МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ
Циклова комісія (кафедра) комп’ютерної інженерії та інформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему

МЕТОДИ ТА ЗАСОБИ АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ

Виконав: студент групи 1К-21
Спеціальності 123 Комп’ютерна інженерія
Дєніс ОСТРОУШКО
Керівник:
Майя ЛЮТА

Черкаси 2025

АНОТАЦІЯ

Кваліфікаційна робота на тему «Методи та засоби аналізу мережевого трафіку» складається з вступу, основної частини, що містить 3 розділи, висновку та списку використаних джерел. Загальний обсяг роботи – 57 сторінок. У роботі 13 рисунків та 5 таблиць. Перелік використаних ресурсів налічує 27 одиниць.

Аналіз мережевого трафіку є важливою складовою забезпечення безпеки, стабільності та ефективності комп'ютерних мереж. Його мета – виявити потенційні загрози, визначити джерела перевантажень або порушень, а також оптимізувати роботу мережевих ресурсів. Основними методами аналізу трафіку є: пасивний аналіз, що передбачає спостереження за передачею даних у мережі без втручання в сам трафік. Використовується для моніторингу активності, збору статистики, виявлення аномалій або шкідливих дій; активний аналіз, що включає в себе створення контрольованих запитів або пакетів для тестування реакції мережі; гібридний аналіз, що поєднує елементи пасивного і активного аналізу, забезпечуючи повніше розуміння ситуації у мережі.

Аналіз мережевого трафіку – ключовий процес для забезпечення надійної роботи IT-інфраструктури. Вибір методу та інструментів залежить від завдань, технічних можливостей та вимог до безпеки. Регулярне дослідження трафіку дозволяє не лише вчасно виявляти загрози, а й ефективно керувати ресурсами мережі.

Ключові слова: мережевий трафік, аналіз трафіку, мережеві пакети, моніторинг мережі, протоколи, кібербезпека, фільтрація трафіку, інструменти аналізу, діагностика мережі, інтернет-трафік, оптимізація мережі, інформаційна безпека.

ABSTRACT

The qualification work on the topic «Methods and tools for analyzing network traffic» consists of an introduction, the main part, which contains 3 sections, a conclusion and a list of sources used. The total volume of the work is 61 pages. The work contains 13 figures and 5 tables. The list of resources used has 27 units.

Network traffic analysis is an important component of ensuring the security, stability and efficiency of computer networks. Its purpose is to identify potential threats, identify sources of overloads or violations, as well as optimize the operation of network resources. The main methods of traffic analysis are passive analysis, which involves observing data transmission in the network without interfering with the traffic itself. It is used to monitor activity, collect statistics, detect anomalies or malicious actions; active analysis, which includes creating controlled requests or packets to test the network's response; hybrid analysis, which combines elements of passive and active analysis, providing a more complete understanding of the situation in the network.

Network traffic analysis is a key process for ensuring reliable operation of IT infrastructure. The choice of method and tools depends on the tasks, technical capabilities and security requirements. Regular traffic analysis allows not only to detect threats in time, but also to effectively manage network resources.

Keywords: network traffic, traffic analysis, network packets, network monitoring, protocols, cybersecurity, traffic filtering, analysis tools, network diagnostics, Internet traffic, network optimization, information security.

ЗМІСТ

ВСТУП

Актуальність теми «Методи та засоби аналізу мережевого трафіку» зумовлена стрімким розвитком цифрових технологій, зростанням обсягів переданої інформації в мережах та необхідністю забезпечення їхньої стабільної, безпечної та ефективної роботи. У сучасному світі майже всі сфери діяльності – освіта, бізнес, державне управління, охорона здоров'я, промисловість – залежать від надійного функціонування комп'ютерних мереж, а отже, потребують якісного моніторингу та управління мережевими ресурсами.

Метою дослідження є розробка чітких рекомендацій застосування засобів мережевого трафіку для різних сфер діяльності на основі обґрунтування практичних прикладів їх використання.

Для досягнення поставленої мети вважатимемо за необхідне вирішення наступних **завдань**:

- дослідити поняття та класифікацію мережевого трафіку;

- охарактеризувати методи збору даних про трафік, що поділяються на пасивні та активні;

- окремо виділити статистичні методи аналізу;

- привести загальний огляд сучасних інструментів для аналізу трафіку;

- виокремити характеристики програм, зокрема Wireshark, Nmap, SolarWinds, PRTG;

- порівняти аналіз засобів мережевого трафіку.

Аналіз опрацьованих наукових джерел щодо даної теми показав важливість да доцільність даного дослідження, обумовлене викликами сьогодення:

Зростанням обсягів трафіку. Адже зі збільшенням кількості пристроїв, підключених до Інтернету (IoT, мобільні телефони, сервери тощо), мережі стикаються з надмірним навантаженням. Аналіз трафіку дозволяє ефективно розподіляти ресурси, уникати перевантажень і збоїв у роботі систем.

Проблемами безпеки. Кіберзагрози стають дедалі складнішими та витонченішими. За допомогою аналізу трафіку можна виявляти аномалії, підозрілу активність та атаки (наприклад, DDoS, фішинг, вторгнення). Це критично важливо для забезпечення кіберзахисту мереж.

Потребами в контролі якості послуг (QoS). Саме якість сервісів залежить від стабільності та швидкості передачі даних. Аналіз трафіку допомагає визначати вузькі місця та регулювати пріоритети для різних типів трафіку (наприклад, відео, голос, дані).

Оптимізацією мережевої інфраструктури. Грамотний аналіз дає змогу приймати обґрунтовані рішення щодо модернізації обладнання, зміни топології, розширення каналів або впровадження нових протоколів.

Вимоги до звітності та аудиту. У багатьох галузях (особливо у фінансовій та державній) необхідне ведення журналів доступу, перевірка відповідності політикам безпеки тощо. Засоби аналізу трафіку забезпечують цю прозорість.

Розвиток новітніх технологій. Впровадження штучного інтелекту, машинного навчання, хмарних сервісів, віртуалізації (SDN, NFV) змінює підходи до управління мережами, а отже – висуває нові вимоги до засобів аналізу трафіку.

У сучасних умовах методи та засоби аналізу мережевого трафіку стають не просто допоміжним інструментом, а важливою складовою ефективного управління IT-інфраструктурою. Їхнє впровадження дозволяє підвищити рівень безпеки, забезпечити безперервність роботи сервісів, зменшити витрати та підвищити якість обслуговування користувачів. Саме тому ця тема має високу наукову та практичну цінність і залишається актуальною для дослідження.

РОЗДІЛ 1
ОСНОВИ МЕРЕЖЕВОГО ТРАФІКУ

1.1 Поняття та класифікація мережевого трафіку

Мережевий трафік – це сукупність даних, які передаються через комп'ютерні мережі. Він включає всі види цифрової інформації, що переміщуються між пристроями: текстові повідомлення, мультимедійні файли, пакети команд, запити до серверів тощо. Аналіз мережевого трафіку є важливим для забезпечення ефективної роботи мережі, оптимізації пропускної здатності, кібербезпеки та діагностики проблем.

Мережевий трафік класифікується за різними критеріями: за типом даних, напрямком руху, рівнем пріоритетності, способом передачі та іншими характеристиками [1].

1. Класифікація мережевого трафіку за способом організації передачі

1.1. Унікаст (Unicast)

Це найпоширеніший тип передачі трафіку, при якому дані передаються від одного відправника до одного конкретного отримувача.

Приклад: перегляд веб-сторінки, завантаження файлу, електронна пошта.

1.2. Мультікаст (Multicast)

Передача даних від одного відправника до групи отримувачів. Використовується для ефективної доставки інформації без дублювання трафіку.

Приклад: трансляція відеоконференцій, потокове відео, IPTV.

1.3. Бродкаст (Broadcast)

Передача даних від одного пристрою до всіх пристроїв у мережі. Застосовується в локальних мережах для пошуку пристроїв або служб.

Приклад: запити ARP (Address Resolution Protocol) для визначення MAC-адрес пристроїв.

1.4. Енікаст (Anycast)

Передача даних від одного відправника до найближчого доступного отримувача в групі. Використовується для розподілу навантаження та балансування трафіку.

Приклад: запити до DNS-серверів.

2. Класифікація за напрямком руху

2.1. Вхідний (Inbound Traffic)

Трафік, що надходить у локальну мережу з зовнішніх джерел. Включає завантаження файлів, перегляд веб-сайтів, отримання електронної пошти.

2.2. Вихідний (Outbound Traffic)

Трафік, що передається з локальної мережі у зовнішні системи. Включає надсилання електронної пошти, запити до серверів, передавання файлів.

2.3. Внутрішній (Internal Traffic)

Обмін даними між пристроями в межах однієї мережі, наприклад, між комп’ютерами корпоративної мережі чи серверами дата-центру.

3. Класифікація за типом протоколу [2]

3.1. Трафік рівня додатків (Application Layer Traffic)

Передається через високорівневі протоколи, які використовуються для комунікації між програмами:

- HTTP/HTTPS (веб-трафік);
- FTP (передача файлів);
- SMTP, POP3, IMAP (електронна пошта);
- DNS (перетворення доменних імен у IP-адреси).

3.2. Транспортний трафік (Transport Layer Traffic)

Забезпечує передачу даних між програмами через мережу:

- TCP (надійна передача з контролем помилок);
- UDP (швидка передача без гарантії доставки).

3.3. Мережевий трафік (Network Layer Traffic)

Відповідає за маршрутизацію пакетів у мережі:

- IP (ідентифікація та адресація пристроїв);
- ICMP (пінг-запити та діагностика).

3.4. Канальний рівень (Link Layer Traffic)

Передача даних між вузлами в межах локальної мережі:

- Ethernet;

- Wi-Fi.

4. Класифікація за характером використання пропускної здатності [3]

4.1. Критичний трафік.

Має пріоритетний доступ до ресурсів мережі, оскільки потребує мінімальних затримок:

- Голосовий зв’язок (VoIP);

- Відеоконференції;

- Термінові фінансові транзакції.

4.2. Некритичний трафік.

Може мати нижчий пріоритет, оскільки не потребує моментальної доставки:

- Завантаження файлів;

- Перегляд веб-сторінок;

- Електронна пошта.

4.3. Фоновий трафік.

Генерується службами та системами у фоновому режимі:

- Автоматичне оновлення програмного забезпечення;

- Синхронізація файлів у хмарних сервісах.

5. Класифікація за рівнем безпеки.

5.1. Легітимний (дозволений) трафік.

Офіційний трафік, що проходить через дозволені протоколи та ресурси:

- Користувацький інтернет-трафік;

- Корпоративний мережевий обмін.

5.2. Підозрілий трафік.

Може містити ознаки потенційної загрози:

- Незвичні запити до серверів;

- Різке збільшення вихідного трафіку.

5.3. Шкідливий (атаки, віруси, ботнети)

Трафік, який несе загрозу для інформаційної безпеки:

- DDoS-атаки;

- Фішингові атаки;

- Шкідливе програмне забезпечення.

6. Класифікація за типом споживача.

6.1. Користувацький трафік.

Генерується звичайними користувачами під час роботи в інтернеті [4].

6.2. Серверний трафік.

Створюється серверами при обробці запитів клієнтів (наприклад, запити до веб-сервера).

6.3. Мережевий службовий трафік.

Включає дані, що передаються між пристроями для підтримки роботи мережі:

- ARP-запити;

- DHCP-запити.

Мережевий трафік є невід'ємною частиною сучасних цифрових комунікацій, і його правильна класифікація дозволяє ефективно керувати ресурсами, забезпечувати безпеку та оптимізувати роботу мереж. Важливо аналізувати трафік з урахуванням його характеру, джерела та впливу на продуктивність мережевих систем. Використання спеціалізованих інструментів для моніторингу та аналізу трафіку (наприклад, Wireshark, NetFlow, SNMP) допомагає запобігати загрозам і забезпечувати стабільну роботу мережевої інфраструктури.

1.2 Методи збору даних про трафік (пасивні та активні методи)

Аналіз мережевого трафіку є важливим завданням для адміністраторів мереж, спеціалістів із безпеки та дослідників у сфері телекомунікацій. Він дозволяє оцінювати продуктивність мережі, виявляти потенційні загрози та

забезпечувати якісний контроль за передачею даних. Для збору інформації про трафік використовуються два основні підходи: пасивні та активні методи.

1. Пасивні методи збору даних про трафік [5].

Пасивний моніторинг передбачає спостереження за трафіком без внесення змін у його потік або впливу на роботу мережі. Це дозволяє отримати точну інформацію про поточний стан мережі, її пропускну здатність та поведінку користувачів.

1.1. Основні характеристики пасивних методів:

- Не впливають на функціонування мережі;
- Використовуються для аналізу реальних даних;
- Не створюють додаткового навантаження на мережу;
- Мають високу точність зібраної інформації.

1.2. Приклади пасивних методів:

1.2.1. Аналіз трафіку на мережевих пристроях.

Спеціальні інструменти (наприклад, Wireshark, tcpdump) встановлюються на маршрутизатори, комутатори або сервери для перехоплення та аналізу переданих пакетів. Це дає змогу виявити зловмисну активність, переглянути використання смуги пропускання та оцінити продуктивність мережі.

