УДК 621.326
Шеременда А. – ст. гр. КСМм-51
*Тернопільський національний економічний університет*

# ВИКОРИСТАННЯ НЕЙРОННИХ МЕРЕЖ (НМ) ДЛЯ ВИЯВЛЕННЯ КОМП'ЮТЕРНИХ АТАК

Науковий керівник: д.т.н., проф. Саченко А.О.

Інтернет на даному етапі свого розвитку є невід'ємною частиною суспільства в цілому. Число користувачів, які хочуть підключитись і використовувати ресурси глобальної мережі Internet, нараховує до мільярда чоловік. Проте загрозою Інтернету є розповсюдження через нього комп'ютерних вірусів та здійснення комп'ютерних атак хакерами. Комп'ютерний вірус – це спеціально створена програма, яка здатна розмножуватись і як правило, виконує на ПК певні деструктивні дії. Сучасні антивірусні бази не дають змогу повністю захистити комп'ютер, а загальні методи виявлення проникнення злодія у комп'ютер не невідомі. Таким чином метою доповіді є дослідження універсальних методів захисту від комп'ютерних вірусів шляхом виявлення аномалій у вхідному трафіку. Для досягнення даної мети буде використано систему Honeynet для збору даних. З неї інформація надходитиме до НМ, яка у свою чергу буде ідентифікувати ці дані як атаку чи ні (Рис1). Нехай М – множина вхідних даних системи виявлення атак, а А і В її підмножини. До А віднесемо дані, які вважаються атакою, а до В – дані, які є безпечними. Тоді справедлива рівність $A \subset M, B \subset M, A \cap B \neq 0, A \cup B = M$.

Метод полягає у використанні НМ, як окремої підсистеми для виявлення атак. Для цього пропонується використовувати уточнюючі сигнатури, які визначатимуть апріорно аномальний трафік.

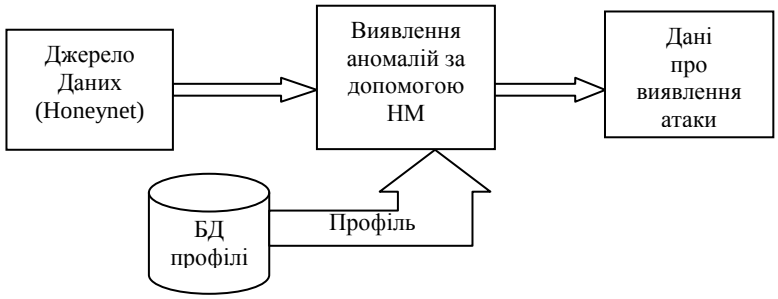


Рис1. Схема методу виявлення аномалій

Введення таких сигнатур в навчальну вибірку НМ дозволить більш точно визначати підмножину В. НМ отримає весь трафік і зможе аналізувати його на наявність аномалій. Роль НМ полягає у проведені класифікації елементів трафіку, а саме заголовків мережевих пакетів, які поступають на вхід. З точки зору НМ «поведінка» трафіку має свої закономірності. Наявність цих закономірностей породжує образи-вектори статистичних ознак, які близькі в багатомірному просторі. На основі аналізу цих ознак НМ буде розділяти сукупність образів на дві області – аномальну і нормальну. Це дозволяє розділити вхідні заголовки IP-пакетів за принципом є у ньому атака чи немає. Доцільно використати, як НМ багаторівневий персептрон, який буде навчатись методом зворотнього розповсюдження помилки. Його вихідний шар повинен буде складатись із двох нейронів, активація одного з них означатиме присутність атаки, а друга відсутність. Цей метод дає переваги по швидкості виконання у порівнянні з статистичними методами. Таким, чином метод є зручнішим для опису і аналізу засобів виявлення атак, як тих котрі раніше зустрічались, так і нових не зареєстрованих.