МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ,
ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ Роман ОДАРЧЕНКО
“_____”_____2022 р.

КВАЛІФІКАЦІЙНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ
“МАГІСТР”

Тема: “Алгоритм підвищення якості передачі мультисервісних даних в телекомунікаційній мережі 5G”

Виконавець: _____ Олександр ДОМАЄВ
(підпис)

Керівник: _____ Володимир КЛИМЧУК

Консультанти з окремих розділів пояснювальної записки:

Консультант розділу «Охорона праці» _____ Батир ХАЛМУРАДОВ
(підпис)

Консультант розділу
«Охорона навколишнього середовища» _____ Євген БОВСУНОВСЬКИЙ
(підпис)

Нормоконтролер: _____ Денис БАХТІЯРОВ
(підпис)

Київ 2022

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроніки та телекомунікацій

Кафедра телекомунікаційних та радіоелектронних систем

Спеціальність 172 «Телекомунікації та радіотехніка»
Освітньо-професійна програма «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Роман ОДАРЧЕНКО

“___”_____2022 р.

ЗАВДАННЯ

на виконання кваліфікаційної роботи

Домаєва Олександра Сергійовича

1. Тема кваліфікаційної роботи: “Алгоритм підвищення якості передачі мультисервісних даних в телекомунікаційній мережі 5G” затверджена наказом ректора від “ 07” вересня 2022р. №1321/ст.
2. Термін виконання роботи: з 05.09.2022 р. по 31.11.2022 р.
3. Вихідні дані до роботи:
   1. Технологія мережі – 5G
   2.Стандарт якості - QoS;
   3. Технологія контролю трафіка - DPI;
4. Зміст пояснювальної записки: 1. Вступ
2.Основи побудови технології Deep packet inspection
3. Побудова алгоритмів використання технології DPI
4.Охорона праці 5. Охорона навколишнього середовища
5.Перелік обов’язкового графічного (ілюстрованого матеріалу):8-9 слайдів за тематикою роботи

6. Календарний план-графік

№ п/п	Завдання	Термін виконання	Відмітка про виконання
1.	Розробити деталізований зміст розділів дипломної (кваліфікаційної) роботи	05.09.2022-06.09.2022	Виконано
2.	Вступ	07.09.2022-10.09.2022	Виконано
3.	Основи побудови технології Deep packet inspection	12.09.2022-05.10.2022	Виконано
4.	Побудова алгоритмів використання технології DPI	07.11.2022-12.11.2022	Виконано
5.	Охорона навколишнього середовища	14.11.2022-19.11.2022	Виконано
6.	Усунення недоліків та захист диплом-ної роботи	21.11.2022-30.11.2022	Виконано

7. Консультанти з окремих розділів

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв
Охорона праці	к.м.н., проф. Батир ХАЛМУРАДОВ		
Охорона навколишнього середовища	к.т.н., доц. Євгеній БОВСУНОВСЬКИЙ		

8. Дата видачі завдання: “22" серпня 2022 р.

Керівник дипломної роботи _____ Володимир КЛИМЧУК
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Олександр ДОМАЄВ.
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, має 97 аркушів основного тексту, 12 рисунків, 5 таблиць, Загальний обсяг роботи 101 аркуш.

В роботі проведено аналіз існуючих проблем з забезпеченням якості передавання мультимедійного трафіку через мережу мобільного зв'язку 5G. Запропоновано використання технології глибокого аналізу пакетів DPI для ідентифікації і блокування пакетів.

Ключові слова: ПОКАЗНИКИ ЯКОСТІ QoS, ТЕХНОЛОГІЯ DPI, СИГНАТУРА, ПРИОРІТЕТИ, МЕРЕЖА 5G, ТЕХНОЛОГІЯ ГЛИБОКОГО АНАЛІЗУ ПАКЕТІВ.

Об'єкт дослідження - процес передавання мультимедійного трафіку, що проходить через мережу оператора зв'язку 5G з заданими показниками якості передавання**.**

Предмет дослідження - алгоритми забезпечення якості передавання мультимедійного трафіку.

Мета: − розробка алгоритму контролю трафіка на основі технології глибокого аналізу пакетів, що приведе до блокування паразитного трафіку і в результаті до покращення показників якості передавання даних.

Методи дослідження- математичний апарат теорії електрозв'язку, теорії масового обслуговування, математичної статистики. Експериментальна перевірка результатів дослідження проводилося за допомогою натурного аналізу та методом моделювання на ПК.

Практичне значення отриманих результатів - матеріали дипломної роботи рекомендується використовувати при побудові сучасних телекомунікаційних мереж передачі даних та в навчальному процесі.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ І ТЕРМІНІВ

5G – телекомунікаційна мережа п’ятого покоління;

ADR (adaptive data rate) - адаптивна зміна швидкості передачі;

AN – Мережа доступу;

CN – базова мережа;

Cellular Network – технології, що базуються на використанні стандартів стільникових мереж у ліцензованому діапазоні;

Cisco- американська телекомунікаційна компанія;

DPI – технологія глибокого аналізу пакетів;

Device-to-Device (D2D) – технологія прямого зв'язку між пристроями стандарту LTE;

ІКТ - Инфокомунікаційні технології;

IP-адреса - адреса Інтернет-протоколу;

IoT- інтернет речей (Internet of Things);

LTE - (Long-Term Evolution) – стандарт бездротової високошвидкісної передачі даних;

M2M - машинно-машинна взаємодія, анг. Machine-to-Machine;

ITC-інтелектуальні транспортні системи;

ЛМ - локальні мережі;

STM - Synchronous Transport Module – синхронний транспортний модуль;

SDH - Synchronous Digital Hierarchy – синхронна цифрова ієрархія;

Single-Cell Point-to-Multipoint - Технологія мультимедійного мовлення в одній соті;

SCS Services Capability Server - Сервер забезпечення можливості реалізації послуг;

QoS – якість обслуговування.

ВСТУП

Актуальність теми. У зв'язку зі швидким розвитком мультисервісних мереж, появою в Інтернеті OTT-сервісів, кожен з яких по-різному використовує ресурси мережі, має різні характеристики і вимоги до обслуговування цього трафіку, постає завдання розробки і впровадження методів управління трафіком. Зростає привабливість таких послуг для користувачів і зменшується використання традиційних послуг операторами зв’язку, які наражаються на ризик падіння доходів від надання своїх послуг та призводять до перевантаження мережі. Ці типи проблем призводять до зниження рівня відмовостійкості в роботі системи[1,2].

Одним із шляхів вирішення цієї проблеми є співпраця операторів зв'язку та OTT-сервісів, заснована на забезпеченні максимальної гнучкості передачі мультимедійної інформації.

Виходячи з цього, слід сказати, що найпопулярнішим засобом є пріоритезація різних типів трафіку за допомогою перспективних підходів і методів технології DPI[1,2].

Тому актуальним є завдання побудови алгоритму підвищення якості мультисервісної передачі даних у телеком-мережі 5G.

Мета та завдання дослідження.Метою даної роботи є дослідження принципів роботи системи DPI та з урахуванням об’єкта дослідження реального мультимедійного трафіку, що протікає через мережу оператора зв’язку 5G, виявлення та аналіз можливості використання системи DPI. для досягнення цього забезпечити якість обслуговування цього трафіку. Для досягнення мети були сформульовані наступні завдання[1,2]:

1. Проаналізувати характеристики мультимедійного трафіку в мережі 5G;
2. Визначити загальні критерії та параметри якості послуг;
3. Розгляд архітектури та принципів роботи систем DPI;
4. Дослідити алгоритми ідентифікації трафіку, проаналізувати їх роботу;
5. Провести статистичний аналіз та узагальнити результати;

6. Виконайте моделювання мережі за допомогою DPI для забезпечення необхідної якості обслуговування трафіку.

Предмет дослідження: процес передачі мультимедійного трафіку, що проходить через мережу оператора зв’язку 5G з фіксованими показниками якості передачі.

Предмет дослідження: Алгоритми забезпечення якості передачі мультимедійного трафіку.

методи дослідження. У роботі використано математичний апарат теорії телекомунікацій, теорії масового обслуговування та математичної статистики. Експериментальна перевірка результатів досліджень проводилась за допомогою натурного аналізу та методу моделювання на ПК.

Практичне значення отриманих результатів. Рекомендується використовувати матеріали дипломної роботи у навчальному процесі.

РОЗДІЛ 1

АНАЛІЗ ВИМОГ ДО ЯКОСТІ ОБСЛУГОВУВАННЯ МУЛЬТИСЕРВІСНОГО ТРАФІКУ

1.1. Характеристика мультимедійних сервісів

Активне впровадження високошвидкісного доступу при зниженні вартості передачі даних і розвиток мережевих технологій призвели до появи сервісів, що дозволяють передавати мультимедійну інформацію. Такий контент генерується сервісами OTT[1,2].

Як відомо, телекомунікаційні послуги можна розділити на керовані послуги та послуги, що надаються службами OTT.

OTT (англ. OVERTHETOP) — спосіб надання контенту через Інтернет для різноманітних пристроїв за допомогою мереж передачі даних без участі оператора в управлінні та розповсюдженні контенту.

З керованими послугами передбачається, що постачальник має частковий контроль над керованими послугами. Провайдер має можливість використовувати засоби керування для вибору параметрів передачі та резервування пропускної здатності мережі для забезпечення необхідної якості обслуговування.

Тому керовані служби тісно пов’язані з базовою мережею[2,3].

Служби OTT і пов’язані програми покладаються на загальнодоступний Інтернет. У цьому випадку провайдер не несе відповідальності за вміст посилок, а також не зобов’язаний гарантувати якість доставки.

На відміну від операторів зв’язку, провайдери OTT не піклуються про обслуговування мережі та збільшують свою пропускну здатність, оскільки вони використовують мережі інших людей.Послуги, що надаються сервісами OTT, можна розділити на[2,3]:

1) потокова передача – безперервна передача матеріалів. Не означає довільну зупинку користувачем і подальше відтворення з тієї ж точки;

1) Video on Demand – система містить вміст відео;

2) Text Messenger - сервіс для миттєвого обміну текстовими повідомленнями;

3) Voice Messenger – сервіс для миттєвого обміну голосовими повідомленнями;

4) соціальні мережі;

5) хмарні послуги;

6) Інше.

Зручні та популярні сервіси можуть ефективно використовувати всі його переваги, що не покриває тільки витрати на його розробку, але й перетворює його на стабільне джерело доходу.

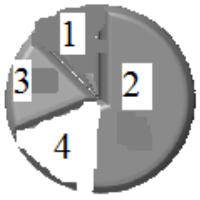
Монетизація проекту – отримуйте прибуток від проекту.

Моделі монетизації, на основі яких працюють OTT-сервіси, можна умовно розділити на чотири категорії[2,3]:

1) Лінійне програмування (LP - Linear Programming) - надає послугу через Інтернет. У цьому випадку послуги OTT здебільшого приносять прибуток, надаючи користувачам доступ до послуги;

2) Модель TVoD (Transactional Video-on-Demand) – де контент знаходиться в каталозі OTT;

3) модель Svod (Subscription VoD) включає в себе mohuses до всього конnarrasse з каталогом сервгх отт пром певноду вечері; 4) Монетизація послуги OTT досягається шляхом надсилання реклами під час відтворення контенту. Цю модель часто називають AVoD (Advertising VoD).



.

Рис 1.1. Співвідношення моделей надання OTT послуг

1.1. Основні оператори OTT послуг.

У зв'язку з появою передових технологій і різноманітних додатків, зараз можна спостерігати появу багатьох представників OTT-сервісів.

Нижче наведено порівняння деяких OTT-сервісів за кількістю місячних відвідувань сервісів російською аудиторією за даними CMSmagazine:

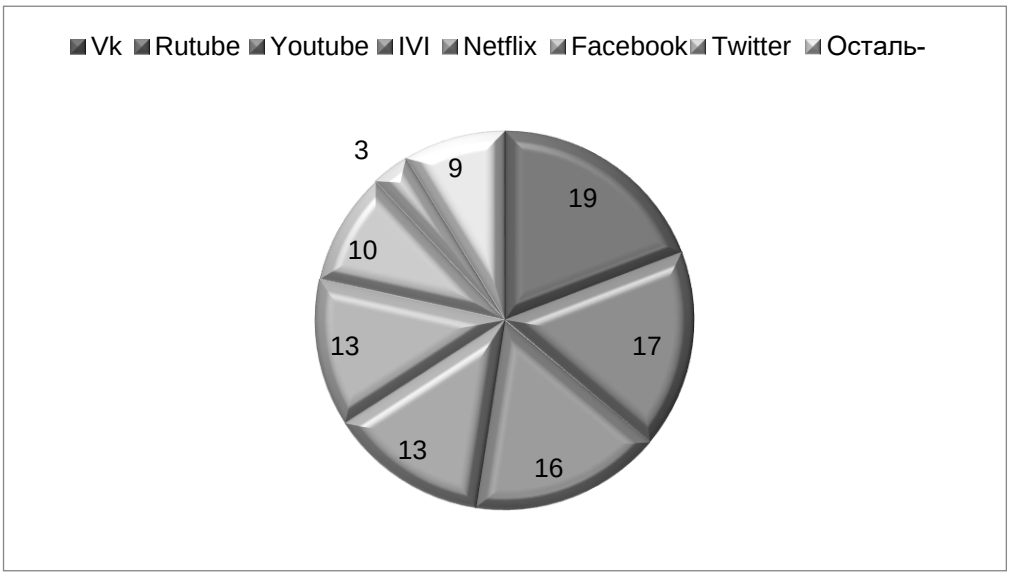


Рис 1.2 Співвідношення користувачів

До найпопулярніших послуг відносяться[3,4]:

1) YouTube — це служба, яка надає користувачам послуги зберігання, доставки та перегляду відео. Користувачі можуть завантажувати, переглядати, оцінювати, коментувати та ділитися певними відео;

2) SopCast — це однорангова служба потокового відео, яка дозволяє переглядати телевізійні канали онлайн і транслювати власні.

3) IVI - програма для перегляду онлайн відео адвокатів;

4) RuTube – сервіс, що надає користувачам послуги зберігання, доставки та перегляду відео;

5) Netflix – сервіс, провайдер фільмів і серіалів на основі потокового мультимедіа;

6) Skype — це програма із закритим кодом, яка забезпечує текстовий, голосовий і відеозв’язок через Інтернет між пристроями;

7) WhatsApp - месенджер з підтримкою голосового зв'язку.Дозволяє надсилати текстові повідомлення та медіадані через Інтернет;

8) Viber — програма, яка дозволяє надсилати текстові повідомлення та дзвонити іншим користувачам Viber;

9) Telegram – месенджер для смартфонів та інших пристроїв, який дозволяє обмінюватися текстовими повідомленнями та медіафайлами в різних форматах;

10) Twitter – соціальна мережа для публічного обміну повідомленнями через веб-інтерфейс, SMS, засоби обміну миттєвими повідомленнями або сторонні клієнтські програми для користувачів Інтернету;

11) Instagram — додаток для обміну фотографіями та відео з елементами соціальної мережі, що дозволяє поширювати їх через свій сервіс та низку інших соціальних мереж;

12) Dropbox - файловий сервіс компанії DropboxInc., що включає персональне хмарне сховище, синхронізацію файлів і клієнтський додаток.

1.3. Актуальність OTT-сервісів

OTT-контент стрімко проникає на всі рівні IT-ринку. Споживачі можуть дивитися відео онлайн замість традиційного телебачення, використовувати комунікаційні платформи, які можна використовувати для обміну миттєвими повідомленнями, здійснювати голосові дзвінки через Інтернет і використовувати відеозв’язок[3,4].

Мобільними месенджерами користуються майже 60% власників смартфонів, тобто 50-60 мільйонів людей. TNS провела опитування жителів міст, де проживає не менше 700 тисяч осіб. від 12 до 64 років на тему найпопулярніших месенджерів[3,4].

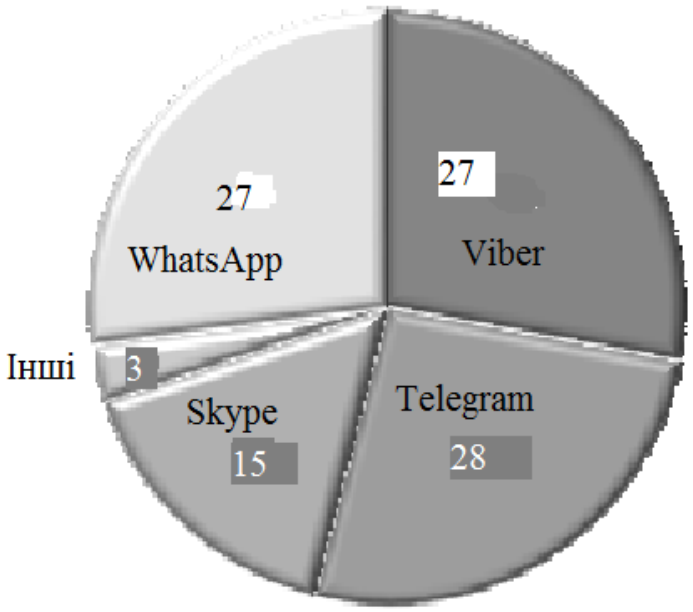


Рис 1.3 Співвідношення популярних OTT-сервісів в Україні

На рисунку 1.4 показано, як зростання Інтернет-додатків для обміну повідомленнями вплинуло на обсяг передачі SMS та прогноз на 2018 р.

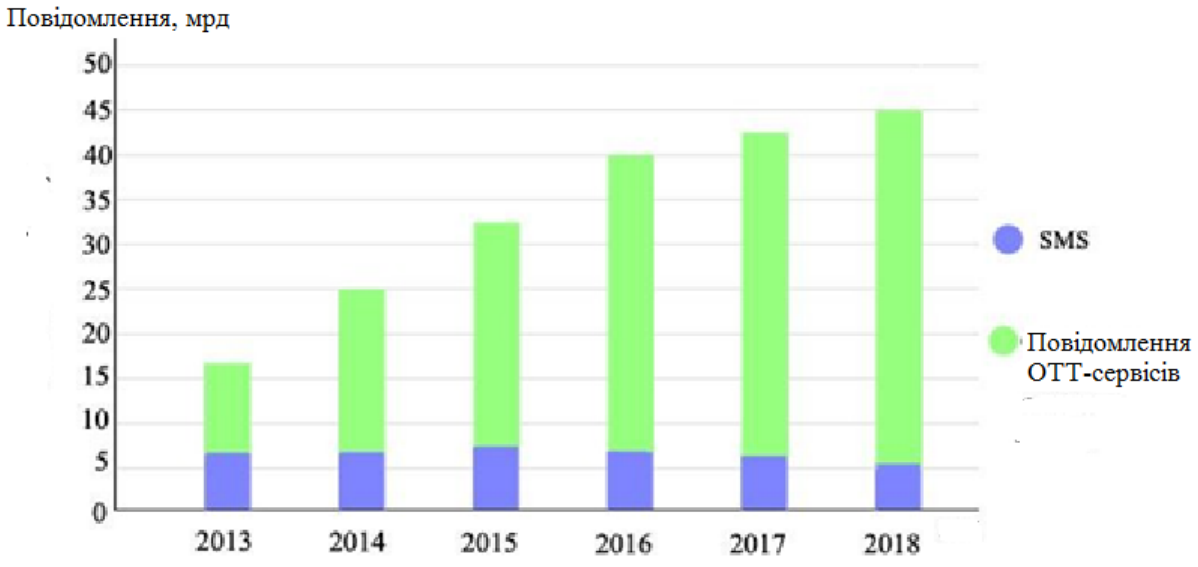


Рис 1.4 Динаміка зростання обсягу SMS-повідомлень

Як показано на малюнку, у 2013 році глобальний обсяг повідомлень, надісланих через OTT-сервіси, такі як Whatsapp, перевищив обсяг повідомлень, наді-

сланих через традиційного оператора. А середній темп зростання ринку OTT послуг з 2014 по 2017 рік склав близько 35%.

На рисунку 1.5 наведено ринок послуг з використанням месенджерів за 2014-2017 роки. та прогноз на 2018-2025 рр. Послуги OTT пропонують глядачеві велику свободу вибору, особистий вибір послуг, незалежний від провайдера, що дозволяє отримати до них доступ у будь-якій точці світу та в будь-який час за наявності підключення до Інтернету[3,4].

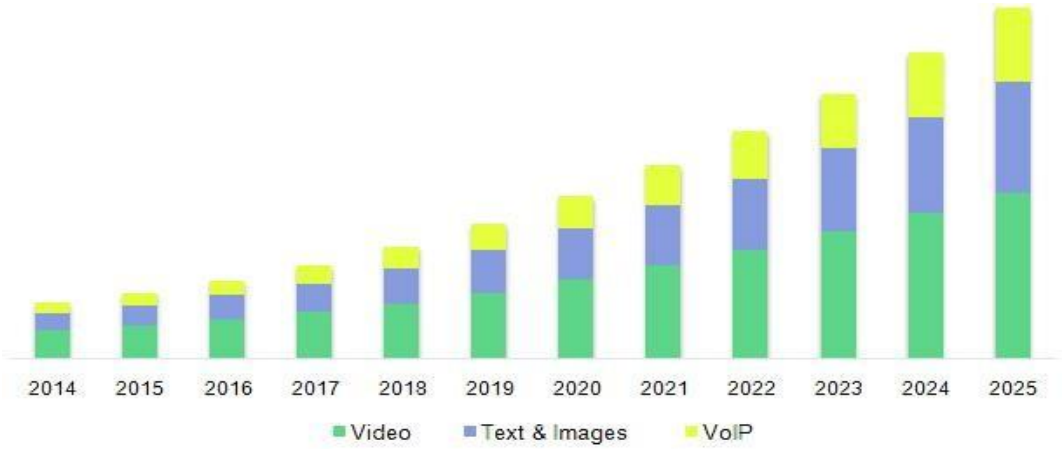


Рис 1.5 Ринок мультимедійних послуг

Незважаючи на те, що використання OTT-сервісів зростає через їх доступність і широке поширення, деякі користувачі готові платити за гарантовану якість під час використання своїх улюблених програм замість використання безкоштовних сервісів з негарантованою якістю.

