УДК 004.492.3

Яцишин В.В. канд. техн. наук, доцент, Демиденко А.О., Яцишин Вік. В.
Тернопільський національний технічний університет імені Івана Пулюя

ПІДХОДИ ДО ВИЯВЛЕННЯ АНОМАЛІЙ ТРАФІКУ У КОМП'ЮТЕРНИХ МЕРЕЖАХ

Yatsyshyn V.V. PhD., Assoc. Prof., Demydenko A.O., Yatsyshyn Vic. V.

APPROACHES OF ANOMALY DETECTION IN COMPUTER NETWORKS

Тренд розвитку галузі інформаційних технології орієнтований на розробку та впровадження нових методів та інструментів опрацювання великих об'ємів інформацій з паралельною імплементацією технологій штучного інтелекту. При цьому комунікаційна інфраструктура є важливим компонентом і «скелетом» будь-якої комп'ютеризованої інформаційної системи перетворення інформації. Окрім прямих функціональних обов'язків щодо трансферу даних, комп'ютерна мережа повинна забезпечувати надання різних сервісів, які пов'язані з контролем типу інформації, що передається, конфіденційністю даних, захисту від потенційних вразливостей та ряду інших. Тому актуальними задачами на сьогодні є інтеграція розумних сервісів щодо виявлення аномалій трафіку у комп'ютерних мережах задля підвищення надійності її функціонування у випадку кіберзагроз.

Виявлення та аналіз аномалій трафіку є критичним процесом в контексті кібербезпеки комунікаційної інфраструктури, а саме поняття аналізу аномалій інтерпретується як здатність виявлення нетипової діяльності або активності, що може вказувати на кібератаку, збій мережі на системному рівні чи на рівні окремих компонентів, або інші загрози. Потрібно відмітити, що виявлення аномалій повинно забезпечувати виявлення нетипової поведінки об'єктів (хостів, пакетів даних, інтенсивності запитів і т.п.) у комп'ютерній мережі на ранніх стадіях. Це обумовлено необхідністю реагування на аномалії до того, як потенційна кіберзагроза завдасть значної шкоди інформаційній інфраструктурі. Виявлення аномалій допомагає захистити чутливу інформацію від несанкціонованого доступу, підвищити доступність і надійність сервісів до появи відмов.

Для підвищення ефективності виявлення аномалій трафіку необхідно проводити заходити регулярного оновлення програмного забезпечення на рівні маршрутизаторів та хостів мережі, формувати резервні копії даних, забезпечувати постійний моніторинг з використанням передових технологій виявлення та аналізу аномалій. Серед сучасних методів виявлення та аналізу аномалій трафіку у комп'ютерних мережах варто виділити:

– Статистичний аналіз – передбачає порівняння характеристик поточного трафіку з історичними даними і забезпечує виявлення відхилень від математичного сподівання, дисперсії та інших статистичних показників.

– Машинне навчання – використовує підхід визначення типу трафіку як нормальний або нетиповий (аномальний) з використанням нейромережевого підходу, дерев чи лісів прийняття рішень, або підходи anomaly detection чи novelity detection – в основі лежать спеціалізовані алгоритми визначення відхилень від типової поведінки у комп'ютерній мережі.

Поведінковий аналіз та експертні системи – базуються на моделюванні нормального стану трафіку з відповідним встановленням відхилення від норми, використовують базу знань експертів для побудови асоціативних правил щодо потенційних загроз мережі.