УДК 004.056.53:[004.7:004.032.26] https://doi.org/10.35546/kntu2078-4481.2023.2.28

В. М. ПАХОМОВА
кандидат технічних наук, доцент,
доцент кафедри електронних обчислювальних машин
Український державний університет науки і технологій
ORCID: 0000-0002-0022-099x

О. О. СУХОМЛИН
аспірант кафедри електронних обчислювальних машин
Український державний університет науки і технологій
ORCID: 0009-0006-7928-4721

ДОСЛІДЖЕННЯ САМООРГАНІЗУЮЧОЇ КАРТИ КОХОНЕНА ЩОДО ВИЯВЛЕННЯ МЕРЕЖЕВИХ АТАК КАТЕГОРІЇ R2L

У даній роботі виконано дослідження можливості самоорганізуючої карти Кохонена щодо виявлення мережевих атак категорії R2L.

Для виявлення атак категорії R2L відповідно до наступних мережевих класів: Ftp_write; Guess_passwd; Imap; Multihop; Phf; Spy; Warezclient та Warezmaster запропоновано самоорганізуючу карту Кохонена конфігурації 41-1-X-9, де 41 – кількість нейронів першого шару (параметри мережевого трафіку на основі використання бази даних NSL-KDD); 1 – кількість прихованих шарів (шар Кохонена); X – кількість прихованих нейронів; 9 – кількість нейронів результуючого шару. Для виявлення мережевих атак категорії R2L створено з використання мови Python програмну модель «SOM_R2L», що заснована на реалізації запропонованої конфігурації самоорганізуючої карти Кохонена та використанні її алгоритму. На створеній програмній моделі «SOM_R2L» проведено дослідження точності на різних картах (5×5, 10×10, 20×20, 30×30) при різній кількості прикладів на кожен клас (5, 10, 15, 20) за різною кількістю епох навчання (20, 40, 60, 80, 100, 200). Визначено оптимальну конфігурацію самоорганізуючої карти Кохонена: 10×10, що навчалася упродовж 40 епох на вибірці із 900 прикладів (по 10 прикладів на клас). На створеній програмній моделі «SOM_R2L» проведено дослідження параметрів якості виявлення атак категорії R2L. Визначені значення помилок другого роду для мережевих класів атак категорії R2L: Ftp_write – 1,11 %; Guess_passwd – 17,78 %; Imap – 1,11 %; Multihop – 4,44 %; Phf – 0 %; Spy – 1,11 %; Warezclient – 2,22 %; Warezmaster – 14,44 %; Normal – 5,56 %.

Ключові слова: *атака, клас, R2L, самоорганізуюча карта, шар Кохонена, вибірка, епоха, точність, якість, помилка другого роду.*

V. M. PAKHOMOVA
Candidate of Technical Sciences, Associate Professor,
Associate Professor at the Department of Electronic Computers
Ukrainian State University of Science and Technology
ORCID: 0000-0002-0022-099x

O. O. SUKHOMLYN
Postgraduate Student at the Department of Electronic Computers
Ukrainian State University of Science and Technology
ORCID: 0009-0006-7928-4721

INVESTIGATION OF SELF-ORGANIZING KOHONEN MAP TO DETECT NETWORK ATTACKS OF R2L CATEGORY

In this work, the possibility of self-organizing Kohonen map to detect network attacks of R2L category is investigated.

To detect attacks of the R2L category according to the following network classes: Ftp_write; Guess_passwd; Imap; Multihop; Phf; Spy; Warezclient and Warezmaster proposed a self-organizing Kohonen map of configuration 41-1-X-9, where 41 – the number of neurons of the first layer (network traffic parameters based on the use of the NSL-KDD database); 1 – number of hidden layers (Kohonen layer); X – number of hidden neurons; 9 – number of neurons of the resulting layer. To detect network attacks of the R2L category, the software model "SOM_R2L" was created using the Python language, which is based on the implementation of the proposed configuration of the self-organizing Kohonen map and the use of its algorithm. On the created software model "SOM_R2L", accuracy studies were conducted on different maps (5×5, 10×10, 20×20, 30×30) with a different number of examples for each class (5, 10, 15, 20) for different numbers of epochs of study (20, 40, 60, 80, 100, 200). The optimal configuration of the self-organizing Kohonen map was determined: 10×10, which was studied for 40 epochs on a sample of 900 examples (10 examples per class). On