1.2.2. Використання NetFlow, IPFIX, sFlow.

- NetFlow (розробка Cisco) – дозволяє зберігати дані про мережеві потоки (IP-адреси джерел і одержувачів, протоколи, об’єм переданих даних тощо).

- IPFIX – удосконалений стандарт збору даних, що використовується у високопродуктивних мережах.

- sFlow – відбирає вибіркові пакети трафіку для аналізу, що зменшує навантаження на систему збору даних.

1.2.3. Аналіз логів (журналів подій).

Журнали роботи серверів, маршрутизаторів, брандмауерів та інших пристроїв містять записи про з’єднання, запити користувачів, спроби доступу тощо. Аналіз логів дає змогу виявляти аномалії в поведінці користувачів і можливі кібератаки.

1.2.4. Моніторинг через мережеві дзеркальні порти (SPAN, TAP)

- SPAN (Switched Port Analyzer) – функція комутаторів, яка дозволяє дублювати трафік із порту або VLAN для його подальшого аналізу.

- TAP (Test Access Point) – апаратний пристрій, який непомітно копіює весь трафік і передає його на систему моніторингу.

1.3. Переваги та недоліки пасивних методів.

Переваги:

- Не впливають на роботу мережі;

- Висока точність даних;

- Можливість довготривалого збору інформації.

Недоліки:

- Не дозволяють виявляти майбутні проблеми;

- Не можуть оцінювати поведінку користувачів у змінених умовах;

- Великий обсяг даних потребує потужних ресурсів для обробки.

2. Активні методи збору даних про трафік [6].

Активний моніторинг передбачає штучне генерування трафіку або запитів для оцінки характеристик мережі. Він використовується для діагностики, тестування продуктивності та виявлення потенційних проблем.

2.1. Основні характеристики активних методів:

- Дозволяють отримати дані про продуктивність мережі

- Генерують власний трафік для тестування;

- Можуть виявляти потенційні проблеми, які ще не виникли;

- Використовуються для аналізу пропускної здатності.

2.2. Приклади активних методів:

2.2.1. Ping (ICMP Echo Request/Reply).

Один із найпростіших способів перевірки доступності хостів у мережі. Визначає час відповіді від сервера або пристрою, а також втрати пакетів.

2.2.2. Traceroute (tracert у Windows).

Метод аналізу маршруту проходження пакетів через мережу. Дозволяє виявити затримки та несправності на різних проміжних вузлах.

2.2.3. Генерування штучного трафіку (Load Testing, Stress Testing).

Спеціальні інструменти (наприклад, iPerf, Ostinato) створюють потік даних для оцінки продуктивності мережі, тестування серверів і балансування навантаження.

2.2.4. Активне сканування портів (Nmap, ZMap).

Використовується для виявлення відкритих портів на пристроях, аналізу їхньої безпеки та перевірки мережевих служб.

2.2.5. Вимірювання пропускної здатності (Speed Test, iPerf).

Дозволяє оцінити швидкість завантаження та відправлення даних між клієнтом і сервером.

2.3. Переваги та недоліки активних методів

Переваги:

- Дозволяють оцінювати продуктивність мережі в режимі реального часу;
- Виявляють потенційні проблеми до їхнього виникнення;
- Дають змогу перевірити роботу конкретних сервісів.

Недоліки:

- Створюють додаткове навантаження на мережу;
- Можуть впливати на продуктивність реальних користувачів;
- Деякі методи (наприклад, сканування портів) можуть сприйматися як шкідливі дії.

Пасивні та активні методи збору даних про трафік є взаємодоповнюючими підходами для аналізу та управління мережею. Пасивні методи забезпечують детальну картину про поточний стан трафіку без впливу на його функціонування, тоді як активні методи дозволяють тестувати продуктивність мережі та виявляти потенційні проблеми.

Таблиця 1.1 – Порівняння пасивних та активних методів [7, 8]

Критерій	Пасивні методи	Активні методи
Вплив на мережу	Мінімальний	Створює додатковий трафік
Точність даних	Висока	Може відрізнятися від реальних умов
Виявлення загроз	Виявляє поточні загрози	Дозволяє передбачити можливі проблеми
Використання ресурсів	Вимагає великих обчислювальних потужностей	Може впливати на продуктивність мережі
Час збору даних	Проводиться постійно	Виконується у певний момент часу

Оптимальний підхід передбачає поєднання обох методів: пасивний моніторинг використовується для виявлення аномалій і довготривалого аналізу, а активний тестинг застосовується для перевірки конкретних гіпотез, оцінки швидкості та діагностики збоїв.

1.3 Статистичні методи аналізу

Статистичний аналіз є ключовим інструментом для дослідження закономірностей у великих обсягах даних, оцінки невизначеності та прийняття обґрунтованих рішень. Використання статистичних методів дозволяє обробляти числову інформацію, визначати тенденції, робити прогнози та оцінювати достовірність результатів.

Залежно від цілей дослідження, статистичні методи аналізу поділяються на описові, дедуктивні, кореляційні, регресійні та інші. Вони використовуються в наукових дослідженнях, економіці, соціології, інженерії, медицини, фінансах та багатьох інших сферах [9].

Статистичні методи аналізу є потужним інструментом для дослідження даних, виявлення тенденцій та прийняття обґрунтованих рішень. Вони включають описові методи, які допомагають узагальнити дані, дедуктивні методи, які дозволяють робити висновки про загальну сукупність, кореляційний аналіз, який оцінює зв’язки між змінними, та регресійний аналіз, що використовується для прогнозування.

Ефективне використання статистичних методів дозволяє отримати точні результати та підвищити якість аналізу в різних сферах діяльності.

Статистичні методи відіграють ключову роль у аналізі мережевого трафіку, дозволяючи виявляти закономірності, аномалії та оптимізувати роботу:

- Оцінка середніх значень і розподілу. Статистика дозволяє визначити середню кількість трафіку за годину, день або місяць. Це допомагає встановити "нормальну" поведінку користувачів і навантаження на мережу.

- Виявлення аномалій. За допомогою дисперсії, стандартного відхилення або міжквартильного розмаху можна виявити різкі стрибки трафіку – наприклад, при DDoS-атаці або активності ботів.

- Аналіз трендів. З використанням регресійного аналізу можливо прогнозувати зростання навантаження, пікові години або необхідність розширення ресурсів.

- Кластеризація трафіку. Методи класифікації (наприклад, кластер-аналіз) дозволяють групувати користувачів за поведінкою: хто активно використовує відео, хто тільки читає новини, а хто завантажує великі об'єми даних.

- Побудова моделей безпеки. На основі статистики створюються базові моделі нормальної активності, і будь-яке відхилення (наприклад, надмірна кількість запитів) сигналізує про можливу загрозу.

- Кореляційний аналіз. Дозволяє виявити зв’язок між різними змінними – наприклад, між типом користувача і способом доступу до ресурсів.

Завдяки цим методам адміністратори можуть приймати обґрунтовані рішення, вчасно виявляти загрози і планувати розвиток мережі з урахуванням реального навантаження.

Приклад реального застосування статистичних методів у мережевому аналізі на основі інструментів PRTG Network Monitor та ntopng:

1. PRTG Network Monitor – прогнозування навантаження і виявлення піків. Адміністратор коледжу хоче визначити, коли найбільше навантаження на сервер Moodle. PRTG збирає часові ряди трафіку: обсяг вхідних/вихідних даних щохвилини. Обчислюється середнє навантаження, стандартне відхилення та виводяться графіки. Якщо спостерігається стрибок трафіку на 200% від середнього – система автоматично надсилає оповіщення. За допомогою тренд-аналізу можна спрогнозувати, коли навантаження буде перевищувати пропускну здатність. Ця статистика дозволяє виявляти пікові години (наприклад, 10:00–

12:00), прогнозувати потреби в додаткових ресурсах або балансуванні навантаження.

2. ntopng – аналіз поведінки користувачів та виявлення аномалій. Інтернет у корпусі повільний. Потрібно з'ясувати, хто генерує найбільше трафіку. Ntopng збирає статистику за IP-адресами, портами, доменами. За допомогою кластеризації трафік групується за типом: веб-серфінг, відео, P2P. Виявляється IP, який генерує аномальний трафік (наприклад, 10 ГБ за годину). Проводиться порівняльний аналіз з попередніми днями: якщо зростання > 3σ (три стандартні відхилення) – це вважається потенційною загрозою. Ця статистика дозволяє ідентифікувати користувачів, які використовують мережу нецільово, захистити від витоку трафіку, торентів, або ботнетів.

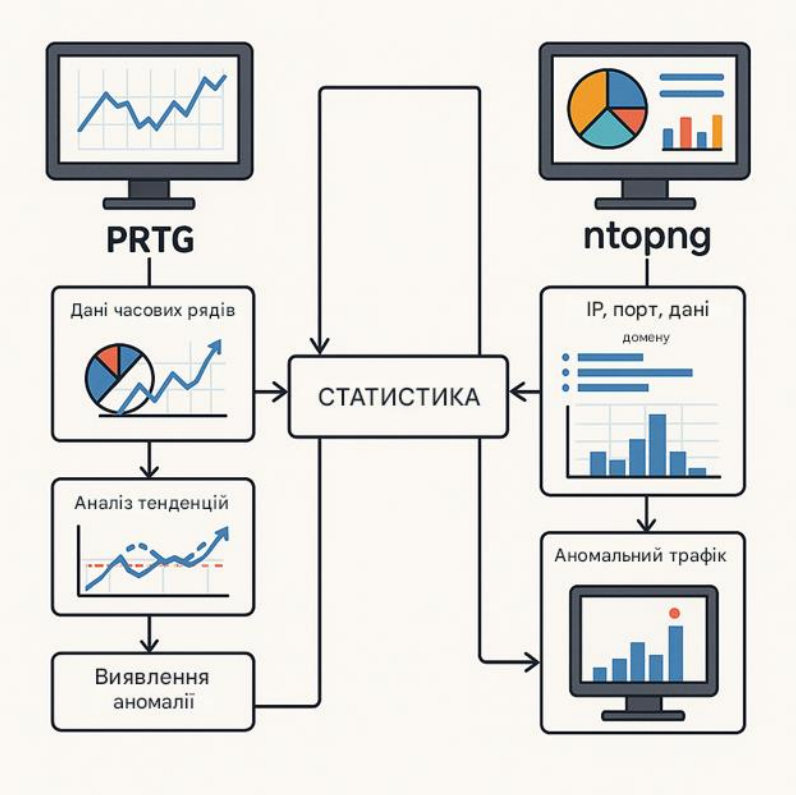

Рисунок 1.1 – Схематична візуалізація процесу статистичного аналізу

У цих прикладах статистика дозволяє не лише аналізувати поточну ситуацію, а й передбачати майбутні проблеми, приймати проактивні рішення та автоматично виявляти аномалії без ручної перевірки.

РОЗДІЛ 2
ЗАСОБИ АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ

2.1 Загальний огляд сучасних інструментів для аналізу трафіку

Аналіз мережевого трафіку є важливим завданням у сфері інформаційної безпеки, адміністрування мереж та оптимізації роботи інформаційних систем. Завдяки сучасним інструментам можна контролювати потоки даних, виявляти загрози, знаходити вузькі місця в інфраструктурі та покращувати продуктивність мережі.

Варто зазначити, що існують ключові сучасні інструменти для аналізу трафіку, які використовуються для різних цілей – від базового моніторингу до детекції аномалій та кіберзагроз.

1. Класифікація інструментів для аналізу трафіку [14].

Сучасні інструменти для аналізу мережевого трафіку можна розподілити на кілька категорій залежно від їх функціоналу та сфери застосування:

- Моніторингові системи – використовуються для постійного відстеження трафіку та візуалізації даних у реальному часі.

- Системи виявлення та запобігання вторгненням (IDS/IPS) – аналізують трафік для пошуку підозрілих активностей.

- Пакетні аналізатори (Sniffers) – захоплюють і детально аналізують мережеві пакети.

- Системи аналізу поведінки мережевого трафіку (NBA – Network Behavior Analysis) – виявляють аномалії та потенційні загрози.

- Програми для діагностики та тестування мережі – використовуються для перевірки пропускної здатності, затримок, якості з’єднання.

2. Популярні інструменти для аналізу мережевого трафіку [15]

2.1. Wireshark

Опис: один із найпопулярніших та найпотужніших аналізаторів мережевого трафіку з відкритим кодом.

Функції:

- Захоплення та детальний аналіз мережевих пакетів.

- Декодування різних мережевих протоколів.

- Візуалізація та фільтрація трафіку за різними параметрами.

Застосування: використовується адміністраторами мереж, інженерами з безпеки та фахівцями з тестування мереж.

2.2. SolarWinds NetFlow Traffic Analyzer

Опис: потужний комерційний інструмент для моніторингу трафіку та аналізу пропускної здатності.

Функції:

- Аналіз потоків NetFlow, J-Flow, sFlow.

- Виявлення перевантажень та аномалій у мережі.

