КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ
КАФЕДРА КІБЕРБЕЗПЕКИ ТА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

ПРЕЗЕНТАЦІЯ

ДО АТЕСТАЦІЙНОЇ ВИПУСКНОЇ РОБОТИ

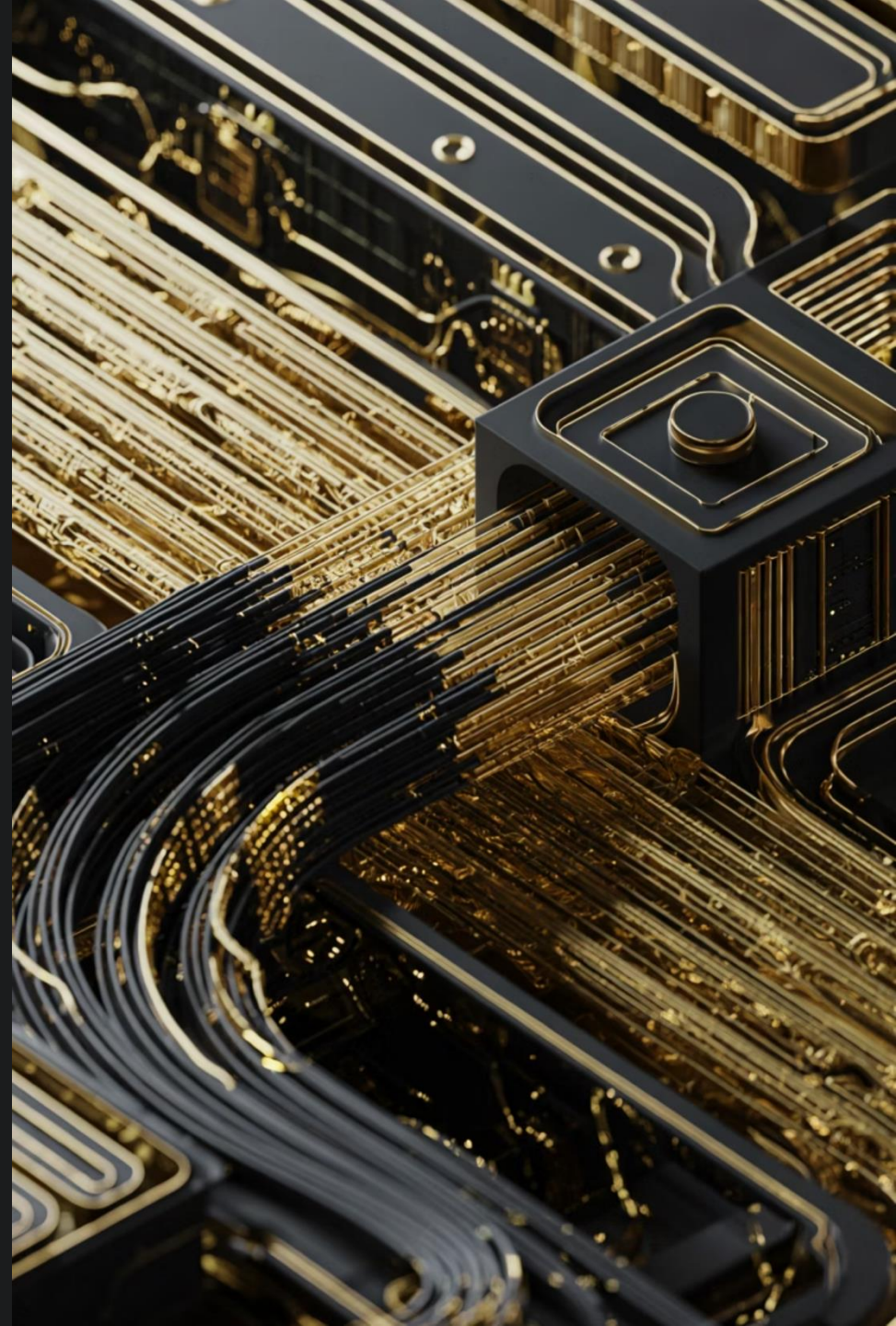
НА ЗДОБУТТЯ СТУПЕНЯ ВИЩОЇ ОСВІТИ МАГІСТР

на тему:

Комплексна діагностика мережі за допомогою засобів аналізу трафіку

Роботу виконав студент
Сарапин Вадим Євгенійович
Керівник
к.т.н., доцент, Шабала Є.Є.

2025 рік



Актуальність проблеми: Зростання складності та ризиків. Традиційні методи діагностики часто нездатні оперативно реагувати на складні, багатофакторні загрози та аномалії в умовах розподілених систем.

Мета дослідження та основні завдання:

- **Розробка підходу.** Комплексна діагностика на основі аналізу мережевого трафіку.
- **Виявлення аномалій.** Своєчасна ідентифікація затримок, відмов та потенційних загроз.
- **Підвищення надійності.** Забезпечення стабільності та безпеки інфраструктури.

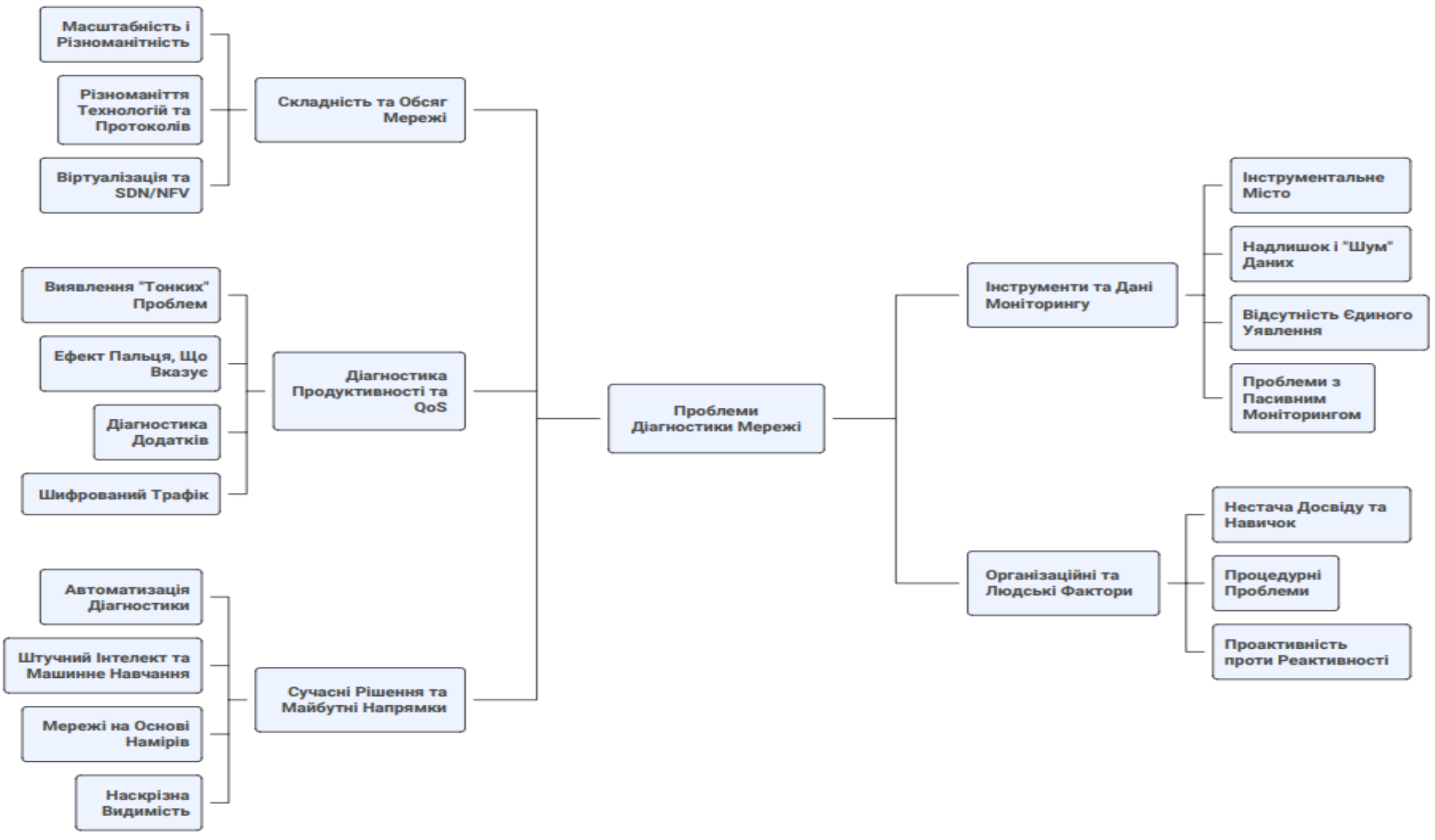
Наукова новизна полягає в інтеграції кількох передових концепцій у єдину діагностичну технологію.