the created software model "SOM_R2L", a study of the quality parameters of detection of attacks of the R2L category was carried out. The values of errors of the second kind are determined for the following network attack classes of R2L: Ftp_write – 1,11 %; Guess_passwd – 17,78 %; Imap – 1,11 %; Multihop – 4,44 %; Phf – 0 %; Spy – 1,11 %; Warezclient – 2,22 %; Warezmaster – 14,44 %; Normal – 5,56 %.

Key words: *attack, class, R2L, self-organizing map, Kohonen layer, sampling, era, accuracy, quality, error of the second kind.*

Постановка проблеми

Наявність і постійний ріст загроз мережевих атак у режимі реального часу створюють необхідність розробки ефективної системи виявлення таких атак. Існуючі методи не завжди здатні виявити нові, раніше невідомі атаки, що створює ризик для безпеки комп'ютерних мереж. Перспективним напрямком у створенні систем виявлення мережевих атак, які повинні ґрунтуватися на адаптивних алгоритмах здатних до самонавчання, є застосування нейромережної технології.

Аналіз останніх досліджень та публікацій

На сучасному етапі для виявлення мережевих атак найчастіше використовуються наступні нейронні мережі (НМ): багатошаровий персептрон (Multi Layer Perceptron, MLP); радіально-базисна мережа (Radial Basis Function Network, RBF) та самоорганізуюча карта Кохонена (Self Organizing Map, SOM). Відомо, що різні різновиди НМ з використанням різноманітних математичних апаратів, можуть неоднаково виявляти різні мережеві атаки наступних категорій: DoS; PROBE; U2R; R2L. З одного боку, для виявлення мережевих атак категорії R2L авторами були використані MLP та RBF, однак властивості SOM [2–3, 7] дозволяють його також використати, щоб підсилити визначення атак на основі комбінованих варіантів. З іншого боку, авторами створювалася самоорганізуюча карта Кохонена для виявлення мережевих атак інших категорій [1, 6], але разом з тим важливим недоліком таких методик є відсутність універсальності їх застосування.

Формулювання мети дослідження

Проведені дослідження ставили за мету розвиток методики виявлення мережевих атак категорії R2L. Для досягнення поставленої мети вирішувалися наступні задачі: розробити методику виявлення мережевих атак засобами самоорганізуючої карти Кохонена; при виконанні машинного навчанні виявити оптимальну конфігурацію самоорганізуючої карти Кохонена, що забезпечить достатньо високий рівень достовірності виявлення вторгнень в комп'ютерну мережу; оцінити помилки першого та другого роду при виявленні мережевих атак категорії R2L на створеній карті Кохонена.

Викладення основного матеріалу дослідження

Категорія R2L мережевих атак характеризуються отриманням доступу незареєстрованого користувача до комп'ютера з боку віддаленого комп'ютера. До категорії R2L надходять наступні мережеві класи атак [4]: Ftp_write – віддалений користувач FTP додає себе у список довірених хостів віддаленого комп'ютера, які можуть входити у систему; Guess_passwd – мережевих атак, де зловмисник намагається вгадати або перебрати пароль для отримання доступу до локальної системи з використанням віддаленого доступу; Imap – віддалене переповнення буфера за допомогою порту imap призводить до можливості відкриття віддаленого root_shell; Multihop – багатоденний сценарій, у якому користувач спочатку проникає в одну машину; Phf – сценарій, який дозволяє клієнту виконувати довільні команди на машині з неправильно налаштованим веб-сервером; Spy – багатоденний сценарій, коли користувач проникає в машину з метою пошуку важливої інформації, але користувач намагається уникнути виявлення, використовує кілька різних методів експлойту для отримання доступу; Warezclient – користувачі, які завантажують нелегальне програмне забезпечення, яке раніше опубліковано через анонімний FTP майстром розробки; Warezmaster – анонімне завантаження на FTP-сервер Warez (нелегальних копій авторського програмного забезпечення) на FTP-сервер.

