Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Методи моніторингу трафіка в корпоративній мережі

(тема)

Виконав:

студент II курсу, групи СПм-22-2

Лукірін Ю.М.
(прізвище, ініціали)

Спеціальність

123 «Комп'ютерна інженерія»
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма

Системне програмування
(повна назва освітньої програми)

Керівник: проф. Міхаль О.П.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри ЕОМ _____ Коваленко А.А.
(підпис) (прізвище, ініціали)

2024 р.

Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

Спеціальність 123 «Комп'ютерна інженерія»
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Системне програмування
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
"____" _____ 20__ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Лукіріну Юрію Михайловичу
(прізвище, ім'я, по батькові)

1. Тема роботи Методи моніторингу трафіка в корпоративній мережі

затверджена наказом по університету від " 06 " листопада 2023 р. № 1299 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 15 січня 2024 р.

3. Вхідні дані до роботи
трафік
корпоративна мережа
метод
моніторинг трафіка

4. Перелік питань, що потрібно опрацювати у роботі
Сучасні тенденції моніторингу трафіка в мережах з пакетною комутацією
Метод моніторингу трафіка корпоративної мережі
Програмна реалізація методів моніторингу та ідентифікації трафіка

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) 14 слайдів

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання та аналіз джерел за темою	06.11.2023–15.11.2023	
	роботи		
2	Аналіз існуючих методів моніторингу трафіка	16.11.2023–25.11.2023	
3	Розробка нового або модифікація існуючого	25.11.2023–10.12.2023	
	методу моніторингу та ідентифікації трафіка		
4	Програмна реалізація розробленого або	11.12.2023–25.12.2023	
	модифікованого методу		
5	Аналіз отриманих результатів	26.12.2023–05.12.2023	
6	Оформлення пояснювальної записки та		
	документів до неї		

Дата видачі завдання 06 листопада 2023 р.

Студент _____
(підпис)

Керівник роботи _____ проф. Міхаль О.П.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 64 с., 16 рис., 2 дод., 22 джерела.

КОМП’ЮТЕРНА МЕРЕЖА, ПРОТОКОЛ, ТРАФІК, МОНІТОРИНГ, ІДЕНТИФІКАЦІЯ, КОМУТАЦІЯ ПАКЕТІВ, ПРОГРАМНИЙ ЗАСІБ.

Метою кваліфікаційної роботи є аналіз методів моніторингу трафіка, методів ідентифікації трафіка та удосконалення технологій передачі трафіка за рахунок підвищення якості кластеризації та класифікації трафіка.

У ході виконання кваліфікаційної проведено аналіз методів моніторингу трафіка, методів ідентифікації трафіка та удосконалення технологій передачі трафіка за рахунок підвищення якості кластеризації та класифікації трафіка. Проаналізовано стан сучасних корпоративних мереж із пакетною комутацією щодо застосовуваних методів ідентифікації та моделей трафіку, технологій та протоколів передачі інформації. Також проведено аналіз алгоритмів класифікації трафіку протоколів, що використовуються у корпоративних телекомунікаційних мережах. Запропонована архітектура програмних засобів поглибленого моніторингу мережевого трафіка, що дозволяє розробляти і налагоджувати модулі підтримки протоколів на попередньо збереженому трафіку і згодом використовувати ці модулі в реальному режимі часу. Розроблені та реалізовано програмні засоби для проведення моніторингу корпоративної мережі.

ABSTRACT

Master’s thesis: 64 pages, 16 figures, 2 appendices, 22 sources.

COMPUTER NETWORK, PROTOCOL, TRAFFIC, MONITORING, IDENTIFICATION, PACKET SWITCHING, SOFTWARE.

The major goal of this thesis is the analysis of traffic monitoring methods, traffic identification methods, and improvement of traffic transmission technologies by improving the quality of traffic clustering and classification.

In the course of the qualification, an analysis of traffic monitoring methods, traffic identification methods and improvement of traffic transmission technologies by improving the quality of traffic clustering and classification was carried out. The state of modern corporate networks with packet switching is analyzed in terms of the applied identification methods and traffic models, technologies and information transmission protocols. An analysis of traffic classification algorithms of protocols used in corporate telecommunication networks is also carried out. The proposed architecture of software tools for in-depth monitoring of network traffic, which allows you to develop and debug protocol support modules on pre-saved traffic and subsequently use these modules in real time. Developed and implemented software tools for monitoring the corporate network.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ПЗ – програмний засіб

ТМ – телекомунікаційна мережа

IGP – протоколи внутрішнього шлюзу

MMPP – метод, що моделюється на основі Марківського процесу

MPLS – багатопротокольнакомутація по міткам

P2P – мережна інфраструктура без централізованого сервера

VPN – віртуальна приватна мережа

ВСТУП

В даний час всі сфери діяльності, пов'язані з інформаційно-телекомунікаційними технологіями, у всьому світі знаходяться на етапі інтенсивного розвитку. Цим визначається перенесення в область телекомунікаційних, обчислювальних мереж та мереж передачі даних тих напрямів діяльності, що раніше існували незалежно. З'являються нові вимоги до послуг, що надаються відповідно до зростаючих очікувань користувачів.

Стан сучасної інфраструктури телекомунікаційних мереж має відповідати цим вимогам. Практично оформлений перехід від різноманітних телекомунікаційних та обчислювальних мереж до мереж, які об'єднують мобільних та фіксованих абонентів. Поряд із зростанням кількості користувачів збільшується перелік послуг, що надаються абонентам телекомунікаційних мереж: електронна пошта, перегляд Web-сторінок, ігри, музика, відео, чати, потокове відео високого дозволу, IP-телефонія, банківські послуги, державні послуги, соціальні мережі та ін.

За результатами досліджень компанії Cisco Systems с 2007 року відбулося приблизно триразове збільшення трафіку різних сервісів мережі Інтернет. Також з'являються нові технології розповсюдження інформації, що вже призвело до появи нових видів та типів трафіку, протоколів інформаційного обміну, а також такого поняття, як мережне поведінка користувачів». Широко поширені в даний час системи з архітектурою «клієнт-клієнт», так звані системи P2P (peer-to-peer system – мережна інфраструктура без централізованого сервера). Трафік подібних мереж є одним з основних джерел зростання навантаження у сучасних телекомунікаційних мереж. В даний час всі сфери діяльності, пов'язані з інформаційно-телекомунікаційними технологіями, у всьому світі знаходяться на етапі інтенсивний розвиток. Цим визначається перенесення в область телекомунікаційних, обчислювальних мереж та мереж передачі даних тих

напрямів діяльності, що раніше існували незалежно. З'являються нові вимоги до послуг, що надаються відповідно до зростаючих очікування користувачів. Стан сучасної інфраструктури телекомунікаційних мереж має відповідати цим вимогам. Практично оформлений перехід від різноманітних телекомунікаційних та обчислювальних мереж до мереж, що об'єднує мобільних та фіксованих абонентів. Поряд із зростанням кількості користувачів збільшується перелік послуг, надаються абонентам телекомунікаційних мереж: електронна пошта, перегляд Web-сторінок, ігри, музика, відео, чати, потокове відео високого дозволи, IP-телефонія, банківські послуги, державні послуги, соціальні мережі та ін. За результатами досліджень компанії Cisco Systems с 2007 року відбулося приблизно триразове збільшення трафіку різних сервісів мережі Інтернет. Також з'являються нові технології розповсюдження інформації, що вже призвело до появи нових видів та типів трафіку, протоколів інформаційного обміну, а також такого поняття, як мережне поведінка користувачів». Широко поширені в даний час системи з архітектурою «клієнт-клієнт», так звані системи P2P (peer-to-peer system – мережна інфраструктура без централізованого сервера). Трафік подібних мереж є одним з основних джерел зростання навантаження у сучасних телекомунікаційних мереж.

Складається ситуація, коли, з одного боку, прогрес підштовхує суспільство до все більш інтенсивного використання засобів передачі інформації, а з іншого боку, необхідно забезпечувати функціонування телекомунікаційних мереж із заданими показниками якості. Це відбувається при зростаючому обсязі інформації, що передається, і появі нових способів та технологій мережевої взаємодії. Гостро це завдання стоїть для корпоративних телекомунікаційних мереж, оскільки вони критичні до втрат та затримок інформації, а також до підтримки постійної працездатності через те, що інформація, що циркулює в них, впливає на ухвалення рішень керівництвом організації. Затребуваність рішень забезпечення якості функціонування мереж у корпоративному сегменті обумовлена його

бурхливим розвитком. При експлуатації корпоративних телекомунікаційних мереж необхідно постійно адаптувати алгоритми та методи управління передачею інформації під сучасні умови уникнення негативних наслідків для компанії та клієнтів. Адаптовані методи управління необхідно закладати на етапі проектування мереж, а для їх розробки необхідно мати чіткі уявлення про об'єкт управління, під яким розуміється динамічний процес передачі трафіку по телекомунікаційним мережам. З вказаних причин необхідно досліджувати трафік корпоративних телекомунікаційних мереж із пакетною комутацією.

Актуальність дослідження обумовлена необхідністю розробки механізму точної ідентифікації різнорідного трафіку, який не має явних ознак класифікації. Цей механізм повинен брати участь у формуванні керуючих впливів під час експлуатації і адміністрування корпоративної телекомунікаційної мережі для підвищення якості передачі трафіку При вирішенні завдань у сфері управління телекомунікаційними мережами ідентифікація нерозривно пов'язана з сегментацією трафіку, виділенням у його структурі однорідних ділянок у відповідно до заданого ознакового простору.

Цей простір ознак бере участь у класифікації трафіку для подальшого вироблення керуючих впливів. Результат класифікації, у свою чергу, залежить від точності визначення меж ділянок трафіку, що має схожі характеристиками. У межах цих ділянок трафік має стійкі класифікаційні ознаки. Якісне вирішення завдання ідентифікації трафіку необхідне для розробки нових алгоритмів функціонування обладнання обчислювальних мереж, маршрутизації, а також в галузі інформаційної безпеки, де гостро стоїть завдання вироблення ідентифікаційних алгоритмів телекомунікаційних мереж та класифікаційних ознак об'єктів з метою виявлення порушників та приховування вразливих параметрів та характеристик. Також результати ідентифікації трафіку телекомунікаційних мереж можуть знайти застосування у завданнях радіомоніторингу та статистичного

демультиплексування, де висока апріорна невизначеність.

Метою кваліфікаційної роботи є аналіз методів моніторингу трафіка, методів ідентифікації трафіка та удосконалення технологій передачі трафіка за рахунок підвищення якості кластеризації та класифікації трафіка.

Об’єкт дослідження: трафік в корпоративних комп’ютерних мережах з пакетною комутацією.

Завдання:

- аналіз стану сучасних корпоративних мереж із пакетною комутацією щодо застосовуваних методів моніторингу, ідентифікації та моделей трафіку, технологій та протоколів передачі інформації;
- аналіз алгоритмів класифікації трафіку протоколів, що використовуються у корпоративних телекомунікаційних мережах;
- аналіз існуючих методів та моделей аналізу мережних пакетів, враховучи особливості передачі данних по мережі (втрата окремих пакетів, стиснення і шифрування даних, вкладене тунелювання);
- розробка програмних засобів моніторингу корпоративної мережі з використанням досліджених моделей та методів.

1 СУЧАСНІ ТЕНДЕНЦІЇ МОНІТОРИНГУ ТРАФІКА В МЕРЕЖАХ З ПАКЕТНОЮ КОМУТАЦІЄЮ

1.1 Мережі з пакетною комутацією, тенденції розвитку

В даний час одним з основних факторів розвитку організацій та підприємств різного рівня є успішне впровадження та розвиток інформаційних технологій. Основу для впровадження таких технологій становлять корпоративні мережі передачі. Корпоративна мережа – це комп'ютерна мережа змішаної топології, куди входять кілька локальних обчислювальних мереж.

Корпоративна мережа об'єднує віддалені філії та адмініструється співробітниками корпорації. Фактично, це транспортна інфраструктура організації, що підтримує вирішення актуальних завдань та що забезпечує досягнення її цілей (тобто виконання місії організації) [1,2]. Це система, за допомогою якої здійснюється передача інформації між різними програмами, що використовуються в системі корпорації. У на даний час існує безліч варіантів побудови корпоративних телекомунікаційних мереж. Архітектура залежить від розв'язуваних завдань конкретної організації. Проте корпоративні мережі мають багато спільного. На рисунку 1.1 представлена загальна структура корпоративної телекомунікаційної мережі. На цьому рисунку показана територіально-розподілена корпоративна мережа, що поєднує внутрішні ресурси корпорації, та мережу загального користування, що є інструментом взаємодії з мобільними користувачами або дистанційними співробітниками. Точками сполучення цих мереж є такі ресурси та інструменти: Web-сервер, сервер електронної торгівлі, сервер доступу та реєстрації, поштовий сервер та ін.

