ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2020, № 3 (87)

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ ТА МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ

УДК 004.7:004.032.26

В. М. ПАХОМОВА[1*], М. С. КОННОВ[2*]

[1*]Каф. «Електронні обчислювальні машини», Дніпровський національний університет залізничного транспорту імені академіка В. Лазаряна, вул. Лазаряна, 2, Дніпро, Україна, 49010, тел. +38 (056) 373 15 89, ел. пошта viknikpakh@gmail.com, ORCID 0000-0002-0022-099X
[2*]Каф. «Електронні обчислювальні машини», Дніпровський національний університет залізничного транспорту імені академіка В. Лазаряна, вул. Лазаряна, 2, Дніпро, Україна, 49010, тел. +38 (056) 373 15 89, ел. пошта mkonnov1997@gmail.com, ORCID 0000-0001-7212-7631

ДОСЛІДЖЕННЯ ДВОХ ПІДХОДІВ ДО ВИЯВЛЕННЯ МЕРЕЖНИХ АТАК ІЗ ВИКОРИСТАННЯМ НЕЙРОМЕРЕЖНОЇ ТЕХНОЛОГІЇ

Мета. На сучасному етапі найчастіше пропонують системи виявлення мережних атак, що побудовані на основі таких нейронних мереж: багатошарового персептрона, мережі Кохонена або самоорганізованої карти та їх комбінацій. У статті передбачено дослідити ефективність двох підходів до виявлення атак на комп'ютерну мережу з використанням нейромережної технології на основі нормалізованих даних відкритої бази NSL–KDD. **Методика.** Як архітектурні рішення системи виявлення мережних атак запропоновано розглянути такі підходи: на основі однієї нейронної мережі, що визначає клас атаки (перший підхід), та ансамблю із п'яти нейронних мереж (другий підхід), який на першому етапі визначає категорію атаки (DoS, Probe, U2R, R2L), а на другому етапі – клас атаки, що належить до певної категорії. **Результати.** На створених у програмі MatLAB нейронних мережах проведено дослідження їх похибки від довжини навчальної вибірки за різними алгоритмами навчання: Levenberg–Marquardt; Bayesian Regularization; Scaled Conjugate Gradient – за різної кількості прихованих нейронів (мінімальної, середньої та максимальної). Визначено оптимальні параметри нейронних мереж за двома підходами. **Наукова новизна**. У ході проведення експериментів за різними підходами отримано результати: TP (True Positive); FP (False Positive); FN (False Negative); TN (True Negative). На їх основі розраховано такі показники оцінки якості рішень: коректність визначення мережних атак; помилкові спрацьовування; достовірність; точність та повнота, що доказують доцільність використання ансамблю нейронних мереж (другого підходу). **Практична значимість**. На створених нейронних мережах за двома підходами проведено дослідження: часу роботи нейронних мереж; помилки першого роду; помилки другого роду. За результатами першого дослідження в середньому час роботи ансамблю нейронних мереж складає 0,92 с, а час роботи нейронної мережі (за першим підходом) дорівнює 2,21 с. За результатами другого дослідження помилка першого роду з використанням ансамблю нейронних мереж складає 2,17 %, а за першим підходом – 7,39 %. За результатами третього дослідження помилка другого роду з використанням ансамблю нейронних мереж складає 3,91 %, а за першим підходом – 6,96 %, що підтверджує ефективність використання ансамблю нейронних мереж (другого підходу).

Ключові слова: атака; ансамбль; нейронна мережа; помилка першого роду; помилка другого роду; достовірність; точність; повнота

doi: https://doi.org/10.15802/stp2020/208233

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2020, № 3 (87)

Вступ

Створення ефективної системи виявлення мережних атак вимагає застосування якісно нових підходів до обробки інформації, які повинні ґрунтуватися на адаптивних алгоритмах, здатних до самонавчання. Найбільш перспективним напрямом у створенні подібних систем виявлення атак на комп'ютерну мережу є застосування нейромережної технології.

На сучасному етапі найчастіше пропонують системи виявлення мережевих атак, що побудовані на основі таких нейронних мереж (НМ): багатошарового персептрона [1, 2, 14, 15], мережі Кохонена або самоорганізованої карти [8, 9, 11, 12] та їх комбінацій [3–5, 7].

Багатошаровий персептрон (Multi Layer Perceptron, MLP). Так, наприклад, А. В. Крижановський за допомогою програми Statistic Neural Networks створив НМ, що допускає середню квадратичну помилку під час виявлення атаки 0,006826 % [1]. А. Г. Мустафаев за допомогою нейропакета Neural Network Toolbox програми MatLAB створив НМ, що в 93 % випадків правильно класифікує атаки [2]. І. В. Жуковицький і В. М. Пахомова за допомогою програми Fann Explorer створили НМ конфігурації 19–1–25–5 (19 – кількість початкових нейронів; 1 – кількість прихованих шарів; 25 – кількість прихованих нейронів; 5 – кількість результуючих нейронів), що дозволить у реальному часі виявити загрози Back, Buffer_overflow, Quess_password, Ipsweep, Neptune на комп'ютерну мережу [15].

Самоорганізована карта (Self Organizing Maps, SOM). Gunes Kayachik, Nur Zincir–Hejvud і Malkolm Hejvud [8] під час використання бази даних KDD99 з'ясували, що система виявляє атаки U2R і R2L в 90,4 % випадків, але при цьому помилкове виявлення атаки складає 1,38 %. Palomo та Esteban [12] провели дослідження на основі зростаючої ієрархічної самоорганізованої карти із застосуванням бази KDD99. У результаті визначено майже максимальний рівень виявлення атаки, що складає 99,99 %, але при цьому є суттєвий недолік, який полягає у великій імовірності помилки у 5,44 % порівняно з іншими НМ. Ortis Andres [11] також проводила дослідження із застосуванням зростаючої ієрархічної самоорганізованої карти. У результаті була створена НМ із підвищенням швидкості виявлення атак, яка для навчання використовувала метод маркування ймовірностей. Для цієї НМ використано базу NSL–KDD. Досягнуто найвищу частоту виявлення атак 99,68 % із найменшим помилковим спрацьовуванням 0,02 %. Отже, краща загальна продуктивність, але рівень виявлення U2R–атак найгірший серед усіх інших атак. Згідно з [9], наявні системи виявлення вторгнень на основі самоорганізованих карт мають труднощі, які пов'язані з тривалим часом обчислень і низькою частотою виявлення атак U2R і R2L. Щоб подолати ці труднощі, кафедра обчислювальної техніки інституту інженерних технологій у запропонованій моделі використаний підхід зі зростаючою ієрархічною самоорганізованою картою з метою збільшення часу обчислень і відповідних функцій для атак U2R і R2L та підвищення продуктивності. У результаті на такій моделі приблизно на 75 % збільшується частота виявлення атак U2R і R2L порівнянно з самоорганізованими картами.