Самоорганізуюча карта Кохонена – це нейронна мережа, що використовується для зображення та дослідження структури результуючих даних на основі двовимірної решітки (карти). Кожен нейрон на карті пов'язаний з вектором ваги, який ініціалізується випадковим чином, а під час навчання ваги оновлюються, щоб нейрони відповідали певним частинам вхідного простору. Навчання SOM складається з двох етапів: пошуку найближчого нейрона (Best Matching Unit, BMU) та оновлення ваги нейронів у топологічній сусідній області BMU.

Для виявлення мережевих атак категорії R2L пропонується використання самоорганізуючої карти Кохонена конфігурації 41-1-X-9, де 41 – кількість нейронів першого шару (параметри мережевого трафіку на основі використання бази даних NSL-KDD [5], табл. 1); 1 – кількість прихованих шарів (шар Кохонена); X – кількість прихованих нейронів, що досліджується; 9 – кількість нейронів результуючого шару.

У якості проміжного шару використано двовимірний масив нейронів R, розмірність *n* якого визначається експериментально. Алгоритм роботи SOM Кохонена може бути описано наступним чином [3]: ініціалізація (створення двовимірної карти нейронів з випадковими початковими вагами); випадковий вибір вхідного вектору; пошук найближчого нейрона BMU (обчислення відстані між вхідним вектором і векторами ваги всіх нейронів на

карті); оновлення ваги (ваги BMU та його сусідніх нейронів оновлюються, щоб підкреслити схожість між ними); оновлення сусідів, окрім BMU (оновлюються також нейрони, які знаходяться в топологічній сусідній області BMU); повторення (кроки 2–5 повторюються для кожного вхідного вектора у навчальному наборі даних протягом декількох епох); кінцева карта (після завершення навчання отримуємо кінцеву карту, де нейрони групуються в залежності від схожості їх векторів ваги).

Таблиця 1

Нейрони першого шару НМ

Нейрон	Параметр	Нейрон	Параметр
x1	duration	x22	is_guest_login
x2	protocol_type	x23	count
x3	service	x24	srv_count
x4	flag	x25	serror_rate
x5	src_bytes	x26	srv_serror_rate
x6	dst_bytes	x27	rerror_rate
x7	land	x28	srv_rerror_rate
x8	wrong_fragment	x29	same_srv_rate
x9	urgent	x30	diff_srv_rate
x10	hot	x31	srv_diff_host_rate
x11	num_failed_logins	x32	dst_host_count
x12	logged_in	x33	dst_host_srv_count
x13	num_compromised	x34	dst_host_same_srv_rate
x14	root_shell	x35	dst_host_diff_srv_rate
x15	su_attempted	x36	dst_host_same_src_port_rate
x16	num_root	x37	dst_host_srv_diff_host_rate
x17	num_file_creations	x38	dst_host_serror_rate
x18	num_shells	x39	dst_host_srv_serror_rate
x19	num_access_files	x40	dst_host_rerror_rate
x20	num_outbound_cmds	x41	dst_host_srv_rerror_rate
x21	is_host_login		

Співвідношення нейронів результуючого шару самоорганізуючої карти Кохонена, структура якої показана на рис. 1, до мережевих класів атак категорії R2L показано в табл. 2.