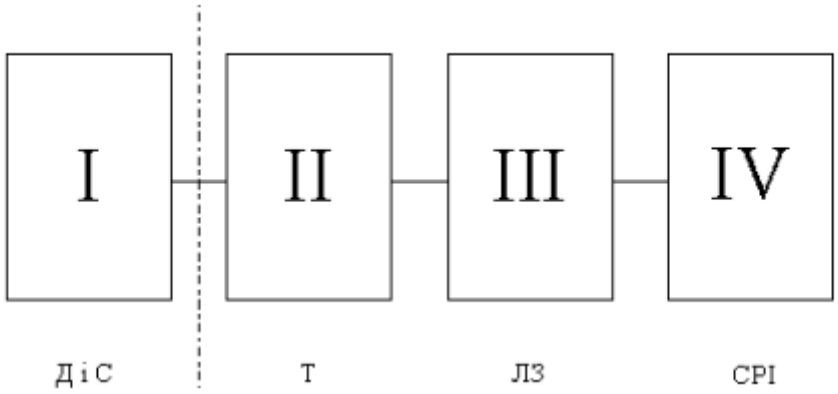

Рисунок 1.1 – Узагальнена структура корпоративної телекомунікаційної мережі

Незважаючи на те, що на рисунку 1.1 опорна корпоративна мережа та мережа загального користування розділені, в даний час ці складові структури корпоративні мережі інтегровані між собою. Організації відмовляються від побудови та утримання власної транспортної інфраструктури. Ця тенденція характерна як для дрібних організацій, які не мають великих фінансових коштів і для великих світових корпорацій. Прикладом може служити банківський сектор, де частина функцій за змістом внутрішньої інфраструктури передано посередникам (аутсорсингові контакт-центри, поштові системи, центри обробки даних (ЦОД) та ін.).

Зв'язок із ними здійснюється через громадські мережі, у тому числі через Інтернет. Відповідно, розташовані у них офіси користуються послугами операторів супутникових систем зв'язку. Іншим прикладом можуть бути віртуальні стільникові оператори (MVNO – Mobile Virtual Network Operator). Мережева інфраструктура цих компаній як для обслуговування внутрішньокорпоративних ресурсів, так і для обслуговування клієнтів, повністю побудована на базі мереж операторів стільникового зв'язку. У випадку з MVNO інтеграція громадських та корпоративних телекомунікаційних мереж послужила розвитку нової галузі бізнесу. Передумовою об'єднання різних мереж у корпоративному сегменті

з'явився розвиток технологій, що задовольняють вимогам щодо якості, швидкості та безпеки передачі контенту.

Основою побудови системи передачі та управління корпоративним контентом стало використання віртуальних приватних мереж (VPN – Virtual Private Network) у мережах операторів зв'язку та в мережах компаній, а також їх використання окремими користувачами. Віртуальна приватна мережа (VPN) є приватною мережевою службою, що організується поверх мережі загального користування. Найкращі ринки послуг VPN: Таїланд - 24%; Індонезія – 22%; Китай – 20%; Бразилія – 19%. Економіки перерахованих країн динамічно розвиваються.

Практично всі великі корпорації та компанії мають у них свої представництва та виробничі потужності, що тягне за собою вимогу щодо наявності у зазначених регіонах внутрішньокорпоративних та міжкорпоративних мереж зв'язку. Зростання мережевих можливостей у країнах Азії та Латинської Америки тягне за собою збільшення трафіку в інших країнах, наприклад, у Європі та Північній Америці. Зростання VPN послуг спостерігається у розвинених країнах: Німеччина – 6 %, США – 5 %, Великобританія – 5%, Австралія – 4%. Такі невисокі показники, по-багатьом параметрам, обумовлені обмежувальним законодавством, однак, і вони свідчать про розвиток ринку надання послуг з організації мереж VPN.

Подана на рисунку 1.2 статистика регулярності використання VPN, за даними ресурсу www.globalwebindex.net, говорить про їхню популярність. З наведеної статистики випливає, що ринок послуг з надання послуг VPN розвивається великими темпами і найближчим часом спостерігатиметься стале зростання числа корпоративних VPN-каналів.

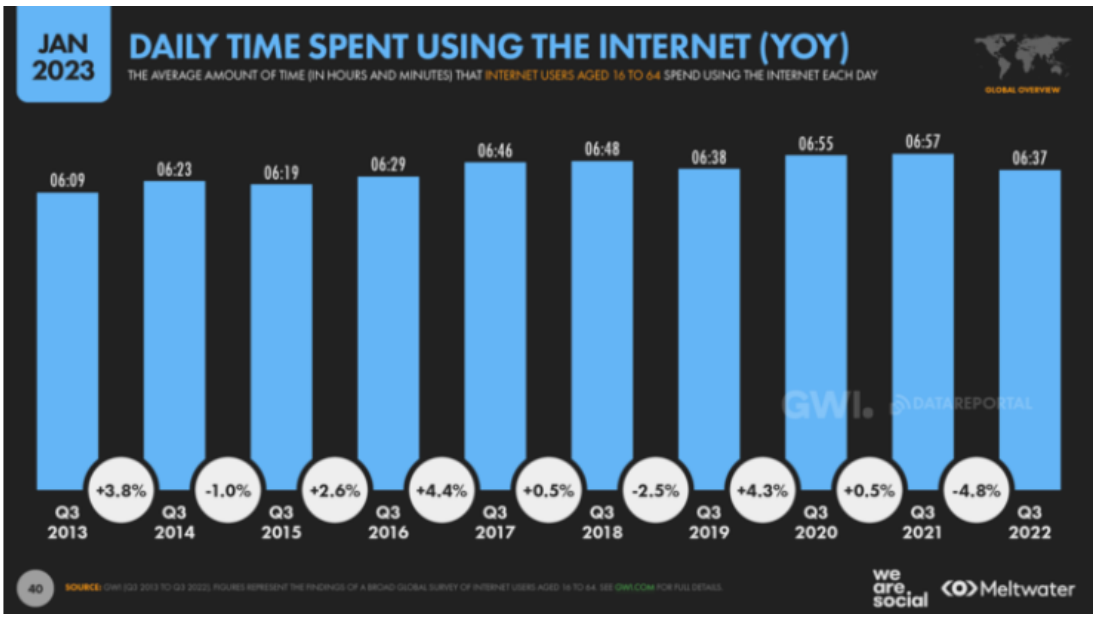

Рисунок 1.2 – Регулярність користування

З боку звичайних користувачів причиною підвищеного інтересу до VPN є анонімність у мережі. На графіку, наведеному на рисунку 1.3, наведено статистику використання сервісів VPN для забезпечення анонімності перегляду мережевих ресурсів (за даними ресурсу www.globalwebindex.net).

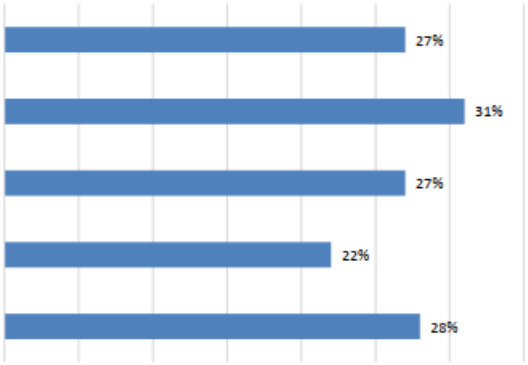

Рисунок 1.3 – Статистика використання VPN

До поширення різноманітних VPN-послуг як засобів забезпечення безпеки мережевого обміну підштовхує страх користувачів та організацій

перед кіберзлочинами, серед яких найчастішими є: крадіжка особистих даних та крадіжка даних кредитних карток. У 2015 році жертвами подібних злочинів стали 63% і 45% від усіх, хто зазнав кібератакам користувачів Інтернету відповідно. Це призвело до того, що майже 30% користувачів у США відмовилися від проведення фінансових транзакцій у мережі у 2015 році. При цьому близько 63% компаній не мають жодних процедур або планів дій на випадок кібератак на їхні ресурси мережі. В результаті бізнес різного рівня та масштабу несе великі витрати, а часто та збитки. Серед основних причин недостатньої захищеності корпоративних даних у мережі називаються такі:

- недостатня кількість компетентного у питаннях мережної безпеки персоналу – 56%;
- недостатність бюджету для закупівлі відповідних рішень та технологій у сфері IT-безпеки – 45%;
- відсутня можливість контролювати співробітників для запобігання витоку інформації – 36 %.

На перший план зараз виходить необхідність попередження загроз, оскільки сучасні рішення у сфері боротьби з атаками зловмисників та усунення їх наслідків часто неефективні через так званої вразливості нульового дня. Зловмисники запускають і завершують атаку того ж дня, так що система безпеки не встигає відреагувати.

Подібні вразливості зросли з 2013 по 2015 рік на 125%. Послуги VPN дозволяють попередити та суттєво знизити негативний вплив перерахованих вище причин витоків корпоративних даних, особливо в умовах збільшення у користувачів різного роду пристроїв, що взаємодіють з мережею.

Стан сучасних корпоративних мереж із пакетною комутацією обумовлено суттєвим числом факторів, що впливають на структуру корпоративної мережі. Ці чинники поділяються на внутрішні та зовнішні. Внутрішні фактори:

- необхідність витрачати значні ресурси для обслуговування підсистем

зберігання, обробки та управління корпоративним контентом;

- складність міжмережевої взаємодії внутрішніх локальних обчислювальних мереж віддалених офісів, розташованих найчастіше в важкодоступних районах;

- економічно обґрунтована необхідність взаємодії з клієнтами та співробітниками за допомогою загальнодоступних мереж (у тому числі Інтернет).

Зовнішні чинники:

- збільшення швидкостей передачі інформації та надання широкосмугового доступу до Інтернету;

- зростання числа та активний розвиток мобільних засобів комунікації (Смартфони, планшети, ноутбуки);

- конвергенція цифрових мереж зв'язку (телефонія, відео, передача даних) за допомогою протоколу IP як основний;

- розширення можливостей операторів та провайдерів по об'єднанню різного трафіку, в тому числі, що з'являється під впливом впровадження нових технологій;

- поява можливості надавати більший обсяг додатків та послуг з мережі провайдерів при одночасному скороченні вимог до обладнання, що розміщується на території користувача.

Таким чином, під впливом вищезгаданих факторів відбувається відмова від опорної корпоративної мережі та передача її функцій мережі загального користування, адміністрованого оператором зв'язку, отримують розвиток послуги VPN. Мережі VPN дозволяють віддаленим вузлам безпечно підключатися через мережу загального користування без додаткових витрат на купівлю чи оренду виділених ліній мережі.

Додатковим поштовхом впровадження VPN у мережах операторів став розвиток технології MPLS (MultiProtocol Label Switching – багатопротокольна комутація за мітками). Технологія MPLS запускає VPN, забезпечуючи подібну канальну структуру, орієнтовану на організацію

з'єднань, дозволяючи операторам розгортати VPN поверх інфраструктури IP-мережі, зазвичай не орієнтованої на з'єднання.

У сучасному корпоративному сегменті технологія MPLS стає основою корпоративної телекомунікаційної мережі з урахуванням мереж загального користування. Цьому сприяють основні переваги технології:

- технологія MPLS дозволяє єдиній конвергованій мережі підтримувати як нові, так і існуючі послуги, створюючи ефективний шлях переходу до IP-інфраструктури. MPLS функціонує поверх як інфраструктура DS3, SONET, 10/100/1000/10G Ethernet і мереж IP, ATM, ретрансляції кадрів, Ethernet та TDM;

- MPLS дозволяє формувати трафік. Явна (точно визначена) маршрутизація та функція формування трафіку дозволяють ущільнити більший обсяг даних у межах наявної пропускної спроможності;

- MPLS підтримує надання послуг із гарантованою якістю обслуговування (QoS – quality of service). Пакети, які мають доставлятися з високою якістю, можуть позначатися, дозволяючи провайдерам забезпечувати певні малі значення затримки для мовних та відео сигналів у наскрізному з'єднанні;

- MPLS спрощує вимоги обробки, які пред'являються до маршрутизаторів, оскільки маршрутизатори просто передають пакети, ґрунтуючись на фіксованих мітках;

- MPLS забезпечує відповідний рівень безпеки, щоб зробити IP-мережу такою ж безпечною, як мережа ретрансляції кадрів у WAN, одночасно скорочуючи потребу на шифрування в IP-мережах загального користування. Мережі VPN з урахуванням MPLS добре регулюються.

