРАТАК

Вперше доведена гарантованість розпізнавання кібератак за допомогою нейронних мереж типу багатошарового персептрону та мережі радіальної базисної функції. Вказаний висновок сформовано на основі робіт Хехт-Нільсена, Д. Парка та І. Сандберга про можливість використання нейронної мережі для апроксимації з заданою точністю будь-якої неперервної багатопараметричної функції, а авторами показано можливість моделювати процес виявлення кібератаки за допомогою вказаної неперервної багатопараметричної функції.

Ключові слова: нейронна мережа, багатошаровий персептрон, мережа радіальної базисної функції, виявлення кібератак

Впервые доказана гарантированность распознавания кибератак с помощью нейронных сетей типа многослойного перспетрона и сети радиальной базисной функции. Указанный вывод сформирован на основе работ Хехт-Нильсена, Д. Парка и И. Сандберга о возможности аппроксимации нейронной сетью с заданной точностью любой непрерывной многопараметрической функции, а авторами показана возможность моделирования процесса обнаружения кидбератаки с помощью указанной многопараметрической функции.

Ключевые слова: нейронная сеть, многослойный персептрон, сеть радиальной базисной функции, выявления кибератак

The article is devoted to the definition of the plausibility of the results of neural network methods for detecting cyber attacks. It is shown that low self because of the discovery of cyber attacks by using neural network techniques is one of the important barriers to improving the security of information systems.
First brought guarantee the cyberattacks recognition using neural networks type multilayer perceptron and radial basis function networks. The study used the work Hecht-Nielsen, J. Park and I. Sandberg which proved approximation guarantee the specified accuracy of any continuous parametric function of many using neural networks type multilayer perceptron and radial basis function. It is shown that the multilayer perceptron parameters sigmoid activation function can be defined a priori, and in the output layer neurons can be used linear activation function type
Determined that the cyber security of the identification depends on the ability to simulate the process of identifying cyber attacks on resource information system using the same continuous function.
This result is used to prove the security of network detection of cyber attacks, which are the signature database KDD- 99.

Keywords: neural network, multilayer perceptron, radial basis function network, detecting cyber attacks

Постановка проблеми

Відповідно Доктрини інформаційної безпеки України, прояви комп'ютерної злочинності та комп'ютерного тероризму належать до основних загроз, що заважають сталому та безпечному функціонуванню національних інформаційних систем (ІС). При цьому захист національних інформаційних ресурсів інформаційних систем (РІС) від кібернетичних атак належить до одного із базових напрямів державної політики у сфері інформаційної безпеки [12]. Очевидно, що

ефективність та надійність такої системи захисту багато в чому залежить від ефективності та надійності виявлення кібератак, для чого застосовуються різноманітні методи, серед яких одними із найбільш перспективних вважаються нейромережеві [1; 3; 5; 6; 10]. Хоча ефективність нейромережевих методів і вважається доведеною, однак проблема надійності таких методів на сьогодні є невирішеною [1; 3; 4; 15]. Це істотно звужує сферу їхнього застосування та значно ускладнює створення надійних систем виявлення кібератак (СВА). Вказані передумови визначають основну проблему цієї статті – підвищення ефективності процесу створення систем захисту інформації за рахунок використання нейромережевих методів виявлення кібератак.

