УДК 681.3.06

СУЧАСНІ НЕЙРОМЕРЕЖЕВІ МЕТОДИ ТА МОДЕЛІ ОЦІНКИ ПАРАМЕТРІВ БЕЗПЕКИ РЕСУРСІВ ІНФОРМАЦІЙНИХ СИСТЕМ

Олександр Корченко, Ігор Терейковський, Андрій Дзюбаненко

Одною із основних перешкод широкому впровадженню нейромережевих методів та моделей в системах виявлення кібератак та в системах виявлення вразливостей ресурсів інформаційних систем є відсутність параметрів на основі яких можливо оцінити їх ефективності. Також відсутні і методи оцінки ефективності такого впровадження. Для вирішення цієї проблеми був проаналізований широкий спектр сучасних нейромережевих методів та моделей, що застосовуються у зазначених системах виявлення. Визначено перелік параметрів і розроблено метод їх використання для оцінки ефективності розробки та вибору вказаних методів та моделей при побудові означених систем виявлення. Отримані результати дозволяють визначити недоліки сучасних нейромережевих засобів виявлення кібератак та засобів виявлення вразливостей і окреслити перспективні шляхи їх вдосконалення.

***Ключові слова**: безпека інформації, виявлення кібератак, інформаційна система, нейромережеві модель, нейромережевих метод, параметр безпеки.*

Вступ. В теперішній час створення перспективних систем забезпечення інформаційної безпеки (ІБ) ресурсів інформаційних систем (РІС) асоціюється з використанням інтелектуальних засобів, що функціонують з використанням методів та моделей теорії нейронних мереж (НМ). Відповідно до результатів [1-4, 9, 13, 19, 27] нейромережеві методи та моделі в основному використовуються для виявлення (розпізнавання) кібератак та вразливостей РІС. Крім того, НМ використовуються для управління параметрами захисту. Перспективність використання нейромережевих методів та моделей підтверджується окремими вдалими застосуваннями НМ в системах виявлення кібератак (СВК) (продукція компанії Cisco) та великою кількістю відповідних теоретико-практичних робіт, огляд яких наведено в [1, 2, 21]. Разом з тим велика кількість хибних спрацювань, довготривалий термін та нестабільність навчання, недостатня адаптація до багатьох особливостей сучасного стану РІС значно обмежують їх практичну цінність. Тому в сучасних умовах гостро стоїть проблема обґрунтованої оцінки ефективності застосування нейромережевих методів та моделей в СВК та в системах виявлення вразливостей (СВВ). Проблема ускладнюється тим, що аналіз [1-25, 27] вказує на відсутність в теперішній час базового набору параметрів, використання яких дозволило б хоча б в першому наближенні визначити ефективність застосування нейромережевого інструментарію в СВК та СВВ. В зв'язку з цим, метою даної статті є визначення базового набору параметрів та методу їх використання для оцінки ефективності застосування сучасних нейромережевих моделей та методів в СВК та СВВ.

Основна часина дослідження. Результати [1, 2, 13, 21] дозволяють стверджувати, що виявлення (розпізнавання) кібератак та вразливостей РІС за допомогою НМ в основному зводиться до оцінок величин параметрів безпеки РІС. Якщо виставлена за допомогою НМ оцінка перевищує певне граничне значення, то вважається, що кібератака (вразливість) виявлені. В протилежному випадку вважається, що рівень безпеки знаходиться в допустимих межах. При цьому, по аналогії з загальновідомим терміном діагностичний параметр, під терміном параметр безпеки РІС будемо розуміти фізичну величину, що характеризує стан забезпечення конфіденційності, цілісності та доступності інформації РІС, а під терміном кібератаки (кібернетичної атаки) на РІС будемо розуміти реалізацію у кібернетичному просторі загроз безпеці його компонентів (а саме конфіденційності, цілісності та доступності) з урахуванням їх вразливостей. Зазначимо, що відповідно [26] кібернетичний простір – це 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 інформаційних ресурсів) з метою забезпечення інформаційних потреб суспільства. Відповідно до визначеної мети, з використанням наведеного терміну кібератака та запропонованого терміну параметр безпеки, проведено аналіз нейромережевих методів та моделей виявлення кібератак та виявлення вразливостей РІС. Зазначимо, що в більшості проаналізованих робіт [1-16, 18, 19, 21-29] є певна невідповідність термінологічного аспекту описаної розробки: нейромережевий метод, модель, система, технологія, засіб. Як правило, наводить-

ся комплексний опис розробки, хоча назва роботи вказує, наприклад, на створення нейромережевої моделі. Тому аналіз цих робіт проведено з єдиних позицій визначення основних характеристик нейромережевих методів та моделей. Наведемо отримані дані.

Методи простої та семантичної класифікації мережевих атак. Методи розроблено в межах нейромережевої технології виявлення мережевих комп'ютерних атак за допомогою програмного комплексу «Snort», описаної в роботі [6]. Технологія передбачає застосування двох нейромережевих методів виявлення атак – **простої класифікації** (**ПСК**) та **семантичної класифікації** (**ССК**). В якості вхідних параметрів використовуються параметри мережевих пакетів транспортного рівня стуку протоколів TCP/IP. В методі ПСК використано багатошаровий персептрон (БШП) з 10 вхідними нейронами та 2 нейронами у вихідному шарі. Для оптимізації кількості схованих нейронів пропонується застосування так званих «конструктивних алгоритмів». Наведено математичний вираз для розрахунку корекції вагових коефіцієнтів нейронів вихідного шару

$$\Delta w_{jk}(i) = -\eta(y_n(i) - f(x_i))\phi'(v_n(i))y_n,$$

де η – коефіцієнт швидкості навчання, n – номер нейрону у вихідному шарі, i – номер навчальної ітерації, v_n – інформаційне поле, отримане на вході функції активації, y_n – вихідний сигнал n-го вихідного нейрону, ϕ' – похідна функції активації, $f(x_i)$ – бажаний відгук і-го нейрону.

Зазначимо відсутність детального опису процесу оптимізації структури БШП. В методі ССК пропонується використання топографічної карти Кохонена (ТК). Вибір ТК обґрунтовується її невисокою ресурсоємністю. В обох методах передбачена методика обробки вхідних параметрів з метою зменшення кількості вхідних параметрів НМ.

