УДК 004.032.26:004.49
[1]Терейковська Л.О., [2]Іванченко Є.В., [2]Погорелов В.В.
[1]Київський національний університет будівництва і архітектури
[2]Національний авіаційний університет

МЕТОД АДАПТАЦІЇ ГЛИБОКОЇ НЕЙРОННОЇ МЕРЕЖІ ДО РОЗПІЗНАВАННЯ КОМП'ЮТЕРНИХ ВІРУСІВ

Терейковська Л.О., Іванченко Є.В., Погорелов В.В. Метод адаптації глибокої нейронної мережі до розпізнавання комп'ютерних вірусів. Аналіз науково-прикладних досліджень присвячених створенню систем захисту від шкідливого програмного забезпечення показує, що одним з найбільш перспективних напрямків розвитку систем розпізнавання шкідливих програм є удосконалення їх математичного забезпечення за рахунок застосування сучасних нейромережевих моделей на базі глибоких нейронних мереж. Також результати проведеного аналізу визначили необхідність створення методу розробки архітектури глибокої нейронної мережі, адаптованої до умов застосування в сучасних засобах розпізнавання. В ході досліджень було запропоновано метод розробки архітектури глибокої нейронної мережі, призначеної для розпізнавання шкідливого програмного забезпечення. На відміну від існуючих метод дозволяє уникнути в процесі розробки нейромережевої моделі довготривалих чисельних експериментів спрямованих на визначення доцільності її застосування та на оптимізацію її структурних параметрів. При цьому шляхом чисельних експериментів з використанням опублікованої компанією Microsoft бази даних комп'ютерних вірусів BIG-2015 показано, що метод дозволяє побудувати нейромережеву модель, яка забезпечує похибку розпізнавання, співрозмірну з похибкою сучасних систем розпізнавання комп'ютерних вірусів. Перспективи подальших досліджень пов'язані з адаптацією запропонованого методу до застосування глибоких нейронних мереж в поведінкових аналізаторах
Ключові слова: шкідливе програмне забезпечення (ШПЗ), система виявлення вторгнень, кібератака, процедура деобфусікації, метод адаптації архітектури ГНМ.

Терейковская Л.А., Иванченко Е.В., Погорелов В.В. Метод адаптации глубокой нейронной сети для распознавания компьютерных вирусов.. Анализ научно-прикладных исследований посвященных созданию систем защиты от вредоносного программного обеспечения показывает, что одним из наиболее перспективных направлений развития систем распознавания вредоносных программ является совершенствование их математического обеспечения за счет применения современных нейросетевых моделей на базе глубоких нейронных сетей. Также результаты проведенного анализа определили необходимость создания метода разработки архитектуры глубокой нейронной сети, адаптированной к условиям применения в современных средствах распознавания. В ходе исследований был предложен метод разработки архитектуры глубокой нейронной сети, предназначенной для распознавания вредоносного программного обеспечения. В отличие от существующих метод позволяет избежать в процессе разработки нейросетевой модели длительных численных экспериментов по выявлению целесообразности ее применения и на оптимизацию ее структурных параметров. При этом путем многочисленных экспериментов с использованием опубликованной компанией Microsoft базы данных компьютерных вирусов BIG-2015 показано, что метод позволяет построить нейросетевой модели, обеспечивающей погрешность распознавания, соразмерный с погрешностью современных систем распознавания компьютерных вирусов. Перспективы дальнейших исследований связаны с адаптацией предложенного метода к применению глубоких нейронных сетей в поведенческих анализаторах
Ключевые слова: вредоносное программное обеспечение (ШПЗ), система обнаружения вторжений, кибератака, процедура деобфусикации, метод адаптации архитектуры ГНС.

Tereykovskaya LO, Ivanchenko Ye.V., Pogorelov V.V. Method of adaptation of the deep neural network to the recognition of computer viruses. The analysis of scientific and applied researches devoted to creation of the systems of protection against harmful software shows that one of the most perspective directions of development of the systems of recognition of malicious software is the improvement of their mathematical support due to the application of modern neural network models on the basis of deep neural networks. The results of the analysis also identified the need to create a method for developing the architecture of deep neural network adapted to the conditions of use in modern means of recognition. In the course of research, a method for developing a deep neural network architecture designed to detect malicious software was proposed. In contrast to the existing methods, this method allows avoiding during the development of a neural network model of long-term numerical experiments aimed at determining the appropriateness of its application and optimizing its structural parameters. Through numerical experiments using computer virus database BIG-2015 published by Microsoft, it is shown that the method allows building a neural network model that provides a recognition error that is commensurate with the error of modern computer virus recognition systems. Prospects for further research are related to the adaptation of the proposed method to the application of deep neural networks in behavioural analyzers.
Key words: malware, intrusion detection system, cyberattack, deobfuscation procedure, DNN architecture adaptation method.