Аналіз останніх досліджень і публікацій

Проаналізовані роботи [1; 4-6; 8-11; 15] присвячені розробці нейромережевих технологій виявлення мережевих атак на РІС. Сучасні дослідження нейромережевих методів виявлення кібератак переважно присвячені розгляду різноманітних технологічних аспектів створення відповідних інструментальних засобів. В [1; 5; 6] запропоновані методи стиснення простору ознак, що використовується в нейронних мережах (НМ) для виявлення мережевих атак. За допомогою числових експериментів показано, що позитивний результат полягає у зменшенні терміну процесу навчання НМ. У [9; 11] розроблено метод визначення типу архітектури НМ, оптимальної з точки зору умов поставленої задачі розпізнавання. Також за допомогою числових експериментів доводиться, що оптимізація архітектури дозволить підвищити точність та оперативність розпізнавання. Робота [10] присвячена задачам вдосконалення структури та алгоритму навчання багатошарового перспетрону, призначеного для використання в системах виявлення атак. Показано, що за рахунок такого вдосконалення можливо підвищити обчислювальну потужність засобів розпізнавання. У [8] створена узагальнена модель комп'ютерної атаки і метод її автоматичного виявлення в процесі моніторингу за поведінкою об'єктів розподілених ІС та їх взаємодією. Робота переважно спрямована на вдосконалення загальнотеоретичних підходів до виявлення мережевих атак та має дещо оглядовий характер, хоча в ній і є задекларовані спроби розпізнавання деяких типів атак. Питання розробки моделей НМ, призначених для виявлення мережевих атак, комп'ютерних вірусів, спаму та витоків текстової інформації, розглянуті в [1; 4; 6; 11]. Показана перспективність розробки відповідних інструментальних засобів. Засобам розпізнавання атак на базі кібернейрону присвячена робота [4], а в [15] пропонується для розпізнавання атак використовувати карту Кохонена, яка функціонує відповідно принципів штучних імунних систем. У цих роботах показана потенційна можливість підвищення якості розпізнавання атак за рахунок використання нових нейромережевих моделей. У [3] проведено порівняльний аналіз методів виявлення кібратак: аналіз сигнатур, статистичний аналіз, контроль цілісності, аналіз станів, графи сценаріїв атак, експертні системи, методи, що базуються на специфікаціях, НМ, імунні мережі, кластерний аналіз, поведінкова біометрія. Доведена висока перспективність застосування НМ для виявлення кібератак. Слід зазначити, що в наведених роботах верифікація нейромережевих методів виявлення кібератак проводилась виключно шляхом числових експериментальних досліджень для окремих видів кібератак. Зазначимо, що під поняттям верифікації нейромережевих методів будемо розуміти доведення спроможності виявити кібератаку за допомогою НМ. При цьому аналіз літератури не виявив теоретичних підходів до верифікації нейромережевих методів виявлення кібератак, що значно ускладнює можливість узагальнення отриманих результатів та не дозволяє навіть принципово оцінити надійність такого виявлення.

Мета статті

Мета статті – розв'язання задачі верифікації нейромережевих методів виявлення кібератак.

Виклад основного матеріалу досліджень

Відповідно до [7], під поняттям кібератаки будемо розуміти реалізацію у кіберпросторі загроз безпеці його компонентів (а саме конфіденційності, цілісності та доступності) з урахуванням їх уразливостей. При цьому кіберпростір визначається як віртуальний простір, отриманий у результаті взаємодії користувачів, програмного та апаратного забезпечення, мережевих технологій (у т.ч. Інтернет) для підтримки та управління процесами перетворення інформації (електронних РІС) з метою забезпечення інформаційних потреб суспільства. Як відповідний пункт дослідження використано результати [2; 14; 16; 17], в яких показана можливість використання НМ для апроксимації з заданою точністю довільної функцій. Так, у [17] доведена теорема Хехт-Нільсена, в якій показана принципова можливість представлення неперервної довільної функції багатьох змінних за допомогою НМ з прямим поширенням сигналу, що містить як мінімум один схований шар нейронів. Структурно така НМ складається з N вхідних нейронів, як мінімум з $2N+1$ схованих нейронів з сигмоїдальнимим

функціями активації виду (1), (2) і *M* вихідних нейронів з невідомими функціями активації:

$$f(x)=\frac{1}{1-e^{-\alpha x}}, \quad (1)$$

$$f(x)=\frac{e^{\alpha x}-e^{-\alpha x}}{e^{\alpha x}+e^{-\alpha x}}, \quad (2)$$

де *f* – сигмоїдальна функція активації, *x* – сумарний вхідний сигнал нейрону; *α* – деякий коефіцієнт.

У [2] результати цієї теореми дещо розширені. Доведено, що параметри сигмоїдальної функції активації можуть бути задані апріорно, а у вихідному шарі нейронів може бути використана лінійна функція активації виду:

$$g(x)=ax+b, \quad (3)$$

де *g* – лінійна функція активації; *x* – сумарний вхідний сигнал нейрону; *a, b* – деякі коефіцієнти.

Зазначимо, що описаний тип НМ з одним шаром схованих нейронів отримав назву двошарового персептрону, а з декількома шарами схованих нейронів – назву багатошарового персептрону (БШП) [9-11]. Структура БШП показана на рис.1.