Метод нейромережевої фільтрації спаму (**НФС**), наведений в роботі [25]. Доводиться оптимальність використання адитивних НМ (АНМ). Тип нейромережевої архітектури обрано з позицій максимізації точності розпізнавання, можливості автоматизації навчання та можливості представлення результатів в графічному вигляді. Тобто використано процедуру багатокритеріальної оптимізації процесу визначення архітектури НМ. В якості вхідних параметрів нейромережевої моделі використано частоти зустрічі в спамі та в цільових електронних листах інформативних слів. Також запропонована процедура багатокритеріальної оптимізації параметрів нейромережевої моделі, в якій використано критерії максимізації обчислювальної потужності та мінімізації терміну навчання.

Метод визначення фрагментів програмного коду (**ВФПК**), описаний в роботі [24]. Метод застосовується для визначення переліку та оцінки значень вхідних параметрів НМ, що використовуються в системах детектування шкідливого програмного забезпечення. Також в роботі [24] наведено опис та результати експериментів по розпізнаванню шкідливого програмного забезпечення, проведених за допомогою НМ типу БШП. Аналіз наведених результатів підтверджує перспективність запропонованого методу. Можна зробити висновок про використання в методі процедури попередньої обробки вхідних параметрів НМ, яка підвищує їх інформативність.

Нейромережева системи виявлення вторгнень (**НСВВ**), описана в роботі [27]. Система орієнтована на використання НМ типу БШП для розпізнавання мережевих атак. Наведено результати експериментів, що підтверджують ефективність системи при розпізнаванні атак, сигнатури яких представлені в базі KDD-99. Вибір типу НМ обґрунтовано з позицій максимальної обчислювальної потужності. Також проведена однокритеріальна оптимізація архітектури БШП.

Нейромережевих підхід виявлення SQL-ін'єкцій (**НПВІ**) представлений роботі [29]. Запропоновано розглядати проблему визначення зловмисних SQL-запитів у вигляді проблеми прогнозування часових рядів. Відповідно вказаній пропозиції пропонується використати рекурентні НМ типу Джордана (НМД) та Елмана (НМЕ). Тобто тип НМ обрано відповідно критерію апробованості в задачах прогнозування часових рядів. Також наведено процедуру попередньої обробки вхідних параметрів та процедуру однокритеріальної оптимізації структури НМ. Використано критерій максимізації обчислювальної потужності. Наведені результати експериментальних досліджень, котрі були проведені на основі даних порталу Php-Nuke, підтверджують перспективність запропонованого підходу.

Бінарний нейромережевих метод (**БНМ**), описаний в роботі [15]. Метод застосовується для вирішення задачі виявлення мережевих атак. В основі методу лежить спеціальна бінарна нейронна мережа (БНМ), яка має дві важливі властивості. По-перше, модель пристосована для вирішення завдань, у яких вхідна інформація має складну, багатозв'язкову і навіть фрактальну стру-

ктуру. По-друге, метод навчання моделі є прямою обчислювальною процедурою і не зводиться до пошуку глобального екстремуму складної нелінійної функції, що не накладає ніяких принципових обмежень на розмірність завдання. Таким чином в методі передбачено вибір типу нейромережевої архітектури по критерію апробованості в задачах певного типу та по критерію мінімізації тривалості навчання. На жаль, в роботі відсутні експериментальні дані, що ускладнює порівняльний аналіз. В методі не передбачено проводити оптимізацію структури НМ, застосування та процедури обробки вхідних даних.

Метод виділення мережевих атак із типового мережевого трафіку (**ВМА**), описаний в роботі [14]. Метод застосовується для розпізнавання мережевих атак. Запропоновано застосування БШП з 2 схованими шарами нейронів. Вхідний шар такого БШП складається із 9 нейронів, а вихідний шар – із 1 нейрону. Зазначено, що вибір БШП з такою структурою пояснюється вимогами гнучкості та функціональності. Тобто використано багатокритеріальну оптимізацію структури НМ. Вказано на попередню обробку статистики, що використовувалась для навчальної та тестової вибірки.

Спосіб виявлення DDoS-атак (**СВДА**), наведений в роботі [18]. Запропоновано використання нечітких НМ (ННМ). Пропозиція ґрунтується на перспективності НМ такого типу. Акцент ставить на розпізнаванні DDoS-атаки типу SYN Flood. Для формалізації знань експертів про DDoS-атаки було створено 5 лінгвістичних змінних, кожна з яких характеризує одну з компонент вектора параметрів мережевого трафіку, що використовується для формування вхідних параметрів НМ. До вказаних лінгвістичних змінних відносяться: X_1 – час отримання пакетів, X_2 – процент пакетів з різних зовнішніх IP-адрес, X_3 – процент пакетів з різних портів, X_4 – процент пакетів з пошкодженими заголовками, S – степінь впевненості. Розроблено предикатні правила виду: Якщо $X_1 =$ «великий»$\rightarrow$ $Y \rightarrow$ «висока». Структура класифікатора показана на рис. 2.

На рис. 2 символом позначено нечіткий нейрон «АБО», символом – нечіткий нейрон «І», а позначення tLittle, tMiddle, tHigh, extraLittle, extraLots, pLittle, pLots, dhLots відповідають функціям активації нечітких змінних. Запропоновано представити нечіткий класифікатор у вигляді НМ з прямим розповсюдженням сигналу, що навчається за допомогою модифікованого алгоритму зворотнього розповсюдження помилки. Модифікація полягає у пристосуванні класичного алгоритму до нечітких нейронів «І» та «АБО». Таким чином, основною відмінністю запропонованого способу виявлення є можливість застосування для навчання НМ експертних знань.

