**Міністерство освіти і науки України**
**Тернопільський національний технічний університет імені Івана Пулюя**

**Факультет прикладних інформаційних технологій та електроінженерії**
(повна назва факультету )
**Кафедра комп'ютерно-інтегрованих технологій**
(повна назва кафедри)

# КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Розроблення та дослідження автоматизованої системи управління виробництвом із використанням технологій мереж наступного покоління (NGN) (комплексна тема)

Виконали: студенти VI курсу, групи КТм-61
спеціальності Автоматизація, комп'ютерно-інтегровані технології та робототехніка
(шифр і назва спеціальності)

_____ Деревяний А.Я.
_____ Павліковський Б.О.
(підпис) (прізвище та ініціали)

Керівник _____ Голотенко О.С.
(підпис) (прізвище та ініціали)

Нормоконтроль _____ Чихіра І.В.
(підпис) (прізвище та ініціали)

Завідувач кафедри _____ Голотенко О.С.
(підпис) (прізвище та ініціали)

Рецензент _____ Трембач Р.І.
(підпис) (прізвище та ініціали)

Тернопіль
2025

**Міністерство освіти і науки України**
**Тернопільський національний технічний університет імені Івана Пулюя**

Факультет **прикладних інформаційних технологій та електроінженерії**
(повна назва факультету)

Кафедра **комп'ютерно-інтегрованих технологій**
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Голотенко О.С.
(підпис) (прізвище та ініціали)
«____» _____ 2025 р.

# ЗАВДАННЯ
## НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 174 Автоматизація, комп'ютерно-інтегровані технології та робототехніка
(шифр і назва спеціальності)

Студенту Деревяному Андрію Ярославовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Розроблення та дослідження автоматизованої системи управління виробництвом із використанням технологій мереж наступного покоління (NGN) (комплексна тема)

Керівник роботи Голотенко Олександр Сергійович, к. т. н., доцент, завідувач кафедри КТ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «12» листопада 2025 року № 4/7-962

2. Термін подання студентом завершеної роботи 15 грудня 2025р.

3. Вихідні дані до роботи вимоги міжнародних стандартів та рекомендацій ITU-T і IETF, технічні характеристики та функціональні можливості обладнання мереж NGN, характер-ки протоколів SIP, RTP/RTCP, MGCP, H.248/MEGACO, SIGTRAN, умови експлуатації обладн.

4. Зміст роботи (перелік питань, які потрібно розробити)

Вступ
Аналітична частина
Технологічна частина
Конструкторська частина
Науково-дослідна частина
Спеціальна частина
Охорона праці та безпека в надзвичайних ситуаціях

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

Титульний слайд
Актуальність роботи
Завдання роботи
Основна частина
Висновки

6. Консультанти розділів роботи

| Розділ | Прізвище, ініціали та посада консультанта | Підпис, дата | |
|---|---|---|---|
| | | завдання видав | завдання прийняв |
| Спеціальна частина | | | |
| Охорона праці та | | | |
| безпека в надзв. ситуаціях | | | |

7. Дата видачі завдання 12 листопада 2025 року

КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів роботи | Термін виконання етапів роботи | Примітка |
|---|---|---|---|
| 1 | Аналіз постановки завдання і огляд матеріалів за | 12.11.2025 | |
| | темою кваліфікаційної роботи | | |
| 2 | Дослідження принципів роботи протоколу Session | 15.11. 2025 | |
| | Initiation Protocol (SIP) | | |
| 3 | Розроблення алгоритму ініціювання, прийняття та | 19.11. 2025 | |
| | завершення SIP-сеансів | | |
| 4 | Реалізація програмного модуля керування SIP- | 23.11. 2025 | |
| | сеансами мовою C# | | |
| 5 | Проведення тестування і аналіз роботи програмного | 30.11. 2025 | |
| | забезпечення | | |
| 6 | Науково-дослідна частина | 03.11. 2025 | |
| 7 | Спеціальна частина | 07.11. 2025 | |
| 8 | Охорона праці та безпека в надзвичайних ситуаціях | 10.12. 2025 | |
| 9 | Оформлення графічної частини | 14.12. 2025 | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Студент _____ Деревяний А.Я.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Голотенко О.С.
(підпис) (прізвище та ініціали)

**Міністерство освіти і науки України**
**Тернопільський національний технічний університет імені Івана Пулюя**

Факультет **прикладних інформаційних технологій та електроінженерії**
(повна назва факультету)

Кафедра **комп'ютерно-інтегрованих технологій**
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Голотенко О.С.
(підпис) (прізвище та ініціали)
«____» _____ 2025 р.

# ЗАВДАННЯ
## НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 174 Автоматизація, комп'ютерно-інтегровані технології та робототехніка
(шифр і назва спеціальності)

Студенту Павліковському Богдану Олександровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Розроблення та дослідження автоматизованої системи управління виробництвом із використанням технологій мереж наступного покоління (NGN) (комплексна тема)

Керівник роботи Голотенко Олександр Сергійович, к. т. н., доцент, завідувач кафедри КТ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «12» листопада 2025 року №_4/7-962

2. Термін подання студентом завершеної роботи 15 грудня 2025р.

3. Вихідні дані до роботи вимоги міжнародних стандартів та рекомендацій ITU-T і IETF, технічні характеристики та функціональні можливості обладнання мереж NGN, характер-ки протоколів SIP, RTP/RTCP, MGCP, H.248/MEGACO, SIGTRAN, умови експлуатації обладн.

4. Зміст роботи (перелік питань, які потрібно розробити)

Вступ

Аналітична частина

Технологічна частина

Конструкторська частина

Науково-дослідна частина

Спеціальна частина

Охорона праці та безпека в надзвичайних ситуаціях

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

Титульний слайд

Актуальність роботи

Завдання роботи

Основна частина

Висновки

6. Консультанти розділів роботи

| Розділ | Прізвище, ініціали та посада консультанта | Підпис, дата | |
|---|---|---|---|
| | | завдання видав | завдання прийняв |
| Спеціальна частина | | | |
| Охорона праці та | | | |
| безпека в надзв. ситуаціях | | | |

7. Дата видачі завдання 12 листопада 2025 року

КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів роботи | Термін виконання етапів роботи | Примітка |
|---|---|---|---|
| 1 | Аналіз постановки завдання і огляд матеріалів за | 12.11.2025 | |
| | темою кваліфікаційної роботи | | |
| 2 | Проведення аналітичного огляду сучасних концепцій | 15.11. 2025 | |
| | мереж наступного покоління (NGN), | | |
| 3 | Проєктування архітектури мережевого комплексу на | 19.11. 2025 | |
| | основі NGN | | |
| 4 | Розрахунок ємнісних, сигнальних і транспортних | 23.11. 2025 | |
| | параметрів мережі | | |
| 5 | Обґрунтування вибору апаратного забезпечення NGN | 30.11. 2025 | |
| 6 | Науково-дослідна частина | 03.11. 2025 | |
| 7 | Спеціальна частина | 07.11. 2025 | |
| 8 | Охорона праці та безпека в надзвичайних ситуаціях | 10.12. 2025 | |
| 9 | Оформлення графічної частини | 14.12. 2025 | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Студент _____ Павліковський Б.О.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Голотенко О.С.
(підпис) (прізвище та ініціали)

*АНОТАЦІЯ*

Кваліфікаційна робота магістра складається з пояснювальної записки та графічної частини (ілюстративний матеріал – слайди).

Об’єм графічної частини дипломної роботи становить 11 слайдів.

Об’єм пояснювальної записки складає 101 друкованих сторінок формату А4.

В роботі використано 31 літературне джерело.

Головною метою роботи є проєктування, дослідження та обґрунтування автоматизованого мережевого комплексу на основі технологій мереж наступного покоління (NGN).

У роботі проаналізовано основні принципи побудови мереж NGN, їхню функціональну архітектуру, класифікацію та характеристики обладнання.

Виконано проєктування мережевої конфігурації NGN для заданої зони автоматизації, проведено розрахунок навантаження шлюзового обладнання, гнучкого комутатора та транспортної пакетної мережі з урахуванням параметрів трафіку та вимог до якості обслуговування.

Досліджено особливості протоколу ініціювання сесій SIP, розглянуто його методи, структуру повідомлень та механізми встановлення з’єднань. Реалізовано програмні алгоритми ініціювання, приймання та відхилення SIP-сесій у середовищі C# з використанням бібліотеки Konnetic Unity SIP .NET SDK, а також описано основні параметри конфігурування SIP-застосунків.

Отримані результати підтверджують доцільність використання мереж наступного покоління як базової телекомунікаційної платформи для автоматизованих систем управління та мультисервісних застосунків. Запропоновані рішення можуть бути використані під час проєктування та модернізації корпоративних і операторських мереж зв’язку, а також у навчальному процесі.

Ключові слова: NGN, SOFTSWITCH, SIP, VOIP, ШЛЮЗ ДОСТУПУ, ПАКЕТНА МЕРЕЖА, СИГНАЛІЗАЦІЯ, МУЛЬТИСЕРВІСНА МЕРЕЖА.

*ЗМІСТ*

# ВСТУП

Стрімкий розвиток цифрових технологій, зростання обсягів мультимедійного трафіку та ускладнення вимог до якості передавання інформації формують нові виклики для телекомунікаційної інфраструктури [1-4, 29]. Традиційні мережі з комутацією каналів поступово вичерпують свій технічний потенціал, оскільки вони проєктувалися переважно під вузький спектр послуг і не забезпечують достатньої гнучкості, масштабованості та ефективності в умовах конвергенції голосу, відео й даних. У цих умовах перехід до мереж наступного покоління (NGN, Next Generation Networks) набуває особливої актуальності як для операторів зв'язку, так і для корпоративного сектору та систем автоматизації [5-7].

Концепція NGN розглядається як ключовий етап еволюції телекомунікацій, що базується на пакетній передачі даних і передбачає інтеграцію різнорідних сервісів у єдиному функціональному середовищі. Архітектура NGN забезпечує відокремлення рівня послуг від транспортного рівня, підтримує різні технології доступу та створює основу для швидкого впровадження нових сервісів без суттєвих змін у транспортній інфраструктурі. Важливою перевагою NGN є підтримка механізмів керування ресурсами та гарантованої якості обслуговування (QoS), що має критичне значення для сервісів реального часу (VoIP, відеоконференції, інтерактивні мультимедійні застосунки) та для мереж, які обслуговують автоматизовані системи управління [7].

Для України модернізація телекомунікаційної інфраструктури є стратегічно важливим завданням, оскільки забезпечує інтеграцію в глобальний цифровий простір, підвищення надійності зв'язку, розширення спектра доступних послуг та імплементацію міжнародних стандартів. Впровадження NGN дає можливість оптимізувати використання мережевих ресурсів і експлуатаційні витрати, а також підвищити керованість, відмовостійкість і безпеку інфраструктури [4, 30] Окрім телекомунікаційного

контексту, NGN є важливою платформою для розвитку «розумних» міст, інфраструктур Інтернету речей (IoT), хмарних рішень, а також для побудови масштабованих корпоративних мереж і комплексів автоматизації [8].

Метою даної роботи є побудова та дослідження автоматизованого мережевого комплексу на основі технологій NGN, який може бути використаний для практичних задач у виробничій, сервісній та управлінській інфраструктурі. Для досягнення мети необхідно вирішити комплекс взаємопов'язаних завдань, що охоплюють аналіз принципів побудови NGN, вибір і класифікацію ключового обладнання (softswitch, шлюзи, сервери додатків, компоненти безпеки), проєктування мережевої конфігурації, розрахунок пропускної здатності для користувацького та сигнального трафіку, а також обґрунтування застосування протоколів сигналізації (зокрема SIP) і реалізацію прикладних алгоритмів встановлення та обробки сеансів зв'язку.

Об'єктом дослідження є мультисервісна телекомунікаційна інфраструктура на основі NGN. Предметом дослідження виступають методи проєктування NGN-мереж для автоматизованих систем, принципи розподілу функцій між рівнями архітектури, а також параметри й механізми передавання сигнального та користувацького трафіку. Практична цінність роботи полягає в отриманих розрахункових і структурних рішеннях, які можуть бути використані як основа для модернізації існуючих мереж, інтеграції різних сегментів доступу та впровадження сервісів реального часу з урахуванням вимог до QoS, надійності та інформаційної безпеки.

Результати роботи формують цілісне уявлення про підходи до побудови NGN-орієнтованого мережевого комплексу, підтверджують доцільність використання NGN у системах автоматизації та демонструють практичні аспекти реалізації сигнальних протоколів і алгоритмів керування сеансами зв'язку.

# 1 АНАЛІТИЧНА ЧАСТИНА

## 1.1 Системи автоматичного управління

Автоматичне управління в технічних системах — це комплекс дій, спрямованих на підтримання або покращення роботи об’єкта керування без безпосередньої участі людини, відповідно до визначеної мети управління [9]. Автоматизовані системи управління широко застосовуються в технічних та біотехнічних галузях тоді, коли людині складно або неможливо виконувати операції через великий обсяг інформації, обмежений час реагування, необхідність підвищеної точності та надійності або роботу в небезпечних чи важкодоступних умовах.

Метою управління є зміна в часі певної регульованої (керованої) величини — вихідного параметра об’єкта. Щоб досягти цієї мети, організовується керуючий вплив на виконавчі механізми об’єкта, який також компенсує зовнішні збурення, що можуть порушувати необхідний режим роботи. Формування цього керуючого впливу забезпечується пристроєм управління (ПУ) [7, 10].

Системи автоматичного управління верхнього рівня реалізують задачі візуалізації та моніторингу процесів. На цьому рівні виконуються такі функції:

- відображення ключових технологічних параметрів із системи керування (стан виконавчих механізмів, температура тощо);
- архівування всіх параметрів поточних процесів;
- передавання команд для впливу на виконавчі пристрої;
- керування зміною параметрів зовнішніх впливів;
- створення, обробка та зберігання інформації, пов’язаної з процесом управління.

## 1.2. Основні принципи мереж наступного покоління (NGN)

Термін NGN (Next Generation Networks) — «мережі наступного покоління» — увійшов до науково-технічного дискурсу на початку XXI століття. Концепція NGN, ініційована у [2001 році Європейським інститутом телекомунікаційних стандартів ETSI (European Telecommunications Standards Institute), була підтримана Сектором стандартизації телекомунікацій Міжнародного союзу електрозв'язку (ITU-T). У липні 2003 року в межах дослідницької комісії ІК 13 ITU-T було створено змішану групу доповідачів (JRG) з питань NGN, яка розробила проєкти перших нормативних документів. Наприкінці 2004 року в спеціально визначеній серії Y.2000 були затверджені дві початкові рекомендації ITU-T — Y.2001 та Y.2011. Станом на початок 2011 року серія вже налічувала близько 70 рекомендацій, що формували основу першої версії NGN (NGN Release 1).

Паралельно здійснювалася розробка NGN Release 2, завершена на початку 2008 року. Ця версія охопила ключові структурні компоненти NGN, зокрема IMS, технології IPTV без IMS, а також рішення для домашніх мереж, користувацьких пристроїв, механізми взаємодії NGN з корпоративними мережами. Подальша еволюція, визначена як NGN Release 3, передбачає збір додаткових даних і розвиток попередніх концептуальних напрацювань [11].

Формуванню ідей мереж наступного покоління передували низка об'єктивних чинників:

• стрімкий розвиток пакетних технологій передавання даних, що спричинив зростання цифрового трафіку, насамперед через поширення Інтернету;

• зростання попиту на засоби мобільного зв'язку та на нові мультимедійні послуги класу Triple Play (інтегроване передавання голосу, відео й даних);

• конвергенція телекомунікаційних та інформаційно-обчислювальних мереж, що зумовила розвиток інфокомунікаційних систем, які поєднують телекомунікаційну та інформаційну складові.

Відповідно до ITU-T Y.2001, NGN визначається як пакетна мережа, здатна забезпечувати широкий спектр вузькосмугових і широкосмугових послуг, включно з телефонним зв’язком, на основі широкосмугової транспортної інфраструктури з підтримкою гарантованої якості обслуговування (QoS).