Наразі спостерігається зростання привабливості користувачів до OTT-сервісів і зменшення користування послугами традиційних операторів зв’язку.

Користувачі очікують передачі даних, голосу та відео з досить високим рівнем обслуговування[3,4].

Однак ці послуги покладаються на мережеву інфраструктуру, побудовану традиційними операторами, у контексті якої оператор надає лише свою мережу. Будь-яке відео, фото чи текстове повідомлення неминуче проходить через апаратуру оператора. Оператори в усьому світі стикаються з ризиком зниження прибутку від надання своїх послуг.

Оператори зв'язку мають заходи для додаткового доходу:

1) спеціальні тарифні плани;

Переваги: Компенсація втраченого заробітку, стимулювання використання даних.

Мінуси: Здешевлення передачі інформації через зростання популярності OTT-сервісів.

2) Розширений пакет для спілкування;

Переваги: Підвищення конкурентоспроможності оператора в порівнянні з OTT-послугами.Недоліки: висока популярність OTT-сервісів, труднощі у взаємодії з іншими операторами.

3) Партнерство з OTT-сервісами.

Переваги: компенсація втраченого доходу, отримання досвіду розвитку бізнес-моделей, пов'язаних з Інтернетом, підвищення привабливості своїх послуг (якісна передача даних в конкретному тарифному плані, що призводить до більш швидкого просування послуг з OTT-сервісів). Можливість роботи OTT-сервісів під брендом оператора.

Недоліки: необхідно визначити межі взаємодії та монетизації співпраці для забезпечення виконання законодавства РФ.

1.4. Правовий статус OTT-операторів

Останнім часом широко обговорюється питання про необхідність регулювання OTT-сервісів в рамках законодавства. Однак це може стати причиною, яка перешкоджає підтримці розвитку вітчизняних технологій у глобальному масштабі та впливає на настрої користувачів цих сервісів. Норми законодавства, що застосовуються до операторів OTT[3,4]:

1) Таємниця спілкування;

2) захист персональних даних;

3) ліцензування;

4) СОРМ;

5) звітність;

6) Державний контроль;

7) перенесення номера;

8) оподаткування;

9) Угоди користувача;

10) Послуги OTT-операторів не потребують ліцензії.

1.5. Питання якості обслуговування

Оскільки Інтернет є «некерованою» мережею, очікується, що користувачі справедливо розподілятимуть доступні мережеві ресурси на всьому шляху передачі. Трафік передається якомога швидше з використанням доступних мережевих ресурсів, але не гарантується надання попередньо визначеної якості обслуговування, тобто немає гарантії, що пакет буде доставлено вчасно або взагалі для типу трафіку[3,4].

Важливо визначити ключові поняття, необхідні для розгляду показників якості послуг.

Якість обслуговування (QoS) — це набір характеристик телекомунікаційних послуг, пов’язаних зі здатністю задовольняти визначені та очікувані потреби користувача послуг.

Надання Послуг - будь-яка діяльність, пов'язана з наданням Послуги Постачальником Послуг з моменту отримання замовлення на Послугу до моменту, коли Послуга стає доступною для використання Абонентом/Користувачем[3,4].

Рис 1.7. Якість обслуговування в галузі телекомунікацій

Параметри якості обслуговування у сфері телекомунікацій можна визначити в ієрархічному порядку:

Продуктивність мережі – вимірюється в частині мережі або підмережі. Вона оцінюється технічними параметрами, що описують роботу цієї ділянки мережі в потрібному напрямку.

Загальна продуктивність мережі – використовується, коли кілька підмереж слід розглядати як єдиний компонент мережі.

Якість послуги «від кінця до кінця» – визначення якості послуги мережі оцінюється без участі користувача.

Для заданого набору певних умов роботи якість послуги QoS може змінюватися під впливом умов середовища, маршрутизації та інтенсивності передачі трафіку.

Етапи, пов'язані з аспектами якості обслуговування:

Доступність мережі – це ймовірність того, що послуги будуть надаватися користувачеві через мережеву інфраструктуру. Імовірність того, що користувач успішно зареєструється в мережі, що надає послугу[3,4].

Доступність послуги — це ймовірність того, що користувач зможе отримати доступ до потрібного контенту.

Цілісність сервісу – описує якість обслуговування під час використання Сервісу та включає такі елементи, як якість вмісту, що передається.

Збереження послуги - визначає припинення надання послуги (відповідно або проти волі користувача) [3,4].

Успіх етапу визначається успішним виконанням, повторними спробами та часом відповіді мережі.

Таблиця 1.1. Основні рекомендації, запропоновані МСЕ-Т щодо забезпеченню QoS

Номер рекомендации	Дата принятия	Название
E.800	23.09.2008	Визначення, що використовуються у міжнародних мережах.
E.801	08.10.1996	Межі угоди щодо якості обслуговування.

E.802	08.02.2007	Принципи та методики визначення та застосування
E.803	14.12.2011	QoS для підтримки аспектів обслуговування.
E.804	13.02.2014	QoS для найпопулярніших послуг мобільної мережі.
E.807	13.02.2014	Визначення параметрів, орієнтованих на користувача, для обробки дзвінків у мобільній мережі.

Продолжение таблицы 1.1. Рекомендации, предложенные МСЭ-Т по обеспечению QoS

E.850	30.10.1992	Підключення та підтримка міжнародного з'єднання.
E.860	29.06.2002	Рамки угод про рівень обслуговування.
E.862	16.06.1992	Надійність планування телекомунікаційних мереж.
E.880	25.11.1988	Збір даних та оцінок на продуктивність мереж,
G.1000	29.11.2001	обладнання та надання послуг.
G.1010	29.11.2001	Визначення, що використовуються телекомунікацій.
G.1011	29.07.2016	Категорії QoS для мультимедійних користувачів.
G.1020	14.07.2006	Довідковий посібник з методу оцінки якості.
G.1021	15.07.2012	Визначення характеристик стосовно додат-
G.1022	29.07.2016	ням у смузі тональних частот, що використовують IP-мережі.
G.1021	15.07.2012	Моделі буфера для розробки показників
G.1022	29.07.2016	ефективності роботи клієнтів
G.1028	06.04.2016	Моделі буфера для медіа-потоків.
G.1029	13.02.2014	Моделі буфера для розробки показників
G.1030	13.02.2014	ефективності роботи клієнтів
G.1050	29.07.2016	Моделі буфера для медіа-потоків.
G.1070	14.07.2016	QoS для передачі голосу у мобільних мережах 4G.

G.1071	29.06.2015	Діагностика для голосових сервісів.
G.1081	22.10.2008	Оцінка продуктивності з кінця до кінця в IP-мережах
G.1082	29.04.2009	для програм передачі даних.
Y.1501	29.07.2004	Мережева модель для оцінки передачі мультимедійних
Y.1530	13.11.2007	програм по Інтернет-протоколу.

Продолжение таблицы 1.1. Рекомендации, предложенные МСЭ-Т по обеспечению QoS

Y.1531	13.11.2007	Продуктивність обробки дзвінка протоколу SIP.
Y.1540	29.07.2016	Параметри передачі та доступності IP-пакетів.
Y.1541	14.12.2011	Продуктивність мережі для послуг IP-мережі.
Y.1542	29.06.2010	Основа для досягнення потрібних показників для
Y.1545	14.05.2013	пакетівIPпри передачі з кінця до кінця.
Y.1563	13.01.2009	Карта QoS взаємопов'язаних мереж, які використовують
Y.1565	14.12.2011	Інтернет-протокол.
Y.1566	14.07.2012	Передача кадрів Ethernet та експлуатаційна готовність.
Y.2111	29.11.2011	Робочі параметри домашньої мережі.
Y.2112	13.06.2007	QoS та взаємозв'язок між Ethernet, Інтернет-протоколом та
Y.2113	23.01.2009	комутацією по мережі.
Y.2173	12.08.2009	Ресурси та керування функціями допуску в мережах

1.6. Загальні аспекти критеріїв і параметрів якості послуг

При визначенні критеріїв, обсягу та методів вимірювання параметрів слід враховувати наступні основні аспекти[3,4]:

1) необхідно враховувати для кожної конкретної послуги;

2) Має бути визначено для наскрізного зв'язку, кінцеві точки якого є точками з'єднання терміналів користувача;

3) Критерії та параметри QoS повинні бути визначені в термінах, зрозумілих клієнту; 1) Профіль QoS рівня клієнта може змінюватися з часом, тому надзвичайно важливо, щоб постачальник послуг знав про зміну вимог клієнта.

Залежно від завдання оцінки якості використовуються відповідні параметри з необхідним рівнем деталізації оцінки якості. Параметри якості обслуговування також можуть бути обрані для вимірювання якості обслуговування, яке сприймає користувач.

Різні сторони можуть нести відповідальність за транспортування, надання та вміст, а також надання кінцевих пристроїв.

Тому необхідна модель, яка дозволяє розглядати ці елементи окремо та визначати відповідні критерії якості. Ця модель забезпечує більш просте визначення та категоризацію критеріїв QoS, пов'язаних із цим типом послуг.

Набір дій із надання мультимедійних послуг, що включає створення контенту, керування послугами, мережу доставки та клієнтське обладнання, відомий як модель чотирьох ринків.

Для даної телекомунікаційної послуги цю модель можна використовувати для розгляду кожного з чотирьох компонентів окремо та для визначення критеріїв якості.

На малюнку 1.8 наведено огляд моделі та пояснення чотирьох компонентів.

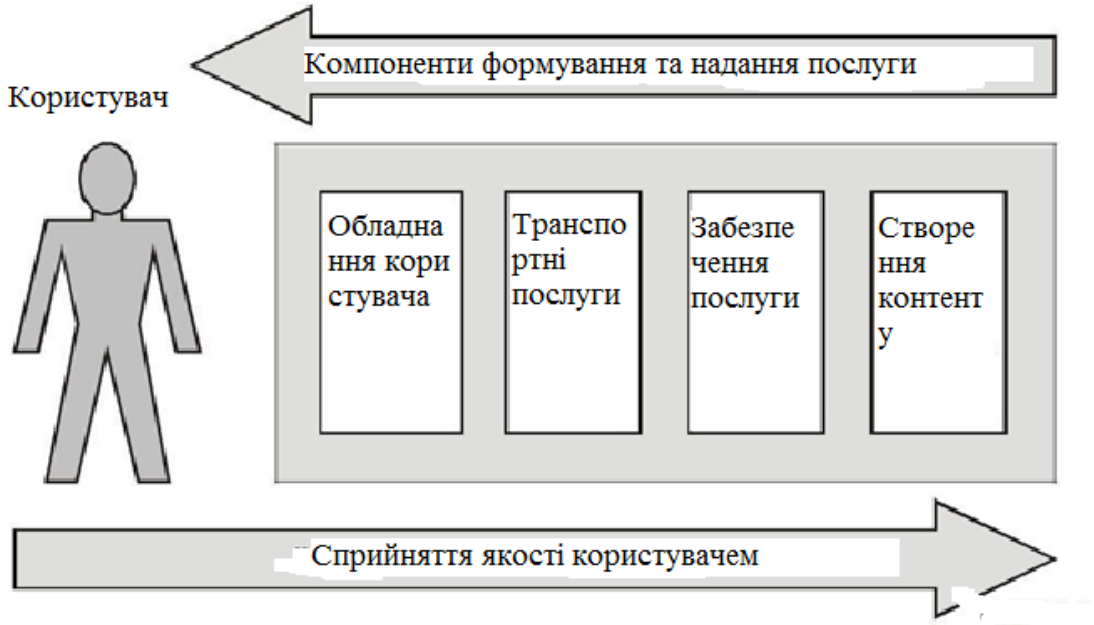


Рис 1.8. Модель чотирьох компонент

Клієнтське обладнання - обладнання всіх видів, яке потрібне Користувачеві для доступу до Мережі, а отже, до Сервісу.

Транспортні послуги – телекомунікаційні мережі всіх типів, що використовуються для розповсюдження телекомунікаційних послуг, наприклад, наземні та супутникові голосові мережі.

Надання послуг – усі дії та функції, пов’язані з наданням та управлінням телекомунікаційними послугами[4,5].

Створення Контенту – усі види діяльності, пов’язані зі створенням і розповсюдженням Контенту, які надаються через Службу електронного зв’язку.

Пропускна здатність є основним параметром QoS, який визначає основний вплив на продуктивність, яку сприймає кінцевий користувач.

Критерії якості, отримані за допомогою моделей, необхідно трансформувати в параметри якості, щоб їх можна було використовувати для кількісних і якісних характеристик QoS телекомунікаційних послуг. Метою є узгоджений

набір параметрів якості, які можна використовувати для оцінки якості телекомунікаційних послуг і можливість порівнювати різні пропозиції.

Загальна якість обслуговування для сеансу зв'язку залежить від того, наскільки дотримані встановлені стандарти для більшості переданих і отриманих пакетів. Це означає, що показники повинні виражати параметри[4,5]:

1) Подивіться на всі аспекти послуги з точки зору користувача;

2) бути орієнтованим на користувача;

3) Ви не залежите від будь-якої конкретної мережевої архітектури чи технології;

4) об'єктивно чи суб'єктивно виміряні в точці доступу до послуги;

5) Легка кореляція з параметрами продуктивності мережі Основні параметри, що впливають на користувача:

Затримка – проявляється різними способами, включаючи час, необхідний для надання певної послуги від початкового запиту користувача до отримання певної інформації після запиту.

Причини затримок:

1) черги на вузлах;

2) термінали (буфер тремтіння);

3) термінали (кодування, декодування, шифрування);

4) затримка розподілу;

5) Механізми обслуговування черги.

Варіація затримки. Варіація затримки зазвичай включається як параметр продуктивності, оскільки вона важлива через зміну часу надходження окремих пакетів на транспортний рівень.

Причини тремтіння:

1) асинхронність IP мережі;

2) динамічна маршрутизація;

3) Пакетний характер трафіку.

Втрата інформації безпосередньо впливає на якість інформації для користувача. Втрата інформації не обмежується впливом бітових помилок або втрати пакетів під час передачі, але включає вплив будь-якого фактора погіршення, представленого кодуванням для більш ефективної передачі.Причини втрати:

1) перевантаження вузла;

2) помилка в каналі;

3) механізми профілювання трафіку;

4) Термінали (через перевищення гранично допустимої затримки).

1.6. Види трафіку та їх особливості

Audio:

1) Розмова. Вимоги до виклику визначаються затримкою в одну сторону. Існує два різні ефекти затримки.

Перший - це виникнення ехосигналу, пов'язаного з дво- і чотирипровідним перетворенням. Другий ефект виникає, коли затримка збільшується до точки, коли починається розмова, тобто. Х. затримка стає помітною. Під час передачі основне джерело погіршення якості пов’язане з використанням стиснення голосових кодеків та їхніх характеристик втрати пакетів[4,5].

1) Голосові повідомлення. Вимоги до затухання по суті такі ж, як і для мовлення (тобто залежать від мовного кодека), але основна відмінність полягає в тому, що, оскільки немає прямого мовлення, допускаються затримки. Затримка порядку кількох секунд виглядає розумним використанням цього типу;

2) Потокове аудіо. Під час потокової передачі аудіо потрібно забезпечити вищу якість, ніж у традиційній телефонії, і відповідно вимоги щодо втрати інформації про втрату пакетів будуть суворішими. Однак, як і у випадку з голосовими повідомленнями, тут немає розмовного аспекту, і вимоги до затримки можуть бути довільними, хоча команди керування мають бути належним чином розроблені.

відео:

1) Відеотелефон. Відеотелефон – це повнодуплексна система, яка обмінюється як відео-, так і аудіоданими і призначена для використання в розмовному середовищі.Вимоги до затримок такі ж, як і для розмов, з додатковою вимогою, що звук і відео мають бути синхронізовані в певних межах;

2) Одностороння передача відео. Ключова відмінність односторонніх відео полягає в тому, що немає розмовного аспекту, тобто вимоги до затримок не такі суворі.

З точки зору користувача, головна вимога до будь-якої програми передачі даних полягає в тому, щоб гарантувати практичну відсутність втрати даних. У той же час тремтіння затримки зазвичай непомітне для користувача, але має бути певне обмеження синхронізації між мультимедійними потоками в сеансі[4,5].

1) Перегляд веб-сторінок. У цій категорії ми зосереджені на відображенні компонента HTML веб-сторінки (інші компоненти, такі як зображення, аудіо- та відеозаписи, розглядаються відповідно до власних категорій). З точки зору користувача, ключовим фактором продуктивності є швидкість завантаження сторінки після її запиту. Невеликі затримки допустимі;

2) Передача даних. До цієї категорії відноситься передача різноманітних файлів. Під час передачі файлу вимоги до затримки трохи нижчі, ніж під час перегляду веб-сторінки;

3) Високопріоритетні операції (електронна комерція). Основна вимога - забезпечення терміновості та надійності, допустима затримка не більше кількох секунд;

4) Інтерактивні програми.Вимоги до інтерактивних програм відрізняються залежно від програми, вимогливі програми вимагають затримки трохи більше частки секунди;

5) Telnet. Для Telnet вимоги до затримки обмежені частками секунди, щоб забезпечити майже миттєвий обмін даними;

6) Електронна пошта (доступ до сервера). Можлива затримка на кілька хвилин;

7) Обмін миттєвими повідомленнями. Миттєві повідомлення передусім стосуються обміну текстовими даними, але також можуть включати аудіо, відео та зображення. У будь-якому випадку, незважаючи на назву, це не зв’язок у реальному часі, і затримки в кілька секунд допустимі;

8) Фонові програми. По суті, єдина вимога до програм цієї категорії полягає в тому, щоб інформація доставлялася користувачеві практично без помилок. Однак затримка обмежена, оскільки застарілі дані практично марні;

1) факс. Факс зазвичай не призначений для супроводу інтерактивного спілкування в режимі реального часу. Однак у більшості бізнес-сценаріїв очікується, що факс буде отримано протягом приблизно 30 секунд;

2) служба коротких повідомлень. Допускається невелика затримка.Для користування послугами OTT необхідно забезпечити оператору зв'язку гарантовану якість обслуговування окремих послуг.

Оператор може встановлювати пріоритети трафіку, що забезпечує максимальну гнучкість надання послуг.

Для трафіку даних визначено чотири рівні пріоритету:

1) Критичний: єдиний рівень пріоритету такого типу, зарезервований для зв'язку в екстрених ситуаціях;

2) високий: послуги для державного управління, послуги для бізнес-абонентів, послуги для VPN;

3) Звичайний: Прикладами таких послуг є телефонні послуги для абонентів;

4) Найкраще з можливих: Прикладами є послуги інтернет-провайдерів.

Кількість класів навмисно обмежена, щоб спростити дизайн мережі оператора, тому цілі в кожному класі повинні відповідати потребам кількох програм.

Виходячи з цільових вимог, параметри різних додатків можуть бути показані в таблиці 1.2. Таблиця чітко показує, яка якість прийнятна для кожного класу застосування[4,5].

Таблиця 1.2. Показники характеристик роботи для програм передачі аудіо, відео та даних

Середовище передачі	Додаток	Типові швидкості передачі	Ключові параметри характеристик работи та цільові значення		
			Затримки	Джитер	Втрата інформації
Аудіо	Розмова	4-64 кбит/с	Бажано < 150 мс межа <400мс	<1мс	<3%
	Передача	4-32 кбит/с	<1с для відновлення <2с для запису	<1мс	<3%
	голосових повідомлень	16-128 кбит/с	<10с	<<1мс	<1%
Відео	Відео-телефон	16-384 кбит/с	Бажано < 150 мс межа<400мс	Синхронизація мови <80мс	<1%
	Одностороння передача відео	16-384 кбит/с	<10с	-	<1%
	Просмотр веб-сторінок	≈ 10кБ	Бажано 2 с/аркуш межа 4 с/страница	-	0

Дані	Передача даних	10кБ – 10МБ	Бажано < 15с межа <60с	-	0
	Операції з високим приорітетом	< 10кБ	Бажано <2с Пре-дел <4с	-	0
	Інтерактивні додатки	< 1кБ	<200мс	-	0
	Управління	≈ 1кБ	<250мс	-	0
	Электронна пошта	< 10 кБ	Бажано <2с	-	0
	Факс	≈ 10 кБ	Бажано <30с/сраница	-	$< 10^{-6}$
	Транзакції з низьким пріоритетом	< 10 кБ	Бажано <30с	-	0

Норми на параметри доставки пакетів IP з поділом за класами обслуговування зазначені у таблиці 1.3.