- Візуалізація топології мережі та аналіз продуктивності.

Застосування: корпоративні мережі, великі організації, постачальники інтернет-послуг (конкретний приклад, як, ким або в якій службі або з якою метою).

2.3. PRTG Network Monitor

Опис: комплексний інструмент для моніторингу мережевої інфраструктури.

Функції:

- Контроль трафіку в режимі реального часу.

- Використання SNMP, WMI та NetFlow для збору даних.

- Автоматичне сповіщення про перевищення порогових значень. Порогове значення – це заздалегідь визначений рівень якогось показника (наприклад, трафіку, навантаження на сервер, температури обладнання), при перевищенні якого система вважає ситуацію потенційно критичною або ненормальною.

Як працює автоматичне сповіщення:

1. Налаштування порогу. Адміністратор задає граничне значення (наприклад, "якщо трафік перевищує 100 Мбіт/с протягом 5 хвилин").

2. Моніторинг у реальному часі. Система постійно збирає і порівнює поточні значення з установленим порогом.

3. Виявлення перевищення. Якщо значення перевищує встановлений рівень – система фіксує подію.

4. Сповіщення адміністратора. Надсилається автоматичне повідомлення (електронною поштою; через SMS або месенджер; у вигляді push-сповіщення або попередження в інтерфейсі.

Застосування: використовується адміністраторами мереж для контролю доступності та продуктивності серверів і пристроїв.

2.4. Zeek (раніше Bro IDS)

Опис: інструмент для аналізу мережевого трафіку та виявлення загроз із відкритим кодом.

Функції:

- Глибокий аналіз мережевих пакетів. Глибокий аналіз мережевих пакетів (англ. Deep Packet Inspection, DPI) – це процес детального вивчення вмісту мережевого трафіку на рівні окремих пакетів даних, а не лише заголовків. Такий аналіз дозволяє побачити, що саме передається, а не просто звідки і куди. Він передбачає: розбір усіх рівнів протоколів (застосовуються методи для аналізу даних з канального до прикладного рівня (наприклад, HTTP, FTP, DNS, TLS. Це дозволяє визначити тип застосунку, запит, передані файли або навіть вміст повідомлення); ідентифікувати застосунки (на основі вмісту, а не лише портів, система розпізнає, чи це YouTube, Telegram, VPN або Tor. Це важливо, оскільки багато сервісів використовують однакові порти; виявляти сигнатури загроз (порівнюються вміст пакетів з базами відомих шаблонів шкідливих дій (наприклад, експлойтів або команд з C2-серверів); фільтрувати та блокувати (DPI дозволяє блокувати конкретні типи трафіку (наприклад, завантаження .exe-файлів або доступ до певних сайтів) на основі вмісту пакета)

Методи, які застосовуються: сигнатурний аналіз – пошук відомих шаблонів трафіку (використовується, наприклад, у Suricata, Snort); статистичний аналіз – вивчення структури трафіку для виявлення нетипової поведінки

(наприклад, частоти запитів); аналіз поведінки – моделювання "нормального" трафіку й виявлення відхилень (метод корисний для zero-day атак); регулярні вирази та парсинг протоколів – для розбору вмісту повідомлень у конкретних форматах.

- Виявлення вторгнень та аномалій у трафіку.

Програма Zeek генерує структуровані журнали (логи), які відображають активність у мережевому трафіку. Основними вихідними результатами є файли логів (conn.log – зведення всіх з'єднань у мережі; dns.log – запити DNS; http.log – HTTP-трафік; notice.log – попередження про підозрілу активність; weird.log – зафіксовані аномалії або нестандартна поведінка).

Zeek не приймає автоматичних рішень щодо блокування або реагування. Він лише аналізує трафік і створює логи, в яких описує події та аномалії. Рішення приймає адміністратор безпеки, який аналізує вихідні дані та вирішує, чи є зафіксована поведінка загрозою. Проте, адміністратор або інженер може вказати правила та політики в скриптах Zeek, що дозволяють визначати підозрілу поведінку автоматично й формувати відповідні сповіщення. Таким чином, Zeek виконує роль детального спостерігача, а остаточне рішення — за фахівцем або заздалегідь налаштованими політиками.

- Автоматизація аналізу трафіку за допомогою скриптів.

Застосування: використовується в кібербезпеці та дослідженні загроз.

2.5. NetFlow Analyzer (ManageEngine)

Опис: потужний інструмент для аналізу мережевого трафіку та виявлення проблем із пропускною здатністю.

Функції:

- Аналіз потоків трафіку NetFlow, sFlow, J-Flow.

- Виявлення перевантажень та неефективного використання мережевих ресурсів. Неефективне використання мережевих ресурсів – це ситуація, коли пропускна здатність, канали зв’язку або серверні ресурси використовуються не за призначенням, надмірно або з низькою продуктивністю. Це знижує загальну ефективність роботи мережі та може призводити до перевантажень або затримок.

Неефективне використання визначається аналізом пропускної здатності каналів, виявленням "важких" користувачів або пристроїв, аналізом простоїв і затримок, виявленням нецільового трафіку, неправильним балансування трафіку.

- Створення детальних звітів про трафік.

Застосування: використовується в середніх та великих організаціях для оптимізації мережевих потоків, що передбачає собою процес покращення способу, яким дані передаються мережею, з метою зменшення затримок, уникнення перевантажень і забезпечення стабільного та ефективного зв’язку між пристроями і сервісами.

Результати даного аналізу можуть застосовуватися:

а) адміністратором мережі. Вручну переглядає звіти, щоб виявити вузькі місця, ненормальну активність або підозрілу поведінку. Приймає рішення щодо оптимізації мережі, зміни конфігурацій або ізоляції потенційних загроз.

б) автоматично (залежно від налаштувань). NetFlow Analyzer може створювати тригери (оповіщення) на основі встановлених порогів чи шаблонів аномальної активності. Інтегрується з системами реагування (SIEM або інші NMS), щоб запускати сценарії автоматичного реагування (наприклад, повідомлення, блокування IP).

Отже, використання результатів може бути як ручним, так і автоматизованим, в залежності від політик безпеки організації та рівня інтеграції з іншими системами.

2.6. Suricata

Опис: високопродуктивна система виявлення вторгнень (IDS) та аналізу трафіку.

Функції:

- Аналіз трафіку на рівні пакетів та потоків.

- Виявлення загроз у реальному часі.

- Підтримка багатопотокової обробки трафіку.

Застосування: кібербезпека, моніторинг мережі, захист корпоративних мереж.

2.7. Tcpdump

Опис: консольний інструмент для перехоплення та аналізу мережевого трафіку.

Функції:

- Захоплення трафіку в режимі реального часу.

- Фільтрація пакетів за допомогою виразів BPF (Berkeley Packet Filter).

- Низькорівневий аналіз трафіку.

Застосування: використовується для швидкого аналізу трафіку в командному рядку.

3. Вибір оптимального інструменту

Вибір конкретного інструменту для аналізу трафіку залежить від поставлених завдань:

Таблиця 2.1 – Рекомендовані інструменти для застосування аналізу трафіку [16, 17]

Завдання	Рекомендований інструмент
Глибокий аналіз пакетів	Wireshark, Tcpdump
Моніторинг трафіку	PRTG Network Monitor, NetFlow Analyzer
Виявлення загроз	Suricata, Zeek
Аналіз пропускної здатності	SolarWinds NetFlow Analyzer
Консольний аналіз трафіку	Tcpdump

Якщо необхідний детальний аналіз окремих пакетів, найкраще підходять Wireshark або Tcpdump. Для моніторингу великих мереж оптимальними будуть SolarWinds NetFlow Analyzer або PRTG Network Monitor. Для виявлення загроз використовуються Suricata або Zeek.

Аналіз мережевого трафіку є важливою частиною адміністрування та кібербезпеки мережі. Сучасні інструменти дозволяють детально вивчати пакети, аналізувати поведінку користувачів, виявляти аномалії та запобігати загрозам. Вибір інструменту залежить від конкретних потреб та можливостей мережі.

Використання сучасних засобів для аналізу трафіку сприяє підвищенню ефективності роботи мережі, зниженню ризиків атак та оптимізації використання ресурсів.

2.2 Характеристика програми (Wireshark, Nmap, SolarWinds, PRTG)

Аналіз мережевого трафіку та моніторинг мережі є ключовими аспектами забезпечення інформаційної безпеки, діагностики проблем у мережі та оптимізації її роботи. Для цього використовуються різні програмні інструменти, які дозволяють отримувати детальну інформацію про пакети, пристрої, трафік та потенційні загрози в мережі.

Серед найпопулярніших та найефективніших програм у цій сфері виділяються Wireshark, Nmap, SolarWinds та PRTG Network Monitor. Кожна з них має свої унікальні можливості, які дозволяють вирішувати широкий спектр завдань.

1. Wireshark

1.1. Загальний опис.

Wireshark – це потужний та популярний аналізатор мережевого трафіку з відкритим вихідним кодом. Він дозволяє захоплювати та аналізувати пакети даних у режимі реального часу, що робить його незамінним інструментом для мережевих адміністраторів, спеціалістів із кібербезпеки та дослідників [18].

1.2. Основні функції:

- захоплення мережевого трафіку в режимі реального часу;

- підтримка великої кількості мережевих протоколів (TCP, UDP, ICMP, HTTP, FTP тощо);

- фільтрація та сортування пакетів для детального аналізу;

- візуалізація даних у вигляді графіків та таблиць;

- аналіз продуктивності мережі та виявлення проблем.

1.3. Сфера застосування:

- виявлення несправностей у мережі (проблеми з підключенням, затримки та втрати пакетів, дублювання або пошкодження пакетів, петлі в мережі, DNS-помилки, неправильна маршрутизація, ARP-конфлікти або отруєння кешу, проблеми з NAT і PAT, зайвий або "шумний" трафік);

- аналіз безпеки трафіку та пошук можливих атак;

- оптимізація продуктивності мережевих з’єднань.

1.4. Переваги та недоліки

Переваги:

- Безкоштовне використання.

- Великий набір фільтрів для аналізу.

- Гнучкість і підтримка багатьох форматів збереження даних.

Недоліки:

- Високий рівень складності для початківців.

- Не підходить для моніторингу трафіку у великих мережах у режимі реального часу через низку технічних обмежень, які пов’язані з його архітектурою, продуктивністю та призначенням (орієнтований на глибокий аналіз, а не моніторинг, високе навантаження на ресурси, обмежена масштабованість, немає системи сповіщень або автоматичної аналітики, відсутність довготривалого зберігання даних, проблеми з безпекою при безперервному захопленні).

2. Nmap

2.1. Загальний опис.

Nmap (Network Mapper) – це потужний інструмент для сканування мереж та збору інформації про пристрої, що до неї підключені. Він широко використовується для виявлення відкритих портів, перевірки безпеки мережі та аудиту підключених пристроїв [19].

2.2. Основні функції:

- визначення активних хостів у мережі;

- сканування відкритих портів і визначення запущених сервісів;

- виявлення операційної системи віддалених пристроїв;

- виявлення вразливостей у мережевих службах (відкриті або небезпечні порти, невірні конфігурації сервісів, анонімний доступ до FTP або SMB, відкриті проксі-сервери або ретранслятори пошти (SMTP relay), DNS-сервери, відкриті для рекурсії);

- використання скриптів для автоматизації аналізу.

2.3. Сфера застосування:

- аудит безпеки мережі;

- виявлення несанкціонованих пристроїв у корпоративній мережі;

- пошук вразливостей у сервісах (застарілі версії сервісів, неправильно налаштовані служби, SMTP-релей, наявність бекдорів або стандартних облікових даних, SNMP з публічними паролями).

2.4. Переваги та недоліки

Переваги:

- висока ефективність у виявленні відкритих портів і сервісів;

- гнучкість завдяки підтримці скриптів;

- безкоштовна ліцензія;

Недоліки:

- використання може бути розцінене як потенційна атака на мережу;

- вимагає глибокого розуміння мережевих технологій.

3. SolarWinds Network Performance Monitor

3.1. Загальний опис

SolarWinds – це комерційна система для моніторингу мережевої інфраструктури, що забезпечує повний контроль за продуктивністю мережі та допомагає швидко реагувати на можливі проблеми.

3.2. Основні функції:

- моніторинг продуктивності мережевого обладнання та серверів. Основою для аналізу є мережеві протоколи моніторингу, такі як SNMP (Simple Network Management Protocol), WMI (Windows Management Instrumentation), NetFlow, а також ICMP-пінги та API-запити. Результатом моніторингу є візуалізація завантаження пристроїв (CPU, пам’ять, диск, трафік); графіки трафіку між вузлами мережі; автоматичні сповіщення (alerts) про перевищення критичних показників або збої; звіти про продуктивність обладнання в реальному часі та за обрані періоди; виявлення “вузьких місць” у мережі, перевантажень або нестабільної роботи; планування оновлення або заміни обладнання на основі історичних даних.

