ТЕХНІЧНІ НАУКИ

Бовкун І.К.
студент,
Науковий керівник: **Шматко О.В.**
кандидат технічних наук, доцент,
Харківський національний університет радіоелектроніки

АВТОМАТИЗАЦІЯ ДОСЛІДЖЕННЯ ТА ВИЯВЛЕННЯ ВТОРГНЕНЬ В КОМП'ЮТЕРНІ МЕРЕЖІ

В даний час інформаційні технології проникли практично в усі сфери життя сучасного суспільства. Причиною такого інтенсивного розвитку інформаційних технологій є зростаюча потреба у швидкій і якісній обробці інформації, моментальної передачі інформації в різні куточки світу. У зв'язку з цим, одним із головних завдань є забезпечення безпеки інформації, яка передається або обробляється в мережі, захист від мережевих атак. На даний момент все більшого значення набувають комплексні системи захисту інформації. Як компоненти такої системи виступають системи антивірусного захисту, системи контролю цілісності, міжмережеві екрани, засоби аналізу вразливостей, системи виявлення та запобігання вторгнень і т.д. Системи виявлення й запобігання вторгнень, або, як їх ще називають, засоби виявлення атак, є саме тим механізмом захисту мережі, на який покладено функції захисту від мережевих атак.

Існує велика кількість методів для визначення мережевих атак, але оскільки атаки постійно змінюються спеціальні бази даних з правилами або сигнатурами для виявлення атак потребують безперервного адміністрування, виникає необхідність додавати нові правила. Одним із шляхів усунення даної проблеми є використання нейронних мережі в якості механізму для виявлення мережевих атак. На відміну від сигнатурного підходу, нейронна мережа проводить аналіз інформації та надає інформацію про атаки, які вона навчена розпізнавати. Крім цього, нейронні мережі мають перевагу – вони здатні адаптуватися до раніше невідомих атак і виявляти їх. Саме тому розробка програмного забезпечення на основі нейронних мереж є актуальною.

Нейронні мережі – це один з напрямків досліджень в області штучного інтелекту, заснований на спробах відтворити нервову систему людини, а саме здатність нервової системи навчатися і виправляти помилки, що має дозволити змоделювати, хоча і досить грубо, роботу людського мозку [1].

Багатошарова нейронна мережа включає в себе вхідний, вихідний та приховані шари (рис. 1).

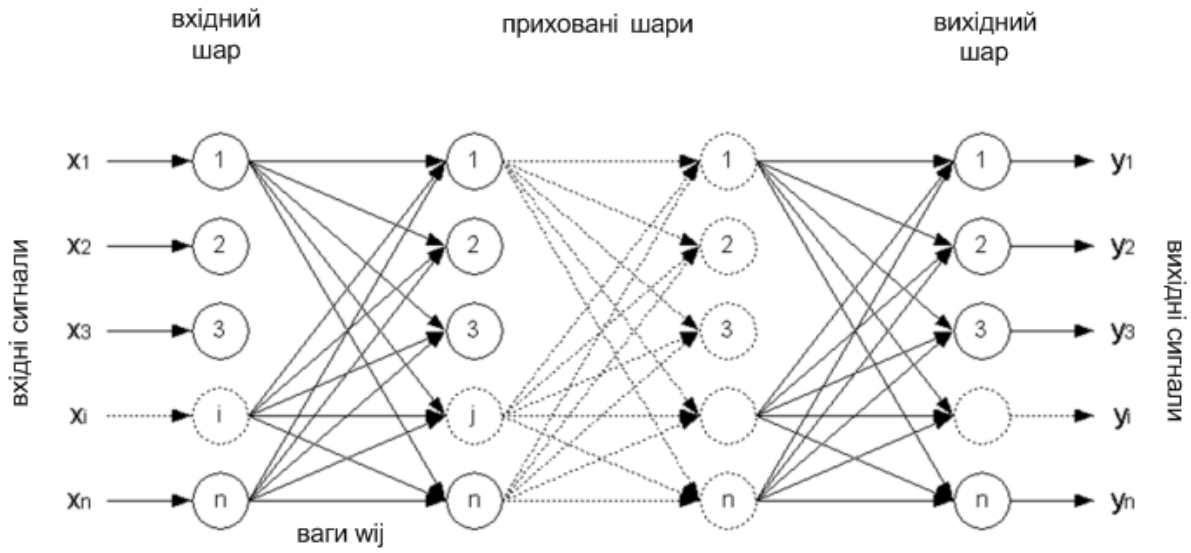

Рис. 1. Багатошарова нейронна мережа

Вхідний шар – служить для розподілу даних по мережі і не робить ніяких обчислень. Виходи цього шару передають сигнали на входи наступного шару (прихованого або вихідного).

