УДК 004.031.6
І. Павлов, В. Сташук, Л. Матійчук, кан. екон. наук; доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ТЕОРЕТИЧНЕ ОБҐРУНТУВАННЯ МЕТОДУ ВИЯВЛЕННЯ КОМП'ЮТЕРНИХ АТАК

UDC 004.031.6
I. Pavlov, V. Stashuk, L. Matiychuk, Ph.D.; Assoc. Prof.

THEORETICAL JUSTIFICATION OF THE METHOD OF DETECTION OF COMPUTER ATTACKS

Мета виявлення вторгнень на перший погляд дуже проста: виявити проникнення в ІС. Проте це вельми складне завдання. Насправді, системи виявлення вторгнень ніяких вторгнень взагалі не виявляють вони тільки виявляють ознаки вторгнень під час таких атак.
Системи виявлення атак призначені для виявлення і протидії мережевим атакам зловмисників. Вони є спеціалізованим програмно-апаратним забезпеченням з типовою архітектурою, що включає наступні компоненти (рис. 1): модулі-датчики для збору необхідної інформації про МТ в ІС; модуль виявлення атак, що виконує обробку даних, зібраних датчиками, з метою виявлення інформаційних атак; модуль реагування на виявлені атаки; модуль зберігання конфігураційної інформації, а також інформації про виявлені атаки. Таким модулем, як правило, виступає стандартна СУБД, наприклад MS SQL Server; модуль управління компонентами системи виявлення атак.

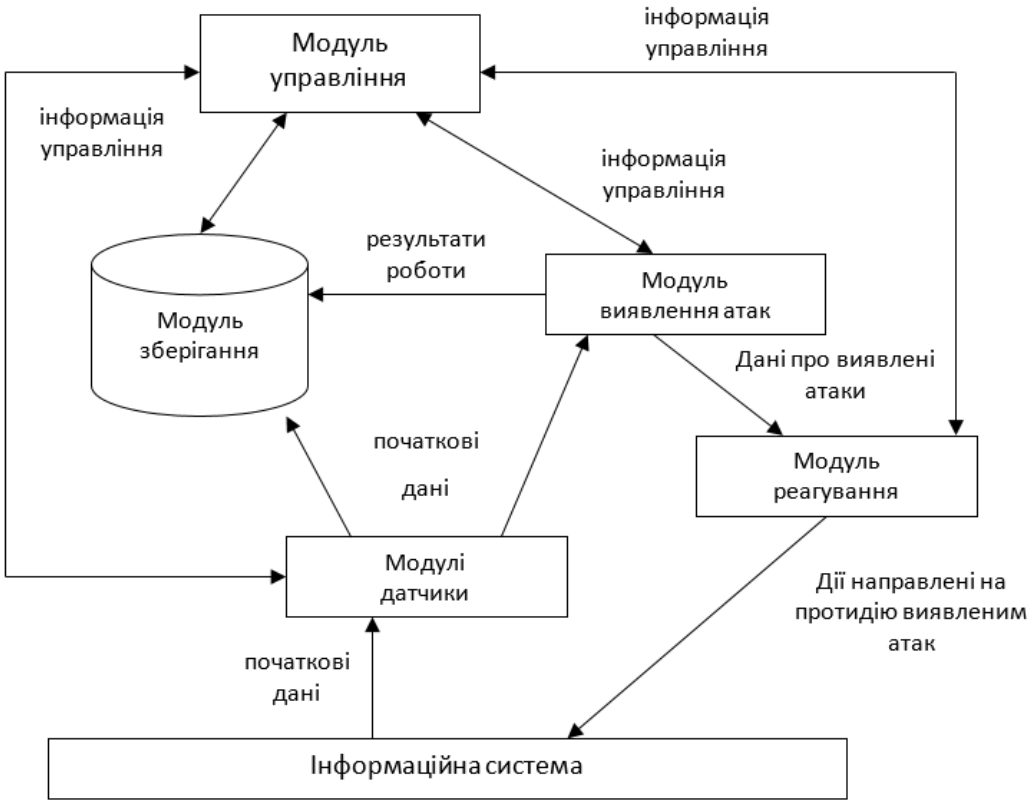

Рисунок 1. Типова архітектура виявлення атак

Для точного виявлення вторгнень необхідні надійні і вичерпні дані про те, що відбувається в системі, яка захищається. Взлом системи можливий як із сторини комп'ютера, що знаходиться в локальній мережі так і через глобальну мережу Інтернет. Проте сучасні атаки (DDOS-атаки –

distributed denial-of-service) для здійснення взлому системи можуть використовувати і проміжні комп'ютери, які прийнято називати зомбі (рис. 2).

Такі системи у мережі Інтернет є незахищені або мало захищені. Зловмисник взломавши їх, бере під свій контроль і при цьому інсталює відповідне програмне забезпечення на кожному з них. Такі компютери після того стають підвладні йому.

Виходячи із відомих методів виявлення атак розглянутих у попередньому розділі, найкращим методом для вирішення задачі ідентифікації атак є застосування СМ на базі нейронних мереж. Вони описують кожну атаку у вигляді спеціальної моделі або сигнатури. Як сигнатура атаки можуть виступати: рядок символів, семантичний вираз на спеціальній мові, формальна математична модель. Алгоритм роботи СМ полягає в пошуку сигнатури атак в початкових даних, зібраних мережевими і хостовими датчиками системи. У разі виявлення шуканої сигнатури, система фіксує факт інформаційної атаки, яка відповідає знайденій сигнатурі.

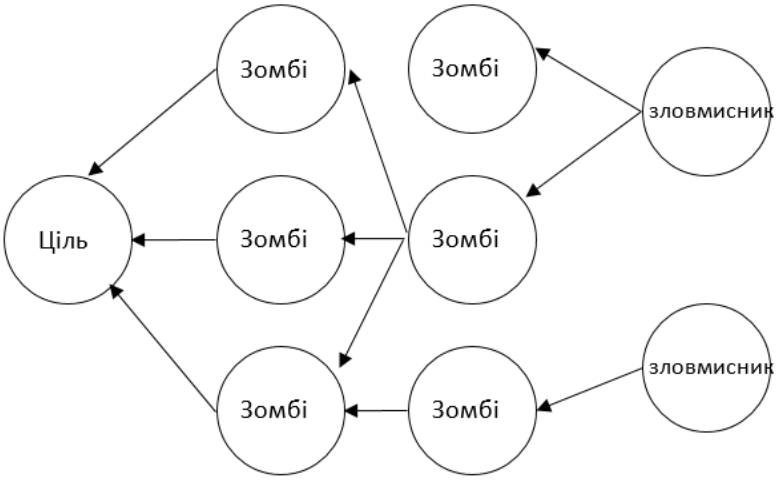

Рисунок 2. Здійснення DDOS-атаки