У рекомендації ITU-T Y.2011 визначено принципи функціональної архітектури NGN:

Підтримка різноманітних технологій доступу.

Розподілене управління..

Відкрите управління.

Незалежність процесів надання послуг.

Підтримка послуг конвергентних мереж.

Підвищені вимоги до безпеки та захисту.

Для реалізації зазначених принципів рекомендація ITU-T Y.2011 пропонує еталонну модель NGN, яка включає два структурні рівні: рівень послуг (service stratum) та рівень транспортування (transport stratum). Кожен із них містить три площини — користувацьку, керування та менеджменту (рис. 1.1).


Рис.1.1. Базова еталонна модель NGN

Функціональні можливості рівнів базової еталонної моделі NGN деталізуються у загальній функціональній архітектурі NGN першої версії (NGN Release 1), описаній у рекомендації ITU-T Y.2012 (рис. 1.2). Кожен із рівнів передбачає використання сукупності спеціалізованих функцій. Для надання послуг та застосунків кінцевим користувачам у NGN застосовуються функції підтримки додатків, функції підтримки послуг, а також відповідні керувальні механізми. NGN передбачає використання спеціальної точки взаємодії з функціональною групою застосунків — інтерфейсу мережевих додатків ANI (Application Network Interface). Цей інтерфейс забезпечує інформаційний обмін і координацію між додатками та мережевими елементами NGN, надаючи необхідні засоби і ресурси для реалізації прикладних сервісів [5, 7, 12].

Транспортний рівень NGN відповідає за надання користувачам послуг IP-з’єднань, що реалізуються через функції управління транспортною підсистемою. До таких функцій відносять:

• NACFs (Network Attachment Control Functions) — функції контролю мережевих підключень;

• RACFs (Resource and Admission Control Functions) — функції управління мережевими ресурсами та доступом.

Ці компоненти спільно забезпечують узгоджену роботу механізмів доступу, транспортування та надання послуг у мережах NGN.

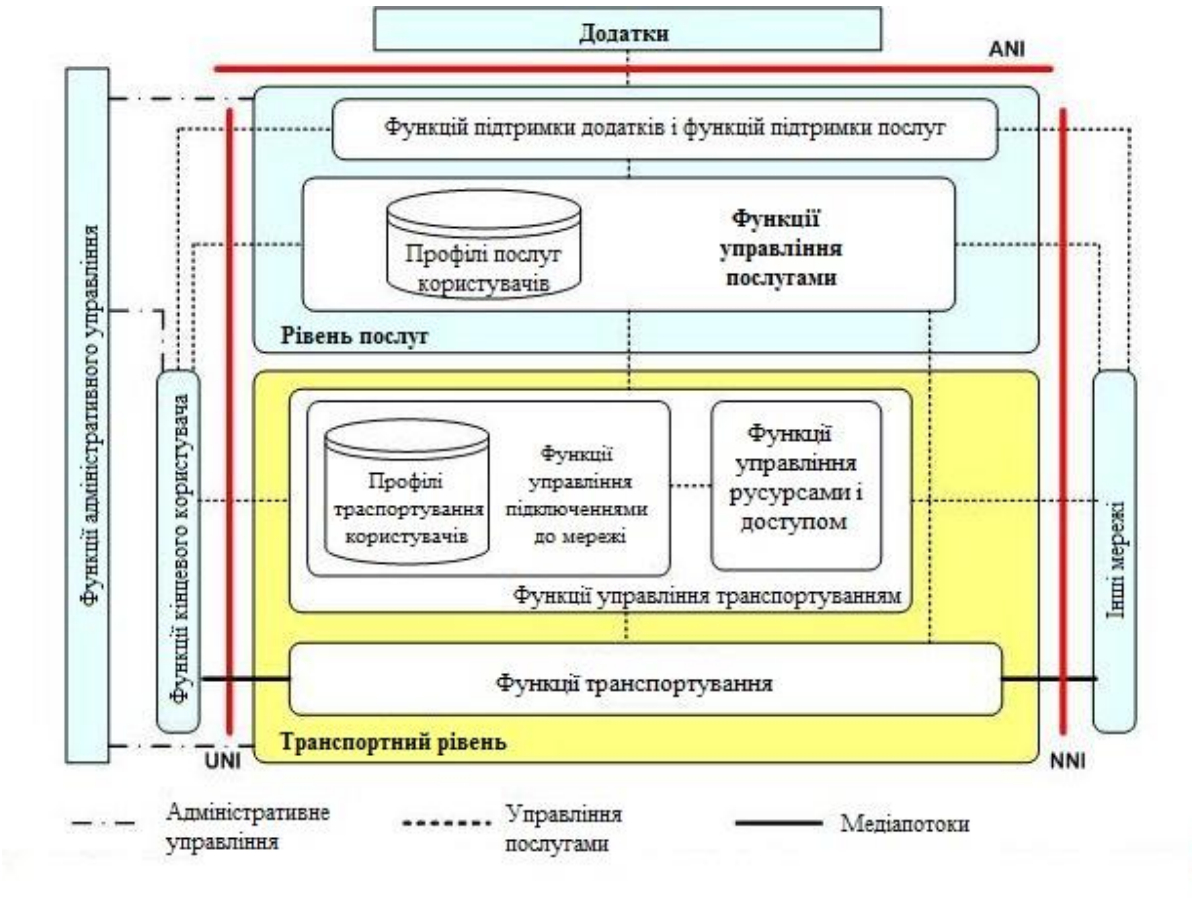


Рис.1.2. Загальна функціональна архітектура NGN (Рекомендація ITU-T Y.2012)

Згідно з рекомендацією ITU-T Y.2011, до складу транспортного рівня входять як власне транспортні функції, так і функції керування процесами транспортування [6, 12].

Для спрощення розуміння принципів побудови мереж наступного покоління у більшості наукових та технічних публікацій із тематики NGN використовується узагальнена чотирирівнева архітектура (рис. 1.3). У її структурі традиційно виділяють такі рівні:

Рівень доступу, що охоплює мережу абонентського доступу та забезпечує підключення користувачів до транспортної пакетної мережі.

Транспортний рівень, який включає магістральну пакетну мережу, побудовану на основі протоколів комутації пакетів IP або ATM; у сучасних реалізаціях — переважно на базі технології MPLS у поєднанні з IP-протоколом.

Рівень керування комутацією, що реалізує комплекс функцій, пов’язаних з управлінням усіма процесами обслуговування викликів у телекомунікаційній мережі.

Рівень послуг та експлуатаційного управління, до складу якого входить логіка виконання послуг і застосунків, а також механізми їх управління; цей рівень забезпечує відкриті інтерфейси для сторонніх розробників з метою створення нових сервісів і програмних рішень.

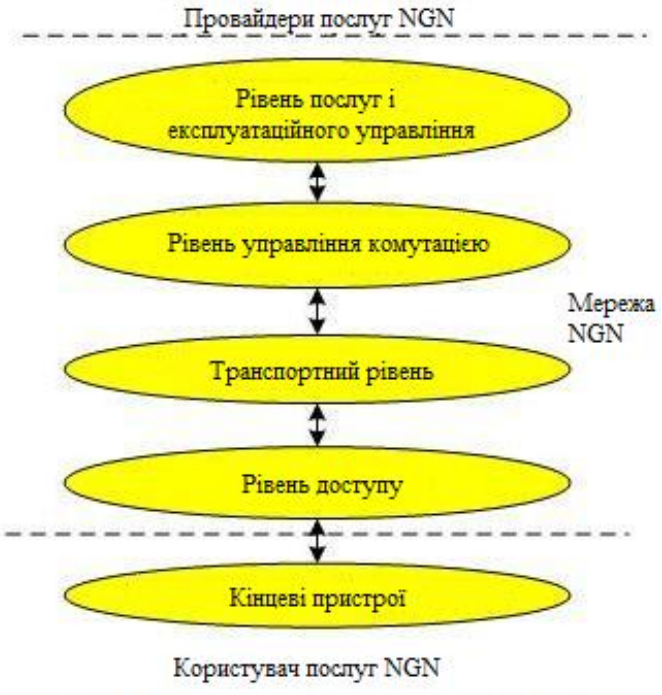


Рис.1.3. Чотири рівнева модель NGN

Кінцеві пристрої не є складовою частиною мережі NGN і, загалом, можуть належати до будь-якого типу абонентського обладнання, що

використовується в наявних дротяних або бездротових мережах. Водночас їх підключення до NGN можливе лише опосередковано — через абонентські шлюзові пристрої рівня доступу. Прямий доступ до мережі надається виключно тим абонентським терміналам, що функціонують на основі пакетної передачі даних та підтримують протоколи SIP або H.323 [13].

### 1.3. Актуальність дослідження NGN

Мережі безпосередньо пов’язані з системами управління, оскільки їхні параметри та характеристики істотно впливають на ефективність роботи всієї інфраструктури. Постійна модернізація мереж є необхідною умовою задоволення зростаючих вимог до пропускної здатності, підвищення якості функціонування, мінімізації колізій, втрат інформації та затримок. Історично розвиток телекомунікаційних мереж відбувався еволюційно, і логічним етапом цієї еволюції стало формування концепції мереж наступного покоління (NGN) [6].

Глобальні тенденції ринку свідчать про сталі зрушення у напрямі масового переходу операторів зв’язку до архітектур NGN. Зростає кількість провайдерів, які впроваджують доступ NGN, розгортають нові волоконно-оптичні інфраструктури (FTTx) або планують перехід до повністю IP-орієнтованих мереж (All-IP). Водночас численні аналітичні дискусії підтверджують відсутність єдиної універсальної стратегії міграції до NGN: оператори та підприємства обирають різні моделі переходу, залежно від економічних, технологічних та організаційних чинників.

Мережеве ядро NGN розглядається як логічний етап комерційного розвитку для операторів і підприємств, що прагнуть підвищити ефективність, покращити якість обслуговування та прискорити впровадження інноваційних сервісів. Хоча основним стимулом до впровадження NGN зазвичай є перспективна економія витрат у довгостроковій перспективі, така економія

може бути неочевидною порівняно з іншими інфраструктурними інвестиціями. У будь-якому разі малоймовірно, що повсюдне розгортання волоконно-оптичних мереж FTTH стане універсальним оптимальним рішенням.

Патентний аналіз підтверджує, що технології NGN мають високий інноваційний потенціал і значний попит. Оскільки традиційні мережеві інфраструктури досягли межі своїх технічних можливостей, модернізація стала неминучою, тоді як повна заміна мережевих систем є практично нереалістичною.

Патентна статистика відображає глобальні тенденції, а цифрова бібліотека українського патентного відомства значною мірою містить патенти, отримані в інших країнах, можна стверджувати, що тематика NGN залишається актуальною для України. Додатково аналіз української патентної бази засвідчив відставання піків патентної активності на кілька років порівняно зі світовими показниками, що створює можливості для формування власної науково-технічної бази та побудови конкурентоспроможних мереж. Важливою перевагою впровадження NGN в Україні є можливість уникнути подальшого оновлення застарілих інфраструктур, орієнтуючись одразу на сучасні глобальні стандарти..

### 1.4. Постановка задач та методи їх вирішення

Для виконання мети нашої магістерського дослідження необхідне виконання ряду завдань, метою яких є побудова мережевого комплексу на основі NGN технології:

1. *Підтримка різних типів даних що передаються та послуг*.

Побудована мережа повинна, підтримувати велику кількість послуг, з можливістю зміни їхніх характеристик, та якості пересилання.

2. *Функціональна гнучкість*.

Спроектована мережа повинна надавати функціональну гнучкість, для підтримки та забезпечення стійкості нових послуг, тобто швидке розгортання нових послуг, що відповідає стрімкому зростанню і змінам потреб.

*Віртуалізація ресурсів.*

Створення таких логічних правил, згідно яких, об’єкт (ресурс) зможе використовувати кілька віртуальних ресурсів.

*Доступ до даних.*

Спроектована мережа, з використанням NGN концепції, забезпечуватиме управління величезними обсягами даних. Розроблена мережа, повинна володіти механізмами швидкого вилучення даних, незалежно від їхнього місця розташування.

*Енергоефективність.*

Новостворена мережа має використовувати технології на рівні пристроїв. Обладнання як і самі мережі, мають забезпечувати енергоефективність, та виконувати покладені на них функції, з заданою точність та якість при мінімальному використанні трафіку..

*Економічність.*

Проектування мережі повинне здійснюватись таким чином, щоб забезпечити стійке конкурентне середовище, для уже існуючих типів мереж, шляхом забезпечення надійних економічних стимулів.

*Гнучкість управління.*

Створена мережа повинна ефективно експлуатуватись, обслуговуватись і запропоновувати значну кількість послуг і об’ктів.

*Мобільність.*

При розробці NGN мережі слід забезпечити мобільність, яка посприяє створенню високошвидкісного та масштабного середовища, де велике число вузлів, може динамічно переміщуватись.

*Оптимізація.*

Мережа NGN що розробляється, не повинна вважатись такою, що немає недоліків. Потрібно постійно оптимізовувати можливості мережевого обладнання, виходячи з вимог послуг і потреб кінцевого користувача.

*Ідентифікація.*

При проектуванні, NGN мережа, має забезпечуватись новою структурою ідентифікації, яка може ефективно підтримувати мобільність і доступ до даних з можливістю зміни масштабу.

*Надійність і безпека.*

Проектування мережі повинне відбуватись, таким чином, щоб забезпечити надійність і здатність до використання, з врахуванням не передбачуваних обставин, а також забезпечувати безпеку і конфіденційність даних, що передаються.

Оскільки NGN мережі повинні служити в якості ключової інфраструктури, підтримуючої діяльність обладнання, вони повинні також надавати будь-який тип послуг, призначених для вирішення найважливіших завдань, таких як інтелектуальне управління трафіком, "розумні" електромережі, електронна безпека і електрозв'язок в надзвичайних ситуаціях, забезпечуючи при цьому їх цілісність і надійність.

Для виконання поставлених цілей, необхідно вирішити ряд ключових завдань, що відображають сучасні вимоги, що постійно з’являються.

# 2 ТЕХНОЛОГІЧНА ЧАСТИНА

## 2.1. Класифікація обладнання NGN

На сьогоднішній день спостерігається активний розвиток та виготовлення значної кількості апаратно-програмних платформ, призначених для побудови мереж наступного покоління на основі гнучких комутаторів (softswitch) [14-17]. Такі мультисервісні платформи включають різноманітні типи обладнання, які можуть бути класифіковані відповідно до виконуваних ними мережевих функцій. Переважна більшість існуючих підходів до класифікації базується на розподілі обладнання NGN за чотирма основними рівнями (площинами) мереж наступного покоління: рівнем доступу, транспортним рівнем, рівнем керування викликами та рівнем додатків. Узагальнена класифікація типів обладнання NGN наведена на рис. 2.1.