Таблиця 1.3. Норми на параметри доставки пакетів IP з розділенням класів обслуговування

Мережеві характеристики Затримка доставки пакету	Класи QoS					
	0	1	2	3	4	5
Варіація затримки пакета	100 мс	400 мс	100 мс	400 мс	1 с	Н
Коефіцієнт втрати пакетів	50 мс	50 мс	Н	Н	Н	Н
Коефіцієнт помилок пакетів	$1x10^{-3}$	$1x10^{-3}$	$1x10^{-3}$	$1x10^{-3}$	$1x10^{-3}$	Н
Мережеві характеристики	$1x10^{-4}$	$1x10^{-4}$	$1x10^{-4}$	$1x10^{-4}$	$1x10^{-4}$	Н

Примітка. Н - не нормується.

Class 0: Додатки реального часу, чутливі до джиттера, характеризуються високим рівнем інтерактивності (особливо для мови з використанням ІЧ-технології), передбачено створення окремої черги з пріоритетною обробкою пакетів;

Клас 1: Додатки реального часу, чутливі до джиттера, інтерактивні, призначені для обміну інформацією в реальному часі, але з менш жорсткими вимогами, передбачається створення окремої черги з пріоритетною обробкою пакетів;

Клас 2: Транзакції даних з високим рівнем інтерактивності (особливо сигнальна інформація), для обробки формується окрема черга, яка виконується з другим пріоритетом;

Клас 3: транзакції даних, інтерактивні програми, пакетні послуги здійснюються з другим пріоритетом;

Клас 4: програми з низькими втратами (короткі транзакції, потокове відео тощо) допускають довгі черги пакетів для обробки другого пріоритету;

Клас 5: Традиційні IP-мережі (електронна пошта, файлові сервери), які обслуговуються з найнижчим пріоритетом.

Розглядаючи питання якості обслуговування трафіку OTT-сервісів, необхідно чітко та однозначно розрізняти різні види OTT-сервісів. А також дати єдине визначення для різних видів OTT-послуг і встановити однакове регулювання у вказаній сфері з технічної точки зору.

Висновок до розділу 1

1.На підставі літературних даних і досліджень ліцензування патентів можна зробити висновок, що мережа 5G є дуже швидкою та надійною. Бездротова мережа мобільного Інтернету 5G - це справжній бездротовий світ. Технології п’ятого покоління пропонують величезний обсяг даних, необмежену кількість дзвінків і нескінченну передачу даних, і все це в новітній мобільній операційній системі. Ця технологія має бути розумнішою, яка з’єднає весь світ без обмежень. Світ універсального, безперебійного доступу до інформації, розваг і спілкування відкриє новий вимір у нашому житті та суттєво змінить наш спосіб життя.

2. Останнє десятиліття в галузі комунікаційних мереж і систем характеризується експоненціальним зростанням як кількості абонентських пристроїв, так і загального обсягу трафіку, що передається на бездротовій ділянці в мережах зв'язку загального користування. За різними джерелами, ця тенденція збережеться і найближчим часом. Значну частину нових пристроїв становлять пристрої, які можна носити, утворюючи абсолютно унікальну екосистему користувачів, відому як Інтернет речей, які можна носити (IoWT). До IoT-пристроїв належать відомі смартфони, розумні годинники, браслети, а точніше окуляри доповненої та віртуальної реальності тощо. Загалом носимі пристрої генерують велику кількість мультимедійної інформації, що викликає винятково високе навантаження на мобільні телекомунікаційні мережі.

3.Як тільки виникає брак ресурсів, що призводить до збільшення ймовірності втрати пакетів і збільшення затримок, неможливо забезпечити необхідні показники якості доставки додатків у реальному часі.

В результаті погіршення швидкості потоку мережа починає надавати низьку якість і періодично припиняє відтворення, або відмовляється виконувати ту чи іншу операцію, що негативно впливає на враження користувача про якість послуг.

Щоб мобільні мережі були повноцінними, необхідно гарантувати високу якість доставки контенту.

Тому традиційні оператори повинні прийняти принципове рішення: або вдосконалити свою мережу та послуги та скористатися перевагами нових технологій, або взяти на себе роль постачальника інфраструктури для інших операторів.

4. Щоб оператор міг ідентифікувати послуги OTT, застосувати унікальні надбудови у вигляді класифікації, пріоритезації для подальшого налаштування пропускної здатності та інших характеристик мережі до послуг, спрямованих на обмін різними типами трафіку, запропоновані технологічні рішення для забез-

печення QoS в мережа провайдера для виділених послуг OTT, які використовують систему DPI для забезпечення певного рівня якості обслуговування.

РОЗДІЛ 2
ОСНОВИ СТРУКТУРИ ТЕХНОЛОГІЇ ГЛИБОКОЇ ПЕРЕВІРКИ ПАКЕТІВ

2.1. Основи технології Deep Packet Inspection (DPI).

Deep Packet Inspection (DPI) — це технологія глибокого аналізу пакетів, за якої пристрій реагує не лише на заголовки пакетів різних рівнів, але й на їх вміст.
DPI з'являється з можливістю контролювати трафік своїх клієнтів, фільтрувати дані відповідно до законодавства країни та захищати авторські права неоднорідних власників контенту.
Способи перевірки трафіку в звичайній ситуації[4,5]:
1) Рівень каналу: керування на основі MAC-адрес або номера VLAN;
2) Рівень мережі: ви можете блокувати користувачів за IP-адресою або забороняти доступ до певних адрес/підмереж у зовнішній мережі;
3) Транспортний рівень: постачальник компанії або IT-служба може обмежити використання портів;
4) Прикладний рівень: доменні імена можна використовувати на проксі-серверах або брандмауерах, але функціональність обмежена порівняно з рішеннями DPI.
Завдяки широкому використанню DPI ця технологія широко застосовується постачальниками послуг через важливість контролю трафіку, що в кінцевому підсумку може значно знизити витрати та залучити більше клієнтів.Де технологія DPI знайшла своє застосування в телекомунікаціях[4,5]:
1) можливість додавання нових послуг;
2) безпека в мережах;
3) блокування від дітей;
4) Здійснення контролю якості;

5) варіація тарифного плану в залежності від індивідуальних потреб користувача;

6) Додаткові послуги Моніторинг мережевої активності підозрілого користувача;

7) прикладний фільтр;

8) Запобігання витоку інформації. Ці системи запобігають поширенню конфіденційних даних через мережеві інтерфейси;

9) система виявлення/попередження порушників;

10) моніторинг;

11) Збір різноманітної статистики та профілювання клієнтів для рекламних і маркетингових цілей.

Для оператора використання технологій DPI може значно спростити життя, додати нові послуги та істотно контролювати управління мережею.

2.1. Архітектурна система DPI

Щоб зрозуміти, як система DPI працює з трафіком, необхідно розглянути, з яких елементів складається ця система і які основні механізми аналізу та контролю трафіку використовуються в технології DPI. Розглянемо структуру системи **DPI.**

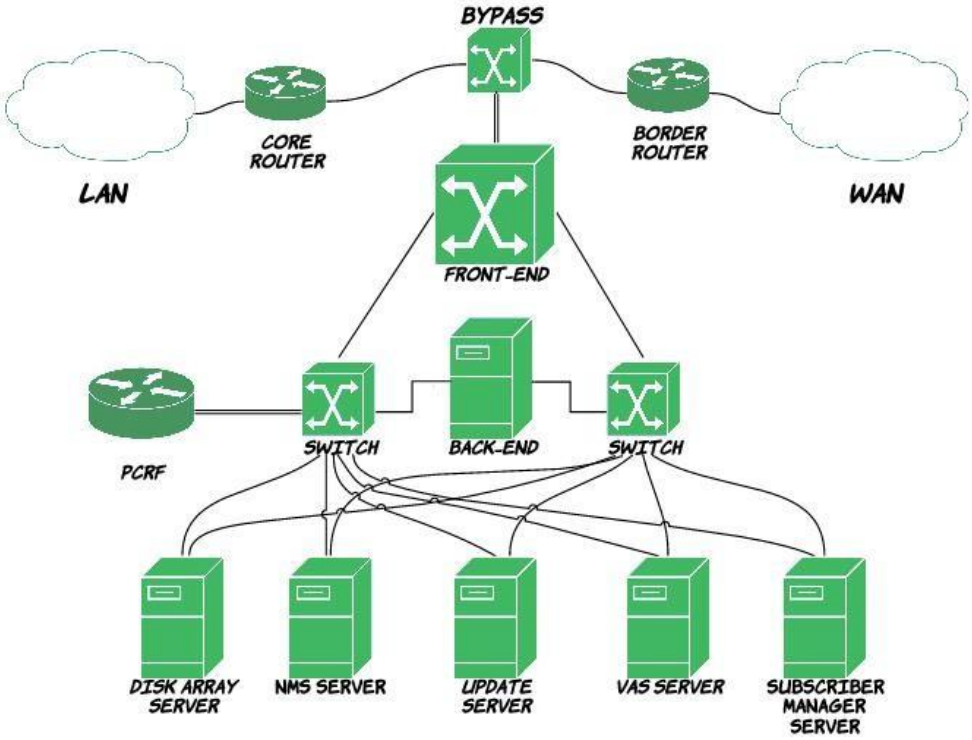


Рис. 2.1. Архітектура DPI-системи

1. 1. Основні компоненти повної системи DPI:
2. 2. 1) Bypass — це високопродуктивний комутатор, основним завданням якого є або перенаправлення трафіку безпосередньо (без обробки), або відправка трафіку на пристрій для обробки та аналізу трафіку — front-end. У разі втрати з'єднання або перевантаження інтерфейс перенаправляє трафік безпосередньо на маршрутизатор.
3. Він має два режими роботи:
4. Захисна. Трафік проходить повз.

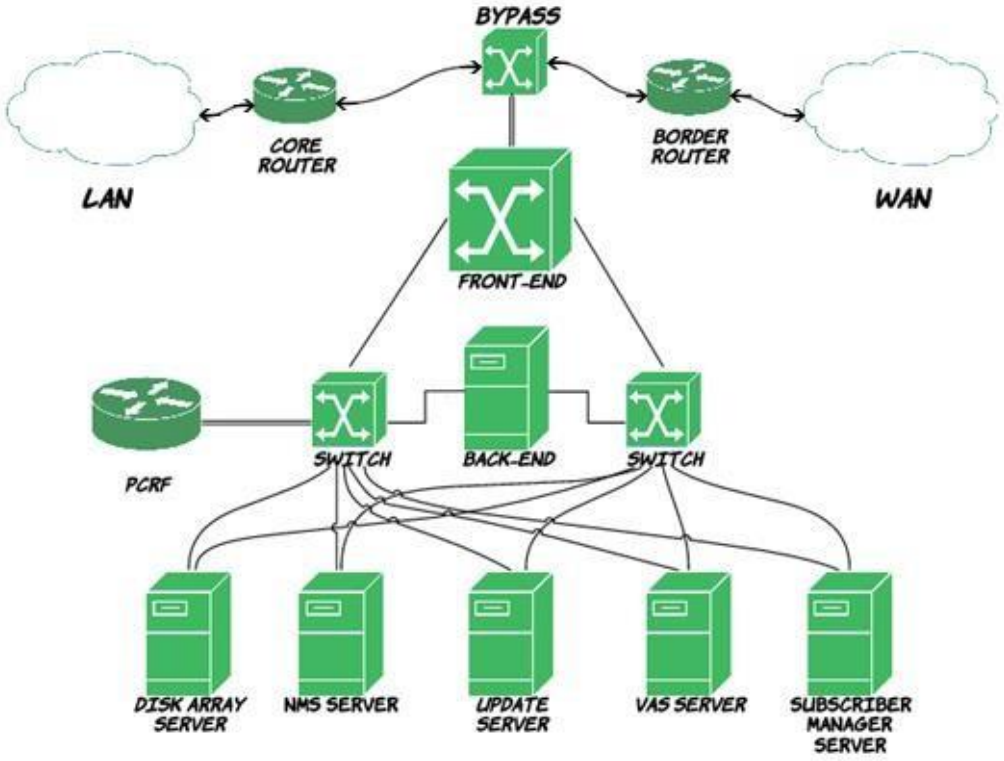


Рис. 2.2. Принцип работи DPI системи в захисному режимі работи

5. Робочий. Трафік направляється на фронтенд, але в цьому випадку він перемикається на прямий канал.

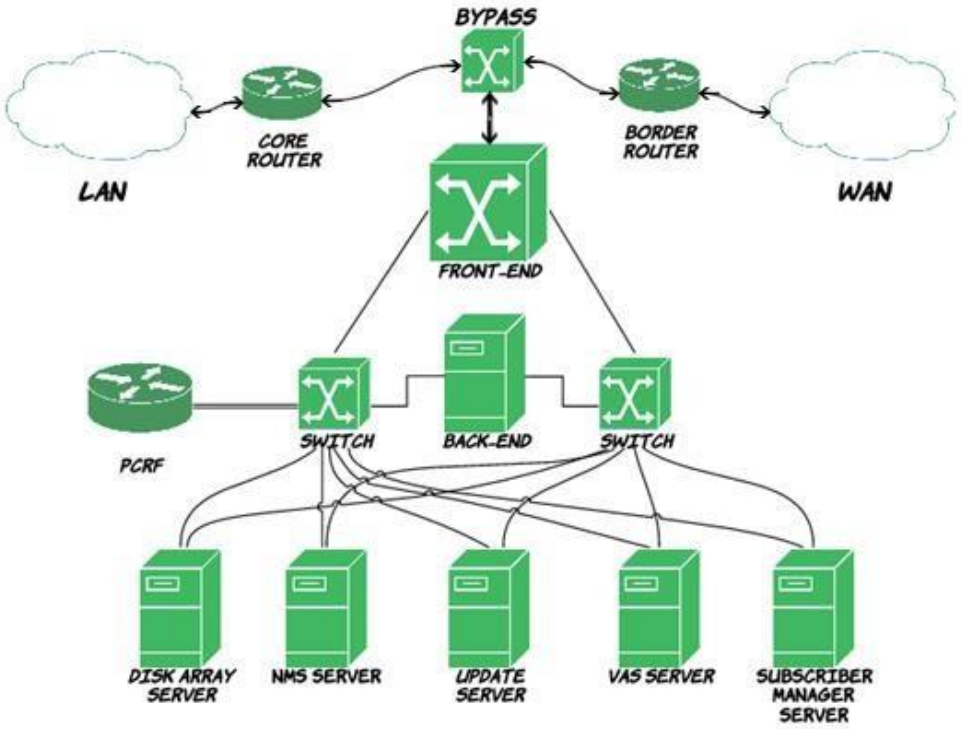


Рис. 2.3. Принцип роботи DPI системи в робочому режимі работи

2) Front-end - центр обробки інформації за доступними видами трафіку.

3) Back-end — це високопродуктивний сервер для оперативного використання баз даних сигнатур, різноманітної статистики, набору сервісів, різних правил перенаправлення трафіку та надання інформації фронтенду.

4) Сервер PCRF (Policy and Charging Rules Function) - сервер для визначення правил і режимів. Основна роль в отриманні ідентифікатора користувача з інтерфейсу полягає в тому, щоб повідомити інтерфейсу про відповідний номер режиму, деталі режиму запитуються з інтерфейсу.

5) Сервер дискового масиву - Сервер дискового масиву призначений для зберігання великих обсягів інформації (статистика, різні бази даних, іноді копії трафіку) [4,5].

6) NMS Server (Network Management Server) - сервер управління системою.

7) Update server - сервер оновлень.

8) Subscriber Manager - програмна складова системи, яка є координаційним центром системи DPI з управління трафіком, реалізує можливості персоналізації послуг (прив'язка до користувача/пристрою/мережі).

9) VAS сервер (Value Added Services Server) – сервер додаткових послуг.

DPI можна розділити на три частини:

1) швидкісна частина;

Трафік користувачів з мінімальними затримками.

2) мережа взаємодії компонентів;

Через цю мережу передається тільки службова інформація, швидкість передачі не висока.

3) Управління та PCRF - роз'єм до зовнішньої (для DPI) мережі;

2.2 Аналіз і контроль DPI трафіку через систему

Існує кілька способів визначення трафіку. Аналіз DPI базується на таких механізмах[6,7]:

1) Чітко визначені правила.

Правила та політики встановлюються системним адміністратором шляхом активації всіх або частини необхідних правил і політик із наборів, наданих розробником системи.

2) аналіз підпису.

Аналіз сигнатур – це аналіз, під час якого система шукає структуру пакета та порівнює її з відомими випадками.

Простіше кажучи, це набір байтів у пакеті, який дозволяє однозначно ідентифікувати програму протоколу, якому належить трафік, і класифікувати його.

Системи DPI використовують механізми сканування, засновані на тому, що всі відомі протоколи мають свої точні підписи. Якщо збіг знайдено, пакет вважається розпізнаним і доступним для інших програм. Це саме те, що стосується аналізу сигнатур трафіку.

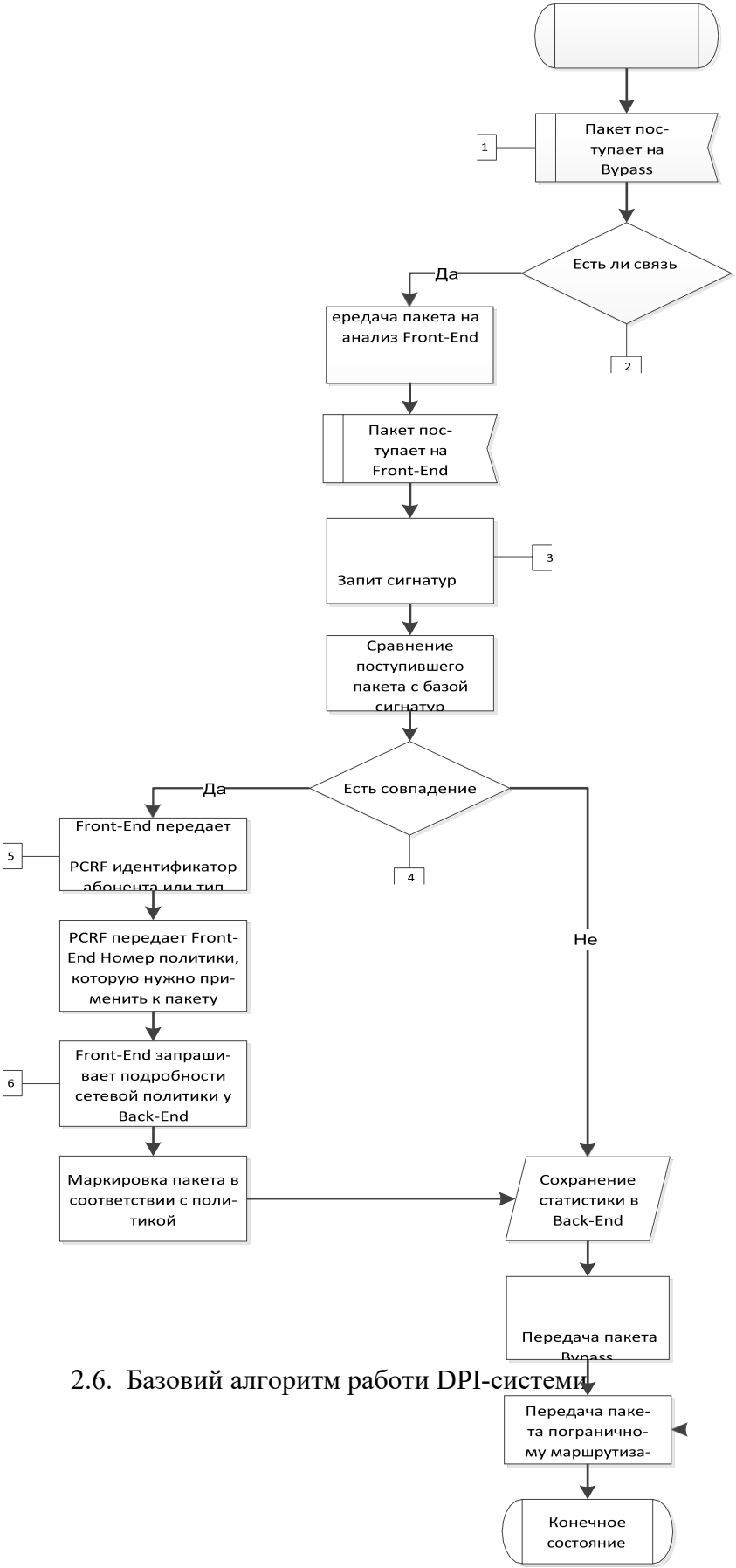
Оскільки щодня з’являються нові програми, які генерують великий обсяг трафіку даних для аналізу, базу даних підписів необхідно регулярно оновлювати. Недоліком цього методу є високе споживання ресурсів і неточність аналізу для нових типів трафіку і нових додатків, для яких обробки підпису недостатньо.

3) Евристичний аналіз.

Евристичний аналіз – це технологія виявлення трафіку на основі характеристик (без гарантії точності).Процедура складається з неповного, але дуже точного порівняння пакетів із відомими підписами. Переваги цього методу полягають у тому, що ви можете ідентифікувати необхідний трафік ще до того, як його підпис буде зіставлено. Основними недоліками цього методу є ймовірність помилкових тривог і низька ефективність.