Комбінований підхід. Для виявлення DDoS–атак у роботі [3] застосовано SOM і MLP. За допомогою самоорганізованої карти відбувається кластеризація 50-символьних подій у вузли матриці, у яких згруповані події аналогічних числових символів. Фактично окремі вузли будуть являти собою певні сценарії атак. Після цього дані заголовків пакетів та інформація про групування подаються на вхід багатошарового персептрона, навченого розпізнавати аномальний трафік, але вже з урахуванням інформації про подію, тобто належності пакета до тієї чи іншої групи. У результаті тестування НМ отримані результати: помилка першого роду (помилкове спрацьовування) склала 3,16 % , а помилка другого роду (пропуск атаки) – 1,23 %. Технологічний університет імені короля Монгкута [5] провів подібний експеримент для виявлення таких типів атак: Neptune, Port Sweep і Satan. У ході експерименту поділено 121 820 навчальних шаблонів даних порівну на 8 наборів. Кожен набір об'єднується в мережу самоорганізованої карти, далі у тришаровий персептрон, що складається з 70 нейронів у першому шарі, 12 нейронів у другому (прихованому) шарі та 4 нейронів у результуючому шарі. У результаті НМ в 90 % випадків виявляє атаку і має менше 5 % помилкових спрацьовувань.

doi: https://doi.org/10.15802/stp2020/208233

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2020, № 3 (87)

Ми вважаємо, що під час обробки великого обсягу мережного трафіка, який постійно змінюється в інформаційно-телекомунікаційній системі залізничного транспорту, застосування системи виявлення мережних атак різних категорій на основі декількох MLP з використанням машинного навчання призводить до великої кількості помилкових спрацьовувань і пропусків атак, що потребує проведення додаткових досліджень для визначення оптимальних параметрів НМ.

Мета

Авторами передбачено розробити методику дослідження ефективності двох підходів до виявлення мережевих атак на комп'ютерну мережу з використанням нейромережної технології на основі нормалізованих даних відкритої бази NSL–KDD.

Методика

Постановка задачі. Як архітектурні рішення пропонуємо розглянути такі підходи до виявлення мережних атак: на основі однієї нейронної мережі (НМ1) та ансамблю нейронних мереж (НМ2, НМ2–1, НМ2–2, НМ2–3, НМ2–4), рис. 1. НМ1 (за першим підходом) визначає, яким класом атаки уражена комп'ютерна мережа. При цьому кількість результуючих нейронів буде дорівнювати кількості класів атак, що виявляє НМ1. Комбінування декількох НМ (за другим підходом), а саме п'яти, сприяє тому, що: НМ2 визначає категорію атаки, НМ2–1, НМ2–2, НМ2–3, НМ2–4 визначають клас атаки: DoS, Probe, U2R, R2L відповідно, що належать до певної категорії.

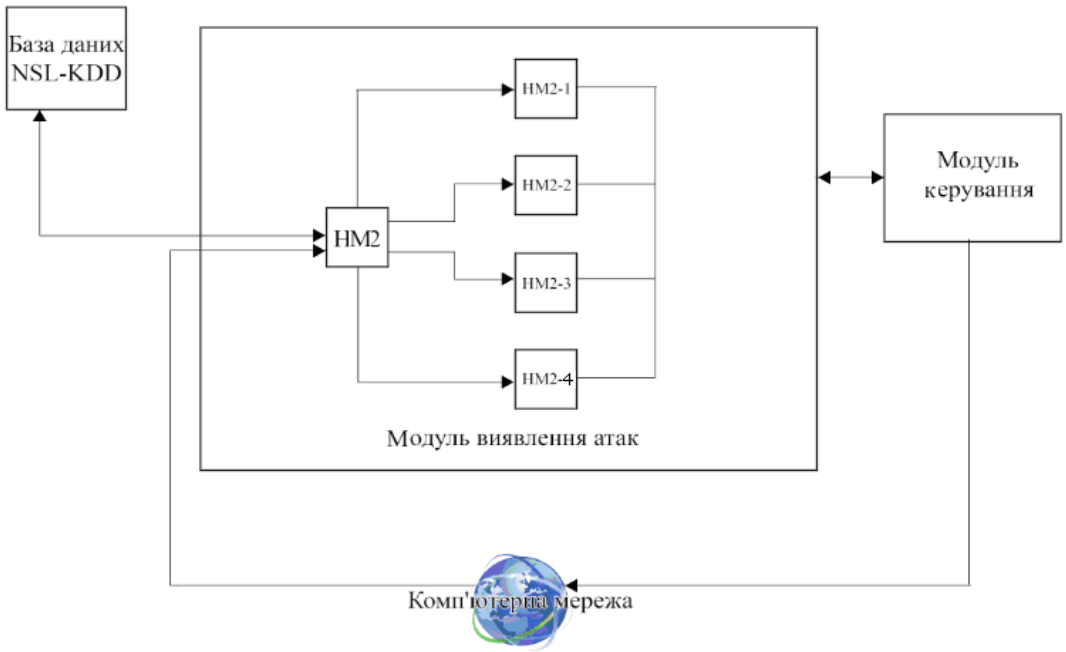

Рис. 1. Загальна схема виявлення мережевих атак (за другим підходом)

Fig. 1. General scheme for detecting network attacks (according to the second approach)