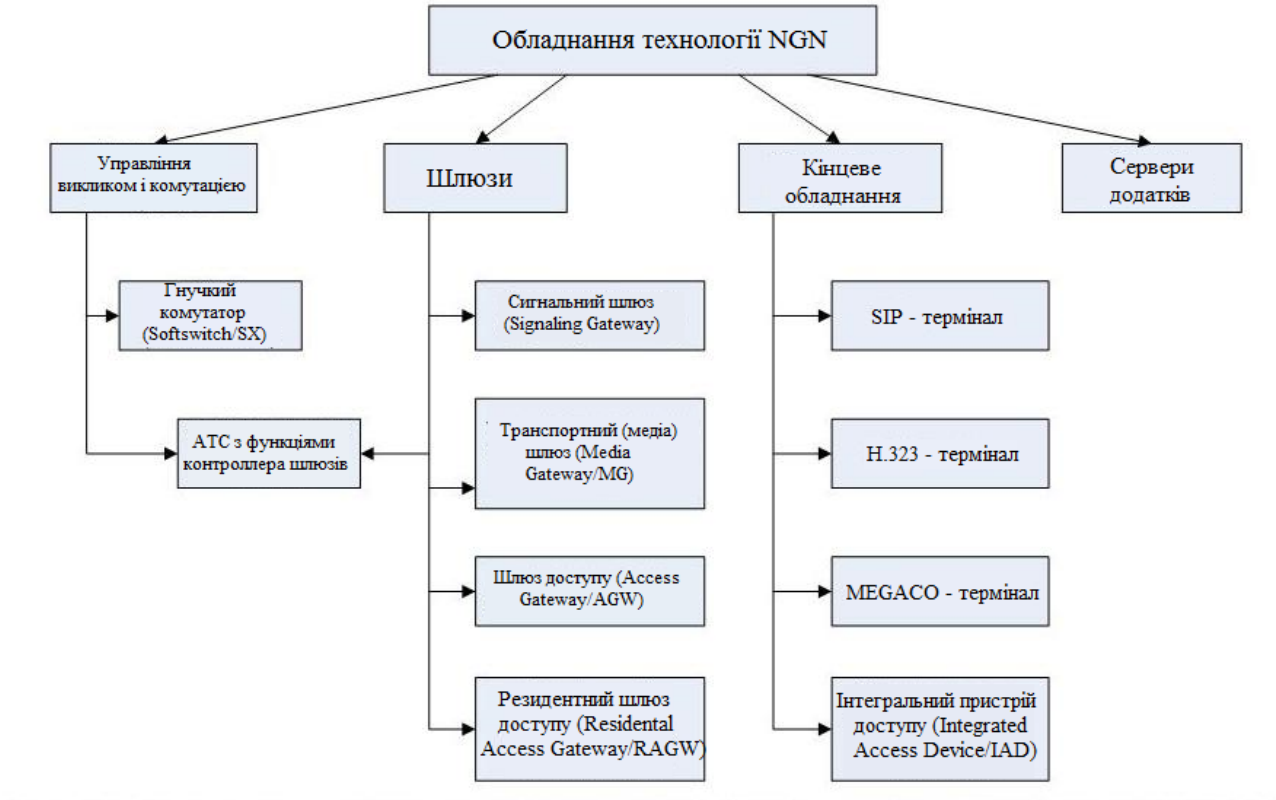


Рис.2.1. Класифікація типів обладнання

Альтернативний, хоча й у багатьох аспектах подібний підхід до класифікації обладнання ґрунтується на визначенні програмного комутатора Softswitch як ключового елемента, що реалізує функції рівня управління комутацією та передаванням інформації. Окрім цього, на даному рівні можуть застосовуватися АТС, оснащені функціоналом контролера шлюзів (MGC — Media Gateway Controller).

До базової мережі, що відповідає транспортному рівню архітектури NGN, можуть входити такі компоненти:

• транзитні вузли, які забезпечують функції перенесення та комутації трафіку;

• кінцеві (граничні) вузли, призначені для організації доступу абонентів до мультисервісної мережі;

• контролери сигналізації, що виконують обробку сигналізаційної інформації та керують процесами встановлення викликів і з'єднань;

• шлюзи, які забезпечують інтеграцію та взаємодію з традиційними мережами електрозв'язку.

До рівня доступу в архітектурі NGN належать такі компоненти:

• шлюзи, що забезпечують взаємодію з іншими мережами та технологіями;

• мережа доступу — телекомунікаційна інфраструктура, яка забезпечує підключення кінцевого користувацького обладнання до граничного вузла транспортної мережі;

• кінцеве абонентське обладнання, що використовується для отримання послуг мережі.

У межах шлюзового обладнання виділяють такі програмно-апаратні конфігурації:

- транспортний шлюз (Media Gateway, MG), який виконує перетворення та передавання медіапотоків;

- сигнальний шлюз (Signalling Gateway, SG), призначений для обробки та транспортування сигналізаційної інформації між різними мережевими середовищами;
- транкінговий шлюз (Trunking Gateway, TGW), що інтегрує функціональність MG і SG та забезпечує одночасну роботу з медіапотоками й сигналізацією.

Окрім двох основних типів термінальних пристроїв, призначених для роботи в мережах NGN — SIP-терміналів та H.323-терміналів — у деяких випадках застосовується також термінальне обладнання, що функціонує на основі протоколу MEGACO. До окремої категорії термінальних засобів належать інтегровані пристрої доступу (IAD), які поєднують у собі функції абонентського обладнання та засобів підключення до мережі [5, 18].

Для реалізації функцій рівня послуг і управління ними використовуються сервери додатків (Application Servers) та сервери додаткових послуг (Feature Servers).

У Рекомендації MCE-T Q.3900 «Methods of testing and model network architecture for NGN technical means testing as applied to public telecommunication networks» подано дещо іншу класифікацію технічних засобів, що реалізують модель NGN. До неї включено низку класів і різновидів обладнання, узагальнених на схемі, представленій на рис. 2.2.)

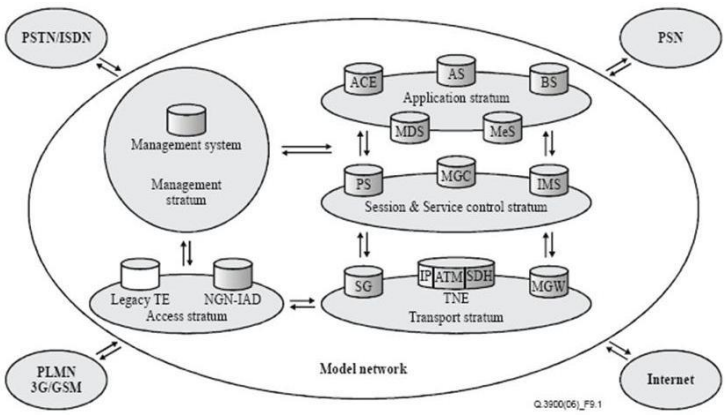


Рис.2.2. Схема розміщення обладнання NGN (рекомендація ITU-T Q.3900)

1. Системи керування сесіями та викликами включають такі компоненти:

• контролер керування медіашлюзами MGC (Media Gateway Controller);

• SIP-проксі-сервер PS (Proxy Server SIP), що забезпечує маршрутизацію SIP-сигналізації;

• IP-мультимедійна підсистема IMS (IP Multimedia Subsystem), призначена для підтримки інтегрованих мультимедійних сервісів.

2. Системи передавання голосової та сигнальної інформації охоплюють:

• медіашлюзи GW (Media Gateway), які виконують перетворення медіапотоків між різними середовищами;

• сигнальні шлюзи SG (Signalling Gateway), що забезпечують транспортування та конвертацію сигналізаційних протоколів;

• середовище транспортної мережі TNE (Transport Network Environment), яке слугує основою для передачі голосових та сигнальних даних.

3. Сервери додатків, що реалізують логіку та функціональність сервісів:

• сервер додатків AS (Application Server);

• медіасервер MDS (Media Server), який забезпечує функції обробки мультимедійних потоків;

• сервер повідомлень MeS (Messaging Server) для підтримки сервісів передачі повідомлень.

4. Системи експлуатаційної підтримки NGN включають:

• систему управління мережею NMS (NGN Management System), що здійснює моніторинг, конфігурацію та підтримку мережевих ресурсів;

• білінгову систему BS (Billing System), призначену для обліку послуг та розрахунків з абонентами.

5. Обладнання середовища доступу охоплює такі компоненти:

• інтегровані пристрої доступу NGN-IAD (NGN Integrated Access Devices), які забезпечують підключення абонентів до мережі;

• медіашлюзи GW-LTE (Media Gateway for Legacy Terminal Equipment), що забезпечують сумісність традиційних термінальних пристроїв з архітектурою NGN.

У Рекомендації ITU-T Q.3900 зазначається, що кожен із перелічених типів технічних засобів NGN має реалізовувати у своєму складі як обов'язкові функціональні компоненти, без яких неможливе виконання ключових операцій системи, так і додаткові функції, що розширюють можливості користувачів та забезпечують підтримку спеціалізованих сервісів. Функціональність, реалізована за допомогою обладнання NGN, може охоплювати функції різних рівнів архітектури — рівня доступу, транспорту, управління та рівня послуг.

Показовим прикладом комплексного рішення є гнучкий комутатор (softswitch), який, окрім обов'язкового компонента — контролера медіашлюзів, часто включає й інші елементи, такі як сигнальний шлюз, SIP-проксі-сервер, сервер автентифікації, авторизації та обліку (AAA), сервери H.323 та інші модулі.

## 2.2. Обладнання гнучких комутаторів (softswitch)

Вважається, що ключовий для концепції NGN термін «softswitch» був уперше запроваджений компанією Lucent Technologies як назва програмно-апаратного рішення, призначеного для керування викликами в мережах ATM та IP. Гнучкий комутатор є центральним і обов'язковим елементом будь-якої мережі наступного покоління першої версії (NGN Release 1). По суті, softswitch являє собою обчислювальний пристрій із відповідним програмним забезпеченням, що має високий рівень доступності та відмовостійкості.

У мережах NGN процес управління викликами включає такі завдання, як маршрутизація сеансів, автентифікація користувачів, установлення та завершення з'єднань, обмін сигналізаційною інформацією та виконання

інших службових функцій. Оскільки гнучкий комутатор виконує роль центрального посередника, він повинен бути здатним інтерпретувати як традиційні телефонні протоколи сигналізації, так і протоколи керування передаванням інформації в пакетних мережах.

Таким чином, softswitch є основним елементом, що реалізує функції рівня управління комутацією в архітектурі NGN (див. рис. 1.3).

У складі гнучкого комутатора мають бути реалізовані такі базові функції:

- Функція управління базовим викликом, що забезпечує приймання й оброблення сигнальної інформації та виконання процедур встановлення з’єднань у пакетній мережі.
- Функція автентифікації та авторизації абонентів, які підключаються до пакетної мережі як безпосередньо, так і через обладнання доступу.
- Функція маршрутизації викликів у середовищі пакетної мережі.
- Функція тарифікації та збору статистичних даних, необхідних для аналітики та подальшої обробки.
- Функція управління транспортними шлюзами, що забезпечує координацію їхньої роботи в рамках обробки мультимедійного трафіку.
- Функція надання додаткових видів обслуговування (ДВО), яка може реалізовуватися безпосередньо гнучким комутатором або у взаємодії із сервером додатків.
- Функції експлуатації, адміністрування, технічного обслуговування та надання інформації (OAM&P — Operation, Administration, Maintenance and Provisioning), що забезпечують керування життєвим циклом обладнання та мережевих ресурсів.

Крім основних можливостей, у гнучкому комутаторі можуть бути реалізовані й додаткові функції, зокрема:

- Функція кінцевого або транзитного пункту сигналізації SP/STP (Signaling Point / Signaling Transfer Point) системи сигналізації № 7.
- Функція взаємодії з серверами додатків, що забезпечує інтеграцію нових сервісів і логіки обслуговування.
- Функція вузла комутації послуг SSP (Service Switching Point) інтелектуальної мережі та інші спеціалізовані можливості.

До категорії гнучких комутаторів належать різні за своєю функціональністю технічні рішення, оскільки єдиної загальноприйнятої класифікації softswitch-обладнання досі не існує. Частина виробників, експертів і операторів під терміном softswitch фактично розуміють контролер медіашлюзів MGW (Media Gateway Controller), пристрій управління викликами CA (Call Agent) або сервер викликів CS (Call Server). Незважаючи на відмінності у реалізації, зазначені пристрої виконують ключову функцію гнучкого комутатора — програмне управління з'єднаннями та передачею користувацького трафіку в мережі NGN, що надходить як від медіашлюзів, так і від пакетних абонентських терміналів [19].

З іншого боку, у складі комплексних (фірмових) апаратно-програмних рішень softswitch часто присутні й додаткові мережеві компоненти, такі як медіашлюзи, сигнальні шлюзи, SIP-проксі-сервери, AAA-сервери (Authentication, Authorization, Accounting) та інші модулі, що розширюють функціональність системи.

Одну з можливих функціональних структур гнучкого комутатора наведено на рис. 2.3.

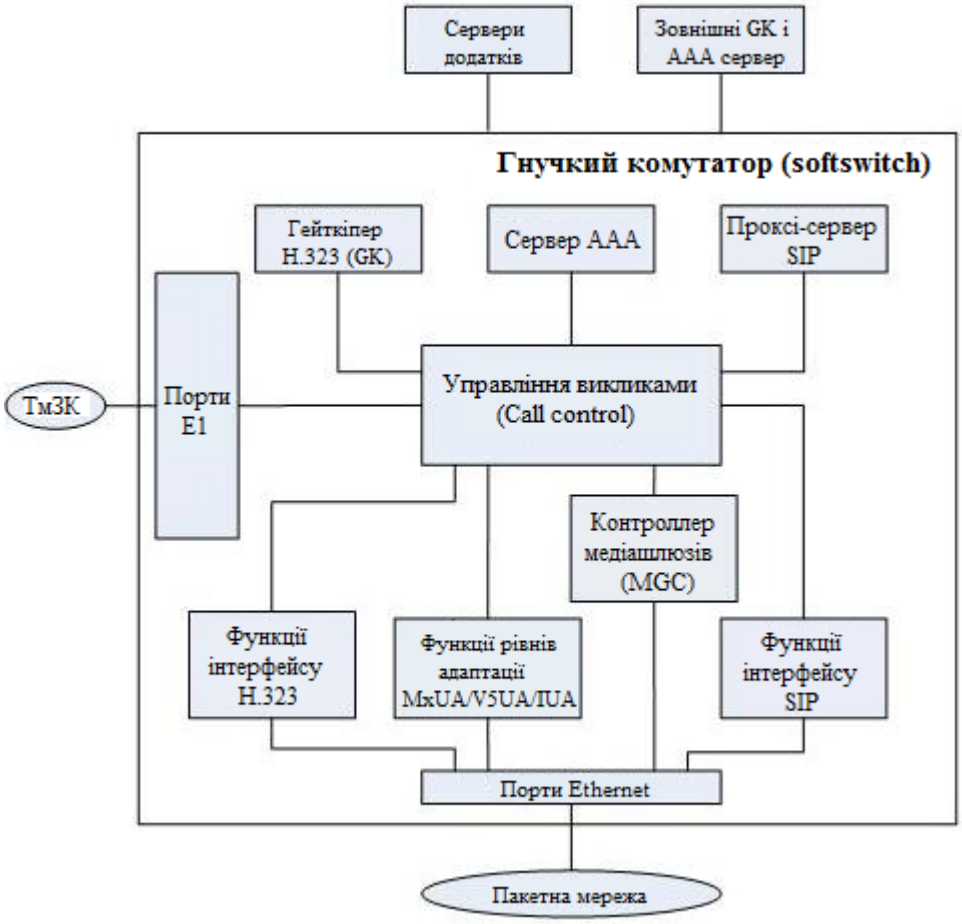


Рис.2.3. Функціональна схема гнучкого комутатора

Незалежно від конкретної реалізації або виробника, будь-який гнучкий комутатор повинен забезпечувати базовий набір функцій, необхідних для управління сеансами зв’язку. До таких функцій належать: керування медіашлюзами за допомогою відповідних сигналізаційних протоколів, передавання таблиць маршрутизації, узгодження та перетворення номерних планів між різними системами нумерації тощо.

До основних технічних характеристик обладнання гнучкого комутатора належать:

1. Продуктивність.
2. Надійність.
3. Підтримувані протоколи.
4. Підтримувані інтерфейси.

Конструктивно гнучкий комутатор може бути реалізований у вигляді окремого пристрою, що виконує спільно функції управління викликами і комутатора (switching fabric). Часто виробники softswitch поділяють його на два і більше пристроїв - контролер шлюзів, сигнальний шлюз SG (Signalling Gateway) і медіашлюзи MGW.

У більшості випадків сучасні гнучкі комутатори мають модульну архітектуру, що забезпечує високий рівень масштабованості системи. Така архітектура дає змогу формувати географічно розподілені мережі, гнучко керувати потоками сигнального та медіатрафіку, а також реалізовувати ефективні механізми резервування.

