УДК 004.056

В.С. Мідзяєв
Н.Р.Кондратенко

ЗАСІБ ВИЯВЛЕННЯ АНОМАЛІЙ ФУНКЦІОНУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ДЛЯ ІДЕНТИФІКАЦІЇ DDOS-АТАК. МОДУЛЬ ВИЯВЛЕННЯ АНОМАЛІЙ НА ОСНОВІ ТЕХНОЛОГІЇ САМООРГАНІЗАЦІЇ

Вінницький національний технічний університет

Анотація
У роботі здійснено аналіз і обґрунтування вибір для реалізації модуля виявлення атак на основі технології самоорганізації. Розроблено математичну модель.
Ключові слова: трафік, кластер, самоорганізована мережа, нейромережа, математична модель.

Abstract
The paper analyzes the selection and justification to implement intrusion detection module-based self-organization. The mathematical model.
Keywords: traffic cluster, self-organizing network, neural network, mathematical model**.**

Вступ

Невпинне розширення інформаційної сфери призводить до того, що підвищує ризики виникнення різних атак. Не зважаючи на широкі технологічні можливості повністю захиститися від таких атак не можливо [1].

Однією з технологій захисту є нейронні мережі. Вони базується на навчанні, яке реалізується багатьма способами. Гарні показники навчання гарантує мережа Кохонена, що базуються на самоорганізації (самонавчанні) [2-4].

Результати досліджень

Структурна схема поєднує в собі 4 головних блоки: обробки і завантеження вхідних даних, передачі даних до мережі Кохонена, передача даних до мережі PNN, отримання вихідних даних. Предтавимо структурну схему програмного засобу.

Для захисту комп'ютерної мережі підприємства було вирішено розробити систему захисту на основі саоорганізованих карт Кохонена.

Для навчання мережі необхідно задати початкові дані.

Коли мережа побудована, невідомий екземпляр подається на вхід мережі і в результаті прямого проходу через мережу вихідний шар покаже клас до якого ймовірнішого усього належить зразок.

Зображено структуру мережі Кохонена та мережі де підключена ймовірнісна мережа PNN (рис.1.1).

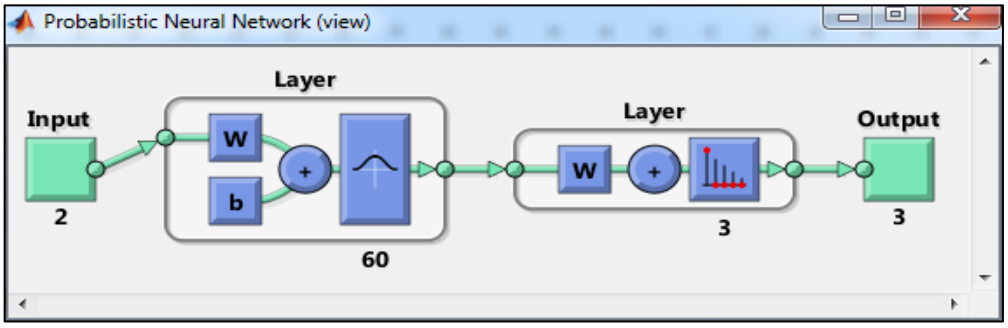

Рисунок 1.3 - Структура мережі Кохонена та PNN

Засіб захисту буде включати в себе 2 входи (поточний час експеремента, кількість запитів до бази даних) та на виході 3 кластери (зелений, жовтий, червоний).

Поточний час буде розраховуватись з початку роботи системи кожного дня, а кількість запитів буде надаватись за кожну хвилину роботи. По завершеню дня, навчена мережа буде переходити на наступний, а час скидуватись на початковий (для вивільнення пам'яті). Таким чином ми буде мати актуальну навчену нейронну мережу кожного дня.

До зеленого кластеру будуть відноситися значення. Що характеризують мережу,при якій аномалія не виявлення, тобто мережа працює у звичайному режимі.