У [13] виконано огляд наявних наборів даних, найбільш поширеним із яких є база даних NSL–KDD, що створена з ініціативи Управління перспективних дослідницьких проєктів Міністерства оборони США (DARPA) на основі бази даних KDD'99 [10]. Набір даних складається з таких множин [6]: KDDTest+, KDDTrain+, KDDTrain+20 % (табл. 1).

doi: https://doi.org/10.15802/stp2020/208233

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2020, № 3 (87)

Таблиця 1

Розподілення атак у базі даних NSL–KDD

Table 1

Attacks distribution in the NSL-KDD database

Dataset	Total	Normal	DoS	Probe	U2R	R2L
KDDTrain+20%	25 192	13 449 (53 %)	9 234 (37 %)	2 289 (9,16 %)	11 (0,04 %)	209 (0,8 %)
KDDTrain+	125 973	67 343 (53 %)	45 927 (37 %)	11 656 (9,11 %)	52 (0,04 %)	995 (0,85 %)
KDDTest+	22 544	9 711 (43 %)	7 458 (33 %)	2 421 (11 %)	200 (0,9 %)	2 654 (12,1 %)

Еталон містить 43 параметри для кожного запису, причому 41 із них стосується самого трафіка, а останні два – Label та Score. До табл. 2 [4] зведені можливі класи: DoS – мережні атаки, спрямовані на виникнення ситуації, коли на атакованій системі відбувається відмова в обслуговуванні; Probe полягає в скануванні мережних портів із метою отримання конфіденційної інформації; U2R передбачає отримання зареєстрованим користувачем привілегій локального суперкористувача; R2L характеризується отриманням доступу незареєстрованого користувача до комп'ютера з віддаленого комп'ютера та відповідні типи атак. Хоча всі атаки існують у базі даних, але розподіл їх надто спотворений, як це видно в табл. 1. Більше половини записів, що існують в кожному наборі даних, відображають нормальний стан, а еталонів для класів U2R і R2L украй мало. Це точне уявлення про розподіл сучасних атак на інтернет-трафіка, де найбільш поширені атаки класу DoS, а атаки класів U2R і R2L практично не зустрічаються.

Вхідним вектором є набір із 41 параметра TCP–з'єднання, фрагмент опису якого наведено в табл. 3.

Нормалізація даних (підготовчий етап). Для моделювання НМ, що призначені виявляти атаки на комп'ютерну мережу, потрібно виконати нормалізацію даних. Проведено аналіз за кількістю еталонів кожного класу атак. Атаки, які мали менше 200 еталонів, виключені розгляду. У результаті залишилися 22 класи атак: 9 класів категорії DoS; 6 класів категорії Probe; 2 класи категорії U2L та 5 класів категорії R2L (див. табл. 2).

Таблиця 2

Класи атак у базі NSL–KDD

Table 2

NSL-KDD database attack classes

DoS	Probe	U2R	R2L
Apache2*	Ipsweep*	Buffer_ overflow*	Ftp_ write
Back*	Mscan*	Load-module	Guess_ passwd*
Land*	Nmap*	Perl	Httptunnel*
Neptune*	Portsweep*	Ps	Lmap
Pod*	Saint*	Rootkit*	Multihop*
Mail-bomb*	Satan*	Sqlattack	Named
Process-table*		Xterm	Phf
Smurf*			Sendmail
Teardrop*			Snmpgetattack
Udpstorm			Spy
Worm			Snmpguess
			Warezclient*
			Wazemaster*
			Xlock
			Xsnoop
9 із 11	6 із 6	2 із 7	5 із 15

Примітка: * тип атаки, який розглядають на НМ

doi: https://doi.org/10.15802/stp2020/208233

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)
Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2020, № 3 (87)

Таблиця 3

Опис початкових елементів

Table 3

Description of the initial elements

Вектор	Параметр	Опис
X_1	Duration	Час з'єднання
X_2	Protocol Type	Тип протоколу
X_3	Service	Мережна служба
X_4	Flag	Статус з'єднання
…	…	…
X_{41}	Sroce	Складність рівня

Далі сформовано 20 таблиць з еталонами (по 10 за кожним підходом). Перша таблиця мала по 2 еталони кожного класу атак (усього 44 еталони атак) і 56 еталонів класу Normal, таким чином, у першій таблиці 100 еталонів. У другій таблиці кількість еталонів атак і еталони типу Normal збільшено. У всіх наступних таблицях кількість еталонів збільшувалася, у результаті сформовано 10 таблиць, що використовуються (за другим підходом) із такою кількістю еталонів: 100, 200, 300, 400, 500, 600, 700, 800, 900 і 1 000. За першим підходом використано подібний спосіб, але всі значення збільшені у 10 разів, у результаті сформовано 10 таблиць (при цьому одна з таблиць, що містить 1 000 еталонів, не формувалася, а запозичена з тих таблиць, які використовувались за іншим підходом), із такою кількістю еталонів: 1 000, 2 000, 3 000, 4 000, 5 000, 6 000, 7 000, 8 000, 9 000 і 10 000. Причиною збільшення кількості еталонів є те, що НМ має велику кількість результуючих елементів.

Окремо сформована контрольна вибірка: по 10 еталонів для кожної атаки і 30 еталонів типу Normal; усього 250 еталонів. Проведено аналіз кожного параметра у відповідних таблицях. Зокрема, 20-ий стовпець, а саме параметр Num Outbound Cmds, який характеризує кількість вихідних команд із FTTP–сервера, завжди має одне й те саме значення – 0. У результаті прийнято рішення видалити цей параметр з усіх таблиць, оскільки він лише збільшує тривалість навчання НМ і не несе ніякого смислового значення.

Крім того, сформовано додаткові таблиці з 23 стовпцями для НМ1, у яких лише одна комірка зі значенням 1 (це значення характеризує, до якого класу належить еталон залежно від розташування його в рядку), а інші значення – 0. За таким принципом сформовано додаткові таблиці і для інших НМ, які будуть виявляти атаку (за другим підходом). Наступний крок – це перетворення параметрів, які містили дані типу String, а саме заміна їх на числові коефіцієнти. Причиною такого перетворення є обмеження нейропакета Neural Network Toolbox, ця утиліта не може працювати з даними типу String або Char. До таких параметрів належить: Тип протоколу, Сервіс, Flag. Наприклад, параметр Тип протоколу має три значення, кожному з яких присвоєний числовий коефіцієнт: протоколу Icmp присвоєно значення 0; протоколу Tcp – значення 1; протоколу Udp – значення 2.