Усі гнучкі комутатори (softswitch) класифікують на два основних типи відповідно до їхніх мережевих функцій — комутатори класу 4 та комутатори класу 5. Згідно з цим підходом, гнучкий комутатор класу 4 призначений для побудови транзитних вузлів управління з’єднаннями в операторських мережах із пакетною комутацією. Він виконує маршрутизацію та розподіл викликів в IP-мережах на магістральному рівні (міжміському, міжнародному або місцевому), забезпечуючи транзит трафіку, що надходить від сегментів мережі з абонентським доступом.

Гнучкі комутатори класу 5 мають принципову відмінність — здатність працювати безпосередньо з кінцевими абонентами мережі. Вони забезпечують надання мультимедійних сервісів та широкого спектра додаткових видів обслуговування (ДВО), таких як:

• інтелектуальна маршрутизація викликів залежно від доступності абонента;

• функції очікування, утримання та переведення виклику;

• трьохсторонні конференції;

• паркування та перехоплення викликів;

• підтримка груп багатолінійних абонентів тощо.

## 2.3. Реалізація Softswitch

Основні способи реалізації Softswitch, що базуються на програмно-апаратних компонентах представленні в таблиці 3.1.

Табл. 2.1. Варіанти реалізації Softswitch

| **Компанія** | **Назва продукту** | **Формула сертифікату** |
|---|---|---|
| Alcatel | 5020 Softswitch | Alcatel 5020 — гнучкий комутатор; Alcatel 5023 — сигнальний шлюз; Alcatel 8690 та Alcatel 8605 — сервери додатків; Alcatel 8688 — медіасервер; Alcatel 5795 — центр управління мережею. Усе зазначене обладнання вироблено компанією Alcatel Bell N.V. та відповідає технічним умовам ТУ 6651-471-04604025-2003, код ОКДП 3222150. |
| Альтертекс | AlterPSS | відсутня |
| CedarPoint Comm. | Safari $C^3$ | відсутня |
| Cirpack | HVS | відсутня |
| Cisco Systems | BTS 10200 Softswitch | відсутня |
| Clarent | CDSNA | відсутня |
| Convergent Networks | PMC (ICSX CMS), ICS2000* | відсутня |
| CopperCom | CSX 1100*, CSX 2100* | відсутня |
| Екран | Протей-МКД | Програмно-апаратний комплекс з функціями гнучкого комутатора Softswitch МКД (версія ПЗ 1.3) виробництва фірми «Екран» Технічні умови: ТУ 4604021.050 402-2.0, код ОКДП 3222150 |
| Ericsson | ENGINE Integral (TeS) | відсутня |
| Hughes Software | HSS Softswitch | відсутня |
| IpGen | Genovation- | відсутня |

| | MSP | |
|---|---|---|
| IntereXchange Carrier | IXC Softswitch | Апаратно-програмний комплекс «IXC System» версії 4.1 виробництва ООО «ай-екс-сі груп», технічні умови ТУ 5600-101-47397453-2003, код ОКДП 3222155 |
| Huawei Technologies | U-SYS SoftX3000 | Комплекс обладнання U-SYS. Що реалізує функції гнучкого комутатора (Softswitch), в складі U-SYS SoftX3000 (версія ПЗ V300), U-SYS MRS6000 (версія ПЗ CMS6000-AO-8441), U-SYS SG7000 (версія ПЗ V100), U-SYS AMG5000 (версія ПЗ V100), U-SYS TMG8010 (версія ПЗ V100), U-SYS UMG8900 (версія ПЗ V100), U-SYS IAD132E(T) (версія ПЗ V100) виробництво компанії Huawei Technologies Co., Ltd. (Китай), технічні умови Huawei_U-SYS/rus.2004, код ОКДП 3222151 |
| Italtel | iMSS Softswitch | Програмно-апаратний комплекс з функціями гнучкого комутатора сімейства iMSS (версії ПЗ 21.20, 21.21, 21.22, 21.23) виробництво компанії Italtel S.p.A. (Італія), Технічні умови ТУ-3222150-045-52614645-20 03, код ОКДП 3222150 |
| Lucent Technologies | Lucent SoftSwitch, | Комплекс апаратних пристроїв і програмного забезпечення IP - телефонії SoftSwitch IP (версія ПЗ Rel. 2.4, 3.1, 3.2) в складі гейткіпера SoftSwitch і шлюзів сімейства MAX (MAX TNT, APX 1000, APX 8000) виробництво фірми Lucent Technologies, технічні умови 4604021.034 101?2.0 ТУ, код ОКДП 3222150 АТМ комутатор Softswitch ATM (версія ПЗ: Rel. 2-3) Виробництво фірми Lucent Technologies (Нідерланди), технічні умови 4604021.036 101-2.0 ТУ, код ОКДП 3222410 |

Підводячи підсумки, та узагальнюючи наведені варіанти реалізації Softswitch, модель реалізації матиме наступний вигляд (рис. 2.4):

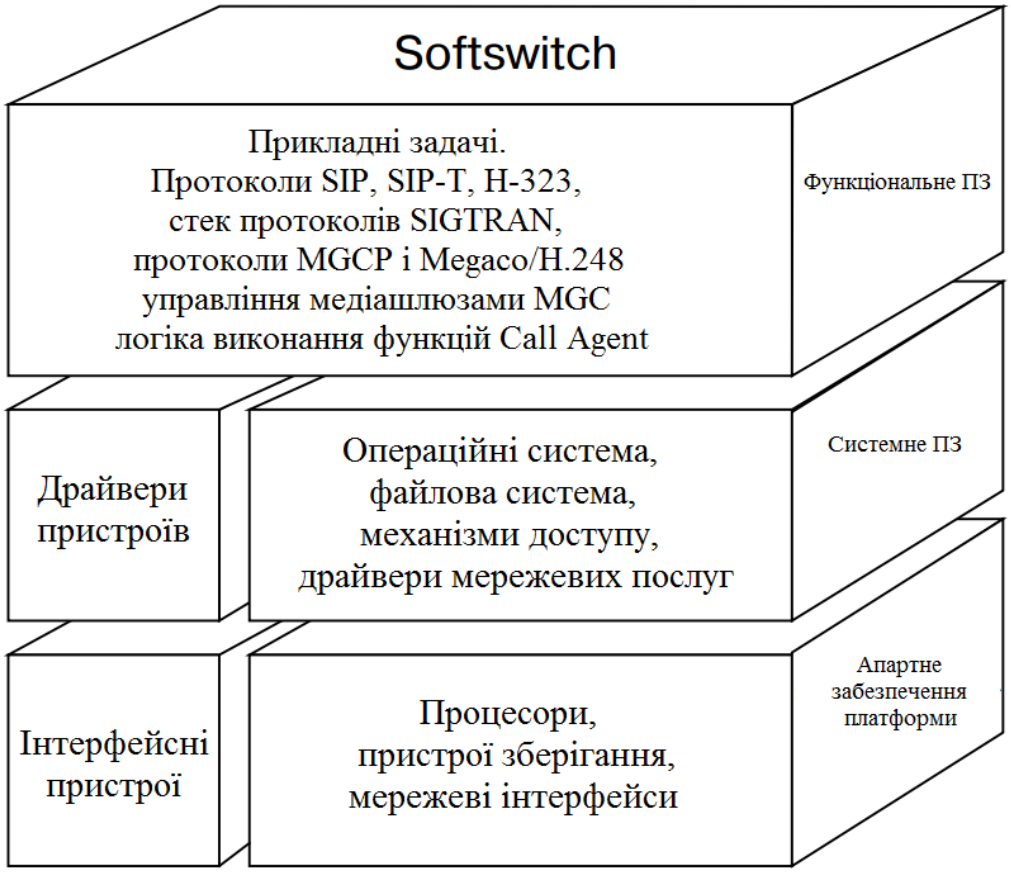


Рис. 2.4. Модель реалізації SoftSwitch

Під час вибору способу реалізації SoftSwitch за основу було взято вже сформовані концептуальні моделі, адаптовані з урахуванням специфіки автоматизованих систем. Зокрема, була використана модель, запропонована компанією Alcatel, з якої вилучено низку модулів, що не мають ключового значення для заданого функціоналу (наприклад, модуль відстеження місцеположення об’єкта). Водночас із архітектури Ericsson Engine було запозичено принцип реалізації функції комутації з’єднань. Таким чином, SoftSwitch у вибраній моделі забезпечує оброблення сигнальної інформації та встановлення комунікаційних сесій.

Функції, пов’язані з обслуговуванням викликів і керуванням системою, розподіляються між кількома незалежними процесорними модулями. Така архітектурна організація дозволяє нарощувати ємність системи шляхом додавання нових знімних плат. Усі елементи конструкції обладнання мають резервовану структуру, що забезпечує рівень надійності 99,999%, який є критично важливим для автоматизованих систем.

## 2.4. Шлюзове обладнання

Шлюзи (Gateways) є пристроями, що забезпечують доступ до мережі NGN та її взаємодію з існуючими телекомунікаційними системами. Функціональність шлюзового обладнання охоплює перетворення сигнальної інформації між мережами з комутацією каналів і мережами з пакетною передачею, а також трансформацію транспортних потоків у IP-пакети або ATM-комірки з подальшою маршрутизацією [14, 18].

Для забезпечення підключення різних типів термінального обладнання до мереж NGN у їхніх платформах використовуються різні апаратні та програмні конфігурації шлюзів:

- Медіа-шлюз MG (Media Gateway) — виконує перетворення мовної інформації з формату TDM у IP-пакети або ATM-комірки та здійснює маршрутизацію трафіку.
- Сигнальний шлюз SG (Signalling Gateway) — забезпечує перетворення сигналізації мережі SS7 (у квазізв’язаному режимі) у протоколи сигналізації пакетних мереж SIGTRAN із застосуванням відповідних адаптаційних рівнів.
- Транкінговий (транзитний) шлюз TGW (Trunking Gateway) — поєднує функціональність медіа- та сигнальних шлюзів.
- Шлюз доступу AGW (Access Gateway) — реалізує функції MG і SG для обладнання доступу (наприклад, УВАТС, абонентські модулі або

концентратори TDM-мереж), що підключається через інтерфейси E1 або V5.x.

- Резидентний шлюз доступу RAGW (Residential Access Gateway) — забезпечує підключення кінцевих користувачів або приватних мереж, що використовують термінальне обладнання, до NGN.

Основними технічними характеристиками шлюзового обладнання є:

*1. Ємність шлюзу, обумовлена як в напрямку приватних мереж, так і в напрямку до пакетної мережі.*

*2. Протоколи, що підтримуються.*

Обладнання шлюзів підтримує протоколи, зазначені в табл. 2.2.

Табл.2.2. Протоколи що підтримують різні типи шлюзів

| **Тип шлюзу** | **Напрямок передачі** | **Протоколи** |
|---|---|---|
| Транспортний шлюз | До гнучкого комутатора | 1. Протоколи H.248, MGCP, IPDC, UNI (При використанні транспортної технології IP)<br>2. протокол BICC (при використанні транспортної технології ATM) |
| | До інших шлюзів, або термінального обладнання пакетної мережі | 1. Протоколи RTP/RTCP (при використанні транспортної технології IP)<br>2. Протоколи PNNI або UNI(при використанні транспортної технології ATM) |
| Сигнальний шлюз | До гнучкого комутатора | Рівні адаптації M2UA або M3UA протоколу SIGTRAN |
| | До приватної мережі (ТМЗК) | Підсистеми MTP2 або MTP3 протоколу сигналізації SS7 |
| Шлюз доступу | До гібридного комутатора для передач сигнальної інформації, зв’язаної з обслуговуванням виклику | 1. Рівень адаптації V5UA протоколу SIGTRAN (при підключені обладнання мережі доступу)<br>2. Протоколи MEGACO/H.248 (при підключенні абонентів, що використовують сигналізацію по |

| | | |
|---|---|---|
| | | аналоговій абаненській лінії)<br>3. Рівень адаптації IUA протоколу SIGTRAN (при підключенні абонентів, що використовують базовий доступ ISDN) |
| | До гнучкого комутатора для передачі сигнальної інформації управління шлюзами | Протоколи MEGACO/H.248, MGCP, IPDC |
| | До мережі ТМЗК | 1. Сигналізація по аналоговим абонентським лініям (шлейфна, DTMF).<br>2. Сигналізація базового доступу ISDN в частині протоколів 2 рівня (протокол LAP-D).<br>3. Сигналізація по інтерфейсу V5 в частині протоколів 2 рівня (протокол LAP-V5). |
| | До інших шлюзів і термінального обладнання пакетної мережі | Протоколи RTP/RTCP |

*3. Інтерфейси, що підтримуються.*

Обладнання шлюзів підтримує інтерфейси, наведені в табл. 2.3.

Табл. 2.3. Інтерфейси, що підтримуються різними типами шлюзів NGN

| **Тип шлюзу** | **Напрямок передачі** | **Інтерфейси** |
|---|---|---|
| Транспортний шлюз | До мережі ТМЗК | E1 (PDH) і/або STM-1/4 (SDH) |
| | До пакетної мережі в основі IP-технологій | Інтерфейси сімейства Ethernet від 10 Base до Gigabit Ethernet (1000 Base), причому використовуване середовище передачі специфікується окремо |
| | До пакетної мережі на основі ATM технологій | Від IMA до NNI 4.0 |
| Сигнальний шлюз | До пакетної мережі | 10 Base Ethernet |
| | До мережі ТМЗК | E1 (PDH) |

| | | |
|---|---|---|
| | До мережі ТМЗК | Для резидентних шлюзів – інтерфейс по аналоговим абонентським лініям і інтерфейси U-, S-, S/T базового доступу ISDN. Для шлюзів доступу, що здійснюють підключення обладнання інтерфейсу V5 – інтерфейс E1 (PDH). |
| | До пакетної мережі на основі IP технології | 10-100 Base Ethernet |
| | До пакетної мережі на основі ATM технологій | IMA або UNI |

Типова фізична архітектура медіа шлюза показана на рис. 2.5. Як правило, шлюз складається з шасі, в якому розташовуються окремі карти (рис. 2.6.).

