МЕТОД ЗАСТОСУВАННЯ ПРОДУКЦІЙНИХ ПРАВИЛ ДЛЯ ПОДАННЯ ЕКСПЕРТНИХ ЗНАНЬ В НЕЙРОМЕРЕЖЕВИХ ЗАСОБАХ РОЗПІЗНАВАННЯ МЕРЕЖЕВИХ АТАК НА КОМП'ЮТЕРНІ СИСТЕМИ

Володимир Тарасенко[1], Олександр Корченко[2], Ігор Терейковський[1]

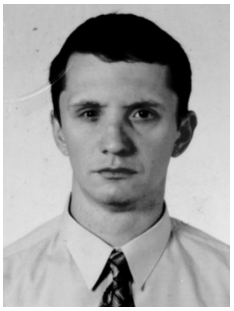
[1]Національний технічний університет України «Київський політехнічний інститут», Україна
[2]Національний авіаційний університет, Україна

ТАРАСЕНКО Володимир Петрович, д.т.н., професор

Рік та місце народження: 1944 рік, Чернігівщина, Україна.
Освіта: Київський політехнічний інститут, 1968.
Посада: завідувач кафедри СПСКС НТУУ «КПІ».
Наукові інтереси: комп'ютерні системи та компоненти.
Публікації: більше 500 статей, авторських свідоцтв, монографій, навчальних посібників і т.ін.
E-mail: vtarasen@scs.ntu-kpi.kiev.ua

КОРЧЕНКО Олександр Григорович, д.т.н., професор

Рік та місце народження: 1961 рік, м. Київ, Україна.
Освіта: Київський інститут інженерів цивільної авіації (з 2000 року – Національний авіаційний університет), 1983 рік.
Посада: завідувач кафедри безпеки інформаційних технологій з 2004 року.
Наукові інтереси: інформаційна та авіаційна безпека.
Публікації: більше 270 наукових публікацій, серед яких монографії, словники, підручники, навчальні посібники, наукові статті та патенти на винаходи.
E-mail: icaocentre@nau.edu.ua



ТЕРЕЙКОВСЬКИЙ Ігор Анатолійович, к.т.н., доцент

Рік та місце народження: 1967 рік, м. Тернопіль, Україна.
Освіта: Київський інститут інженерів цивільної авіації (з 2000 року – Національний авіаційний університет), 1992 рік.
Посада: доцент кафедри системного програмування та спеціалізованих комп'ютерних систем з 2009 року.
Наукові інтереси: інформаційна безпека.
Публікації: більше 50 наукових публікацій, серед яких монографія, навчальні посібники, та наукові статті.
E-mail: terejkowski@ukr.net

Анотація. *Використання теорії штучних нейронних мереж є одним із шляхів підвищення ефективності функціонування систем виявлення атак на комп'ютерні мережі. У цій статті запропоновано метод подання експертних знань в нейромережевих засобах розпізнавання мережевих атак на комп'ютерні системи. Особливістю методу є використання продукційних правил та нейронної мережі PNN. Отримані результати дозволяють підвищити оперативність розпізнаваннята розширити множину видів мережевих атак, характеристики яких не представлені в зареєстрованих статистичних даних.*

Ключові слова: *захист інформації, мережева атака, комп'ютерна система, нейронна мережа, експертна система, продукційні правила.*

Вступ

Протягом декількох останніх років однією із найбільш актуальних проблем в галузі захисту інформації є підвищення ефективності методів розпізнавання мережевих атак на інформаційні ресурси комп'ютерних систем (КС) [1, 6]. При цьому важливим напрямком підвищення ефективності є

«інтелектуалізація» методів розпізнавання за рахунок використання теорії штучних нейронних мереж (НМ) [1-5,11-14]. Перспективність вказаного напрямку підтверджується окремими вдалими застосуваннями НМ в засобах розпізнавання атак (продукція компанії Cisco) та великою кількістю відповідних теоретико-практичних робіт, огляд яких наведено в [1, 2, 12]. Разом з тим велика кількість хибних спрацювань, довготривалий термін та нестабільність навчання, недостатня адаптація до багатьох особливостей сучасного стану КС, що пов'язана в першу з методологічними недоліками, значно обмежують їх практичну цінність. Отже терміново слід вирішити проблему, викликану з одного боку необхідністю та перспективністю використання існуючих нейромережевих засобів розпізнавання, а з іншого – недосконалістю методів розробки та застосування таких засобів.