Багатошарова нейронна мережа як математичний апарат. Кількість нейронів у прихованому шарі багатошарової НМ можна визначити за відомою формулою, що є наслідком теореми Колмогорова–Арнольда–Хехт–Нильсена:

$$\frac{N_y Q}{1+\log_2(Q)} \le \mathrm{N}_w \le$$

$$\le N_{\mathrm{y}}\left(\frac{Q}{N_{\mathrm{x}}}+1\right)\left(N_{\mathrm{x}}+N_{\mathrm{y}}+1\right)+N_{\mathrm{y}}, \quad (1)$$

де N_y – довжина вихідного сигналу; Q – кількість елементів множини навчальних прикладів; N_w – необхідна кількість синаптичних зв'язків; N_{x} – розмірність вхідного сигналу.

Оцінивши необхідну кількість синаптичних зв'язків, можна розрахувати необхідну кількість нейронів у прихованому шарі (N):

$$N = \frac{N_w}{N_x + N_y}.$$

Для всіх НМ проведено розрахунок мінімальної ($N_{\min}$), середньої (N_{avg}) та максимальної ($N_{\max}$) кількості прихованих нейронів (табл. 4). Як приклад на рис. 2 зображена конфігурація НМ2 за максимальної кількості прихованих

doi: https://doi.org/10.15802/stp2020/208233

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2020, № 3 (87)

нейронів: 41–1–8–4, де 41 – кількість початкових нейронів; 1 – кількість прихованих шарів; 8 – кількість прихованих нейронів; 4 – кількість результуючих нейронів (якщо $Y_1 = 1$, то категорія DoS; якщо $Y_2 = 1$, то категорія Probe; $Y_3 = 1$, то категорія U2R; $Y_4 = 1$, то категорія R2L; інакше $Y_i = 0$, де $i = 1,\ldots,4$).

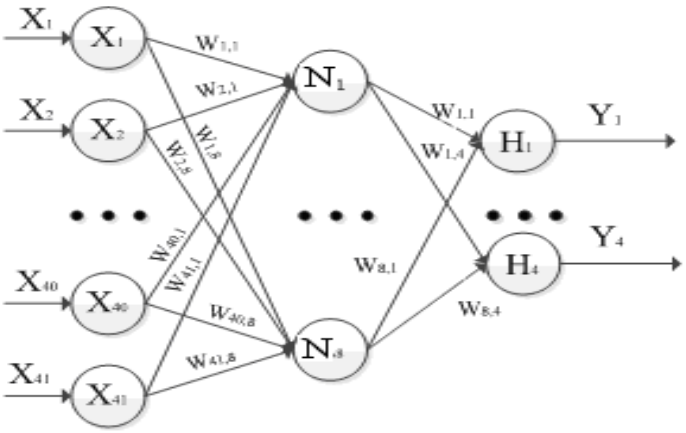

Рис. 2. НМ2 конфігурації 41–1–8–4

Fig. 2. HM2 configurations 41–1–8–4

Дослідження похибки навчання НМ. На створених НМ за допомогою пакета Neural Network Toolbox програми MatLAB проведено дослідження значення MSE від довжини навчальної вибірки за алгоритмами навчання: Levenberg-Marquardt; Bayesian Regularization; Scaled Conjugate Gradient за різної кількості прихованих нейронів ($N_{\min}, N_{avg}, N_{\max}$). Найменше значення похибки навчання завжди надає алгоритм Levenberg–Marquardt, отримані результати подано в табл. 4.

Із таблиці видно, що у всіх випадках достатньо використання мінімальної кількості прихованих нейронів. Так, наприклад, для НМ2 найменше значення MSE досягається за вибірки з 500 навчальних еталонів.

Таблиця 4

Параметри НМ за алгоритмом Levenberg-Marquardt

Table 4

HM parameters according to Levenberg-Marquardt algorithm

НМ	Призначення НМ	Кількість прихованих нейронів			Оптимальна конфігурація НМ	Кількість навчальних еталонів	MSE
		$N_{\min}$	N_{avg}	$N_{\max}$			
НМ1	Виявлення типу атаки	33	313	593	41–1–33–23	7 000	2,71
НМ2	Виявлення категорії класу атаки	8	56	104	41–1–8–4	500	3,79
НМ2–1	Виявлення типу атаки категорії DoS	16	138	259	41–1–16–9	500	3,74
НМ2–2	Виявлення типу атаки категорії Probe	12	84	156	41–1–12–6	400	4,79
НМ2–	Виявлення типу атаки категорії U2R	4	28	52	41–1–4–2	300	1,47
НМ2–4	Виявлення типу атаки категорії R2L	10	70	130	41–1–10–5	400	1,98

doi: https://doi.org/10.15802/stp2020/208233

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2020, № 3 (87)

Результати

Перше дослідження: дослідження часу роботи НМ. Для цього в програмі MatLAB використано функцію tic/toc, яка замірює час роботи коду та зберігає його в секундному значенні. За НМ1 узято конфігурацію 41–1–33–23 з довжиною вибірки із 7 000 прикладів (перший підхід). Для реалізації другого підходу обрано такі конфігурації: 41–1–8–4 (НМ2, 500 еталонів); 41–1–16–9 (НМ2–1, 500 еталонів); 41–1–12–6 (НМ2–2, 400 еталонів); 41–1–4–2 (НМ2–3, 300 еталонів); 41–1–10–5 (НМ2–4, 400 еталонів).