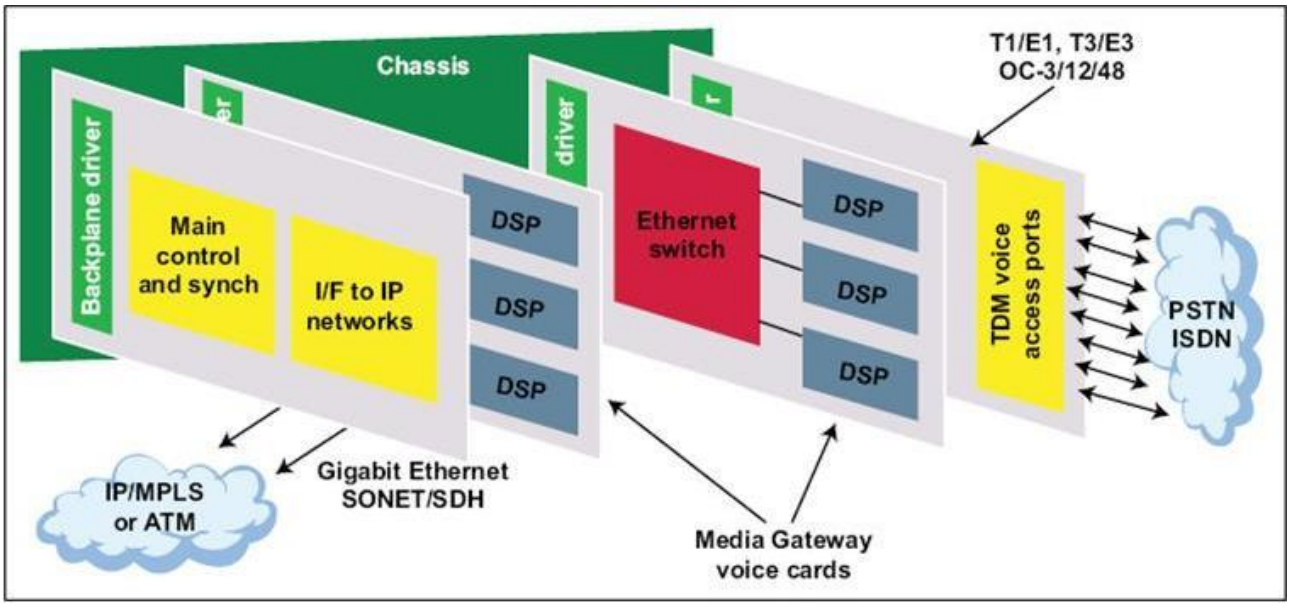


Рис.2.5. Типова фізична архітектура медіа шлюза

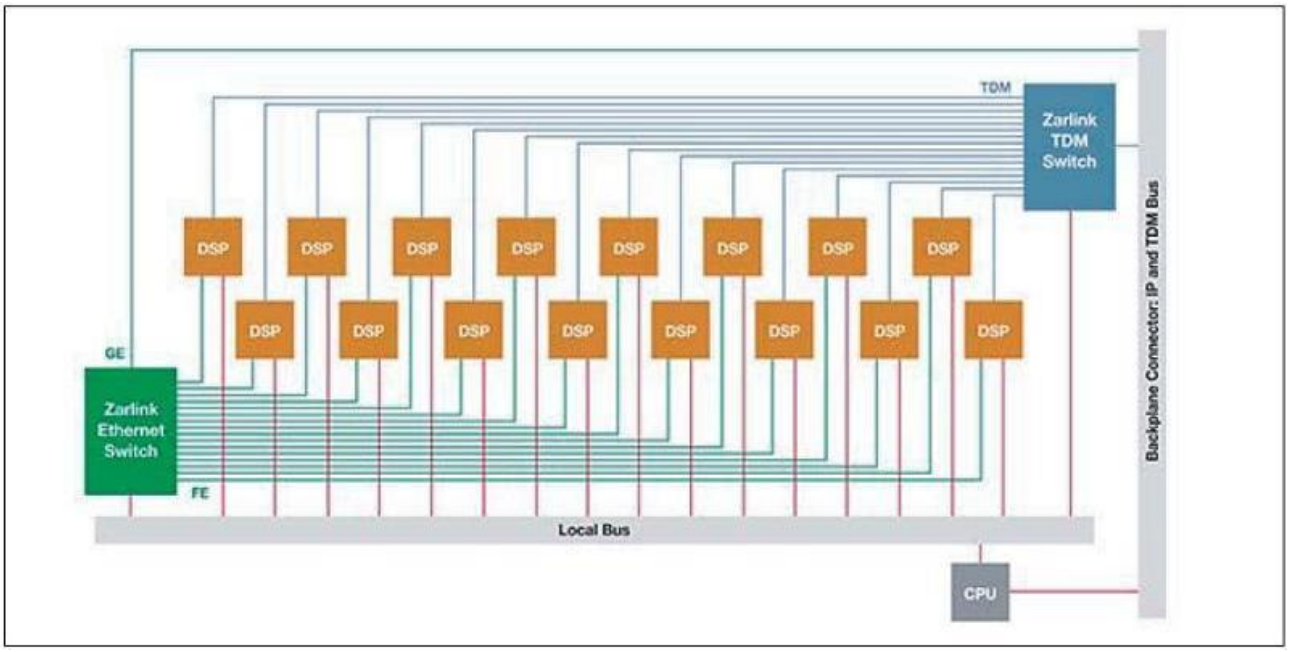


Рис.2.6. Структурна схема типової карти медіа шлюзу

Сигнальний шлюз SG (Signalling Gateway) за архітектурою близький до медіашлюзів, однак, на відміну від них, не обробляє медіаінформацію. Його основне призначення — перетворення та передавання сигналізаційного трафіку мережі ТМЗК до гнучкого комутатора або контролера управління викликами (MGC). SG підтримує перетворення різних типів сигналізації, зокрема SS7 та DSS1 (ISDN).

Для передавання сигналізаційних даних мережі ТМЗК у середовищі пакетної комутації використовуються протоколи стеку SIGTRAN, включаючи:

• IUA — адаптація сигналізації Q.931 (ISDN);

• V5UA — адаптація сигналізації V.5.2;

• M3UA — адаптація користувацького рівня 3 підсистеми MTP мережі SS7;

• M2UA — адаптація рівня 2 підсистеми MTP SS7.

Протоколи SIGTRAN передаються поверх транспортного протоколу SCTP. Сигнальні шлюзи застосовуються на межі мереж NGN і ТМЗК, забезпечуючи їх взаємодію та узгодження сигналізації.

На практиці виробники часто пропонують комбіновані рішення, у яких в одному пристрої реалізовано функції як медіашлюзу, так і сигнального шлюзу.

## 2.5. Апаратно-програмні рішення рівня додатків

На рівні додатків у мережах NGN застосовуються різноманітні апаратно-програмні комплекси, серед яких виділяють такі основні типи:

- Сервер додатків AS (Application Server), що реалізує логіку надання послуг;
- Медіасервер MS (Media Server), призначений для оброблення мультимедійних потоків;
- Сервер повідомлень MeS (Message Server), який забезпечує функції обміну повідомленнями;
- Середовище створення комунікаційних додатків ACE (Application Creation Environment);
- Системи керування та конфігурації мережі;
- Система оперативно-розшукових заходів (СОРМ);
- Білінгові системи та інші допоміжні модулі.

Сервер додатків AS (Application Server) є програмним сервером, що забезпечує користувачам доступ до нових сервісів. Серед типових прикладів послуг, які можуть реалізовуватись на AS, — електронна комерція (e-commerce) та електронна торгівля (e-market). У мережах NGN сервер додатків відіграє ключову роль, оскільки здатний виконувати функції різних

елементів архітектури на рівні управління сеансами та сервісами, включаючи функції MGC, медіасервера MS, сервера повідомлень MeS тощо.

Застосування AS забезпечує гнучке керування мережевими можливостями та сприяє створенню нових, перспективних сервісних сценаріїв у NGN.

Сервер додатків AS підтримує широкий набір протоколів та інтерфейсів, серед яких:

1. транспортні протоколи: IP, UDP, TCP;
2. сигналізаційні протоколи: MGCP, H.248/MEGACO, SIP;
3. додаткові протоколи: LDAP, HTTP, CPL, XML;
4. відкриті інтерфейси: JAIN, PARLAY тощо;
5. інтерфейси IP-мереж: Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI, CDDI;
6. ATM-інтерфейси: E1, E3, STM-1, STM-4, STM-16.

Медіасервер MS (Media Server) забезпечує взаємодію користувача з мережевими додатками та додатковими послугами зв’язку за допомогою голосових команд і сигналів DTMF. Архітектура MS складається з двох основних функціональних блоків:

1. Блок управління медіаресурсами, який виконує розпізнавання DTMF, синтез та розпізнавання мовлення тощо.
2. Блок управління послугами, що забезпечує відтворення й запис повідомлень, підтримку факсимільних сервісів, організацію конференцзв’язку та інші функції.

Медіасервери можуть реалізовуватися на різних програмно-апаратних платформах і підтримують, зокрема, використання мов опису голосових додатків, таких як VoiceXML.

Сервер повідомлень MeS (Message Server) відповідає за зберігання та доставку повідомлень користувачам, а також забезпечує доступ до низки додаткових послуг зв’язку. Подібно до медіасервера MS, MeS може

реалізовуватися на різних програмно-апаратних платформах із використанням широкого спектра мов програмування.

Середовище створення додатків ACE (Application Creation Environment) призначене для розроблення та формування завершених сервісів і додатків, що імпортуються до сервера додатків AS. Процес створення додатків включає аналіз вимог, проєктування, тестування та подальший розвиток функціональності. ACE, як і інші компоненти NGN, може бути реалізоване на різних програмно-апаратних платформах.

Система управління і конфігурації забезпечує централізований контроль та керування всіма технічними засобами NGN. Такі системи зазвичай мають розподілену, об’єктно-орієнтовану архітектуру та підтримують мультипротокольність. Важливою вимогою є відкритість інтерфейсів, зокрема використання стандартизованих протоколів (IIOP, CMIP, SNMP, FTP, FTAM тощо) та формальних мов опису інтерфейсів (CORBA IDL, Java, GDMO, ASN.1). Стабільність інтерфейсів має гарантувати внесення лише тих змін, що зберігають зворотну сумісність.

Система управління NGN виконує такі ключові функції:

- керування обробкою помилок, включно з виявленням, локалізацією та усуненням збоїв;
- керування конфігурацією обладнання, що забезпечує налаштування та підтримку параметрів мережевих пристроїв;
- взаємодію з білінговою системою, необхідну для обліку та тарифікації послуг;
- експлуатаційне керування послугами, спрямоване на підтримку їх коректного функціонування;
- забезпечення безпеки, зокрема контроль доступу, аудит та захист інформації.

Реалізація системи оперативно-розшукових заходів (СОРЗ), або LEMF (Law Enforcement Monitoring Facility) у європейських специфікаціях, у мережах NGN суттєво відрізняється від її реалізації в традиційних телефонних мережах із комутацією каналів. Це зумовлено тим, що в NGN сигнальна інформація та медіатрафік (мовні потоки) передаються різними маршрутами й обробляються різними мережевими елементами, а не єдиним комутаційним вузлом, як у випадку з АТС.

Взаємодія між пунктом управління СОРЗ та обладнанням оператора здійснюється через спеціальний пристрій — Посередник СОРЗ (SORM Mediation). Він пов'язується з основними елементами NGN-мережі, такими як гнучкий комутатор (softswitch), медіашлюзи, пристрої абонентського доступу, а також з IP-маршрутизаторами. Посередник виконує функції перетворення сигналізації та медіапотоків, забезпечуючи доставку необхідної інформації до пункту управління СОРЗ. Архітектурна схема цієї взаємодії наведена на рис. 2.7.

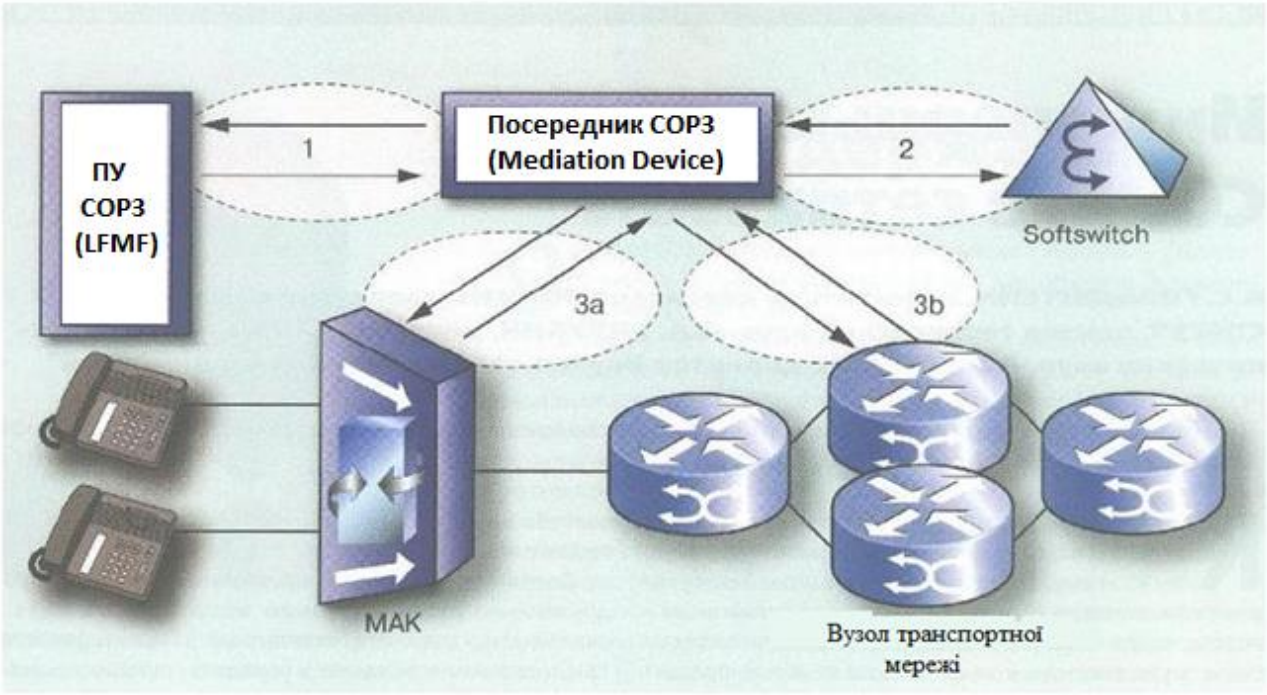


Рис.2.7. Схема підключення обладнання СОРМ до мережі NGN.

Інтерфейс 2 використовується для взаємодії посередника СОРЗ і пристрою керування мережею з метою розміщення користувачів для контролю, отримання повідомлення про їхні дії в мережі і т.д.. Узгодження інтерфейсів 1 і 3 забезпечується посередником, тим самим досягається незалежність функцій СОРЗ від обладнання NGN різних виробників. Інтерфейс 3 між посередником і медіа шлюзами (пристроями доступу або обладнанням транспортного рівня) призначений для отримання інформації користувача і що також може налаштовуватися на певний тип обладнання.

# 3 КОСТРУКТОРСЬКА ЧАСТИНА

## 3.1. Автоматизовані системи управління верхнього рівня

Автоматизована система управління (АСУ) розглядається як людино-машинна система, що забезпечує раціональне функціонування об’єкта керування шляхом використання обчислювальної, периферійної та організаційної техніки. Її розвиток супроводжується поступовим розширенням взаємозв’язків між окремими системами та підсистемами, які охоплюють керування технологічними процесами, оперативне управління, а також поточне й стратегічне планування. Сучасною тенденцією є інтеграція цих компонентів у багаторівневі комплексні системи управління.

АСУ визначається як сукупність математичних методів, технічних засобів (ЕОМ, телекомунікаційного обладнання, систем відображення інформації) та організаційних структур, що забезпечують ефективне керування складними об’єктами чи процесами відповідно до поставленої мети. Структурно система складається з базової та функціональної частин: перша охоплює інформаційне, технічне та математичне забезпечення, тоді як друга включає програмні комплекси, призначені для автоматизації управлінських функцій.

Інформаційне забезпечення АСУ являє собою комплекс рішень щодо складу, структури, розміщення та форм організації даних, які циркулюють у системі під час її роботи. Значна частина інформації, необхідної для ефективного функціонування виробничих та невиробничих об’єктів, сьогодні вже переведена у цифровий формат, а наявні мережеві інфраструктури здатні забезпечити її повноцінний обмін.

Разом з тим розвиток інформаційних технологій продовжує удосконалювати сучасні АСУ. Автоматизація технологічних процесів на верхньому рівні дедалі частіше включає програмні рішення з використанням

графічних інтерфейсів, новітніх засобів візуалізації та мультимедійних функцій, що підвищує інформативність і зручність керування.

Зокрема:

**SCADA-система iFIX** є високопродуктивним програмним комплексом для реалізації HMI, розробленим компанією Intellution, яка нині входить до складу GE Fanuc Automation. Лінійка продуктів FIX (Fully Integrated Control System) призначена для інтеграції у виробничі процеси різного масштабу та поєднує переваги рішень, створених для платформ UNIX і Windows.

Історично SCADA FIX охоплювала такі основні компоненти:

- клієнт-серверні HMI-додатки, що забезпечують збір, обробку, архівування та візуалізацію технологічних даних;
- VisualBatch — інструмент для конфігурації графічних інтерфейсів SCADA-систем;
- Web-сервер для відображення HMI в реальному часі через Інтернет;
- Broadcast Network — система передачі даних за технологією push;
- Paradym-31 — конфігуратор LCADA для керування програмованими логічними контролерами класу SoftLogic;
- PlantTV — застосунок для перегляду технологічних даних.

