ВИКОРИСТАННЯ НЕЙРОННИХ МЕРЕЖ У ВИЯВЛЕННІ ВТОРГНЕНЬ

Шаповалов М.С., к.т.н., доц. Заковоротний О.Ю, ст. викл. Гугнін В.М., д.т.н., с.н.с. Семенов С.Г.
Національний технічний університет «ХПІ», Харків

В даний час в різних галузях науки і техніки підвищується інтерес до використання штучних нейронних мереж. Таку популярність нейронних мереж можна пояснити можливістю їх ефективного застосування в задачах, з якими «аналітичні» методи погано справляються. Одним із таких завдань є створення системи виявлення вторгнень.

Мінливий характер мережевих атак вимагає гнучку захисну систему, яка здатна аналізувати величезну кількість мережевого трафіку за методом, який менш структурований ніж той, що заснований на побудові певних правил. Система виявлення вторгнень на основі нейронної мережі може потенційно вирішити багато з проблем, які мають місце бути в системах, заснованих на правилах.

Реалізація нейронних мереж в системах виявлення вторгнень передбачає включення їх в існуючі або модифіковані експертні системи. На відміну від попередніх спроб використовувати нейронні мережі в виявленні аномалій, використовуючи їх в якості заміни для існуючих компонентів статистичного аналізу, цей варіант пов'язаний з використанням нейронної мережі для фільтрації вхідних даних з метою виявлення підозрілих подій, які можуть вказувати на вторгнення і направляти ці події експертної системі. Ця конфігурація поліпшить ефективність системи виявлення за рахунок зменшення помилкових тривог експертної системи. Нейронна мережа визначає ймовірність того, що певна подія є показником атаки, тому можна встановити поріг, при якому подія направляється в експертну систему для додаткового аналізу. Оскільки експертна система тільки отримує дані про події, які розглядаються як підозрілі, чутливість експертної системи може бути збільшена.

Таким чином, завдяки інтеграції нейронних мереж в систему виявлення вторгнень на основі правил, можна домогтися більшої ефективності системи в цілому та більш раціонального використання експертної системи.