Вступ. На думку багатьох авторитетних дослідників, вже довгий час шкідливе програмне забезпечення (ШПЗ) є однією з найбільш небезпечних загроз сучасних комп'ютерних систем, як загального, так і спеціального призначення [1, 5, 10, 11]. Підтвердженням цього факту можуть служити відомі випадки успішних кібератак, реалізованих з використанням різних шкідливих програм [12, 15]. Хоча розробкою відповідних засобів захисту займається багато висококваліфікованих фахівців, але проблема ще далека свого рішення. Основні труднощі виникають в процесі детектування ШПЗ на стадії його проникнення в комп'ютерну систему. Для цього в сучасних системах захисту все більш широке застосування знаходять рішення з області теорії штучних нейронних мереж (ШНМ). Перспективність

вказаного напрямку підтверджується окремими вдалими застосуваннями ШНМ в засобах розпізнавання комп'ютерних вірусів (антивірус з відкритим програмним кодом ClamAV, стартап Deep Instinct) та великою кількістю відповідних теоретико-практичних робіт, огляд яких наведено в [7, 9, 16]. Разом з тим, недостатня точність розпізнавання та недостатня адаптованість до умов експлуатації, закритість використаних рішень значно обмежують сферу їх застосування.

Постановка проблеми. Постійний прогрес в області теорії нейронних мереж вказує на можливість значного вдосконалення апробованих нейромережевих засобів (НМЗ) розпізнавання ШПЗ. Цим пояснюється актуальність досліджень в області вдосконалення існуючих НМЗ, що за рахунок використання сучасних теоретичних рішень дозволили б забезпечити ефективне розпізнавання ШПЗ.

Аналіз попередніх досліджень. Основною задачею застосування ШНМ в засобах протидії ШПЗ являється розпізнавання ШПЗ на основі узагальнення контрольованих параметрів, відображених в навчальних прикладах [13, 14, 16]. При цьому процес нейромережевого розпізнавання ШПЗ, як правило полягає в нейромережеві оцінці величин множини контрольованих параметрів. Якщо виставлена за допомогою ШНМ оцінка знаходиться в певному діапазоні, то вважається, що ШПЗ розпізнано, а у випадку виходу за межі цього діапазону вважається, що в комп'ютерній системі ШПЗ відсутнє. Відповідно описаній в [9] методології розробки НМЗ захисту інформації основні напрямки підвищення ефективності таких засобів пов'язані з адаптацією виду та параметрів нейромережевої моделі (НММ) до очікуваних умов застосування, які в першу чергу визначаються використаною множиною вхідних параметрів.

Так в [2, 3] наведено опис методів визначення фрагментів програмного коду, призначених для визначення переліку та оцінки значень вхідних параметрів ШНМ, що використовуються в системах детектування ШПЗ та в системах антивірусного захисту. Для підвищення інформативності контрольованих параметрів в методі застосована процедура їх попередньої обробки. Також описано підхід до застосування НММ на базі топографічної карти Кохонена. Задекларовано, що вибір виду НММ відбувався за рахунок проведення порівняльних числових експериментів. В якості критерію порівняння використано термін навчання. В [9] наведено опис та результати експериментів в яких для розпізнавання ШПЗ було використано ШНМ на базі двохшарового персептрону. При цьому оптимізація параметрів та оптимізація процедури навчання НММ не проводилась.

В роботі [5] запропоновано підхід до визначення вхідних параметрів НММ, призначеної для розпізнавання ШПЗ на основі аналізу програмного коду. Підхід передбачає використання для деобфусикації теоретичних рішень, що використовуються для оптимізації програмного коду. Також розроблена процедура деобфускації програмного коду з використанням графа залежності значень і станів. Встановлено, що використання розробленої процедури дозволяє представити функціональну семантику тестованих програм у вигляді графа. В результаті стало можливим нейромережеве виявлення ШПЗ на основі його семантики виконання.