4) Аналіз поведінки трафіку

Аналіз поведінки трафіку вважається найбільш перспективним методом аналізу в системах управління трафіком DPI, ще одна причина полягає в тому, що можна описати практично будь-яку модель поведінки трафіку з високою швидкістю обробки та високою точністю ідентифікації трафіку. Цей метод підвищує ідентифікацію програм із зашифрованим корисним навантаженням. Для ідентифікації трафіку за аналізом поведінки відстежується час, протягом якого трафік передається, і на основі аналізу поведінки трафіку на цьому сегменті приймається рішення шляхом порівняння з базовим.



2.6. Базовий алгоритм работи DPI-системи

Ідентифікація трафіку на основі аналізу поведінки також може базуватися на наступних критеріях: програма, що генерує трафік, сканує порти; Трафік одного типу надходить з багатьох вузлів; Трафік має певний розмір пакета.

Основними функціями для ідентифікації потоку є[6,7]:

1) порядок розмірів сегментів транспортного шару;

2) послідовність розмірів фрагментів даних;

3) Розміри перших IP-пакетів.

Використовуючи разом інші методи аналізу, можна підвищити точність загального виявлення трафіку. Коли система DPI знаходиться на межі мережі оператора, система працює за наступним алгоритмом.

Таким чином, алгоритм роботи всієї системи виглядає так:

1) Пакет, що виходить з мережі оператора зв'язку або надходить ззовні, спочатку надсилається в обхід. Bypass перевіряє, чи є з'єднання з переднім кінцем;

2) Якщо з'єднання немає, пакет надсилається на прикордонний маршрутизатор і система повертається до початкового стану;

Якщо з'єднання є, пакет передається на головний елемент інтерфейсної системи для подальшого аналізу;

3) Щоб визначити програму, яка створила цей пакет, інтерфейс посилається на базу даних підписів, що зберігаються у внутрішньому елементі. Пакет перевіряється на відомі підписи;

4) Якщо збігів не знайдено, серверна частина зберігає отриманий результат, а пакет надсилається назад на обхід і далі на прикордонний маршрутизатор. Така ситуація можлива, якщо мова йде про нову програму, нову версію програми, нову версію інформаційного елемента, що стосується програми, а відповідний підпис ще не внесено в базу даних. Якщо є збіг підпису пакета, система визначила протокол;

5) На наступному кроці інтерфейс запитує номер політики в PCRF, яку потрібно застосувати до пакета;

6) Інтерфейс запитує деталі політики, збережені у сервері, які відповідають ідентифікатору абонента/типу послуги.

Далі зовнішній пакет позначається відповідно до отриманої мережевої політики. Статистика зберігається у серверній частині, а пакет надсилається на вихід системи.

2.3. Реалізація забезпечення якості обслуговування

Проблему можна вирішити за допомогою комплекту з трьох моделей[6,7]:

1) Послуга найкращих зусиль (доставка даних не гарантована) – ця модель не гарантує доставку даних у реальному часі, інші характеристики та визначений пріоритет, але підтримує зв’язок між вузлами;

2) Інтегровані послуги (Integrated Services) - Ця модель передбачає передбачуване резервування мережевих ресурсів із забезпеченням гарантованої виділеної смуги пропускання на всьому шляху відстеження трафіку. RSVP (протокол резервування ресурсів). Маршрутизатори мають обмежені вичерпні ресурси, що забороняє класифікувати склад усіх можливих потоків додатків у самому пристрої. Цей підхід не масштабується. Підходить для невеликих мереж.

3) Диференційоване обслуговування (диференційоване обслуговування) — передтривожна модель.

У разі перевантаження мережі порядок передачі пакетів через інтерфейс визначає механізм обслуговування черги (механізм черги), який включає наступні механізми обслуговування черги:

1. Механізм FIFO (першим увійшов, першим вийшов) - передача пакетів визначає порядок, у якому пакети надходять у чергу, тобто. Х. пакет, який надійшов першим, обробляється раніше, ніж другий пакет. Цей механізм не поділяє пакунки на класи, а розглядає їх як належні до одного класу[6,7];

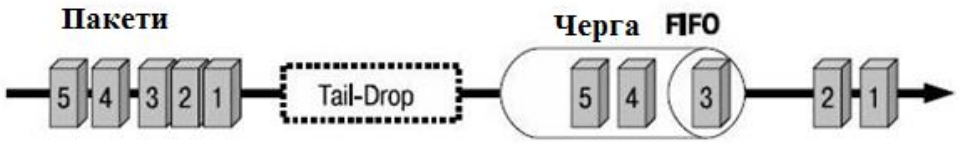


Рис. 2.7. Черга FIFO

2. Пріоритетний механізм черги. Передбачається наявність 4 черг, що відповідають пріоритетам обслуговування: високий, середній, нормальний і низький. Пакети з низьким пріоритетом обслуговуються лише після вичерпання черги з високим пріоритетом[6,7];

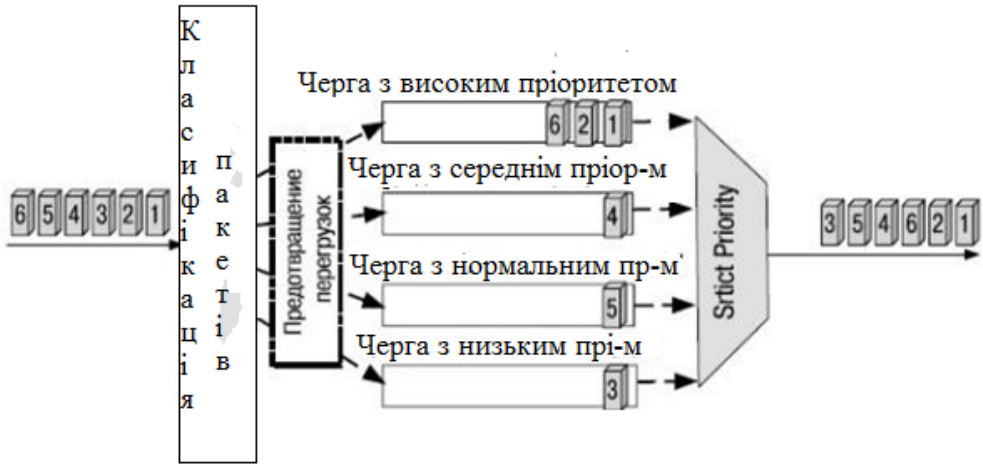


Рис. 2.8. Черги пріоритетів з жорстким режимом

3. Алгоритм круглого обслуговування (Weighted Round Robin, WRR) - забезпечує обробку пакетів відповідно до визначеного вагового коефіцієнта та забезпе-

чує пропускну здатність для пакетів із пропорційно розподіленим коефіцієнтом;

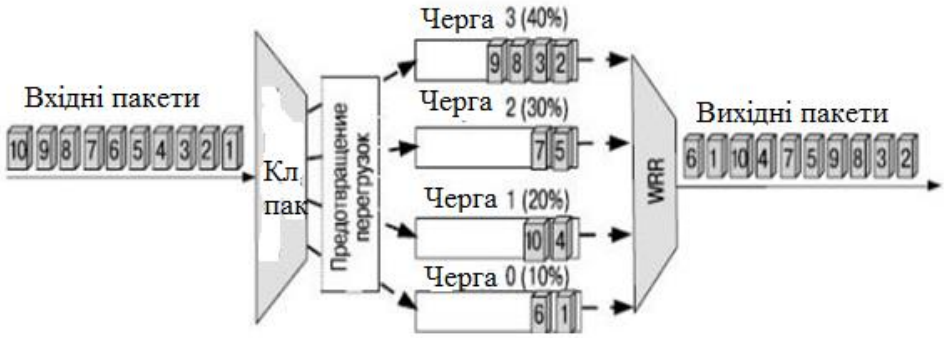


Рис. 2.9. Алгоритм кругового обслуговування

Настроювана черга - надається керування розподілом пропускної здатності каналу для кожної черги. Підтримуються 17 відділів. Системна черга 0 зарезервована для високопріоритетного керування пакетами (похідна маршрутизація тощо).

Механізм пересилання перевантажувача — це процес вибору пакетів із відключення перевантажувачів у мережі у випадку, якщо вихідні черги досягають максимальної довжини.

«Tail-Drop» Коли всі вихідні черги переповнюються, усі оброблені пакети відкидаються, і це триває, доки довжина черги не зменшиться.

Алгоритм випадкового раннього виявлення (RED) видаляє оброблені пакети на основі вирівнювання середнього розміру. Він не чекає, поки черги повністю заповняться, а починає відбирати пакети з іншою ймовірністю, коли середній розмір перевірки черги перевищує певний мінімальний поріг. Основним ін-

струментом обмеження трафіку є алгоритм «token bucket».

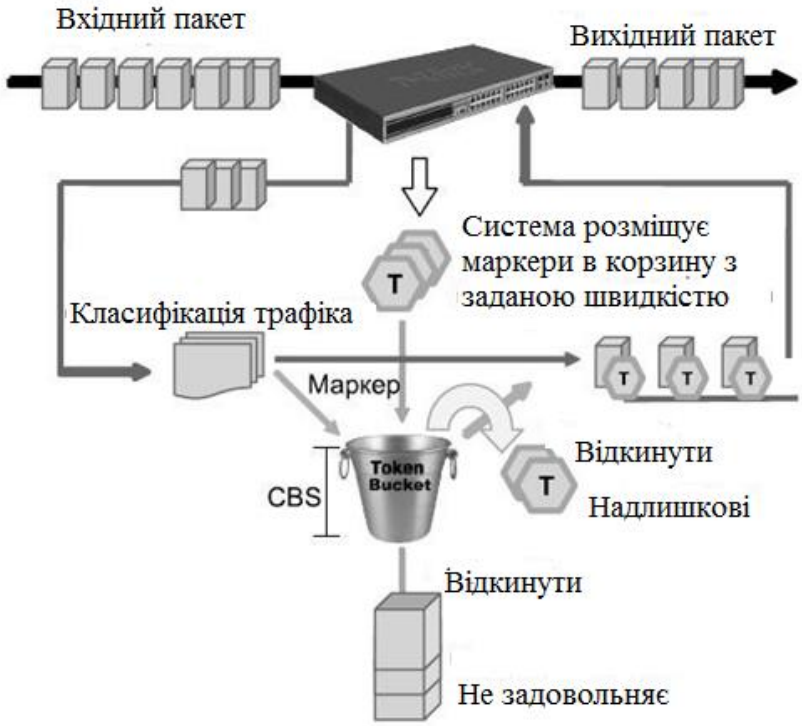


Рис. 2.10. Алгоритм "корзина маркерів"

Даний алгоритм передбачає наявність наступних параметрів[6,7]:

1) Committed Information Rate (CIR) – середня швидкість передачі трафіку. Якщо кошик переповнюється, жетони прогресу скидаються;

2) Committed Burst Size (CBS) - обсяг трафіку (в бітах), до якого може бути розширений бак маркера в даний момент часу;

3) Extended Burst Size (EBS) — це обсяг трафіку (у бітах), на який можна збільшити розмір кошика токенів у надзвичайних ситуаціях.

Для передачі посилки необхідно доставити кількість жетонів з кошика,

дорівнює розміру пакета в бітах. Якщо в кошику достатньо маркерів, пакет переміщається. Якщо розмір пакунка виявиться більшим за теги в кошику, теги не будуть видалені з кошика, пакунок вважатиметься зайвим і може бути відірваний або перенаклеєний.

В якості механізму агрегації трафіку використовується шейпінг, а також використовується алгоритм «маркування кошика», оскільки пакети, для яких недостатньо позначок у кошику, не відхиляються, а ставляться в чергу (буферизуються) для подальшої передачі. Після того як у кошику накопичено кількість токенів, достатню для передачі пакета, він передається.

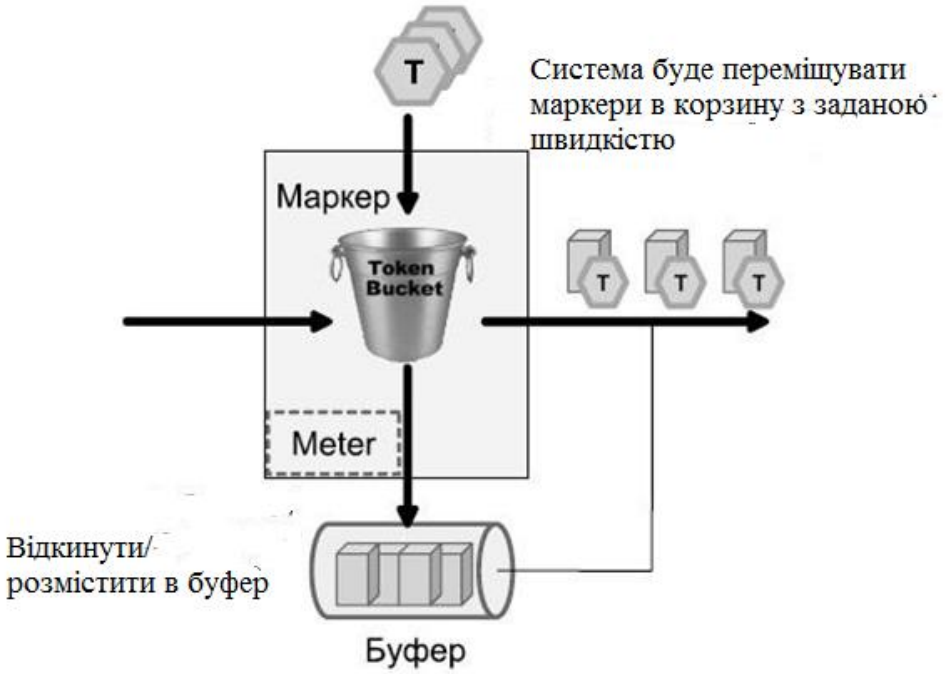


Рис. 2.11. Алгоритм "корзина маркеров" в рамках механизма Traffic Shaping

Як наслідок, через мережі операторів зв’язку передається все більш різноманітний трафік і зростає потреба в інтелектуальному управлінні цим обсягом даних. Такі методи дозволяють позначати, обмежувати різні типи програм і застосовувати політики QoS.

Одним із підходів до оптимізації передачі трафіку є:

Тимчасова доставка ресурсів у зону пріоритетного класу руху

залежно від важливості, чутливості до того чи іншого параметра.

Щоб зрозуміти процес пріоритезації трафіку системи DPI, необхідно розглянути вже існуючі можливості покращення якості обслуговування за допомогою пріоритетів.

Класифікація пакетів - це механізм отримання пакета певного класу трафіку.

При обробці пакетів необхідно маркувати пакети. Позначення зазвичай виконується на пристроях Edge за допомогою списків контролю доступу (ACL, AccessControlLists) у snaDme.

Найважливішими ідентифікаторами для управління трафіком є[6,7]:

1) реалізація апріорів у канальних протоколах;

Відповідно до стандарту IEEE 802.3 Ethernet організація IEEE (Інститут інженерів з електротехніки та електроніки) розробила стандарт для створення віртуальних локальних мереж IEEE, де вихідний кадр Ethernet містить додаткове чотирибайтове поле тегу VLAN, це це позначення пріоритету (Priority) класу обслуговування (Class of Service - CoS) IEEE 802.1p.

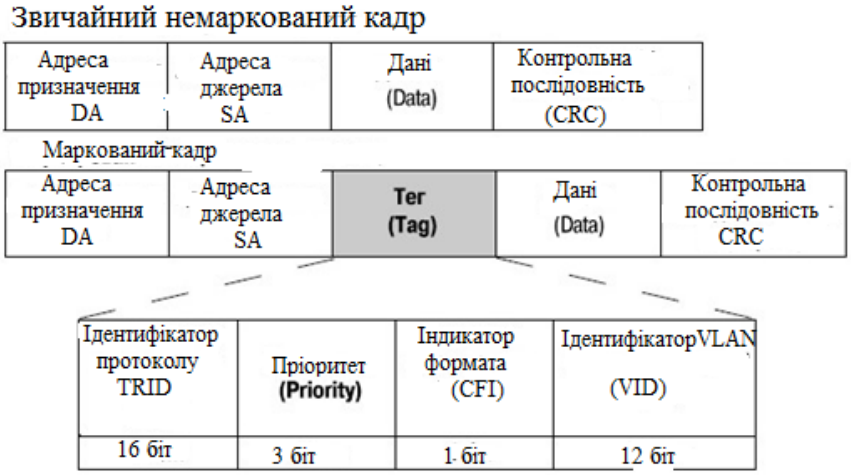


Рис. 2.12. Структура кадру Ethernet стандарту IEEE 802.3 и 802.1p/802.1q

1) Реалізувати пріори в протоколах одного віку;

В IPv4 для маркування виділено поле – TypeofService (ToS, Тип обслуговування) розміром один байт.

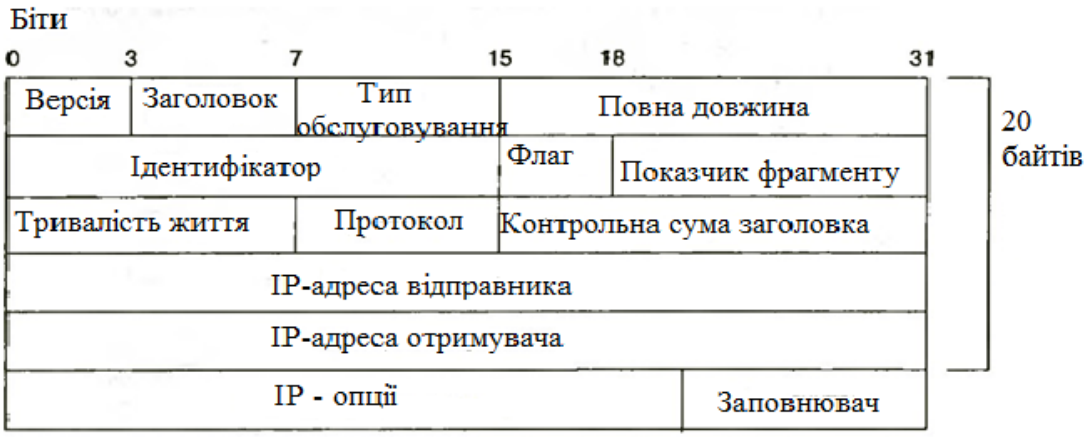
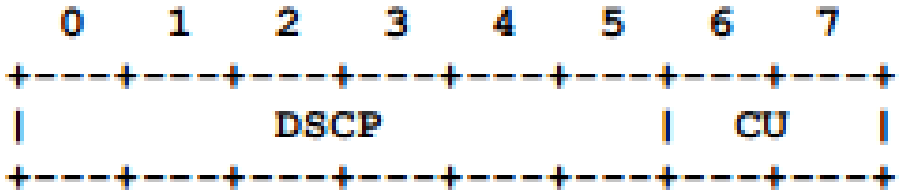


Рис. 2.13. Формат заголовка пакета IPv4

Поле «Тип служби» містило класифікатор пріоритету IP-адреси, але пізніше було замінено на DSCP (точка коду DiffServ).

Пріоритет IP (IPP) потрібен для трьох бітів перед пакетом. Біти C (вартість), D (затримка), T (пропускна здатність) і R (надійність) доступні заздалегідь. Пріоритет IP 6 і 7 зарезервовано для інформації про мережу (оновлення маршруту, приватні пакети), інші шість значень пріоритету представляють звичайний IP-Verkehrsströme zur Verfügung.

Рис. 2.14. Формат поля Тип обслуговування



Якщо вибрано TOS, потрібен код DSCP (Differentiated Services Code Point). DSCP відноситься до моделі DiffServ і складається з 6 біт, що дозволяє пакетам отримувати значення пріоритету від 0 до 63. За замовчуванням перші шість бітів дорівнюють нулю. Двобітове поле CU зарезервовано[6,7].

У протоколі IPv6 поле «Клас трафіку» використовується для встановлення пріоритетів. Довжина поля становить 8 біт, перші 6 біт використовуються DSCP для класифікації пакетів, а два біти використовуються для контролю перевантаження.

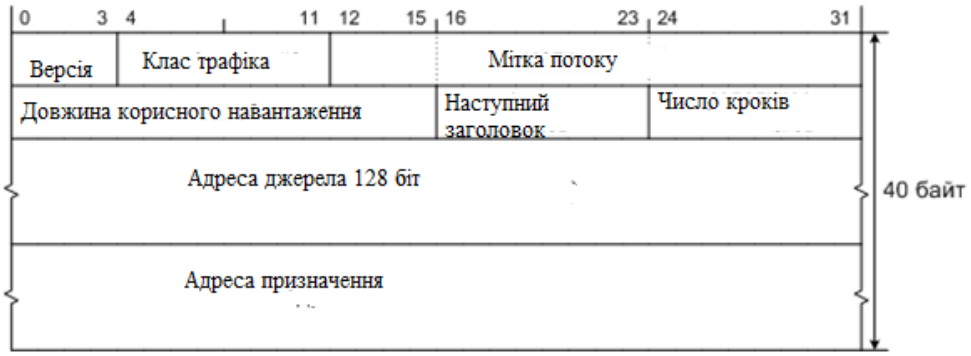


Рис. 2.16. Формат заголовка пакета IPv6

1. Реалізація пріоритетів у протоколах транспортного рівня;

У протоколі TCP (Transmission Control Protocol) заголовок містить 6-бітне поле з прапорцями, які допомагають контролювати трафік. Наприклад, у випадку значення PSH одержувач повинен передати ці дані програми якомога швидше.