**Розподілена система управління (Distributed Control System, DCS)** — це комплекс апаратних і програмних засобів, призначених для побудови автоматизованих систем управління технологічними процесами, ключовими ознаками якого є децентралізована обробка даних, розподілені засоби введення та виведення інформації, підвищена відмовостійкість і єдина стандартизована база даних.

Поява та активний розвиток DCS пов’язані зі зростанням кількості датчиків, розширенням виробничих площ, ускладненням алгоритмів керування та необхідністю підвищення гнучкості систем. У таких системах

контролери, модулі введення/виведення, датчики та виконавчі механізми розташовуються територіально розподілено. Кожен ПЛК керує своєю частиною технологічного процесу і функціонує автономно, проте за потреби взаємодіє з іншими контролерами та контурами, забезпечуючи виконання загальних виробничих завдань і досягнення необхідних показників якості.

Сегменти DCS можуть бути віддалені один від одного на значні відстані, а їх взаємодія підтримується через мережеві канали, зокрема Інтернет. Такий підхід отримав додатковий імпульс розвитку завдяки поширенню об'єктно-орієнтованого програмування, яке сприяло стандартизації структур і методів опису технологічних об'єктів.

Оптимізація роботи DCS передбачає мінімізацію обміну даними між контролерами, тоді як узгодження їх роботи виконується на вищих рівнях ієрархії АСУ ТП [19].

**SCADA-система TRACE MODE** є спеціалізованим програмно-апаратним комплексом, призначеним для реалізації верхніх рівнів АСУ ТП, розробленим компанією AdAstra Research Group. Основними сферами її застосування є автоматизація будівель, технологічних процесів, систем обліку, а також програмування контролерів.

Після двох десятиліть інтенсивного розвитку TRACE MODE перетворилася на потужну інтегровану платформу, що включає понад десять редакторів для створення проектів різних рівнів АСУ. У межах системи поєднано широкі можливості SCADA/HMI, інструменти програмування контролерів типу SOFTLOGIC, а також модулі T-FACTORY, орієнтовані на інтеграцію з рівнем MES/ERP-систем..

**SCADA-система Citect** є одним із найефективніших програмних рішень для моніторингу та керування в АСУ ТП. Продукт, що спочатку розроблявся австралійською компанією Citect, нині входить до портфеля корпорації Schneider Electric — одного з провідних світових виробників рішень у сфері автоматизації. Завдяки високій масштабованості, надійності та гнучким

механізмам конфігурації CitectSCADA посідає провідне місце серед систем верхнього рівня АСУ ТП.

CitectSCADA ефективно масштабується як для невеликих виробництв, так і для великих підприємств із сотнями тисяч параметрів. Модульна клієнт-серверна архітектура дає змогу розподіляти функціональні компоненти між різними робочими станціями. Це забезпечує можливість адаптації системи до зростання навантаження та підтримання необхідного рівня продуктивності..

**MasterSCADA** є універсальною платформою для розроблення та конфігурації систем диспетчеризації та супервізорного керування в АСУ ТП. Продукт створений компанією InSAT і поєднує функціональні можливості як SCADA-систем, так і SoftLogic-рішень.

MasterSCADA фактично являє собою інтегроване середовище, яке об’єднує засоби розробки SCADA-додатків і конфігурації ПЛК. Усі параметри системи зосереджені в межах одного проекту, що істотно спрощує налаштування внутрішніх зв’язків і підвищує узгодженість функціонування всієї автоматизованої системи..

**SCADA-система InTouch** є однією з найпоширеніших програмних платформ для створення людино-машинних інтерфейсів.

Система забезпечує широкі можливості інтеграції з обладнанням провідних виробників автоматизаційних рішень, зокрема Siemens, ABB, Rockwell Automation та іншими. Завдяки великій бібліотеці графічних об’єктів і розвинутим засобам сценарного програмування InTouch використовується у багатьох галузях — від нафтогазової промисловості до харчового виробництва — для створення інформативних та функціонально насичених HMI-панелей. Wonderware InTouch складається з двох основних компонентів: середовища розробки та середовища виконання.

**Transparent Factory** — це концепція, запропонована компанією Schneider Electric, що слугує основою для створення інтегрованої промислової інфраструктури. Її головною метою є забезпечення ефективного

обміну інформацією між різними рівнями АСУ ТП, а також підтримка роботи OPC-серверів, Web-серверів та мережевої взаємодії на базі Ethernet. Таким чином концепція сприяє побудові єдиного інформаційного простору підприємства.

**ERP-системи** (Enterprise Resource Planning Systems) являють собою корпоративні програмні комплекси, призначені для автоматизованого обліку, планування та аналізу ключових бізнес-процесів підприємства.

Інформація, сформована ERP-системами, може передаватися на нижчі рівні автоматизації, зокрема до MES-систем, де вона використовується для оперативного перепланування, розподілу ресурсів та уточнення виробничих завдань. Попри певну спорідненість функцій, ERP і MES значно різняться: MES працюють ближче до реального часу і забезпечують швидку реакцію на зміни у виробничому процесі, тоді як ERP орієнтовані на стратегічне й тактичне планування підприємства..

**MES-системи** (Manufacturing Execution Systems) — це спеціалізовані програмні комплекси верхнього рівня АСУ ТП, призначені для аналізу, координації та оптимізації виробничих процесів у режимі, максимально наближеному до реального часу, на рівні цехового управління. Основною їхньою метою є забезпечення ефективного виконання виробничих планів і підвищення продуктивності виробничих підрозділів.

Одним із визначальних чинників ефективності MES є якість мережевої інфраструктури. Для забезпечення надійного обміну даними, масштабованості та підтримки зростаючих вимог до автоматизації необхідний розвиток телекомунікаційних технологій.

### 3.2. Необхідність автоматизації

Автоматизація забезпечується завдяки спільному використанню програмних додатків, що дозволяє організувати колективну роботу з різними

спеціалізованими інструментами для розв’язання професійних завдань. Це охоплює застосування засобів машинної графіки, формування звітної документації, підготовку публікацій тощо. Окрім внутрішніх сервісів, обчислювальні мережі дають змогу розгортати зовнішні інформаційні служби, такі як телетайпний зв’язок, електронні дошки оголошень чи електронні газети.

Сучасні засоби інформатики знайшли своє втілення в технологіях телеконференцій. Їхні учасники мають доступ до необхідних баз даних і можуть здійснювати автоматизоване опрацювання інформації. Поряд із цим мережеві технології забезпечують можливість проведення відеоконференцій, що дозволяють організовувати спільні зустрічі учасників з різних регіонів світу. Формування таких технологій потребує використання широкосмугових каналів зв’язку, комп’ютерних мереж і систем телебачення.

Невисока складність і відносно низька вартість мереж, побудованих на базі персональних комп’ютерів, сприяла їх широкому застосуванню в автоматизації технологічних і виробничих процесів. Їх використовують для побудови розподілених управлінських, інформаційно-довідкових, контрольно-вимірювальних систем, а також систем промислових роботів і гнучких виробничих комплексів. Успішність упровадження таких мереж визначається їх доступністю та значним соціально-економічним ефектом, який вони спричиняють у різних сферах діяльності.

Разом із тим відповідність апаратного забезпечення поставленим вимогам передбачає достатню продуктивність обчислювальної техніки та наявність необхідних периферійних пристроїв. Комплекс технічних засобів є фундаментом технічного забезпечення інформаційної системи менеджменту й охоплює всі пристрої, що реалізують функції обробки даних. Капітальні витрати на створення такої системи включають закупівлю та встановлення обладнання, а також модернізацію чи ремонт приміщень.

Більшість сучасних організацій мають географічно розподілену структуру, що зазвичай включає:

• центральний офіс;

• регіональні підрозділи;

• віддалені офіси;

• віддалених клієнтів.

Концепція побудови інформаційного середовища організації базується на таких принципах:

- інформація групується та зберігається в спеціалізованих підрозділах, відповідальних за її опрацювання та надання;
- програмні засоби розміщуються безпосередньо в точках їх практичного використання;
- доступ користувачів до необхідних даних здійснюється через комунікаційні засоби з пунктів концентрації інформації.

### 3.3. Прикордонний контролер сесій SBC

Одним із сучасних апаратно-програмних рішень мереж наступного покоління є прикордонний контролер сесій (Session Border Controller, SBC). Він призначений для забезпечення взаємодії різнорідних VoIP-мереж, підтримуючи роботу терміналів із різними протоколами сигналізації та наборами кодеків. Завдяки функціям Firewall, NAT і проксінгу сигнального та медіатрафіку SBC також виконує роль елемента захисту, приховуючи внутрішню структуру корпоративної мережі та запобігаючи зовнішнім атакам [19-20, 28].

SBC традиційно розміщується на межі корпоративної або операторської VoIP-мережі та виконує функції, які недоцільно покладати на гнучкий комутатор (softswitch). Softswitch відповідає за управління медіашлюзами та маршрутизацію викликів у межах ТМЗК та IP-мережі, тоді як SBC

орієнтований на підтримку широкого спектра сервісів реального часу — відео, мультимедіа, служб миттєвих повідомлень тощо. Пропускаючи через себе медіатрафік, SBC забезпечує контроль якості обслуговування, безпеку та управління смугою пропускання. Водночас маршрутизацію трафіку він не здійснює, тому взаємодія мереж потребує одночасного використання обох компонентів — Softswitch і SBC.

Важливо враховувати, що SBC взаємодіє з такими мережевими пристроями, як softswitch, міжмережевий екран і пристрої NAT, однак не замінює їх. Це обладнання є складовою NGN-інфраструктури та забезпечує надійність функціонування мережі, не надаючи послуги безпосередньо. Деякі виробники інтегрують SBC у складі інших продуктів, зокрема у softswitch або пристрої доступу, проте загальноприйнятою є концепція використання SBC як окремого елемента. Такий підхід забезпечує чітке розмежування функцій, зон безпеки та відповідальності.

*Основні функції SBC включають:*

- фільтрацію трафіку на мережевому рівні (3-й рівень моделі OSI);
- трансляцію мережевих адрес (NAT — Network Address Translation).

*До додаткових функцій SBC належать:*

- контроль і аналіз сигнального трафіку;
- нормалізація та узгодження різних версій протоколів сигналізації;
- обмеження обсягів трафіку (rate limiting) з метою захисту інфраструктури від DoS- та DDoS-атак;
- забезпечення механізмів обходу NAT-пристроїв (NAT traversal) для коректної роботи клієнтських терміналів.

Схема підключення SBC загалом відповідає принципам встановлення брандмауера — він розміщується між зовнішньою мережею та захищеними ресурсами. Для підвищення надійності застосовують резервування за схемою «гарячого» дублювання, коли один пристрій працює в активному режимі, а

інший перебуває в режимі очікування. Підключення SBC здійснюється через стандартні інтерфейси Fast Ethernet або Gigabit Ethernet.

Вибір конкретного рішення визначається вимогами до продуктивності (кількість одночасних сесій, обсяг трафіку) та функціональними потребами — підтримкою різних версій сигнальних протоколів, простим передаванням медіатрафіку або його транскодуванням тощо.

На практиці існує два основних способи включення SBC у мережеву інфраструктуру (рис. 3.1).

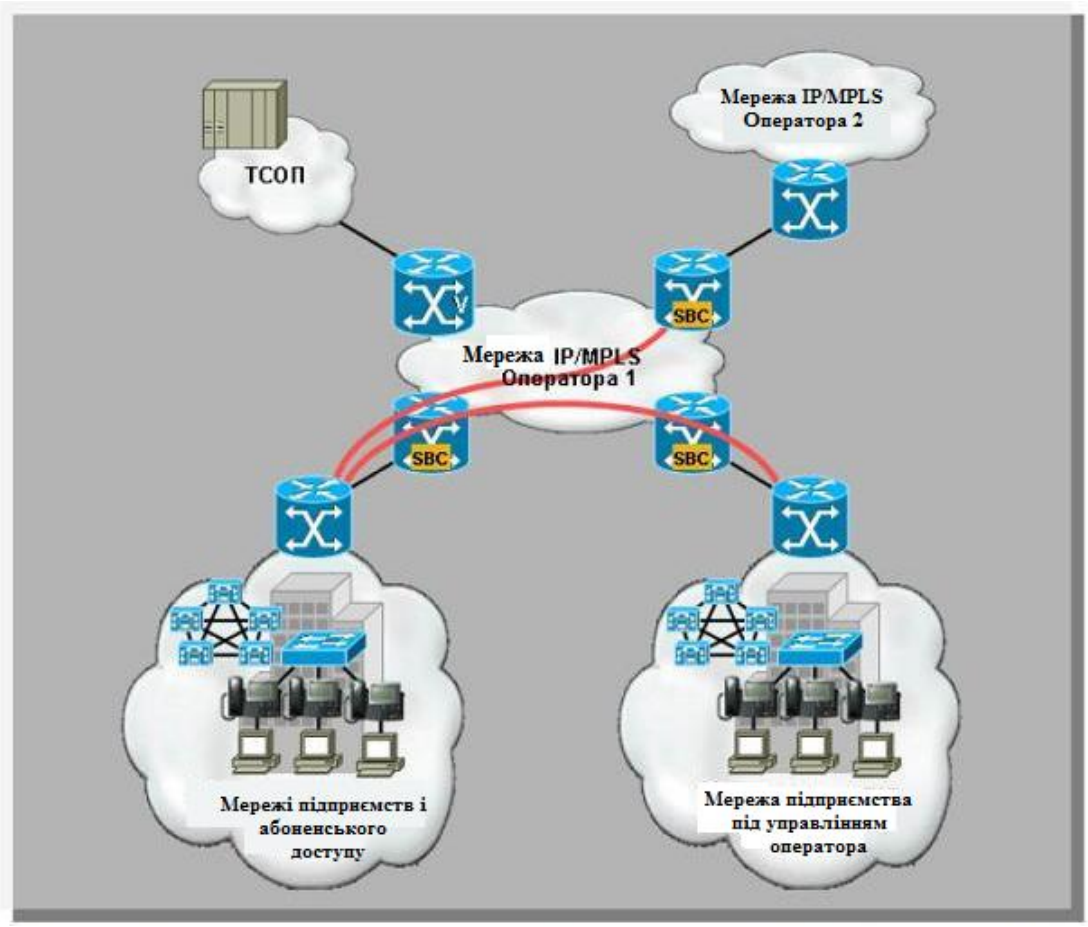


Рис. 3.1. Схема варіантів підключення SBS в мережі NGN

1. Установлення SBC на межі мереж різних операторів, що забезпечує узгодження протоколів, безпечний обмін трафіком та контроль взаємодії між операторськими платформами.

2. Установлення SBC на межі операторської мережі та корпоративних мереж, що дає змогу організувати захищений доступ корпоративних систем до сервісів оператора та забезпечити узгодження параметрів VoIP-трафіку.

### 3.4. Централізоване збереження даних

Мережа зберігання даних (Storage Area Network, SAN) — це високошвидкісна мережа передавання даних, що об’єднує сервери, робочі станції, дискові масиви, стрічкові бібліотеки та інші зовнішні пристрої зберігання. Її архітектура забезпечує таке підключення цих пристроїв до серверів, за якого операційна система розпізнає їх як локальні ресурси. У SAN застосовуються протоколи Fibre Channel та iSCSI, що дає змогу передавати інформацію на значні відстані — до десятків кілометрів.

Основними призначеннями SAN є оптимізація інфраструктури підприємства та забезпечення безперервності бізнес-процесів. Найпоширеніший сценарій використання SAN — консолідація корпоративної інформації у випадках, коли існує велика кількість різних систем зберігання і виникає потреба в об’єднанні їхніх можливостей [17,27].

Використання мереж SAN суттєво покращує управління даними та підвищує ефективність роботи систем, що здійснюють диспетчеризацію ресурсів зберігання. Застосування технології SAN дозволяє:

- підвищити швидкість і надійність передавання даних;
- оптимізувати доступ до віддалених систем зберігання;
- прискорити процеси резервного копіювання та відновлення;
- здійснювати масштабування інфраструктури без її зупинки;
- інтегрувати різнотипні пристрої зберігання в єдину систему;
- забезпечити централізоване управління підсистемою зберігання.