Оскільки вони базуються на мережі провайдера, то для споживача відсутня потреба конфігурування та управління. Видно, що переваги, що надаються технологією MPLS, задовольняють сучасним напрямам розвитку корпоративних телекомунікаційних мереж. Широке впровадження мереж MPLS продиктовано впливом на сектор корпоративних комунікацій

зазначених вище зовнішніх та внутрішніх чинників, які впливають структуру корпоративної мережі.

З використанням технології MPLS мережі VPN поділяються на дві категорії:

- на основі споживача: VPN конфігурується виключно в устаткуванні, розташованому на території користувача, та використовує протоколи тунелювання через мережу загального користування, як правило, IPSec (IP Security).
- на базі мережі: VPN конфігурується в апаратурі провайдера послуг та керується провайдером. MPLS VPN є прикладом VPN на базі мережі. Сучасні корпоративні мережі з пакетною комутацією включають обидві категорії. Перша категорія забезпечує безпеку віддалених з'єднань. Для решти всіх цілей використовується друга категорія.

1.2 Актуальність досліджень в області моніторингу трафіка

Виходячи із сучасного стану корпоративних телекомунікаційних мереж для успішного впровадження VPN у корпоративний сегмент необхідно удосконалювати методи розподілу ресурсів мережі, вибору маршрутів передачі контенту та підвищення ефективності використання мережевих ресурсів. Ті можливості керування трафіком, які пропонують сучасні протоколи внутрішньої маршрутизації недостатні.

Протоколи IGP (Interior Gateway Protocol – протоколи внутрішнього шлюзу), що використовуються операторами, засновані на алгоритмах пошуку найкоротшого шляху. Вони вносять суттєвий внесок у проблеми перевантаження у внутрішній мережі оператора. Алгоритми маршрутизації SPF (Shortest Path First – перевага найкоротшого) шляхи), у випадку, оптимізуються з урахуванням простий адитивної метрики. Ці протоколи залежать від топології, і характеристики трафіку не приймаються у увагу при вирішенні питань щодо вибору маршруту.

В результаті цього перевантаження часто виникає, коли спостерігається будь-яке з наведених нижче умов:

- трафік від джерела до адресата перевищує пропускну спроможність каналу на найкоротшому шляху. На каналі (і, отже, найкоротшому шляху) виникає перевантаження, а більш довгі шляхи між цією парою вузлів при цьому можуть бути не завантаженими. Потік трафіку маршрутизується через канал або інтерфейс маршрутизатора, який не забезпечує необхідної потоку смуги пропускання;

- найкоротші шляхи для різних відправників можуть збігатися на деяких каналах, і якщо загальний трафік від усіх джерел перевищить можливості такого каналу, виникає навантаження.

Проблеми можуть також виникати внаслідок зміни трафіку з часом, якщо маршрутна конфігурація не зміниться досить швидко. Це призводить до того, що топологія мережі та маршрутна конфігурація з часом стають не оптимальними, що може призводити до виникнення постійного навантаження. Зазначені ситуації виникають навіть у випадках, коли є інші шляхи з достатньою пропускною спроможністю.

Саме цей аспект проблеми насичення (симптом неоптимального розподілу ресурсів) є предметом вирішення актуальної задачі управління трафіком. Розв'язання задачі оптимального розподілу навантаження між рівноцінними шляхами на етапі проектування мережі може допомогти при виникненні другої з наведених вище умов. Однак у процесі експлуатації мереж із застосуванням протоколів IGP воно мало допомагає при вирішенні першої проблеми особливо в невеликих мережах із щільною топологією, якими і є переважно корпоративні мережі.

Інше завдання – ідентифікація мережевого трафіку з метою створення оптимального алгоритму управління ним. Проводячи ідентифікацію та якісний аналіз трафіку, можна прогнозувати зміну параметрів (наприклад, інтенсивності) у часі. Вирішення цього завдання дозволяє виробляти керуючі впливи в процесі експлуатації мережі в умовах навантаження, або зміни виду

навантаження, що передається.

Процес перенесення корпоративного трафіку та оброблюваних даних у громадські мережі стикаються з низкою труднощів. Багато протоколів, застосовувані з успіхом у корпоративних віртуальних мережах, побудованих своїми силами, не мають майбутнього в операторів зв'язку, які прагнуть надавати бізнес-клієнтам послуги організації та управління VPN. Наприклад, протокол IPSec у тунельному режимі визнаний одним із самих надійних способів передачі трафіку, він підходить для захисту будь-яких додатків, що базуються на транспортному та вищих рівнях базової еталонної моделі взаємодії відкритих систем (open systems interconnection basic reference model - OSI). Однак у процесі експлуатації мережевий Інфраструктури виявились проблеми з інтероперабельністю VPN обладнання різних виробників.

Отже, основним актуальним завданням у галузі проектування, експлуатації та управління корпоративними мережами є ефективним спільне використання мережевих ресурсів для безлічі потоків трафіку при мінімізації можливих навантажень (насичення). Якісне рішення цієї завдання дозволяє досягти економічної переваги використання мереж з комутацією пакетів загалом та MPLS-мереж, зокрема, як основи побудови корпоративних телекомунікацій тією чи іншою мірою, всі завдання, що виникають під час експлуатації та проектування телекомунікаційних мереж, зводяться до вироблення керуючих впливів, і процес управління передбачає вирішення завдань практично у всіх аспектах функціонування телекомунікаційної мережі.

Відповідно до рекомендацій ITU-T X.700 та стандарту ISO 7498-4 можна виділити п'ять функціональних груп завдань управління мережею [3, 4]: 1-я група: управління конфігурацією мережі та ім'ям – ці завдання полягають у конфігуруванні параметрів як окремих елементів мережі, так і телекомунікаційної мережі в цілому. Для елементів мережі за допомогою цієї групи завдань визначаються мережеві адреси, ідентифікатори (імена), географічне положення.

Для мережі загалом управління конфігурацією зазвичай починається з побудови карти мережі, тобто відображення реальних зв'язків між елементами мережі та зміни зв'язків між елементами мережі. 2-я група: обробка помилок – ця група завдань включає виявлення, визначення та усунення наслідків збоїв та відмов мережі. 3-я група: аналіз продуктивності та надійності – завдання цієї групи пов'язані з оцінкою таких параметрів, як час реакції системи, пропускна здатність реального або віртуального каналу зв'язку, інтенсивність трафіку в окремих сегментах і каналах мережі, ймовірність спотворення даних за їх передачі через мережу, і навіть коефіцієнт готовності мережі. Функції аналізу продуктивності та надійності мережі потрібні як для оперативного управління мережею, так планування розвитку мережі. 4-а група: управління безпекою – завдання цієї групи включають у контроль доступу до даних при їх зберіганні і передачі через мережу.

Базовими елементами управління безпекою є процедури автентифікації користувачів, призначення та перевірки прав доступу до ресурсів мережі, управління повноваженнями тощо. 5-а група: облік роботи мережі – завдання цієї групи полягають у реєстрації часу використання різних ресурсів мережі – пристроїв, каналів та транспортних служб.

На сучасному етапі розвитку систем моніторингу та управління корпоративними телекомунікаційними мережами основними завданнями є [5, 6]:

- автоматичне виявлення мережевих пристроїв та визначення відносин між ними;
- збирання та зберігання ключових параметрів вузлів мережі;
- автоматична реакція на події; створення аналітичних звітів для аналізу та планування розвитку мережі;
- підтримка баз даних пристроїв для керування IT-активами; – управління за допомогою стратегій;
- керування великими мережами за допомогою розподіленої

архітектури з будь-якої точки мережі.

Для вирішення перелічених завдань в даний час починає активно застосовуватися технологія Traffic Engineering (далі – TE). У широкому трактуванні під нею розуміється глобальна оптимізація мережі за рахунок зміни всіх можливих параметрів: кількості та продуктивності мережевих пристроїв, топології зв'язків між ними, швидкостей каналів передачі даних, пріоритетів обслуговування потоків тощо [7].

У зазначеному документі у технологію TE включаються методи різних часових масштабів:

- керування в реальному масштабі часу, коли параметри змінюються з періодом кілька секунд і навіть мікросекунд. До цього типу належать методи забезпечення якості обслуговування в маршрутизаторах, які використовують різні дисципліни обслуговування черг та оперують кожним окремим пакетом;
- оперативне керування параметрами з періодичністю в декілька годин чи днів. Сюди входять і методи вибору шляхів проходження трафіку через мережу, в яких шляхи трафіку варіюються тільки в тому випадку, коли вимірювання показують стійку зміну інтенсивностей потоків у продовженні кількох годин чи днів – більш швидкоплинні флуктуації відпрацьовуються методами QoS кожним із вузлів;
- планування мережі, що регламентує зміни параметрів мережі один раз на кілька місяців чи років. В цьому випадку як параметр25 виступають структурні характеристики мережі: кількість та типи маршрутизаторів, топологія та типи каналів зв'язку, а також інші параметри, зміна яких потребує великих витрат часу та коштів.

Складність для керування мережним трафіком у корпоративних мережах представляє велику кількість різних класів трафіку з різними вимогами щодо обслуговування. При цьому поява диференційованих послуг додатково загострює ці вимоги. Необхідно вирішувати завдання ідентифікації та аналізу трафіку. На етапі вирішення цих завдань

застосовуються такі методи: пакети групуються в поведінкові агрегати, кожен із яких має певний набір характеристик поведінки чи параметрів доставки. на практиці вимоги щодо доставки конкретної множини пакетів можуть виражатися явно чи неявно.

Два найбільш важливі параметри доставки трафіку пов'язані з обмеженнями можливостей та QoS. Обмеження можливостей можуть виражатися статистично через пікову та середню швидкість, величину сплесків або тим чи іншим детермінованим вказівкою ефективної пропускну здатність. Вимоги QoS можуть виражатися у термінах обмеження цілісності (наприклад, втрати пакетів) та обмеження часу (наприклад, затримки окремих пакетів та варіації затримки послідовних пакетів одного потоку).

Однак якщо подібна класифікація задовольняє виконання вимог QoS (обмеження цілісності та тимчасові обмеження), то відповідності параметрів, пов'язаних з обмеженням можливостей, вона не задовольняє. Обмеження можливостей оперують зі статистикою великого кількості параметрів і припускають, внаслідок цього, велику різноманітність класи трафіку. Трафік об'єднується відповідно до поведінкових характеристиками певні моделі. Процес отримання та накопичення всіляких моделей триває протягом усього часу функціонування мережі передачі і зводиться, зрештою, до ідентифікації трафіку, виділення трафіку певної моделі та наступної класифікації. У документі RFC 2475 описується модель процесу організації трафіку, яка складається з 4 фаз.

Визначення правил управління з критеріїв оптимізації.

Визначення результатів вимірювання параметрів мережі. Якщо дані мережевих вимірів не доступні, замість них може використовуватися теоретична модель завантаження, що відображає очікуваний стан мережі. Така модель може бути побудована на основі оцінки або екстраполяції результатів проведених раніше вимірів. Для побудови теоретичної моделі може також застосовуватися математичне моделювання характеристик трафіку чи інші методи.

Аналіз стану мережі та визначення навантажувальних характеристик Аналіз продуктивності може бути превентивним та/або реактивним. Превентивний аналіз дозволяє ідентифікувати потенційні проблеми, яких ще немає, але можуть виникнути у майбутньому. Реактивний аналіз визначає існуючі проблеми та причини їх виникнення за допомогою діагностики, а також оцінює за необхідності підходи до вирішення проблем. В процесі аналізу може використовуватися безліч кількісних та якісних методів, включаючи аналіз на основі моделей та імітацію. Фаза аналізу може включати дослідження концентрації та розподілу трафіку по мережі або її27 підмережам, визначення навантажувальних характеристик, виявлення наявних або потенційних "пробок", а також ідентифікацію мережевих "патологій" типу неефективного розташування каналів, конструктивних помилок, конфігураційних проблем. У процесі аналізу може бути створена матриця трафіку. Результати аналізу мережі можуть бути описовими чи директивними.

Оптимізація продуктивності мережі.