Аналіз існуючих досліджень. Постановка задачі

Аналіз науково-практичних робіт, присвячених вдосконаленню систем виявлення атак (СВА) дозволяє стверджувати, що в таких системах НМ застосовуються для виявлення атак на основі узагальнення статистичних даних, відображених в навчальних прикладах [1-5, 11-13]. Крім того, можна зробити висновок, що більшість відповідних науково-практичних робіт присвячені адаптації архітектури НМ до умов поставленої задачі. Так в роботі [12] розроблено метод визначення оптимального типу архітектури НМ. Робота [11] присвячена задачам вдосконалення структури та алгоритму навчання багатошарового персептрону, призначеного для використання в СВА. Ще одним напрямком досліджень є розробка підходів до використання нових малоапробованих нейромережевих моделей. Наприклад, робота [2] присвячена засобам розпізнавання на базі кібернейрону, а в роботі [13, 14] пропонується використовувати карту Кохонена, що функціонує відповідно принципів штучних імунних систем.

Разом з тим критики використання НМ [7, 9] вказують на те, що в багатьох випадках мережева атака являє собою набір нестандартних операцій, характеристики яких не відображаються в зареєстрованих статистичних даних – навчальних прикладах. Відповідно і розпізнати новий тип мережевої атаки за допомогою НМ можливо тільки після її реалізації. Таким чином, використанню НМ заважає її суттєвий недолік – погана адаптація до нових типів мережевих атак. Наведене твердження дещо суперечливе. Наприклад, в роботі [1] запропоновано методи моделювання параметрів, які характеризують мережеву атаку. Однак традиційний підхід до використання НМ виключно в якості статистичного аналізатора, становить серйозну перепону їх подальшому впровадженню в СВА. На нашу думку виправити вказаний недолік можливо за рахунок використання в НМ експертних знань, що дозволить в першу чергу підвищити оперативність розпізнавання нових типів мережевих атак характеристики яких не представлені в навчальній вибірці, яка сформована на основі зареєстрованих статистичних даних. Крім того, розширюється множина видів мережевих атак яку може розпізнати СВА. При цьому в доступній літературі не знайдено методу подання експертних знань в НМ, призначених для використання в контурах розпізнавання систем захисту інформації, хоча в [14, 16] запропоновані відповідні загальнотеоретичні підходи.

Слід зазначити, що на сьогодні відомі різноманітні підходи до подання та використання експертних знань [8]. На початковому етапі досліджень доцільно орієнтуватись на базові методи подання. Один із таких методів базується на продукційних правилах типу [8]:

Якщо умова істина/хибна → (Висновок). (1)

Зазначимо, що продукційні правила дозволяють описати експертні знання у вигляді взаємозв'язків: «причина» → «наслідок», «явище» → «реакція», «ознака» → «факт». Крім того, застосування логічних операторів дозволяє проводити комбінування взаємозв'язків. Очевидно, що вказані взаємозв'язки та їх комбінації можуть бути використані для подання експертних знань щодо виявлення мережевих атак на основі аналізу параметрів, котрі характеризують функціонування КС. Таким чином **метою** даної статті є розробка методу подання експертних знань в нейромережевих засобах розпізнавання мережевих атак на КС за рахунок застосування продукційних правил.

Принципи застосування продукційних правил в мережі PNN

Насамперед слід відзначити, що концептуально теорія НМ об'єднує багато досить різнотипних моделей. Спільною рисою цих моделей є методологія обробки даних, яка полягає в:

– отриманні зовнішнього сигналу;

– передачі отриманого сигналу до штучних нейронів по синаптичним (зваженим) зв´язкам;

– обробці в штучному нейроні отриманого сигналу шляхом застосування активаційної функції.

При цьому кожен синаптичний зв'язок може мати свій унікальний ваговий коефіцієнт, попередньо визначений при навчанні НМ в процесі подання навчальних прикладів. Саме багатоітераційна процедура подання деяким типам НМ навчальних прикладів – статистичних даних – є підґрунтям для їх інтерпретації як аналізатора статистичної інформації. До цих типів НМ передусім відносяться: багатошаровий персептрон, карта Кохонена, машина Больцмана. Однак достатньо відомі та апробовані інші типи НМ, котрі навчаються методом «з вчителем» шляхом запам'ятовування представлених навчальних прикладів, які в певному сенсі можна вважати аналогом продукційних правил типу (1). Адже по своїй суті окремий навчальний приклад це комбінація продукційних правил:

$$Якщо\ X_1 = a_1 \wedge X_2 = a_2 \wedge \ldots \rightarrow Y\ , \quad (2)$$

де X_i – i-ий вхідний параметр, Y – очікуваний вихід НМ.