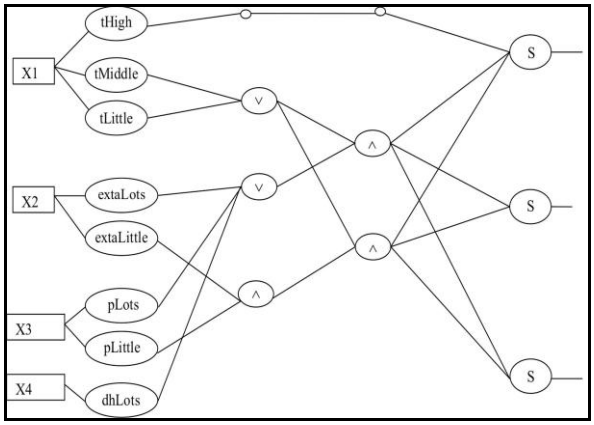

Рис. 2. Схема нечіткого класифікатора для виявлення SYN Flood-атак

Метод використання нейронної мережі гібридної структури типу CounterPropagation (**НМГС**), описаний в роботах [5, 21]. Метод призначено для виявлення мережевих атак на Вебсервер. Особливістю мережі CounterPropagation є комбінація ТК з БШП. Вхідними даними методу є параметри мережевого трафіку, що передається по протоколам IP, TCP, HTTP, HTTPS, CGI, SQLNet. В методі передбачена процедура попередньої обробки вхідних параметрів НМ за рахунок представлення їх у вигляді графічних образів (піфограм), котрі використовуються в когнітивній графіці. Метою попередньої обробки є мінімізація розмірності вхідних даних. Графічне представлення визначило необхідність застосування в методі шару Кохонена. Використання персептронного шару обґрунтоване з позицій обчислювальної ефективності. Таким чином в методом передбачено багатокритеріальну оптимізацію типу НМ та однокритеріальна оптимізація параметрів її архітектури. Також в методі передбачена процедура пошуку оптимальних параметрів навчання НМ, яка дозволяє до 10 разів зменшити величину помилки розпізнавання атак.

Метод побудови сукупного класифікатора трафіку (**ПСКТ**), запропонований в роботі [11]. Метод призначений для ієрархічної класифікації комп'ютерних атак на інформаційно-телекомунікаційні мережі. Особливістю даного методу є використання математичного методу головних компонент для стиснення статистичних даних, що використовуються в якості навчальної вибірки НМ. В методі використано об'єднання з

22 нейромережевих детекторів, кожен із яких навчений розпізнавати певний тип атаки, наведений в базі даних KDD-99. Детектор представляє собою трьохшарову НМ з 12 вхідними нейронами та 2 вихідними нейронами, один із яких відповідає за наявність, а другий за відсутність атаки. В якості схованого шару використано шар Кохонена. Зазначимо, що обґрунтування архітектури та параметрів нейромережевого детектора не наведено. При виявленні детектором атаки вихід першого вихідного нейрону дорівнює 1. Для унеможливлення ситуації, коли декілька детекторів одночасно сигналізують про власний тип атаки, на другий вихід кожного з них передається мінімальна евклідова відстань між вхідним образом (вхідними параметрами – x_i) і ваговими коефіцієнтами схованих нейронів ($w_{i,j}$):

$$E_j = \min_i \sqrt{\left(x_1 - w_{1,j}\right)^2 + ...\left(x_{12} - w_{12,j}\right)^2}\ .$$

Надалі класифікується та атака, детектор якої має мінімальну евклідову відстань. В методі ПСКТ також в неявному вигляді передбачено оптимізацію навчання та функціонування нейромережевого детектора.

Нейромережевий підхід до виявлення мережевих атак (**ПВМА**) на комп'ютерні системи, наведено в роботі [12]. Акцент ставиться на розпізнавання атак, сигнатури яких представлені в БД KDD-99. Відповідно даних цієї БД кількість вхідних параметрів – 41. Запропоновано використовувати критерій вибору оптимального типу нейромержевої моделі у вигляді мінімуму обсягу навчальної вибірки. Шляхом аналізу літературних джерел визначено, що до допустимих типів відносяться: ТК, БШП з одним схованим шаром нейронів та мережа радіальної базисної функції (РБФ). Зазначено, що для ТК мінімальний обсяг навчальної вибірки (L) повинен в 2 рази перевищувати кількість вхідних нейронів (n). Тобто $L \geq 2n$. Для БШП та РБФ обсяг навчальної вибірки розраховується так $L \approx W / \varepsilon$, де W – кількість синоптичних зв'язків, ε – допустима помилка навчання. Надалі в [12] зроблена спроба визначити оптимальну структуру БШП. Заявлено, що визначена експериментальним шляхом кількість схованих нейронів дорівнює $m = 10$. При цьому кількість вихідних нейронів дорівнює 2. Відповідно, необхідний обсяг навчальної вибірки ТК складає $L = 82$ приклади, а для БШП та РБФ при $\varepsilon = 0{,}1$, $L = (m(n+3)+2)/\varepsilon = 4420$. Тому оптимальним типом нейромережевої моделі обрано ТК. Зазначимо, що правильність розрахованих величин викликає сумніви, адже відповідно теорії НМ [17] при заданій точності навчання, кількість схованих нейронів БШП безпосередньо залежить від величини навальної вибірки. Надалі в [12] проводиться оптимізація структури ТК. Неявно використано критерій максимізації точності навчання. Також використано аналогічна [12], процедура попередньої обробки вхідних параметрів.

Адаптивна система виявлення атак (**АСВА**), описана в роботі [19]. Система призначена для розпізнавання мережевих атак та базується на спільній роботі ТК і БШП, що виконують завдання кластеризації і класифікації даних. Виявлення атак, котре проводиться в декілька етапів, стало можливим завдяки тому, що в базу даних експертної системи вносилася інформація про зміни в поведінці конкретного об'єкта на протязі деякого відрізка часу. Доводиться, що оптимізація архітектури дозволить підвищити точність та оперативність розпізнавання. В якості вхідних даних використано параметри мережевого трафіку по протоколу TCP. Для обробки вхідних даних використано метод ковзаючого часового вікна. ТК використана для попередньої обробки даних, що поступають на вхід БШП з метою їх стиснення та підвищення інформативності. Наведено математичний вираз для розрахунку частоти визначення нейрону в позиції (i,j) в якості нейрону-переможця:

$$\beta_{i,j} = f_{i,j} + \sum_{x=1}^{r}\left(\frac{f_{i-x,j} + f_{i,j-x} + f_{i+x,j} + f_{i,j+x}}{1+x}\right),$$

де $f_{i,j}$ – кількість разів, коли нейрон в позиції (i,j) був нейроном-переможцем, r – відстань між центрами кластерів, x – довжина вхідного вектора.

Надалі ця частота використовується для визначення центрів та границь кластерів. Структура БШП оптимізована з точки зору обсягу контрольованих ресурсів.