В [13] запропоновано систему розпізнавання комп'ютерних вірусів на основі нейромережевого аналізу нормалізованих сигнатур. Декларується точність розпізнавання в межах 80-91%. Вказується на можливість розпізнавання поліморфних вірусів. В якості базової НММ використано двохшаровий персептрон. Схожі результати отримані і в [2, 3, 7, 13] де для розпізнавання також використано двохшаровий персептрону з одним або двома вихідними нейронами. При цьому вхідні нейрони співвідносяться із параметрами, що характеризують структуру PE-файлів. Основною відмінністю між результатами [2, 3, 7, 13] є використання різних підходів до попередньої обробки вхідних параметрів ШНМ. Також в роботі [2] описані експерименти, що свідчать про точність розпізнавання комп'ютерних вірусів на рівні 91%. Використано сигнатури комп'ютерних вірусів представлені в базі даних malwr. Відзначимо, що в [2, 3, 7, 13] механізму оптимізації структури двохшарового персептрону та механізму формування навчальної вибірки не наведено. Також викликають певні сумніви у доцільності використання НММ на базі достатньо застарілих ШНМ типу двохшарового персептрону та топографічної карти Кохонена. Зазначимо, що сучасні НМЗ базуються НММ типу глибокої нейронної мережі (ГНМ) [4, 6-9].

Так в [8] використана ГНМ з переднавчанням на основі автоенкодера. Мережа складається із 8 шарів, кожен із яких містить 30 нейронів. Для отримання множини вхідних даних ГНМ використано спеціально розроблений метод автоматичної генерації сигнатур комп'ютерних вірусів. Наведено результати числових експериментів в яких точність розпізнавання досягає 98%. Разом з тим в [8] вказано, що ГНМ навчається тільки за допомогою механізму автоендкодера на не маркованих даних. Це дещо знижує достовірність отриманих результатів, оскільки вважається, що для забезпечення високої

точності розпізнавання також необхідно передбачити навчання ГНМ за допомогою алгоритму зворотного поширення помилок на маркерованих навчальних даних.

В [1] наведено опис застосування згорткових нейронних мереж (ЗНМ) для розпізнавання ШПЗ. Зазначимо, що ЗНМ є одним із різновидів ГНМ, який традиційно використовується для розпізнавання зображень. Для цього в [1] розроблено спосіб перетворення сигнатури програмного коду у сіре масштабоване зображення розміром 32х32 пікселів. Наведено описи проведених експериментів, в яких досліджувався вплив структурних параметрів ЗНМ на точність розпізнавання. Розглянуто три варіанти структурних рішень ЗНМ. Для найкращого варіанту точність розпізнавання становить 93.86%. Сформульовано пропозицію про необхідність розробки теоретичних положень щодо адаптації структурних параметрів ЗНМ до умов задачі розпізнавання ШПЗ.

Для поглиблення результатів аналізу також були розглянути науково-практичні роботи, присвячені розробці НМЗ оцінки параметрів безпеки інформаційних систем. Так, в [4] сформовано базову множину критеріїв ефективності виду НММ, що використовується для оцінки параметрів безпеки. Визначені шляхи розширення цієї множини. Також в роботі створено методологію розробки НМЗ для оцінки параметрів безпеки ресурсів інформаційних систем, що може бути використана при побудові систем розпізнавання ШПЗ. Крім того розроблено метод оцінки ефективності НМЗ розпізнавання Інтернет-орієнтованих кібератак, до складу яких також можна віднести і Інтернет-орієнтоване ШПЗ.

В [4] розроблено НММ, призначену для розпізнавання мережевих кібератак на інформаційні ресурси. Показано доцільність використання ГНМ. Це пояснюється тим, що даному виду нейромережевої моделі притаманна висока здатність до навчання, високі обчислювальні можливості та висока адаптованість до особливостей умов застосування. Наведено результати експериментів розпізнавання мережевих кібератак, сигнатури яких представлені в базі даних NSL-KDD.

В результаті проведеного аналізу можна стверджувати, що одним із найбільш перспективних напрямків підвищення ефективності систем протидії ШПЗ є застосування в них нейромережевих засобів розпізнавання на базі ГНМ. При цьому множина вхідних параметрів ГНМ залежить від особливостей системи розпізнавання. Для поведінкового аналізатора перелік може визначатись набором ознак викликів потенційно небезпечних функцій прикладного програмного інтерфейсу операційної системи. Для антивірусного сканера перелік ознак може співвідноситься із сигнатурами ШПЗ. Також можна сформувати висновок про те, що в більшості відповідних науково-практичних робіт відсутнє теоретичне обґрунтування доцільності використання ГНМ в засобах розпізнавання ШПЗ, також не наведене обґрунтування адаптації архітектурних параметрів ГНМ до очікуваних умов застосування.