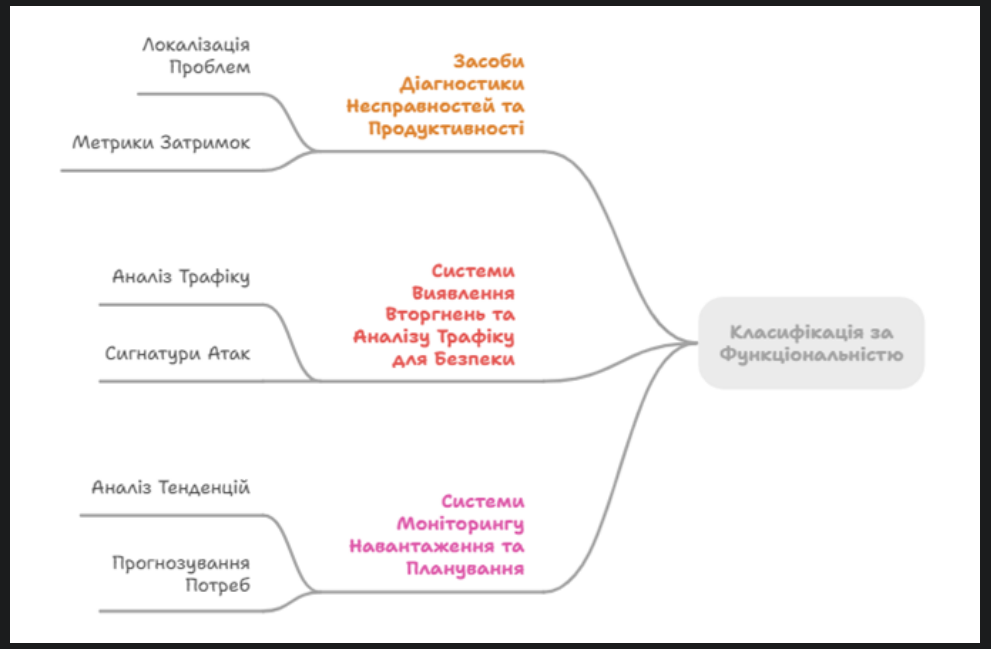
Предмет дослідження - методи та засоби діагностики мережевих аномалій на основі аналізу трафіку.

Об'єкт дослідження - комп’ютерна мережа з багаторівневою системою безпеки.

Розроблено схему, що ілюструє ключові аспекти важливості комп'ютерних мереж, класифіковані за їхніми функціями та сферами застосування, такими як зв'язок, спільне використання ресурсів, освіта, комунікації, обмін даними, бізнес та розваги.

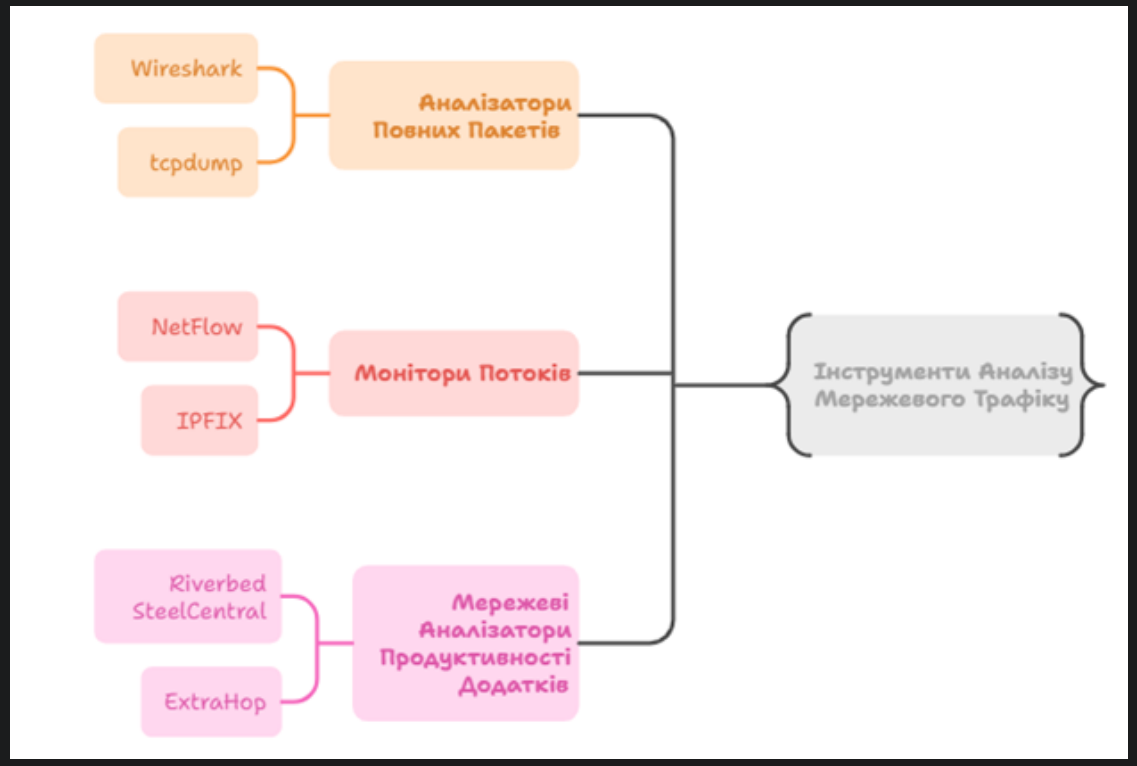
Цей слайд підкреслює, наскільки комп'ютерні мережі є критично важливими для сучасного суспільства. Він візуалізує їхній вплив на різноманітні сфери нашого повсякденного життя та професійної діяльності.