Таким чином в НМ, що навчається шляхом запам'ятовування навчальних прикладів, можливо подати експертні знання у вигляді продукційних правил. При цьому вважається [12], що з точки зору застосування в СВА серед таких мереж високий потенціал має ймовірнісна НМ (PNN – Probabilistic Neural Network). Класифікація невідомих прикладів реалізується мережею PNN на основі оцінок їх схожості з навчальними прикладами за допомогою методу Байєса [11,12]. Невідомий приклад відноситься до класу, у якого щільність розподілу в області даного прикладує найбільшою. Для оцінки щільності розподілу в області певного навчального прикладу використовується функція Гауса з центром в точці, якій відповідає даний приклад. Класична мережа PNN складається із чотирьох шарів нейронів – вхідного, образів, додавання та вихідного. Кількість нейронів вхідного шару (ВШ) дорівнює кількості контрольованих параметрів аналіз яких дозволяє розпізнати мережеву атаку. Кількість нейронів шару образів (ШО) дорівнює кількості навчальних прикладів, а кількість нейронів шару додавання (ШД) дорівнює кількості класів, які розпізнаються. ВШ та ШО складають повнозв'язну структуру, а кожен нейрон ШО пов'язаний тільки з тим нейроном ШД якому відповідає клас образу. Для зв'язків, що входять в нейрон ШО, вагові коефіцієнти встановлюються такими ж, як нормалізовані складові частини відповідного навчального прикладу. Вагові коефіцієнти зв'язків, що входять до нейронів ШД та до нейрону вихідного шару (ШВ) дорівнюють 1. Таким чином, структура і вагові коефіцієнти зв'язків мережі PNN безпосередньо визначаються навчальними даними.

Структура мережі PNN, призначеної для класифікації двох станів *A* і *B* показана на рис. 1. В цій мережі нейрони ШО з номерами від *1* до *L* відповідають навчальним прикладам, які співвідносяться з безпечним станом, а нейрони з номерами від *L+1* до *N* – співвідносяться з реалізацією мережевої атаки. Вихідний сигнал *j*-го нейрону шару образів (θ_j^o) розраховується так:

$$\theta_j^o = \sum_{i=1}^{N} \exp\left(\frac{-(w_{i,j} - x_i)^2}{2\sigma^2} \right), \qquad (3)$$

де x_i–*i*-а компонента невідомого образу, $w_{i,j}$ – ваговий коефіцієнт зв'язку між *i*-им вхідним нейроном та *j*-им нейроном шару образів, *N* – кількість компонент вхідного вектора-образу, σ – радіус функції Гауса.

У нейронах ШД використовується лінійна функція активації. Вихідний сигнал *j*-го нейрону ШД (θ_j^s) розраховується так

$$\theta_j^s = \sum_{i=1}^{N} \theta_i^o \ , \qquad (4)$$

де *N* – кількість нейронів ШО, пов'язаних з *j*-им нейроном ШД, θ_i^o – активність *i*-ого нейрону шару образів, пов'язаного з *j*-им нейроном ШД.

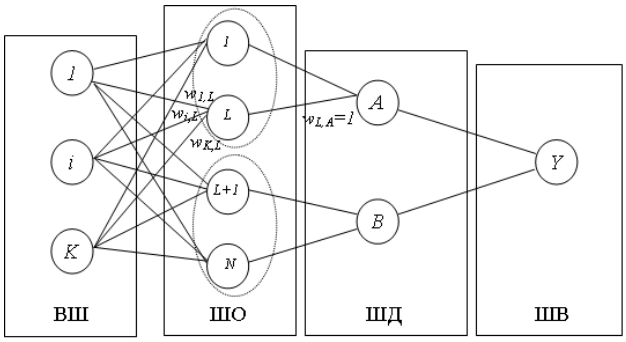


Рис. 1. Структура мережі PNN

Вихідний сигнал нейрону ШД дорівнює ймовірності віднесення вхідного образу до класу, що відповідає даному нейрону. Задачею вихідного нейрону є тільки визначення нейрону ШД з максимальною активністю. В багатьох випадках вихідний нейрон відсутній, а визначення нейрону ШД з максимальною активністю реалізують засобами, які не входять до складу нейронної мережі. Зазначимо, що відповідно [10] для підвищення ефективності процесу розрахунку вихідного сигналу мережу PNN доцільно представитив матричній формі. При цьому елементами матриць будуть вагові коефіцієнти зв'язків між сусідніми шарами нейронів. Якщо ж зв'язок між нейронами не передбачено, то вважається що його ваговий коефіцієнт дорівнює 0.