Таким чином **метою** даного дослідження є забезпечення ефективності систем розпізнавання шкідливого програмного забезпечення за рахунок адаптації виду архітектури та архітектурних параметрів глибокої нейронної мережі до очікуваних умов застосування.

Результати досліджень. ***Вдосконалення методологічної бази.*** У відповідності до загальноприйнятої методології розробки НМЗ захисту інформації на першому етапі досліджень було розроблено елементи методологічної бази адаптації архітектурних параметрів ГНМ до очікуваних умов застосування.

Принцип допустимості використання виду ГНМ. Серед множини доступних *i*-ий вид ГНМ ($\mathbf{DNN}_i$) входить до множини допустимих видів ($\mathbf{DNN}_{avl}$), якщо його основні характеристики ($Q(\mathbf{DNN}_i), \tau(\mathbf{DNN}_i)$) задовольняють вимогам щодо допустимого терміну (τ_{avl}) і допустимої ресурсоємнос11ті побудови (Q_{avl}) НМЗ:

$$if\ \left(Q(\mathbf{DNN}_i) \le Q_{avl}\right) \& \left(\tau(\mathbf{DNN}_i) \le \tau_{avl}\right) \to \mathbf{DNN}_i \in \mathbf{DNN}_{avl}, \quad (1)$$

Принцип розрахунку ефективності виду ГНМ. Ефективність *i*-го виду ГНМ ($\mathbf{DNN}_i$) співвідноситься із тим наскільки даний вид ГНМ задовольняє основним функціональним вимогам, що описуються за допомогою критеріїв ефективності. Для кількісного оцінювання ефективності використовується вираз:

$$V(\mathbf{DNN}_i) = \sum_{k=1}^{K} \alpha_k \mathrm{H}_k(\mathbf{DNN}_i), \quad (2)$$

де $V(\mathbf{DNN}_i)$ - значення функції ефективності, $\mathrm{H}_k(\mathbf{DNN}_i)$ - значення *k*-го критерію для ГНМ з *i*-ою архітектурою, $\alpha_k = [0..,1]$ - ваговий коефіцієнт *k*-го критерію ефективності, *K* - кількість критеріїв.

Принцип оцінювання ефективності виду ГНМ. Серед множини допустимих *i*-ий вид ГНМ (**ГНМ**$_i$) є найбільш ефективним, якщо для нього функція ефективності (V_i) має максимальне значення:

$$\max_{V_i} = \{V_1, V_2, .. V_I\}. \quad (3)$$

Розробка наведених принципів дозволила запропонувати *модель визначення ефективних видів ГНМ*:

$$\mathbf{DNN}_{\mathbf{ent}} \rightarrow \mathbf{DNN}_{\mathbf{avl}} \rightarrow \mathbf{DNN}_{\mathbf{eff}},$$

де $\mathbf{DNN}_{\mathbf{ent}}$ - множина доступних видів ГНМ, $\mathbf{DNN}_{\mathbf{avl}}$ – множина допустимих видів ГНМ, $\mathbf{DNN}_{\mathbf{eff}}$ - множина ефективних видів ГНМ.

Базуючись на теоретичних розробках в області ШНМ визначено:

$$\mathbf{DNN}_{\mathbf{ent}} = \{dnn_1, dnn_2, dnn_3, dnn_4\};$$

де dnn_1 - повнозв'язні ГНМ, при навчанні яких процедура переднавчання не передбачена, dnn_2 - повнозв'язні ГНМ, при навчанні яких використовується процедура переднавчання, dnn_3 - ЗНМ з прямим поширенням сигналу, dnn_4 - рекурентних ЗНМ (RCN).

Визначена умова допустимості ГНМ типів dnn_1 та dnn_4:

$$if\left(20N_x\left(\vartheta_w + 0{,}2\lambda\left(N_x + N_y\right)\right) \le \tau_{avl}\right) \rightarrow \{dnn_1, dnn_4\} \in \mathbf{DNN}_{\mathbf{avl}}, \quad (4)$$

де N_x, N_y - кількість вхідних та вихідних параметрів ГНМ, ϑ_w - середній час, необхідний на створення одного навчального прикладу з очікуваним вихідним сигналом, λ – тривалість однієї навчальної ітерації.