Проблеми Діагностики Мережі
Інструменти та Дані Моніторингу
Інструментальне Місто
Надлишок і "Шум" Даних
Відсутність Єдиного Уявлення
Проблеми з Пасивним Моніторингом
Організаційні та Людські Фактори
Нестача Досвіду та Навичок
Процедурні Проблеми
Проактивність проти Реактивності
Складність та Обсяг Мережі
Масштабність і Різноманітність
Різноманіття Технологій та Протоколів
Віртуалізація та SDN/NFV
Діагностика Продуктивності та QoS
Виявлення "Тонких" Проблем
Ефект Пальця, Що Вказує
Діагностика Додатків
Шифрований Трафік
Сучасні Рішення та Майбутні Напрямки
Автоматизація Діагностики
Штучний Інтелект та Машинне Навчання
Мережі на Основі Намірів
Наскрізна Видимість

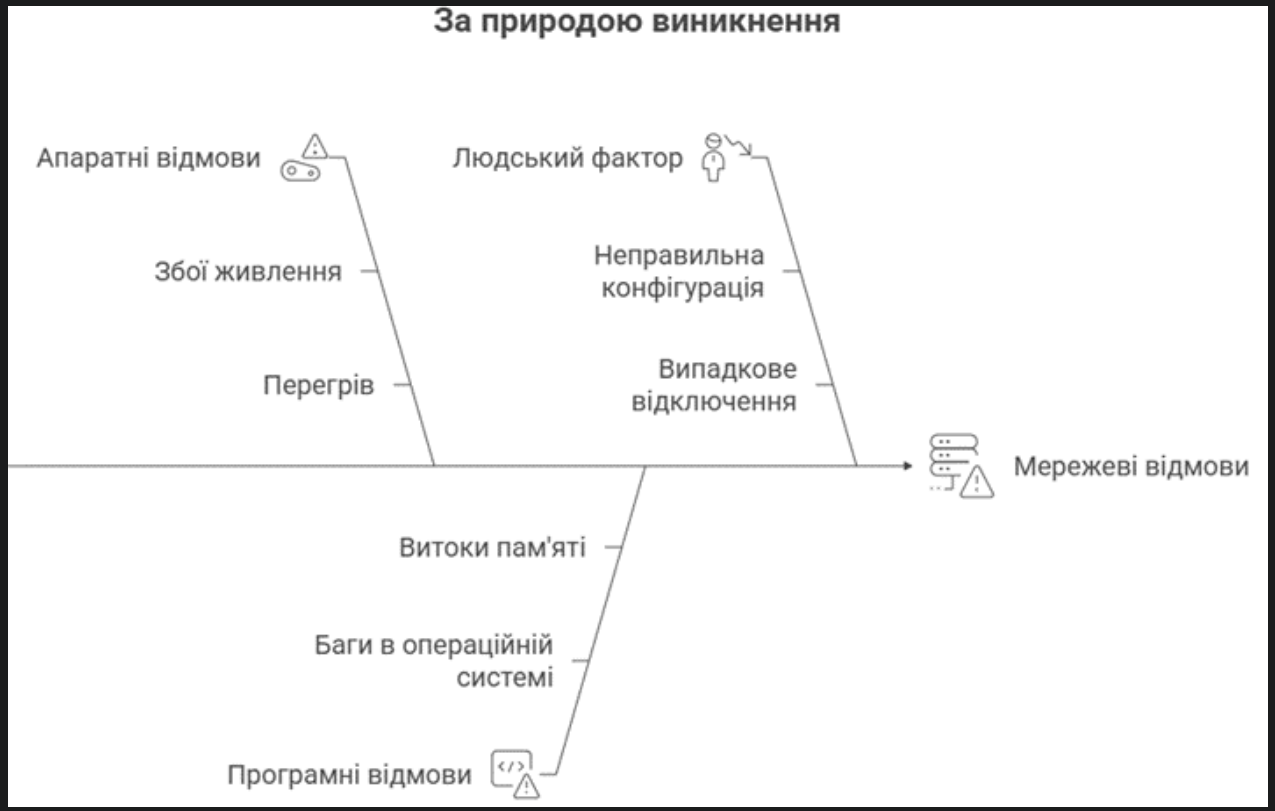


Розроблено три окремі схеми: перша класифікує інструменти аналізу за типом розгортання; друга представляє класифікацію за функціональністю; і третя деталізує інструменти аналізу мережевого трафіку за їхнім принципом роботи з конкретними прикладами.

Цей слайд охоплює методи та засоби, що використовуються для аналізу комп'ютерних мереж. Він демонструє різноманіття рішень, доступних для забезпечення ефективності, безпеки та стабільності мережевої інфраструктури.



Розроблено дві окремі схеми:
перша демонструє причини мережевих відмов за природою їхнього виникнення (апаратні, програмні, людський фактор), а друга класифікує відмови мережі за ступенем їхнього впливу на доступність (повні, часткові, а також специфічні відмови типу "Візантійський генерал").



Цей слайд аналізує різні типи та джерела мережевих відмов. Він допомагає краще зрозуміти складність і різноманітність проблем, що можуть виникнути в комп'ютерних мережах.

Розроблено таблицю, що класифікує та описує чотири основні типи відмов у розподілених системах: відмова за збоєм, відмова за пропуском, відмова за часом та візантійська відмова. Для кожного типу надано його характерні особливості та відповідну модель поведінки.

В роботі було розглянуто візантійські збої, які моделюють ситуації ненадійної або зловмисної поведінки вузлів у розподілених системах.

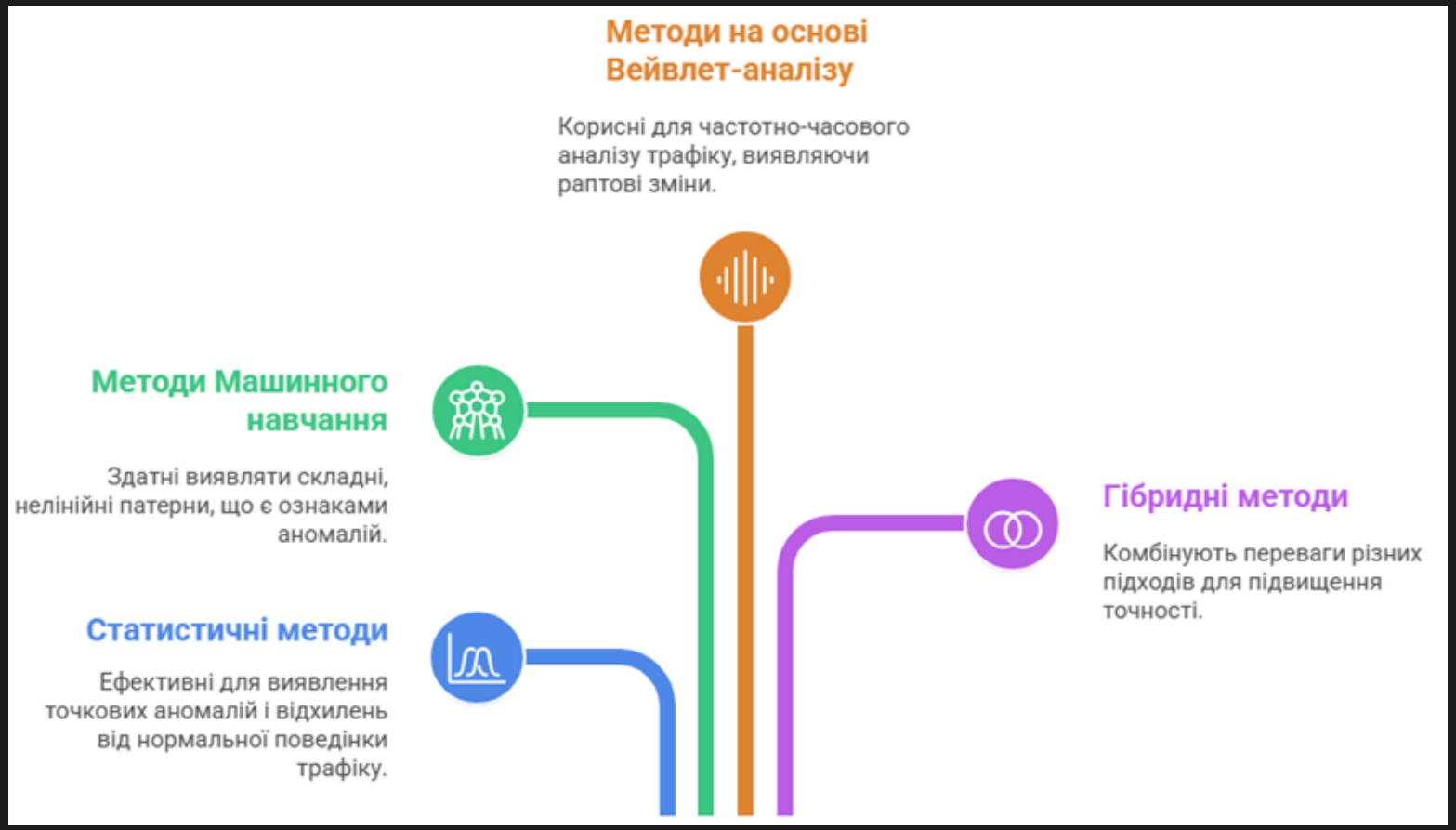
Тип відмови	Характеристика	Модель поведінки
Crash fault	Вузол перестає відповідати (вимкнувся або завис)	Втрата повідомлень
Omission fault	Деякі повідомлення губляться або не доходять	Часткова втрата даних
Timing fault	Повідомлення запізнюються або приходять із затримкою	Асинхронність
Byzantine fault	Вузол діє довільно: підробляє, бреше, надсилає різним вузлам різні дані	Повна недовіра

