УДК 004.7

ДОСЛІДЖЕННЯ ШЛЯХІВ ІДЕНТИФІКАЦІЇ АТАК У КОМП'ЮТЕРНИХ МЕРЕЖАХ СТАТИСТИЧНИМИ МЕТОДАМИ

Г. С. Захарченко, студентка
Н. Р. Кондратенко, к.т.н., проф.
Вінницький національний технічний університет
galina_sergeevna@hotmail.com

У зв'язку зі стрімким розвитком комп`ютерних мереж значно зросла кількість та різноманітність атак на мережу. Деякі атаки відрізняються великою складністю, інші по силі будь-якому користувачу, який може навіть не підозрювати до яких наслідків призведе його діяльність. В залежності від цілі, атака може вивести систему з ладу або порушити цілісність чи конфіденційність інформації. Тому важливим і актуальним є питання ідентифікації несанкціонованих дій та їх, хоча б приблизної, мети, щоб якісно захистити мережу та інформацію в ній.

Існують різні методи виявлення атак, основними з яких можна визначити такі: метод виявлення аномалій та сигнатурний метод. Останній базується на описі вже відомих порушень або атак і якщо поведінка суб`єкта співпадає з описом атаки то суб`єкт вважається зловмисником. Основною перевагою сигнатурного методу є низький рівень помилок системи виявлення та її висока швидкодія. Але система здатна виявити лише відомі для неї атаки, якщо модель атаки не міститься у базі даних сигнатур, вона не буде виявлена.

Метод виявлення аномалій ґрунтується на формуванні «образу» нормального функціонування суб`єкта, і відхилення від неї вважається аномальним. Недоліком цього методу є велика кількість помилкових тривог, пов`язана з тим, що важко точно задати граничні значення, щоб адекватно ідентифікувати аномальну діяльність. Водночас є великий плюс у тому, що метод виявлення аномалій дає можливість виявити раніше невідомі атаки.

Для використання такої системи потрібна структурована інформація про поведінку мережі у період її нормально функціонування, при чому чим більше даних, тим краще. Використовуючи різні статистичні методи, можна з тою чи іншою вірогідністю стверджувати, що ситуація в мережі стала аномальною відносно її «еталонної» поведінки.

Для цього можна застосувати критерій максимальної правдоподібності. Метою цього методу є визначення чи є наявне відхилення в поведінці аномальним та небезпечним чи це випадковість, яка навряд має зловмисний характер. Якщо такі дані отримано є доцільним більш детальне вивчення проблеми, що виникла.