Допустимість ГНМ типу dnn_3 визначається виразом

$$if\left(N_x\left(\vartheta_w + 0{,}2\lambda\left(N_x + N_y\right)\right) \le \tau_{avl}\right) \rightarrow dnn_3 \in \mathbf{DNN}_{\mathbf{avl}}, \quad (5)$$

Допустимість типу dnn_2 – виразом

$$if\left(22{,}2N_x\left(\vartheta_n + 0{,}01\lambda N_x\left(N_x + N_y\right)\right) + 200N_x\left(\vartheta_m + 0{,}2\lambda\left(N_x + N_y\right)\right)\right) \le \tau_{avl} \rightarrow dnn_2 \in \mathbf{DNN}_{\mathbf{avl}}, \quad (6)$$

де ϑ_n – середній час, необхідний на створення одного навчального прикладу без очікуваного вихідного сигналу.

Також використовуючи результати [4, 9] запропонована, представлена в табл. 1, множина критеріїв ефективності виду ГНМ, що співвідносяться з основними вимогами до НММ в задачі розпізнавання ШПЗ. Запропоновані критерії ефективності мають безрозмірний характер. Надалі зазначений перелік може бути змінений відповідно до конкретних умов задачі розпізнавання ШПЗ.

Таблиця 1. Критерії ефективності виду НММ

Критерій	Вимога
H_1	Можливість використання маркованих навчальних прикладів
H_2	Можливість використання не маркованих навчальних прикладів
H_3	Пристосованість до навчання
H_4	Пристосованість до навчання окремими частинами
H_5	Стабільність навчання
H_6	Мінімізація терміну навчання
H_7	Максимізація обчислювальної потужності
H_8	Можливість врахування топології аналізуємих даних
H_9	Максимізація швидкості прийняття рішення
H_{10}	Пристосованість до аналізу динамічних рядів даних

За аналогією з [4, 9] прийнято, що значення запропонованих критеріїв можуть зміняться в межах від 0 до 1. При цьому для *i*-ої архітектури ГНМ значення *k*-го критерію дорівнює 1, якщо відповідна *k*-та вимога повністю забезпечується в даній архітектурі, і дорівнює 0, якщо не забезпечується.

Розраховані значення критеріїв для ГНМ, що входять до складу наведені в табл. 2.

Таблиця 2. Значення критеріїв ефективності для апробованих видів ГНМ

Критерій	$ГНМ_1$	$ГНМ_2$	$ГНМ_3$	$ГНМ_4$
H_1	1	1	1	1
H_2	0	1	0	0
H_3	0	1	0	0
H_4	0	1	0	0
H_5	1	0,5	1	0,5
H_6	1	0,5	0,5	0,5
H_7	1	0,5	0,5	0,5
H_8	0	0	1	1
H_9	1	1	1	1
H_{10}	0	0	0	0,5

Метод адаптації архітектури ГНМ. Інтеграція загальноприйнятої методології розробки нейромережевих засобів захисту інформації з розробленими принципами, критеріями та моделлю визначення ефективних видів ГНМ дозволила запропонувати метод адаптації архітектури ГНМ до умов задачі розпізнавання ШПЗ, що складається із 5 етапів.

Крок 1. Формалізація умов задачі розпізнавання з метою отримання числових значень параметрів, що використовуються в розрахункових виразах (1-6).

Крок 2. Визначення доцільності використання нейромережевої моделі типу ГНМ. Для цього слід використати математичне забезпечення представлене виразами (1, 4-6).

Крок 3. Визначення значущості кожного із критеріїв ефективності, представлених в табл. 2.

Крок 4. Визначення за допомогою виразів (2, 3) найбільш ефективного виду архітектури НММ типу ГНМ.

Крок 5. Визначення параметрів архітектури найбільш ефективного виду. В базовому варіанті для визначення параметрів повнозв'язних ГНМ доцільно використовувати результати [9, 16], а для визначення параметрів CNN та RCN - результати [14, 15].

Вхідними даними методу являються параметри, що характеризуються очікувані умови застосування ГНМ в засобах розпізнавання ВОП, а виходом – вид та параметри архітектури ГНМ.