Для виконання завдання забезпечення необхідної якості обслуговування в мережах доцільно використовувати механізми якості, які забезпечують необхідні показники QoS при раціональному використанні ресурсів мережі.

Щоб співвіднести трафік з таким класом і виконати необхідні дії, необхідно визначити його тип (голос, дані, відео), для цього використовується технологія DPI.

Якщо DPI підлаштовується під оператора, роздільна здатність каналу буде іншою. Глибока перевірка пакетів виконується за допомогою методів, контролю трафіку та різноманітних блокуючих пристроїв. За допомогою глибокої перевірки пакетів можна визначити кількість матеріалу.

Крім того, налаштувань DPI недостатньо для вирішення наступних проблем[8,9]:

1. Неправильні рішення при застосуванні неправильних вказівок;

2. Затримки в обробці пакетів;

3. Просування нових видів шифрування трафіку;

4. Дестабілізація ринку через домінування пріоритетних протоколів.

ВИСНОВКИ ДО РОЗДІЛУ 2

1.У розділі аналізуються основні особливості та можливості технології глибокого аналізу пакетів, актуальність застосування технології для аналізу даних, перспективи її використання в телекомунікаційному середовищі, а також застосування технології глибокого аналізу пакетів для маркування трафіку.

2. Необхідно оцінити можливість використання системи DPI для ідентифікації трафіку в мережі та використання цієї технології для забезпечення якості обслуговування.

3. Завдяки технології DPI і рішенням на її основі можна виконувати важливі завдання для юридичних і фізичних осіб:

• Моніторинг і запобігання несанкціонованому трафіку даних;

•Покращення показників QoS

• Перехоплення мережевих пакетів з юридичних причин.

• Управління якістю Інтернет-послуг.

• Пріоритезація веб-сервісів.

• Збір статичних даних з мережі.

4. DPI вирішує наступні завдання QoS:

• Пріоритезація та сегрегація трафіку.

• Організація єдиного транспортного потоку.

• Підвищення якості та швидкості мережевого з'єднання.

• Уникнення перевантаження мережі.

РОЗДІЛ 3

ПОБУДОВА АЛГОРИТМІВ З ТЕХНОЛОГІЄЮ DPI

3.1. Загальна модель використання DPI у стільниковій мережі

Модель використання технології DPI включає робоче місце користувача, мережу доступу та програмне забезпечення DPI, розташоване в хмарі (рис. 3.1).

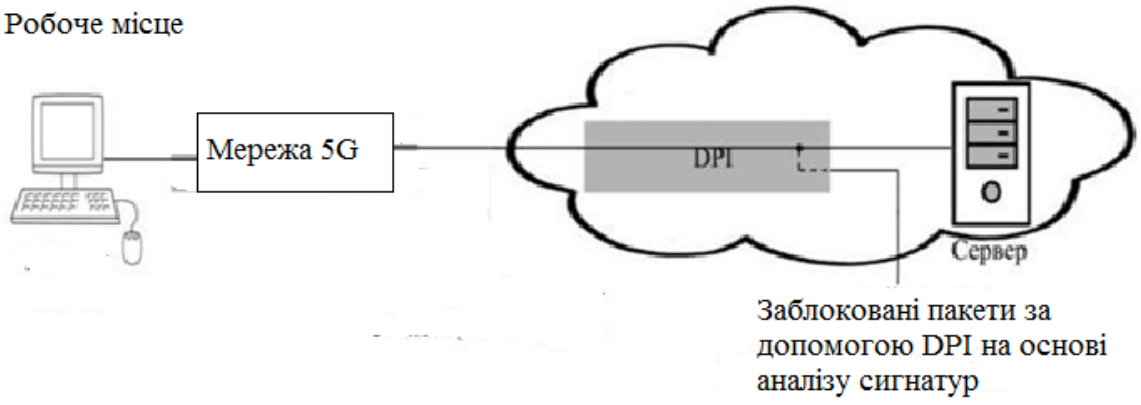
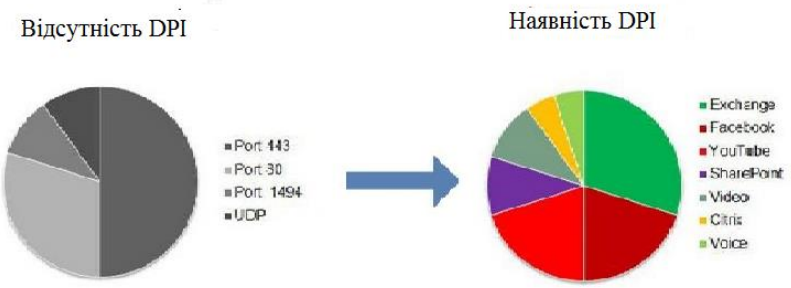


Рисунок 3.1. Модель використання технології DPI

Система DPI відображає інформацію про мережу з можливістю сортування за залученими програмами, протоколами, хостами чи портами, а також може записувати трафік і збирати статистику[9].



Існує кілька способів аналізу трафіку[9,10]:

1. Згідно з протоколами

2. Підпис

3. Евристика

Щоб забезпечити індикатори QoS, метод, який раніше базувався на створенні черг із призначенням пріоритету трафіку, тепер оператори можуть контролювати знищення підключених каналів за допомогою глибокої перевірки пакетів на рівні програми.

Основним методом DPI є перевірка підписів протоколу та програми. Підпис — це шаблон опису даних, який однозначно відповідає програмі/протоколу. Наприклад, це може бути пошук за такими ключовими словами в даних PaILet, Ilak BitTorrent або запитах GET/POST протоколу HTTP. Найпростіші підписи базуються на URL-адресі в HTTP-заголовку, а сам файл підпису постачальника регулярно оновлюється.

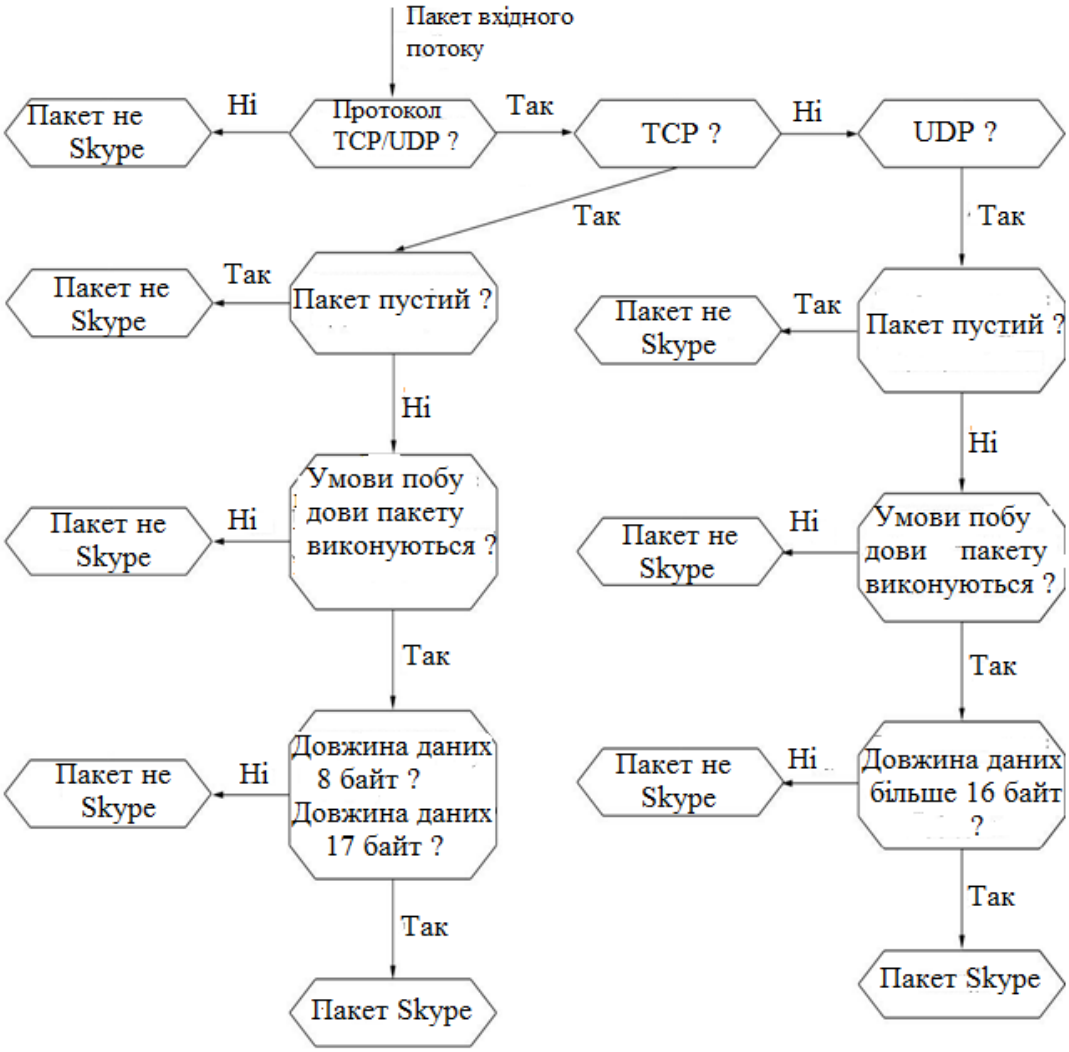
TCP - протокол керування передачею. протокол керування передачею. Він служить для забезпечення та встановлення надійного зв'язку між двома пристроями та надійної передачі даних. У той же час протокол TCP контролює оптимальний розмір пакета даних, що передається, і створює новий пакет у разі помилки передачі.

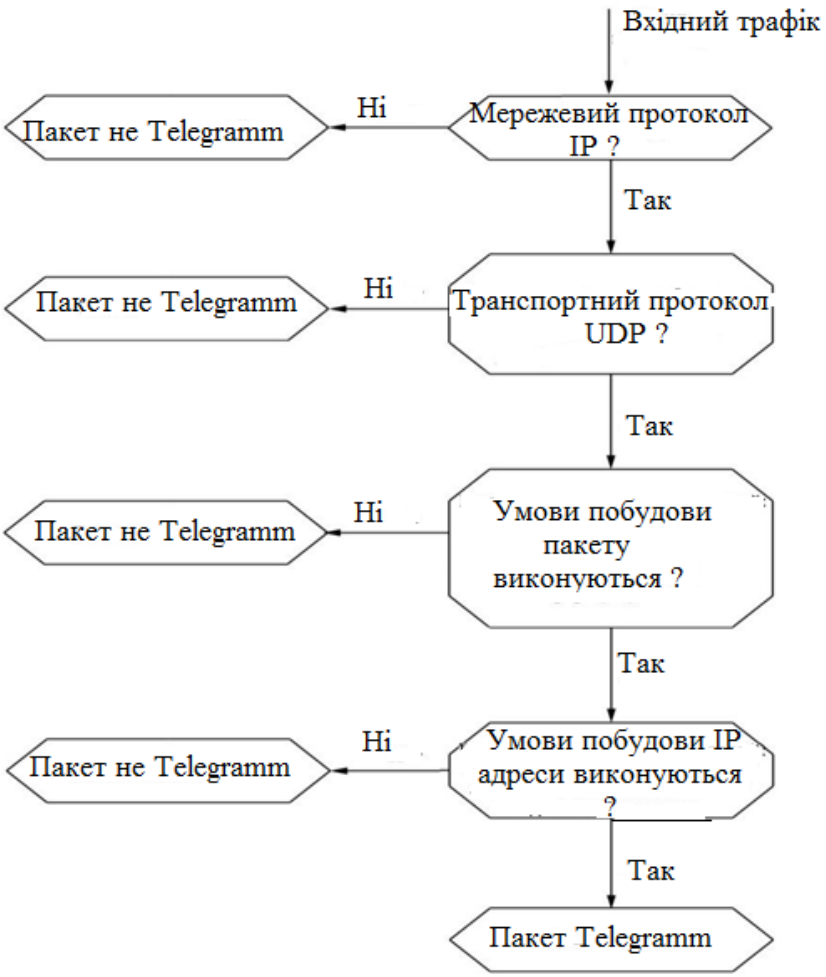
IP - Інтернет-протокол. Інтернет-протокол або протокол адреси є основою всієї архітектури передачі. Протокол IP служить для доставки мережевого пакета даних на потрібну адресу.При цьому інформація розбивається на пакети, які самостійно рухаються по мережі до потрібного адресата. Частина методів DPI базується на статистичних і поведінкових критеріях аналізу потоку даних. Це поведінковий аналізатор, який дозволяє виявляти сканування портів з одного джерела.

У більш складних випадках підпис базується на аналізі параметрів підключених потоків програми. Усі ці підписи використовуються для виявлення IP-адрес і транспортних портів, які використовує потік програми для подальшого контролю потоку даних: статистика , тарифікація, моніторинг або блокування. Створені підписи зберігаються в банках підписів.

Для прикладу розглянемо реакцію системи на три різні типи трафіку від трьох різних популярних OTT-сервісів: Skype, Telegram, Vyber.

Для виявлення пакетів необхідно виділити або встановити необхідні сигнатури, характерні для аналізованого трафіку. Тому пропонується наступний алгоритм аналізу трафіку Skype (рис. 3.2):





3.2. Результати використання запропонованих алгоритмів DPI

Оскільки нам необхідно перевірити надійність ідентифікації OTT-сервісів існуючими системами DPI, тобто наскільки точно ми можемо виявляти різні програми за допомогою цієї системи, ми проведемо експериментальне тестування.

Для проведення експерименту використовувалася передова система DPI з відкритим кодом для аналізу трафіку та перевірки правильності та повноти письмового підпису. Також для перевірки коректності системи DPI використовувався сніффер Wireshark.

Програма Wireshark призначена для захоплення, запису та аналізу мережевого трафіку, тобто є сніфером (сніфером) і аналізатором. З Wireshark ви можете:

перехоплювати мережевий трафік і обмінюватися захопленими пакетами;

відображення вмісту пакетів у структурованому вигляді та «як є»;

підбирати мережеві пакети за гнучкими критеріями;

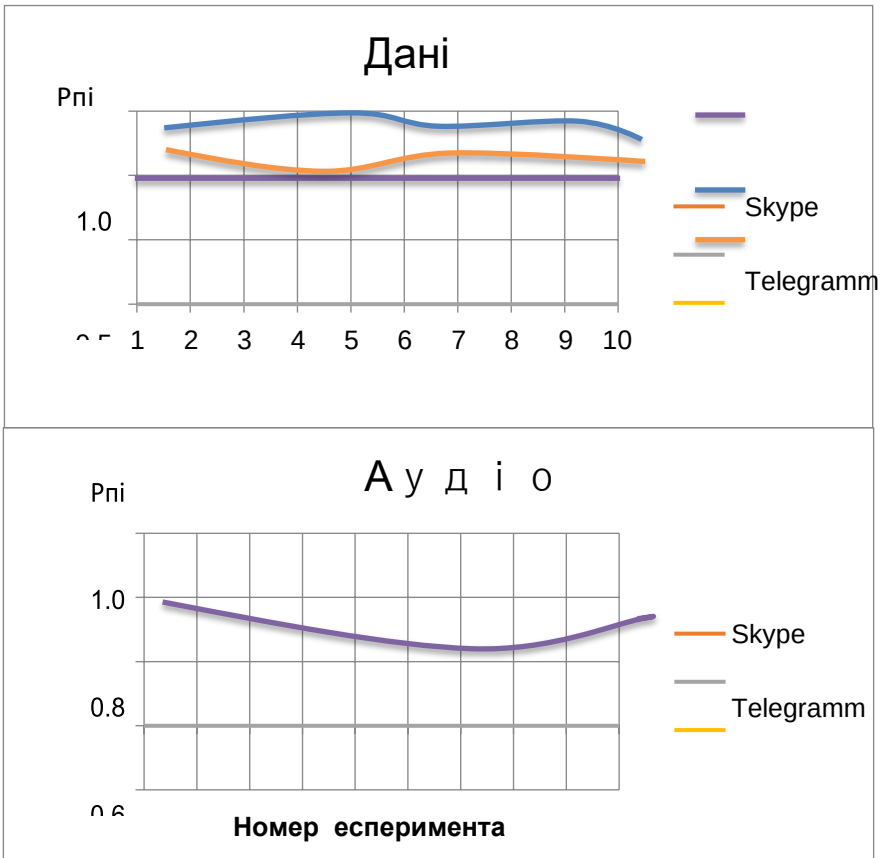
Аналізуйте окремі пакети, сесії та статистику багатьох пакетів;

відновлює потоки даних, розташовані в наборах пакетів.

Для прикладу розглянемо реакцію системи на три різні типи трафіку від трьох різних популярних OTT-сервісів (Skype, Telegram? Viber).

Ці алгоритми показують, що існує значна розбіжність у методах перевірки руху. Перевіримо валідність цих підписів під час експерименту. Було проведено понад 100 експериментів з перевірки прийняття заяв через систему DPI.

Той самий файл розміром 1,7 МБ було передано для ідентифікації даних, той самий 20-секундний звук відтворювався для мови та 20-секундна передача для відео. Результати наведено на графіках (рис. 3.5).



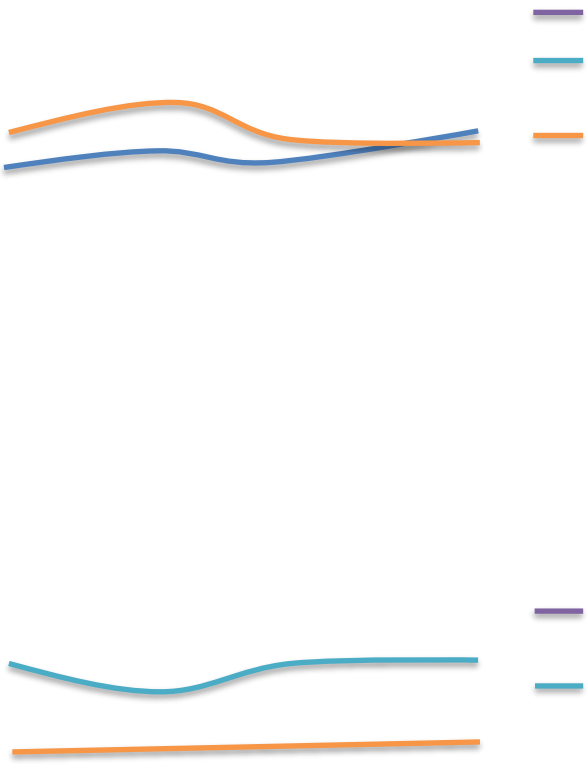


Рис. 3.5. Графики, отражающие вероятность срабатывания системы в результате эксперимента

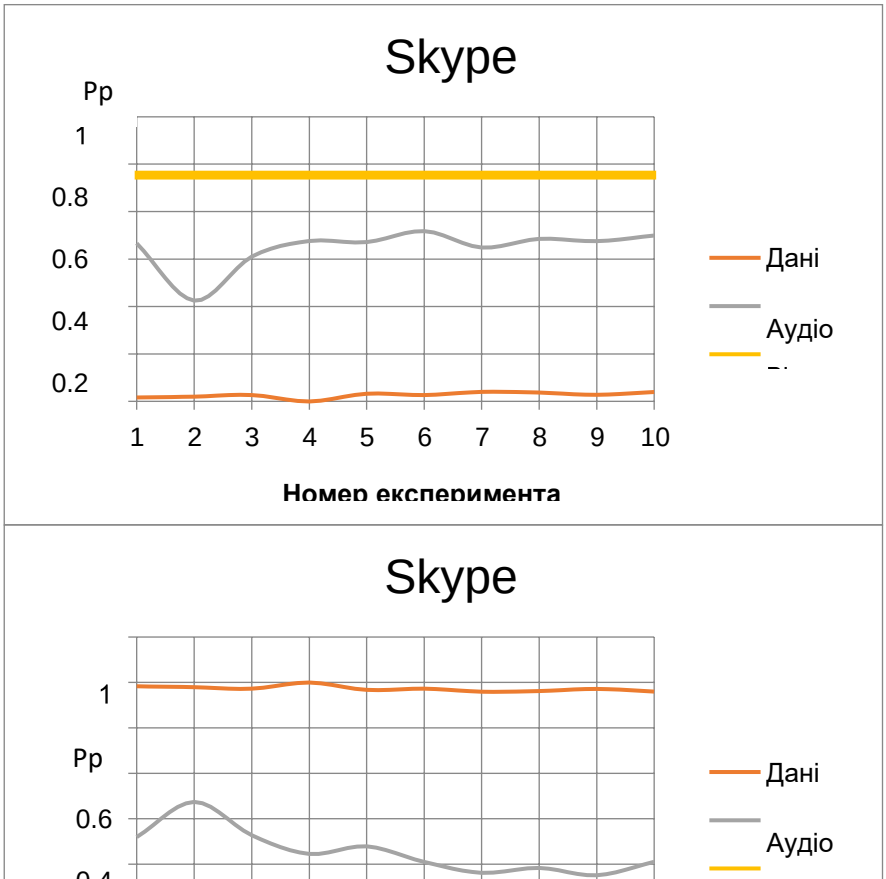


Таблица 3.1. Значення ймовірності правильної ідентифікації OTT- сервисов.

