УДК 004.353
О. Максимець
(Тернопільський національний технічний університет імені Івана Пулюя)

МЕТОДИ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННІ АТАК НА КОМП'ЮТЕРНІ СИСТЕМИ

Для більшої ефективності та кращого обміну інформацією комп'ютерні системи комунікують між собою. Через таку інтеграцію кількість потенційних загроз збільшується. Оцінка ймовірного впливу на систему можлива тоді, коли відомі її характерні особливості, тип та можливі загрози.

Виявлення аномалій є дуже важливим кроком для ідентифікації атаки. Метою виявлення аномалій є класифікація подій, що виходять за рамки попередньо встановленого профілю нормальної поведінки. Програми виявлення аномалій передбачають, що будь-яка підозріла подія є підмножиною аномальної активності.

Методи машинного навчання відіграють ключову роль при побудові нормальних профілів та виявлення вторгнення в системах виявлення аномалій. При виявленні аномалій, як правило, доступні лише промарковані дані, що відповідають нормальній поведінці. Методи машинного навчання з учителем потребують також і промаркованих даних аномальної поведінки. Проте дані такого роду зазвичай важко отримати в реальних умовах. Відсутність такого набору даних призводить до незбалансованого розподілу навчальної вибірки. Крім того, при зміні мережевого середовища або послуг, шаблони нормальної поведінки змінюються. Відмінності між навчальними та тестовими даними призводять до значної кількості помилок першого роду у виявлення вторгнень в систему. Виявлення аномалій за допомогою методів машинного навчання без вчителя дозволяє подолати ці недоліки. Тому на практиці ці методи, а також методи гібридного навчання, застосовуються частіше.

Вибір найкращого алгоритму для конкретного завдання може бути непростою проблемою. Виконувати одне і те ж завдання можуть різні алгоритми, але кожен з них дає різні результати. Отримуючи на вхід набір даних, алгоритми класифікації прогнозують дискретні величини. Алгоритми регресії ж прогнозують одну або декілька неперервних величин, таких як прибуток або збиток. Алгоритми сегментації ділять дані на групи або кластери об’єктів, які мають подібні властивості.

У задачах виявлення аномальної поведінки найбільш поширеним є застосуванням алгоритмів на основі правил.

Очевидно, що проблема автоматичного виявлення аномалій є розв’язною, і система може отримати можливість автоматично реагувати на атаки. Однак підходи до виявлення аномалій можуть мати високі показники помилкового спрацювання. Оскільки ці методи позначають будь-яке значне відхилення від базового значення як вторгнення, ймовірно, що невтручання в поведінку, що виходить за межі нормального діапазону, також позначатиметься як вторгнення, в результаті чого буде хибно позитивним.

Тим не менше, підхід, який виявляє аномалії за допомогою алгоритму на основі правил, є достатнім для виявлення раніше невидимих атак. Таким чином, шляхом виявлення аномалій адміністратор може застосувати захисні заходи для припинення програми з підозрілою поведінкою, додавання IP-адреси передбачуваного атакуючого до фільтра брандмауера або навіть тимчасового відключення системи від мережі.