Розглянемо використання запропонованого методу на конкретному прикладі адаптації архітектури ГНМ до наступних умов застосування:

- система розпізнавання орієнтована на загально розповсюджене апаратно-програмне забезпечення;

- НММ використовується для розпізнавання Windows-орієнтованих комп'ютерних вірусів на основі аналізу використаних програмою потенційно небезпечних API-функцій операційної системи;
- на вхід НММ подається інформація, отримана в результаті сканування піддослідних файлів;
- допустимий термін створення НМЗ складає 1 місяць (2592000 с);
- для навчання та тестування НММ використовується опублікована компанією Microsoft база даних комп'ютерних вірусів BIG- 2015.

Зазначимо, що в БД BIG-2015 представлено приклади сигнатур 9 комп'ютерних вірусів, характеристики яких наведено в табл. 3. Загальна кількість прикладів становить 10868.

Таблиця 3. Характеристика БД BIG-2015

Назва вірусу	Кількість навчальних прикладів	Тип вірусу (класифікація компанії Microsoft)
Ramnit	1541	Worm
Lollipop	2478	Adware
Kelihos_ ver3	2942	Backdoor
Vundo	475	Trojan
Simda	42	Backdoor
Tracur	751	TrojanDownloader
Kelihos_ ver1	398	Backdoor
Obfuscat or.ACY	1228	Any kind of obfuscated malware
Gatak	1013	Backdoor

БД BIG-2015 сформована за допомогою програмного комплексу Interactive DisAssembler, що дозволяє вилучити із бінарного файлу метадані які стосуються інструкцій мови Assembler, вміст регістрів та дані і функції, імпортовані із DLL. При цьому застосування до дизасембльованого коду технології Flirt дозволяє визначити наявність в ньому потенційно небезпечних функцій управління розділами, управління файлами, роботи з реєстром, використання системної інформації, використання мережевих з'єднань, управління пам'яттю, використання сервісів, управління системою захисту об'єктів. В якості прикладу можна навести функцію DeleteFile, що може бути використана для нанесення шкоди файловій системі операційної системи Windows. Наведений в [5, 9] перелік таких функцій в першому наближенні становить 300 найменувань. Окреслення умов застосування дозволило перейти до реалізації методу розробки ГНМ.

Крок 1. Оскільки для формування навчальної вибірки передбачається використання доступних баз даних, то при оціночних розрахунках можна вважати, що навчальні приклади вже сформовані. Тобто $\vartheta_w = \vartheta_n = 0$. При цьому τ_{avl}=2592000 с, а розраховано, що кількість навчальних прикладів становить БД P=10868. Передбачено, що вхідні параметри НММ співвідносяться з множиною всіх потенційно небезпечних функцій операційної системи Windows, а вихідні параметрів співвідносяться з назвами вірусів представлених в БД BIG-2015 та безпечним програмним забезпеченням. Таким чином $N_x = 300$, а $N_y = 9$. Також шляхом експертного оцінювання визначено, що при використанні загальнодоступного апаратно-програмного забезпечення тривалість однієї навчальної ітерації не перевищує 0,01 с. Тобто $\lambda = 0,01\ c$.

Крок 2. Підставивши отримані значення N_x, N_y, ϑ_w ϑ_n та λ в вирази (1, 4-6) отримано $\tau(dnn_1, dnn_4) = 3708\ c$, $\tau(dnn_3) = 185\ c$, $\tau(dnn_2) = 98818\ c$. Оскільки ці всі величини менші ніж τ_{avl}, то можливо вважати, що доцільність використання всіх видів ГНМ доведена.

Крок 3. Оцінка значущості кожного з критеріїв ефективності, представлених в табл. 2, була реалізована за допомогою експертного методу парного порівняння. Отримані результати показані в табл. 4.

Таблиця 4. Вагові коефіцієнти критеріїв ефективності виду ГНМ

□1	□2	□3	□4	□5	□6	□7	□8	□9	□10
0,1	0,02	0,03	0,02	0,2	0,15	0,2	0,15	0,1	0,03

Крок 4. Підставивши для кожного доступного виду ГНМ дані табл.4 в вираз (3) отримано: $V(ГНМ_1)$=0,75, $V(ГНМ_2)$=0,535, $V(ГНМ_3)$=0,725, $V(ГНМ_4)$=0,64. З використанням виразу (4) визначено, що найбільш ефективним видом є $ГНМ_1$.

Крок 5. При відомих значенням N_x та N_y, основними архітектурними параметрами $ГНМ_1$ є кількість схованих нейронних шарів, кількість нейронів у кожному схованому шарі та вид функції активації. З позицій спрощення архітектури в якості базового варіанту $ГНМ_1$ було обрано трьохшаровий персептрон в якому кількість схованих шарів K_h =2.