Ця фаза включає процес рішення щодо вибору та реалізації дій з числа наявних варіантів. Дії оптимізації можуть включати застосування відповідних методів для контролю пропонованого трафіку або розподілу трафіку по мережі. До числа таких дій може відноситися і додавання каналів або збільшення пропускної спроможності наявних каналів, розгортання додаткового обладнання (маршрутизатори, комутатори), систематичне підстроювання параметрів, пов'язаних з маршрутизацією (таких як метрики IGP та атрибути BGP), та параметрів керування трафіком.

Оптимізація продуктивності може також включати ініціювання процесу планування мережі з метою покращення архітектури та організації мережі, розширення ємності, вибору технології та конфігурації мережевих елементів з урахуванням поточних та перспективних потреб. Для подолання перерахованих вище труднощів поряд із методами ТЕ використовуються технології програмно-визначуваних територіально розподілених мереж

(software-defined networking in a wide area network – SDWAN).

Перевагами використання мереж SD-WAN є динамічна маршрутизація додатків найбільш ефективним з'єднанням WAN в кожен момент часу та використання підтримки додатків замість маршрутизації пакетів, коли ресурси WAN резервуються та виділяються під конкретні бізнес-завдання. Існує попит на так звані захищені рішення SD-WAN (Secure SD-WAN), які використовують міжмережевий екран з інтегрованими засобами SD-WAN. Увімкнення цього сервісу дозволяє керувати віддаленими з'єднаннями VPN, а також здатне динамічно застосовувати відповідні28 рівні аналізу та захисту трафіку, забезпечує високий рівень контролю за даними та додатками, що проходять через середовище SD-WAN.

Основними вимогами до SD-WAN є:

- автоматична адаптація до змін у конфігурації та якості каналів доступу;
- розпізнавання широкого спектра додатків;
- централізоване управління та моніторинг додатків;
- можливість автоматичного розгортання;
- моніторинг фізичних та логічних мережевих топологій, завантаженості каналів та поведінки мережевих пристроїв та додатків.

До провайдерів та операторів пред'являються, у свою чергу, наступні вимоги:

- прикордонні пристрої повинні виконувати всю найбільшу інтелектуальну роботу із забезпечення безпеки та гнучкості мережі;
- користувачі та сервери повинні переміщатися з одного сегмента мережі в інший для створення віртуалізації в рамках хмарних обчислень та мобільних технологій.

Розробка та впровадження нових методів та алгоритмів управління та ідентифікації трафіку та додатків необхідні для виконання згаданих вище вимог та можуть бути оцінені через показники ефективності використання обчислювальних мереж.

Таким чином, при сучасному розвитку технологій побудови телекомунікаційних мереж залишаються невирішеними повною мірою завдання ефективного використання мережевих ресурсів та запобігання перевантаженням у корпоративних мереж. Ці завдання продовжують бути актуальними незважаючи на постійне збільшення мережевих ресурсів та можливостей. З'являються нові методи вирішення зазначених завдань, проте вони пред'являють додаткові вимоги до телекомунікаційних мереж та системи управління. З урахуванням цього продовжує бути актуальним завдання розробки нових методів проектування, експлуатації та управління корпоративними мережами. Методи, що розробляються повинні бути, по можливості, універсальними та швидкодіючими.

2 МЕТОД МОНІТОРИНГУ ТРАФІКА КОРПОРАТИВНОЇ МЕРЕЖІ

2.1 Завдання моніторингу та ідентифікації трафіка в корпоративній мережі

З результатів розгляду актуальних завдань у галузі управління корпоративними телекомунікаційними мережами з пакетною комутацією слід, що у них можна назвати два аспекти: управління мережевим обладнанням та інфраструктурою та управління мережним навантаженням (корпоративним контентом та трафіком). Аспект управління мережним навантаженням тісно пов'язаний з вирішенням завдань ідентифікації, класифікації та кластеризації трафіку різного виду.

Значне місце ідентифікація разом із класифікацією займають у сучасних системах моніторингу та управління. У задачах автоматичного виявлення мережевих пристроїв та визначення відносин між ними необхідно звертатися до ідентифікації та класифікації для побудови образів (моделей) мережевих пристроїв у різних режимах функціонування, Використовуючи профіль мережевого трафіку. При моніторингу трафіку у процесі експлуатації мережі можна класифікувати стан мережних пристроїв визначати відносини з-поміж них. Автоматична реакція на подію неможлива без своєчасного виявлення події щодо того, що відбувається змін у мережі, їх ідентифікації та класифікації. Як випливає з викладеного вище, завдання ідентифікації та моделювання трафіку формулюються ще на етапі формування спільних завдань проектування телекомунікаційних мереж та систем управління. Але й у процесі функціонування під впливом різних сучасних факторів вирішення задач ідентифікації, моделювання та класифікації трафіку виявляється затребуваним.

У рамках запровадження спеціалізованих рішень оптимізації каналів зв'язку та роботи додатків виникає конкуренція між провайдером та

замовником: хто перший встановить на своєму боці ці рішення, той і отримає додаткові конкурентні переваги. Інша сторона знаходить свої методи оптимізації телекомунікаційної інфраструктури Подібна ситуація веде до появи у магістральних телекомунікаційних мережах різноманітного трафіку, що погано піддається аналізу та адмініструванню, що згодом негативно впливає управління корпоративним контентом. Розробка способів ідентифікації такого трафіку підвищує ефективність керування мережею.

В умовах сучасного розвитку техніки програмні засоби, що забезпечують шифрування вихідного трафіку, маскування навантаження, що використовують нестандартні мережеві протоколи та порти, знаходяться у вільному (неліцензійному) зверненні, прості в установці та адмініструванні. Це призводить до того, що не тільки державні структури (міністерства, великі державні корпорації), а й приватні компанії застосовують у своїх мережах шифрування та інші засоби безпеки зв'язку. Такі протоколи як IPSec і SSL, фактично, стали стандартами через свою поширеність.

Перелічені фактори ведуть до ускладнення управління комунікаційним обладнанням за рахунок того, що практично відсутні ознаки диференціації навантаження абонентів у мережі, стає невизначеним числом працюючих абонентів, неможливе прогнозування. Необхідно постійно створювати нові статистичні моделі мережевих процесів. Тому рішення завдання ідентифікації телекомунікаційної мережі знаходять своє місце у управління шифрованим трафіком.

В актуальних завданнях забезпечення інформаційної безпеки необхідність ідентифікації трафіку обчислювальних мереж виникає при вирішенні наступних завдань [8]:

- імітації етапу збору інформації про мережу при формуванні комплексної моделі порушника;

- виявлення безлічі спостережуваних з боку транспортної мережі параметрів, які потенційно можуть бути використані для подолання системи захисту;

- ідентифікації мережі порушника для ефективної протидії атакам;
- збору відомостей про порушника під час розслідування комп'ютерних злочинів.

Ідентифікація та моделювання трафіку корпоративних телекомунікаційних мереж знаходять своє місце у сучасних методах вирішення завдань проектування, експлуатації та управління корпоративними мережами. У технології ТЕ під час оперативного управління параметрами для вибору шляхів проходження трафіку моделюється його поведінка та відстежуються зміни параметрів. З метою забезпечення заданої якості обслуговування різних класів трафіку ідентифікація та класифікація необхідні для групування пакетів у поведінкові агрегати із заданим набором Показників поведінки. З появою такого параметра доставки, як обмеження можливостей, виникла потреба у розширенні класифікації трафіку відповідно до вимог обслуговування.

Ідентифікація необхідна при керуванні трафіком, не віднесеним до одному класу. Повною мірою результати ідентифікації застосовуються до моделі процесу організації трафіку згідно з RFC 2475. За відсутності даних мережевих вимірювань використовується теоретична модель, отримана за допомогою ідентифікації та математичного моделювання характеристик трафіку.

У процесі проведення аналізу мережі використовуються теоретичні моделі. розподілу трафіку по мережах, моделі навантажувальних характеристик, здійснюється ідентифікація мережевих "патологій". Розробка моделей поведінки джерел трафіку, що узгоджуються з емпіричними даними з працюючої мережі, є основою організації трафіку мереж різного рівня. Ці моделі джерел мають бути гнучкими та придатними для аналізу щодо різних мережевих процесів. Методи ідентифікації знаходять своє застосування при оптимізації продуктивності мережі з метою оцінки її якості.

Питання ідентифікації та моделювання трафіку корпоративних телекомунікаційних мереж з пакетною комутацією ставляться як на етапі

постановки завдань проектування мереж, а також у вже розроблених методах і способи управління мережами передачі. Зі збільшенням вимог до сучасним телекомунікаційним мережам і зростаючим різноманіттям мережевих процесів завдання ідентифікації, моделювання та класифікації трафіку перестають бути допоміжними. Результат їх вирішення визначає ефективність застосування методів керування мережею. Окремі класи завдань будуються на успішності вирішення задач моделювання та ідентифікації мережевого трафіку.

Під завданням ідентифікації розуміється завдання побудови математичної моделі динамічних систем за даними спостережень за їх поведінкою. Під системою, своєю чергою, розуміється об'єкт, у якому відбувається взаємодія між різнотипними змінними та формуються спостерігаються сигнали. Сигнали, що цікавлять, називають вихідними сигналами.

Усі інші сигнали називають обуреннями, які можуть бути розбиті на два класи: вимірювані безпосередньо та доступні лише непрямої оцінки за впливом, що надається ними на вихідний сигнал [9]. У такому формулюванні завдання ідентифікації може бути застосоване до трафіку корпоративних мереж. Як динамічна система (об'єкт), в даному випадку, виступає корпоративна телекомунікаційна мережа з пакетною комутацією.

Практично всі актуальні завдання проектування, експлуатації та управління корпоративними телекомунікаційними мережами вирішуються на стороні оператора чи провайдера, що надає послуги зв'язку. Повсюдне застосування VPN при активному впровадженні технології MPLS ускладнює або унеможливлює спостереження процесу формування множини Y з множини X. Часто безліч X недоступне для спостереження, і щодо оцінок його елементів діють лише апріорні припущення. Таким чином, завдання ідентифікації вирішується в умовах апріорної невизначеності щодо вхідного сигналу:

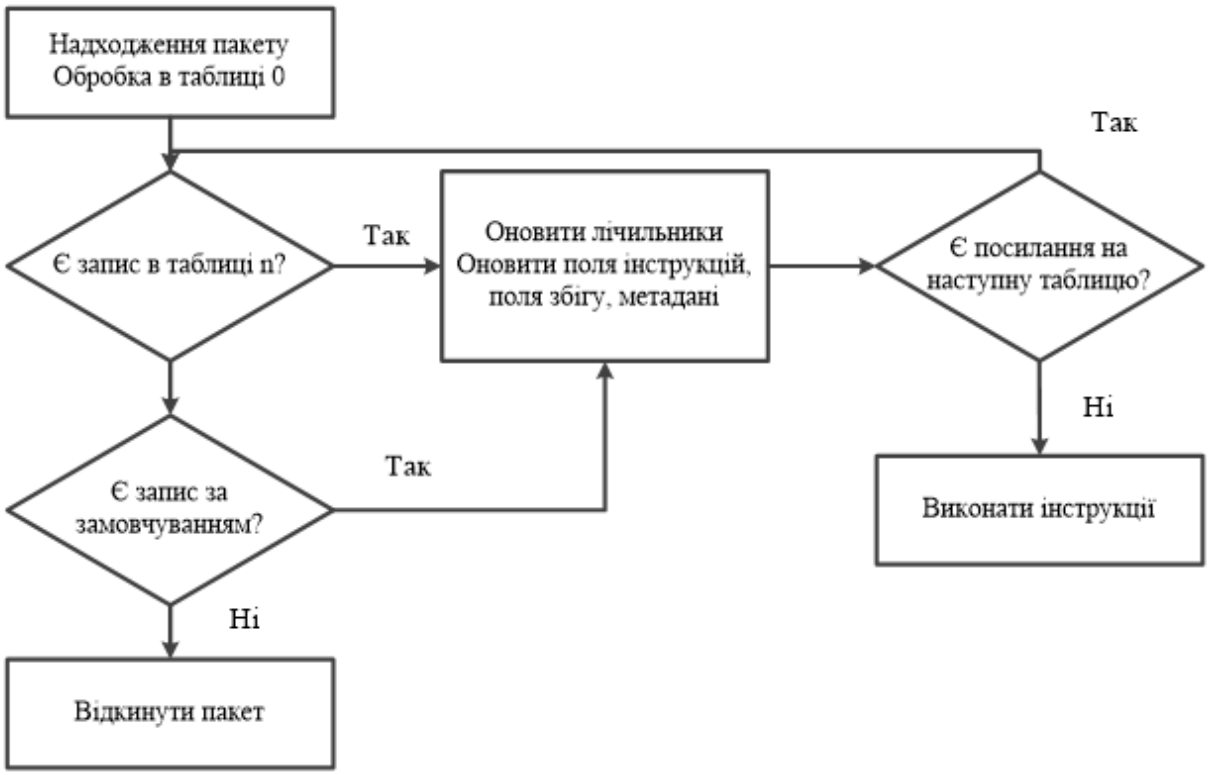

Рисунок 2.1 – Спрощена схема обробки потоків

На рисунку функція, що перетворює вхідні сигнали та впливу у вихідний сигнал, що спостерігається. Під керуванням функціонуванням корпоративної телекомунікаційної мережі розуміється вироблення реакції на певні вхідні дії з метою виконання вимог до якості та безпеки передачі даних. Ця реакція є собою керуючий вплив $B(t)$. $B(t)$ формується відповідно до вимогами до функціонування мережі при вступі на вхід множини елементів $X' = \{x_k(t) \in X\}$, $k = 1,2, \dots, n$ протягом певного часу у певній послідовності. Керуюча дія $B(t)$ застосовується до вихідної множини $Y' = \{y_l(t) \in Y\}$, $l = 1,2, \dots, m$. Функція $A(t)$ ставить у відповідність сигналу $X' \in X$ його образ $Y' \in Y$: $Y' = A(t)X'$.