Додаток	Вид трафіка	Середнє значення	Дисперсія значення	Розмах варіації	Середнє відхилення	Відносна варіація	Коефіцієнт варіації
Skype	Дані	0,9231	0,0002	0,0402	0,0092	0,0001	0,0126
	Аудіо	0,8564	0,0096	0,3230	0,0710	0,0188	0,3826
	Відео	0,4282	0,0007	0,0128	0,0050	0,0003	0,1351
Telegramm	Дані	0,6131	0,0011	0,0039	0,0034	0,0011	0,1234
	Аудіо	0,3611	0,0021	0,0048	0,0015	0,0023	0,1728
	Відео	0,2501	0,0004	0,0056	0,0017	0,0040	0,2110
Viber	Дані	0,3123	0,0006	0,0064	0,0022	0,0017	0,0000
	Аудіо	0,4170	0,0070	0,2060	0,0660	0,0724	1,7547
	Відео	0,2510	0,0009	0,0102	0,0020	0,0051	3,1623

Таблица 3.2. Значення ймовірності помилкової ідентифікації

Додаток	Вид трафіка	Середнє значення	Дисперсія значення	Розмах варіації	Середнє відхилення	Відносна варіація	Коефіцієнт варіації
Skype	Дані	0,0369	0,0002	0,0402	0,0090	0,0028	0,4564
	Аудіо	0,1575	0,0070	0,2932	0,0810	0,0054	0,1288
	Відео	0,5465	0,0000	0,0205	0,0140	0,0000	0,0073
Telegramm	Дані	0,2810	0,0000	0,0272	0,0041	0,0000	0,0080
	Аудіо	0,5081	0,0001	0,0264	0,0080	0,0000	0,0090
	Відео	0,2030	0,0000	0,0221	0,0050	0,0000	0,0070
Viber	Дані	0,3010	0,0000	0,0000	0,0000	0,0000	0,0000
	Аудіо	0,3080	0,0610	0,8075	0,1392	0,0361	0,2940
	Відео	0,2040	0,0000	0,0443	0,0120	0,0001	0,0150

Таблица 3.3. Значення ймовірності неспрацювання

Додаток	Вид трафіка	Середнє значення	Дисперсія значення	Розмах варіації	Середнє відхилення	Відносна варіація	Коефіцієнт варіації
Skype	Дані	0,0500	0,0000	0,0000	0,0010	0,0000	0,0000
	Аудіо	0,0501	0,0030	0,1751	0,0870	0,0155	0,5679
	Відео	0,0611	0,000046	0,0204	0,0150	0,0015	0,4438
Telegramm	Дані	0,1208	0,0001	0,0272	0,0040	0,0024	0,6339
	Аудіо	0,2079	0,0514	0,5600	0,1720	0,2181	1,9239
	Відео	0,6069	0,0000	0,0221	0,0050	0,0033	0,9839
Viber	Дані	0,4011	0,0000	0,0000	0,0010	0,0000	0,0000
	Аудіо	0,3044	0,2405	1,6748	0,2770	0,3951	1,6113
	Відео	0,5501	0,0003	0,0529	0,0120	0,0051	0,6385

3.2. Результати статистичного аналізу

Наведені розрахунки показують, що для ймовірності правильного виявлення трафіку розкид середніх значень для різних типів трафіку надзвичайно великий, що може свідчити про відсутність позитивної системності в роботі системи DPI при виявленні різних типів трафіку та програм.

Слід зазначити, що при однаковому підписі різні типи трафіку мають різні значення ймовірності правильної ідентифікації трафіку, що свідчить про необроблений підпис і неможливість використання одного підпису для різних типів трафіку в контексті цю програму.

Результати досліджень.

1. Аналіз підписів різних OTT-сервісів показує, що в Skype, як це було вже давно, існуючі додатки для підписів розвинені значно краще, ніж у нових додатках (з досліджуваних), в яких підписи зараз обробляються менше, що виявляється негативним при впровадженні DPI, системи накладення певних політик на певний тип трафіку (трафік, що залежить від програми).

2. Дослідження показали, що для програм із слабко обробленими підписами неможливо використовувати DPI для ідентифікації служб OTT через упущення та неправильні рішення через близькість або фальшивість підписів.Таким чином, можна пропустити певний трафік або застосувати до нього неправильні політики, що призведе до спотворення результатів застосування системи.

Рішення цих проблем полягає в наступному:

1. Використання комбінованих методів аналізу трафіку для покращення виявлення трафіку, включаючи ведучий та евристичний аналіз;

2. подальший розвиток підписів;

3. Чітка ідентифікація послуг (з боку постачальника послуг OTT). Співпраця OTT-сервісів з операторами зв'язку необхідна для забезпечення актуальних сигналів та ідентифікаторів.

4. Забезпечення взаємодії не на рівні невідомого трафіку, а на рівні домовленості оператора зв’язку та OTT-сервісів.

Ідентифікація трафіку в загальному потоці за допомогою маркування трафіку вимагає великої надбудови від оператора на кожному крайовому вузлі, що можна легко вирішити в SDN, оскільки правила можна вказати на контролері.

3.3. Формування вдосконаленого алгоритму роботи DPI

QoS (Quality of Service) — здатність мережі обробляти особливо важливий трафік з обмеженими поточними можливостями. QoS надає пріоритет обробці деяких класів даних, коли пропускна здатність маршрутизатора обмежена. Технологія вміє розставляти пріоритети, визначає, який трафік є більш важливим для користувача, і виділяє значну кількість пропускної здатності для користувача. При правильному налаштуванні QoS потокове відео відтворюватиметься без затримок під час завантаження великого файлу, а відеоконференція в

ZOOM не буде зависати, навіть коли колеги в сусідньому офісі дивляться Netflix. Ми детально пояснюємо, як це працює. Як працює QoS У більшості випадків якість інтернет-трафіку визначається 4 параметрами[9,10]:

1. Бітрейт або швидкість передачі даних - визначає максимально допустиму швидкість обробки трафіку. Зазвичай вимірюється в мегабітах на секунду - Мбіт/с

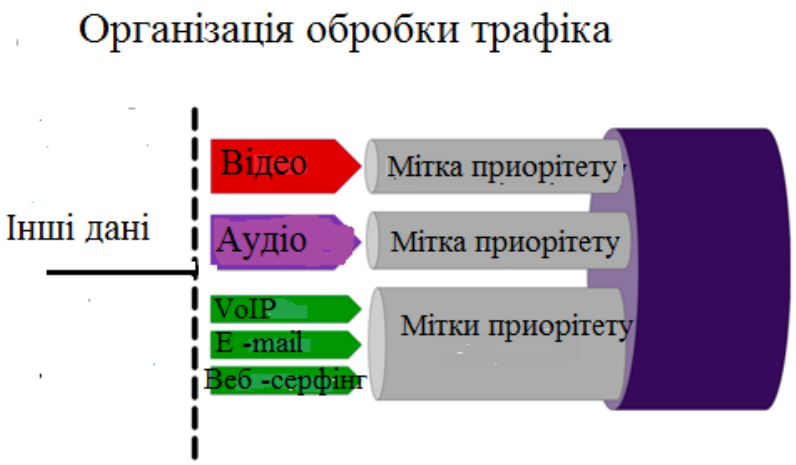
2. Величина затримки в передачі пакета даних. Зазвичай вимірюється в мілісекундах.

3. Індикатор джиттера - це коливання фази цифрового сигналу

4. Кількість втрачених даних.

Якщо мережа в офісі сильно завантажена, будь-який з цих параметрів може постраждати, користувач отримає неякісне інтернет-з'єднання - гальмуватиме відео, не завантажуватимуться файли, дзвінки. QoS допомагає вирішити цю проблему. Він ефективно розподіляє пропускну здатність і визначає пріоритет трафіку.Уявімо, що канал зв'язку - це труба, а її діаметр - її пропускна здатність. Інтенсивний трафік може спричинити затори на вході цієї труби, свого роду ефект «вузького місця». Зазвичай у такій ситуації під час прийому та відправлення даних через маршрутизатор діє принцип звичайної черги: перший прийшов, перший обслужений.

Якщо даних забагато, усі пакети, які не потрапили до буфера черги, будуть втрачені. QoS усуває цю проблему, застосовуючи принцип «інтелектуальної черги». Він визначає пріоритетність пакетів даних на основі мітки типу послуги, призначеної кожному Paket призначається.



Дані з міткою нижчого пріоритету ставляться в чергу та очікують, поки пропускна здатність покращить класифікацію даних. QoS передбачає розподіл вхідного трафіку за допомогою засобів класифікації. Це дозволяє мережевому адміністратору контролювати доступ і визначати пріоритет більш важливих програм. Вхідні пакети даних можна класифікувати за портом, IP-адресою, назвою програми, користувачем. управління чергою. Коли трафік класифікується, інструменти черги та керування смугою пропускання отримують правила для керування трафіком. Адміністратор визначає, якому типу пакетів даних надається вищий пріоритет і яка пропускна здатність виділяється для пріоритетних черг. QoS зберігає пакети даних із нижчим пріоритетом у черзі «кому», доки мережа не буде готова їх прийняти. Це означає, що програми з високим пріоритетом отримують необхідну пропускну здатність, а пакети даних з нижчим пріоритетом не втрачаються й обробляються, коли мережа готова. Інструменти регулювання дорожнього руху. QoS дозволяє уникнути перевантаження мережі та керувати трафіком за допомогою ряду інструментів. Використовуючи цей механізм, технологія пакетної черги може: формувати трафік, обмежувати швидкість з'єднання, збільшувати використану пропускну здатність, планувати пропускну здатність тощо.

Коли QoS важливий?

Деякі мережеві програми вимагають пріоритетного керування вхідними пакетами даних, щоб забезпечити їх правильну роботу.Сюди входять додатки потокового медіа та сервіси потокового передавання, такі як IPTV або Netflix.Вони споживають значну частину пропускної здатності мережі, і без визначення пріоритетів за високого навантаження IP-телефонія та служби відеоконференцій, такі як Zoom або Slack, можуть не працювати. Через високу затримку та коливання мережі пакети VoIP відкидаються, що призводить до переривання відеовикликів і переривання конференцій додатків, які вимагають гарантованої надійності та безперебійної передачі даних. Наприклад, веб-камери систем безпеки, засоби дистанційної хірургії, автоматизовані системи управління виробництвом тощо. Моделі QoS BES – Best Effort Service. Проста модель розширення пропускної здатності, не пов'язана з пріоритезацією трафіку та маркуванням окремих типів даних. Зазвичай використовується для невимогливих програм, які нечутливі до низьких швидкостей передачі даних, великих затримок і тремтіння. IntServ - інтегрований сервіс. Модель резервування ресурсів за протоколом RSVP: перед відправленням пакету даних протокол інформує мережу про параметри трафіку та рівень застосування QoS.Після отримання початкових параметрів мережа резервує певну кількість пропускної здатності відповідно до запитуваних вимог протоколом і з урахуванням заданих параметрів Після отримання інформації про зарезервовані ресурси програма надсилає мережеві пакети даних на задані параметри DiffServ - Differentiated Service.Модель диференціації ресурсів і класифікації пакетів. Технологія поділяє трафік на класи та групи та виконує певний набір дій для кожного класу та призначає рівень QoS. Ця модель є найбільш вдалим прикладом інтелектуального управління чергою пакетів даних і пріоритезації трафіку. Позначає пакети даних, керує інтенсивність мережевого трафіку, розподіляє ресурси та застосовує політику відхилення пакетів. Як QoS розподіляє трафік? Класифікація є основою технології QoS. Залежно від параметрів, установлених адміністратором, пакети даних можна класифікувати за: IP-адресою місця призначення даних вхідного інтерфейсу, значенням MRLS, ECR, кодом кла-

сифікації CoS тощо. Маршрутизатор класифікує вхідний трафік і призначає його кожному з класи, а потім позначає це пакетами даних. Тег допомагає мережевим маршрутизаторам визначати та ставити в чергу дані. За допомогою маркування мережа розпізнає трафік у кожній зоні, а QoS допомагає пристроям у мережі правильно застосовувати правила пріоритету.

QoS може обробляти черги наступним чином[9,10].

1. Немає черг FIFO. Модель обробки, яка застосовується, коли QoS вимкнено. Працює простий принцип: першим обробляється пакет даних, який першим надходить у мережу, і в цій моделі немає пріоритетів. Схема моделі FIFO — відсутність черг і пріоритетів. Дійсний, коли QoS вимкнено для мережі.

2. PQ — це черга із суворим пріоритетом. Модель, де мережа розділяє пакети даних на класи - кожен клас має свій власний пріоритет. Мережа спочатку обробляє дані з мережі з найвищим пріоритетом і так далі в порядку спадання.Поки пакети даних найвищого пріоритету не будуть оброблені, трафік, що залишився, заморожено і чекає своєї черги. Схема моделі PQ, в якій дані обробляються відповідно до пріоритету. Коли мережа завантажена пріоритетним трафіком, вона обробляє весь інший трафік.

3. Колова система. Модель, де кожна черга відповідає мережі, і кожній черзі виділяється однаковий час обробки. Черги формуються на етапі класифікації. Якщо в черзі закінчуються пакети даних до закінчення терміну дії черги, мережа переходить до наступної черги. Чим більша черга пакетів, тим більше часу потрібно для обробки.

4. FQ - це чесна черга. Принцип черги та обробки такий же, як і в циклічній системі. З тією різницею, що той самий пакет даних обробляється з кожної черги одночасно. Мережа обробляє дані не за часом або кількістю пакетів, а за певною кількістю бітів. Чим більший пакет даних знаходиться в даній черзі, тим довше триває його обробка.

Схема моделі FQ. Він базується на принципі чесної обробки даних. Черга з більшим обсягом буде в черзі довше.

5. WRR – Weighted Round Robin Модель, де кожній черзі виділяється власний час для обробки даних, а кожна черга має власне значення. Чим вищий час обробки даних для даної черги, тим вищий її пріоритет. Мережа обробляє пакети даних з найвищим пріоритетом довше, ніж інші, незалежно від порядку, в якому ці пакети даних надходять у мережу.

6. WFQ — це зважена чесна черга. Модель, у якій пакети даних із кожної черги приймаються мережею послідовно. При цьому пріоритет надається чергам залежно від кількості даних у черзі. Враховуючи цей пріоритет, мережа визначає, скільки даних із заданої черги вона обробить за один цикл. Мережа обробляє дані за принципом справедливості з урахуванням пріоритетів, призначених чергам.

Перераховані вище 6 моделей обробки черги пакетів даних є класичними. Різні системи використовують гібридні методи роботи з інформацією, які поєднують представлені вище моделі.

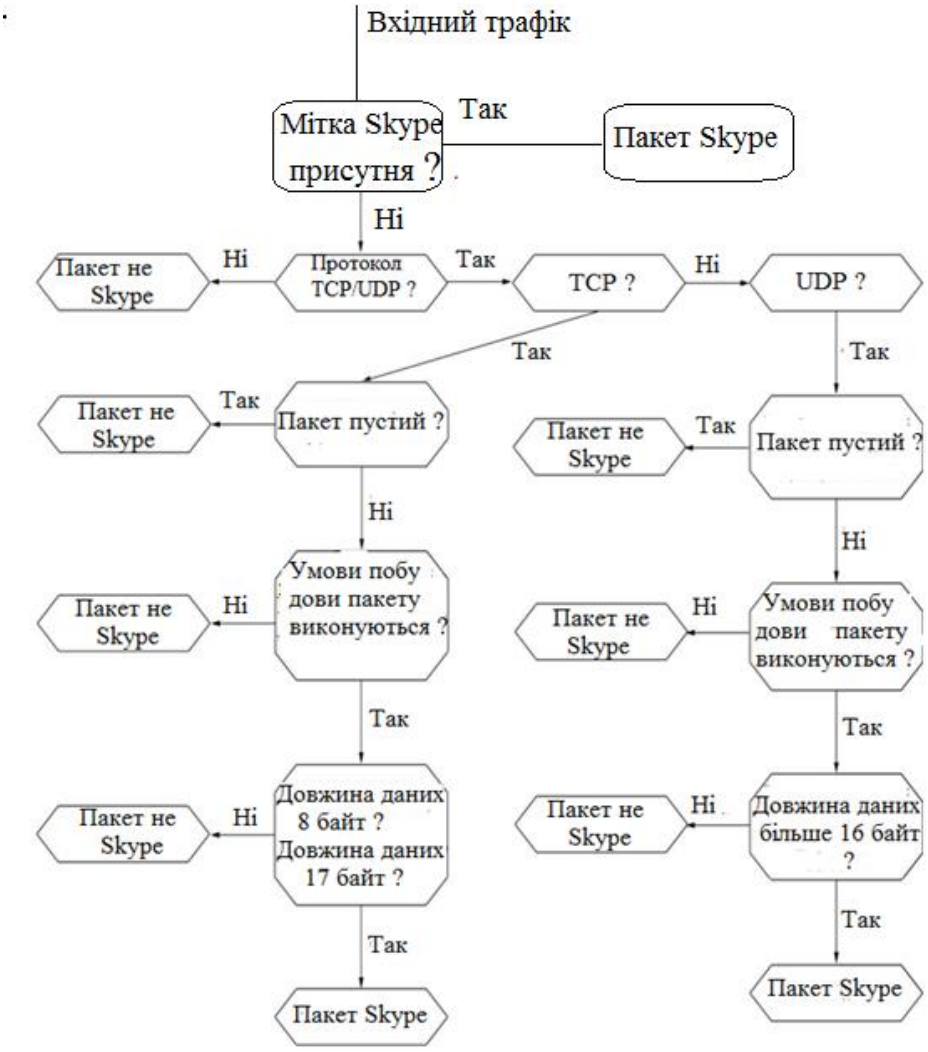


Рис.3.7. Алгоритм роботи технології DPI для ідентифікації трафіку Skype

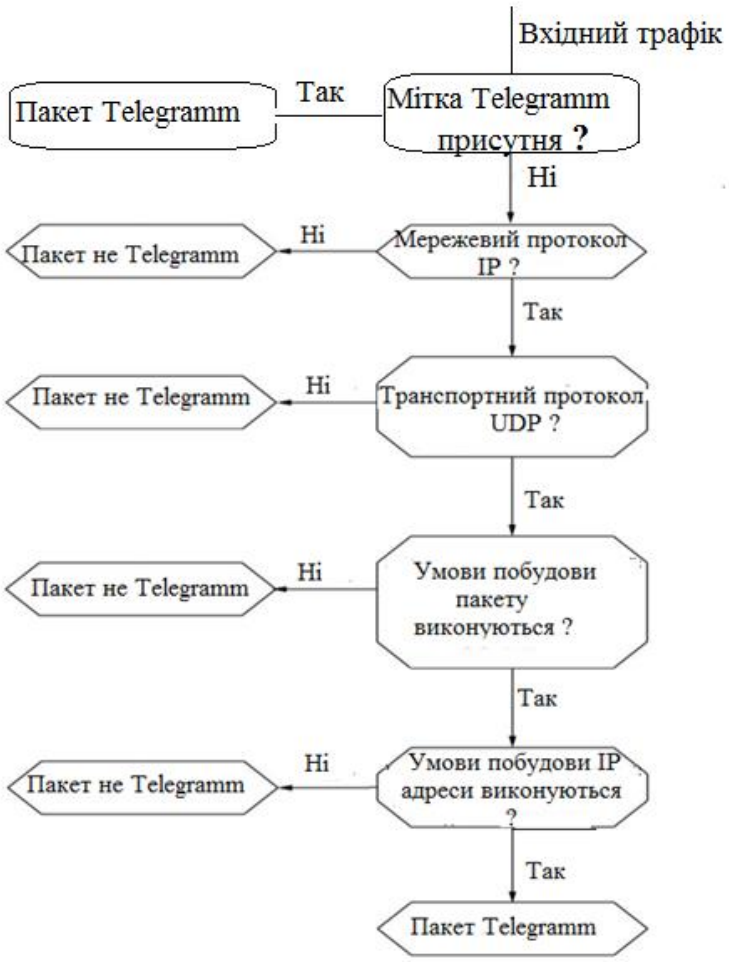


Рис.3.8. Алгоритм роботи технології DPI для ідентифікації трафіку Telegramm

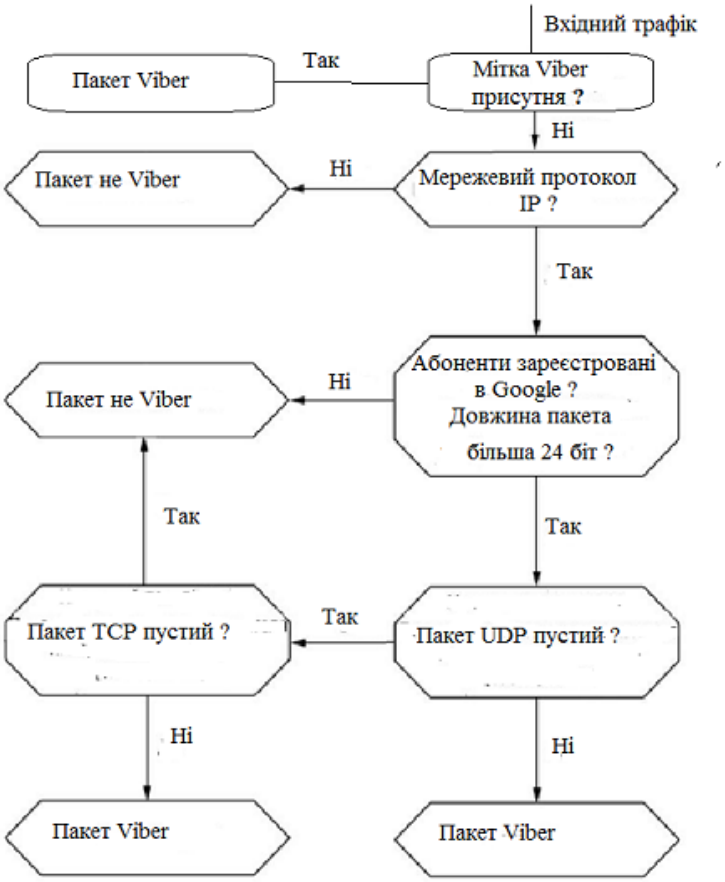


Рис.3.9. Алгоритм роботи технології DPI для ідентифікації трафіку Viber

В результаті повторного експерименту отримані статистичні дані приведені у таблиці 3.4.