Єдиним емпіричним параметром такої моделі мережі PNN є величина радіуса функції Гауса, що використовується у виразі (3) для розрахунку вихідного сигналу нейрону ШО. При цьому в теоретичних роботах [8, 10] зазначається, що для багатьох практичних випадків в першому наближенні можна прийняти $\sigma = 1$.

В [12] описану мережу PNN пропонується використовувати для розпізнавання мережевих атак за рахунок класифікації одного із двох можливих станів КС:

A – безпечний стан;

B – небезпечний стан – реалізація мережевої атаки.

Безпечний стан співвідноситься з нейроном ШД *A*, а стан реалізації мережевої атаки – з нейроном ШД *B*.

На нейрони ВШ подають інформацію, яка відповідає нормалізованим величинам контрольованих параметрів КС, значення яких можуть сигналізувати про наявність/відсутність мережевої атаки – частота мережевих запитів, завантаженість лінії зв´язку, кількість неправильних пакетів, протокол, по якому передаються дані, завантаженість процесора, IP-адреса, з якої передаються дані і т. ін. Кількість вхідних нейронів дорівнює кількості контрольованих параметрів захищеності.

Для внесення в НМ знань про правило класифікації безпечного стану або реалізації атаки достатньо:

− визначити в ШД два нейрони А та В, котрі співвідносяться з безпечним та небезпечним станом КС;

− внести в ШО новий нейрон;

– співвіднести для нього вагові коефіцієнти вхідних зв´язків з величинами параметрів які відповідають заданому прикладу безпечного стану або реалізації атаки;

– встановити для нового нейрону вихідний зв´язок з відповідним нейроном ШД *A* або *B*.

Для прикладу на рис. 1 показано вагові коефіцієнти $w_{L,1}$, $w_{i,L}$, $w_{K,L}$ та $w_{L,A}$ за рахунок яких в мережу PNN внесено приклад *i*, який відповідає безпечному стану КС.

Розробка методу застосування продукційних правил в мережі PNN

Аналіз [1, 9, 12] відомих прикладів правил визначення безпечного/небезпечного стану КС, що застосовуються в СВА, вияв дві властивості які недостатньо враховуються в структурі та математичному забезпеченні класичної мережі PNN:

1. Кожному окремому типу мережевої атаки може відповідати одна комбінація параметрів захищеності. Тобто кількість класів, що розпізнаються, може дорівнювати кількості навчальних прикладів. Таким чином, кількість нейронів в ШД буде дорівнювати кількості нейронів в ШО. Очевидно, що в таких випадках використання ШД буде недоцільним. Вихідний сигнал від нейронів ШО може безпосередньо подаватись до нейрону ШВ. Відповідно змінена структура мережі PNN показана на рис. 2.

2. У багатьох випадках умова, яка використовується в продукційних правилах (1) має наступний вигляд:

$$p_1 \in \left[P_1^{\min}, P_1^{\max}\right] \wedge p_2 \in \left[P_2^{\min}, P_2^{\max}\right] \wedge \ldots , \qquad (5)$$

де $p_1, p_2 \ldots$ – підконтрольні параметри, $\left[P_1^{\min}, P_1^{\max}\right]$, $\left[P_2^{\min}, P_2^{\max}\right], \ldots$ – задані діапазони величин підконтрольних параметрів.

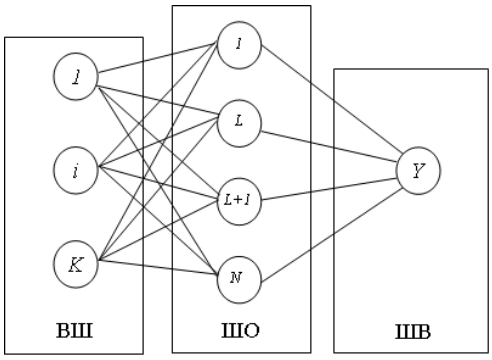


Рис. 2. Структура мережі PNN без ШД

Безпосереднє визначення такого правила в класичній моделі PNN неможливе, оскільки лінійна активаційна функція ШО не в змозі відобразити складову

$$p_i \in \left[P_i^{\min}, P_i^{\max}\right]. \qquad (6)$$

Разом з тим, умову (5) можна представити за допомогою системи вигляду:

$$\begin{cases} p_1 = P_1^{\min} \wedge p_2 = P_2^{\min} \wedge \ldots \\ p_1 = P_1^{\min} + \Delta_1 \wedge p_2 = P_2^{\min} + \Delta_2 \wedge \ldots . \\ p_1 = P_1^{\max} \wedge p_2 = P_2^{\max} \wedge \ldots \end{cases} \qquad (7)$$

де $\Delta_1, \Delta_2, \ldots$ – задані коефіцієнти.