Приховані шари – шари звичайних нейронів, які виконують обробку даних, отриманих із попереднього шару та передають сигнали від входу до виходу. Їх входом служить вихід попереднього шару, а вихід – входом наступного шару.

Вихідний шар – зазвичай містить один нейрон (може і більше), який видає результат розрахунків усієї нейронної мережі [2].

Нейронна мережа аналізує інформацію і надає можливість дати оцінку, наскільки узгоджуються дані з розпізнаваними їй характеристиками. Для цього нейромережу навчають точній ідентифікації на підібраній вибірці прикладів з предметної області. Реакція нейронної мережі піддається аналізу, після чого систему налаштовують таким чином, щоб досягти задовільних результатів. У міру того, як нейромережа проводить аналіз даних, вона набирається додаткового досвіду.

Дослідження процесу виявлення вторгнень проводилось за допомогою багатошарового перцептрону (рис.2) та карт Кохонена (рис. 3).

Багатошаровими перцептроном називають нейронні мережі прямого поширення. Вхідний сигнал в таких мережах поширюється в прямому напрямку, від шару до шару. Багатошаровий перцептрон в загальному уявленні складається з наступних елементів [3]:

– множини вхідних вузлів, які утворюють вхідний шар;

– одного або декількох прихованих шарів обчислювальних нейронів;

– одного вихідного шару нейронів.

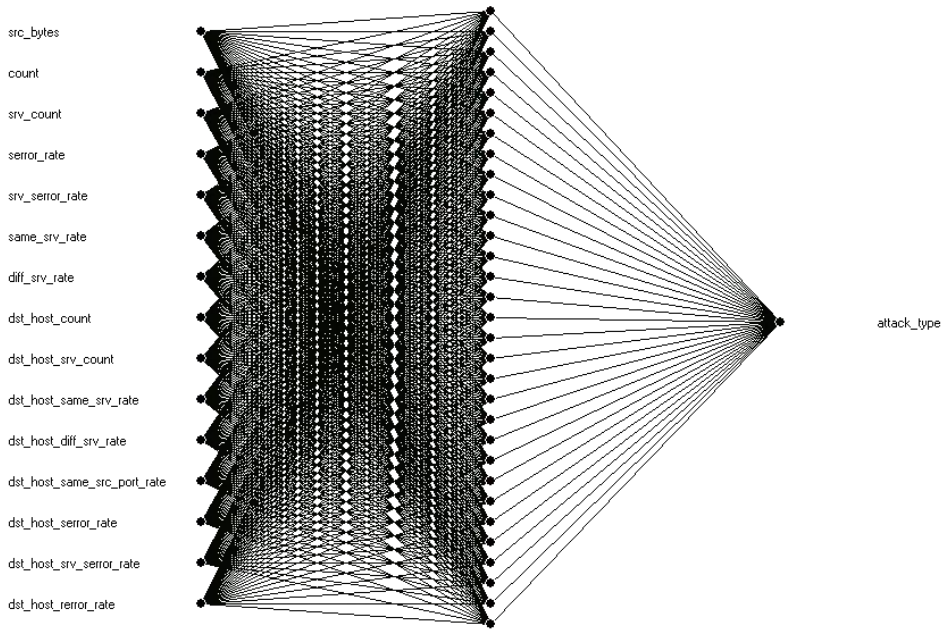

Рис. 2. Багатошаровий перцептрон 15x31x1

Карти Кохонена – це один з різновидів нейронних мереж, однак вони принципово відрізняються від перцептронів, оскільки використовують алгоритм навчання без учителя, тобто навчальна множина складається лише зі значень вхідних змінних, в процесі навчання немає порівнювання виходів нейронів з еталонними значеннями. Карти Кохонена є методом проектування багатовимірного простору в простір з більш низькою розмірністю. При використанні цього алгоритму вектора, схожі в вихідному просторі, виявляються поруч і на отриманій карті [4].