Відповідно рекомендацій [4, 9] архітектурні параметри такої ГНМ визначаються наступними виразами:

$$N_h = Round\left(\frac{\sqrt{P \times N_x}}{N_y \times K_h}\right), \qquad (7)$$

$$f(z_k) = \max(0, z_k),$$

де N_h - кількість нейронів в кожному із схованих шарів, K_h - кількість схованих шарів, $f(z_k)$ - функція активації нейронів схованого та вихідного шару, де z_k – сумарний вхідний сигнал k-го нейрону в схованому або вихідному шарі.

Підставивши в вираз (7) відомі значення P, N_x,N_y та K_h отримано, що N_h=135.

Визначення архітектурних параметрів дозволило перейти до розробки відповідного програмного забезпечення. Для цього використано мову програмування Python та бібліотеку TensorFlow (розробка компанії Google). Експерименти проводились на персональному комп'ютері (AMD FX-9800P (2.7 - 3.6 ГГц) / RAM 8 ГБ / HDD 1 ТБ / AMD Radeon RX 540, 2 ГБ), що функціонував під управлінням операційної системи Windows 10.

Навчання проводилось на протязі 100 епох. Приблизно після 90 навчальних епох помилка навчання стабілізувалась на рівні 0.01. Після цього на вхід ГНМ із БД BIG-2015 були подані тестові приклади, що не використовувались при навчанні. Похибка розпізнавання для різних вірусів показана на рис. 1.

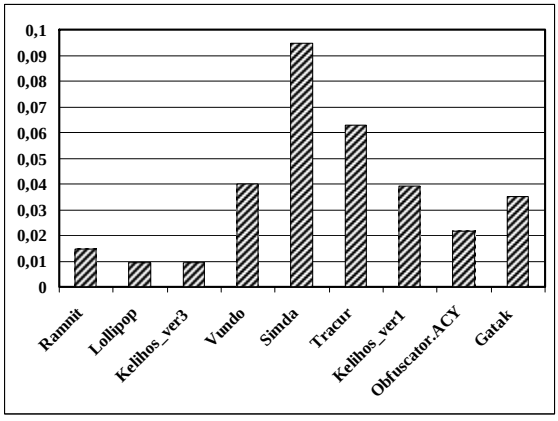

Рис. 1. Похибка розпізнавання на тестовій виборці

Аналіз рис. 2 вказує на те, що найбільша похибка розпізнавання характерна для вірусів Simda, Tracur та Vundo. Це можна пояснити невеликою кількістю навчальних прикладів, що відповідають цим вірусам. При цьому середня похибка розпізнавання всіх видів вірусів дорівнює 0,036. Також слід зазначити, що за рахунок використання запропонованого методу при розробці НМ вдалось уникнути довготривалих чисельних експериментів спрямованих на визначення доцільності її використання та на оптимізацію її структурних параметрів. Враховуючи, що досягнута похибка розпізнавання відповідає похибці сучасних антивірусних засобів [1, 2, 5, 7, 11, 12], це свідчить про ефективність запропонованих рішень.

Висновки. Показано, що одним з найбільш перспективних напрямків розвитку систем розпізнавання шкідливих програм є удосконалення їх математичного забезпечення за рахунок

застосування сучасних нейромережевих моделей на базі глибоких нейронних мереж. Визначено необхідність створення методу розробки такої моделі, адаптованої до умов застосування в антивірусних засобах. Запропоновано метод розробки архітектури глибокої нейронної мережі, призначеної для розпізнавання шкідливого програмного забезпечення. На відміну від існуючих метод дозволяє уникнути в процесі розробки нейромережевої моделі довготривалих чисельних експериментів спрямованих на визначення доцільності її застосування та на оптимізацію її структурних параметрів. При цьому шляхом чисельних експериментів з використанням опублікованої компанією Microsoft бази даних комп'ютерних вірусів BIG-2015 показано, що метод дозволяє побудувати нейромережеву модель, яка забезпечує похибку розпізнавання, співрозмірну з похибкою сучасних систем розпізнавання комп'ютерних вірусів. Перспективи подальших досліджень пов'язані з адаптацією запропонованого методу до застосування глибоких нейронних мереж в поведінкових аналізаторах.