Розроблено ієрархічну схему "Моделі мережевого трафіку", яка класифікує підходи до моделювання на дві основні категорії: "Класифікація та базові моделі" (включаючи випадкові процеси, Пуассонівський процес, Марківські моделі, а також моделювання взаємодії та обслуговування через теорію черг) та "Моделі прогнозування та оцінки продуктивності" (охоплюючи моделі самоподібного трафіку, авторегресійні моделі, імітаційне моделювання та діагностичні метрики).

Розроблено таблицю, яка порівнює Пуассонівський та Марківський процеси за типом, основними властивостями та використанням. В рамках дипломної роботи було детально розглянуто Пуассонівський процес, включаючи його опис як послідовності незалежних випадкових подій з експоненційним розподілом міжприхідного часу, а також формули для обчислення кількості подій, середнього значення та дисперсії, з акцентом на його застосування для моделювання простих потоків запитів або пакетів у мережах. Також було розглянуто Марківський процес як станову модель, де майбутній стан залежить виключно від поточного, з поясненням його властивості відсутності післядії та застосування у моделюванні черг, навантаження та зміни режимів роботи каналів.

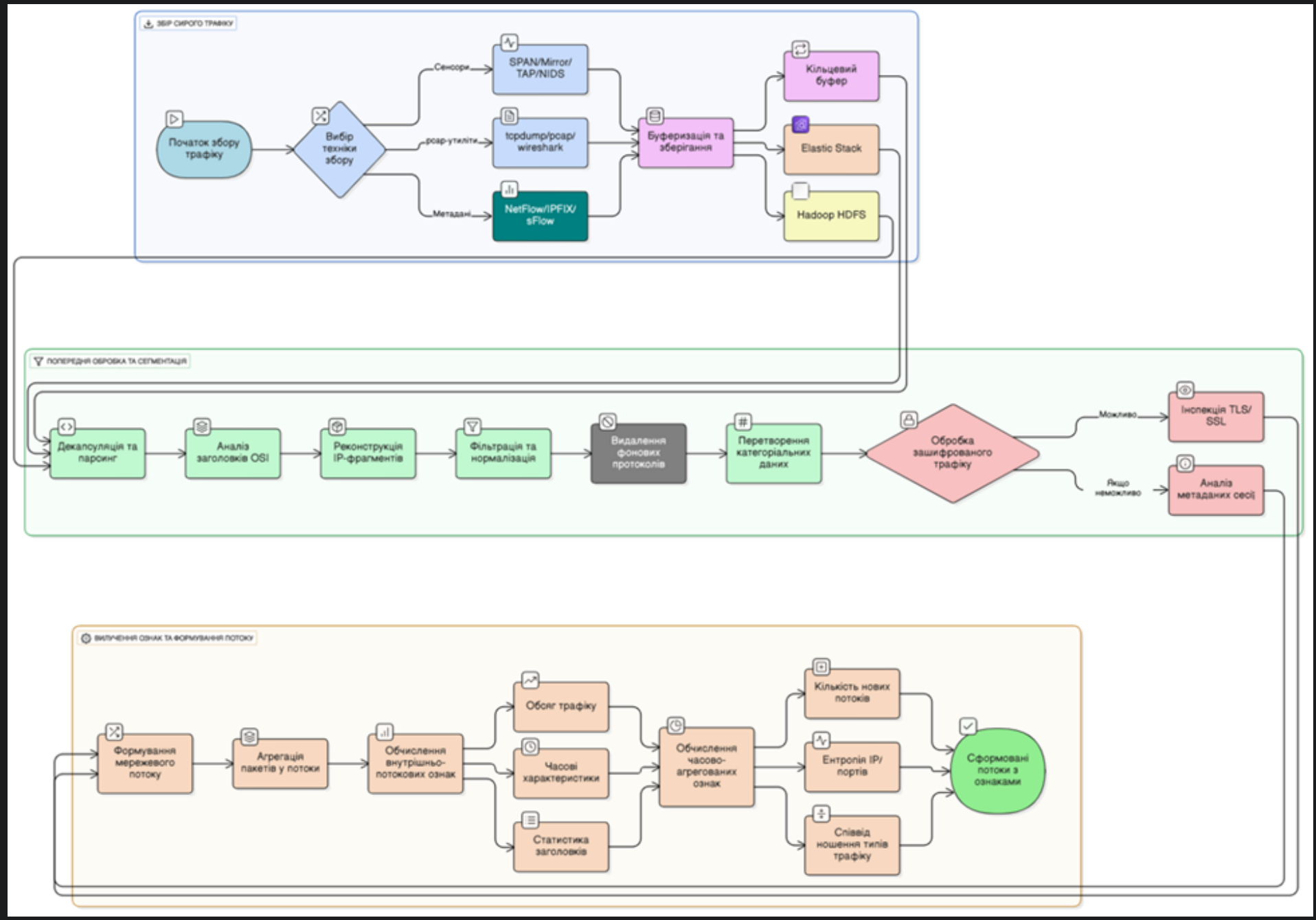
Модель	Тип процесу	Основна властивість	Використання
Пуассонівський	Потік подій	Незалежні прибуття (експоненційний розподіл)	Моделювання простих потоків запитів або пакетів
Марксівський	Станова модель	Наступний стан залежить тільки від поточного	Моделювання черг, навантаження, зміни режимів роботи кана

Розроблено схему, що класифікує та описує чотири основні групи методів для аналізу трафіку та виявлення аномалій: методи машинного навчання, статистичні методи, методи на основі вейвлет-аналізу та гібридні методи.