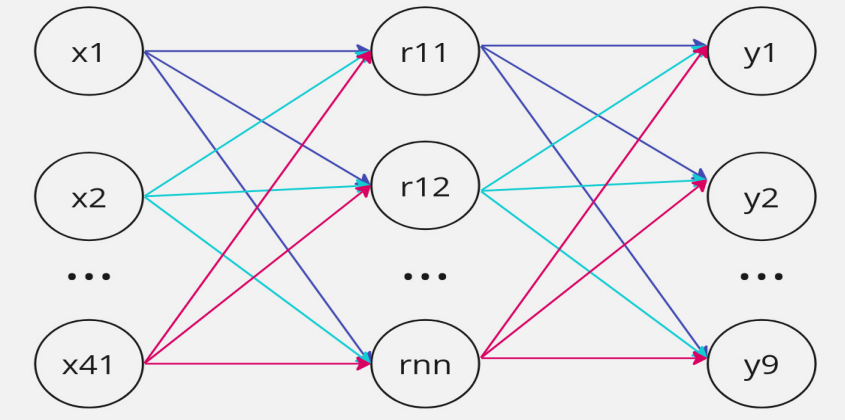

Рис. 1. Самоорганізуюча карта Кохонена конфігурації 41-1-X-9

Таблиця 2

Нейрони результуючого шару НМ

Нейрон	Параметр	Нейрон	Параметр
y1	Ftp_write	y6	Spy
y2	Guess_passwd	y7	Warezclient
y3	Imap	y8	Warezmaster
y4	Multihop	y9	відсутність атаки
y5	Phf		

Для виявлення атак категорії R2L створено мовою Python програмну модель «SOM_R2L», в основі якої закладено запропоновану конфігурацію мережі Кохонена та розглянутий алгоритм її роботи. Структура програмної моделі «SOM_R2L», що представлена на рис. 2, потребує використання стандартних складових: MiniSom; Numpy; Matplotlib; JobLib; Pandas.

Через недостатню кількість прикладів на кожний мережевий клас формування вибірки виконувалось штучно. У якості прикладу наведений фрагмент навчальної вибірки:

44, 1, 18, 10, 55, 9609, 0, 0, 0, 2, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 2, 0.0, 0.0, 0.0, 0.0, 1.0, 0.0, 0.89, 217, 71, 0.57, 0.04, 0.17, 0.48, 0.24, 0.0, 0.01, 0.0, ftp_write

0, 1, 59, 3, 126, 179, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 2, 0.00, 0.00, 1.00, 1.00, 1.00, 0.00, 0.00, 16, 16, 1.00, 0.00, 0.06, 0.00, 0.06, 0.06, 0.94, 0.94, guess_passwd