Однак використання виразу (7) призводить до вагомого ускладнення НМ за рахунок значного збільшення кількості нейронів ШО. Можливим шляхом адаптації моделі PNN до умови (5) є введення до її складу проміжного (фільтруючого) шару нейронів, завданням якого буде фільтрація вхідного сигналу відповідно виразу (6). Вказаний фільтруючий шар (ШФ) має знаходитись між ВШ та ШО. Структура модифікованої мережі PNN, показана на рис. 3.

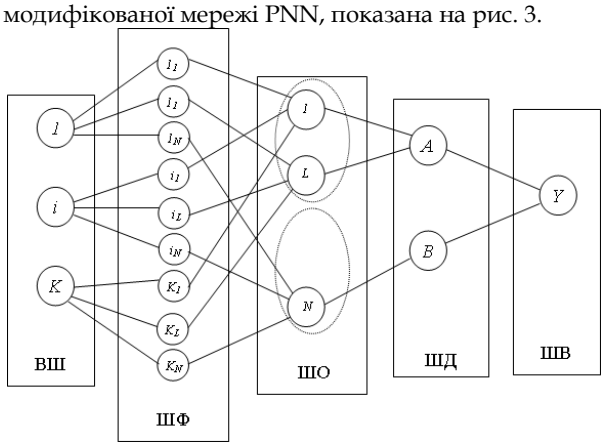


Рис. 3. Структура модифікованоїмережі PNN

Зазначимо, що кожен нейрон ВШ пов'язаний з такою кількістю нейронів ШФ, яка дорівнює кількості нейронів ШО. Прицьому кожен нейрон ШФ пов'язаний тільки з одним нейроном ШО, для якого власне і реалізується фільтрація вхідного сигналу. Для зручності нейрони ШО пронумеровані як i_L, де *i* – номер пов'язаного з ним вхідного нейрону, а *L*– номер пов'язаного х ним нейрону шару образів. Відповідно [10] для реалізації фільтру (6) в проміжних нейронах слід застосувати функцію активації вигляду

$$\begin{cases} 0 \text{ при } x \le P^{\min} \\ Kx + A \text{ при } P^{\min} \le x \le P^{\max} \\ 0 \text{ при } x \ge P^{\max} \end{cases}, \qquad (8)$$

де *K* та *A* – деякі коефіцієнти.

Ця функція отримала назву лінійної біполярної з насиченням. Графік даної функції показано на рис. 4.

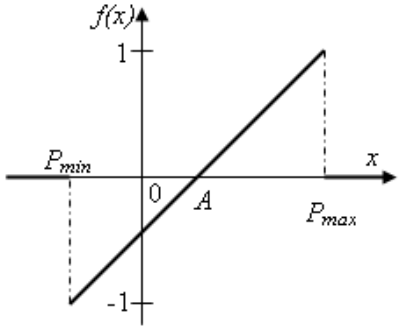


Рис. 4. Графік лінійної біполярної функції активації з насиченням

У першому наближенні можна вважати, що K=1, а A=0. Також зазначимо, що по суті нейрони ШФ в модифікованій мережі PNN відіграють роль вагових коефіцієнтів зв'язків між ВШ та ШО у класичній мережі. Тому всі вагові коефіцієнти зв'язків в модифікованій мережі PNN дорівнюють 1.

Крім адаптації структури та математичного забезпечення необхідність використання продукційних правил виду (5) призводить і домодифікації алгоритму навчання мережі:

− додати в ШО новий нейрон, який буде відповідати новому навчальному прикладу – продукційному правилу;

− в залежності від класифікації навчального прикладу встановити для нового нейрону вихідний зв´язок з відповідним нейроном ШД.

− додати в ШФ нейрони що будуть відповідно виразу (6) перетворювати сигнали, які передаються від вхідних нейронів до нового нейрону ШО;

− встановити зв'язки між новим нейроном ШО та новими нейронами ШФ;

− встановити зв'язки між новими нейронами ШФ та відповідними вхідними нейронами.

− встановити в мережі PNN всі вагові коефіцієнти рівними 1.

− співвіднести для нього вагові коефіцієнти вхідних зв´язків з величинами параметрів які відповідають заданому прикладу безпечного стану або реалізації атаки.

В підсумку узагальнений метод подання експертних знань в модифікованій мережі PNN, призначеній для розпізнавання мережевих атак на КС за рахунок застосування продукційних правил, складається з наступних етапів:

1. Використовуючи технології обробки експертної інформації [7, 8] визначити:

− множину параметрів захищеності КС.

− множину станів яку повинна розпізнавати НМ. В найпростішому випадку НМ буде розпізнавати всього два стани КС – безпечний та небезпечний.