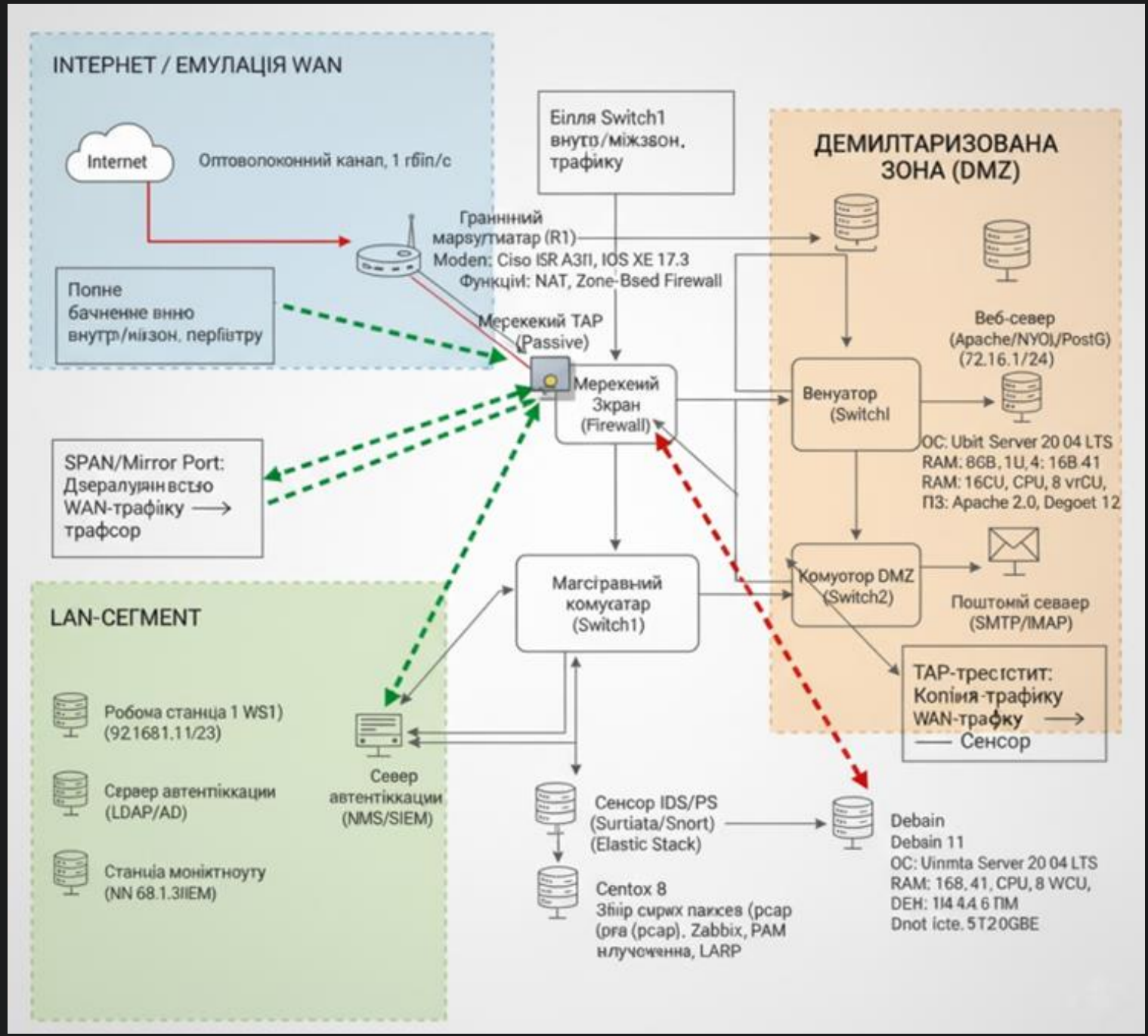
У дипломній роботі було досліджено статистичні методи, а саме Z-оцінку, яка дозволяє ідентифікувати аномалії, вимірюючи відхилення спостережень від середнього значення в стандартних відхиленнях, з визначеними порогами для нормальної, підозрілої та аномальної поведінки трафіку. Також було досліджено вейвлет-аналіз, який дозволяє розкладати мережевий трафік на різні частотні та часові складові для виявлення раптових змін та аномалій на різних масштабах, використовуючи дискретне вейвлет-перетворення для відокремлення фонових змін від високочастотних аномалій.

Цей слайд відображає життєвий цикл аналізу мережевого трафіку, від його початкового збору до вилучення значущих характеристик.



Розроблено схему топології тестового полігону, яка візуалізує розміщення сенсорів для захоплення мережевого трафіку. Схема включає основні сегменти: Internet/Емуляція WAN з граничним маршрутизатором, LAN-сегмент з робочими станціями та серверами автентифікації, а також демілітаризовану зону з веб-серверами та поштовими серверами.

На схемі позначено точки встановлення різних типів сенсорів, таких як мережевий TAP, SPAN/Mirror Port, сенсор IDS/PS та Centos 8 для збору сирих пакетів, що дозволяє проводити всебічний моніторинг та аналіз трафіку всередині та між сегментами мережі.



Клас атаки	Фаза атаки	Мета моделювання
Сканування портів (SYN Scan)	Фаза 1: Розвідка	Перевірка чутливості NADS до зміни розподілу портів та порушення TCP-рукостискання (Half-open connections).
DDoS-атака (UDP Flood)	Фаза 2: Використання	Перевірка реакції NADS на різкий сплеск об’єму трафіку та високу ентропію джерел (імітація ботнету).

На цьому слайді представлено дві таблиці, що деталізують мережеві атаки та їхнє моделювання.

Перша таблиця "Клас атаки" описує два типи атак - сканування портів (SYN Scan) та DDoS-атаку (UDP Flood), розкриваючи фази цих атак та мету їхнього моделювання для перевірки систем виявлення аномалій (NADS). Друга таблиця надає докладні параметри, інструменти та деталі для відтворення атаки SYN Scan (Half-open), включаючи IP-адреси, інтенсивність, тривалість та ознаки аномальної поведінки.

Параметр	Техніка / Інструмент	Деталізація для відтворюваності
Інструмент	Nmap або hping3 (у режимі SYN).	Команда Nmap: nmap -sS -p 1-65535 -T2 <IP_Жертви>
Жертва	Веб-сервер / фаєрвол.	IP-адреса жертви: 192.168.1.10.
Джерело	Єдиний зовнішній вузол.	IP-адреса джерела: 10.0.0.5.
Тип сканування	SYN Scan (Half-open).	Використовується прапор SYN, але без завершення TCP-сесії.
Інтенсивність	Низька	5 пакетів/секунду (опція -r у Nmap або -rate 5).
Тривалість		300 секунд (5 хвилин).
Ознаки аномалії	Збільшення SYN-пакетів без відповідного ACK; високе співвідношення SYN/RST для сканованих портів.	

Моделювання мережевих атак

Параметр	Техніка / Інструмент	Деталізація для відтворюваності
Інстру-мент	hping3 або спеціалізований гене-ратор трафіку (наприклад, TFN2K імітація).	Команда hping3: hping3 --flood --rand-source -2 -p 53 <IP_Жертви>
Жертва	DNS-сервер / інший сервер UDP.	IP-адреса жертви: 192.168.1.10. Порт: 53 (DNS) або 161 (SNMP)
Джерело	Розподілені, рандомізовані IP-адреси	Використовується спуфінг IP-ад-рес джерела (опція --rand-source). Кількість імітованих джерел: >1000.
Тип атаки	UDP Flood (об'ємна).	Надсилання великої кількості па-кетів UDP.
Інтенсив-ність	Висока	10,000 пакетів/секунду або зага-льний бітрейт 1 Гбіт/с.
Тривалість		120 секунд (2 хвилини).
Ознаки аномалії	Різкий стрибок загального об-сягу UDP-трафіку; висока ентро-пія IP-адрес джерела (через спу-фінг); зміна співвідношення вхі-дного/вихідного трафіку (асиме-трія).	

Сплановано експеримент для тестування NADS, що включає фази нормального трафіку для калібрування, фазу SYN Scan для виявлення розвідки, фазу "затишшя" для оцінки повернення до нормального стану та фазу UDP Flood для виявлення аномалії перевантаження та її розподіленої природи. Цей план забезпечує відтворюваність та оцінку здатності NADS ідентифікувати різні типи мережевих аномалій.

Час (від початку)	Тривалість	Фаза трафіку	Дії / результат
T_0	1800 с (30 хв)	Нормальний трафік	Генерація фонового трафіку для навчання/калібрування NADS.
T_1 =30 хв	1800 с (30 хв)	Фаза 1: SYN Scan	NADS повинна виявити аномалію розвідки (порушення TCP-рукостискання).
T_2 =35 хв	300 с (5 хв)	Нормальний трафік	Фаза "затишшя" для оцінки здатності NADS до повернення до нормального стану.
T_3=40 хв	120 с (2 хв)	Фаза 2: UDP Flood	NADS повинна виявити аномалію перевантаження (різкий сплеск трафіку) та її розподілену природу.