Таблиця 3.4. Значення ймовірності правильної ідентифікації

Додаток	Вид трафіка	Середнє значення	Дисперсія значення	Розмах варіації	Середнє відхилення	Відносна варіація	Коефіцієнт варіації
Skype	Дані	0,9631	0,0002	0,0402	0,0092	0,0001	0,0126
	Аудіо	0,9164	0,0096	0,3230	0,0710	0,0188	0,3826
	Відео	0,7982	0,0007	0,0128	0,0050	0,0003	0,1351
Telegramm	Дані	0,9131	0,0011	0,0039	0,0034	0,0011	0,1234
	Аудіо	0,6411	0,0021	0,0048	0,0015	0,0023	0,1728
	Відео	0,6801	0,0004	0,0056	0,0017	0,0040	0,2110
Viber	Дані	0,6423	0,0006	0,0064	0,0022	0,0017	0,0000
	Аудіо	0,6270	0,0070	0,2060	0,0660	0,0724	1,7547
	Відео	0,5810	0,0009	0,0102	0,0020	0,0051	3,1623

Таблиця №3.3. Порівняльні результати використання алгоритму з міткою трафіка

	Skype		Telegramm		Viber	
	Традиційний алгоритм	Алгоритм з міткою	Традиційний алгоритм	Алгоритм з міткою	Традиційний алгоритм	Алгоритм з міткою
Дані	0,9231	0,9631	0,6131	0,9131	0,3123	0,6423
Аудіо	0,8564	0,9164	0,3611	0,6411	0,4170	0,6270
Відео	0,4282	0,7982	0,2501	0,6801	0,2510	0,5810

ВИСНОВКИ ДО РОЗДІЛУ 3

1. У цьому розділі пропонується використовувати сигнатурний аналіз згенерованого трафіку за допомогою спеціальної програми сніферної системи DPI «Wireshark».

2. Дослідження показали, що для додатків зі слабко обробленими кадрами підписів неможливо використовувати DPI для ідентифікації служб OTT через пропуски та неправильні рішення через близькість або неправильність підписів.

3. Усунення несправностей дивіться нижче:

- Використання комбінованих методів аналізу traffic для покращення виявлення трафіку, включаючи ведучий та евристичний аналіз;

- додаткова обробка підписів;

- унікальна ідентифікація послуг (з боку постачальника послуг OTT).

- Забезпечення взаємодії не на рівні невідомого трафіку, а на рівні домовленості між оператором зв'язку та OTT-сервісами.

4. Запропоновано алгоритми ідентифікації трафіку з використанням додаткових ідентифікаторів типу трафіку.

РОЗДІЛ 4

ОХОРОНА ПРАЦІ

При роботі з елементами телекомунікаційної мережі, в тому числі з центрами обслуговування абонентів, для яких в даній роботі розробляється алгоритм управління трафіком, необхідно дотримуватись умов і засобів охорони праці, а також належне дотримання всіх норм передбачені чинним законодавством України[12,13].

Тема дипломної роботи – розробка алгоритмів забезпечення якості передачі трафіку в мережі 5G. Отже, відповідно до теми та ефективності дипломної роботи суб’єктом охорони праці є інженер, який досліджує методи підтримки та оцінки якості послуг, розробляє алгоритми та їх моделювання за допомогою персонального комп’ютера та спеціалізованого програмного забезпечення.

4.1. Аналіз умов праці інженера для дослідження методів забезпечення та оцінки якості обслуговування

4.1.1. Організація робочого місця інженера для дослідження методів підтримки та оцінки якості послуг

Інженер виконує роботи, пов'язані з розробкою та моделюванням нових алгоритмів підвищення якості обслуговування в стільникових мережах з використанням спеціального програмного забезпечення. Характеризується як робота із залученням зорового зусилля, помірного нервового напруження і виконується у вільному темпі[12,13].

Робоче місце інженера розташоване в лабораторії телекомунікаційної компанії на третьому поверсі дев'ятиповерхового залізобетонного будинку. Кімната має такі розміри: довжина - 7 м, ширина - 4,5 м, висота - 3,2 м. Загальна площа кімнати: S_(загальна)=31,5 м^2 і загальний об'єм: V_(загальний) =100,8 м^3. У лабораторії є 4 робочих місця, кожне з яких оснащено ПК, екраном і телефо-

ном. Також в приміщенні є БФП (принтер, сканер, ксерокс), яким користуються всі працівники лабораторії. Є система вентиляції.

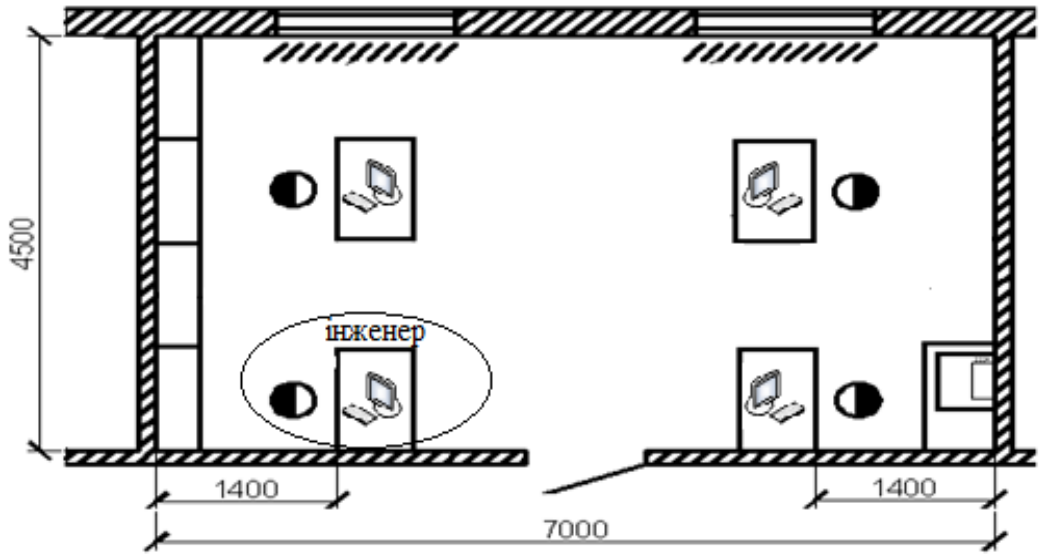


Рис. 5.1. Схема лабораторного приміщення, де працює інженер

Робоча площа на одного інженера складає:

$$S_{\text{роб.}} = \frac{S_{\text{заг.}}}{N} = \frac{31{,}5}{4} \approx 7{,}9 \text{ м}^2 ,$$

а робочий об’єм:

$$V_{\text{роб.}} = \frac{V_{\text{заг.}}}{N} = \frac{100{,}8}{4} = 25{,}2 \text{ м}^3 ,$$

де N – кількість робітників у відділку,

$S_{\text{роб.}}$, $V_{\text{роб.}}$ – площа та об’єм у приміщенні на одного працівника,

$S_{\text{заг.}}$, $V_{\text{заг.}}$ – загальні площа та об’єм приміщення.

Згідно з НПАОП 0.00-1.31-98, робоче місце кожного робітника повинно мати наступні параметри: мінімальна площа – 6 м^2, мінімальний об’єм – 20 м^3. Виходячи з розрахунків, кожне робоче місце даного приміщення задовольняє норми НПАОП 0.00-4.15-98.

4.1.2. Перелік шкідливих і небезпечних факторів виробництва

Під час роботи інженер може зазнавати впливу таких небезпечних і шкідливих виробничих факторів[12,13]:

1) недолік природного освітлення;

2) перевищення рівня шуму на робочому місці;

3) збільшення електромагнітного випромінювання;

4) збільшення статичної електрики;

5) Підвищення або зниження температури повітря в робочій зоні.

4.2. Аналіз шкідливих і небезпечних факторів виробництва на робочому місці інженера для вивчення методів підтримки та оцінки якості обслуговування

4.2.1. Відсутність або недолік природного освітлення

Параметром природного освітлення за замовчуванням є коефіцієнт природного освітлення (KPL). Робоче місце інженера природно освітлюється двома вікнами з боку робочої поверхні. Коефіцієнт природного освітлення регламентується ДБН В.2.5-28-2006 [19]. Робота інженера відноситься до робіт середньої точності (IV розряд зорової роботи, мінімальний розмір об'єкта роздільної здатності 0,5 - 1,0 мм), для яких при використанні бокового освітлення КПО = 1,5%. Фактично – 1,2%. Офісні приміщення мають бічне природне освітлення, яке створює високу освітленість біля вікон і низьку освітленість у глибині приміщення.

4.2.2. Розрахунок природного освітлення робочого приміщення інженера

Проведемо розрахунок фактичного значення коефіцієнта природного освітлення (КПО) офісного приміщення, в якому працює інженер-дослідник, та порівняємо його з нормативами.

Приміщення розмірами $L = 7$ м, $B = 4{,}5$ м, $H = 3{,}2$ м з двома метало-пластиковими вікнами з подвійним склопакетом розміром 1,4×1.5 м. Визначаємо сумарну площу вікон: $S_{\text{вік.}} = 2 \times 1{,}4 \times 1{,}5 = 4{,}2$ м^2. Площа підлоги становить $S_{\text{під.}} = 31{,}5$ м^2.

Нормоване значення КПО для аналітичних лабораторій та проектних кімнат становить: $(\text{КПО})_{\text{норм.}} = 1{,}5\ \%$.

Умовна робоча поверхня розташована на висоті 0,8 м від підлоги, висота підвіконня – 1м, а висота вікон – 1,5 м, тому висота від рівня робочої поверхні до верхнього краю вікна: $h = 1 + 1{,}5 - 0{,}8 = 1{,}7$ м. Розрахункова точка А умовної робочої поверхні знаходиться на відстані 0,5 м найбільш віддаленої від вікон стіни, тобто відстань від точки А до зовнішньої стіни приміщення дорівнює: $b = B - 2 = 4{,}5 - 0{,}5 = 4$ м.

$$\frac{L}{B} = \frac{7}{4{,}5} = 1{,}56 \approx 1{,}5, \quad \frac{B}{h} = \frac{4{,}5}{1{,}7} \approx 2{,}5$$

Світлова характеристика вікон: $\eta_B = 15$.

Визначається відношення: $\frac{b}{B} = \frac{4}{4{,}5} = 0{,}89$.

Визначимо площу стін $S_{\text{стін}}$, стелі $S_{\text{стелі}}$, підлоги $S_{\text{підлоги}}$ та відповідні коефіцієнти відбиття. Бокові стіни мають площу $2 \times 4{,}5$ м $\times\ 3{,}2$ м $= 28{,}8$ м^2, протилежна від вікон стіна, включно з дверима: 7 м $\times\ 3{,}2$ м $= 22{,}4$ м^2, тоді загальна площа стін: $S_{\text{стін}} = 28{,}8 + 22{,}4 = 51{,}2$ м^2.

$S_{\text{стелі}} = S_{\text{підлоги}} = 31{,}5$ м^2.

Для побіленої стелі $\rho_{\text{стелі}} = 0{,}7$; для стін, що пофарбовані світлоблакитною фарбою $\rho_{\text{стін}} = 0{,}6$; а для підлоги $\rho_{\text{підлоги}} = 0{,}25$. Середнє значення коефіцієнта відбиття $\rho_{\text{сер.}}$ стелі, стін, підлоги:

$$\rho_{\text{сер.}} = \frac{\rho_{\text{стелі}} \times S_{\text{стелі}} + \rho_{\text{стін}} \times S_{\text{стін}} + \rho_{\text{підлоги}} \times S_{\text{підлоги}}}{S_{\text{стелі}} + S_{\text{стін}} + S_{\text{підлоги}}} =$$

$$= \frac{0{,}7 \times 31{,}5 + 0{,}6 \times 51{,}2 + 0{,}25 \times 31{,}5}{31{,}5 + 51{,}2 + 31{,}5} = \frac{60{,}645}{114{,}2} = 0{,}531 \approx 0{,}5$$

Значення коефіцієнта r_1 вибираємо для $\frac{B}{h} = 2{,}65$, $r_1 = 1{,}15$. Коефіцієнт світлопропускання матеріалу вікон з подвійним склопакетом з листового віконного скла: $\tau_1 = 0{,}8$; для подвійних металевих рам, що відкриваються, коефіцієнт $\tau_2 = 0{,}85$; для регульованих внутрішніх жалюзі $\tau_3 = 1$. Тоді загальний коефіцієнт світлопропускання вікон:

$$\tau_{\text{заг.}} = \tau_1 \times \tau_2 \times \tau_3 = 0{,}8 \times 0{,}85 \times 1 = 0{,}68$$

Коефіцієнт $К_{\text{буд.}}$, що враховує затінення вікон будівлями, розташованими навпроти, приблизно $К_{\text{буд.}} = 1{,}1$.

Враховуючи реальні умови та характеристики приміщення, розрахуємо необхідну площу вікон для забезпечення бокового природного освітлення:

$$S_{\text{вік. розрах.}} = \frac{(\text{КПО})_{\text{норм}} \times К_з \times \eta_B \times К_{\text{буд.}} \times S_{\text{підлоги}}}{\tau_{\text{заг.}} \times r_1 \times 100} = \frac{1{,}5 \times 1{,}2 \times 6{,}5 \times 1{,}1 \times 31{,}5}{0{,}68 \times 1{,}15 \times 100} = 5{,}7 \text{ м}^2$$ ура-

хуванням реальних умов та характеристик приміщення обраховуємо фактичний коефіцієнт природного освітлення:

$$(\text{КПО})_{\text{Ф}} = \frac{S_{\text{вік.}} \times \tau_{\text{заг.}} \times r_1 \times 100}{К_з \times \eta_B \times К_{\text{буд.}} \times S_{\text{підлоги}}} = \frac{4{,}2 \times 0{,}68 \times 1{,}15 \times 100}{1{,}2 \times 6{,}5 \times 1{,}1 \times 31{,}5} = 1{,}2\ \%$$

Так як фактичне значення КПО менше за нормоване, то це свідчить про те, що в цьому приміщенні недостатня кількість природного освітлення, тому додатково треба застосовувати штучне освітлення.

4.2.3. Підвищення рівня шуму на робочому місці

У кімнаті розташовано 4 робочих місця, кожне з яких обладнано ПК з жорстким диском у системному блоці, трьома вентиляторами охолодження ПК та телефоном. Крім того, поруч працює периферія. Так, у космосі виникають шуми механічного та аеродинамічного походження, широкосмугові з аперіодичним посиленням під час роботи принтерів. Приблизні еквівалентні рівні звукового тиску від джерел шуму, що працюють на робочому місці інженера[12,13]:

1) Принтер - 55 дБА;

2) Сканери - 50 дБА;

3) Вентилятор - 45 дБА;

4) жорсткий диск - 45dBA;

5) Телефон - 70 дБА.

Відповідно до ДСН 3.3.6.037-99 [40] допустимий замінний рівень шуму для робочого місця інженера становить 50 дБА.

Розрахуємо середній рівень шуму на робочому місці при роботі всіх вказаних пристроїв. Рівень шуму від кількох одночасно працюючих некогерентних джерел розраховується за принципом енергетичного підсумовування рівня інтенсивності окремих джерел:

$$L_{(середнє)}=10 \lg \sum_{i=1}^{n} 〖10〗^{(0,1 \times L_i)} \quad (4,1)$$

де L_i – рівень звукового тиску і-го джерела шуму;

n – кількість джерел шуму.

Якщо у формулу (4.1) підставити значення рівня звукового тиску для кожного типу приладу, то отримаємо:

L_Σ=10 lg(〖10〗^5,5+ 〖10〗^5+ 〖10〗^4,5+ 〖10〗^4,5 〖+10〗^7)=70,2 дБ

Якщо є кілька джерел звуку з однаковим рівнем інтенсивності L_i, загальний рівень звуку визначається за формулою L=L_i+10 lgn.У цьому випадку таких джерел 5, тому сумарний рівень шуму:

L=70,2+10lg 〖4=76,2дБ〗

Отримані результати перевищують допустимий рівень, тому в приміщенні необхідні спеціальні заходи шумозаглушення.

4.2.4. Захист від промислового шуму і вібрації

Для зниження рівня шуму в приміщенні рекомендується акустична обробка приміщень, під час якої стелю і верхню частину стін покривають звукопоглинальним матеріалом. Це зменшує інтенсивність відбитих звукових хвиль. Ефективність акустичної обробки приміщень залежить від звукопоглинальних властивостей використовуваних матеріалів і конструкцій, специфіки їх розташування, об'єму приміщення, його геометрії та розташування джерел шуму[14,15].

Іншим варіантом є ізоляція пристроїв, які створюють найбільший шум, наприклад Б. БФП. Їх можна розмістити в окремій кімнаті або обладнати додатковою перегородкою, внутрішні стіни якої обшити звукопоглинаючим матеріалом. Корпус повинен мати достатню звукопоглинальну здатність, не впливати на обслуговування обладнання під час експлуатації, не псувати зовнішній вигляд приміщення.

4.2.5. Захист від електромагнітних полів і радіації

Інженер, який вивчає методи підтримки та оцінює якість обслуговування, щодня працює на ПК зі спеціальним програмним забезпеченням, оточений 3 іншими ПК, які створюють електромагнітні поля та поширюють електромагнітне випромінювання. Підвищений рівень ЕМП шкідливий для здоров'я людини. В першу чергу від цього страждає нервова і серцево-судинна системи, з'являються головні болі і втомлюваність, знижується точність пологових рухів, порушується сон. Електромагнітне випромінювання викликає зміни артеріального тиску, гіпотонію або гіпертонію.

Для захисту працівників лабораторії застосовуються такі методи[14,15]:

1) використання приладів, ЕРС яких мінімальна;

2) кількість випромінювальних пристроїв ЕБМ - необхідний мінімум;

3) перевірка робочих місць;

4) По можливості здійснювати дистанційне керування пристроями, які випромінюють EVM.

4.3. Захист від вогню

Загальні вимоги до системи протипожежного, протипожежного та вибухозахисту регламентовані НАПБ А.01.001-2004 [18]. Причинами пожежі в приміщеннях можуть бути несправності електрообладнання та короткі замикання в електромережі, неналежне виконання працівниками правил пожежної безпеки та порушення правил експлуатації обладнання.

Відповідно до НАПБ В.01.053-2000[14,15] приміщення, в якому працює інженер, за пожежною небезпекою відноситься до категорії Д. У приміщенні, де знаходиться обладнання, знаходяться негорючі рідини та матеріали в холодному стані, кабелі та ел. провідники для приладів і предметів меблів.

В якості основного засобу гасіння використовується порошковий вогнегасник переносний ВП-5, який гасить пожежі класу А, В, С, Е. Крім того, передбачено використання акустичної пожежної сигналізації категорії Л5. Для виявлення

джерел запалювання використовується одноточковий димовий пожежний сповіщувач, який реагує тільки на дим і не спрацьовує при займанні газів або рідин.

Робоче місце інженера знаходиться на 3-му поверсі, тому має бути не менше двох евакуаційних виходів (рис. 4.2) на випадок, якщо під час пожежі один вихід стане непридатним для евакуації.

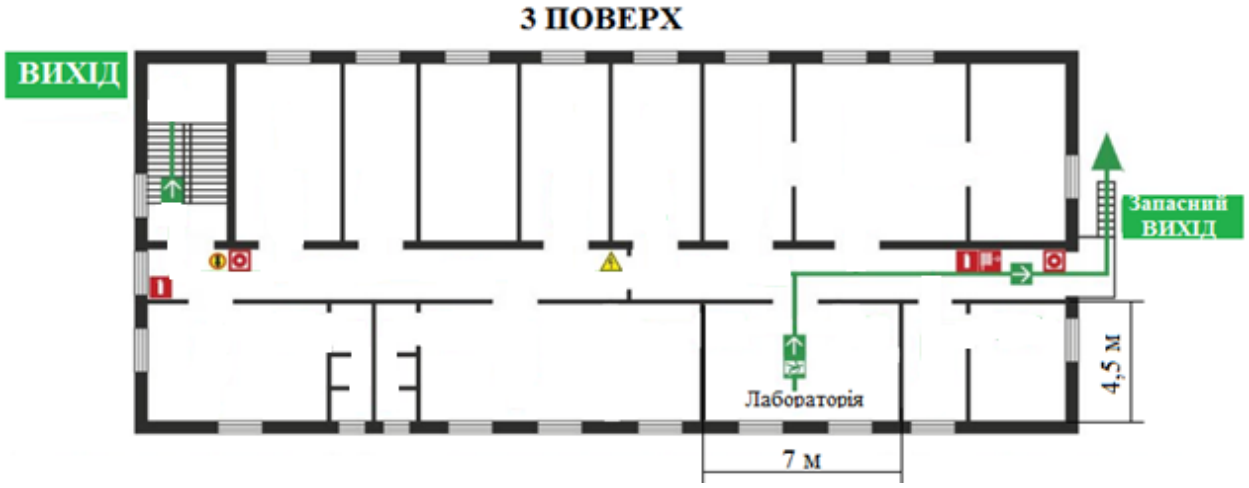


Рис. 5.2. План евакуації з лабораторного приміщення

4.4. Інструкція з охорони праці

Особа, яка приймається на роботу, повинна пройти навчання з охорони праці, промислової гігієни, пожежної безпеки, знати прийоми і методи надання долікарської допомоги постраждалим, правила поведінки в надзвичайних ситуаціях.