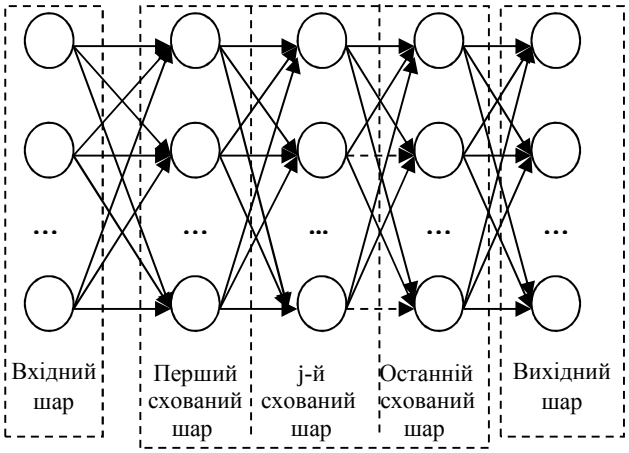

Рис. 1. Структура БШП

Схожий результат, але вже для НМ типу радіальної базисної функції (РБФ) отримано в роботах Д. Парка та І. Сандберга [14]. Доведено, що при виконанні певних структурних правил (достатня кількість схованих нейронів), за допомогою РБФ можливо апроксимувати довільну гладку функцію. Спрощена структура РБФ показана на рис. 2.

Таким чином, верифікації підлягають нейромережеві методи, які базуються на використанні НМ типу БШП або РБФ.

Наступним етапом верифікації стало дослідження функціоналу процесу виявлення кібератак. Розглядали лише кібератаки, спрямовані на РІС.

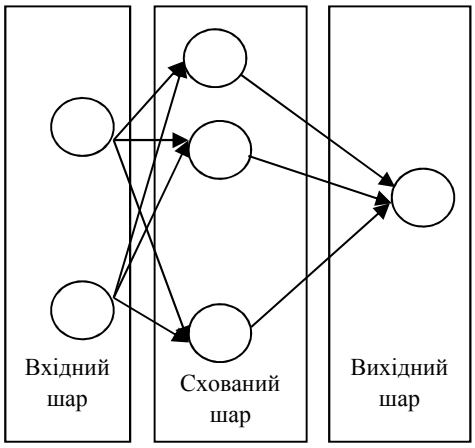

Рис. 2. Структура РБФ

Оскільки стан захищеності таких ресурсів залежить від подій, які в ньому відбуваються, та характеризуються набором певних підконтрольних параметрів захищеності, то в першому наближенні модель виявлення кібератак можна записати у вигляді таких виразів:

$$\exists\, s(t)\in S_a(t)\wedge p(t)\in P_a(t)\Rightarrow A, \quad (4)$$

$$\exists\, s(t)\notin S_n(t)\vee p(t)\notin P_n(t)\Rightarrow A, \quad (5)$$

де *s(t)* – множина подій, що відбулись ІС; *p(t)* – множина значень параметрів захищеності ІС на момент часу *t*; $S_a(t), P_a(t)$ – множина подій в ІС та множина значень параметрів захищеності, характерних при реалізації атаки; $S_n(t), P_n(t)$ – множина подій та множина значень параметрів захищеності, характерних для нормального стану ІС на момент часу *t*; *A* – реалізація кібератаки.

Доповненням до виразів (4), (5) можуть бути вирази (6), (7), за допомогою яких можна виявити нормальний стан захищеності РІС:

$$\exists\, s(t)\notin S_a(t)\wedge p(t)\notin P_a(t)\Rightarrow N, \quad (6)$$

$$\exists\, s(t)\in S_n(t)\wedge p(t)\in P_n(t)\Rightarrow N, \quad (7)$$

де *N* – нормальний стан захищеності РІС.

Метод виявлення кібератак за допомогою виразів (4), (6) називають "виявлення зловживань", а метод виявлення кібератак за допомогою виразів (5), (7) – "виявлення аномалій" [1; 3; 5]. Використавши (4) – (6) узагальнюючу модель виявлення кібератаки, можна записати у вигляді неперервної функції багатьох змінних:

$$\begin{cases} U=F(s(t),p(t),S_a(t),S_n(t),P_a(t),P_n(t)) \\ U\in(A,N) \end{cases}. \quad (8)$$

Зазначимо, що подібна модель виявлення кібератак на РІС використана в [1; 5; 6; 13]. При цьому модель (8), як і моделі (4) – (7), носить узагальнений характер. В багатьох випадках для виявлення атак використовуються тільки окремі

компоненти. Отже, застосування до функціоналу (8) теореми Хехт-Нільсена та результатів Д. Парка та І. Сандберга дозволяє стверджувати, що за допомогою НМ типу БШП та РБФ можна із заданою точністю виявити кібератаки на РІС. Також можна стверджувати, що необхідною умовою для верифікації нейромережевих засобів виявлення кібератак є можливість представлення параметрів та подій, які сигналізують про стан захищеності, у вигляді неперервних функцій.