1. Sujyothi A., Acharya S. Dynamic Malware Analysis and Detection in Virtual Environment / A. Sujyothi, S. Acharya // International Journal of Modern Education and Computer Science. – 2017. – Vol. 9. – No. 3. – P. 48. doi: 10.5815/ijmecs.2017.03.06.
2. Артеменко А., Головко В. Анализ нейросетевых методов распознавания компьютерных вирусов / А. Артеменко, В. Головко // Молодежный инновационный форум «ИНТРИ. – 2010. Минск: ГУ «БелИСА». – 239 с.
3. Оценка точности алгоритма распознавания вредоносных программ на основе поиска аномалий в работе процессов / М. В. Баклановский, А.Р., Ханов, К.М. Комаров [и др]. //Научно-технический вестник информационных технологий, механики и оптики. – 2016. – Т. 16. – №. 5. – С. 823–830.
4. Deep neural networks in cyber attack detection systems / Bapiyev I. M. B.H. Aitchanov, I.A. Tereikovskyi [et al.] //International Journal of Civil Engineering and Technology (IJCIET). – 2017. – Vol. 8. – No. 11. – P. 1086-1092.
5. Deobfuscation of Computer Virus Malware Code with Value State Dependence Graph / I. Dychka, I. Tereikovskyi, L. Tereikovska [et al.] // International Conference on Theory and Applications of Fuzzy Systems and Soft Computing. – Springer, Cham, 2018. – P. 370-379.
6. Parametric equation for capturing dynamics of cyber attack malware transmission with mitigation on computer network / A Falaye Adeyinka, E. S. Oluyemi, N. V. Adama [et al.] // International Journal of Mathematical Sciences and Computing (IJMSC). – 2017. – Vol. 3. – No.4. – P. 37-51.
7. Virus detection using artificial neural networks / Shah S., H. Jani, S. Shetty [et al.] //International Journal of Computer Applications. – 2013. – Vol. 84. – No. 5. – P. 17–23.
8. Киселевская А. Ю. Глубокие нейронные сети: автоматическое обучение распознаванию вредоносных программам. Генерация и классификация подписей / А. Ю. Киселевская // Молодой ученый. – 2017. – №. 47(181). – С. 15-18.
9. Neyrosetevye modeli, metody i sredstva otsenki parametrov bezopasnosti Internet-oriyentirovIIIHMykh informatsionnykh system / A. Korchenko, I. Tereykovskiy, N. Karpinskiy [et al.]. Kiev: TOV «Nash Format», 2016. – 275 p.
10. Development of the intelligent decision-making support system to manage cyber protection at the object of informatization / V. Lakhno,Y. Boiko, A. Mishchenko, V. Kozlovskii, [et al.] // Eastern-European Journal of Enterprise Technologies. – 2017. – Vol. 2, Iss. 9 (86). – P. 53–61.
11. Lakhno V. Creation of the adaptive cyber threat detection system on the basis of fuzzy feature clustering / V. Lakhno // Eastern-European Journal of Enterprise Technologies. – 2016. – Vol. 2, Iss. 9 (80). – P. 18–25.
12. Novel feature extraction, selection and fusion for effective malware family classification / M. Ahmadi, D. Ulyanov, S. Semenov [et al.] // Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy. – New York : ACM, 2016. – P. 183-194.
13. Omotayo F. A. Dlamini and Jonathan M. Blackledge Asiru. Application of Artificial Intelligence for Detecting Derived Viruses / F. A. Omotayo, T. Moses // 16th European Conference on Cyber Warfare and Security (ECCWS 2017) (Dublin 2017 June 29-30). – University College Dublin. – P. 217-227.
14. Rudenko O.H., Bodianskyi Ye. Shtuchni neironni merezhi. – Kharkiv : «Kompaniia SMIT», 2016. – 404 p.
15. Encoding of neural network model exit signal, that is devoted for distinction of graphical images in biometric authenticate systems / L.Tereykovska, I.Tereykovskiy, E. Aytkhozhaeva // News of the National Academy of Sciences of the Republic of Kazakhstan, Series of Geology and Technical Sciences. – 2017, Vol. 6, No. 426, P. 217 – 224.
16. Determination of structural parameters of multilayer perceptron designed to estimate parameters of technical systems / Z. Hu, I. A. Tereykovskiy, L. O. Tereykovska [et al.] // International Journal of Intelligent Systems and Applications. – 2017. – Vol 9. – No.10.P.57-62