# ВИКОРИСТАННЯ АНАЛІЗАТОРУ WIRESHARK ЩОДО ОПТИМІЗАЦІЇ МЕРЕЖЕВОГО ТРАФІКУ

Поліканов Д. А., Іванісенко І. М.
Харківський національний університет радіоелектроніки, Харків, Україна

**Метою доповіді** є запропонований формат застосування ПЗ Wireshark щодо задач оптимізації трафіка у розподілених системах. **В доповіді** наводяться результати застосування ПЗ Wireshark та перелік важливих мережевих протоколів, які використовуються у роботі.

Аналіз мережного трафіку може бути доповненням до вже існуючих засобів виявлення мережевих атак. Копія мережного трафіку дозволяє відновити послідовність дій зловмисників - проаналізувати взаємодії між вузлами мережі, підключення до зовнішніх ресурсів, командних серверів і детально розібратися в отриманих даних

Використовуючи інтерфейс Wireshark, можна вибрати, наприклад, пакет HTTP і побачити, що HTTP інкапсулюється в TCP (транспортний рівень), TCP інкапсулюється в IP (мережевий рівень), а IP у свою чергу інкапсулюється в Ethernet (перед цим навіть використовується 802.1Q)[1]. Це дає змогу побачити детальну інформацію з кожного рівня та розробити стратегію оптимізації трафіку:

- Основною причиною втрати пакетів є недостатня пропускна здатність мережі для необхідного з'єднання. Це відбувається, коли надто багато пристроїв намагаються встановити зв'язок в одній мережі.

- Недостатньо потужне обладнання. Будь-яке обладнання в мережі, яке маршрутизує пакети, може призвести до втрати пакетів.

- Пошкоджені кабелі. Втрата пакетів може статися на фізичному та мережному рівні.

- Програмні помилки: Мікропрограма вашого мережного обладнання або програмного забезпечення комп'ютера може містити помилки, які можуть призвести до втрати пакетів[2].

Також за допомогою аналізатору можно виявити не зашифрований трафік та слабкі міста системи. Таким чином, залишається вибір між шифруванням всього мережевого трафіку або здійснюючи шифрування на 3 рівні моделі, можливо продовжувати використовувати небезпечні протоколи

**Список літератури**

1. Антон Т. Руководство по использованию Wireshark [Електронний ресурс] / Трасковский Антон. – 2021. – Режим доступу до ресурсу: https://timeweb.com/ru/community/articles/rukovodstvo-po-ispolzovaniyu-wireshark.

2. Как исправить потерю пакетов [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://ip-calculator.ru/blog/ask/kak-ispravit-poteryu-paketov/.