Окрім того, написано скрипт, що працює за таким принципом: у разі визначення певної категорії вхідний вектор передається на ту НМ, яка виявляє клас атаки певної категорії, що була визначена НМ2. Розглянуто три паралельні серії за чотирьох можливих комбінацій виявлення загроз на основі ансамблю НМ, отримані результати зведено до табл. 5. Із таблиці видно, що в середньому виявлення мережних загроз на НМ1 (за першим підходом) складає 2,21 с, за другим підходом – 0,92 с. Тобто використання ансамблю з п’яти НМ швидше приблизно в 2,4 раза.

Таблиця 5

Результати першого дослідження (часу роботи НМ за можливими комбінаціями, с)

Table 5

The results of the first study (HM operating time according to possible combinations, s)

НМ	1 серія				2 серія				3 серія			
	1	2	3	4	5	6	7	8	9	10	11	12
НМ1	2,41	1,97	2,07	1,71	2,00	2,02	2,17	1,99	2,22	2,00	2,10	1,89
НМ2	0,40	0,54	0,54	0,59	0,68	0,67	0,43	0,37	0,58	0,63	0,48	0,48
НМ2–1	0,77	–	–	–	0,77	–	–	–	0,97	–	–	–
НМ2–2	–	0,56	–	–	–	0,28	–	–	–	0,44	–	–
НМ2–3	–	–	0,05	–	–	–	0,06	–	–	–	0,04	–
НМ2–4	–	–	–	0,26	–	–	–	0,22	–	–	–	0,24
Загальний час, с (2-й підхід)	1,17	1,10	0,59	0,85	1,45	0,95	0,49	0,59	1,55	1,07	0,52	0,72

Друге дослідження: дослідження помилки першого роду. Помилка першого роду – це кількість неправильно виявлених атак (FP, False Positive). Результати дослідження помилки першого роду зведено до табл. 6. Із таблиці видно, що помилка першого роду на НМ1 складає 7,39 %, а в разі використання ансамблю нейронних мереж НМ2, НМ2–1, НМ2–2, НМ2–3, НМ2–4 (другий підхід) – 2,17 %.

Третє дослідження: дослідження помилки другого роду. Помилка другого роду – це кількість пропусків атак (FN, False Negative). Результати дослідження помилки другого роду подано в табл. 7. Із таблиці видно, що помилка другого роду на НМ1 складає 6,96 %, а в разі використання ансамблю НМ (другий підхід) – 3,91 %.

doi: https://doi.org/10.15802/stp2020/208233

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2020, № 3 (87)

Таблиця 6

Результати другого дослідження (кількості неправильно виявлених атак)

Table 6

The results of the second study (number of incorrectly detected attacks)

Категорія (клас) атаки	1-й підхід	2-й підхід				
	НМ1	НМ2	НМ2–1	НМ2–2	НМ2–3	НМ2–4
DoS	–	20 зі 900	–	–	–	–
Probe	–	10 зі 600	–	–	–	–
U2R	–	10 зі 200	–	–	–	–
R2L	–	10 зі 500	–	–	–	–
Normal	0 зі 100	0 зі 100	–	–	–	–
Ipsweep	20 зі 100	–	–	0 зі 100	–	–
Satan	10 зі 100	–	–	0 зі 100	–	–
Portsweep	10 зі 100	–	–	0 зі 100	–	–
Nmap	0 зі 100	–	–	10 зі 100	–	–
Saint	20 зі 100	–	–	0 зі 100	–	–
Mscan	20 зі 100	–	–	0 зі 100	–	–
Neptune	20 зі 100	–	0 зі 100	–	–	–
Smurf	0 зі 100	–	10 зі 100	–	–	–
Back	0 зі 100	–	0 зі 100	–	–	–
Teardrop	10 зі 100	–	0 зі 100	–	–	–
Pod	0 зі 100	–	0 зі 100	–	–	–
Land	0 зі 100	–	0 зі 100	–	–	–
Apache2	0 зі 100	–	10 зі 100	–	–	–
Mailbomb	10 зі 100	–	0 зі 100	–	–	–
Processtable	10 зі 100	–	0 зі 100	–	–	–
Buffer_overflow	0 зі 100	–	–	–	10 зі 100	–
Rootkit	20 зі 100	–	–	–	0 зі 100	–
Httptunnel	0 зі 100	–	–	–	–	0 зі 100
Guess_passwd	0 зі 100	–	–	–	–	0 зі 100
Wazemaster	0 зі 100	–	–	–	–	0 зі 100
Multihop	20 зі 100	–	–	–	–	10 зі 100
Warezclient	0 зі 100	–	–	–	–	0 зі 100
Усього:	170 зі 2 300	50 зі 2 300				

doi: https://doi.org/10.15802/stp2020/208233

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2020, № 3 (87)

Таблиця 7

Результати третього дослідження (кількості пропусків атак)

Table 7

The results of the third study (number of missed attacks)

Категорія (клас) атаки	1-й підхід	2-й підхід				
	НМ1	НМ2	НМ2–1	НМ2–2	НМ2–3	НМ2–4
DoS	–	30 зі 900	–	–	–	–
Probe	–	20 зі 600	–	–	–	–
U2R	–	20 зі 200	–	–	–	–
R2L	–	20 зі 500	–	–	–	–
Normal	10 зі 100	0 зі 100	–	10 зі 100	–	–
Ipsweep	0 зі 100	–	–	0 зі 100	–	–
Satan	20 зі 100	–	–	0 зі 100	–	–
Portsweep	0 зі 100	–	–	0 зі 100	–	–
Nmap	10 зі 100	–	–	0 зі 100	–	–
Saint	10 зі 100	–	–	0 зі 100	–	–
Mscan	10 зі 100	–	10 зі 100	–	–	–
Neptune	0 зі 100	–	0 зі 100	–	–	–
Smurf	0 зі 100	–	0 зі 100	–	–	–
Back	10 зі 100	–	0 зі 100	–	–	–
Teardrop	0 зі 100	–	0 зі 100	–	–	–
Pod	0 зі 100	–	0 зі 100	–	–	–
Land	10 зі 100	–	10 зі 100	–	–	–
Apache2	0 зі 100	–	0 зі 100	–	–	–
Mailbomb	10 зі 100	–	0 зі 100	–	–	–
Processtable	0 зі 100	–	0 зі 100	–	–	–
Buffer_overflow	20 зі 100	–	–	–	10 зі 100	–
Rootkit	20 зі 100	–	–	–	0 зі 100	–
Httptunnel	0 зі 100	–	–	–	–	10 зі 100
Guess_passwd	10 зі 100	–	–	–	–	0 зі 100
Wazemaster	0 зі 100	–	–	–	–	0 зі 100
Multihop	0 зі 100	–	–	–	–	0 зі 100
Warezclient	20 зі 100	–	–	–	–	0 зі 100
Усього:	160 зі 2 300	90 зі 2 300				

doi: https://doi.org/10.15802/stp2020/208233

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2020, № 3 (87)