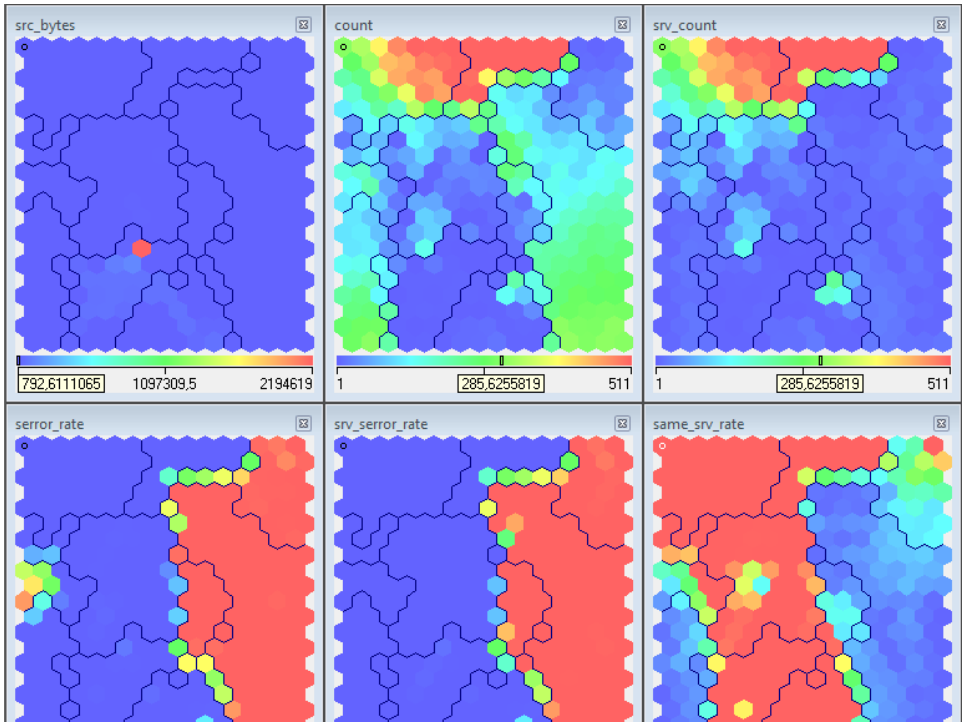

Рис. 3. Карти Кохонена 16x20

Виходячи з проведених тестів, переважним варіантом для виявлення вторгнень є багатошаровий перцептрон. У таблиці 1 наведено порівняння карт Кохонена 16х20, та перцептрону 15х31х1, що надали найкращі результати у своїх тестах.

Таблиця 1

Результат тестування нейромереж

Тип	Розмір	Виявлення відомих атак,%	Виявлення нормальних векторів,%	Виявлення невідомих атак,%
Перцептрон	15х31х1	99,7	96,8	34,7
Карти Кохонена	16х20	99,46	87,07	25,57

Як можна побачити хоча карти Кохонена, також, як і багатошаровий перцептрон успішно виконують поставлену задачу, їх результати є менш точними. Тому у якості нейромережі для виявлення вторгнень більш переважним є багатошаровий перцептрон.

Список використаних джерел:

1. Стівен Норткатт, Джуді Новак. Виявлення вторгнень в мережу. Настільна книга фахівця з системного аналізу. – М., «Лорі», 2001. – 384 с.

2. Нейронні мережі – Від теорії до практики. Режим доступу: https://www.mql5.com/ru/articles/497, 22.11.2018

3. Нейронні мережі для початківців. Частина 1. Режим доступу: https://habr.com/post/312450, 24.11.2018

4. Карти Кохонена, що самоорганізуються – математичний аппарат. Режим доступу: https://basegroup.ru/community/articles/som, 24.11.2018

Буря О.І.

кандидат технічних наук, професор;

Єрьоміна К.А.

кандидат технічних наук, науковий співробітник,
Дніпровський державний технічний університет

ВПЛИВ НАНОКРИСТАЛІЧНОГО СПЛАВУ FINEMET НА НАДМОЛЕКУЛЯРНУ СТРУКТУРУ ФЕНІЛОНУ С-1

Відомо [1], що введення наповнювачів у полімери зумовлює появу широкого спектра взаємодій: від слабких фізичних до хімічних, що виникають на межі розділу полімер – наповнювач. Природа цих взаємодій значною мірою залежить від хімії поверхонь наповнювача. Співвідношення різних типів