Після первинного інструктажу на виробництві робітник повинен пройти стажування під керівництвом досвідченого кваліфікованого робітника протягом 2-15 змін.

Працівник має право відмовитися від дорученої роботи, якщо виникла виробнича ситуація, яка загрожує його життю чи здоров'ю, життю оточуючих і навколишньому природному середовищу.

Вимоги безпеки перед початком роботи:

1. Відвідайте робоче місце. Організувати робоче місце та переконатися, що на робочому місці немає сторонніх предметів, а всі пристрої та блоки ПК під’єднані до системного блоку кабельними роз’ємами згідно зі схемою монтажу.

2. Перевірте:

- справність роз'ємів кабелю живлення та блоків обладнання;

- відсутність обривів і пошкоджень ізоляції силових кабелів;

- відсутність відкритих струмоведучих частин в техніці персонального комп'ютера;

3. Підготувати робоче місце для роботи з приладами типу «Дисплей»:

- відрегулювати сидіння робочого стільця (крісла) на оптимальну зручну висоту; Кут нахилу спинки крісла повинен варіюватися від 90 до 11 градусів. до рівня сидіння;

- Розташуйте крісло та дисплей так, щоб кут огляду на екрані становив 15 градусів, а відстань до екрана 400-800 мм;

- Вжити заходів, щоб при нормальному освітленні робочого місця на екрани не потрапляло пряме світло.

4.Протріть клавіатуру (для зменшення статичної електрики) і зовнішню поверхню екрана злегка вологою серветкою (бязь або марля).

Вимоги безпеки на виробництві

1. Перш ніж підключати шнур живлення до розетки 220 В, переконайтеся, що всі перемикачі живлення на всіх пристроях ПК знаходяться в заземленому (нульовому) положенні.

2. Після того, як ви підключили пристрої ПК до джерела живлення, використовуйте ручки регулювання, щоб відрегулювати яскравість і чіткість зображення VDT відповідно до вашого особливого зору.

3. Не залишайте робоче місце, не попередивши керівника.

4. Не залишайте без нагляду працюючий ПК та його пристрої.

5. Підключайте та від’єднуйте штекери кабелів від пристроїв ПК лише при вимкненому живленні.

6. Подавати напругу в прилади та відключати блоки ПК тільки після ретельної перевірки надійності заземлювачів, працездатності проводів і з’єднань електромережі.

7. Вимкніть ВДТ (відеотермінал) і повідомте про несправність, якщо при його включенні на екрані не з'являється інформація (екран порожній) або в центрі екрана світиться яскрава біла смуга.

8. При виявленні запаху гару в пристроях ПК необхідно негайно вимкнути пристрій, не вмикати його повторно та звернутися до спеціаліста технічної служби ПК.

9. Для операторів ПК ввести дві-три регламентовані перерви по 10 хвилин, при 8-годинному робочому дні – дві, для операторів ПК – три перерви по 2 години 15 хвилин.

10. Кількість оброблених символів (або символів VDT) не повинна перевищувати 30 000 за 4 години роботи.

11. З метою усунення або зменшення нервово-психічної, зорової та м'язової напруги, попередження перевтоми необхідно виконувати комплексні вправи під час чергових перерв, фізкультхвилинок і після закінчення робочого дня.

Вимоги безпеки після закінчення роботи

1. Вимкніть усі тумблери (вимикачі) на обладнанні, з яким ви працювали, а також вимикачі (рубильники) на електрощитах.

2. Вийміть вилки з розеток.

3. Вимкніть вентиляцію.

4. Проводити вологе прибирання робочого місця. Витирайте екран ВДТ від пилу принаймні один раз за зміну. Видаліть пил з обладнання, коли живлення вимкнено.

5. Про виявлені під час роботи недоліки та вжиті заходи щодо їх усунення доповідати керівнику з відповідним записом у трудовій книжці.

6. Вимийте руки з милом.

ВИСНОВКИ ДО РОЗДІЛУ 4

Аналіз умов праці інженера для дослідження методів забезпечення та оцінки якості обслуговування виявив, що фактичний коефіцієнт природного освітлення становить 1,2%, при нормованому значенні КПО = 1,5%, тому достатньо лише природного освітлення. достатній для виконання зорової роботи IV категорії. Загальний рівень шуму в приміщенні становить 76,2 дБА при допустимому рівні 50 дБА, тому необхідно вжити додаткових заходів щодо захисту працівників від шуму та вібрації.

РОЗДІЛ 5
ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА

5.1. Аналіз впливу на навколишнє середовище роботи аналізатора потоку Е1 цифрових телекомунікаційних систем.

Основними складовими частинами аналізатора потоку Е1 є: генератор тестового сигналу, процесор і різноманітні пристрої керування та відображення інформації: клавіатура, дисплей, дисководи для гнучких дисків тощо (рис. 1). Апарат оснащений мережевими фільтрами, джерелами безперебійного живлення та іншими допоміжними електричними пристроями. Під час роботи всі ці елементи утворюють складну електромагнітну обстановку на робочому місці користувача, яка вносить свій негативний внесок у навколишнє середовище[24].

Рис. 1 Зовнішній вигляд аналізатора потоку

До основних факторів, відповідальних за негативний вплив пристрою на навколишнє середовище, відносяться[20]:

1. Електромагнітне випромінювання від генератора тестового сигналу та процесора.

2. Ергономічні параметри екрану[20]:

а) зниження контрастності зображення при інтенсивному зовнішньому освітленні;

б) дзеркальні відбиття від передньої частини екранів;

в) наявність мерехтіння зображення на екрані дисплея;

3. Радіаційні характеристики дисплея:

а) електромагнітне поле монітора в діапазоні від 5 Гц до 1000 МГц;

б) статична електрика на екрані;

в) ультрафіолетове випромінювання в діапазоні 200-400 нм;

г) інфрачервоне випромінювання в діапазоні 1050 нм - 1 мм

Опишемо деякі з перерахованих вище факторів погіршення роботи комп'ютера більш детально.

Під час роботи дисплея на екрані накопичується електростатичний заряд, створюючи електростатичне поле. У різних дослідженнях значення електростатичного поля становили від 8 до 75 м²/м² за різних умов вимірювання. У той же час люди, що працюють з монітором, сприймають електростатичний потенціал.

Помітний внесок у загальне електростатичне поле вносять клавіатури, які електризуються від поверхневого тертя, і сполучні кабелі. Досліди показують, що навіть після роботи з клавіатурою електростатичне поле швидко зростає від 2 до 12 кВ/м. На окремих робочих місцях в руках виміряно напруженість статичного електричного поля понад 20 кВ/м.

Основними джерелами шуму в приміщеннях, обладнаних вимірювальними приладами, є принтери, множинні прилади та кондиціонери, вентилятори систем охолодження та трансформатори в самих приладах.Рівень шуму в таких приміщеннях іноді досягає 85 дБ.

5.2. Вплив електромагнітних полів пристрою на здоров'я користувача

Існує достатньо даних, які свідчать про негативний вплив роботи за комп’ютером на всі життєво важливі системи людини. Крім того, тривалий вплив електромагнітних полів може сукупно стати причиною серйозних захворювань[20].

Фізично людська тканина є парамагнітним матеріалом, тобто її можна «намагнічувати» для відчуття магнітних полів. Медичні дослідження показують, що вплив таких полів викликає зміни метаболізму на клітинному рівні. Електромагнітні змінні поля викликають в організмі людини коливання іонів, що також має певні наслідки.

За загальними даними, функціональні розлади центральної нервової системи зустрічаються в середньому в 4,6 рази частіше, ніж у контрольних групах, захворювання серцево-судинної системи - в 2 рази, захворювання верхніх дихальних шляхів у працюючих до спостереження. від 2 до 6 годин на добу - в 1,9 раза частіше, захворювання опорно-рухового апарату - в 3,1 раза частіше. Зі збільшенням тривалості роботи за комп'ютером різко зростає співвідношення здорових і хворих користувачів.

За даними Бюро статистики праці США, з 1982 по 1990 рік кількість випадків розладу здоров'я користувачів зросла у вісім разів.Встановлено, що частий вплив електромагнітного випромінювання від моніторів також призводить до ненормальних результатів вагітності

Дослідження функціонального стану користувача комп'ютера, проведені Центром електромагнітної безпеки в 1996 році, показали, що навіть при короткочасній роботі (45 хвилин) в організмі користувача під впливом електромагнітного випромінювання монітора відбуваються значні зміни. в гормональному стані і специфічні зміни біострумів головного мозку

Параметри електромагнітних полів монітора, такі як інтенсивність і частота випромінювання, тривалість впливу і модуляція сигналу, частотний спектр і періодичність дії, впливають на біологічну реакцію людини.

5.2. Захист користувача від негативного впливу електромагнітного поля

Дисплеї пристроїв створюють сильне електростатичне поле, яке не є абсолютно безпечним для людського організму. Правда, на відстані 50-60 см від екрану його вплив значно знижується. Загалом, за допомогою спеціальних фільтрів, що покривають екран, можна звести його до нуля. Також варто відзначити, що під час роботи монітора електризується не тільки його екран, але і повітря в кімнаті. Крім того, він набуває позитивний заряд. Позитивно заряджена молекула кисню не сприймається організмом як кисень, що призводить до кисневого голодування у користувача.

Шведські TSO-92, 95, 99 і MPR-II широко визнані як технічні стандарти безпеки моніторів. Вони обмежують параметри випромінювання монітора, енергоспоживання, візуальні параметри тощо. Деякі основні параметри, визначені стандартом MPR, перераховані в таблиці 5.1[21].

Таблиця 5.1

Вимоги до електромагнітного поля дисплея

Найменування параметра	MPRII
Напруженість електромагнітного поля у 50см навколо дисплея по електричній складовій, В/м, не більше в діапазоні частот: • 5Гц – 2кГц • 2кГц – 400кГц	 25 2.5
Щільність магнітного потоку у 50 см навколо дисплея, нТл, не	

більше в діапазоні частот: • Гц – 2кГц • 2кГц – 400кГц	 250 25
Поверхневий електростатичний потенціал, В, не більше	500

Враховуючи всі вищевикладені підсумки, можна зробити висновок про необхідність проведення комплексної оцінки електромагнітного середовища на робочих місцях із засобами вимірювальної техніки (з урахуванням взаємного розташування робочих місць).

По-перше, дослідження показали, що встановлення на екранах фільтрів, які зменшують електричну складову електромагнітного поля в безпосередній близькості від екрана, може призводити до її посилення на відстанях понад 1,0-1,5 м за рахунок перерозподілу поля від екрана вздовж екрана. осі електронно-променевої трубки та з боків від неї.

По-друге, рівень електромагнітного поля сильно залежить від типу та якості проводки. Так, наприклад, у багатьох приміщеннях, де знаходиться техніка, немає загального заземлення, третій контакт роз'єму ПК «висить» у повітрі, що значно підвищує рівень електромагнітного поля. Крім того, низькочастотні поля випромінюють електроприлади, люмінесцентні лампи та пучки кабелів, які часто заплутуються на робочих місцях.

Рекомендації по роботі з приладом[21].

• Неприпустима відстань монітора від користувача становить 0,3 м, критична - 0,5 м, оптимальна - більше 1 м.

• Не залишайте пристрій увімкненим на тривалий час, коли він не використовується. Для дисплея також бажано використовувати «сплячий режим».

• Через максимальне електромагнітне випромінювання генератора тестового сигналу для роботи необхідно використовувати екрановані кабелі.• Оскільки електромагнітне випромінювання також виходить від дисплея, необхідно роз-

ташувати пристрій таким чином, щоб воно не випромінювалося на сусідні робочі місця.

• По можливості слід скоротити час роботи з приладом і якомога частіше переривати роботу.

• Прилад повинен бути заземлений. Якщо є захисний екран, то його також слід заземлити, для цього спеціально передбачений провід, на кінці якого є металева скоба.

ВИСНОВКИ ДО РОЗДІЛУ 5

Рівень впливу на людину електромагнітного випромінювання від телекомунікаційного вимірювального обладнання залежить від випромінювання, яке досягає очей користувачів.

В Україні безпека іонізуючого випромінювання від моніторів комп'ютерів регламентується стандартами НРБУ-97. Стандарти обмежують потужність дози рентгенівського випромінювання до 100 мкР/год на відстані 5 см від поверхні екрана та встановлюють для населення граничну річну еквівалентну дозу опромінення кришталика ока до 15 мЗв. . На практиці, однак, це значення менше і відповідає приблизно 0,7 мЗв. Такий результат свідчить про радіаційну безпеку дисплеїв, оскільки річна еквівалентна доза, накопичена кришталиком ока, у 20 разів менша за допустиму нормами НРБУ-97.

Тому ми охарактеризували аналізатор потоку E1 як джерело забруднення, описали вплив електромагнітних полів пристрою на здоров'я користувача та описали методи захисту користувача від негативного впливу електромагнітних полів пристрою та дисплея.

ВИСНОВКИ

1. Технології п’ятого покоління пропонують величезну ємність даних, необмежену кількість дзвінків і нескінченну передачу даних у новітній мобільній операційній системі. Показники якості передачі трафіку в основному обмежені паразитним і спам-трафіком.

2. За останні 5 років трафік мобільних даних зріс приблизно в 10 разів, причому більшість трафіку становлять відео. VOIP. Згідно зі статистичними даними, наразі більше третини всіх відвідувань веб-сайтів відбувається зі смартфонів (3/4 від загальної кількості) та інших портативних пристроїв. Збільшення трафіку призводить до значного зниження якості передачі контенту. Для вирішення проблеми пропонується використовувати технологію Deep Packet Analysis (DPI).

3. DPI дозволяє вирішувати різноманітні завдання:

• визначення типу трафіку;

• Контроль, розділення та організація єдиного потоку руху;

• уникнення перевантаження мережі;

• Моніторинг і запобігання несанкціонованому трафіку даних;

• Покращення показників QoS;

• Виявлення спаму, вірусної активності, кібератак, несанкціонованого використання інформації та контроль доступу до мережевих сервісів.

• Управління якістю надання послуг Інтернет;

• Пріоритезація веб-сервісів;

• Збір статичних даних з мережі;

• Підвищення якості та швидкості мережевого з'єднання.

4. Кваліфікаційна робота пропонує використання технології DPI у формі сигнатурного аналізу.Дослідження, проведені в рамках роботи, показали, що для додатків зі слабко обробленими підписами використання DPI для ідентифікації мультимедійного трафіку є неефективним через пропуски та неправильні рішення через близькість або неправильність підписів.

Рішення проблем такі:

- Використання комбінованих методів аналізу трафіку для покращення детектування трафіку, включаючи ведучий та евристичний аналіз;

- додаткова обробка підписів;

- унікальна ідентифікація послуг (з боку постачальника послуг OTT).

- Забезпечення взаємодії не на рівні невідомого трафіку, а на рівні угоди між оператором зв'язку та сервісами, що надають контент.

5. Запропоновано алгоритми ідентифікації трафіку з використанням додаткових ідентифікаторів типу трафіку.

6. Проведено експериментальні дослідження запропонованого алгоритму DPI з використанням маркерів трафіку, які показали значне підвищення ймовірності виявлення типу трафіку та його складу, що в кінцевому результаті призвело до покращення показників QoS.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про технологію 5G [Електронний ресурс]. – Режим доступу: https://www.huawei.com/minisite/russia/5g/about.html.

2. Тихвінський, В. О. Мережі мобільного зв'язку 5G: технології, архітектура та послуги = 5G mobile networks. Технології, архітектура та послуги / В. О. Тихвінський, С. В. Терентьєв, В. А. Коваль. - Москва: Медіа Паблішер, 2019. - 375 с. :

3. Мардер Н.С. Сучасні телекомунікації. - М.: APIAC, 2006.-384с.

4. Александров В.В. Якість обслуговування в IP мережах. - М.: "Вільямс", 2003. - 368с.: Іл.

5. Шелухін О.І., Лук'янцев Н.Ф. Цифрова обробка та передача мови. - М.: Радіо і зв'язок, 2000. - 456 с.

6. Забезпечення високої надійності та низької затримки трафіку в 5G NR/H. В. Дупліщева, Є. В. Рогожніков, Е. М. Дмитрієв [та ін.]. - Текст: електронний // T-Comm: Телекомунікації та транспорт. - 2022. - Т. 16. - № 1. - С. 22-29. - URL: https://elibrary.ru/item.asp?id=47809225.

7. Воронцов, Н. Н. Технології мобільного зв'язку п'ятого покоління: аналіз та перспективи розвитку / Н. Н. Воронцов. - Текст: електронний / / Матриця наукового пізнання. - 2021. - № 8-2. - С. 19-22. - URL: https://elibrary.ru/item.asp?id=46483122.

8. Горєлов Г.В., Ромашкова О.М., Чан Туань Ань. Якість управління мовним трафіком у телекомунікаційних мережах - М.: Радіо та зв'язок, 2001. - 112 с.

9. Гольдштейн Б.С., Пінчук О.В. IP-телефонія - М.: Радіо та зв'язок, 2001. - 367с.

10. Гольдштейн Б.С. Протоколи мережі доступу - М.: Радіо та зв'язок, 1999. - 215 с.

11. Яновський Г.Г. Сучасні проблеми науки в галузі телекомунікацій – СПб: СПбГУТ ім. проф. А.Б. Бонч-Бруєвича-2008, 262с.

12. НПАОП 0.00-4.09-07 «Типове положення про комісію з питань охорони праці підприємства». Наказ Держгірпромнагляду від 21.03.2007 р. No 55.

13. НПАОП 0.00-4.11-07 «Типове положення про діяльність уповноважених найманими працівниками осіб з питань охорони праці». Наказ Держгірпромнагляду від 21.03.2007 р. No 56.

14. НПАОП 0.00-4.12-05 «Типове положення про порядок проведення навчання і перевірки знань з питань охорони праці». Наказ Держнаглядохоронпраці від 26.01.2005 р. No 15.

15. НПАОП 0.00-4.15-98 «Положення про розробку інструкцій з охорони праці». Наказ Держнаглядохоронпраці від 29.01.1998 р. No 9.

16. НПАОП 0.00-4.21-04 «Типове положення про службу охорони праці». Наказ Держнаглядохоронпраці від 15.11.2004 р. No 255.

17. НПАОП 0.00-4.33-99 «Положення щодо розробки планів локалізації та ліквідації аварійних ситуацій і аварій. Наказ Держнаглядохоронпраці від 17.06.1999 р. No 112.

18. НПАОП 0.00-6.03-93 «Порядок опрацювання та затвердження власником нормативних актів про охорону праці, що діють на підприємстві». Наказ Держнаглядохоронпраці від 21.12.1993 р. No 132.

19. НПАОП 0.00-6.13-05 «Порядок організації державного нагляду за охороною праці та гірничого нагляду в системі Держнаглядохоронпраці України». Наказ Держнаглядохоронпраці від 30.03.2004 р. No 92.

20. Рекомендації щодо організації роботи кабінету промислової безпеки та охорони праці. Затверджено Головою Держгірпромнагляду 16.01.2008 р.
21. Рекомендації щодо побудови, впровадження та удосконалення системи управління охороною праці. Затверджено Головою Держгірпромнагляду 07.02.2008.

22.Білявський Г.О., Падун ММ., Фурдуй Р.С. Основи загальної екології. — К.: Либідь, 1995. — 368 с.

23.Бойчук Л Д., Соломенно Е.М., Бугай О.В. Екологія і охорона навколишнього середовища: Навч. посіб. — Суми: Університетська книга, 2003. — 284 с.
24.Голубець М А., Кучерявий В.П.,Генсіру к СА. таін. Конспект лекцій з курсу "Екологія та охорона природи** (теоретичні основи загальної екології, охорони природи, комплекс природоохоронних заходів). — К.: УМКВО, 1990. — 216 с.
25.Запольсъкий А.К. Основи екології: Підручник. — К.: Вища шк., 2001. —358 с.
26.Серебряков В.В. Основи екології: Підручник. К.: Знання-Прес, 2002. — 300 с.
27.Сухарев С М., Чудак С О., Сухарева О.Ю. Технологія та охорона навколишнього середовища: Навч. посіб. — Львів: Новий Світ — 2000, 2004. — 256 с.
28.Ісаєнко В.М., Криворотько В.М, Франчук Г.М Екологія та охорона навколишнього середовища. Дипломне проектування: Навч. посіб. – К.: Книжкове видавництво НАУ, 2005. – 192 с.