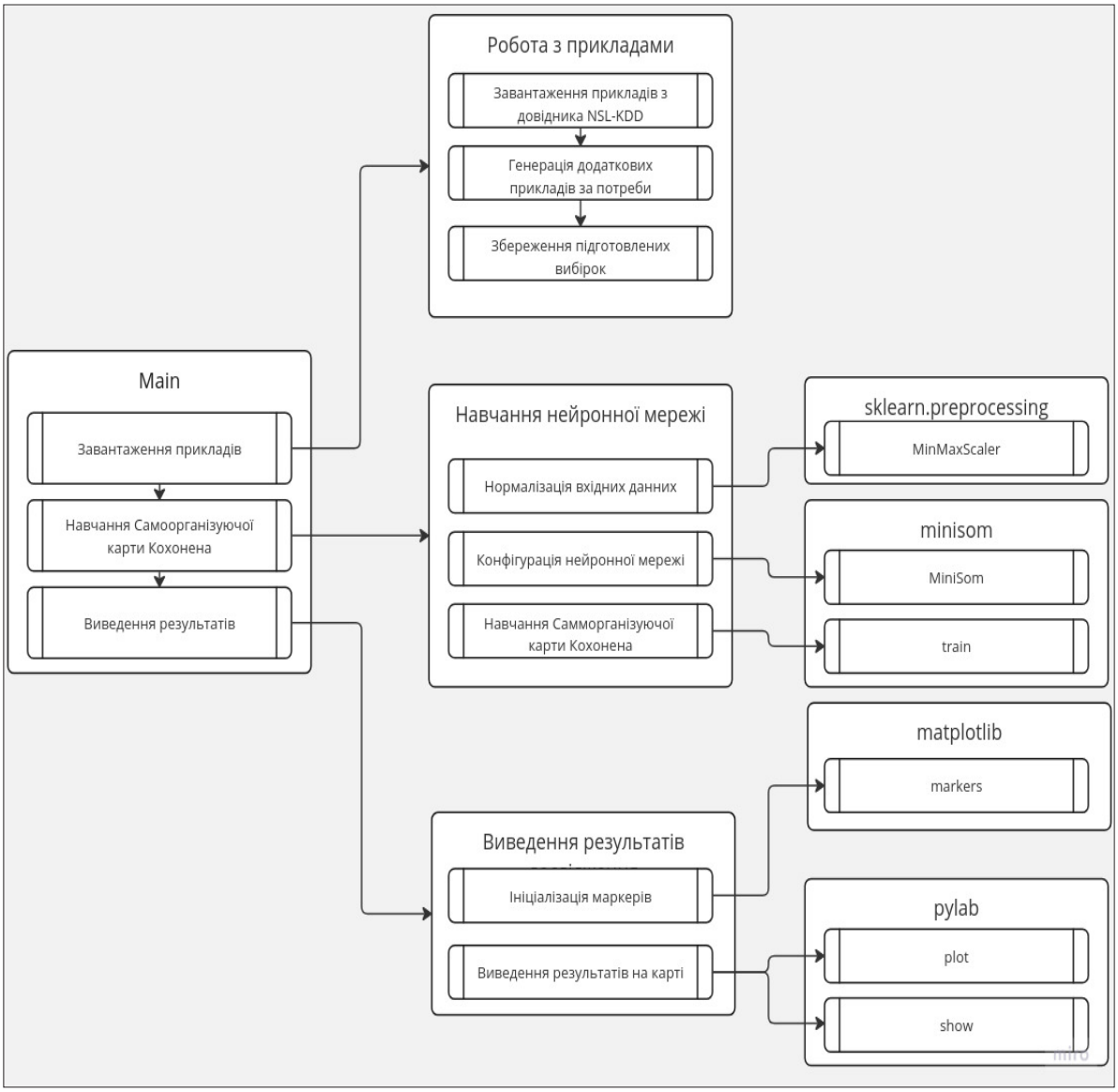

Рис. 2. Структура створеного програмної моделі «SOM_R2L»

На створеній програмній моделі «SOM_R2L» проведено дослідження точності нейронної мережі на різних картах (5×5, 10×10, 20×20, 30×30) при різній кількості прикладів на кожен клас (5, 10, 15, 20) за різною кількістю епох навчання (20, 40, 60, 80, 100, 200). Визначено оптимальну конфігурацію самоорганізуючої карти Кохонена: 10×10, що навчалася упродовж 40 епох на вибірці із 900 прикладів (по 10 прикладів на клас); рис. 3.

У результаті дослідження виявилося, що найкращі результати точності визначення на тестовій вибірці надає конфігурація прихованого шару у 10×10 нейронів. Далі необхідно дослідити точність при конфігурації SOM з розміром карти 10×10, в залежності від кількості ітерацій; рис. 4.