Таким чином, кожен елемент $y(t) \in Y$ є однозначним відображенням елемента $x(t) \in X$. Вирішенням задачі ідентифікації мережі є побудова оцінки $A*(t)$ функції $A(t)$ за спостережуваною послідовністю сигналів $y_1(t)$, $y_2(t)$, … , $y_l(t)$, що належать безлічі Y. Із застосуванням $A*(t)$ визначається оцінка

вихідного сигналу $Y* = A*(t)X$. На рисунку 2.2 представлена структурна схема ідентифікації телекомунікаційної мережі

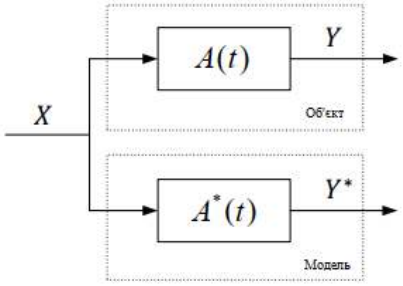

Рисунок 2.2 – Структурна схема ідентифікації телекомунікаційної мережі

При даному поданні схеми ідентифікації модель ставиться в відповідність об'єкту на підставі близькості спостережень $y(t) \in Y$ та $y*(t) \in Y*$. Це єдина вимога, що пред'являється до $A*(t)$ з позиції спостереження за функціонуванням мережі передачі. Дотримання вимог до мінімального значенню різниці відповідних елементів $y(t)$ та $y*(t)$ достатньо для вирішення завдань із проектування корпоративних телекомунікаційних мереж та прогнозування їх роботи.

Однак для здійснення поточного управління необхідно пред'явити до функції $A*(t)$ додаткову вимогу. Це вимога полягає в тому, щоб $A*(t)$ мала можливість розбивати безліч $Y*$ на m непересічних класів $Y1*$, $Y2*$, … , $Ym*$. Розбиття має здійснюватися відповідно до розбиття безлічі X на m класів $X1$, $X2$, … , Xm, які становлять інтерес для завдань управління мережею. При38 відсутності апріорних відомостей про вхідний сигнал $x(t) \in X$ відсутня інформація про поточний клас k ($k \in \{1,2, \dots , m\}$) множини X. Фактично оцінка вихідного сигналу визначається як $y*(t) = A*(t)$.

Побудова моделі сигналу, що розповсюджується в часі $y(t) \in Y$, що представляє собою трафік, фактично вирішує завдання ідентифікації. При цьому модель, що розробляється повинна мати параметри, за різними значеннями яких можна було б судити про зміну сигналу $x(t) \in X$.

Моделюється поведінка об'єкта, і ця модель підміняє завдання ідентифікації модель об'єкта. При управлінні функціонуванням корпоративної телекомунікаційної мережі буде використовуватися модель трафіку, що спостерігається.

Завдання ідентифікації трафіку під час здійснення управління функціонуванням корпоративної телекомунікаційної мережі з пакетною комутацією формулюється наступним чином: за трафіку, що спостерігається $y(t) \in Y$, отриманому в результаті апріорно невідомого перетворення $A(t)$ вхідного абонентського трафіку $x(t)$ з безлічі X, в загальному випадку, також невідомого, побудувати модель $A*(t)$, що описує $y*(t) \in Y*$ як максимально наближений до $y(t) \in Y$ образ невідомої спостерігачеві реалізації $x(t) \in X$. Оскільки ідентифікація трафіку, виходячи з постановки задачі, відбувається за результатам спостереження, необхідно включити опис наступних компонентів: даних спостережень, безлічі моделей та правил оцінки ступеня відповідності моделі даним спостережень [9].

Рисунок 2.3 – Метод моніторингу та ідентифікації трафіка

Оскільки невідомі параметри $x(t)$ та $A(t)$, що беруть участь у формуванні $y(t)$, то впливати на хід проведення ідентифікаційного

експерименту неможливо. Завдання ідентифікації ставиться даних нормальної експлуатації. Виходячи з постановки завдання, загальну схему ідентифікації трафіку представлено на рисунку 2.3

Подана схема ідентифікації слідує природній логіці дій:

- зібрати дані;
- вибрати безліч моделей;
- вибрати найкращу модель.

Слід зазначити, що стосовно завдання ідентифікації трафіку корпоративної телекомунікаційної мережі під гіпотетичною множиною реалізацій вхідного трафіку X розуміється як безліч застосовуваних видів та протоколів передачі інформації та режимів роботи, так і безліч типів поведінки трафіку телекомунікаційних мереж, що групуються у класи. Спостерігаються параметри (структурні та статистичні) формують простір спостережень Y.

Існує описана послідовність кроків розв'язання задачі ідентифікації:

- визначити безліч X, виходячи з цілей розв'язання задачі ідентифікації;
- вибрати модель та супутні параметри;
- вибрати критерій близькості об'єкта та моделі; – сформулювати алгоритм ідентифікації.

Ця послідовність етапів застосовна повною мірою до завдання ідентифікації трафіку корпоративної телекомунікаційної мережі У подальшому описі розв'язання задачі ідентифікації трафіку буде використовуватися позначення моделі $A(t)$ замість $A*(t)$ як еквівалентне.

2.2 Існуючі методи моніторингу та ідентифікації трафіка

Серед існуючих методів ідентифікації трафіку та подальшої його класифікації широко поширені такі методи: простий байєсовський класифікації; метод подання трафіку нестаціонарним пуассонівським

процесом; на основі процесів із модуляцією; на основі детермінованих процесів; на підставі флюїдного потоку (Fluid Flow); на основі структурних аспектів моделі; методи, що базуються на тимчасових рядах; на основі фільтра Калмана; на основі нейронних мереж та самонавчальних систем; на основі фракталів та ефекту правдоподібності; на основі марківських та прихованих марківських процесів. Ці методи широко висвітлені у літературі [10 - 13].

Байєсовський метод. Через відносно високий рівень оптимізації байєсовський метод дозволяє створювати дуже точні моделі потоку трафіку, доки джерело істотно не змінить свої характеристики, і є потужним інструментом для опису нелінійного або пачечного трафіку. Недоліком методу Байєса є те, що оцінки зазвичай, високо «настроювані» та оптимізовані для деякого джерела трафіку та не вносять велику стійкість рішення.

Методи з урахуванням фільтра Калмана. Проблемою у використанні фільтра Калмана є вибір методу моделювання нестаціонарної та нелінійної системний динамік. Недоліком цього методу є нестача стійкості фільтрів Калмана.

Нейронні мережі та самонавчальні системи. Алгоритми пристосовані до адаптивним моделям з високою нелінійністю процесів при мінімумі апріорних припущень. Мають переваги: стійкість до шумів та здатність до самонавчання. Однак, при пакетному трафіку ігноруються питання, що стосуються фізичної основи. В результаті складні моделі трафіку вимагають великої кількості параметрів, але забезпечують мале проникнення в динаміку трафіку, який спостерігається на реальних мережах.

Методи, що ґрунтуються на детермінованих процесах. мають переваги в плані точності класифікації, проте слабо адаптуються під динамічну систему телекомунікаційної мережі, що швидко змінюється.

Методи на основі процесів із модуляцією. Найпопулярнішим із цих методів є метод на основі пуассонівського процесу, що модулюється

марківським (MMPP). Цей процес заснований на тимчасових лавах і має негативний експоненційний розподіл часу перебування в стані. Модель найчастіше застосовується для пакетизованого трафіку. Однак моделі MMPP мають на увазі незалежність джерел і не враховують періодичності у структурі трафіку, яка є при передачі відеопотоків та деяких потоків даних. Таким чином, представлені методи мають місце при вирішенні задачі ідентифікації, проте мають недоліки.

Ключовим моментом є адекватна модель, що лежить в основі алгоритму та методу, тому необхідно зосередитись на створенні нової моделі ідентифікації трафіку корпоративної телекомунікаційної мережі із пакетною комутацією.

2.3 Уявлення трафіка як математичної моделі

Предмет дослідження передбачає детальний опис моделі трафіку корпоративної телекомунікаційної мережі з пакетною комутацією, а також алгоритми та методи ідентифікації, що ґрунтуються на цій моделі. Визначення трафіку представлено у [14].

Мережевий трафік (англ. Traffic - "рух", "вантажообіг") - обсяг інформації, що передається через комп'ютерну мережу за певний період. Кількість трафіку вимірюється як у пакетах, так і в бітах, байтах та їх похідних: кілобайт (Кб), мегабайт (Мб) тощо. Спосіб вимірювання трафіку застосовується залежно від задач, котрим вимір проводиться. Наприклад, з погляду проектування пропускної спроможності мережі оперують бітами, байтами тощо. У разі дослідження питань, пов'язаних з управлінням потоками та маршрутизацією зручно розглядати трафік на рівні пакетів, оскільки вони несуть дані, необхідні розробки керуючого впливу. В даний час не існує єдиного підходу до мережевого опису трафіку.

Опис формується під конкретне завдання. Структурним підходом до цього питання має робота [15]. Трафік у ній описується виходячи з

характеристик якості обслуговування мережі: прозорості, доступності та надається пропускну здатність. Прозорість характеризує тимчасову і семантичну цілісність даних, що передаються. Доступність характеризується ймовірністю відмови у доступі та затримці для повторного підключення у разі блокування. Пропускна здатність, що надається повинна задовольняти запити користувачів щодо якісної передачі даних та комфортну роботу в мережі. Представлені характеристики якості обслуговування застосовні до будь-якої телекомунікаційної мережі. Такий підхід45 задовольняє цілі дослідження, що полягає у підвищенні ефективності функціонування телекомунікаційної мережі із пакетною комутацією. У роботі [15] визначено види мережевого трафіку: безперервний, еластичний та трафікові об'єднання.

Об'єкти безперервного трафіку - це потоки, мають характерну тривалість і швидкість, чия тимчасова цілісність повинна зберігатись мережею (телефонні, інтерактивні відеосервіси тощо). До еластичного трафіку належать цифрові об'єкти або «документи», які повинні бути передані з одного місця до іншого (файли даних, тексти, картинки і т.д.). Два описані види трафіку повно характеризують трафік, що породжується множиною мережевих протоколів, виходячи з мережевої діяльності користувачів.

Третій поданий у роботі [15] вид трафіку - трафікові об'єднання. Він виникає, коли окремі потоки та повідомлення групуються разом у об'єднаний трафіковий потік. Фактично, трафікове об'єднання складається з об'єктів безперервного та еластичного трафіку. Мережеве управління цим видом трафіку найбільш складно через велику мінливість. В силу цього сучасні засоби управління мережевими ресурсами не розглядають трафіку як окремий об'єкт управління.

Сучасна концепція управління телекомунікаційною мережею вимагає, щоб окремі безперервні та еластичні потоки відрізнялися з цілями управління доступом та маршрутизації. Зазначені вище характеристики якості застосовуються для окремого потоку, а чи не для всієї сукупності. Однак на

спостерігається в сучасних телекомунікаційних мережах трафік впливають чинники, наведені у розділі 1.