- виявлення перевантажень у мережі;

- візуалізація трафіку та звітність;

- виявлення аномальної поведінки в мережі. Аномальна поведінка в мережі – це дії чи події, які відхиляються від звичного або очікуваного шаблону роботи мережі. Звіти про аномалії зазвичай надаються у вигляді інтерактивних дашбордів з візуалізацією даних (графіки, часові шкали, карти трафіку); автоматичних сповіщень (email, SMS, push) у разі виявлення підозрілої активності; докладних логів або журналів подій, де зазначено джерело, тип аномалії, час, IP-адреси, користувача тощо; аналітичних звітів із поясненням потенційного ризику, ймовірності загрози та рекомендаціями щодо реагування;

- інтеграція з іншими системами безпеки та адміністрування.

3.3. Сфера застосування:

- корпоративні мережі з великою кількістю пристроїв;

- Інтернет-провайдери та центри обробки даних;

- оптимізація продуктивності мережі. Продуктивність мережі в системах типу SolarWinds (використовується для мережевого моніторингу, продуктивності серверів, баз даних і систем безпеки.) визначається за сукупністю ключових показників, зокрема:

а) пропускна здатність (Bandwidth Usage) — кількість даних, що передається через мережу за певний період;

б) затримка (Latency) – час, необхідний для передачі пакету від джерела до призначення;

в) втрати пакетів (Packet Loss) – кількість пакетів, які не дійшли до адресата;

г) час відгуку (Response Time) – швидкість реакції мережевих пристроїв або сервісів на запит;

д) завантаження мережевих інтерфейсів і пристроїв — використання процесора, пам’яті, дискових ресурсів тощо.

Оптимізація продуктивності з використанням SolarWinds здійснюється за допомогою таких механізмів:

а) моніторинг у реальному часі. Система постійно відстежує стан мережевих елементів, аналізуючи трафік, навантаження та інші показники, щоб виявляти вузькі місця або потенційні проблеми;

б) визначення базових значень (Baseline). SolarWinds формує уявлення про нормальний стан мережі на основі історичних даних. Відхилення від цієї норми сигналізують про потенційні проблеми.

в) автоматичні оповіщення та звіти. При виявленні порушень у продуктивності система надсилає повідомлення та формує звіти, які допомагають адміністраторам швидко реагувати.

г) Ідентифікація “вузьких місць”. Виявляються сегменти мережі або пристрої, які працюють на межі своїх можливостей, що дозволяє вчасно розширити ресурси або змінити конфігурацію.

д) оптимізація маршрутів і балансування навантаження. Система може рекомендувати зміни в маршрутизації чи впровадження механізмів рівномірного розподілу трафіку між ресурсами.

е) історичний аналіз і прогнозування. За допомогою аналізу трендів можна передбачити майбутні проблеми продуктивності та вжити заходів до їх виникнення.

3.4. Переваги та недоліки

Переваги:

- висока точність аналізу продуктивності;

- зручний інтерфейс із візуалізацією даних;

- інтеграція з різними пристроями та сервісами.

Недоліки:

- висока вартість ліцензії;

- високі вимоги до ресурсів сервера, зокрема:

А. Процесор (CPU). SolarWinds виконує постійний аналіз великої кількості мережевих даних, збирання метрик, обробку SNMP-запитів, NetFlow, syslog-повідомлень тощо. Ці задачі потребують потужного багатоядерного процесора, особливо при моніторингу великої кількості пристроїв чи інтерфейсів.

Б. Оперативна пам’ять (RAM). У системі активно використовуються аналітичні модулі, візуалізація даних у реальному часі та обробка історичних логів. Це все завантажує оперативну пам’ять. При великих обсягах даних або складних звітах RAM може швидко заповнюватися, що впливає на загальну швидкодію.

В. Місце на диску (Storage). SolarWinds зберігає велику кількість даних: журнали подій, історичні метрики, NetFlow-записи, конфігураційні архіви та резервні копії. Чим більше точок моніторингу й довший період зберігання даних, тим більше потрібно дискового простору.

Г. База даних (SQL Server). Система активно взаємодіє з базою даних (переважно Microsoft SQL Server), в яку записуються всі зібрані дані. Високе навантаження на диск і пам’ять також зумовлене потребами бази у швидкому зчитуванні та збереженні інформації, особливо під час формування звітів або виконання запитів.

Д Мережеві ресурси. SolarWinds постійно обмінюється даними з пристроями в мережі. Для цього потрібна стабільна й пропускна мережева інфраструктура. Якщо мережа перевантажена, зростає час збору даних, що впливає на точність і актуальність аналітики.

Через ці вимоги розгортання SolarWinds потребує ретельного планування інфраструктури, особливо в масштабних середовищах. Потрібно враховувати не лише технічні характеристики, але й передбачуване зростання навантаження з часом.

4. PRTG Network Monitor [20]

4.1. Загальний опис

PRTG Network Monitor – це універсальний інструмент для моніторингу мережі, який дозволяє контролювати використання ресурсів, трафік та доступність сервісів у режимі реального часу.

4.2. Основні функції:

- моніторинг серверів, маршрутизаторів, комутаторів (моніторинг доступності (Uptime Monitoring), контроль за навантаженням і ресурсами, аналіз трафіку, моніторинг портів і інтерфейсів, виявлення несправностей та оповіщення, моніторинг служб і додатків, візуалізація та звітність, моніторинг віртуального середовища);

- виявлення проблем у роботі пристроїв (приклад: виявлення перевантаження мережевого комутатора. PRTG встановлює датчики (сенсори) на порти комутатора через SNMP. У звичайному режимі система фіксує стабільний трафік, але раптом один із портів починає показувати різке зростання навантаження – швидкість передачі даних наближається до максимальної пропускної здатності порту. У той же час зростає кількість втрачених пакетів і помилок передачі. PRTG визначає, що трафік перевищує встановлений поріг, і: автоматично надсилає адміністратору попередження електронною поштою; відображає інцидент на дашборді як критичний; пропонує переглянути джерело трафіку (наприклад, IP-адресу чи пристрій, який генерує надмірне навантаження).Таким чином, адміністратор має змогу швидко локалізувати проблему – наприклад, цикл у мережі, неправильне налаштування або вірусну активність – і вжити заходів до того, як це вплине на всю мережу);

- аналіз використання мережевого трафіку у зручній та наочно візуалізованій формі, що дозволяє швидко оцінити стан мережі та виявити потенційні проблеми (графіки та діаграми, інтерактивні дашборди, таблиці зі статистикою, тор-списки ("Top Talkers"), автоматичні звіти, історичні дані та тренди);

- автоматичне оповіщення про збої (втрата зв’язку з пристроєм, перевищення допустимого навантаження, збій у роботі сервісу, проблеми з мережею, недоступність інтерфейсів або портів);

- інтеграція з іншими системами моніторингу.

4.3. Сфера застосування:

- моніторинг корпоративних мереж;

- контроль продуктивності серверів;

- аналіз трафіку та пошук аномалій.

4.4. Переваги та недоліки

Переваги:

- простота налаштування та використання;

- візуалізація даних у вигляді графіків і звітів;

- гнучка система сповіщень.

Недоліки:

- безкоштовна версія має обмежену кількість сенсорів (у безкоштовній версії PRTG Network Monitor доступно до 100 сенсорів. Один сенсор в PRTG – це окрема точка моніторингу, Кількість необхідних сенсорів залежить від розміру інфраструктури та глибини моніторингу: а) невеликий офіс (5–10 пристроїв) – може вкластися у межі безкоштовної версії, якщо моніторити лише базові параметри (наприклад, ping, CPU, пам’ять, диск – по 3–5 сенсорів на пристрій); б) середня мережа (20+ пристроїв) – часто потребує 300–1000 сенсорів, якщо включити більш детальний контроль: служби, порти, трафік, журнали подій тощо; в) великі або критичні системи – використовують тисячі сенсорів, щоб забезпечити безперервне, глибоке спостереження за всіма компонентами);

- високе навантаження на сервер при аналізі великих мереж.

Програми Wireshark, Nmap, SolarWinds та PRTG є одними з найкращих інструментів для аналізу мережевого трафіку та моніторингу продуктивності мережі.

Таблиця 2.2 – Переваги та недоліки програм (Wireshark, Nmap, SolarWinds, PRTG) [21, 22]

Програма	Основне призначення	Переваги	Недоліки
Wireshark	Аналіз трафіку на рівні пакетів	Потужні фільтри, безкоштовна	Складність для початківців

Nmap	Сканування портів та виявлення пристроїв	Гнучкість, безкоштовність	Вимагає знань мереж
SolarWinds	Корпоративний моніторинг	Висока точність, гнучкість	Висока вартість
PRTG	Загальний моніторинг мережі	Простота, зручність	Обмеження в безкоштовній версії

Вибір відповідного інструменту залежить від завдань, масштабів мережі та бюджету.

Для мережевої інфраструктури коледжу найкращим вибором часто є PRTG Network Monitor, оскільки він пропонує зручний інтерфейс, автоматичне оповіщення про збої, візуалізацію трафіку та загальний контроль за пристроями. Безкоштовної версії з 100 сенсорами зазвичай вистачає для базового моніторингу серверів, маршрутизаторів, принтерів і точок доступу.

Однак у залежності від конкретних потреб можуть застосовуватись й інші інструменти:

Wireshark – корисний для глибокого аналізу мережевого трафіку на рівні пакетів, але він не забезпечує постійного моніторингу і не підходить для спостереження за всією мережею в реальному часі. Зручний для викладачів та студентів у навчальних цілях.

Nmap – ефективний для сканування мережі, виявлення пристроїв, відкритих портів і перевірки безпеки. Добрий як додатковий інструмент, але не замінює повноцінну систему моніторингу.

SolarWinds – дуже потужна та гнучка платформа, але вимагає значних ресурсів і коштів, що може бути надмірним для типового коледжу.

PRTG – оптимальний варіант для коледжу: достатньо функціональний, безкоштовний у базовій версії, простий у налаштуванні та обслуговуванні. Для навчання й аналізу можна доповнити його Wireshark та Nmap.

2.3 Порівняльний аналіз засобів мережевого трафіку

Мережевий трафік є ключовим аспектом функціонування сучасних інформаційних систем. Його аналіз дозволяє не лише діагностувати проблеми в

мережі, а й виявляти потенційні загрози, контролювати використання ресурсів та забезпечувати оптимальну продуктивність мережевих з’єднань. Для цих цілей існує широкий спектр інструментів, які відрізняються своїм функціоналом, підходами до аналізу, можливостями моніторингу та рівнем складності використання.

У цьому доцільно провести саме порівняльний аналіз найпопулярніших засобів для аналізу мережевого трафіку: Wireshark, Nmap, SolarWinds Network Performance Monitor та PRTG Network Monitor.

1. Основні критерії для порівняння [23]

Щоб об’єктивно оцінити кожен інструмент, розглянемо їх за такими параметрами:

- призначення – основна функціональність програми;

- спосіб збору даних – активний чи пасивний моніторинг;

- можливості аналізу трафіку – які типи даних аналізуються та як вони представлені;

- зручність використання – простота налаштування та інтерфейсу;

- гнучкість та масштабованість – можливість використання у малих і великих мережах;

- вартість – наявність безкоштовної версії чи ліцензійної моделі.

2. Порівняння засобів аналізу мережевого трафіку

Таблиця 2.3 – Параметри порівняння засобів аналізу мережевого трафіку [24, 25]

Критерій	Wireshark	Nmap	SolarWinds Network Performance Monitor	PRTG Network Monitor
Призначення	Глибокий аналіз мережевого трафіку на рівні пакетів	Сканування мережі, виявлення пристроїв та портів	Моніторинг продуктивності мережі та обладнання	Комплексний моніторинг мережі та її складових
Спосіб збору даних	Пасивний – захоплення та аналіз трафіку	Активний – сканування мережі та пристроїв	Пасивний – моніторинг мережі в режимі реального часу	Пасивний – аналіз мережевого середовища
Можливості аналізу	Аналіз мережевих пакетів, виявлення аномалій, детальна інформація про протоколи	Визначення активних хостів, відкритих портів, виявлення сервісів та операційних систем	Виявлення перевантажень, контроль серверів, аналіз продуктивності мережі	Моніторинг трафіку, контроль серверів, управління мережею
Зручність використання	Висока складність для початківців	Складний у налаштуванні, необхідні знання про мережі	Інтуїтивно зрозумілий інтерфейс	Простий у налаштуванні та використанні
Гнучкість та масштабованість	Підходить для аналізу невеликих та середніх мереж	Використовується для різного масштабу мереж	Найкраще підходить для великих корпоративних мереж	Підходить як для малих, так і для великих компаній
Вартість	Безкоштовний	Безкоштовний	Платний, висока вартість	Безкоштовний до 100 сенсорів, далі платний

3. Детальний аналіз кожного інструменту

3.1. Wireshark

Переваги:

- найдетальніший аналіз мережевого трафіку;

- безкоштовний і підтримує велику кількість протоколів;

- можливість збереження та повторного аналізу трафіку.

Недоліки:

- висока складність для початківців;

- не підходить для аналізу трафіку великих мереж у режимі реального часу;

- потрібен досвід у використанні фільтрів для ефективного аналізу.

Використовувати Wireshark ідеально підходить для глибокого аналізу мережевого трафіку, виявлення проблем із мережевими протоколами, аналізу атак на рівні пакетів.