Нейромережева технологія виявлення та класифікації мережевих атак (**ВКМА**), описана в роботі [28]. В технології запропоновано використання трьохшарової НМ, що навчається методом зворотного поширення помилки. При цьому для розпізнавання кожного виду мережевої атаки застосовується окрема НМ. В якості вхідних параметрів пропонується використання параметрів мережевого трафіку по стеку протоколів TCP/IP. В якості навчальної вибірки пропонується використати дані із бази даних KDD-99. Наведено словесний опис та фрагменти програмного коду для підготовки вхідних даних із цієї

бази даних до виду вхідних параметрів НМ. При цьому однією із цілей підготовки є зменшення обсягу навчальної вибірки НМ. Описи підходів до оптимізації архітектури та параметрів нейромережвої моделі відсутні.

Система виявлення аномальної поведінки обчислювальних процесів (**ВАОП**), розроблена в роботі [7]. Система призначена для виявлення атак на компоненти інформаційної системи, які функціонують на базі мікроядерних операційних систем. Детально розроблено методику збору та підготовки вхідних параметрів для НМ. Пропонується використання ТК та БШП. Опису процедури оптимізації архітектури та параметрів нейромережевої моделі не наведено.

Модель кібернейрону (**МКН**), розроблена та описана в роботі [16]. Модель пропонується використовувати для розпізнавання комп'ютерних вірусів. Основною відмінністю моделі кібернейрону (КН) є відсутність функції активації, замість якої використовується таблиця підстановки, а основною перевагою – потенційно висока обчислювальна потужність. Розроблені алгоритми навчання кібернейрону. В якості вхідних параметрів використовуються або фрагменти піддослідного файлу, або хеш-коди вказаних фрагментів. Визначення вказаних фрагментів пропонується реалізувати методом ковзаючого вікна. Завданням НМ являється розпізнавання чистих та заражених фрагментів. Слід зазначити, що модель кібернейрона з'явилась відносно недавно, являється практично не апробованою, а використання табличної активаційної функції теоретично малообґрунтоване. Відповідно застосування кібернейрону в сфері захисту інформації потребує серйозного доопрацювання.

Метод розпізнавання аномалій мережевого трафіку (**РАМТ**), розроблений в роботі [1]. Методом передбачене використання НМ типу БШП. В якості вхідних даних НМ використано параметри заголовків IP-дейтаграм. Вибір архітектури НМ базується на твердженні про високі апроксимаційні можливості БШП. БШП складається із трьох шарів нейронів. Кількість нейронів першого (вхідного) шару – 18, що дорівнює кількості параметрів заголовку IP-дейтаграми. Кількість нейронів у вихідному шарі 2. Вихід нейрону №1 відповідає за наявність аномалії, а вихід нейрону №2 за безпечний стан мережевого трафіку. Наведені вирази для розрахунку кількості нейронів у схованому шарі. Таким чином методом передбачено оптимізацію параметрів архітектури НМ. Для спрощення створення репрезентативної вибірки розроблено метод уточнюючих сигнатур, суть якого полягає у введенні додаткових штучно створених сигнатур, що описують апріорно аномальний трафік. Таким чином в методі в неявному вигляді можливо використати експертні дані про мережеві атаки.

Нейромережева штучна імунна система (**НШІС**), описана в роботі [3, 23]. НШІС призначена для розпізнавання в сканованих файлах шкідливого програмного забезпечення. Використано НМ типу ТК. Вибір тину НМ обґрунтовано по критерію мінімізації допустимого обсягу навчальної вибірки (L), який для ТК залежить тільки від кількості нейронів схованого шару (m): $L \geq 2m$. В свою чергу $m = p + r$, де p – кількість прикладів безпечних програм в навчальній вибірці, а r – кількість прикладів шкідливого програмного забезпечення. Процедури попередньої обробки вхідних параметрів та оптимізації процесу навчання не передбачені.

Модель топографічної карти Кохонена для розпізнавання комп'ютерних вірусів (**МТК**), розроблена в роботі [2]. Модель призначена для використання в антивірусних сканерах. Передбачено блок попередньої обробки вхідних параметрів. Вибір типу моделі реалізовано шляхом порівняльних числових експериментів. В якості критерію порівняння використано термін навчання. Оптимізація параметрів та процедури навчання нейромережевої моделі не проводилась.

Метод виявлення несанкціонованого доступу до бази даних (**ВНДБД**), розроблено в роботі [10]. Крім виявлення атак метод передбачає виявлення вразливостей в БД. Запропоновано використання БШП з одним схованим шаром. Вхідний шар БШП складається із 4 нейронів, а вихідний із 1. В якості вхідних даних використано: обсяг інформації, що завантажується в базу даних, кількість транзакцій за одну хвилину, кількість операцій модифікації за одну хвилину, ознаки звернень до словника. Попередня обробка вхідних параметрів полягає у їх ранжуванні та нормалізації.

Алгоритм перетворення параметрів трафіку (**АППТ**), описано в роботі [4]. Алгоритм призначений для отримання із мережевого трафіку вхідних даних для нейромережевої системи виявлення мережевих атак. В якості вхідної інформації зазначеного алгоритму використовуються параметри TCP-сесії. Перетворення параметрів трафіку застосовується з метою зменшення кількості вхідних параметрів НМ і збільшення їх інформативності та реалізується за допомогою ма-

тематичного апарату, що базується на методі головних компонент. В алгоритмі оптимізація архітектури та параметрів нейромережевої моделі не передбачена. Також зазначимо, що роботи [3, 11] мають аналогічний характер.

Нейромержева технологію виявлення мережевих атак (**ТВМА**) на інформаційні ресурси, описана в [8, 9, 19]. В технології передбачено модуль стиснення вхідних даних, котрий базується на застосуванні нейромережевого аналогу методу головних компонент – рециркуляційної нейронної мережі (РНМ) з двома шарами нейронів. Структура РНМ показана на рис. 2.

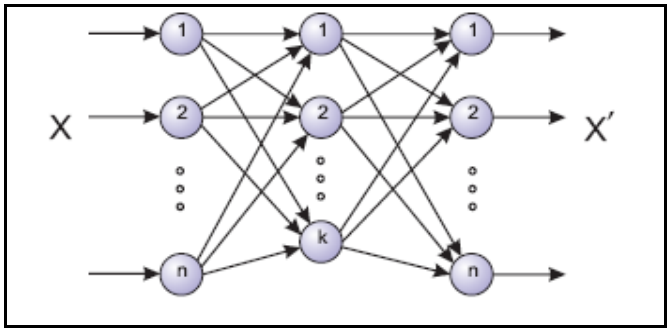

Рис. 2. Структура рециркуляційної нейронної мережі

Перший шар, що складається із k нейронів, дозволяє управляти кількістю інформаційних ознак (x), а другий шар з n нейронів дозволяє проводити фільтрацію даних (x'). Налаштування першого шару дозволяють отримати стиснену до k ознак форму представлення вхідного n-мірного об'єкту, тобто визначити k головних компонент.