− множину продукційних правил вигляду (1).

2. Визначити множину вхідних параметрів НМ, що співвідносяться з параметрами захищеності. При цьому можливо застосувати запропонований в [10] метод кодування параметрів захищеності до виду прийнятного НМ.

3. Визначити в ШД стільки нейронів, скільки класів повинна розпізнавати НМ.

4. Використовуючи розроблений алгоритм навчання визначити структуру та вагові коефіцієнти зв'язків.

Експериментальні дослідження

Для перевірки ефективності запропонованого методу проведено експериментальні дослідження в яких модифікована мережа PNN застосовувалась для виявлення мережевих атак.

У якості джерела статистичних даних для формування навчальної та тестової множини НМ використана база даних KDD-99, котра містить близько 5000000 записів – образів мережевих з'єднань [15]. Кожен запис складається з 42 полів. В 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. В 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). Кількість записів бази даних для кожного виду атак показано в табл. 1. Кількість записів, що відповідають відсутності атаки – 972781.

Таблиця 1

Характеристика записів бази даних KDD-99

Клас атаки	Вид атаки	Кількість записів
DoS	neptune	1072017
	smurf	2807886
	Pod	264
	teardrop	979
	land	21
	back	2203
U2R	buffer_overflow	33
	loadmodule	9
	perl	3
	rootkit	10
R2L	guess_passwd	53
	ftp_write	8
	imap	12
	phf	4
	multihop	7
	warezmaster	20
	warezclient	1020
	spy	2
Probe	portsweep	10413
	ipsweep	12481
	satan	15892
	nmap	2316

Оскільки основною передумовою застосування експертних знань в НМ є недостатня повнота навчальних даних, то основну увагу було зосереджено на розпізнаванні атак U2R, для яких кількість записів в KDD-99 найменша. Типовий приклад запису дляатаки виду buffer_overflow– *113, tcp, telnet, SF, 6274, 16771, 0, 0, 0, 5, 0, 1, 2, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0.00, 0.00, 0.00, 0.00, 1.00, 0.00, 0.00, 1, 1, 1.00, 0.00, 1.00, 0.00, 0.00, 0.00, 0.00, 0.00, buffer_overflow*, для атаки виду loadmodule– *31, tcp, telnet, SF, 142, 1278, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0.00, 0.00, 0.00, 0.00, 1.00, 0.00, 0.00, 5, 3, 0.60, 0.60, 0.20, 0.00, 0.00, 0.00, 0.00, 0.00, loadmodule*; для атаки виду perl –*54, tcp, telnet, SF, 260, 2635, 0, 0, 0, 0, 0, 1, 0, 1, 0, 2, 2, 1, 0, 0, 0, 0, 1, 1, 0.00, 0.00, 0.00, 0.00, 1.00, 0.00, 0.00, 255, 1, 0.00, 0.01, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, perl* і для атаки виду rootkit – *0, udp, other, SF, 32, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0.00, 0.00, 0.00, 0.00, 1.00, 0.00, 0.00, 255, 1, 0.00, 0.02, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00, rootkit.*

З залученням експертів в галузі захисту інформації розроблено 14 продукційних правил для розпізнавання атак вказаного типу. При цьому 4 правила стосуються розпізнавання buffer_overflow, 4 правила – loadmodule, 3 правила – perl і 3 правила – rootkit. Приклад продукційного правила для розпізнавання buffer_overflowмає наступний вигляд:

Якщо тривалість з'єднання (duration) = 0 ∧ протокол (protocol_type) – tcp ∧сервіс (service)– ftp_data ∧flag – SF ∧кількість отриманих байт (src_bytes) – 0 ∧ кількість переданих байт (dst_bytes) – від 2000 до 6000 ∧land – 0 ∧wrong_fragment – 0 iurgent – 0 ihot – 0 ∧num_failed_logins – 0 ∧logged_in =1 ∧ num_compromised= 0 ∧root_shell – від 0 до 1 ∧su_attempted= 0 ∧num_root= від 0 до 1 ∧num_file_creations – 0 ∧inum_shells= 0 ∧num_access_files= 0 ∧num_outbound_cmds – 0 ∧is_host_login= 0 ∧is_guest_login= від 1 до 3∧count= від 1 до 3 ∧srv_count= 0 ∧serror_rate= 0 ∧srv_serror_rate= 0 ∧rerror_rate= 0 ∧srv_rerror_rate= 1.00 ∧same_srv_rate= 0 ∧diff_srv_rate= 0 ∧srv_diff_host_rate= від 1 до 4 ∧dst_host_count= від 1 до 84 ∧dst_host_srv_count = 1.00 ∧ dst_host_same_srv_rate= 0.00 idst_host_diff_srv_rate= 0.00 ∧dst_host_same_src_port_rate= 1.00 ∧dst_host_srv_diff_host_rate= 0.02 ∧dst_host_serror_rate= 0 ∧dst_host_srv_serror_rate= 0 ∧dst_host_rerror_rate= 0 ∧dst_host_srv_rerror_rate= 0.