У разі приховування адресної частини, маскування під роботу інших протоколів, появи великого кількості нерегламентованих протоколів стерті межі між видами трафіку при його аналізі на мережному рівні. Тому найперспективнішим виглядає опис для подальшого моделювання саме трафікового об'єднання як універсального об'єкта управління мережею.

Опис формується на основі спостереження за трафіком шляхом отримання значень параметрів, що спостерігаються, протягом часу спостереження. Число вимірюваних параметрів залежить від рівня, на якому розглядається реалізація: фізичний, мережевий, транспортний, рівень застосування. Для досягнення цілей роботи, визначених у главі 1, пропонується розглянути параметри, що отримуються на мережному та транспортному рівнях. Опис трафіку здійснюється на пакетному рівні. Даний підхід обумовлений апріорною невизначеністю щодо адресних, структурних та семантичних ознак класифікації даних, що передаються, а також застосовуваних протоколів передачі даних та мережних додатків, що їх використовують.

На основі наведеного опису необхідно розробити модель трафіку корпоративної мережі з пакетною комутацією. Модель має бути орієнтована вирішення завдання ідентифікації.. Зокрема, необхідно визначити безліч моделей, придатних для ідентифікації та виконати збір даних на основі параметрів трафіку. Для застосування моделі на практиці розрахунки для складання моделі не повинні мати велику обчислювальну складність. При розв'язанні задачі ідентифікації переважно слід розглядати математичні моделі, де всі залежності виражаються функціонально.

Оскільки розв'язання задачі ідентифікації зводиться до побудови оцінки відповідності моделі спостережуваному об'єкту, то при складанні математичної моделі трафіку48 корпоративної обчислювальної мережі з пакетною комутацією має бути використано математичний апарат теорії

ймовірностей [26]. Якість результату виконання етапів побудови та розрахунку моделі, що лежать в основі схеми ідентифікації системи (див. рисунок 2.2), визначає якість розв'язання задачі ідентифікації та залежить від коректного розбиття на етапи з відповідною постановкою завдання для кожного з них. Пропоновані етапи постановки завдань на побудову математичної моделі представлені на рисунку 2.3.

Згідно зі схемою (див. малюнок 2.1) на першому етапі проводиться змістовна постановка задачі. Обстеження об'єкта моделювання (обробка пакетів) та формування поточних даних для розрахунку моделі проведено у параграфі 2.1.

Виходячи з проведеного обстеження об'єкта та поставлених цілей завдання на розробку моделі формулюється так: розробити математичну модель трафіку корпоративної телекомунікаційної мережі з пакетною комутацією, що дозволяє проводити ідентифікацію в умовах апріорної невизначеності щодо адресної та структурної інформації.

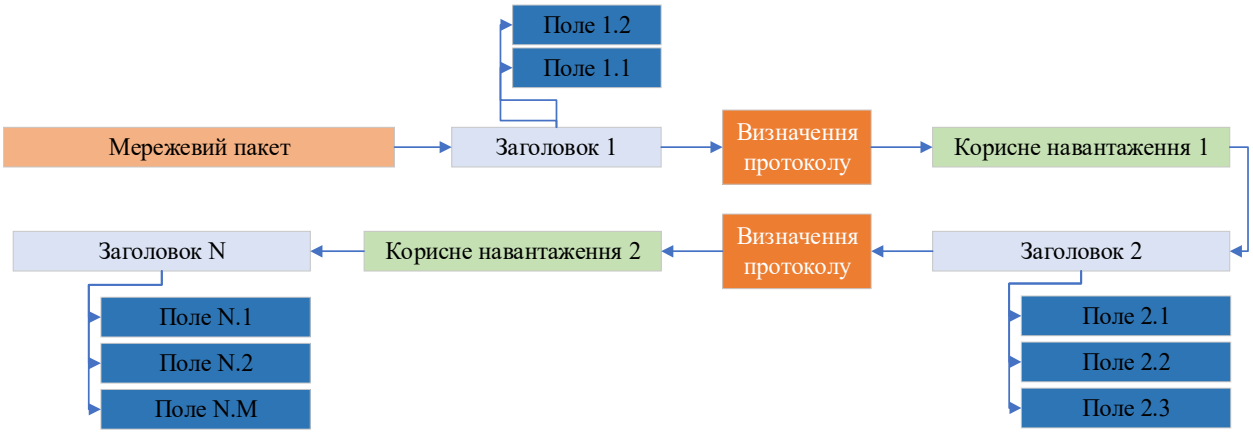

Рисунок 2.4 – Етапи виділення і розбору заголовків протоколів в пакеті

Умова апріорної невизначеності щодо адресної інформації свідчить про те, що послідовності довжин пакетів $\{l\}$ і інтервалів між пакетами $\{\tau\}$ розглядаються як послідовності однорідних спостережень.

Умова апріорної невизначеності относительно49 структурної

інформації свідчить про те, що внутрішня структура мережі що породжує трафік, невідома, тобто невідома кількість мережевих процесів і кількість користувачів мережі, що беруть участь у формуванні інформаційних потоків. Проте визначення телекомунікаційної мережі як корпоративної дозволяє встановити максимальну кількість абонентів.

Для застосування отриманої моделі завдання ідентифікації необхідно, щоб на основі параметрів функції, що змінюються в часі, $q(\omega)$ було можливе отримання функції $A(t)$. Фактично, після визначення та розрахунку моделі трафіку подальше вирішення задачі ідентифікації зводиться до отримання індикаторної функції $g(\omega)$: $\Omega \rightarrow \mathcal{M}$, $\mathcal{M} = \{1, \dots, m\}$ та класифікації множини Y для вироблення керуючого впливу $B(t)$. Якість класифікація Y залежить від якості моделі. Отже, критерієм коректності моделі служить близькість спостережень $y(t) \in Y$ та $y*(t) \in Y*$ з урахуванням точності визначення меж спостереження класів 1,2, …, m.

Для розрахунку моделі суттєвим є аналіз існуючих моделей трафіку з метою визначення безлічі моделей, які застосовуються для вирішення завдання ідентифікації трафіку

2.4 Моделі трафіка

Дослідження щодо моделювання трафіку ведуться давно, про що свідчить велика кількість публікацій [15,17]. Найбільш структурований огляд моделей та способів моделювання представлений у [15]. В даний час моделі трафіку видаються у вигляді двох великих класів: традиційні та фрактальні. Існуючі моделі трафіку мереж із пакетною комутацією представлені на рисунку 2.4.

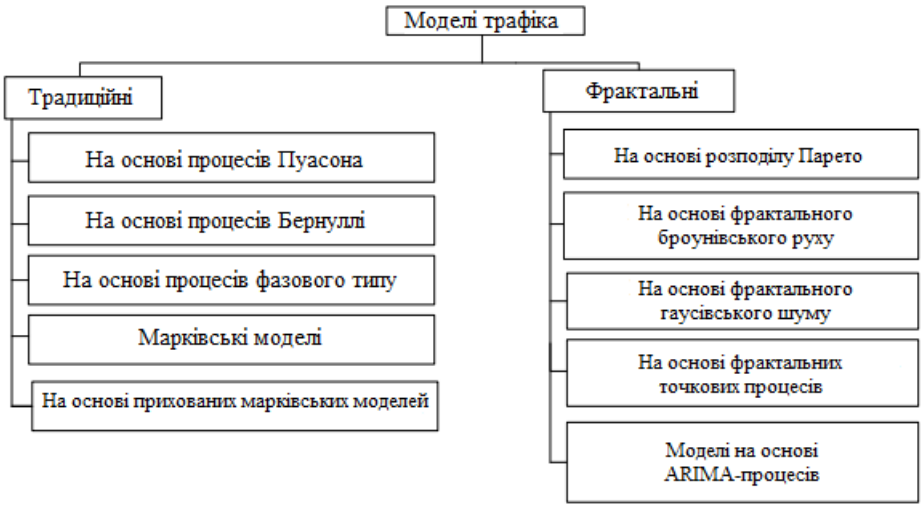

Рисунок 2.5 – Існуючі моделі трафіку мереж із пакетною комутацією

До традиційних моделей, насамперед, належать так звані відновлювальні моделі трафіку [15]. Ці моделі називають моделями відновлення. Відмінністю даних моделей є те, що величини τn є незалежними та однаково розподіленими. Подібним чином описують трафік моделі на основі процесів Пуассона, на основі процесів Бернуллі на основі процесів фазового типу.

Перевагами використання пуасонівських моделей є те, що при накладенні незалежних пуасонівських процесів виходить новий пуасонівський процес, інтенсивність якого дорівнює сумі інтенсивностей складових його процесів. Процеси Пуассона не мають пам'яті, що спрощує процес побудови на них черг обслуговування трафікових надходжень. Застосування пуасонівських моделей розширюється шляхом введення Залежно від часу параметра інтенсивності λ. Моделі з урахуванням процесів Бернуллі. Процеси Бернуллі – це дискретний у часі аналог пуассонівських процесів. Тут ймовірність надходжень у будь-якому тимчасовому слоті p не залежить від будь-якого іншого надходження.

Моделі з урахуванням процесів фазового типу. У цьому типі моделей інтервали між надходженнями пакетів $\{\tau n\}$ описуються процесом

поглинання у безперервному марківському процесі $C = (C(t))t$ ∞=0 з простором станів {0,1, …, m} [15]. Основною перевагою використання моделей на основі процесів фазового типу є те, що будь-який розподіл {τn} може бути як завгодно близько апроксимовано процесами фазового типу.53 Однак усі перелічені моделі, незважаючи на простоту опису, мають істотний недолік, що обмежує їхнє застосування.

Моделі не враховують пульсуючий характер трафіку, доведений у роботі [15]. Кореляційна функція процесу {τn} перетворюється на нуль однаково всім ненульових затримок. В силу зазначених причин поновлювальні моделі не застосовуються для моделювання трафіку в широкосмугових мережах, оскільки це призведе до значного погіршення характеристик мережі.

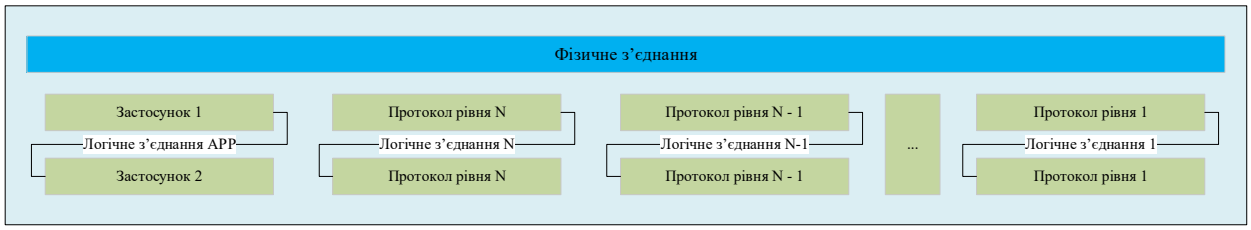

Рисунок 2.6 – Модель мережної взаємодії між двома застосунками

Незважаючи на це клас відновлюваних моделей може застосовуватися для проектування мережевих пристроїв, у яких облік кореляцій перестав бути критичним. Наступним класом традиційних моделей трафіку є марківські моделі та моделі на основі прихованих марківських моделей. Математичний апарат цих моделей повною мірою досліджено [10, 11, 12, 30]. В основі марківських моделей лежить властивість, яка говорить про те, що майбутнє стан залежить від поточного та не залежить від попередніх станів або часу, проведеного у поточному стані. Внаслідок цього, час, проведене у певному стані, описується геометричним або експоненційним розподілом.

3 ПРОГРАМНА РЕАЛІЗАЦІЯ МЕТОДІВ МОНІТОРИНГУ ТА ІДЕНТИФІКАЦІЇ ТРАФІКА

3.1 Завдання якісності ідентифікації трафіка

Для якісної ідентифікації трафіку мереж із пакетною комутацією необхідно визначити приватні завдання, які потрібно розв'язати. Ідентифікація передбачає вибір моделі об'єкта спостереження, її параметрів з подальшою їх оцінкою на основі статистичних даних, отриманих у результаті спостереження чи експерименту. Розв'язання цих завдань описано в попередні параграфи. Проте застосування результату ідентифікації трафіку у функціональних групах завдань управління вимагає виконання наступних дій:

- однозначне визначення об'єкта;
- розпізнавання об'єктів за їх властивостями;
- групування об'єктів за певними ознаками;
- виділення об'єкта з багатьох подібних.