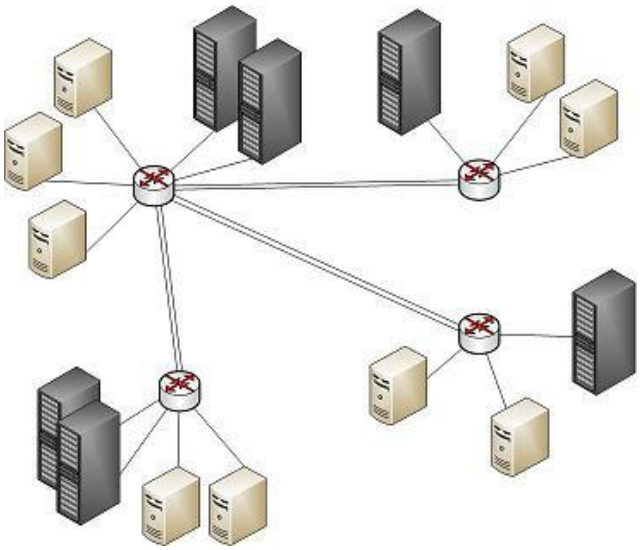

Рисунок 3.2. Каскадна структура SAN

Обрано топологію SAN каскадної структури. Каскадована топологія (cascaded fabric) являє собою сукупність комутаторів, об’єднаних у деревоподібну структуру за допомогою міжкомутаторних каналів ISL (Inter-Switch Links) (рис. 3.2). Під час первинного налаштування мережі комутатори автоматично визначають головний вузол (principal switch) і присвоюють міжкомутаторним з’єднанням статуси «upstream» або «downstream» залежно від їх напрямку — відповідно до центрального комутатора чи периферійних пристроїв.

Для забезпечення взаємодії між серверами та системами зберігання в межах шинної топології використовується протокол SCSI, тоді як передавання команд SCSI по мережі здійснюється за допомогою низькорівневого протоколу iSCSI, який інкапсулює ці команди у стек TCP/IP.

Найбільш ефективним підходом до оптимізації централізованого зберігання даних є консолідація серверів і систем зберігання. У традиційній інфраструктурі кожен сервер використовує власний масив даних, що ускладнює управління та знижує ефективність використання ресурсів. Впровадження SAN дозволяє зменшити витрати, скоротити час простоїв,

підвищити масштабованість і керованість інфраструктури завдяки спільному використанню накопичувачів.

Застосування SAN також підвищує продуктивність інфраструктури, оскільки спеціалізовані протоколи, використовувані в цих мережах, оптимізовані для інтенсивного передавання даних. Інтенсивні потоки, зокрема запити до баз даних або трафік резервного копіювання, можуть передаватися в обхід основної корпоративної мережі, що зменшує навантаження на неї та підвищує швидкодію критично важливих застосунків.

Для вирішення завдань керування системами зберігання доцільно використовувати спеціалізоване програмне забезпечення, яке забезпечує централізований контроль і оптимізацію ресурсів у розподілених інфраструктурах. Одним з таких рішень є BrightStor SRM компанії Computer Associates International, Inc. (CA) — потужний кросплатформенний інструмент для моніторингу, аналізу, формування звітів, прогнозування трендів і планування ресурсів зберігання. Використання цього програмного забезпечення забезпечує ефективне планування ємності та автоматизоване управління подіями, пов’язаними з обробкою та зберіганням даних.

### 3.5. BrightStor SRM

До ключових можливостей BrightStor SRM належать:

- наскрізне централізоване управління ресурсами зберігання даних у розподіленому середовищі;
- аналіз взаємодії прикладних програм і підсистем зберігання, що дозволяє оцінити вплив додатків на використання ресурсів і оптимізувати їхню роботу;
- орієнтація на бізнес-процеси**,** що забезпечується застосуванням розширеної класифікації даних відповідно до пріоритетів організації;

- розширені функції системного управління**,** включаючи автоматизацію операцій, пов’язаних із зберіганням, аналізом та обслуговуванням даних;
- планування готовності систем зберігання за допомогою засобів візуалізації Virtualization Engine.

BrightStor SRM реалізує сучасні методи управління ресурсами зберігання даних, що дозволяє підвищити продуктивність інфраструктури, забезпечити високу якість послуг та досягти низки переваг, серед яких:

- повторне використання та ефективне планування ємності систем зберігання;
- планування консолідації даних і серверів;
- планування переміщення та міграції даних;
- оптимізація процесів резервного копіювання та відновлення;
- управління квотами користувачів;
- контроль використання ресурсів пам’яті;
- підвищення рівня сервісного обслуговування;
- централізоване управління розподіленими середовищами;
- моніторинг та оптимізація роботи прикладних програм, що інтенсивно використовують ресурси;
- забезпечення безперервного та надійного доступу до даних;
- формування масштабованої та ефективної інфраструктури мереж зберігання.

## 3.6. Підбір серійного обладнання

### IES-5000 — модульний IP NGN-комутатор

Модульний комутатор IES-5000 належить до рішень нового покоління широкосмугового доступу та підтримує надання послуг традиційної телефонії, а також технологій ADSL2/2+, SHDSL та VDSL2. Пристрій вирізняється зниженим енергоспоживанням, високою надійністю,

розширеним діапазоном робочих температур, а також підтримкою гарячої заміни та резервування критично важливих модулів.

IES-5000 забезпечує гнучку інтеграцію в IP-мережі завдяки використанню лінійних модулів FXS, ADSL2/2+, VDSL2 та SHDSL.bis з високою щільністю портів. Наявність модулів пакетної телефонії, розвиненої підтримки багатоадресної розсилки та механізмів пріоритизації й захисту абонентського трафіку робить цей комутатор ефективним рішенням для масового впровадження послуг Triple Play.

Шасі IES-5000M призначене для монтажу в 19-дюймову стійку і при висоті 6,5U передбачає розміщення восьми лінійних модулів, двох модулів керування та комутації, а також двох блоків живлення. Така конфігурація забезпечує повне резервування критично важливих компонентів. Комутатор підтримує підключення:

до 576 абонентів ADSL2+,

до 384 абонентів традиційної телефонії,

до 384 абонентів SHDSL,

до 192 абонентів VDSL2,

Допускаючи довільне поєднання модулів та видів послуг. ADSL-спліттери можуть монтуватися в окремому шасі висотою 5U або безпосередньо на кросі.

Комутатор підтримує використання:

72-портових модулів ADSL2+ (ALC1272G-51);

48-портових модулів FXS (VOP1248G-61);

48-портових модулів ADSL2+ Annex A (ALC1248-51) або Annex B (ALC1248-53);

48-портових модулів SHDSL (SLC1248-22);

24-портових модулів VDSL2.

Усі модулі підтримують гарячу заміну без зупинки роботи комутатора. Агрегація трафіку відбувається на модулях керування і комутації через шини

Gigabit Ethernet, що дає змогу реалізувати повну пропускну здатність сучасних стандартів і забезпечити абонентам максимально високі швидкості доступу.

Для підвищення надійності комутатор може комплектуватися двома однаковими керуючими модулями MSC1000G, які забезпечують повне резервування функцій управління та комутації. У менш критичних застосуваннях допускається робота лише з одним модулем.

**Медіа-шлюз операторського класу (Media Gateway Carrier Grade)**

Медіа-шлюз SI2000 є високонадійним шлюзом операторського класу, призначеним для забезпечення взаємодії між мережами з комутацією каналів (потоки E1 зі швидкістю 2 Мбіт/с) та мережами наступного покоління NGN, що використовують пакетну комутацію. Завдяки підтримці як традиційних послуг комутації каналів, так і IP-послуг на єдиній платформі, шлюз характеризується високою масштабованістю та надійністю, що робить його придатним як для операторських мереж загального користування, так і для корпоративних інфраструктур.

Продукт розроблений на основі перевіреного ПЗ транзитної станції SI2000 і може функціонувати автономно або під управлінням сервера обробки викликів SI2000 CS, а також сумісний із комутаторами, що працюють за протоколом H.323.

Для взаємодії з вищими мережевими елементами використовуються протоколи, реалізовані відповідно до стандартів SIGTRAN (IUA/SCTP) або H.323. На стороні потоків E1 шлюз підтримує сигналізації SS7 та DSS1, що забезпечує його сумісність із традиційними мережами ТМЗК.

Оскільки SI2000 розрахований на експлуатацію в конфігураціях з високою щільністю, він оснащений резервованими блоками електроживлення та дубльованим Ethernet-комутатором, що гарантує безперервність роботи та відмовостійкість системи.

**Мультисервісний вузол доступу (MSAN)**

Мультисервісний вузол доступу SI2000 є ключовим елементом конвергентних мереж, оскільки забезпечує універсальний і економічно ефективний спосіб впровадження послуг наступного покоління. Гнучка модульна архітектура, потужний процесор, пул цифрових сигнальних процесорів (DSP), вбудований TDM-комутатор і DSLAM-мультиплексор з підтримкою IP дозволяють застосовувати систему як у глобальних корпоративних мережах, так і в інфраструктурах локальних операторів.

MSAN виконує перетворення інформації між мережами з комутацією каналів і пакетів, а також забезпечує узгодження сигналізації між лініями ТМЗК або ISDN (BRI, PRI) та мережевими інтерфейсами H.323 чи MGCP-SIGTRAN. Завдяки вбудованому DSLAM широкосмугові DSL-лінії можуть забезпечувати безпосередній доступ користувачів до IP-мережі через інтерфейс Ethernet.

Конструктивно вузол являє собою 24-слотове шасі, до якого можна підключити до 22 периферійних плат із такими характеристиками:

- 32 аналогові лінії,
- 16 ISDN-ліній,
- 24 DSL-лінії.

ISDN-термінали підключаються безпосередньо через шину або через блоки NT та шину Uko. DSL-лінії можуть підключатися напряму або через плату роздільників. У цьому випадку два слоти можуть бути використані для підключення міні-вузла широкосмугового доступу (mBAN).

**Міні-вузол широкосмугового доступу (mBAN)**

mBAN — це компактне DSLAM-рішення у вигляді однієї плати, яка містить:

- плату управління;

- абонентські DSL-інтерфейси;
- мережевий інтерфейс.

Підтримуються технології ADSL та G.shdsl, що використовують традиційні виті пари як фізичне середовище передавання. Модуль оснащений 24-портовою платою DSL (ADSL або G.shdsl) і має три слоти для дочірніх плат:

- слот плати управління,
- слот каскадного підключення,
- слот висхідної лінії.

Електроживлення забезпечується системами SI2000 або сумісними рішеннями сторонніх виробників; можливе підключення резервних акумуляторних модулів для підвищення відмовостійкості.

# 4 НАУКОВО-ДОСЛІДНА ЧАСТИНА

## 4.1. Проектування та дослідження мережевої конфігурації на основі NGN рішень

Проєктування здійснюється для визначеної зони автоматизації з подальшою інтеграцією наявних мереж. Для кожної групи мереж передбачається встановлення шлюзу доступу, який забезпечує функціонування відповідної зони та її підключення до NGN-сегмента.

Кількість зон автоматизації та комутаторів, що здійснюють їх підключення до NGN, приймається відповідно до даних (табл. 4.1).

***Розрахунок обладнання шлюзів:***

Кількість шлюзів доступу визначається з урахуванням критичної довжини абонентських ліній, топології первинної мережі, можливостей розміщення обладнання, а також технічних характеристик обраних рішень.

Табл. 4.1. Сегменти під’єднані до NGN мережі

| Шлюз доступу | Число абонентів ТМЗК | Число абонентів ISDN-BRA | Число мереж доступу/ число потоків Е1 | Число підключених УВАТС/ число потоків Е1 | Число підключених LAN/ кількість абонентів в кожній | Число абонентів, з терміналами SIP/H.223/MGCP |
|---|---|---|---|---|---|---|
| 1 | 1000 | 50 | AN11:15E1<br>AN12:5E1<br>AN13:8E1 | PBX11:1E1<br>PBX12:3E1 | LAN11:350 | 700 |
| 2 | 500 | 200 | AN21:10E1<br>AN22:8E1<br>AN23:10E1 | PBX21:1E1<br>PBX22:1E1<br>PBX23:5E1 | LAN21:400<br>LAN22:500 | 800 |
| 3 | 800 | 100 | AN31:5E1<br>AN32:6E1 | PBX31:3E1<br>PBX32:4E1 | LAN31:150<br>LAN32:200<br>LAN33:250 | 900 |

Відповідно до критерію граничної довжини абонентської лінії зона обслуговування шлюзу доступу формується таким чином, щоб її максимальна протяжність не перевищувала 3–4 км. У разі підключення через інтерфейси V5, LAN або УВАТС зона обслуговування шлюзу охоплює також зони обслуговування під'єднаних об'єктів.

На основі визначеної зони обслуговування встановлюються ємнісні параметри шлюзу, що характеризують загальну кількість абонентів та розподіл ємностей за типами підключення.

Введемо наступні позначення:

$N_{ISDN}$ – кількість абонентів, підключених за базовим доступом ISDN.

$N_{LAN}$ – кількість локальних мереж (LAN), підключених до Ethernet-маршрутизатора на рівні шлюзу доступу;

$N_{i\_LAN}$ – кількість абонентів, підключених до і-тої локальної мережі.

$N_{PBX}$ – кількість установчих виробничих автоматичних телефонних станцій (УВАТС), підключених до шлюзу доступу;

$N_{k\_PBX}$ – кількість каналів в інтерфейсі підключення k-тої УВАТС;

$N_{V5}$ – кількість сесій доступу інтерфейсу V5, підключених до шлюзу;

$N_{j\_V5}$ – кількість каналів в інтерфейсі V5 j-тої мережі доступу;

$N_{PSTN}$ – кількість абонентів, підключених за аналоговими абонентськими лініями;

$N_{SHM}$ – кількість абонентів із терміналами SIP/H.323/MGCP, які не використовують Ethernet-підключення на рівні маршрутизатора шлюзу доступу.

Нехай:

1. $Y_{PSTN}$ – загальне навантаження, що потрапляє на шлюз доступу від абонентів PSTN.

$y_{PSTN}$ – віддалене навантаження від абонентів ТМЗК. Вважатимемо, що $y_{PSTN}$=0,1 ерл.

Тоді:

$$Y_{PSTN} = N_{PSTN} \cdot y_{PSTN} \quad (4.1)$$

$$Y_{PSTN1} = N_{PSTN1} \cdot y_{PSTN} = 1000 \cdot 0{,}1 = 100 \text{ ерл.}$$

$$Y_{PSTN2} = N_{PSTN2} \cdot y_{PSTN} = 500 \cdot 0{,}1 = 50 \text{ ерл.}$$

$$Y_{PSTN3} = N_{PSTN3} \cdot y_{PSTN} = 800 \cdot 0{,}1 = 80 \text{ ерл.}$$

2. $Y_{ISDN}$ – загальне навантаження, що потрапляє на шлюз доступу віл абонентів ISDN

$y_{ISDN}$ – віддалене навантаження від абонентів ISTN. Вважатимемо, що $y_{ISDN}$=0,2 ерл.

Тоді:

$$Y_{ISDN} = N_{ISDN} \cdot y_{ISDN} \quad (4.2)$$

$$Y_{ISDN1} = N_{ISDN1} \cdot y_{ISDN} = 50 \cdot 0{,}2 = 10 \text{ ерл.}$$

$$Y_{ISDN2} = N_{ISDN2} \cdot y_{ISDN} = 200 \cdot 0{,}2 = 40 \text{ ерл.}$$

$$Y_{ISDN3} = N_{ISDN3} \cdot y_{ISDN} = 100 \cdot 0{,}2 = 20 \text{ ерл.}$$

3. $Y_{j\_V5}$ – загальне навантаження, від мережі доступу j інтерфейсу V5, що підключається до шлюзу доступу.