3.2. Nmap

Переваги:

- висока швидкість сканування мережі;

- дозволяє виявляти відкриті порти, запущені сервіси та операційні системи;

- гнучкість завдяки можливості написання скриптів.

Недоліки:

- вимагає глибоких знань про мережеві протоколи та технології;

- використання може викликати підозри в мережевих адміністраторів (розцінюється як потенційна атака);

- відсутність візуального представлення результатів.

Nmap найкраще підходить для сканування мережі, виявлення вразливостей та перевірки безпеки мережевого оточення.

3.3. SolarWinds Network Performance Monitor

Переваги:

- висока точність у виявленні перевантажень мережі;

- інтуїтивно зрозумілий інтерфейс із візуалізацією даних;

- інтеграція з іншими мережевими рішеннями. Приклад інтеграції: з системою ServiceNow. SolarWinds NPM можна інтегрувати з ServiceNow – платформою для управління IT-процесами та інцидентами. Завдяки цій інтеграції: при виявленні збою або критичної події в мережі SolarWinds автоматично створює інцидент у ServiceNow. Інцидент містить детальну інформацію про пристрій, час помилки, тип збою та інші діагностичні дані; служба підтримки отримує сповіщення й одразу бачить джерело проблеми без

необхідності перемикатися між системами; після усунення проблеми SolarWinds може оновити або закрити інцидент у ServiceNow автоматично. Це дозволяє значно пришвидшити реагування на проблеми, покращити координацію між командами та зменшити простої. Окрім ServiceNow, SolarWinds також може інтегруватися з такими інструментами, як Splunk (для аналітики логів), Microsoft Teams (для сповіщень), VMware (для моніторингу віртуалізації) тощо).

Недоліки:

- висока вартість ліцензії;

- вимагає значних обчислювальних ресурсів;

- надмірно складний для малих підприємств. Основні причини складності:

а) складна структура розгортання. Програмне забезпечення вимагає встановлення на потужному сервері, налаштування бази даних (наприклад, SQL Server) і конфігурації мережевих елементів. Для малого бізнесу без окремого IT-відділу це може бути проблематично.

б) Перевантаженість функціями. NPM орієнтований на великі мережі та корпоративне середовище, тому містить безліч функцій, які малому бізнесу просто не потрібні — наприклад, глибока сегментація мережі, SLA-аналітика, підтримка розподілених середовищ тощо.

в) Складність в інтерфейсі та налаштуваннях. Інтерфейс системи хоч і гнучкий, але містить багато рівнів конфігурацій, панелей, параметрів моніторингу. Для новачка або адміністратора без досвіду це може виглядати заплутано й вимагати додаткового навчання.

г) Високі вимоги до технічних ресурсів. Для стабільної роботи NPM потребує значного обсягу оперативної пам’яті, дискового простору та обчислювальної потужності, що може виявитися надмірним для невеликого офісного сервера.

д) дорогі ліцензії та обслуговування. Окрім складності, важливим бар’єром є висока вартість самої платформи, що не завжди виправдано при невеликій кількості пристроїв у мережі.

Для малого підприємства, де достатньо базового моніторингу доступності та навантаження пристроїв, SolarWinds NPM може бути надмірним за функціоналом і складністю. У таких випадках простіші рішення – як-от PRTG, Zabbix або Nagios – часто виявляються ефективнішими та зручнішими. SolarWinds найкраще підходить для моніторингу корпоративних мереж великих підприємств та провайдерів.

3.4. PRTG Network Monitor

Переваги:

- простий у використанні;
- гнучка система оповіщень;
- візуалізація даних у вигляді графіків і звітів.

Недоліки:

- безкоштовна версія обмежена до 100 сенсорів;
- високе навантаження на сервер при аналізі великих мереж.

PRTG є чудовим рішенням для моніторингу середніх і великих компаній, оскільки забезпечує комплексний контроль за мережею та її продуктивністю.

Вибір інструменту для аналізу мережевого трафіку залежить від поставлених цілей:

- Wireshark – для глибокого аналізу пакетів.
- Nmap – для активного сканування мережі та пошуку уразливостей.
- SolarWinds – для корпоративного моніторингу продуктивності мережі.
- PRTG – для комплексного контролю мережі з простим інтерфейсом.

Кожен із цих інструментів має свої сильні сторони та найкраще підходить для певних сценаріїв використання.

РОЗДІЛ 3
ПРИКЛАДИ ВИКОРИСТАННЯ ЗАСОБІВ МЕРЕЖЕВОГО ТРАФІКУ

3.1 Використання інструментів мережевого трафіку на практиці

Використання засобів аналізу мережевого трафіку є ключовим елементом в управлінні сучасними комп'ютерними мережами. Ці інструменти дозволяють здійснювати моніторинг, аналіз, безпеку, оптимізацію і прогнозування навантажень, забезпечуючи надійну, стабільну й безпечну роботу всієї мережевої інфраструктури.

Засоби моніторингу та аналізу трафіку – це програмні або апаратно-програмні рішення, що дозволяють збирати, обробляти та аналізувати дані, що проходять через мережу. Вони визначають, які пристрої використовують трафік, якого типу цей трафік (HTTP, FTP, VoIP тощо), і чи є підозріла активність або аномалії.

Основні задачі, які вирішують такі інструменти [26]:

- виявлення перевантажень та "вузьких місць";
- аналіз ефективності використання пропускної здатності
- забезпечення кібербезпеки (виявлення DDoS-атак, шкідливого ПЗ);
- контроль використання ресурсів (QoS, політики доступу);
- аудит діяльності користувачів та служб;
- прогнозування та планування масштабування інфраструктури.

Доцільно навести актуальні приклади використання засобів моніторингу трафіку.

1. Локальна мережа організації

Досліджено, що під час іспитів виникають скарги на уповільнення Wi-Fi. Інструмент: NetFlow Analyzer або ntopng. Результат - виявлено великий обсяг трафіку, пов'язаний із стримінговими сервісами. Запроваджено фільтрацію по URL на час іспитів – зменшення навантаження на 40%. (Рис.3.1)

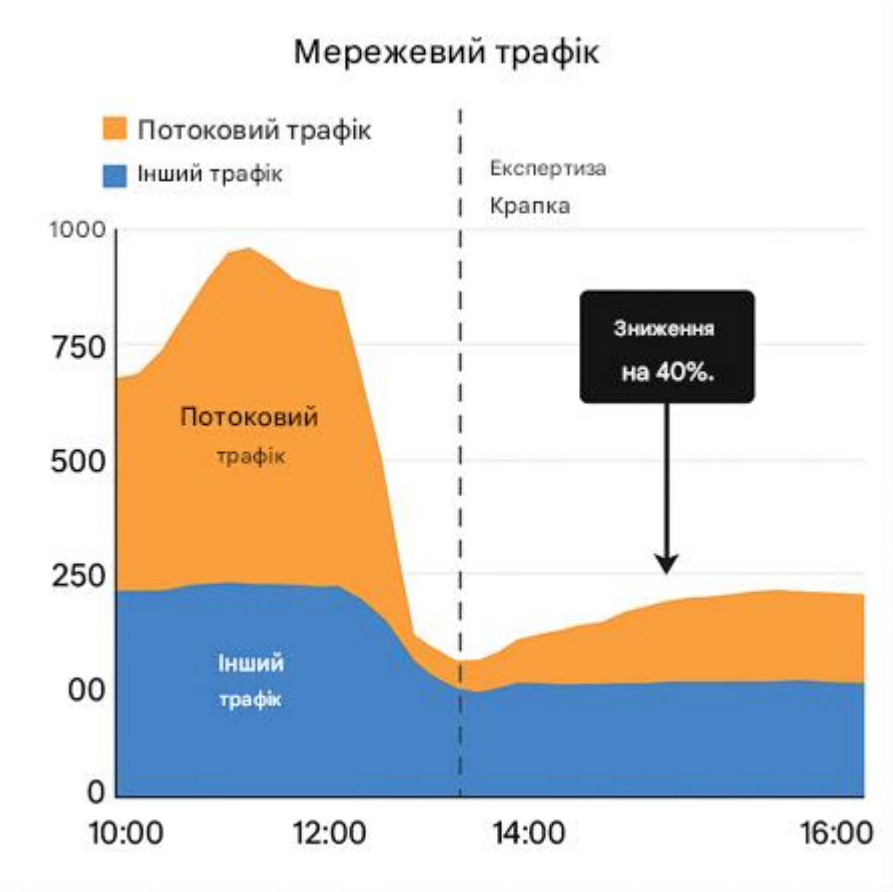

Рисунок 3.1 – Фільтрацію по URL на час іспитів та зменшення навантаження

Засоби моніторингу трафіку в мережі навчального закладу використовуються для забезпечення стабільної, безпечної та ефективної роботи всієї IT-інфраструктури. На практиці вони виконують кілька ключових функцій:

1. Контроль пропускної здатності. Моніторинг дозволяє визначити, які пристрої або додатки споживають найбільше трафіку. Наприклад, під час дистанційного навчання можна виявити, що відеоконференції (Zoom, Google Meet) створюють пікові навантаження на мережу, і відповідно – оптимізувати розподіл пропускної здатності.

Приклад: за допомогою інструменту NetFlow Analyzer або PRTG Network Monitor адміністратор бачить, що велика частина трафіку витрачається на потокове відео неакадемічного характеру (YouTube – найпоширеніше джерело неакадемічного відео, TikTok – короткі відео, що часто споживають багато трафіку, Instagram (Reels, Live) – відеоконтент, який навантажує мережу,

Facebook Video – стримінги, записи, прямі ефіри). Це може призвести до обмеження доступу до непотрібних ресурсів у робочий час.

2. Виявлення аномалій і загроз. Моніторингові системи в режимі реального часу виявляють незвичайну активність — наприклад, великі об’єми вихідного трафіку, спроби доступу до заборонених сайтів або підозрілу активність, що може вказувати на шкідливе ПЗ.

Приклад: система Zabbix або Wireshark виявляє численні підключення з певного комп’ютера до зовнішніх IP-адрес — це може бути симптомом ботнет-інфікування, і такий пристрій ізолюють для перевірки.

3. Планування інфраструктури. Аналітика, отримана з моніторингу, використовується для планування оновлення мережевого обладнання, розширення вузлів, або підключення нових корпусів до основної мережі закладу.

Приклад: щомісячні звіти з SolarWinds Network Performance Monitor демонструють постійне перевантаження маршрутизатора в головному корпусі – це сигнал для модернізації обладнання або впровадження балансувальника навантаження.

4. Підвищення продуктивності користувачів. Моніторинг допомагає виявити та усунути "вузькі місця", що впливають на якість доступу студентів і викладачів до онлайн-платформ, бібліотек, хмарних сервісів тощо.

Приклад: якщо Moodle постійно зависає в певні години, моніторинг за допомогою Nagios допоможе визначити причину – наприклад, перевантаження сервера або повільний DNS-запит.

2. Організація з віддаленими офісами

Завдання: Оптимізувати маршрутизацію трафіку між офісами. Інструмент: Wireshark + SolarWinds NTA Результат: Аналіз показав неефективну маршрутизацію для офісів, розташованих у східному регіоні. Проведено зміну маршрутів – зниження затримок на 25%. (Рис. 3.2)

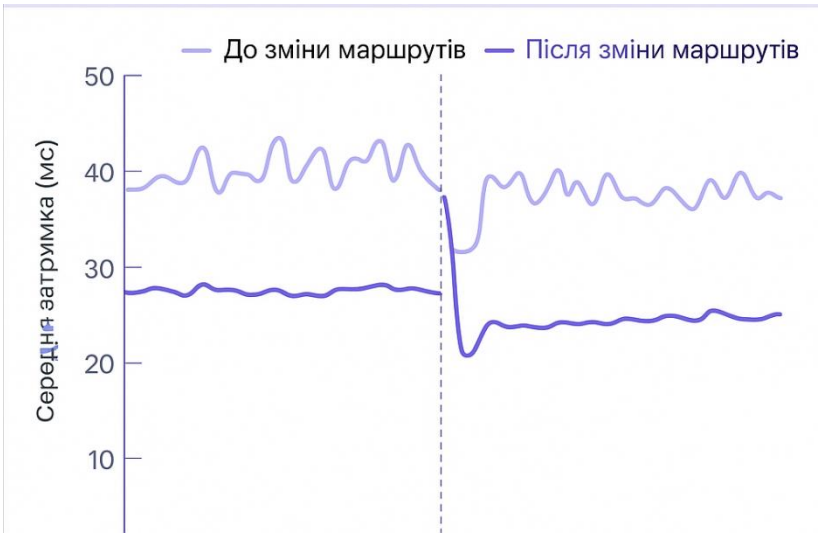

Рисунок 3.2 – Маршрутизація для офісів інструментами Wireshark + SolarWinds NTA

В організаціях з віддаленими офісами засоби моніторингу мережевого трафіку є важливою частиною IT-інфраструктури, оскільки дозволяють забезпечити стабільний, безпечний та ефективний обмін даними між головним офісом і філіями, а також контролювати якість сервісів незалежно від географічного розташування.