Наукова новизна та практична значимість

У ході проведення експериментів на НМ (рис. 3) отримано такі результати: TP (True Positive); FP (False Positive); FN (False Negative); TN (True Negative), на основі яких на завершальному етапі залишилось дати оцінку якості рішень за різними підходами (табл. 8).

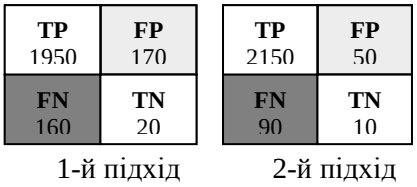

Рис. 3. Результати моделювання

Fig. 3. Simulation results

Таблиця 8

Показники оцінки якості рішень за різними підходами

Table 8

Indicators for assessing the quality of solutions according to different approaches

Показник	TP	FP	FN	TN	TPR	FPR	Accuracy	Precision	Recall
1-й підхід	1950	170	160	20	0,92	0,89	0,86	0,92	0,92
2-й підхід	2150	50	90	10	0,96	0,83	0,94	0,98	0,96

Із таблиці видно, що найкращі результати досягаються на основі використання ансамблю НМ (другий підхід): TPR (показник коректності визначення мережних атак) складає 0,96 (проти 0,92); FPR (показник помилкових спрацьовувань) – 0,83 (проти 0,89); достовірність (Accuracy) – 0,94 (проти 0,86), точність (Precision) – 0,98 (проти 0,92) і повнота (Recall) – 0,96 (проти 0,92) порівнянно з першим підходом на основі НМ1.

Висновки

1. Проведений огляд наукових джерел показав, що для виявлення атак на комп'ютерну мережу можливе використання багатошарового персептрона, самоорганізованої карти та комбінованого підходу. Як математичний апарат для розв'язання поставленої задачі обрано багатошаровий персептрон, як нейрозасіб – пакет Neural Network Toolbox програми MatLAB.

2. Виявлення атак на комп'ютерну мережу здійснено за допомогою двох підходів: використання багатошарової нейронної мережі (НМ1, перший підхід), на вхід якої подається 41 параметр із метою класифікації 22 класів атак; використання ансамблю із п'яти нейронних мереж (НМ2; НМ2–1; НМ2–2; НМ2–3; НМ2–4, другий підхід) для визначення категорії атаки DoS, Probe, U2R чи R2L (на першому етапі) та визначення класу атаки відповідно до категорії (на другому етапі). Для моделювання НМ використовуються нормалізовані дані з відкритої бази NSL–KDD.

3. Проведено дослідження похибки НМ від довжини вибірки за різними алгоритмами навчання: Levenberg–Marquardt, Bayesian Regularization, Scaled Conjugate Gradient за різної кількості прихованих нейронів (мінімальної, середньої та максимальної). Визначено оптимальні параметри НМ. Так, наприклад, найменше значення MSE = 3,79 досягається на НМ2 за 8 прихованих нейронів на вибірці з 400 прикладів за методом Levenberg–Marquardt.

4. На створених НМ за різними підходами проведено такі дослідження: часу роботи (перше дослідження); помилки першого роду (друге дослідження); помилки другого роду (третє дослідження). За результатами першого дослідження в середньому час роботи ансамблю НМ складає 0,92 с, а час НМ1 – 2,21 с, що менше приблизно в 2,4 раза. За результатами другого дослідження помилка першого роду з використанням ансамблю НМ складає 2,17 %, а на НМ1 – 7,39 %, за результатами третього дослідження помилка другого роду з використанням ансамблю НМ складає 3,91 %, а на НМ1 – 6,96 %, що доводить доцільність використання другого підходу.