Розглянемо використання отриманого результату на практичному прикладі.

Дано: база даних KDD-99, яка містить приклади нормального функціонування ІС та сигнатури мережевих атак на РІС.

Довести: гарантованість розпізнавання представлених мережевих атак за допомогою нейромережевих методів.

Розв'язання. База даних KDD-99 містить близько 5 000 000 записів – образів мережевих з'єднань, зареєстрованих через певні проміжки часу [18]. Кожен запис складається з 42 полів. У полях від 1 до 41 записані такі параметри мережевого з'єднання, як тривалість, тип протоколу, мережевий сервіс, кількість отриманих байтів, кількість переданих байтів, статус з'єднання і т. ін. У 42 полі записана інформація, що характеризує стан захищеності ІС – або відсутність атаки (normal), або її тип. У базі представлено 22 види атаки, які розділяються на 4 основних класи – відмова в обслуговуванні (DoS), несанкціоноване отримання прав доступу незареєстрованим користувачем (R2L), несанкціоноване підвищення привілеїв (U2R) зареєстрованим користувачем та сканування портів (Probe). Тому для виявлення атак можна використати тільки величини 41 параметру захищеності (параметри мережевого трафіку), множина виявлених атак складається із 22 елементів (представлених видів атак), множина нормальних станів із одного елемента. Це дозволяє переписати (8) у вигляді функції:

$$\begin{cases} U = F(p_1, p_2, \ldots p_{41}) \\ U \in (A_1, A_2, \ldots A_{22}, N_1\}' \end{cases} \qquad (9)$$

де $p_1, p_2, \ldots p_{41}$ – параметри захищеності; $A_1, A_2, \ldots A_{22}$ – види мережевих атак; N_1 – нормальний стан ІС.

Застосування до функції (9) теореми Хехт-Нільсена та результатів Д. Парка та І. Сандберга вказує на можливість використання БШП та РБФ для виявлення кібератак.

Висновки

1. Вперше розв'язана задача верифікації нейромережевих методів виявлення кібератак. Рішення базуються на можливості моделювати кібератаку неперервною багатопараметричною функцією та використанні теорем Колмогорова-Арнольда та Хехт-Нільсена.

2. Верифіковано виявлення мережевих атак, сигнатури яких представлені в базі даних KDD-99.

3. Перспективи подальших досліджень пов'язані з розробкою методів проектування нейронних мереж, призначених для виявлення кібератак.

Список літератури

1. *Абрамов Е.С. Разработка и исследование методов построения систем обнаружения атак: дис. … канд. техн. наук: 05.13.19 / Абрамов Е.С. – Таганрог, 2005. – 199 с.*

2. *Алексеев Д. В. Приближение функций нескольких переменных нейронными сетями / Д.В. Алексеев // Фундаментальная и прикладная математика. – 2009. – Том 15, № 3. – С. 9 – 21.*

3. *Анализ существующих методов обнаружения удаленных сетевых атак. Перспективы развития средств и комплексов связи. Подготовка специалистов связи: Материалы межвузовской научной конференции. В 2 ч. Ч. 2 / Новочеркасское высшее военное командное училище связи. – Новочеркасск, 2009. – С. 56-61.*

4. *Артеменко А.В., Головко В.А. Анализ нейросетевых методов распознавания компьютерных вирусов /Материалы секционных заседаний. Молодежный инновационный форум «ИНТРИ» – 2010. – Минск: ГУ «БелИСА», 2010. – 239 с.*

5. *Большев А.К. Алгоритмы преобразования и классификации трафика для обнаружения вторжений в компьютерные сети: авторефер. дисс. на соискание научн. степени канд. техн. наук: спец. 05.13.19 – Методы и системы защиты информации, информационная безопасность / А.К. Большев – Санкт-Петербург, 2011. – 36 с.*

6. *Гамаюнов Д.Ю. Обнаружение компьютерных атак на основе анализа поведения сетевых объектов: авторефер. дисс. на соискание научн. степени канд. техн. наук: спец 05.13.11 – математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей / Д.Ю. Гамаюнов – Москва, 2007. – 11 с.*

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

8. *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.*

9. Комар М.П. Нейросетевой подход к обнаружению сетевых атак на компьютерные системы / М.П. Комар, И.О. Палий, Р.П. Шевчук, Т.Б. Федысив // Інформатика та математичні методи в моделюванні – 2011. – Том 1, №2. – С. 156-160.