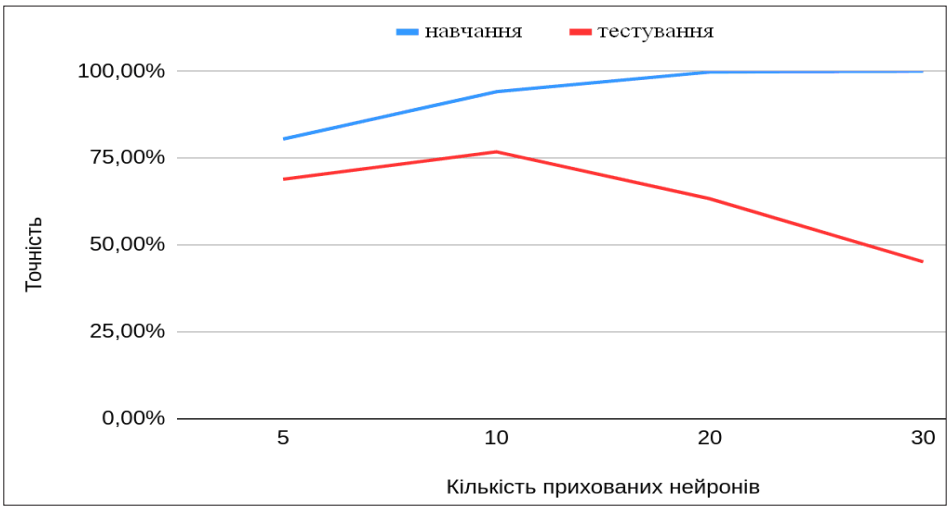

Рис. 3. Точність НМ за різною кількістю прихованих нейронів

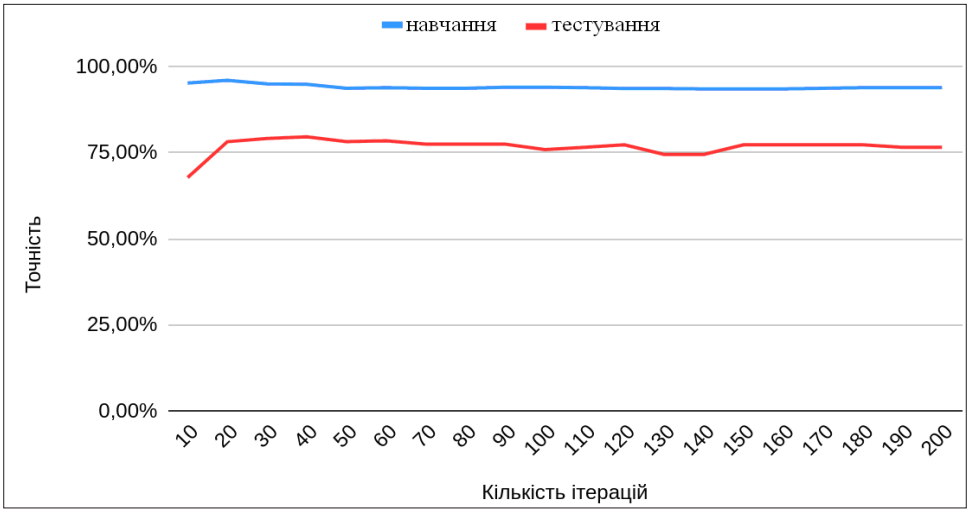

Рис. 4. Точність НМ (карта 10×10) за кількістю ітерацій

У результаті дослідження, що проведено на створеній програмній моделі «SOM_R2L», визначено оптимальну конфігурацію SOM Кохонена: 10×10, яка навчається впродовж 40 ітерацій на вибірці із 900 прикладів (по 10 прикладів на кожен клас) та надала точність у 93 % та 89 % на навчальній та тестовій вибірках відповідно. Результати програмної моделі «SOM_R2L» можна побачити на рис. 5.