doi: https://doi.org/10.15802/stp2020/208233

5. На основі отриманих даних дано оцінку якості рішень за різними підходами. Найкращі результати досягаються на основі використання ансамблю НМ (другий підхід): показник коректності визначення мережних атак складає 0,96 (проти 0,92); показник помилкових спрацьовувань – 0,83 (проти 0,89); достовірність – 0,94 (проти 0,86), точність – 0,98 (проти 0,92) і повнота – 0,96 (проти 0,92) порівнянно з першим підходом на основі НМ1.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Крыжановский А. В. Применение искусственных нейронных сетей в системах обнаружения атак. *Доклады ТУСУР*. 2008. № 2 (18). Ч. 1. С. 104–105.
2. Мустафаев А. Г. Нейросетевая система обнаружения компьютерных атак на основе анализа сетевого трафика. *Вопросы безопасности*. 2016. № 2. С. 1–7. DOI: https://doi.org/10.7256.2409-7543.2016.2.18834
3. Тарасов Я. В. Метод определення низкоинтенсивных DDOS-атак на основе гибридной нейронной сети. *Известия ЮФУ : Технические науки.* 2014. № 8. С. 47–48.
4. A Deeper Dive into the NSL-KDD Data Set. URL: https://towardsdatascience.com/a-deeper-dive-into-the-nsl-kdd-data-set-15c753364657 (дата звернення: 14.05.2020).
5. Chaivat J., Naruemon W., Prasert K. *Hybrid Neural Networks for Intrusion Detection System*. 2002. URL: https://www.researchgate.net/publication/266608342 (дата звернення: 14.05.2020).
6. CIC DATASET FORM for «NSL-KDD». URL: http://205.174.165.80/CICDataset/NSL-KDD/Dataset/ (дата звернення: 14.05.2020).
7. Grill M., Pevný T., Rehak M. Reducing false positives of network anomaly detection by local adaptive multivariate smoothing. *Journal of Computer and System Sciences*. 2017. Vol. 83. Iss. 1. P. 43–57. DOI: https://doi.org/10.1016/j.jcss.2016.03.007
8. Gunes K. H., Nur Z.-H. A., Heywood M. I. A hierarchical SOM-based intrusion detection system. *Engineering Applications of Artificial Intelligence*. 2007. Vol. 20. Iss. 4. P. 439–451. DOI: https://doi.org/10.1016/j.engappai.2006.09.005
9. Kruti C., Bhavin S., Ompriya K. Improving user-to-root and remote-to-local attacks using growing hierarchical self organizing map. *International Journal of Engineering Sciences & Research Technology*. 2015. Vol. 4, № 6. P. 611–618
10. *NSL-KDD dataset*. Canadian Institute for Cybersecurity. URL: https://www.unb.ca/cic/datasets/nsl.html (дата звернення: 14.05.2020).
11. Ortiz A. *Improving Network Intrusion Detection with Growing Hierarchical Self-Organizing Maps*. 2011. URL: https://pdfs.semanticscholar.org/f3fb/cf7dfd84d9f2f2ace73580c32eb7c469b6e7.pdf
12. Palomo E. J., Domínguez E., Luque R. M., Muñoz J. *A new GHSOM Model applied to network security*. Springer, Berlin, Heidelberg, 2008. P. 680–689. DOI: https://doi.org/10.1007/978-3-540-87536-9_70
13. Ring M., Wunderlich S., Scheuring D., Landes D., Hotho A. A Survey of Network-based Intrusion Detection Data Sets. *Computers & Security.* 2019. Vol. 86. P. 147–167. DOI: https://doi.org/10.1016/j.cose.2019.06.005
14. Saied A., Overill R. E., Radzik T. Detection of known and unknown DDoS attacks using Artificial Neural Networks. *Neurocomputing*. 2016. Vol. 172. P. 385–393. DOI: https://doi.org/10.1016/j.neucom.2015.04.101
15. Zhukovyts'kyy I. V., Pakhomova V. M. Identifying threats in computer network based on multilayer neural network. *Наука та прогрес транспорту*. 2018. № 2 (74). С. 114–123. DOI: https://doi.org/10.15802/stp2018/130797

В. Н. ПАХОМОВА[1*], М. С. КОННОВ[2*]

[1*]Каф. «Электронные вычислительные машины», Днипровский национальный университет железнодорожного транспорта имени академика В. Лазаряна, ул. Лазаряна, 2, Днипро, Украина, 49010, тел. +38 (056) 373 15 89, эл. почта viknikpakh@gmail.com, ORCID 0000-0002-0022-099X

[2*]Каф. «Электронные вычислительные машины», Днипровский национальный университет железнодорожного транспорта имени академика В. Лазаряна, ул. Лазаряна, 2, Днипро, Украина, 49010, тел. +38 (056) 373 15 89, эл. почта mkonnov1997@gmail.com, ORCID 0000-0001-7212-7631

doi: https://doi.org/10.15802/stp2020/208233

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2020, № 3 (87)

ИССЛЕДОВАНИЕ ДВУХ ПОДХОДОВ К ВЫЯВЛЕНИЮ СЕТЕВЫХ АТАК С ИСПОЛЬЗОВАНИЕМ НЕЙРОСЕТЕВОЙ ТЕХНОЛОГИИ

Цель. На современном этапе чаще всего предлагают системы обнаружения сетевых атак, построенные на основе следующих нейронных сетей: многослойного персептрона, сети Кохонена или самоорганизующейся карты и их комбинаций. В статье предусмотрено исследовать эффективностьь двух подходов к выявлению атак на компьютерную сеть с использованием нейросетевой технологии на основе нормализованных данных открытой базы NSL–KDD. **Методика.** В качестве архитектурного решения системы обнаружения сетевых атак предложено рассмотреть следующие подходы: на основе одной нейронной сети, определяющей класс атаки (первый подход), и ансамбля из пяти нейронных сетей (второй подход), который на первом этапе определяет категорию атаки (DoS, Probe, U2R, R2L), а на втором этапе – класс атаки, относящийся к определенной категории. **Результаты.** На созданных в программе MatLAB нейронных сетях проведено исследование их ошибки от длины выборки по различным алгоритмам обучения: Levenberg–Marquardt; Bayesian Regularization; Scaled Conjugate Gradient – при разном количестве скрытых нейронов (минимальном, среднем и максимальном). Определены оптимальные параметры нейронных сетей для двух подходов. **Научная новизна.** В ходе проведения экспериментов для двух подходов получены результаты: TP (True Positive); FP (False Positive); FN (False Negative); TN (True Negative). На их основе рассчитаны следующие показатели оценки качества решений: корректность определения сетевых атак; ложные срабатывания; достоверность; точность и полнота, что доказывают целесообразность использования ансамбля нейронных сетей (второго подхода). **Практическая значимость.** На созданных нейронных сетях для обоих подходов проведены исследования: времени работы нейронных сетей; ошибки первого рода; ошибки второго рода. По результатам первого исследования в среднем время работы ансамбля нейронных сетей составляет 0,92 с, а время работы нейронной сети (первый подход) достигает 2,21 с. По результатам второго исследования ошибка первого рода на ансамбле нейронных сетей составила 2,17 %, а на нейронной сети (первый подход) – 7,39 %. По результатам третьего исследования ошибка второго рода на ансамбле нейронных сетей составила 3,91 %, а на нейронной сети (первый подход) – 6,96 %, что подтверждает эффективность использования ансамбля нейронных сетей (второй подход).

