УДК 004.7

АНАЛІЗ СУЧАСНИХ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Захарченко Г.С.
Науковий керівник – проф., к.т.н. Кондратенко Н.Р.

З інтенсивним розвитком комп`ютерних мереж значно зросла кількість та різноманітність атак на мережу. Під атакою на інформаційну систему розуміють навмисні дії, які використовують вразливості системи, з метою порушити доступність, цілісність або конфіденційність даних у ній. Кожна атака складається з трьох етапів: збору інформації, реалізації, завершення атаки. Перший етап є однаковим для всіх видів атак, зловмисник вивчає її особливості, перевіряє рівень захищеності системи. Краще та легше ідентифікувати атаки на цьому рівні, оскільки значно зростає активність зловмисника та його легше виявити. Деякі атаки відрізняються великою складністю, інші по силі будь-якому користувачу, який може навіть не підозрювати до яких наслідків призведе його діяльність. Залежно від цілі атаки, вона (атака) може вивести з ладу систему 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.

Одним з механізмів аналізу поведінки мережі є система виявлення вторгнень (СВВ), яка слідкує за ввіреними їй ресурсами і в разі виявлення підозрілих або нетипових подій, здатна виконувати деякі самостійні дії по ідентифікації та усуненні їх причин. Враховуючи велику кількість параметрів, що характеризують СВВ існує досить широка їх класифікація.

За методом аналізу інформації системи поділяють на ті, які використовують сигнатурний метод та ті, що виявляють статистичні аномалії. Перший базується на описі відомих порушень або атак і якщо поведінка суб`єкта збігається з описом атаки то суб`єкт вважається зловмисником. Основною перевагою сигнатурного методу є низький рівень помилок системи та 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 наявності певної «нормальної» поведінки 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, які зможуть адекватно ідентифікувати аномальну діяльність. Водночас є великий плюс у тому, що метод виявлення аномалій дає можливість виявити раніше невідомі атаки. Ефективність системи виявлення атак, яка знаходить аномалії шляхом статистичного аналізу сильно залежить від об’єму бази даних подій у мережі. Важливим є не лише кількість даних, а й їх репрезентативність.