Ось як це працює на практиці:

1. Централізоване спостереження за мережею. Організація зазвичай використовують централізовані системи моніторингу, які дозволяють з одного інтерфейсу бачити трафік усіх філій. Це полегшує адміністрування і прискорює реагування на проблеми.

Приклад: компанія використовує PRTG Network Monitor або SolarWinds NPM, щоб переглядати трафік з усіх віддалених офісів, виявляти затримки, розриви VPN-з’єднань чи перевантаження каналів зв’язку.

2. Оптимізація пропускної здатності каналів. Використовуючи моніторинг, IT-фахівці можуть визначити, чи не перевантажені канали в окремих офісах, і в разі потреби оптимізувати трафік, впроваджуючи QoS (Quality of Service) або пріоритезацію критичних додатків.

Приклад: у логістичній компанії моніторинг показав, що під час відеоконференцій уповільнюється обробка замовлень у CRM-системі. Трафік було переналаштовано, щоб дати перевагу бізнес-додаткам через QoS (Quality of Service) та налаштування пріоритетів трафіку на мережевому обладнанні, а саме: налаштування QoS (якість обслуговування), обмеження ширини каналу (Bandwidth Throttling), використання моніторингових систем (Рис. 3.3).

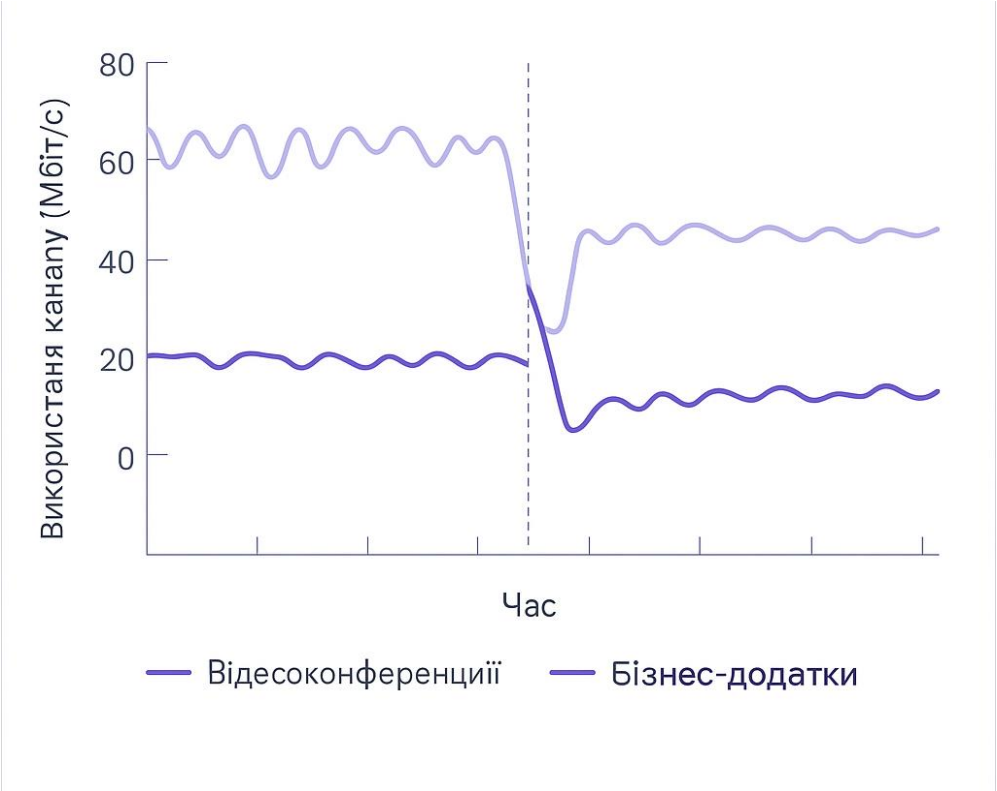

Рисунок 3.3 – Налаштування пріоритетів трафіку на мережевому обладнанні

3. Контроль доступу до ресурсів. Засоби моніторингу дозволяють відстежувати, які сервіси використовуються в офісах, що допомагає виявити несанкціоновані підключення або використання мережі не за призначенням.

Приклад: за допомогою NetFlow Analyzer було виявлено підозрілу активність з боку одного з філіалів, де працівники активно використовували стримінгові сервіси, що створювало зайве навантаження на мережу (Рис 3.4).

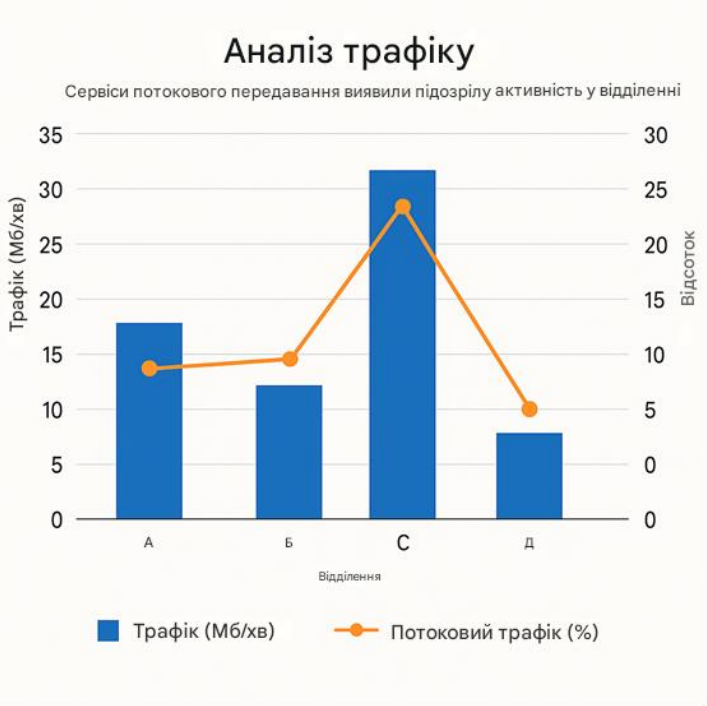

Рисунок 3.4 – Аналіз трафіка і підозріла активність

Покращення безпеки. Інструменти моніторингу дозволяють виявляти підозрілу активність у режимі реального часу, що особливо важливо для філіалів, де можуть бути слабші засоби захисту.

Приклад: у регіональному офісі з’явився підозрілий трафік на зовнішні IP-адреси. За допомогою Wireshark виявили зловмисне ПЗ, яке передавало службові дані за межі компанії. Пристрій було ізольовано, проблему усунено (Рис. 3.5).

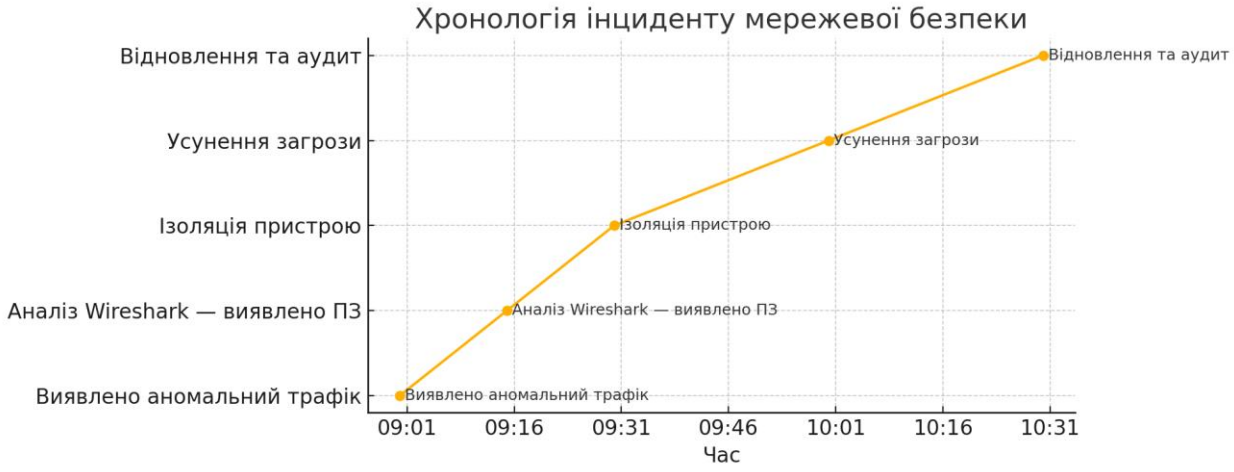

Рисунок 3.5 – Сценарій інциденту з підозрілим трафіком

3. Інтернет-провайдер

Завдання: Виявлення шкідливої активності в мережі. Інструмент: Suricata (IDS/IPS), Zeek Результат: Зафіксовано спроби ботнет-інфекцій через порт 445. Швидке реагування з блокуванням IP та оновленням політик брандмауера (Рис. 3.6).

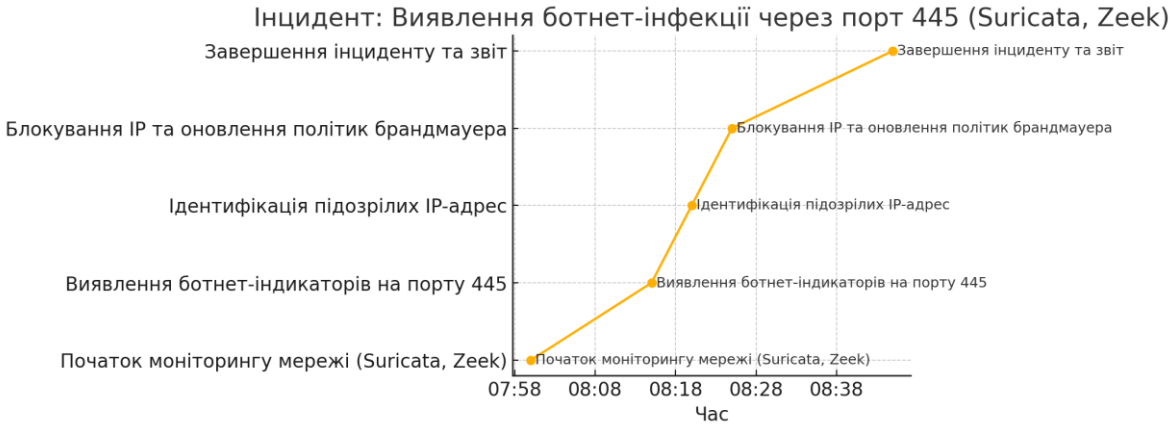

Рисунок 3.6 – Інцидент з ботнет-активністю, виявленою за допомогою Suricata і Zeek

На практиці Інтернет-провайдери (ISP) активно використовують засоби моніторингу мережевого трафіку для забезпечення стабільної, безпечної та якісної роботи своїх послуг.

Застосування	Інструмент(и)	Опис
Моніторинг продуктивності мережі	PRTG Nikwork Monitor	Постійний моніторинг пропускної здатності та завантаженості каналів зв'язку
Виявлення DDoS-атак	Arbor Sightline	Виявлення збоїв на графіках тряфіку та активація стратегії пом'якшення
Тестування продуктивності	iPerf	Вимірювання швидкості з'єднань і тестування мережеви маршрутів
Аналіз безпеки	NetFlow Collector/Analyzer	Виявлення аномалій для оперативного реагування на загрози

Рисунок 3.7 – Інструменти та застосування Інтернет-провайдерами засобів моніторингу мережевого трафіку

Ці інструменти дозволяють провайдерам в режимі реального часу контролювати обсяг і напрямок трафіку, виявляти аномалії, реагувати на збої та покращувати обслуговування клієнтів.

1. Контроль пропускної здатності мережі. Провайдери використовують моніторинг для визначення, наскільки ефективно використовуються канали передачі даних.

Приклад: Якщо на певному вузлі спостерігається надмірне навантаження, система моніторингу (наприклад, Cacti або MRTG) може показати пікові години споживання, що дає змогу своєчасно збільшити пропускну здатність або оптимізувати розподіл трафіку. У Cacti та MRTG збір і візуалізація автоматичні, але висновки й дії приймаються вручну. Це добре підходить для невеликих мереж або для задач, де потрібна гнучкість, але не оперативна реакція.

2. Виявлення та локалізація проблем. Засоби моніторингу дозволяють швидко виявляти збої в мережі або зниження якості обслуговування (затримки, втрати пакетів, проблеми з маршрутизацією).

Приклад: За допомогою Zabbix або Nagios, ISP може оперативно зафіксувати відключення обладнання на одному з вузлів і перенаправити трафік через альтернативний маршрут (Рис.3.8). Зміна мережевого трафіку або затримка (latency) відбувається у момент втрати зв’язку з одним із вузлів і подальшої автоматичної перемаршрутизації даних.

Рис. 3.8. – Реагування ISP на відключення вузла з подальшим перенаправленням трафіку через альтернативний маршрут

3. Аналіз трафіку за протоколами та напрямками. Провайдери використовують інструменти на зразок NetFlow, sFlow або IPFIX, щоб бачити, які сервіси (YouTube, Netflix, Torrents тощо) найбільше навантажують мережу, і за потреби застосовувати політику керування трафіком (Traffic Shaping).