Також розроблено 14 продуційних правил для визначення нормального стану КС за відсутності атаки. Використавши вказані продукційні правила та наведений вище метод, побудовано модифіковану мережу PNN призначену для виявлення атак типу U2R. Основні параметри мережі такі: кількість вхідних параметрів мережі *K*=41, кількість нейронів ШД дорівнює 2 (нейрон А відповідає атаці, нейрон В – нормальному стану), кількість нейронів ШО дорівнює 28, а кількість нейронів ШФ дорівнює 1148, основу математичного забезпечення складають вирази (3,4,8).

Апробація розробленої нейромережевої моделі на даних KDD-99 показала абсолютну точність розпізнавання всіх видів атак класу U2R, що відповідає загальновизнаному твердженню – СВА які базуються на використанні експертних знань безпомилково розпізнають відомі атаки.

Для порівняльного аналізу запропонованого методу використано роботи [3-5], в яких наведено результати застосування різноманітних методів розпізнавання мережевих атак на сигнатурах представлених в базі даних KDD-99.

Так в роботах [4, 5] для розпізнавання атак використано багатошаровий персептрон і мережу Кохонена. В роботі [4] показано, що точність розпізнавання атак класу U2R мережею Кохонена становить: для buffer_overflow – 0.0458, для loadmodule – 0.0208, для perl – 0.2857, а для rootkit – 0.0063. При цьому багатошаровий персептрон, по причині малого обсягу навчальних даних, взагалі не вдалось навчити розпізнавати атаки типу U2R. В роботі [5] наведено дещо інші дані. Точність розпізнавання атак класу U2R мережею Кохонена становить близько 0.21.

Також в роботах [3, 5] для розпізнавання застосовано спеціальну адаптивну модель, яка базується на статистичному аналізі головних компонент. Точність розпізнавання цієї моделі не перевищує 0.5, що пояснюється не великою кількістю статистичних даних.

Порівняння результатів [3-5] з результатами представленої роботи вказує на те, що запропонований метод дозволить розширити повноту класифікації атак, сигнатури яких не достатньо представленів базах даних.

Перспективи подальших досліджень

Не зважаючи на можливості подання експертних знань, широкому застосуванню модифікованої мережі PNN заважає основний недолік – низька здатність узагальнювати навчальну інформацію. Зазначимо, що здатність НМ до узагальнення загальноприйнято оцінювати відношенням кількості синаптичних зв´язків до кількості навчальних прикладів, яку вона може безпомилково або з певною похибкою запам´ятати. Для мережі PNN одному навчальному прикладу відповідає один нейрон ШО з кількістю синаптичних зв´язків, яка на одиницю перевищує кількість вхідних параметрів. У той же час в багатошаровому персептроні з одним вихідним нейроном з такою ж кількістю синаптичних зв´язків співвідноситься 10-100 навчальних прикладів [10, 12]. Відповідно при розпізнаванні мережевих атак узагальнюючі можливості багатошарового персептрону в 10-100 вищі ніж у мережі PNN. Разом з тим PNN та багатошаровий перспетрон мають досить схожі структурні схеми та відносяться до одного класу НМ з прямими розповсюдженням сигналу.

Крім того, аналіз [10, 12] вказує на те, щоза допомогою конструктивних алгоритмів можливо створити багатошаровий перспетрон базою якого являється мережа PNN. Тому перспективною є розробка методу закладення експертних знань в багатошаровий перспетрон, призначений для розпізнавання мережевих атак.

Ще одним важливим напрямком вдосконалення запропонованого методу повинна бути його адаптація до використання експертних знань про мережеві атаки, поданих за допомогою апарату нечіткої логіки [7].

Висновки

Вище отримала подальший розвиток методологія розробки нейромережевих засобів виявлення мережевих атак, яка на відміну від відомих, застосовує продукційні правила для подання в НМ експертних знань, що дозволяє підвищити оперативність розпізнавання та розширити множину видів мережевих атак, характеристики яких не представлені в статистичних даних.

Література

[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] Артеменко А.В., Головко В.А. Анализ нейро-сетевых методов распознавания компьютерных вирусов / Материалы секционных заседаний. Молодежный инновационный форум «ИНТРИ» – 2010. — Минск: ГУ «БелИСА», 2010. — 239 с.