Ключевые слова: атака; ансамбль; нейронная сеть; ошибка первого рода; ошибка второго рода; достоверность; точность; полнота

V. M. PAKHOMOVA[1*], M. S. KONNOV[2*]

[1*]Dep. «Electronic Computing Machines», Dnipro National University of Railway Transport named after Academician V. Lazaryan, Lazaryana St., 2, Dnipro, Ukraine, 49010, tel. +38 (056) 373 15 89, e-mail viknikpakh@gmail.com, ORCID 0000-0002-0022-099X

[2*]Dep. «Electronic Computing Machines», Dnipro National University of Railway Transport named after Academician V. Lazaryan, Lazaryana St., 2, Dnipro, Ukraine, 49010, tel. +38 (056) 373 15 89, e-mail mkonnov1997@gmail.com, ORCID 0000-0001-7212-7631

RESEARCH OF TWO APPROACHES TO DETECT NETWORK ATTACKS USING NEURAL NETWORK TECHNOLOGIES

Purpose. At the present stage, network attack detection systems based on the following neural networks are most often offered: multilayer perceptron, Kohonen network or self-organizing map and their combinations. The efficiency problem of two approaches to detect attacks on a computer network using neural network technology based on the normalized data of the open NSL-KDD database is considered. **Methodology.** As an architectural solution to the network attack detection system, it is proposed to consider the following approaches: based on one neural network determining the attack class (first approach) and an ensemble of five neural networks (second approach), which at the first stage determines the attack category (DoS, Probe, U2R , R2L), and in the second stage, the attack class belonging to a certain category. **Findings.** Based on the neural networks created in the MatLAB program, a study was conducted of their error on the length of the training sample using various training algorithms: Levenberg-Marquardt; Bayesian Regularization; Scaled Conjugate Gradient with different numbers of hidden neurons (minimum, average and maximum). Certain optimal parameters of neural networks with two approaches were determined. **Originality.** In the course of

doi: https://doi.org/10.15802/stp2020/208233

conducting experiments with various approaches, the results obtained were: TP (True Positive); FP (False Positive); FN (False Negative); TN (True Negative), based on which the following indicators were calculated for assessing the quality of solutions: correct determination of network attacks; false positives; reliability; accuracy and completeness, which prove the feasibility of using an ensemble of neural networks (second approach). **Practical value.** On the created neural networks with various approaches, studies were conducted: the operating time of neural networks; errors of the first kind; errors of the second kind. According to the results of the first study, the average operating time of an ensemble of neural networks is 0.92 s, and the operating time of a neural network (according to the first approach) is 2.21 s. According to the results of the second study, the error of the first kind using an ensemble of neural networks is 2.17%, and using the neural network (the first approach) – 7.39%. According to the results of the third study, the error of the second kind using an ensemble of neural networks is 3.91%, and using the neural network (the first approach) – 6.96%, which is confirmed by the efficiency of using an ensemble of neural networks (second approach).

Keywords: attack; ensemble; neural network; error of the first kind; error of the second kind; reliability; accuracy; completeness

REFERENCES

1. Krjzijzanovsky, A. V. (2008). Application of artificial neural networks in systems of attacks detection. *Doklady TUSUR, 2*(18), 104-105. (in Russian)
2. Mustafaev, A. G. Neyrosetevaya sistema obnaruzheniya kompyuternykh atak na osnove analiza setevogo trafika. *Voprosy bezopasnosti,2*, 1-7. DOI: https://doi.org/10.7256/2409-7543.2016.2.18834 (in Russian)
3. Tarasov, Ya. V. (2014). Metod opredelennya nizkointensivnykh DDOS atak na osnove gibridnoy neyronnoy seti. *Izvestiya sfedu. Engineering sciences, 8,* 47-58. (in Russian)
4. A Deeper Dive into the NSL-KDD Data Set. Retrieved from https://towardsdatascience.com/a-deeper-dive-into-the-nsl-kdd-data-set-15c753364657
5. Chaivat, J., Naruemon, W., & Prasert, K. (2002). *Hybrid Neural Networks for Intrusion Detection System*. Retrieved from https://www.researchgate.net/publication/266608342 (in English)
6. CIC DATASET FORM for «NSL-KDD». Retrieved from http://205.174.165.80/CICDataset/NSL-KDD/Dataset/ (in English)
7. Grill, M., Pevný, T., & Rehak, M. (2017). Reducing false positives of network anomaly detection by local adaptive multivariate smoothing. *Journal of Computer and System Sciences, 83*(1), 43-57. DOI: https://doi.org/10.1016/j.jcss.2016.03.007 (in English)
8. Gunes, K. H., Nur, Z.-H. A., & Heywood, M. I. (2007). A hierarchical SOM-based intrusion detection system. *Engineering Applications of Artificial Intelligence, 83*(1), 439-451. (in English)
9. Kruti, C., Bhavin, S., & Ompriya, K. (2015). Improving user-to-root and remote-to-local attacks using growing hierarchical self organizing map. *International Journal of Engineering Sciences & Research Technology, 4*(6), 611-318. (in English)
10. *NSL-KDD dataset*. Canadian Institute for Cybersecurity. Retrieved from https://www.unb.ca/cic/datasets/nsl.html (in English)
11. Ortiz, A. (2011). *Improving Network Intrusion Detection with Growing Hierarchical Self-Organizing Maps*. Retrieved from https://pdfs.semanticscholar.org/f3fb/cf7dfd84d9f2f2ace73580c32eb7c469b6e7.pdf (in English)
12. Palomo, E. J., Domínguez, E., Luque, R. M., & Muñoz, J. (2008). *A new GHSOM Model applied to network security* (pp. 680-689). Springer Berlin Heidelberg. (in English)
13. Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. (2019). A survey of network-based intrusion detection data sets. *Computers & Security, 86*, 147-167. DOI: https://doi.org/10.1016/j.cose.2019.06.005 (in English)
14. Saied, A., Overill, R. E., & Radzik, T. (2016). Detection of known and unknown DDoS attacks using Artificial Neural Networks. *Neurocomputing, 172*, 385-393. DOI: https://doi.org/10.1016/j.neucom.2015.04.101 (in English)
15. Zhukovyts'kyy, I. V., & Pakhomova, V. M. (2018). Identifying threats in computer network based on multilayer neural network. *Science and Transport Progress*, *2*(74), 114-123. DOI: https://doi.org/10.15802/stp2018/130797 (in English)

Надійшла до редколегії: 21.01.2020
Прийнята до друку: 21.05.2020

doi: https://doi.org/10.15802/stp2020/208233