Список завдань може бути конкретизовано або розширено в залежності від цілей ідентифікації. Але незалежно від цього, порядок вирішення завдання ідентифікації наступний:

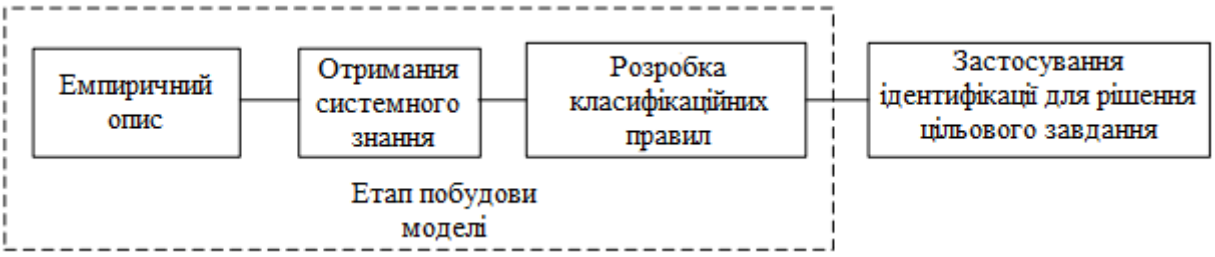

Рисунок 3.1 – Порядок рішення завдання ідентифікації

Перші три етапи проводяться для розробки моделі та вивчення її властивостей та об'єднуються у загальний етап побудови моделі. Фактично на цьому етапі та вирішується завдання ідентифікації..

На початковому етапі завжди відбувається емпіричне опис об'єкта ідентифікації, що супроводжується збиранням параметрів спостережуваного процесу, породженого об'єктом. На цьому етапі не використовується апріорна інформація про можливий об'єкт спостереження. Далі вся зібрана інформація використовується для отримання системного знання про ідентифікований об'єкт. На даному етапі відбувається обробка отриманих в результаті емпіричного опису параметрів із встановленням закономірностей, яким вони підкоряються. Особливістю перших двох етапів є те, що модель має бути пристосована до розробки класифікаційних правил Розробка класифікаційних правил має на меті свою мету однозначне визначення об'єкта як спостережуваного образу деякої одержаної на попередніх етапах моделі.

Розробка класифікаційних правил є наслідком вирішення підзавдань розпізнавання об'єктів щодо їх властивостями та групування об'єктів за певними ознаками.

На цьому етапі досліджується безліч об'єктів $X = \{x1, x2, \dots, xn\}$, кожен об'єкт характеризується набором змінних $Xj = \{a1, a2, \dots, am, y\}$. Змінні ai спостерігаються, їх значення відомі, y – залежна змінна, значення якої потрібно визначити. Змінна y визначає ознаку поділу об'єктів ідентифікації. Багато практичних завдань у галузі ідентифікації та розпізнавання образів обмежуються класифікацією з урахуванням розроблених правил. Однак для вирішення багатьох цільових завдань у галузі управління корпоративними мережами передачі даних недостатньо класифікувати трафік.

Як правило, у умовах апріорної невизначеності щодо часу появи та порядку проходження об'єктів, що класифікуються, виникає необхідність в попередній обробці даних для наступних кластеризації, класифікації та

прийняття рішень. Попередня обробка трафіку з подальшим використанням результатів, отриманих на етапі побудови моделі, що становить сутність етапу застосування ідентифікації для вирішення цільового завдання. З алгоритмічної точки зору класифікація – це функція $f: X \to C$, яка кожному об'єкту $xi \in X$ ставить у відповідність мітку $cj \in C$, де C – безліч значень змінної y.

В умовах зазначеної апріорної невизначеності необхідно вирішувати завдання кластеризації. Попередня обробка полягає у застосуванні методів виділення об'єкта з множини. Відповідно, алгоритми та методи ідентифікації трафіку корпоративної телекомунікаційної мережі з пакетною комутацією повинні містити в собі способи локалізації об'єктів, що ідентифікуються. Поставивши завдання локалізації об'єктів, необхідно доповнити алгоритм ідентифікації методами, що дозволяють виділити безліч C, що належить одному об'єкту. Таким чином, для вирішення задачі ідентифікації, поставленої в розділі 1 необхідно вирішити завдання локалізації об'єктів, що ідентифікуються.

Під час вирішення завдання ідентифікації трафіку мереж передачі даних локалізацією є процес виділення об'єктів, що являють собою певний мережевий процес.

Передача даних, що супроводжують різні мережеві процеси, розглядається як послідовність динамічно змінюваних у часі об'єктів. Для таких об'єктів необхідно визначати структуру та параметри за даними, що спостерігаються, тобто провести структурний аналіз. Сутність структурного аналізу мережного трафіку полягає в розробці схеми, що дозволяє локалізувати різні мережеві процеси, що породжують трафік, і в залежності від результатів ідентифікації зробити їх класифікацію чи кластеризацію. Таким чином, в залежності від цільової Завдання локалізація мережевого процесу може передувати процес ідентифікації, так і здійснюватись після нього, як представлено на рисунку 3.1.

Якщо розглядати процес передачі телекомунікаційного трафіку в

сучасних мереж передачі даних з пакетною комутацією на третьому рівні семирівневої моделі функціонування відкритих систем OSI-ISO послідовність пакетів трафіку є реалізація групового сигналу $s\sum$, утвореного роздільною системою ущільнення, у разі тимчасового. Однак частина загального ресурсу часу, виділеного мережному процесу, фіксована. Мультиплексування є статистичним(рисунок 3.2).

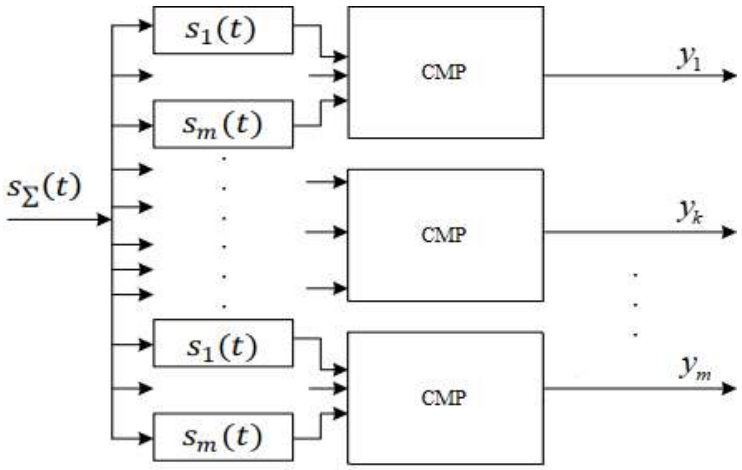

Рисунок 3.2 – Схема демульплексування

Узгоджені фільтри порівнюють m гіпотез про те, якому мережному процесу відповідає реалізація трафіку $s(t)1$, $s(t)2$, … , $s(t)N$. Потім пристрій порівняння індивідуальних реалізацій робить висновок про вірну гіпотезі та обирає рішення yi. Схема, представлена на рисунку 3.2, працює в у разі передачі трафіку кожного мережевого процесу протягом фіксованого інтервалу часу, тобто статичне часове мультиплексування. В разі передачі трафіку кожного мережевого процесу протягом довільного інтервалу часу вхідний трафік $s\sum(t)$ формується як реалізація статистичного мультиплексора. Подану на рисунку 3.2 схему необхідно доповнити. При реалізації поділу трафіку у разі статичного ущільнення функціонал, що розділяє повідомлення абонентів, відомий заздалегідь, у разі статистичного ущільнення є стохастичну величину. Схема поділу трафіку у разі

статистичного ущільнення представлено на рисунку 3.3.

3.2 Моніторинг трафіка мережі та ідентифікація мережевого вузла

Для ідентифікації мережевого вузла задається відповідний протокол і імена полів в його повідомленнях, в яких міститься адресна інформація. Для уніфікації опису використовується трійка (ProtoType, ValueType, Value), де прототипом - протокол, ValueType - тип розбору блоку, що описує «адресне» поле, Value - значення «адресного» поля.

Якщо для одних протоколів дані про мережеві вузлах містяться в заголовку безпосередньо у вигляді полів, то для інших є лише непрямі ознаки: незважаючи на те, що в HTTP-заголовку в явному вигляді відсутня поле, яке ідентифікує відправника (клієнт або сервер), можна зробити відповідний висновок, проаналізувавши вміст стартовою рядка. Для роботи з такими сценаріями Value може приймати зумовлені значення, відповідні мережевий ролі вузла: client, server, peer, unknown. При цьому значення поля ValueType буде порожнім.

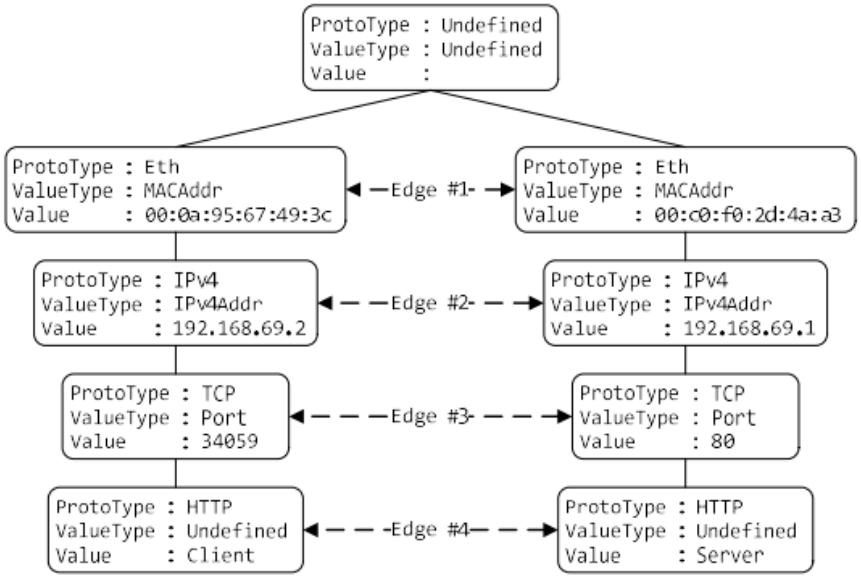

Рисунок 3.3 – NetworkTree

NetworkTree дозволяє розглядати мережевий обмін на різних рівнях, починаючи від канального і закінчуючи прикладним (відповідно до рівнів моделі OSI).

Була розроблена архітектура системи, що дозволяє обходитися єдиним комплектом вихідних кодів розбирачів протоколів, застосовуючи їх як в online-, так і в offline- режимі. Запропонована модель представлення даних реалізована у вигляді ядра системи, яке компілюється в динамічну бібліотеку. На базі API ядра побудована робота модулів розбору і розпізнавання даних. Було розроблено два інструменти - для проведення online- і offline-аналізу відповідно, - причому обидва використовують єдину інфраструктуру. Система є модульною, як і більшість аналізаторів мережевого трафіку: для кожного протоколу створюється окремий модуль, в якому локалізована функціональність по роботі з цим протоколом. Кожен з інструментів використовує свій комплект модулів розбору.