В методі шляхом числових експериментів доведено можливість використання в ньому НМ типу ТК та БШП для виявлення мережевих атак, сигнатури яких представлено в базі даних KDD-99.

Базові характеристики проаналізованих нейромережевих методів та моделей наведено в табл. 1. Аналіз даних цієї таблиці вказує на те, що більшість відомих нейромережевих систем призначені для розпізнавання мережевих атак. При цьому в якості базових типів нейромережевих моделей використовуються БШП та ТК.

Крім того в результаті проведеного аналізу визначено, що підвищення ефективності сучасних нейромережевих методів та моделей йде шляхом забезпечення в них певних можливостей, котрі характеризуються за допомогою наступних параметрів: $P_{по}$ – попередня обробка вхідних параметрів, $P_{ота}$ – однокритеріальна оптимізація типу архітектури, $P_{бва}$ – багатокритеріальна оптимізація виду архітектури, $P_{опа}$ – однокритеріальна оптимізація параметрів архітектури, $P_{бпа}$ – багатокритеріальна оптимізація параметрів архітектури, $P_{омн}$ – оптимізація методу навчання, $P_{веп}$ – можливість використання експертних правил. На наш погляд наведений перелік слід доповнити параметрами $P_{мна}$ та $P_{одв}$, які б вказували на можливість застосуванні в методі класичних і перспективних типів нейромережевих архітектур та на можливість принципової оцінки доцільності застосування НМ для вирішення поставленої задачі. Підґрунтям використання параметру $P_{мна}$ є наведене в роботах [17, 20] твердження про те, що в галузі ІБ, як і в більшості відомих застосувань, розвиток нейромережевих методів та моделей йде шляхом пристосування базових та перспективних нейромережевих архітектур до умов поставлених практичних задач. Підґрунтям використання параметру $P_{одв}$ є об'єктивна необхідність чіткого окреслення області застосувань НМ в галузі забезпечення ІБ. Величини запропонованих параметрів першому наближенні можна оцінити так: параметр дорівнює -1, коли відповідна можливість в нейромережевому методі або моделі не забезпечується, 0 – коли забезпечується опосередковано і 1 – коли забезпечується безпосередньо. Для проаналізованих випадків величини означених параметрів наведено в табл. 2. При цьому для всіх проаналізованих методів $P_{мна}=P_{одв}=0$. Лише для АППТ $P_{мна}=1$, а $P_{одв}=0$. Тобто в більшості із проаналізованих методів не можна використати всього переліку класичних та перспективних нейромережевих архітектур і в жодному із методів (моделей) не передбачена оцінка принципової доцільності його застосування. Крім того, використання запропонованих критеріїв дозволяє визначити інтегральний показник ефективності нейромережевого методу (P_Σ) за допомогою наступного виразу:

$$P_\Sigma = \sum_{i=1}^{9} \alpha_i 2^{P_i}, \qquad (1)$$

де α_i – ваговий коефіцієнт і-го критерію.

В загальному випадку визначення вагових коефіцієнтів потребує окремого дослідження, а в базовому варіанті припустимо, що $\alpha_i = 1$.

Також зазначимо, що базовий перелік параметрів може бути в подальшому розширений.

Зазначимо, що практична цінність даних табл. 2 полягає у окресленні недоліків та перспектив вдосконалення сучасних нейромережевих методів та моделей. Наприклад, величини $P_{по}=0$, $P_{бва}=-1$ свідчать про те, що до недоліків методу НСВВ, описаного в [1, 3, 6], можна віднести недостатню оптимізацію виду архітектури нейромережевої моделі. Це свідчить про можливість

відповідного вдосконалення вказаних методів. При цьому жоден із розглянутих методів не передбачає повноцінної оптимізації нейромережевої моделі, відповідно умов поставленої задачі та повноцінного використання в такій моделі експертних правил. Зазначимо, що величина параметру P_{Σ} дозволяє оцінити інтегральну ефективність нейромережевого методу.

Таблиця 1

Базові характеристики нейромережевих методів та моделей

№	Метод	Розпізнавання				Тип НМ								
		Комп'ютерних	Атак та вразливостей БД	Спаму	Мережевих атак	БПШ	КН	ТК	НМД, НМЕ	АНМ	ННМ	БНМ	РНМ	Всі типи
1	ВФПК	+	-	-	-	+	-	-	-	-	-	-	-	-
2	МКН					-	+	-	-	-	-	-	-	-
3	МТК					-	-	+	-	-	-	-	-	-
4	НШІС													
5	НПВІ	-	+	-	-	-	-	-	+	-	-	-	-	-
6	ВНДБД					+	-	-	-	-	-	-	-	-
7	НФС	-	-	+	-	-	-	-	-	+	-	-	-	-
8	АППТ	-	-	-	+	-	-		-	-	-	-	-	+
9	ПСК													
10	НСВВ													
11	ТВМА					+	-		-	-	-	-	-	-
12	РАМТ													
13	ВМА													
14	ССК					-	-	+	-	-	-	-	-	-
15	НМГС													
16	ПСКТ													
17	ПВМА					+	-	+	-	-	-	-	-	-
18	АСВА													
19	ВАОП													
20	СВДА					-	-		-	-	+	-	-	-
21	БНМ					-	-		-	-	-	+	-	-
22	ВКМА					-	-		-	-	-	-	+	-

В підсумку можна запропонувати наступний метод визначення напрямків вдосконалення та розрахунку інтегральної ефективності сучасних нейромережевих методів оцінки параметрів безпеки ІС:

Етап 1. В результаті аналізу можливостей нейромережевого методу визначити величини параметрів: $P_{по}$, $P_{ота}$, $P_{бва}$, $P_{опа}$, $P_{бпа}$, $P_{омн}$, $P_{вап}$, $P_{мна}$, $P_{одв}$.

Етап 2. Якщо величина деякого і-го параметру менша від 1, то це означає на необхідність вдосконалення нейромережевого методу у відповідному напрямку.