Приклад: У години пік значна частина трафіку йде на відеострімінг. Провайдер може тимчасово обмежити швидкість для менш пріоритетних сервісів, аби забезпечити якість голосового трафіку чи хмарних сервісів.

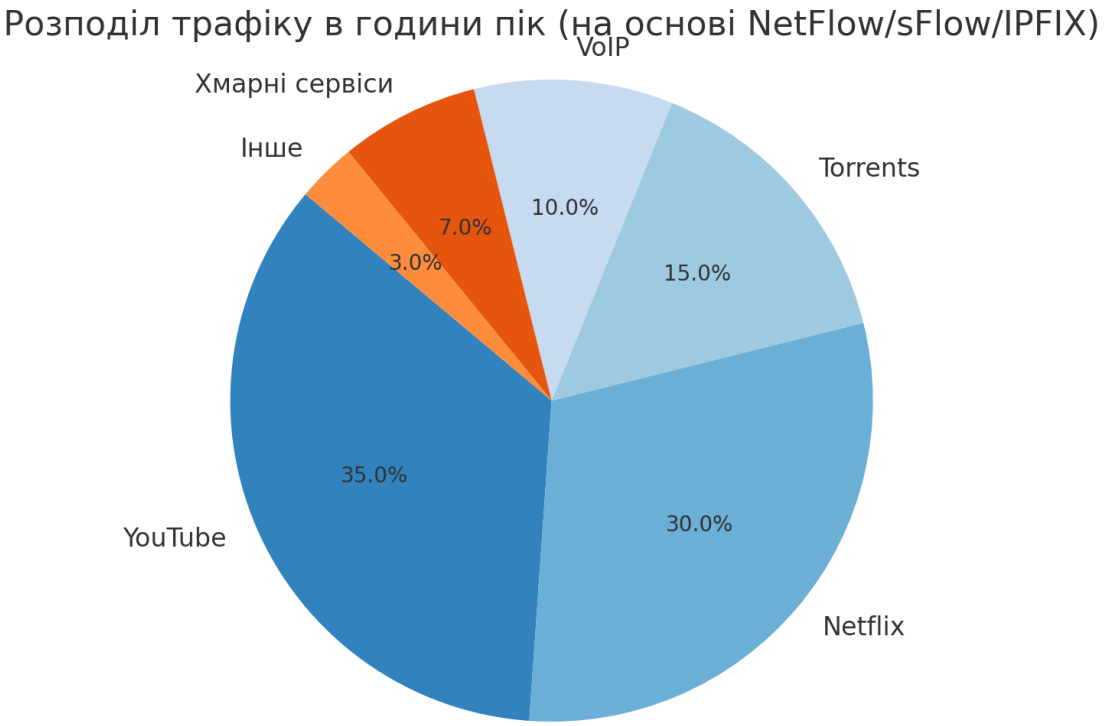

Рисунок 3.9 – Розподіл мережевого трафіку в години пік

4. Виявлення кіберзагроз та DDoS-атак. Моніторинг трафіку є ключовим елементом виявлення спроб злому, ботнет-активності або DDoS-атак.

Приклад: Система ntopng або Darktrace може виявити нетипову активність, наприклад масову кількість запитів з однієї IP-адреси, та ініціювати блокування або ізоляцію сегмента мережі.

Система ntopng або Darktrace, при виявленні аномальної активності (наприклад, масового потоку запитів із підозрілої IP-адреси), може автоматично ініціювати захисну реакцію, щоб обмежити поширення потенційної загрози.

Блокування сегмента мережі відбувається такими етапами:

А) Виявлення аномалії. Інструмент в режимі реального часу аналізує мережевий трафік та зіставляє поведінку з типовими шаблонами. При фіксації великої кількості підозрілих запитів, система класифікує це як потенційну DDoS-атаку, сканування або спробу проникнення.

Б) Ініціювання дії. На основі політик безпеки або вбудованого штучного інтелекту програма може:

- відправити запит до мережевого комутатора або фаєрвола (через API, SNMP або NetFlow) для блокування певного IP;

- оновити правила фаєрвола або список доступу (ACL), щоб відсікти шкідливий трафік;

- активувати механізм ізоляції сегмента, наприклад, перевести заражений вузол у окрему VLAN або обмежити його зовнішні з’єднання.

У результаті такого блокування:

- порушник втрачає доступ до мережевих ресурсів;

- зменшується навантаження на інші вузли;

- локалізується потенційна загроза — наприклад, вірус або шкідливий код не може поширитися далі в мережі;

- адміністратор отримує сповіщення для подальшого аналізу ситуації.

Блокування ініціюється автоматично або напівручним способом через інтеграцію з мережевим обладнанням, а його головна мета – швидко ізолювати загрозу та захистити інші частини інфраструктури від зараження чи перевантаження.

Застосовувати цю систему варто в:

- корпоративних мережах – виявлення підозрілої активності, спроб вторгнень, ботнетів, сканування портів;

- провайдерах інтернету (ISP) – аналіз мережевих потоків, агрегація трафіку, контроль пропускної здатності;

- ЦОДи (центри обробки даних) – аналіз трафіку між віртуальними машинами;

- операційні центри безпеки (SOC) – як частина екосистеми з SIEM та IDS/IPS.

Ntopng встановлюється на спеціалізованому сервері або віртуальній машині, що має доступ до дзеркального порту (SPAN) або трафіку TAP на мережевому комутаторі, може бути встановлена на edge-роутері, на шлюзі або навіть на розподілених вузлах для агрегації даних.

Darktrace встановлюється як апаратний пристрій або віртуальний сенсор у точці, де проходить основний трафік: зазвичай після мережевого комутатора core level, біля фаєрвола або на маршрутизаторі виходу в Інтернет. Для повноцінної роботи може потребувати інтеграції з Active Directory, DNS, проксі-серверами, тощо.

5. Тарифікація та облік. Провайдери використовують дані трафіку для нарахування плати за обсяг спожитих послуг, а також для планування ресурсів у таких сферах:

- Інтернет-провайдери (ISP) – для нарахування плати за трафік чи швидкість.

- Хот-споти та публічні Wi-Fi мережі – для контролю трафіку користувачів і надання доступу на певний час або обсяг.

- Корпоративні мережі – для обліку споживання ресурсів співробітниками.

- Мобільні оператори – для моніторингу трафіку в реальному часі (наприклад, Київстар, Vodafone, lifecell).

Приклад: Інструменти на зразок Radius Manager збирають статистику трафіку для кожного абонента і дозволяють формувати рахунки згідно з тарифним планом.

- Lanet (Україна). Використовує комбіновані тарифні плани (безліміт + пріоритет по швидкості). Застосовується контроль трафіку для обмеження в годину пік.

- Fregat (Дніпро). Використовує Radius-систему з динамічною зміною IP і авторизацією PPPoE. Працює з MikroTik як NAS.

- Triolan. Пропонує обмеження на швидкість залежно від часу доби. Веде облік трафіку для внутрішніх сервісів (телебачення, FTP).

- Kyivstar Home Internet. Для деяких тарифів використовує облік не лише швидкості, але й обсягів – наприклад, для модемів та мобільного інтернету.

Аналіз мережевого трафіку – це не просто контроль навантаження, а інструмент стратегічного управління мережею. Завдяки грамотному впровадженню цих рішень можна оптимізувати ресурси, підвищити рівень кібербезпеки та забезпечити високу доступність сервісів. Для сучасних навчальних закладів, підприємств чи дата-центрів – це вже не опція, а необхідність.

3.2 Сфери застосування засобів мережевого трафіку

Засоби моніторингу мережевого трафіку знаходять практичне застосування у різних галузях завдяки своїй здатності забезпечувати стабільність, безпеку та ефективність роботи комп’ютерних мереж.

Таблиця 3.1 – Популярні засоби аналізу трафіку [27]

Засіб	Призначення	Особливості
Wireshark	Глибокий аналіз пакетів	Вільне ПЗ, потужна фільтрація, GUI
ntopng	Аналіз потоків трафіку, статистика	Веб-інтерфейс, інтеграція з NetFlow
SolarWinds	Корпоративний моніторинг трафіку	Потужна аналітика, інтеграція з SNMP
PRTG	Повний мережевий моніторинг	Легка візуалізація, алерти
Zeek (Bro)	Розширений аналіз трафіку з фокусом на безпеку	Створює журнали подій, підтримка скриптів
NetFlow Analyzer	Потіковий аналіз мережі (Cisco)	Графіки в реальному часі, звітність

У Черкаському державному фаховому бізнес-коледжі можна ефективно використати кілька із зазначених інструментів залежно від цілей:

1. Wireshark. Призначення: Аналіз мережевого трафіку на рівні пакетів.

Поради до використання:

- на заняттях з комп’ютерних мереж, інформаційної безпеки, адміністрування;

- у лабораторії для демонстрації реального мережевого трафіку студентам.

Цей інструмент має такі переваги: безкоштовний, зручний для навчання, наочно показує структуру пакетів (TCP/IP, DNS, HTTP, тощо).

2. ntopng. Призначення: Моніторинг трафіку в реальному часі, аналіз активності користувачів, статистика.

Поради до використання:

- у серверній для спостереження за використанням мережі у корпусі;

- у навчальних цілях для демонстрації сучасного мережевого моніторингу.

Цей інструмент має такі переваги: має веб-інтерфейс, деталізує активність по IP, портах, протоколах. Можна бачити «хто що качає».

3. Zeek (раніше Bro). Призначення: Система мережевого моніторингу та виявлення загроз.

Поради до використання:

- на курсах з кібербезпеки для аналізу атак, вторгнень, аномалій;

- у дослідницьких проектах або практиці студентів IT-спеціальностей.

Цей інструмент має таку перевагу: має скриптову мову для створення власних політик безпеки.

4. PRTG Network Monitor. Призначення: Загальний моніторинг мережевої інфраструктури (стан пристроїв, трафік, ресурси).

Варто використовувати у серверній для моніторингу серверів, маршрутизаторів, комутаторів, принтерів.

Цей інструмент має такі переваги: має зручний інтерфейс, можна слідкувати за статусом обладнання та споживанням ресурсів.

5. SolarWinds (наприклад, NetFlow Traffic Analyzer) Це потужний комерційний пакет для моніторингу мережі та аналізу NetFlow. Можна використовувати переважно у централізованому IT-управлінні. В коледжі можливо лише у демонстраційних цілях через складність і ціну: дуже потужний, але дорогий – для навчального закладу, можливо, надмірний.

6. NetFlow Analyzer (ManageEngine). Для аналізу трафіку з підтримкою NetFlow/sFlow.

Варто використовувати в IT-відділі (контроль за потоками трафіку у всій мережі закладу), навчальній демонстрації з інженерії та безпеки. Має переваги, зокрема: візуалізація потоків трафіку, можливість виявлення підозрілої активності.

Нижче наведено сфери застосування та конкретні приклади, які демонструють, як саме використовуються ці інструменти на практиці.

1. Освітні установи: наприклад, університет або коледж застосовує моніторинг трафіку для:

- контролю доступу до навчальних платформ (Moodle, Google Classroom);
- обмеження доступу до соцмереж або розважальних сайтів під час занять;
- виявлення підозрілої активності, наприклад масових завантажень, які можуть свідчити про витік даних або використання P2P-мереж.

Засоби: Wireshark, PRTG, NetFlow Analyzer

Якщо Черкаський державний фаховий бізнес-коледж застосовує моніторинг трафіку для контролю доступу до навчальних платформ (як-от Moodle, Google Classroom), то найкращим варіантом для збору такої інформації буде ntopng або Wireshark, залежно від цілей.

Рекомендована програма: ntopng. Ця програма дає аналіз трафіку в реальному часі: показує, хто з користувачів (IP/MAC-адреси) звертається до Google Classroom, Moodle та інших сайтів. Визначення доменів: легко відслідковує звернення до такого домену як moodle.edu.ua. Статистика за протоколами HTTP/HTTPS, DNS, SSL – видно, які сервіси використовуються. Графіки активності дають змогу побачити пікові години доступу до навчальних платформ. Класифікація трафіку дозволяє розпізнавати типи застосунків (освітні, соціальні, медіа тощо). Ця платформа встановлюється на сервер або окремий комп'ютер, підключений до дзеркального порту комутатора або через маршрутизатор, автоматично класифікує трафік та відображає активність у веб-інтерфейсі.

Альтернативою є Wireshark. Можна вручну фільтрувати трафік за адресами (ip.addr == classroom.google.com). Ця платформа дає повний пакетний

аналіз, але вимагає глибших знань. Підходить для одноразового детального аналізу, а не для постійного моніторингу.

Можна стверджувати, що коледж з ntopng отримає таку інформацію:

- скільки студентів використовують Moodle у певний час;

- чи відвідуються Moodle-сервери, і скільки трафіку вони генерують;

- які групи або пристрої генерують найбільше запитів до освітніх ресурсів;

- можливість виявити сторонню активність (наприклад, YouTube під час уроку).