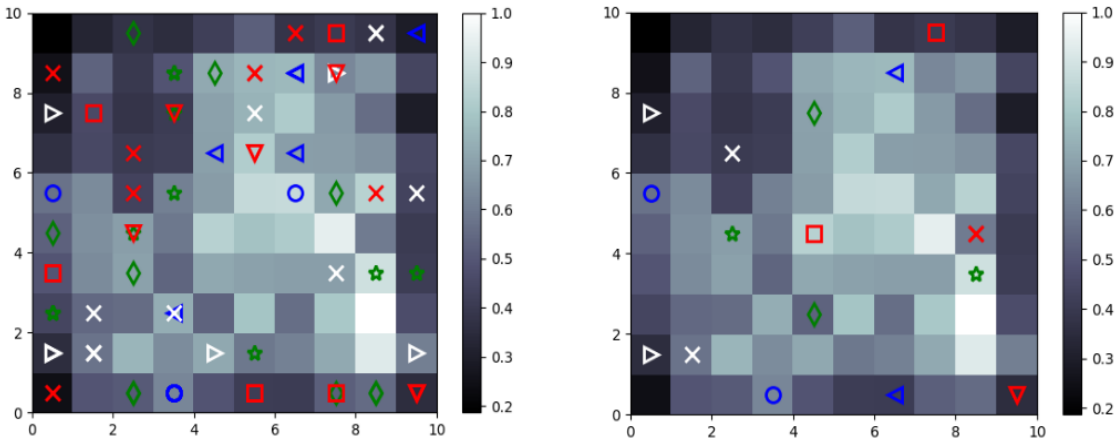

Рис. 5. Результати навчання та тестування НМ на створеній моделі

Для виявлення мережевих класів категорії R2L використані наступні умовні позначення (див. рис. 6): «хрест» (білого кольору) – Normal; «хрест» (червоного кольору) – Ftp_write; «коло» (синього кольору) – Guess_passwd; «ромб» (зеленого кольору) – Imap; «зірка» (зеленого кольору) – Multihop; «квадрат» (червоного кольору) – Phf; «трикутник» (синього кольору) – Spy; «трикутник» (білого кольору) – Warezclient; «трикутник» (червоного кольору) – Warezmaster.

На створеній програмній моделі «SOM_R2L» проведено дослідження якості виявлення мережевих атак категорії R2L за наступними показниками**:** TP (True Positive) – модель коректно розпізнала вхідну послідовність до розглядаємого класу; TN (True Negative) – модель коректно розпізнала, що вхідна послідовність не належить до розглядаємого класу; FP (False Positive) – модель неправильно визначила, що вхідна послідовність належить до розглядаємого класу; FN (False Negative) – модель неправильно визначила, що об'єкт не належить до розглядаємого класу. Результати цього дослідження зведені до табл. 3.

TPR (True Positive Rate) – показує пропорцію визначених послідовностей розглядаємого класу; FPR (False Positive Rate) – показує пропорцію неправильно визначених вхідних послідовностей до розглядаємого класу; Precision – показує частку об'єктів класу серед об'єктів, виділених класифікатором; Recall – показує частку знайдених об'єктів класу в загальній кількості об'єктів класу; F-measure – це середнє гармонічне значення між точністю та повнотою.

Таблиця 3

Результати дослідження на створеній моделі «SOM_R2L»

	TP	FP	TN	FN	TP, %	FP, %	TN, %	FN, %
Ftp_write	2	19	68	1	2,22	21,11	75,56	1,11
Guess_passwd	0	0	74	16	0,00	0,00	82,22	17,78
Imap	4	0	85	1	4,44	0,00	94,44	1,11
Multihop	8	14	64	4	8,89	15,56	71,11	4,44
Phf	4	1	85	0	4,44	1,11	94,44	0
Spy	1	0	88	1	1,11	0,00	97,78	1,11
Warezclient	14	4	70	2	15,56	4,44	77,78	2,22
Warezmaster	3	2	72	13	3,33	2,22	80,00	14,44
Normal	11	3	71	5	12,22	3,33	78,89	5,56

Із таблиці видно, що найбільша кількість помилок другого роду склала 17,78 % при виявленні атак Guess_ passwd на створеній програмній моделі. Обчислені значення інших параметрів якості зведені до табл. 4.

Таблиця 4

Параметри оцінки якості виявлення атак на моделі «SOM_R2L», %

	Precission	Recall	F-measure	TPR	FPR
Ftp_write	10,00	67,00	17,00	66,67	21,84
Guess_passwd	0,00	0,00	0,00	0,00	0,00
Imap	100,00	80,00	89,00	80,00	0,00
Multihop	36,00	67,00	47,00	66,67	17,95
Normal	79,00	69,00	73,00	100,00	1,16
Phf	80,00	100,00	89,00	50,00	0,00
Spy	100,00	50,00	67,00	87,50	5,41
Warezclient	78,00	88,00	82,00	18,75	2,70
Warezmaster	60,00	19,00	29,00	68,75	4,05

Створена програмна модель «SOM_R2L» добре розпізнає мережеві атаки класу Imap та Phf із точністю 98,89 %, але вона погано виконує розпізнавання мережевих атак класу Ftp_write, точність якого склала 77,78 %.