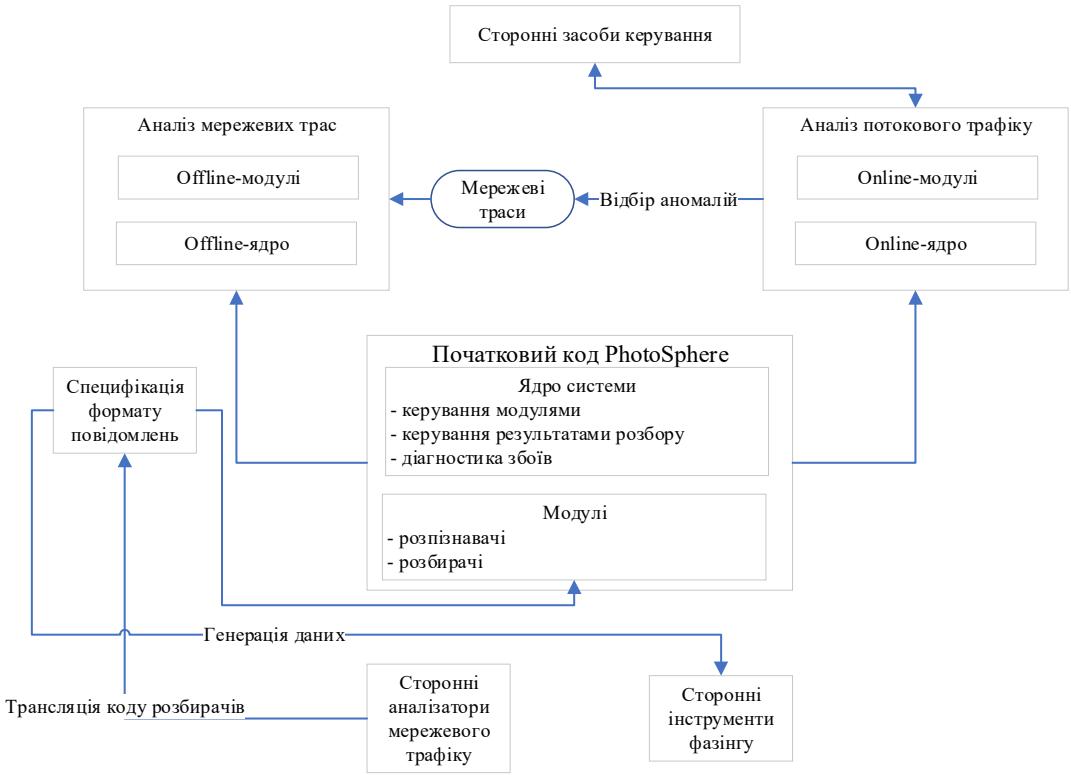

Рисунок 3.4 – Програмні засоби моніторингу мережі для ідентифікації трафіка. Схема взаємодії програмних модулів

API системи дозволяє аналітику реєструвати і розпізнавачі, створювати блоки-потоки, одиночні і складові фрагменти, управляти відновленням потоків. Зокрема, для коректного відновлення потоку з переупорядкуванням пакетів передбачена функція об'єднання двох блоків-потоків в один.

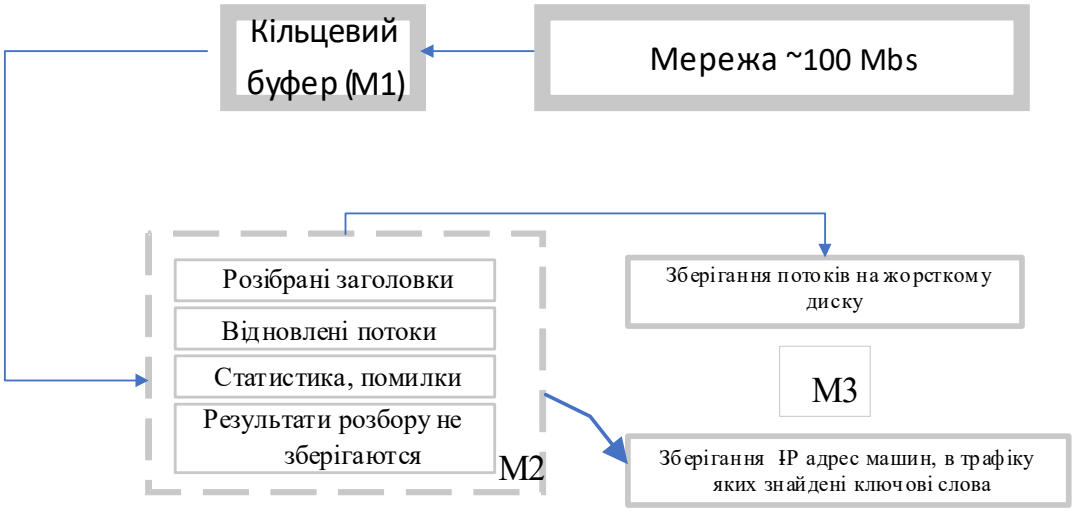

Рисунок 3.5 – API системи

Інструмент online-аналізу призначений для отримання даних з трафіку в режимі реального часу: він повинен працювати безперервно з продуктивністю, достатньою для розбору пакетів, що надходять на мережевий інтерфейс (потенційно нескінченний вхідний потік даних). Інструмент складається з трьох компонентів:

- модуль M1 здійснює взаємодію з мережевим інтерфейсом і зберігає вступники пакети в кільцевої буфер;

- модуль M2 виконує розбір пакетів кільцевого буфера і витягує необхідні дані;

- модуль M3 зберігає витягнуті дані в файли на жорсткому диску (формат файлу визначається модулем побудови).

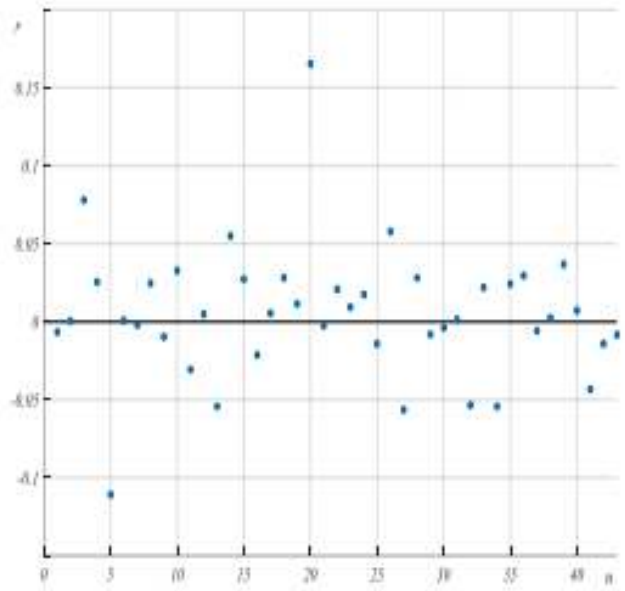

Рисунок 3.6 – Результати роботи

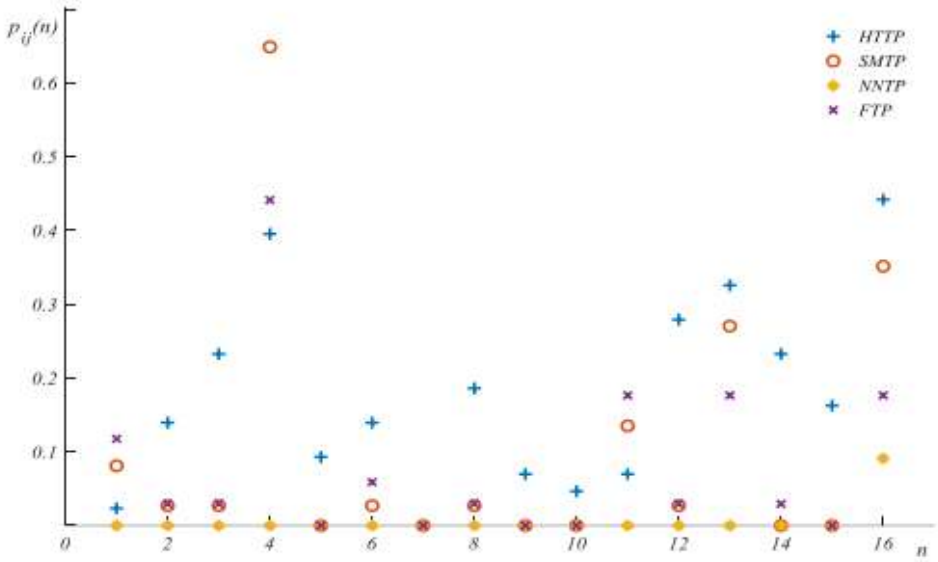

Рисунок 3.7 – Результати роботи

Гістограми значень ризику прийняття помилкового рішення R при побудові прихованої марківської моделі під час опису моделі трафіку корпоративної телекомунікаційної мережі з пакетною комутацією.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи проведено аналіз методів моніторингу трафіка, методів ідентифікації трафіка та удосконалення технологій передачі трафіка за рахунок підвищення якості кластеризації та класифікації трафіка. Проаналізовано стан сучасних корпоративних мереж із пакетною комутацією щодо застосовуваних методів ідентифікації та моделей трафіку, технологій та протоколів передачі інформації. Також проведено аналіз алгоритмів класифікації трафіку протоколів, що використовуються у корпоративних телекомунікаційних мережах. Запропонована архітектура програмних засобів поглибленого моніторингу мережевого трафіка, що дозволяє розробляти і налагоджувати модулі підтримки протоколів на попередньо збереженому трафіку і згодом використовувати ці модулі в реальному режимі часу. Розроблені та реалізовано програмні засоби для проведення моніторингу корпоративної мережі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. 2-е изд. СПб.: Питер, 2003. 864 с.

2. Ладыженский Г.М. Архитектура корпоративных информационных систем // Системы Управления Базами Данных. 1997. № 5-6. С. 18-24.

3. CCITT Recommendation X.700 (1992), Management framework for open systems interconnection (OSI) for CCITT applications. Сайт Международного союза электросвязи (МСЭ). 2022.

4. ГОСТ РИСО/МЭК 7498-4-99 Информационная технология (ИТ). Взаимосвязь открытых систем. Базовая эталонная модель. Часть 4. Основы административного управления. М.: ИПК Издательство стандартов, 1999. 16 с.

5. Леохин Ю.Л. Научные основы управления параметрами структур корпоративных сетей: Автореферат диссертации на соискание ученой степени доктора технических наук: 05.13.13. М., 2009. 36 с.

6. Леохин Ю.Л. Архитектура современных систем управления корпоративными сетями // Качество Инновации Образование. 2009. № 2. С. 54-63.

7. Виктор Олифер, Наталья Олифер. Искусство оптимизации трафика // Журнал сетевых решений/LAN. 2002. № 12. Сайт журнала сетевых решений. URL. https://www.osp.ru/lan/2002/12/135572 (дата обращения: 02.07.2021).

8. Бочков М.В., Копчак Я.М. Метод идентификации вычислительных сетей при ведении компьютерной разведки // Сб. докл. VI Междунар. конф. SCM'2003 СПб.: СПГЭТУ, 2003. т. 1. С. 288-290.

9. Льюнг Л. Идентификация систем. Теория для пользователя: Пер. с англ. / Под ред. Я.З. Цыпкина. М.: Наука. гл. ред. физ.-мат. лит., 1991. 432 с.

10. Zucchini, W. and MacDonald, I. L. Hidden Markov Models for Time

Series: An Introduction using R. Chapman & Hall (CRC Press), 2009. 265 p.

11. MacDonald, I. L. and Zucchini, W. Hidden Markov and Other Models for DiscreteValued Time Series. London: Chapman and Hall, 1997. 238 p.170

12. T. Lane. Hidden markov models for human/computer interface modeling. In Proceedings of the IJCAI-99 Workshop on Learning about Users. International Joint Conferences on Artifficial Intelligence, August 1999. P. 35-44.

13. Моттль В.В., Мучник И.Б. Скрытые марковские модели в структурном анализе сигналов. М.: ФИЗМАТЛИТ, 1999. 352 с.

14. Шелухин, О.И., Тенякишев, А.М., Осин, А.В. Фрактальные процессы в телекоммуникациях. Монография. / Под ред. О.И. Шелухина. М.: Радиотехника, 2003. 480с.

15. Вапник В.Н., Червоненкис А.Я. Теория распознавания образов. М.: Наука, 1974. 415 с.

16. V.Paxson, Empirically derived analytic models of wide-area TCP connections, IEEE/ACM Trans. Netw., 1994, vol. 2, no. 4, P. 316–336.

17. V.Paxson and S.Floyd, Wide area traffic: the failure of Poisson modeling, IEEE/ACM Trans. Netw., 1995, vol. 3, no. 3, P. 226–244.

18. T.Karagiannis, K.Papagiannaki, and M.Faloutsos, BLINC: multilevel traffic classification in the dark // Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Pomputer Communications, New York, USA, 2005, P. 229–240.

19. L. Zhanh and J. Tang, Characterization and performance study of IP traffic in WDM networks // Computer communications, 2001, No.24, P. 1702–1713.

20. Bruce A. Mah. An Empirical Model of HTTP Network Traffic. Copyright 1997 IEEE. Published in the Proceedings of INFOCOM`97, vol. 2, April 1997. P.592-600.

21. Wright, C., Monrose, F., Masson, G.: HMM profiles for network traffic classification(extended abstract). In: Proc. of Workshop on Visualization and Data Mining for Computer Security (VizSEC/DMSEC), Fairfax, VA, USA (2004). P. 9

22. Лукірін Ю.М., Климова І.М. Методи моніторингу трафіка в корпоративних комп’ютерних мережах // Проблеми інформатизації : одинадцята міжнародна науково-технічна конференція. Черкаси – Баку– Харків – Бельсько-Бяла, 2023, т.1, с.82.