Метрика	Фомула	Призначення
True positive rate (TPR) (чутливість, Recall)	$TPR = \frac{TP}{TP + FN}$	Визначає чутливість. Показує частку правильно виявлених атак від усіх фактичних атак. Прагнення до 100%.
False positive rate (FPR)	$FPR = \frac{FP}{FP + TN}$	Визначає надійність. Показує частку хибних спрацювань серед усього нормального трафіку. Високий FPR робить систему непридатною через постійні хибні тривоги.
Accuracy (точність)	$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$	Загальна правильність класифікації. Не завжди інформативна в контексті мережевих аномалій, оскільки нормальний трафік значно переважає аномальний (незбалансований датасет).
F1-Score	$F1 = 2 \cdot \frac{Precision \cdot Recall}{Precision + Recall}$	Ключова інтегральна метрика. Є гармонійним середнім між Precision (точністю прогнозу: $Precision = \frac{TP}{TP + FP}$) та TPR. Вона особливо важлива для оцінки NADS на незбалансованих даних, оскільки балансує між ризиком

Визначення та призначення основних метрик для оцінки систем виявлення аномалій

```
с максимальным числом переходов 30:
  0  DESKTOP-K9LTHFB.itotolink.net [192.168.0.9]
  1  192.168.0.1
  2  10.135.0.1
  3  v505.cat-4.volia.net [82.144.194.198]
  4  v1204.po4.agg-2.vo3.kiev.volia.net [77.120.2.142]
  5  192.168.0.42
  6  meta-gw.br02-kiev-vlan1595.top.net.ua [77.88.212.193]
  7  192.178.68.164
  8  74.125.245.61
  9  74.125.245.64
 10  142.251.242.41
 11  192.178.99.97
 12  108.170.234.101
 13  dns.google [8.8.8.8]

Подсчет статистики за: 325 сек. ...
          Исходный узел      Маршрутный узел
Прыжок   RTT    Утер./Отпр.   %   Утер./Отпр.  %   Адрес
  0                                             DESKTOP-K9LTHFB.itotolink.net [192.168.0.9]
                                0/ 100 =  0%    |
  1    1мс     0/ 100 =  0%     0/ 100 =  0%   192.168.0.1
                                0/ 100 =  0%    |
  2   15мс     0/ 100 =  0%     0/ 100 =  0%   10.135.0.1
                                0/ 100 =  0%    |
  3   13мс     0/ 100 =  0%     0/ 100 =  0%   v505.cat-4.volia.net [82.144.194.198]
                                0/ 100 =  0%    |
  4   11мс     0/ 100 =  0%     0/ 100 =  0%   v1204.po4.agg-2.vo3.kiev.volia.net [77.120.2.142]
                                0/ 100 =  0%    |
  5   —     100/ 100 =100%   100/ 100 =100%   192.168.0.42
                                0/ 100 =  0%    |
  6   12мс     0/ 100 =  0%     0/ 100 =  0%   meta-gw.br02-kiev-vlan1595.top.net.ua [77.88.212.193]
                                0/ 100 =  0%    |
  7   18мс     0/ 100 =  0%     0/ 100 =  0%   192.178.68.164
                                0/ 100 =  0%    |
  8   14мс     0/ 100 =  0%     0/ 100 =  0%   74.125.245.61
                                0/ 100 =  0%    |
  9   16мс     0/ 100 =  0%     0/ 100 =  0%   74.125.245.64
                                0/ 100 =  0%    |
 10   34мс     0/ 100 =  0%     0/ 100 =  0%   142.251.242.41
                                0/ 100 =  0%    |
 11   32мс     0/ 100 =  0%     0/ 100 =  0%   192.178.99.97
                                0/ 100 =  0%    |
 12   36мс     0/ 100 =  0%     0/ 100 =  0%   108.170.234.101
                                0/ 100 =  0%    |
 13   38мс     0/ 100 =  0%     0/ 100 =  0%   dns.google [8.8.8.8]

Трассировка завершена.
```

На цьому слайді представлено консоль, яка демонструє результати виконання команди traceroute до IP-адреси 8.8.8.8 (DNS-сервер Google).

Ці результати показують шлях проходження мережевих пакетів від джерела до цілі, включаючи список проміжних маршрутизаторів (хопів) та час затримки до кожного з них, що є важливим для діагностики проблем з підключенням або визначення маршруту трафіку.

```
C:\Users\User>tracert 8.8.8.8

Трассировка маршрута к dns.google [8.8.8.8]
с максимальным числом прыжков 30:

  1     1 ms     1 ms     1 ms  192.168.0.1
  2     9 ms     8 ms    12 ms  10.135.0.1
  3     8 ms     9 ms     9 ms  v505.cat-4.volia.net [82.144.194.198]
  4    11 ms    10 ms     9 ms  v1204.po4.agg-2.vo3.kiev.volia.net [77.120.2.142]
  5     9 ms    12 ms     9 ms  192.168.0.42
  6     9 ms    27 ms     9 ms  meta-gw.br02-kiev-vlan1595.top.net.ua [77.88.212.193]
  7    11 ms     8 ms    10 ms  192.178.68.164
  8    11 ms    10 ms    10 ms  74.125.245.61
  9    14 ms    16 ms    16 ms  74.125.245.64
 10   101 ms    28 ms    26 ms  142.251.242.41
 11    23 ms    72 ms    28 ms  192.178.99.97
 12    29 ms    24 ms    26 ms  108.170.234.101
 13    21 ms    23 ms    21 ms  dns.google [8.8.8.8]

Трассировка завершена.
```

Файл Правка Вигляд Перехід Захоплення Аналіз Статистика Телефонія Wireless Інструменти Довідка

not (http or dns or tcp or udp or icmp or arp)

No.	Time	Source	Destination	Protocol	Length	Info
59	17.983367	0.0.0.0	224.0.0.1	IGMPv2	46	Membership Query, general
60	17.987030	fe80::52d2:f5ff:feb…	ff02::1	ICMPv6	86	Multicast Listener Query
62	18.212084	192.168.31.62	224.0.0.252	IGMPv2	46	Membership Report group 224.0.0.252
63	18.212407	fe80::6603:6dc5:50c…	ff02::1:ff0c:a3b6	ICMPv6	86	Multicast Listener Report
64	18.212501	fe80::6603:6dc5:50c…	ff02::c	ICMPv6	86	Multicast Listener Report
65	19.219317	192.168.31.62	224.0.0.251	IGMPv2	46	Membership Report group 224.0.0.251
66	19.219808	fe80::6603:6dc5:50c…	ff02::fb	ICMPv6	86	Multicast Listener Report
67	19.220068	fe80::6603:6dc5:50c…	ff02::1:3	ICMPv6	86	Multicast Listener Report
68	19.719435	192.168.31.62	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
3542	143.417800	0.0.0.0	224.0.0.1	IGMPv2	46	Membership Query, general
3543	143.419152	fe80::52d2:f5ff:feb…	ff02::1	ICMPv6	86	Multicast Listener Query
3544	143.713274	192.168.31.62	224.0.0.251	IGMPv2	46	Membership Report group 224.0.0.251
3546	144.711847	192.168.31.62	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
3578	146.215852	192.168.31.62	224.0.0.252	IGMPv2	46	Membership Report group 224.0.0.252
3579	146.216511	fe80::6603:6dc5:50c…	ff02::1:ff0c:a3b6	ICMPv6	86	Multicast Listener Report
3580	146.216764	fe80::6603:6dc5:50c…	ff02::fb	ICMPv6	86	Multicast Listener Report
3581	147.210860	fe80::6603:6dc5:50c…	ff02::1:3	ICMPv6	86	Multicast Listener Report