До жовтого кластеру будуть відноситися значення, які виявляють певну аномалію, але вони не є критичними. Сам експерт вирішує яке рішення приймати, адже це може бути. Наприклад, святковий день і така активність буде нормальною. Але для звичайного повсякденного використання таке значення матиме вигляд аномалії. І рішення прийматиметься експертом, адже це може слугувати початком атаки на мережу.

До червоного кластеру будуть відноситись значення. Які є аномальними у будь якому випадку, що можна сказати - аномалія дійсно є і потрібно приймати рішення.

Результати досліджень наведено на рис.1.2.

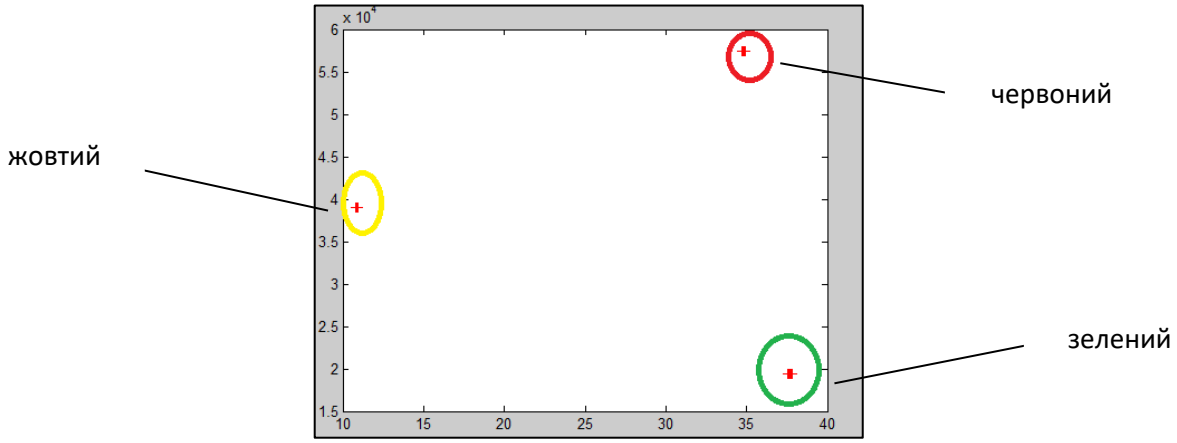

Рисунок 1.2 – Графічне подання результатів виконання моделювання

Висновки

Було виконано розробку математичної моделі виявлення аномалій на основі технології самоорганізації з детальним описом її складових. Виконано дослідження нейромережевого підходу його архітектури та задач які такий підхід дозволяє вирішити.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Штучні нейронні мережі. мережа Кохонена. [Електрронний ресурс]. – Режим доступу: URL: http://www.uatur.com/html/neural_nets/. – Назва з екрану.

2. Котенко И.В. Перспективные направления исследований в области компьютерной безопасности /И.В. Котенко, Р.М. Юсупов // Защита информации. Инсайд. 2006. – № 2. – 57с.

3. Рудик І.І. Виявлення аномалій в комп'ютерній мережі на основі нейромережевих технологій – Штучний інтелект – 2002 - №2 – С. 151-155.

4.Нейронные сети. Сеть Кохонена [Електрронний ресурс]. – Режим доступу:URL:http://www.statsoft.ru/home/textbook/modules/stneunet.html#kohonen – Назва з екрану.

Мідзяєв Вадим Сергійович – студент групи 1БС-16м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, Україна, e-mail: vadim14121993@gmail.com

Науковий керівник Кондратенко Наталя Романівна - канд. техн. наук, професор кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, Україна.

Midzyayev Vadim - student group 1BS-16m, Department of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, Ukraine, e-mail: vadim14121993@gmail.com

Kondratenko Natalia - candidate. Sc. , professor of information security, Vinnytsia National Technical University. Vinnitsa, Ukraine.