УДК 004.415.5
А. Ухман
(Тернопільський національний технічний університет імені Івана Пулюя)

МЕТОД ВИЯВЛЕННЯ МЕРЕЖЕВИХ АНОМАЛІЙ ТА ПОТЕНЦІЙНИХ ЗАГРОЗ НА ПРИКЛАДІ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТНТУ

Сучасний вектор суспільного розвитку тісно пов'язаний з процесом вдосконалення інформаційних і комунікаційних технологій. Поряд із загальною інформаційною насиченістю та інтеграцією швидко росте кількість інформації, що передається з використанням мережевих технологій. Тому забезпечення безпеки та цілісності комп'ютерних мереж є одним з ключових завдань кібербезпеки. Актуальність цієї задачі лише посилюється зважаючи на активний розвиток мережевої інфраструктури та технологій, виникнення нових протоколів та зростання кількості підключених користувачів. Популярність Інтернету речей та так звані "розумні мережі" ставлять нові виклики перед фахівцями в сфері захисту комп'ютерних мереж.

Існують різні методи та засоби для виявлення аномального трафіку, зокрема розроблені цілі автоматизовані комплекси, що дозволяють боротись зі шкідливим чи аномальним трафіком в масштабованих комп'ютерних мережах. Проте вони є достатньо дорогими. Тому виникає потреба у створенні ефективних і доступних алгоритмів, що дозволять проводити фільтрацію мережевого трафіку.

Метою дослідження є побудова методу для аналізу мережевого трафіку в Тернопільському національному технічному університеті імені Івана Пулюя в умовах завантаженості комп’ютерної мережі, моніторингу небезпек пов’язаних з несанкціонованим доступом та розповсюдженням шкідливого програмного забезпечення. Для збору мережевого трафіку використовуються програми аналізатори, для прикладу Wireshark, які дозволяють оцінити не лише кількість трафіку, але й здійснити його розподіл за мережевими протоколами.

В досліджуваній локальній мережі є близько 400 кінцевих пристроїв користувачів, частина з них підключена як стаціонарні ПК, частина через портативні (мобільні) пристрої (нетбуки, лептопи тощо). Певний відсоток пристроїв також підключений до мережі опосередковано, за допомогою самостійно встановлених комутаторів чи маршрутизаторів та з використанням різноманітних типів технологій передачі та обміну даними. Ключовим фактором є наявність певної хаотичності у підключенні користувачів і пов’язані з цим труднощі з ефективним контролем і забезпеченням якості роботи мережі. Тому, зібравши дані щодо потоку трафіку і динаміки його структури у певні моменти часу (підвищеної активності користувачів чи відсутності активного навантаження), можна класифікувати певні патерни, які можуть слугувати індикаторами рівня “здоров’я” мережі, що, своєю чергою, дозволяє розробити механізми зворотної дії для компенсації негативних тенденцій. На відміну від активних систем моніторингу, які вже реалізовані, потрібні гнучкіші засоби для контролю потоку трафіку, засоби, які спільно із системами моніторингу можуть застосовувати точковий аналіз мережі, своєрідну реакцію на виникнення тих чи інших “подразників” та порушень штатного режиму роботи мережі.

В доповіді буде розглянуто результати аналізу трафіку ТНТУ з допомогою ймовірнісного підходу, що використовує ентропію. Порівняння показників нормалізованої ентропії дає змогу вибрати сумнівний трафік.