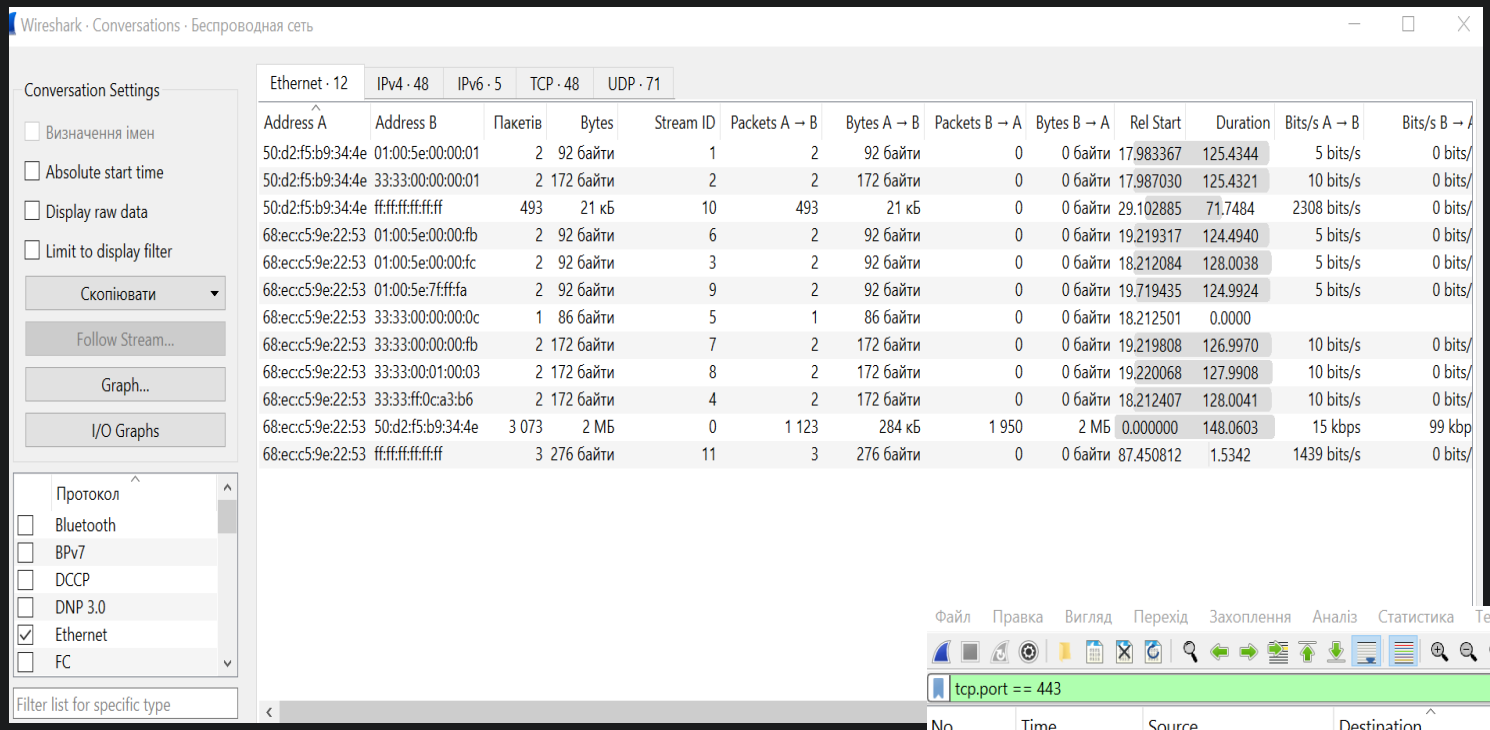
Результати аналізу мережевого трафіку за допомогою Wireshark.

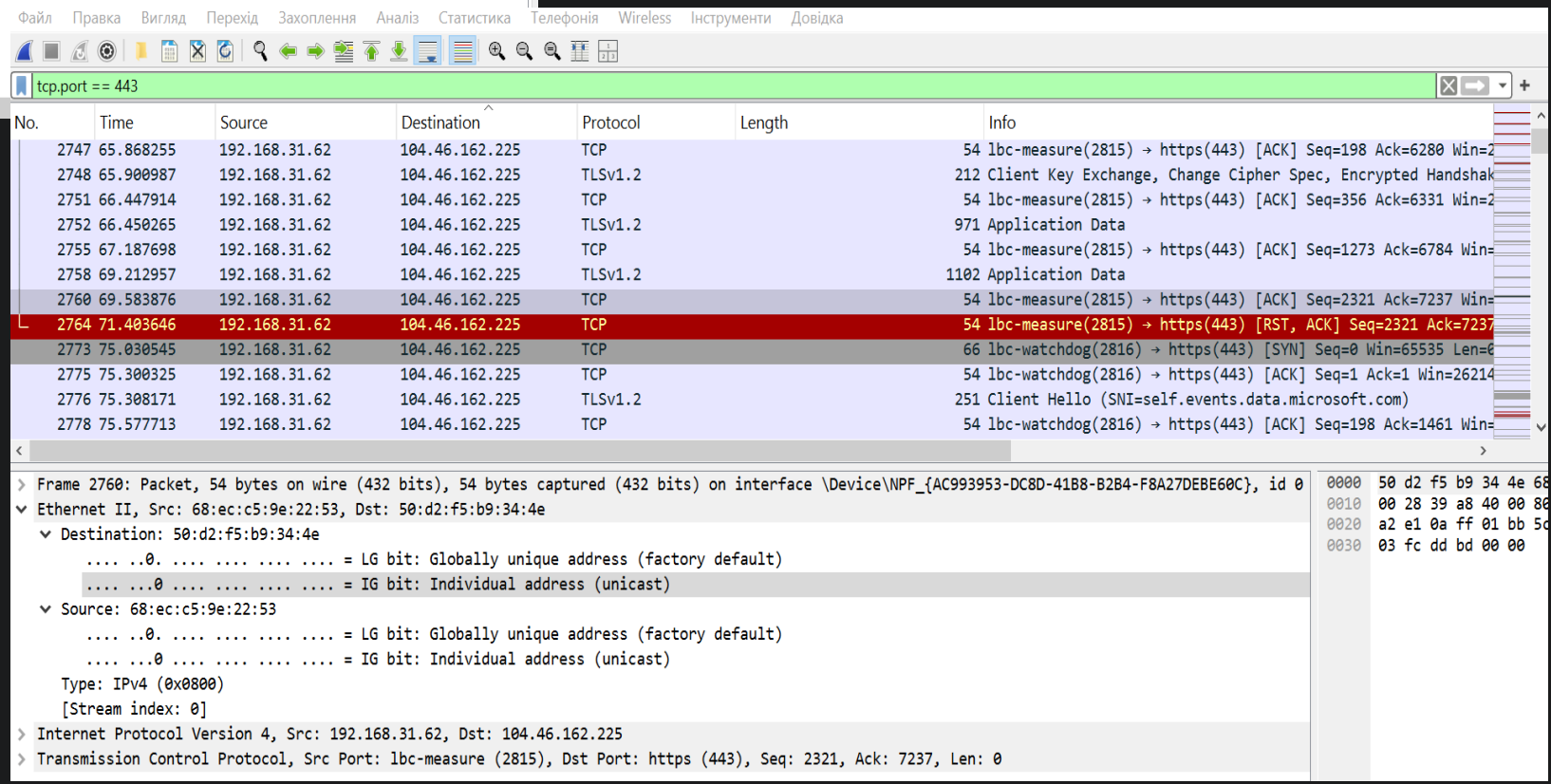
Мережевий трафік переважно складається з пакетів Internet Protocol Version 4 (85.7% від загальної кількості) та User Datagram Protocol (62.5% від загальної кількості), при цьому значну частку UDP-трафіку становить Simple Service Discovery Protocol та QUIC IETF.