Висновки

Для виявлення мережевих атак категорії R2L запропоновано самоорганізуючу карту Кохонена 41-1-X-9, де 41 – кількість нейронів першого шару; 1 – кількість прихованих шарів (шар Кохонена); X – кількість прихованих нейронів; 9 – кількість нейронів результуючого шару. Для виявлення мережевих атак категорії R2L створено з використання мови Python програмну модель «SOM_R2L», що заснована на реалізації запропонованої конфігурації самоорганізуючої карти Кохонена та її алгоритму. На моделі «SOM_R2L» проведено дослідження точності на різних картах при різній кількості прикладів на кожен клас за різною кількістю епох навчання. Визначено оптимальну конфігурацію SOM: 10×10, що навчалася упродовж 40 епох на вибірці із 900 прикладів. На моделі «SOM_R2L» проведено дослідження параметрів якості виявлення атак категорії R2L.

Список використаної літератури

1. Пахомова В. М., Павленко І. І. Дослідження параметрів якості визначення мережевих атак категорії PROBE з використанням самоорганізуючої карти. *SworldJournal*. 2022. Issue 11. Part 1. pp. 100–104. DOI: 10.30888/2663-5712 .2022-11-01-022

2. Esteban J. A New GHSOM Model applied to network security. *Artificial Neural Networks*-ICANN 2008. 2008. pp. 680-689.

3. Kohonen T. The self-organizing map. Proceedings of the IEEE. № 78(9). 1990. pp. 1464–1480.

4. Lincoln Laboratory. Massachusetts Institute of Technology. Publications Archive. URL: https://archive.ll.mit.edu/ideval/docs/detections_1999.html

5. NSL-KDD dataset. URL: https://www.unb.ca/cic/datasets/nsl.html

6. Pakhomova V., Mehelbei Y. Detection of attacks of the U2R category by means of the SOM on database NSL-KDD. *Системні технології.* Вип. 5 (142). Дніпро. 2022. С. 18–26. URL: https://journals.nmetau.edu.ua/index.php/st/issue/view/126/99

7. Zhukovitsky I., Pakhomova V., Tsykalo I., Bikovska D. Study of possibilities of combined approach to detecting network attacks using artificial intelligence mechanisms // The 12th International Conference on Dependable Systems, Services and Technologies *(DESSERT*: 9–11 December 2022).

References

1. Pakhomova, V. M., & Pavlenko, I. I. (2022) Research of parameters of quality of definition of network attacks of the PROBE category with use of the Self organizing Map. *SworldJournal*, 11, 1, 100–104. DOI: 10.30888/2663-5712.2022-11-01-022 [in Ukrainian].

2. Esteban, J. (2008) A New GHSOM Model applied to network security. *Artificial Neural Networks*-ICANN. pp. 680–689. [in English].

3. Kohonen, T. The self-organizing map (1990) *Proceedings of the IEEE*, 78(9), 1464–1480. [in English].

4. Lincoln Laboratory. Massachusetts Institute of Technology. *Publications Archive*. URL: https://archive.ll.mit.edu/ideval/docs/detections_1999.html

5. NSL-KDD dataset. URL: https://www.unb.ca/cic/datasets/nsl.html

6. Pakhomova, V., & Mehelbei, Y. (2022) Detection of attacks of the U2R category by means of the SOM on database NSL-KDD. *System Technologies,* 5(142), 18–26. URL: https://journals.nmetau.edu.ua/index.php/st/issue/view/126/99 [in English].

7. Zhukovitsky, I., Pakhomova, V., Tsykalo, I., & Bikovska, D. (2022) Study of possibilities of combined approach to detecting network attacks using artificial intelligence mechanisms // The 12th International Conference on Dependable Systems, Services and Technologies *(DESSERT*). [in English].