Розробка програмного забезпечення виявлення дестабілізуючого широкомовного трафіку у мережі

О.В. Лаврентьєва, *студент,*
О.А. Смірнов, *доцент, канд. техн. наук,* **Є.В. Мелешко**, *канд. техн. наук*
Кіровоградський національний технічний університет

Більшість сучасних комп'ютерних мереж складаються із сегментів, об'єднаних на другому рівні моделі OSI. Це спрощує адресацію й дозволяє вузлам обмінюватися даними без застосування протоколів мережного рівня. Самими нестабільними ділянками в таких мережах є сегменти рівня доступу. Вони найбільше піддані дестабілізуючому впливу кінцевих вузлів, тому що їхні несанкціоновані дії можуть привести до непрацездатності всього сегмента. Підвищення захищеності й надійності роботи цього рівня є одним з найважливіших завдань.

Залежно від розміру мережі й політики проектування кількість вузлів, що працюють в одному сегменті, може доходити до тисячі. Це спрощує проведення атак, спрямованих на виведення з ладу встаткування й каналів зв'язку. Використання технології віртуальних мереж (VLAN) дозволяє зменшити розміри сегментів, але не позбутися від них зовсім.

Метою роботи є підвищення захищеності й надійності функціонування комп'ютерної мережі за рахунок автоматизації процесу виявлення дестабілізуючого широкомовного трафіку на основі аналізу мережної статистики.

Об'єктом дослідження є процес підвищення захищеності й надійності функціонування комп'ютерної мережі.

Предмет дослідження – методи й алгоритми виявлення дестабілізуючого широкомовного трафіку на основі аналізу мережної статистики.

Методи дослідження базуються на теорії ймовірностей і математичної статистики, теорії алгоритмів, теорії обчислювальних систем і мереж.

Наукова новизна результатів, отриманих автором, полягає в наступному: 1) розроблено метод, що дозволяє в автоматичному режимі будувати логічну топологію мережі; 2) запропоновано математичні моделі, використовувані для пошуку широкомовного шторму і його джерела; 3) розроблено новий метод виявлення інтенсивних широкомовних потоків трафіку в мережі.

Практична значимість роботи. Запропоновані методи й розроблені додатки підвищують безпека й розширюють можливості по виявленню аномалій завдяки виявленню дестабілізуючих широкомовних потоків трафіку в мережі. Створені механізми дозволяють підвищити інформованість системних адміністраторів і фахівців з мережної безпеки про процеси, що відбуваються в комп'ютерних мережах. Результати проведених досліджень можуть бути використані в системах моніторингу й збору статистики як основа для створення нових функціональних модулів. Розроблені методи можуть застосовуватися для динамічної побудови топології, що дозволяє автоматизува-ти процеси виявлення й локалізації джерел погроз безпеки, пов'язаних з несанкціоно-ваним впливом на мережну інфраструктуру або несправністю встаткування.

Достовірність наукових результатів підтверджена теоретичними викладеннями, даними комп'ютерного моделювання, коректними дослідженнями параметрів на функціонуючій обчислювальній мережі, а також відповідністю отриманих результатів окремим результатам, наведеним у науковій літературі.