Wireshark · Protocol Hierarchy Statistics · Беспроводная сеть

Протокол	Percent Packets	Пакетів	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	3586	100.0	2147691	116 k	0	0	0	3586
Ethernet	100.0	3586	2.3	50204	2712	0	0	0	3586
Internet Protocol Version 6	0.3	9	0.0	432	23	0	0	0	9
Internet Control Message Protocol v6	0.3	9	0.0	216	11	9	216	11	9
Internet Protocol Version 4	85.7	3072	2.9	61472	3321	0	0	0	3072
User Datagram Protocol	62.5	2242	0.8	17936	969	0	0	0	2242
Simple Service Discovery Protocol	3.1	110	2.2	47970	2591	110	47970	2591	110
QUIC IETF	55.7	1999	75.3	1618144	87 k	1999	1603300	86 k	2031
NetBIOS Name Service	0.1	3	0.0	150	8	3	150	8	3
Domain Name System	3.0	108	0.4	8700	470	108	8700	470	108
Data	0.6	22	0.0	925	49	22	925	49	22
Transmission Control Protocol	22.7	814	0.8	17148	926	455	9968	538	814
Transport Layer Security	10.0	359	16.3	350297	18 k	359	331271	17 k	366
Internet Group Management Protocol	0.2	8	0.0	64	3	8	64	3	8
Internet Control Message Protocol	0.2	8	0.0	320	17	8	320	17	8
Address Resolution Protocol	14.1	505	0.7	14140	764	505	14140	764	505
802.1Q Virtual LAN	1.0	37	0.0	148	7	0	0	0	37

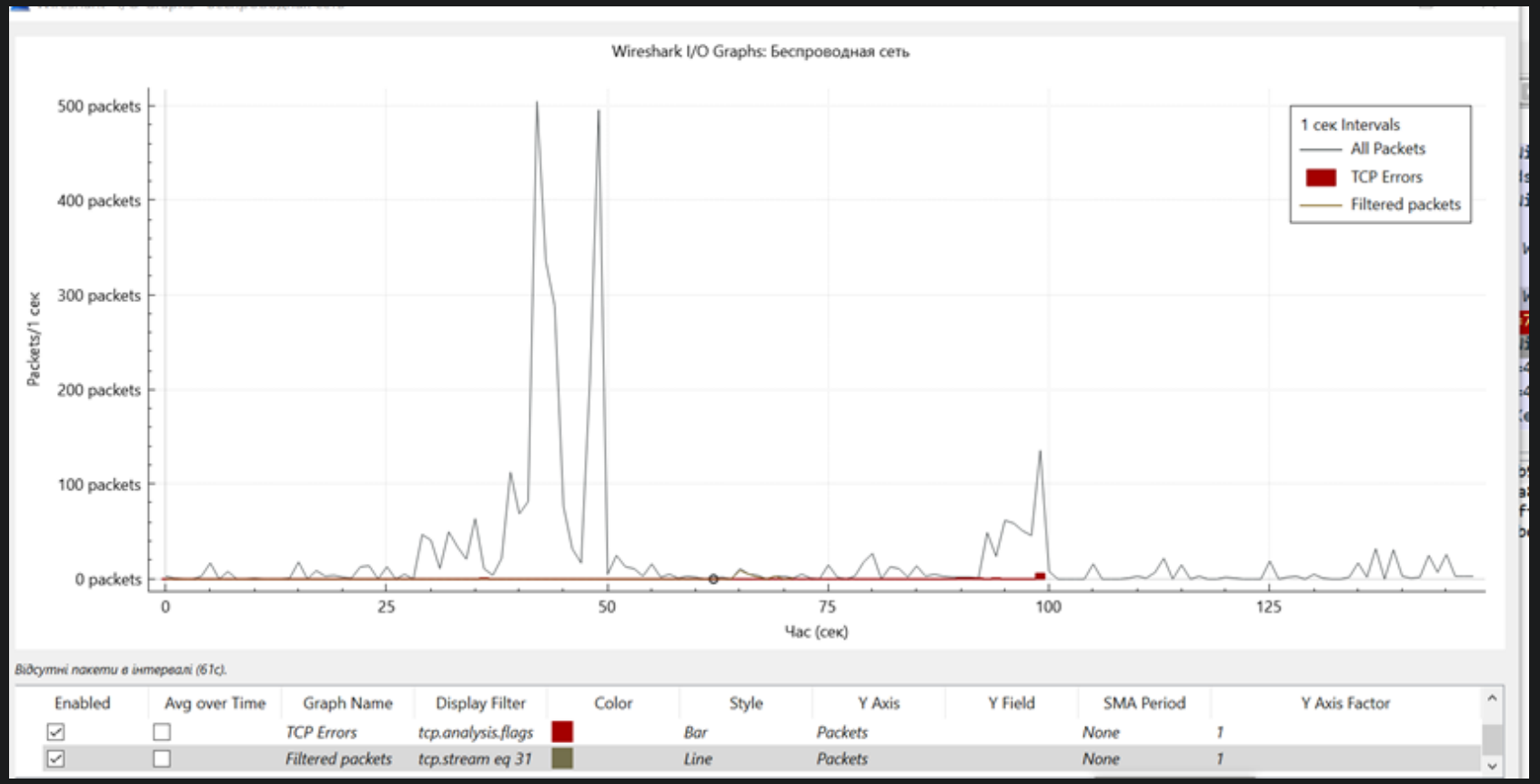
Результати аналізу мережевих розмов та окремих пакетів TCP/TLS з використанням Wireshark.





Було виявлено активну TCP/TLS комунікацію на порт 443 (HTTPS) між IP-адресами 192.168.31.62 та 184.46.162.225, яка включала обмін даними, Client Key Exchange та Handshake. Зафіксовано пакет TCP з прапорами RST, ACK, що свідчить про аномальне завершення або скидання одного з TCP-з'єднань у цьому трафіку.

Графік демонструє періодичні сплески мережевого трафіку, зокрема навколо 45-ї та 95-ї секунд. Аналіз в таблиці вказує, що джерелом затримок є зовнішній маршрутизатор (хоп 10, IP-адреса 142.251.242.41), що інтерпретується як пристрій провайдера або магістралі. Проблема затримок характеризується як тимчасові сплески, а не системна. Виявлено TCP-помилки під час сплесків пакетів, що потребує налаштування QoS або додаткового моніторингу. Аномалій протоколів не виявлено, що свідчить про "чисту мережу" з точки зору протокольних порушень. Ефективність NADS, виміряна як затримка менше 5 секунд і показник TPR близько 100%, оцінюється як висока.



Параметр	Значення	Висновок
Джерело затримки	Хоп 10 (142.251.242.41)	Зовнішній маршрутизатор (провайдер/магістраль
Характер проблеми	Тимчасові сплески	Не системна
TCP-помилки	Є, під час піків	Потребує QoS або моніторингу
Аномалії протоколів	Немає	Мережа чиста
Ефективність NADS	Tlatency < 5 с, TPR ≈ 100%	Висока

АПРОБАЦІЯ

Результати дослідження апробовано шляхом публікації тез доповідей:

Житомирська політехніка – VIII Всеукраїнська науково-технічна конференція (02.12.2025 - 03.12.2025)

1.Сарапин В.Є., Шабала Є.Є. ГІБРИДНИЙ ПІДХІД ДЛЯ ДІАГНОСТИКИ МЕРЕЖЕВИХ АНОМАЛІЙ ЧЕРЕЗ ПАРАМЕТР ХЕРСТА ТА QOS-МЕТРИКИ
2.САРАПИН В.Є. ВИЯВЛЕННЯ МЕРЕЖЕВИХ АНОМАЛІЙ ЗАСОБАМИ АНАЛІЗУ ТРАФІКУ.

Висновки та результати

Проведено комплексний аналіз архітектури мереж, класифікацію відмов (включаючи візантійські збої) та дослідження QoS. Це сформувало теоретичну базу для розробки ефективної системи діагностики.

Аналіз архітектури

Визначено вплив фізичної та логічної структури на процеси аналізу трафіку.

Експериментальна перевірка

Створено тестовий полігон та змодельовано двофазну атаку (сканування + DDoS).

Класифікація відмов

Розглянуто апаратні, програмні, людські та візантійські чинники збоїв.

Підтвердження ефективності

Практична реалізованість діагностики та її здатність до виявлення складних аномалій підтверджена метриками.