[3] Брюховецкий А.А. Обнаружение вредоносных программ на основе инфрмативных признаков сетевого трафика / А.А. Брюховецкий, А.В. Скатков // Тези доповідей міжнародної конференція з автоматичного управління, присвячена 100-річчю з дня народження академіка О.Г. Івахненка.

[4] Емельянова Ю.Г. Нейросетевая технология обнаружения сетевых атак на инфрмационные ресурсы / О.Г. Емельянова, Талалаев А.А., Тищенок И.П., Фраленко В.П. // Программные системы: теорія и практика – 3(7). – 2011. – С. 3-15.

[5] 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. — Том.1, №2. — 2011. — С. 156-163.

[6] Корченко О.Г. Ознаковий принцип формування класифікацій кібератак / О.Г. Корченко, С.О. Гнатюк, В.М. Кінзерявий, С.В. Казмірчук, Є.В. Паціра // Вісник Східноукраїнського національного університету імені Володимира Даля – № 4 (146) — Ч. 1, 2010. — С. 184–193.

[7] Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / А. Г. Корченко. — К. : НАУ, 2005. – 339 с.

[8] Люгер Ф. Искусственный интеллект: стратегии и методы решения сложных проблем, 4-е издание / Люгер Ф. ; пер. с англ. Н. И. Галагана — М. : Вильямс, 2003. — 864 с.

[9] Норткат С., Новак Дж.Обнаружение вторжений в сеть. /Норткат С., Новак Дж.; пер. с англ. — М.: ЛОРИ, 2001. — 384 с.

[10] Руденко О.Г. Штучні нейронні мережі. Навч. посіб. / О.Г. Руденко, Є.В. Бодянський. – Харків: ТОВ «Компанія СМІТ», 2006. — 404 с.

[11] Терейковський І.А. Вдосконалення алгоритму навчання багатошарового персептрону призначеного длярозпізнавання мережевих атак / І.А. Терейковський // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні – 2012. — Вип. 2(24). — С. 65–70.

[12] Терейковський І.Нейронні мережі в засобах захисту комп'ютерної інформації /І. Терейковський. – К. : Поліграф Консалтинг. — 2007. — 209 с.

[13] 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.

[14] Ishikawa M. Rule Extraction by Successive Regularization / Proc. 1996 IEEE ICNN, Washington, DC, USA. Vol.2. — PP.1139-1143.

[15] KDD cup 99 Intrusion detection data set [Электронный ресурс]. Электрон. текстовые данные (752 Мб). — Darpa: Irvine, CA 92697-3425, 1999. — Режим доступу: http://kdd.ics.uci.edu/databases/kddcup99/kddcup/task.html Monday, 1 March 2013 19:07:34.

[16] Sun R., Peterson T. Learning in Reactive Sequential Decision Tasks: the CLARION Model / Proc. 1996 IEEE ICNN, Washington, DC, USA. Plenary, Panel and Special Sessions Volume. — PP. 70-75.

УДК 004.8.565.5 (045)

Тарасенко В.П., Корченко А.Г., Терейковский И.А. Метод использования продукционных правил для представления экспертных знаний в нейросетевых средствах распознавания сетевых атак на компьютерные системы

Аннотация*. Использование теории искусственных нейронных сетей является одним из путей повышения эффективности функционирования систем обнаружения атак на компьютерные сети. В статье предложен метод представления экспертных знаний в нейросетевых средствах распознавания сетевых атак на компьютерные системы. Особенностью метода является использование продукционных правил и нейронной сети PNN. Полученные результаты позволяют повысить оперативность распознавания и расширить множество видов сетевых атак, характеристики которых не представлены в зарегистрированных статистических данных.*

Ключевые слова*: защита информации, сетевая атака, компьютерная система, нейронная сеть, экспертная система, продукционные правила.*

Tarasenko V.P., Korchenko O.G., Tereykovskiy I.A. Methods of presentation expertise in neural networks means of identification network attacks on computer systems

Abstract. *Theory of artificial neural networks using is one of the ways to improve the efficiency of attacks detection systems in computer networks. In this paper the method of presentation of expert knowledge in neural mass detection network attacks on computer systems. The feature of the method is the use of production rules and neural network PNN. The results can improve the efficiency of recognition and expand multiple types of network attacks, characteristics of which are registered in the statistics.*

Key words*: information security, network attack, computer system, neural network expert system production rules.*

Отримано *23 вересня 2013 року*, затверджено редколегією *16 жовтня 2013 року*