Етап 3. В результаті аналізу умов поставленої задачі захисту визначити вагові коефіцієнти: $\alpha_{по}$, $\alpha_{ота}$, $\alpha_{бва}$, $\alpha_{опа}$, $\alpha_{бпа}$, $\alpha_{омн}$, $\alpha_{вап}$, $\alpha_{мна}$, $\alpha_{одв}$.

Етап 4. Використовуючи вираз (1) визначити величину показника інтегральної ефективності методу.

Також в результаті проведеного аналізу доведено, що в сучасних СВА та СВВ в основному використовуються класичні типи нейромережевих моделей, які в тій чи іншій мірі адаптовані до умов поставленої задачі. Це дозволяє звузити коло допустимих нейромережевих моделей, що в свою чергу дозволяє підвищити оперативність визначення нейромережевої моделі, оптимальної з точки зору поставленої задачі. Таким чином з'являється можливість підвищення оперативність створення відповідних СВА та СВВ.

Таблиця 2

Величини параметрів, що характеризують нейромережеві методи та моделі

№	Метод	Параметр									
		$P_{по}$	$P_{ота}$	$P_{бва}$	$P_{опа}$	$P_{бпа}$	$P_{омн}$	$P_{вап}$	$P_{мна}$	$P_{одв}$	P_{Σ}
1	ВФПК	1	0	-1	0	-1	0	1	-1	-1	0,25
2	МКН	1	1	-1	-1	-1	-1	-1	-1	-1	0,03125
3	МТК	1	1	-1	0	-1	-1	-1	-1	-1	0,0625
4	НШІС	-1	1	-1	1	-1	-1	-1	-1	-1	0,03125
5	НПВІ	1	1	0	0	-1	0	-1	-1	-1	0,25
6	ВНДБД	1	0	-1	0	-1	-1	-1	-1	-1	0,03125
7	НФС	0	1	1	1	1	0	-1	-1	-1	2
8	АППТ	1	-1	-1	-1	-1	-1	-1	0	-1	0,015625
9	ПСК	1	0	-1	0	-1	0	-1	-1	-1	0,0625
10	НСВВ	0	0	-1	0	-1	0	-1	-1	-1	0,03125
11	ТВМА	1	0	-1	0	-1	-1	-1	-1	-1	0,03125
12	РАМТ	-1	1	-1	0	-1	-1	0	-1	-1	0,03125
13	ВМА	0	0	-1	0	-1	-1	1	-1	-1	0,0625
14	ВМА	1	0	-1	0	-1	0	-1	-1	-1	0,0625
15	ВМА	1	1	0	0	-1	-1	-1	-1	-1	0,125
16	ПСКТ	1	0	-1	0	-1	0	-1	-1	-1	0,0625
17	ПВМА	1	1	-1	0	-1	0	-1	-1	-1	0,125
18	АСВА	1	1	0	1	0	0	-1	-1	-1	2
19	ВАОП	1	-1	-1	-1	-1	-1	-1	-1	-1	0,0078125
20	СВДА	0	0	-1	0	-1	0	-1	-1	-1	0,03125
21	БНМ	-1	0	-1	-1	-1	1	-1	-1	-1	0,003907
22	ВКМА	1	-1	-1	-1	-1	-1	-1	-1	-1	0,007813

Висновки. Визначено перелік параметрів та розроблено метод їх використання для оцінки інтегральної ефективності розробки сучасних нейромережевих методів і вибору цих методів для застосування в СВК та СВВ. Це дозволяє окреслити недоліки вказаних методів та моделей, визначити перспективні напрямки їх вдосконалення, що дозволяє підвищити ефективність створених на їх базі систем. Крім того показана можливість обмеження кола допустимих нейромережевих архітектур, котрі використовуються в системах виявлення, що надає можливість підвищити оперативність створення означених систем.

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 нейросетевых методов распознавания компьютерных вирусов /Материалы секционных заседаний. Моло-

дежный инновационный форум «ИНТРИ» – 2010. – Минск: ГУ «БелИСА», 2010. – С. 47-48.

[3]. Безобразов С.В. Алгоритмы исскуственных имунных систем и нейронних сетей для обнаружения вредоносных программ / С.В. Безобразов, В.А. Головко // Нейроинформатика. – 2010. – №7. – С. 273-288.

[4]. 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.

[5]. Васильев В.И. Нейронные сети при обнаружении атак в сети Internet (на примере атаки SYNFLOOD) / В.И. Васильев, А.Ф. Хафизов // Нейрокомпьютеры в информационных и экспертных системах. – М.: Радиотехника, 2007. – №6. – С. 34-38.

[6]. Гришин А.В. Нейросетевые технологии в задачах обнаружения компьютерных атак / А.В. Гришин // Информационные технологии и вычислительные системы – 2011. – №1. – С. 53 -64.

[7]. Дьяконов М.Ю. Нейросетевая система обнаружения аномального поведения вычислительных процессов микроядерных операционных систем: авторефер. дисс. на соискание научн. степени канд. техн. наук : спец. 05.13.19 – Методы и системы защиты информации, информационная безопасность / М. Ю. Дьяконов – Уфа, 2010. – 28 с.

[8]. Емельянова Ю.Г. Анализ проблем и перспективы создания интеллектуальной системы обнаружения и предотвращения сетевых атак на облачные вычисления / Ю.Г. Емельянова, В.П. Фраленко // Программные системы: теория и приложения: электрон. научн. журн. – 2011. – № 4(8). – С. 17-31. [Электронный ресурс]. URL: http://psta.psiras.ru/ read/ psta2011_4_17-31.pdf.

[9]. 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.

[10]. Зайцев О. Нейросети в системах безопасности / О. Зайцев // IT-Спец. – 2007. – № 6. – С. 54–59.

[11]. Комар М.П. Метод построения совокупного классификатора трафика информационно-телекоммуникационных сетей для иерархической классификации компьютерных атак / М.П.Комар // Системи обробки інформації. – 2012. – Випуск 3 (101), том 1 – С.134-138.

[12]. 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.

[13]. Корченко О. Г. Метод оцінки нейромережевих засобів щодо можливостей виявлення інтернет-орієнтованих кібератак / О.Г. Корченко, І.А. Терейковський, С.В. Казимірчук // Вісник інженерної академії наук. – 2014. – Випуск 2. – С. 87-93.

[14]. Крыжановский А.В. Применение искусственных нейронных сетей в системах обнаружения атак / А.В. Кржыжановский // Доклады ТУСУРа. – 2008. – № 2 (18), часть 1. – С. 37-41.