10. 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.

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

12. Указ Президента України № 514/2009 "Про Доктрину інформаційної безпеки України" [Електронний ресурс]. – Режим доступу: http:// www.rada.gov.ua.

13. Шангин В.Ф. Защита компьютерной информации. Эффективные методы и средства / В.Ф. Шангин – М.: ДМК Пресс, 2010. – 544 с.

14. Bishop C.M. Neural Network for Pattern Recognition. – Oxford: Oxford University Press, 1997. – 482 p.

15. 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.

16. Gorban A.N. and Wunsch D.C. The General Approximation Theorem // Proceedings of Intern. Joint Conf. on Neural Networks'98. – 1998.

17. Hecht-Nielsen R. Kolmogorov's mapping neural network existence theorem // IEEE First Annual Int. Conf. on Neural Networks, San Diego, 1987. Vol. 3.–P. 11–13.

18. KDD cup 99 Intrusion detection data set [Електронний ресурс]. Електрон. текстові дані (752 Мб). – Darpa: Irvine, CA 92697-3425, 1999. – Режим доступу: http://kdd.ics.uci.edu/databases/kddcup99. Thursday, 5 December2013 19:07:34.

References

1. *Abramov E.S. (2005). Development and research methods for constructing intrusion detection systems. Taganrog. 199.*

2. *Alekseev D.V. (2009). Approximation of functions of several variables by neural networks. Fundamental and Applied Mathematics. Volume 15, № 3. 9-21.*

3. *Analysis of existing methods for the detection of remote network attacks. Prospects for the development of communication systems and equipment. Training specialists saints. (2009). Proceedings of the Inter-University Scientific Conference. Novocherkassk. 56-61.*

4. *Artyomenko A.V., Golovko V.A. (2010). Analysis of neural network pattern recognition methods of computer viruses owls. Materials breakout sessions. Youth Innovation Forum "intro". Minsk. 239.*

5. *Bol'shev A.K. (2011). Conversion algorithms and classification of traffic for intrusion detection in computer networks. St. Petersburg, 36.*

6. *Gamayunov D.Y. (2007). Detection system based on the analysis of the behavior of network objects. Moscow. 11.*

7. *Hnatiuk S. (2013). Cyberterrorism: history of current trends and countermeasures. Safety information. Volume 9, № 2. 118 - 129.*

8. *Emelyanova Y.G., Talalaev A.A., Tishchenko I.P., Fralenko V.P. (2011). Neural network intrusion detection technology to information resources. Software Systems: Theory and Applications. Number 3 (7). 13-15.*

9. *Komar M.P., Paly I.O., Shevchuk R.P., Fedysiv T.B. (2011). Neural network approach to detect network attacks on computer systems. Computer and mathematical methods in modeling. Vol 1, № 2. 156-160.*

10. *Tereykovskiy I. (2012). Improving the training algorithm of multilayer perceptron designed to detect network attacks. Legal, regulatory and metrological support information security system in Ukraine. Issue 2 (24). 65 – 70.*

11. *Tereykovskiy I. (2007). Neural network means of information protection. Kiev, PolihrafKonsaltynh, 209.*

12. *Decree of the President of Ukraine № 514/2009 "On the Doctrine of Information Security of Ukraine". http:// www.rada.gov.ua.*

13. *Shangin V.F. (2010). Protection of computer information. Effective methods and means. Moscow. 544s.*

14. *Bishop C.M. Neural Network for Pattern Recognition. – Oxford: Oxford University Press, 1997. – 482 p.*

15. *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.*

16. *Gorban A.N. and Wunsch D.C. The General Approximation Theorem // Proceedings of Intern. Joint Conf. on Neural Networks'98. – 1998.*

17. *Hecht-Nielsen R. Kolmogorov's mapping neural network existence theorem // IEEE First Annual Int. Conf. on Neural Networks, San Diego, 1987. Vol. 3.–P. 11–13.*

18. *KDD cup 99 Intrusion detection data set. Darpa. (1999). http://kdd.ics.uci.edu/databases/kddcup99.*

Стаття надійшла до редколегії 17.02.2014

Рецензент: д-р техн. наук, проф. С.В. Цюцюра, Київський національний університет будівництва та архітектури, Київ.