2. Організації з віддаленими офісами

Міжнародна компанія з офісами у кількох країнах застосовує моніторинг для (Рис. 3.10):

- оцінки якості з’єднання між головним офісом і філіями;

- оптимізації використання VPN;

- забезпечення кібербезпеки при передаванні конфіденційних документів.

Рисунок 3.10 – Організація моніторингу засобами Zabbix, SolarWinds, ntopng

3. Фінансові установи (банки, страхові компанії): наприклад, Банк контролює трафік для:

- виявлення спроб фішингу або шахрайських транзакцій;

- аналізу навантаження на банківські сервіси в режимі 24/7;

- захисту від атак типу DDoS на онлайн-банкінг.

Засоби: FortiAnalyzer, Darktrace, NetScout

4. Інтернет-провайдери (ISP): наприклад, провайдер контролює трафік для:

- балансування навантаження в мережі;

- визначення типу трафіку (стрімінг, VoIP, FTP тощо);

- тарифікації абонентів за обсягом спожитого трафіку.

Засоби: NetFlow, sFlow, Cacti

5. Державні установи та критична інфраструктура: наприклад, Міська адміністрація або енергетична компанія використовує моніторинг для (Рис. 3.11):

- захисту SCADA-систем (керування електромережами, водопостачанням);

- аудиту доступу до внутрішніх ресурсів;

- виявлення загроз на ранніх стадіях кібератак.

Рисунок 3.11 – Використання моніторингу даних державними установами чи критичною інфраструктурою засобами ELK Stack (Elasticsearch, Logstash, Kibana), Nagios

6. Компанії в сфері електронної комерції та IT

Приклад: Онлайн-магазин застосовує аналіз трафіку для:

- відстеження трафіку клієнтів до сайтів (для оптимізації UX);

- запобігання крадіжці даних користувачів;

- виявлення ботів і спроб автоматизованого парсингу цін (Рис. 3.12).

Засоби: Cloudflare Analytics, Grafana, Suricata

Рисунок 3.12 – Застосування аналізу трафіку онлайн-магазином

Варто зазначити, що аналіз трафіку повинен застосовуватися у всіх середовищах, де важливі безпека, ефективність використання ресурсів та якість обслуговування. Основні місця застосування:

- Освітні заклади – для контролю доступу до освітніх платформ (Moodle, Google Classroom), обмеження небажаних сайтів і оптимізації пропускної здатності.

- Бізнес-компанії – для виявлення аномалій, контролю роботи VPN, обліку активності співробітників, захисту від витоку даних.

- Онлайн-магазини – для аналітики поведінки клієнтів, виявлення ботів, запобігання крадіжкам даних.

- Провайдери інтернету – для тарифікації, балансування навантаження, виявлення DDoS-атак.

- Міські адміністрації та критична інфраструктура – для захисту SCADA-систем, раннього виявлення кібератак.

- Міжнародні компанії – для контролю якості зв'язку між офісами, оптимізації трафіку між країнами та захисту передаваних даних.

Рекомендації щодо використання засобів застосовує аналіз трафіку:

- потрібно впроваджувати автоматичні алерти для швидкого реагування на інциденти.

- доцільно використовувати агрегацію логів для аналітики в одному вікні (наприклад, через Splunk).

- варто комбінувати пасивний та активний моніторинг для повної картини мережевої активності.

- доцільно інтегрувати AI/ML-рішення для виявлення аномалій у поведінці користувачів.

ВИСНОВКИ

Мережевий трафік відіграє ключову роль у функціонуванні сучасних цифрових систем, а його правильне розмежування дозволяє ефективно розподіляти ресурси, підвищувати рівень безпеки та покращувати загальну продуктивність мережевої інфраструктури. Для ефективного керування мережею важливо враховувати джерела, характер трафіку та його вплив на систему. Застосування спеціалізованих засобів аналізу, таких як Wireshark, NetFlow чи SNMP, сприяє виявленню загроз, аналізу продуктивності та стабільному функціонуванню мережі.

У процесі аналізу використовуються активні та пасивні методи моніторингу, які виконують взаємодоповнюючі функції. Пасивний підхід надає змогу відслідковувати стан мережі в реальному часі без втручання в її роботу, тоді як активний – дозволяє проводити тестування та діагностування проблем, визначаючи, наприклад, затримки чи втрати пакетів. Раціональна комбінація обох методів є найефективнішою: перший забезпечує довгостроковий аналіз і виявлення аномалій, а другий – підтвердження гіпотез та оцінку продуктивності.

Аналіз трафіку стає невід’ємною складовою кібербезпеки та адміністрування мереж. Сучасні інструменти дозволяють глибоко досліджувати пакети даних, відслідковувати активність користувачів, оперативно виявляти підозрілу активність і запобігати потенційним загрозам. Вибір програмного забезпечення напряму залежить від масштабів мережі, фінансових можливостей та технічних потреб.

Засоби на кшталт Nmap, SolarWinds, Wireshark чи PRTG користуються широкою популярністю завдяки своїй ефективності у моніторингу мережевої продуктивності. Правильний вибір інструменту дозволяє не лише відслідковувати навантаження, а й стратегічно керувати мережею — знижуючи ризики, покращуючи якість сервісів і забезпечуючи їхню постійну доступність.

У контексті освітніх закладів, комерційних підприємств або дата-центрів, впровадження таких рішень уже не є додатковою перевагою, а стало необхідною умовою для стабільної та захищеної роботи інфраструктури.

Рекомендації щодо впровадження засобів мережевого трафіку в закладах освіти:

– використовувати системи з автоматичними повідомленнями (alert'ами), щоб адміністратор міг швидко реагувати на критичні ситуації.

– інтеграція з системою кібербезпеки – поєднувати моніторинг трафіку з антивірусними шлюзами та системами виявлення вторгнень (IDS/IPS).

– захист персональних даних – моніторинг має здійснюватися відповідно до політики конфіденційності, без втручання у приватну переписку студентів чи працівників.

Рекомендації застосування засобів мережевого трафіку для підприємств з філіями:

– використовувати SD-WAN-рішення, які інтегрують моніторинг трафіку з маршрутизацією і автоматично обирають найкращий маршрут передачі даних.

– інтегрувати моніторингові рішення з системами кібербезпеки, такими як IDS/IPS.

– автоматизувати звітність – встановити регулярну генерацію звітів про трафік, навантаження та інциденти для аналітики та управлінських рішень.

– навчати співробітників – інформувати персонал філіалів про політику використання мережі, щоб уникати перевантаження або витоку даних.

Рекомендації застосування засобів мережевого трафіку для провайдерів щодо моніторингу трафіку:

– інвестувати в масштабовані платформи, які підтримують аналіз великого обсягу даних у реальному часі.

– впроваджувати автоматичні тригери для реагування на перевантаження або атаки.

– регулярно оновлювати політики безпеки та адаптувати їх до змін у мережевому трафіку.

– використовувати багаторівневий моніторинг: трафік, обладнання, сервіси, користувацький досвід.

– впроваджувати AI/ML-алгоритми для передбачення аномалій і проактивного реагування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Data Traffic Monitoring and Analysis / ed. M. Mellia, R. Sadre, A. Finamore. – Springer, 2013. – 328 p. – ISBN 978-3-642-36783-0. – DOI: 10.1007/978-3-642-36784-7. URL: https://link.springer.com/book/10.1007/978-3-642-36784-7.

2. A Methodical Review on Network Traffic Monitoring and Analysis Tools / M. A. Khan, M. A. Khan. In: International Journal of Computer Applications, 2019. Vol. 178, No. 7. P. 1–7. URL: https://www.researchgate.net/publication/337481341_A_Methodical_Review_on_Network_traffic_monitoring_and_Analysis_tools.

3. Network Traffic Analysis – An Overview / S. G. Rao. In: ScienceDirect Topics. URL: https://www.sciencedirect.com/topics/computer-science/network-traffic-analysis.

4. Network Traffic Classification: Techniques, Datasets, and Challenges / A. A. Diro, N. Chilamkurti. In: Journal of Network and Computer Applications, 2022. URL: https://www.sciencedirect.com/science/article/pii/ S2352864822001845.

5. Deep Learning for Network Traffic Monitoring and Analysis (NTMA) / Y. Zhang, L. Wang, Y. Wang. In: Computer Networks, 2021. Vol. 183. URL: https://www.sciencedirect.com/science/article/pii/S0140366421000426.

6. A Survey of Network Traffic Monitoring and Analysis Tools / C. So-In. In: IEEE Communications Surveys & Tutorials, 2010. Vol. 12, No. 1. P. 56–69. URL: https://www.researchgate.net/publication/241752391_A_Survey_of_ Network_Traffic_Monitoring_and_Analysis_Tools.

7. Wireshark: An Effective Tool for Network Analysis / S. S. Sahu, S. K. Jena. In: International Journal of Computer Applications, 2023. URL: https://www.researchgate.net/publication/374675769_Wireshark_An_Effective_Tool_for_Network_Analysis.

8. Application of SNORT and Wireshark in Network Traffic Analysis / M. A. Khan, M. A. Khan. In: International Journal of Computer Applications, 2021. URL: https://www.researchgate.net/publication/350572993_Application_of_ SNORT_and_Wireshark_in_Network_Traffic_Analysis.

9. Real-Time Network Traffic Analysis Using Artificial Intelligence, Machine Learning, and Deep Learning: A Review of Methods, Tools, and Applications / M. A. Khan, M. A. Khan. In: International Journal of Computer Applications, 2023. URL: https://www.researchgate.net/publication/376287072_Real_Time_Network_Traffic_Analysis_Using_Artificial_Intelligence_Machine_Learning_and_Deep_Learning_A_Review_of_Methods_Tools_and_Applications.

10. A Review of Network Traffic Analysis and Prediction Techniques / T. Aldhyani, A. Alzahrani. – In: Journal of Network and Computer Applications, 2020. URL: https://www.researchgate.net/publication/339927785_A_review_of_network_traffic_analysis_and_prediction_techniques.

11. Network Traffic Analysis and SCADA Security / M. Cheminod, L. Durante, A. Valenzano. In: Springer, 2010. URL: https://link.springer.com/chapter/10.1007/978-3-642-04117-4_20.

12. Network Traffic Analysis / R. Bace. In: Springer, 2004. URL: https://link.springer.com/chapter/10.1007/978-1-4302-0007-9_9.

13. Machine Learning for Traffic Analysis: A Review // Procedia Computer Science. 2020. Vol. 170. P. 911–916. DOI: 10.1016/j.procs.2020.03.111.

14. Deep Learning for Network Traffic Monitoring and Analysis (NTMA): A Survey // Computer Communications. 2021. Vol. 170. P. 19–41. DOI: 10.1016/j.comcom.2021.01.021.

15. Application of SNORT and Wireshark in Network Traffic Analysis // IOP Conference Series: Materials Science and Engineering. 2021. Vol. 1119. P. 012007. DOI: 10.1088/1757-899X/1119/1/012007.

16. Zeek (Bro) Network Security Monitor // Wikipedia. https://en.wikipedia.org/wiki/Zeek.

17. A Survey on Network Traffic Analysis and Prediction Techniques // IEEE Communications Surveys & Tutorials. 2019. Vol. 21, No. 3. P. 2053–2081. DOI: 10.1109/COMST.2019.2916180.

18. Network Traffic Analysis Using Machine Learning Techniques: A Review // Computer Networks. 2020. Vol. 172. P. 107161. DOI: 10.1016/j.comnet.2020.107161.

19. An Overview of Network Traffic Monitoring and Analysis Techniques // Journal of Network and Computer Applications. 2018. Vol. 100. P. 70–85. DOI: 10.1016/j.jnca.2017.12.001.

20. Traffic Analysis and Intrusion Detection in Wireless Networks // IEEE Wireless Communications. 2017. Vol. 24, No. 4. P. 22–29. DOI: 10.1109/MWC.2017.1600400.

21. Real-Time Network Traffic Monitoring Using Deep Learning // Future Generation Computer Systems. 2021. Vol. 115. P. 34–45. DOI: 10.1016/j.future.2020.08.012.

22. Network Traffic Analysis for Anomaly Detection Using Machine Learning // Computers & Security. 2019. Vol. 87. P. 101568. DOI: 10.1016/j.cose.2019.101568.

23. A Comprehensive Survey on Network Traffic Monitoring and Analysis Tools // Computer Science Review. 2020. Vol. 38. P. 100307. DOI: 10.1016/j.cosrev.2020.100307.

24. Flow-Based Network Traffic Analysis and Monitoring // Computer Communications. 2018. Vol. 120. P. 1–16. DOI: 10.1016/j.comcom.2018.02.009.

25. Anomaly Detection in Network Traffic Using Unsupervised Learning // Expert Systems with Applications. 2020. Vol. 160. P. 113696. DOI: 10.1016/j.eswa.2020.113696.

26. Network Traffic Analysis Using Deep Packet Inspection // Journal of Network and Computer Applications. 2019. Vol. 137. P. 35–50. DOI: 10.1016/j.jnca.2019.04.005.

27. A Review of Network Traffic Analysis Techniques for Cybersecurity // Computers & Security. 2021. Vol. 102. P. 102123. DOI: 10.1016/j.cose.2020.102123.