[15]. Магницкий Ю.Н. Использование бинарной нейронной сети для обнаружения атак на ресурсы распределенных информационных систем / Ю.Н. Магницкий // Динамика неоднородных систем. – 2008. – С. 200-205.

[16]. Поликарпов С.В., Дергачёв В.С., Румянцев К.Е., Голубчиков Д.М. Новая модель искусственного нейрона: кибернейрон и области его применения / Електронний ресурс http://arxiv.org/ftp/arxiv/ papers/ 0907/0907.0229.pdf.

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

[18]. Слеповичев И.И. Обнаружение DDoS-атак нечеткой нейронной сетью / И.И. Слеповичев, П.В. Ирматов, М.С. Комарова, А.А. Бежин // Известия Саратовского университета. – 2009. – Т. 9, сер. Математика. Механика. Информатика, вып. 3. – С. 84-89.

[19]. Талалаев А.А.Разработка нейросетевого модуля мониторинга аномальной сетевой активности / А.А. Талалаев, И.П. Тищенко, В.П. Фраленко, В.М. Хачумов // Нейрокомпьютеры: разработка и применение. – 2011. – № 7. – С. 32-38.

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

[21]. Тимофеев А. Исследование и моделирование нейросетевого метода обнаружения и классификации сетевіїх атак / А. Тимофеев, А. Браницкий // International Journal Information Technologies & Knowledge. – 2012. – Vol.6, Number 3. – P. 257-265

[22]. Хафизов А.Ф. Нейросетевая система обнаружения атак на WWW-сервер: дис. ... канд. техн. наук : 05.13.11 / А.Ф. Хафизов– Уфа, 2004 – 172 с.

[23]. Bezobrazov S., Golovko V. Neural Networks for Artificial Immune Systems: LVQ for Detectors Construction // International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications. – Dortmund, 2007. – P. 180-184.

[24]. Bivens A., Palagiri C., Smith R., Szymansky B., Embrechts M. Network–Based Intrusion Detection Using Neural Networks // Proc. Intelligent Engineering Systems through Artificial Neural Networks ANNIE–2002, St. Louis, MO, Volume 12. – New York: ASME Press, 2002. P. 579–584.

[25]. Chen Y., Narayanan A., Shaoning Pang, Ban Tao. Multiple sequence alignment and artificial neuralnetworks for malicious software detection // Natural Computation, 2012, P. 261 – 265.
[26]. Du Toit T., Kruger H. Filtering spam e-mail with Generalized AdditiveNeural Networks // Information Security for South Africa. 2012., P.1-8.
[27]. Hnatiuk S. Cyberterrorism: History of current trends and countermeasures. / S. Hnatiuk // Privacy Notice . – 2013 . – Volume 9 , № 2. – P. 118 -129.
[28]. Skaruz J., Seredynski F. Recurrent neural networks towards detection of SQL attacks // Parallel and Distributed Processing Symposium, 2007.

REFERENCES

[1]. Abramov E.S. Development and building a Study methods of detection of attacks: dis. ... Candidate. Sc. sciences: 05.13.19 // Abramov E.S. – Taganrog, 2005. – 199 p.
[2]. Artemenko A., Golovko V.A. Analysis neyrosetevыh methods of computer viruses raspoznavanyya // Materials sektsyonnih zasedanyy. Molodezhny ynnovatsyonny Forum «YNTRY» – 2010. – Minsk: PG «BelYSA», 2010. – 239 p.
[3]. Bezobrazov S.V., Golovko V.A. Algorithms of artificial immune systems and neural networks for malware detection // Neyroniformatika. – 2010. – №7. – P. 273-288.
[4]. Bolshev A. K. Transformation and classification algorithms for traffic detection in vtorzhenyy kompyuternыe Network : avtorefer. diss. on soyskanye Nauchn. Exponentiation candidate. Sc. sciences specials. 05.13.19 – Methods and systems of protection of information , ynformatsyonnaya Safety // A.K Bolshev – St. Petersburg, 2011. – 36 p.
[5]. Vasilyev V.I., Hafiz A.F. Neural network detection of attacks on the Internet (for example, attack SYNFLOOD) // Neurocomputers in information and expert systems. – M : Radio Engineering, 2007. – №6. – P. 34-38.
[6]. Grishin A.V. Neural network technology in problems of detection of computer attacks // Information technology and computer systems. – 2011. – №1. – P. 53 -64.
[7]. Dyakonov M.Y. Neural network system to detect anomalous behavior of computational processes microkernel operating systems: avtorefer. diss. for the scientific. Ph.D. degree. tehn. Sciences: special. 05.13.19 – Methods and systems for information security, information security / Deacons M. Y. – Ufa, 2010. – 28 p.
[8]. Emelyanova Y.G., Fralenko V.P. Analysis of problems and prospects for the creation of intelligent system to detect and prevent network attacks on cloud computing // Software Systems: Theory and Applications: electron. Nauchn. Zh. – 2011. – № 4 (8). – P. 17-31. [Electronic resource]. URL: http://psta.psiras.ru/ read/psta2011_4_17-31.pdf.
[9]. Emelyanova Y.G., Talalaev A.A., Tishchenko I.P., Fralenko V.P. Neural network intrusion detection technology to information resources // Software Systems: Theory and Applications. – 2011. – № 3 (7). – P. 3-15.
[10]. Zaitsev A. Neural networks in security systems // IT-Spec. – 2007. – № 6. – P. 54-59.
[11]. Komar M.P. The method of constructing a classifier aggregate traffic information and telecommunication networks for hierarchical classification of computer attacks // Information processing systems. – 2012 – Issue 3 (101), Volume 1 – P.134-138.
[12]. Komar M.P., Paly I.O., Shevchuk R.P., Fedysiv T.B. A neural network approach to the detection of network attacks on computer systems // Informatics and mathematical methods in modeling. – 2011 – Volume 1, №2. – P. 156-160.
[13]. Korchenko O.G., Tereykovsky I.A., Kazimirchuk S.V. Method for the assessment of neural network tools on how to identify Internet-based cyber attacks // Bulletin of the Academy of Engineering Sciences. – 2014. – Issue 2 – P. 87-93.
[14]. Kryzhanovsky A.V. Application of artificial neural networks in intrusion detection systems // Reports TUSUR. – 2008. – № 2 (18), Part 1 – P. 37-41.
[15]. Magnitsky J.N. The use of binary neural network for intrusion detection on the resources allocated to information systems // Dynamics of inhomogeneous systems. – 2008 – P. 200-205.
[16]. Polikarpov S.V., Dergatchev V.S., Rumyantsev K.E., Golubchikov D.M. A new model of artificial neuron kiberneyron and its use / [Electronic resource]. URL:http://arxiv.org/ftp/arxiv/ papers/0907/0907.0229.pdf.
[17]. Rudenko O.G., Bodyanskiy E.V. Artificial Neural Networks. Teach. guidances. – Kharkiv: «Company Smith», 2006 - 404 p
[18]. Slepovitch I.I., Irmatov P.V., Komarova M.S., Bezhin A.A. Detection of DDoS-attacks fuzzy neural network // News Saratov University. – 2009 – T. 9, Ser. Mathematics. Mechanics. Computer Science, vol. 3 – P. 84-89.
[19]. Talalaev A.A., Tishchenko I.P., Fralenko V.P., Khachumov V.M. Development of neural network module for monitoring abnormal network activity // Neurocomputers: development and application. – 2011. – № 7. – P. 32-38.
[20]. Tereykovsky I. Neural networks in the mass of information protection – K.: PolihrafKonsaltynh. – 2007. – 209 p.
[21]. Tymofeev A., Branytskyy A. Research and modeling of neural network method of detection and classification of attacks seteviih. // International Journal Information Technologies & Knowledge. – 2012. – Vol.6, Number 3. – P. 257-265
[22]. Hafyzov A.F. Neyrosetevaya system obnaruzhenyya attacks on the WWW-server: Thesis. ... Candidate. techn. sciences: 05.13.11 / Hafyzov A.F. – Ufa, 2004 – 172 p.

[23]. Bezobrazov S., Golovko V. Neural Networks for Artificial Immune Systems: LVQ for Detectors Construction // International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications. – Dortmund, 2007. – P. 180-184.
[24]. Bivens A., Palagiri C., Smith R., Szymansky B., Embrechts M. Network–Based Intrusion Detection Using Neural Networks // Proc. Intelligent Engineering Systems through Artificial Neural Networks ANNIE–2002, St. Louis, MO, Volume 12. – New York: ASME Press, 2002. P. 579–584.
[25]. Chen Y., Narayanan A., Shaoning Pang, Ban Tao. Multiple sequence alignment and artificial neuralnetworks for malicious software detection // Natural Computation, 2012, P. 261 – 265.
[26]. Du Toit T., Kruger H. Filtering spam e-mail with Generalized AdditiveNeural Networks // Information Security for South Africa. 2012., P.1-8.
[27]. Hnatiuk S. Cyberterrorism: History of current trends and countermeasures. // Privacy Notice . – 2013 . – Volume 9 , № 2. – S. 118 – 129.
[28]. Srivastav H., Challa R.K. Novel intrusion detection system integrating layered framework with neural network // Advance Computing Conference (IACC), 2013 IEEE 3rd International, P. 682-689.
[29]. Skaruz J., Seredynski F. Recurrent neural networks towards detection of SQL attacks // Parallel and Distributed Processing Symposium, 2007, P. 1 – 8.

СОВРЕМЕННЫЕ НЕЙРОСЕТЕВЫЕ МЕТОДЫ И МОДЕЛИ ОЦЕНКИ ПАРАМЕТРОВ БЕЗОПАСНОСТИ РЕСУРСОВ ИНФОРМАЦИОННЫХ СИСТЕМ

Одним из основных препятствий широкому внедрению нейросетевых методов и моделей в системах обнаружения кибератак и в системах обнаружения уязвимостей ресурсов информационных систем является отсутствие параметров, на основе которых можно оценить их эффективность. Также отсутствуют и методы оценки эффективности такого внедрения. Для решения этой проблемы был проанализирован широкий спектр современных нейросетевых методов и моделей, применяемых в системах обнаружения. Определен перечень параметров и разработан метод их использования для оценки эффективности разработки и выбора указанных методов и моделей при построении указанных систем обнаружения. Полученные результаты позволяют определить недостатки современных нейросетевых средств обнаружения кибератак и средств обнаружения уязвимостей и очертить перспективные пути их совершенствования.
Ключевые слова: безопасность информации, выявления кибератак, информационная система, нейросетевые модели, нейросетевой метод, параметр безопасности.

MODERN NEURAL NETWORK METHOD EVALUATION MODEL SECURITY SETTINGS RESOURCES INFORMATION SYSTEMS

One of the main obstacles to widespread adoption of neural network methods and models in cyber attacks and detection systems to detect vulnerabilities in the systems resources information systems is the lack of options on which to evaluate their effectiveness. Also, there are no methods for assessing the effectiveness and implementation of such. To solve this problem has been analyzed a wide range of modern neural network methods and models used in the detection systems. The list of parameters and a method of their use for assessing the effectiveness of the design and selection of these methods and models in the construction of these detection systems. The obtained results allow us to determine the shortcomings of modern neural network detection tools and means of cyber vulnerability detection and outline promising ways to improve them.
Keywords: information security, detection of cyber attacks, information system, neural network model, the neural network method, the security setting.

Корченко Олександр Григорович, доктор технічних наук, професор, завідувач кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: icaocentre@nau.edu.ua
Корченко Александр Григорьевич, доктор технических наук, профессор, заведующий кафедрой безопасности информационных технологий Национального авиационного университета.
Korchenko Alexander, Professor, Doctor of Science in Eng., Head of Academic Department of IT-Security, National Aviation University.

Терейковський Ігор Анатолійович, кандидат технічних наук, доцент, докторант кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: terejkowski@ukr.net
Терейковский Игорь Анатольевич, кандидат технических наук, доцент, докторант кафедры безопасности информационных технологий Национального авиационного университета.
Terejkowski Igor, PhD in Eng., Associate Professor, doctoral student of Academic Department of IT-Security, National Aviation University.

Дзюбаненко Андрій Васильович, здобувач кафедри комп'ютеризованих електротехнічних систем та технологій Національного авіаційного університету.
E-mail: dzubanenko_av@ukr.net
Дзюбаненко Андрей Васильевич, соискатель кафедры компьютеризированных электротехнических систем и технологий Национального авиационного университета.
Dzubanenko Andriy, Researcher in Academic Dept of Computerized Electrotechnical Systems and Technology at National Aviation University.