$y_{V5}$ – віддалене навантаження одного користувацького каналу інтерфейсу V5. Вважатимемо, що $y_{V5}$=0,8 ерл.

Тоді:

$$Y_{j\_V5} = N_{j\_V5} \cdot y_{V5} \quad (4.3)$$

$$Y_{1\ V5} = N_{1\ V5} \cdot y_{V5} = (15 + 5 + 8) \cdot 0{,}8 = 22{,}4 \text{ ерл.}$$

$$Y_{2\ V5} = N_{2\ V5} \cdot y_{V5} = (10 + 8 + 10) \cdot 0{,}8 = 22{,}4 \text{ ерл.}$$

$$Y_{3\ V5} = N_{3\ V5} \cdot y_{V5} = (5 + 6) \cdot 0{,}8 = 8{,}8 \text{ ерл.}$$

4. $Y_{k\_PBX}$ – загальне навантаження, від МВАТС л, підключеної до шлюзу.

$y_{PBX}$ – віддалене навантаження одного користувацького каналу первинного доступу ISDN. Вважатимемо, що $y_{k\_PBX}$ =0,8 ерл.

Тоді:

$$Y_{k\ PBX} = N_{k\ PBX} \cdot y_{PBX} \quad (4.4)$$

$$Y_{1\ PBX} = N_{1\ PBX} \cdot y_{PBX} = (1 + 3) \cdot 0{,}8 = 3{,}2 \text{ ерл.}$$

$$Y_{2\ PBX} = N_{2\ PBX} \cdot y_{PBX} = (1+1+5) \cdot 0{,}8 = 5{,}6 \text{ ерл.}$$

$$Y_{3\ PBX} = N_{3\ PBX} \cdot y_{PBX} = (3+4) \cdot 0{,}8 = 5{,}6 \text{ ерл.}$$

Виходячи з цього:

1. Загальне навантаження, що надходить від абонентів ТМЗК і ISDN на резедентний шлюз доступу рівне.

$$Y_{RAGW} = Y_{PSTN} \cdot Y_{ISDN} = 0{,}1 \cdot N_{PSTN} + 0{,}2 \cdot N_{ISDN} \qquad (4.5)$$

$$Y_{RAGW1} = Y_{PSTN1} \cdot Y_{ISDN1} = 100 + 10 = 110 \text{ ерл.}$$

$$Y_{RAGW2} = Y_{PSTN2} \cdot Y_{ISDN2} = 50 + 40 = 90 \text{ ерл.}$$

$$Y_{RAGW3} = Y_{PSTN3} \cdot Y_{ISDN3} = 80 + 20 = 100 \text{ ерл,}$$

Оскільки шлюз поєднує функції резидентного шлюзу доступу, шлюзу доступу та транкінгового шлюзу підключення УВАТС, сумарне навантаження, що припадає на нього, визначається як:

$$Y_{GW} = Y_{RAGW} + Y_{k_{PBX}} + Y_{j\_V5} \qquad (4.6)$$

$$Y_{GW1} = Y_{RAGW1} + Y_{1\ PBX} + Y_{1\ V5} = 110 + 3{,}2 + 22{,}4 = 136{,}5 \text{ ерл.}$$

$$Y_{GW2} = Y_{RAGW2} + Y_{2\ PBX} + Y_{2\ V5} = 90 + 5{,}6 + 22{,}4 = 118 \text{ ерл.}$$

$$Y_{GW3} = Y_{RAGW3} + Y_{3\ PBX} + Y_{3\ V5} = 100 + 5{,}6 + 8{,}8 = 114{,}4 \text{ ерл.}$$

Нехай $V_{COD\_m}$ – швидкість передачі кодеку типу m обслуговування виклику.

Однією з ключових характеристик кодеків є складність алгоритму кодування, зумовлена необхідністю обробки даних у реальному часі. Алгоритмічна складність визначає швидкодію, яка оцінюється показником MIPS (Millions of Instructions per Second), та безпосередньо впливає на габарити, вартість і енергоспоживання кодуючих, декодуючих або комбінованих пристроїв.

Розмір кадру кодека істотно впливає на якість мовного сигналу: збільшення тривалості кадру підвищує ефективність моделювання, однак одночасно призводить до зростання затримки обробки. Таким чином, вибір

розміру кадру є компромісом між якістю передавання та допустимою затримкою.

Загальна затримка зростає зі збільшенням як розміру кадру, так і складності алгоритму кодування. Для мовного трафіку допустима одностороння затримка не повинна перевищувати 250 мс.

За результатами узагальненої оцінки технічних характеристик обрано кодек G.726. Відповідно, транспортний ресурс, який необхідно виділити в пакетній мережі для передавання трафіку на шлюз, визначається за умови використання кодека m (G.726).

$$V_{GW\ LSER} = k \cdot V_{COD\ m} \cdot Y_{GW} \qquad (4.7)$$

Де $k$ – коефіцієнт використання ресурсу. $k$ = 1,25

$V_{COD\ m}$ – для кодека G.726 рівне 69 кбит/с

$V_{GW\_LSER1} = k \cdot V_{COD_m} \cdot Y_{GW1} = 1{,}25 \cdot 69 \cdot 136{,}5 = 11{,}773$ Мбит/с.

$V_{GW\_LSER2} = k \cdot V_{COD_m} \cdot Y_{GW2} = 1{,}25 \cdot 69 \cdot 118 = 10{,}178$ Мбит/с.

$V_{GW\_LSER3} = k \cdot V_{COD_m} \cdot Y_{GW3} = 1{,}25 \cdot 69 \cdot 114{,}4 = 9{,}867$ Мбит/с.

З урахуванням підтримки підключення користувачів із терміналами SIP, H.323 та LAN, необхідний транспортний ресурс шлюзів доступу підлягає збільшенню. Частка цього збільшення визначається на основі характеристик трафіку відповідних сервісів.

Транспортний ресурс шлюзу повинен забезпечувати передавання не лише користувацького, а й сигнального трафіку. Розрахунок необхідної пропускної здатності виконується після визначення параметрів комутаційного обладнання.

Після встановлення величини транспортного ресурсу визначаються ємнісні показники підключення, зокрема кількість і тип інтерфейсів, за допомогою яких шлюзи доступу інтегруються з пакетною мережею. Вибір кількості інтерфейсів залежить як від необхідної пропускної здатності, так і від топології мережі..

***Розрахунок обладнання гнучкого комутатора:***

Основною функцією гнучкого комутатора є обробка сигнальної інформації викликів і керування процесом встановлення з'єднань. Для реалізації цих функцій застосовуються різні протоколи сигналізації.

Введемо наступні змінні:

$P_{PSTN}$ – питома інтенсивність викликів від абонентів, підключених через аналогові абонентські лінії.

$P_{ISDN}$ – питома інтенсивність викликів від абонентів, що використовують базовий доступ ISDN.

$P_{V5}$ – питома інтенсивність викликів, приведена до одного каналу інтерфейсу V5, від абонентів, підключених до пакетної мережі.

$P_{PBX}$ – питома інтенсивність викликів, приведена до одного каналу інтерфейсу, від УВАТС, підключених до пакетної мережі.

PSHM – питома інтенсивність викликів від абонентів, які використовують термінали SIP, H.323 або MGCP.

Приймемо інтенсивність викликів рівною наступним значенням:

$P_{PSTN}$ = 10 викликів/ГНН.

$P_{ISDN}$ = 20 викликів/ГНН.

$P_{PBX}$ = 70 викликів/ГНН.

Значення $P_{SHM}$ можна прийняти рівним $P_{PSTN}$, значення $P_{V5}$ можна прийняти рівним $P_{PBX}$

Загальна інтенсивність викликів, що потрапляє на гнучкий комутатор від джерел всіх типів рівна:

$$P_{CALL} = P_{PSTN}\left(\sum_{i=1}^{L} N_{PSN} + \sum_{i=1}^{L} N_{SHM}\right) + P_{ISDN}\sum_{i=1}^{L} N_{ISDN} +$$

$$+P_{V5}\left(\sum_{i=1}^{L} N_{j_{V5}} + \sum_{i=1}^{L} K_{k_{PBX}}\right) \qquad (4.8)$$

$$P_{CALL} = 10(1000 + 500 + 800 + 700 + 800 + 900) + 20(50 + 200 +$$

$+100) + 70 \cdot (28 + 28 + 11 + 4 + 7 + 7) = 59950$

Де L – число шлюзів , що обслуговує гнучкий комутатор.

Питома продуктивність комутаційного обладнання може відрізнятися в залежності від типу виклику, що обслуговується. В документації на комутаційне обладнання, як правило, вказується продуктивність для найбільш «простого» типу викликів. В зв'язку з чим при визначенні вимог до продуктивності вводяться поправочні коефіцієнти, які характеризують можливості системи по обслуговуванню даного типу викликів відносно «ідеального» типу.

Таким чином, нижня межа продуктивності гнучкого комутатора по обслуговуванні потоку викликів з врахуванням значення інтенсивності викликів.

$$P_{SX} = 5(k_{PSTN} \cdot N_{PSTN} + 2 \cdot k_{ISDN} \cdot N_{ISDN} + 7 \cdot k_{V5} \cdot N_{V5} + 7 \cdot k_{PBX} \cdot N_{PBX} + k_{SHM} \cdot N_{SHM}) \quad (4.9)$$

$P_{SX1} = 5(1{,}25 \cdot 1000 + 2 \cdot 1{,}3 \cdot 50 + 7 \cdot 1{,}5 \cdot 28 + 7 \cdot 1{,}6 \cdot 4 + 1{,}5 \cdot 700) = 15412$ викликів/ГНН.

$P_{SX2} = 5(1{,}25 \cdot 500 + 2 \cdot 1{,}3 \cdot 200 + 7 \cdot 1{,}5 \cdot 28 + 7 \cdot 1{,}6 \cdot 7 + 1{,}5 \cdot 800) = 13587$ викликів/ГНН.

$P_{SX3} = 5(1{,}25 \cdot 800 + 2 \cdot 1{,}3 \cdot 100 + 7 \cdot 1{,}5 \cdot 11 + 7 \cdot 1{,}6 \cdot 7 + 1{,}5 \cdot 900) = 14020$ викликів/ГНН.

*Ємнісні параметри:*

Ємнісні параметри абонентської бази гнучкого комутатора мають забезпечувати обслуговування всіх типів абонентів, підключення яких передбачається під час вибору абонентського концентратора.

*Параметри інтерфейсів підключення до пакетної мережі:*

Параметри інтерфейсу підключення до пакетної мережі визначаються з урахуванням інтенсивності обміну сигнальними повідомленнями під час обслуговування викликів.

Нехай:

$L_{MEGACO}$ – середня довжина повідомлення протоколу MEGACO (у байтах), що використовується для передавання сигнальної інформації по абонентських лініях.

$N_{MEGACO}$ – середня кількість повідомлень протоколу MEGACO під час обслуговування одного виклику.

$L_{V5UA}$ – середня довжина повідомлення протоколу V5UA.

$N_{V5UA}$ – середня кількість повідомлень протоколу V5UA при обслуговуванні виклику.

$L_{IUA}$ – середня довжина протоколу IUA.

$N_{IUA}$ – середня кількість повідомлень протоколу IUA при обслуговуванні виклику

$L_{SH}$ – середня довжина повідомлення протоколу SIP.

$H_{SH}$ – середня кількість SIP-повідомлень під час обслуговування виклику.

$L_{MGCP}$ – середня довжина повідомлення протоколу MGCP, що використовується для керування комутацією в шлюзі.

$N_{MGCP}$ – середня кількість повідомлень протоколу MGCP при обслуговуванні виклику.

Тоді:

$$V_{SX} = k_{sig} \cdot [(L_{MEGACO} \cdot N_{MEGACO} \cdot P_{PSTN} \cdot N_{PSTN} + L_{V5UA} \cdot N_{V5UA} \cdot P_{V5} \cdot N_{V5} +$$
$$+L_{IUA} \cdot N_{IUA} \cdot (P_{ISDN} \cdot N_{ISDN} + P_{PBX} \cdot N_{PBX}) + L_{SH} \cdot N_{SH} \cdot P_{SH} \cdot N_{SH} +$$
$$+L_{MGCP} \cdot N_{MGCP} \cdot (P_{PSTN} \cdot N_{PSTN} + P_{V5UA} \cdot N_{V5UA} + P_{ISDN} \cdot N_{ISDN} +$$
$$+P_{PBX} \cdot N_{PBX})]/450 \qquad (4.10)$$

$V_{SX}$ – мінімальний корисний транспортний ресурс у біт/с, з яким SX має бути підключений до пакетної мережі, визначається з умови забезпечення обслуговування викликів в інфраструктурі абонентського концентратора..

$k_{sig}$ – коефіцієнт використання транспортного ресурсу під час передавання сигнального навантаження. По аналогії з розрахунком сигнальної мережі SS7, приймемо значення $k_{sig} = 5$, що відповідає завантаженню в 0,2 ерл.

1/450 – результат проведення розмірностей «байт в год» до «біт в секунду» (8/3600=1/450). Значення 1/90, приведене нижче отримується при використанні $k_{sig} = 5$. Тоді $5 \cdot 1/450 = 1/90$.

Оскільки наведені параметри визначаються на основі моніторингу наявних мереж, аналізу статистичних даних і порівняння з очікуваними результатами, для подальших розрахунків приймаються узагальнені значення: середня довжина сигнальних повідомлень — 50 байт, середня кількість повідомлень під час обслуговування одного виклику — 10.

Підставивши ці значення у формулу визначення мінімального корисного транспортного ресурсу, отримаємо її спрощений вигляд:

$$V_{SX} = 5 \cdot (11 \cdot N_{PSTN} + 78(N_{V5} + N_{PBX}) + 22 \cdot N_{ISDN} + 6{,}5 \cdot N_{SH}) \text{ біт/с}$$

$$V_{SX1} = 5(11 \cdot 1000 + 78(28 + 700) + 22 \cdot 50 + 6{,}5 \cdot 700) = 367170 \text{біт/с}$$

$$V_{SX2} = 5(11 \cdot 500 + 78(28 + 800) + 22 \cdot 200 + 6{,}5 \cdot 800) = 398420$$

біт/с

$$V_{SX3} = 5(11 \cdot 800 + 78(11 + 900) + 22 \cdot 100 + 6{,}5 \cdot 900) = 439540$$

біт/с

Для розрахунку транспортного ресурсу шлюзів, призначеного для передавання сигнальної інформації, доцільно використовувати ті самі параметри, що й при визначенні транспортного ресурсу гнучкого комутатора. Відповідно, для забезпечення обслуговування викликів різних типів необхідно передбачити такі смуги пропускання:

$$V_{PSTN} = (P_{PSTN} \cdot N_{PSTN} \cdot L_{MEGACO} \cdot N_{MEGACO})/90 \text{ біт/с} \quad (4.11)$$

$V_{PSTN1} = (10 \cdot 1000 \cdot 50 \cdot 10)/90 = 55556$ біт/с

$V_{PSTN2} = (10 \cdot 500 \cdot 50 \cdot 10)/90 = 27778$ біт/с

$V_{PSTN3} = (10 \cdot 800 \cdot 50 \cdot 10)/90 = 44445$ біт/с

$$V_{ISDN} = (P_{ISDN} \cdot N_{ISDN} \cdot L_{IUA} \cdot N_{IUA})/90 \text{ біт/с} \quad (4.12)$$

$V_{ISDN1} = (20 \cdot 50 \cdot 50 \cdot 10)/90 = 5556$ біт/с

$V_{ISDN2} = (20 \cdot 200 \cdot 50 \cdot 10)/90 = 22222$ біт/с

$V_{ISDN3} = (20 \cdot 100 \cdot 50 \cdot 10)/90 = 11111$ біт/с

$$V_{V5} = (P_{V5} \cdot N_{V5} \cdot L_{V5UA} \cdot N_{V5UA})/90 \text{ біт/с} \quad (4.13)$$

$V_{1\ V5} = (70 \cdot 28 \cdot 50 \cdot 10)/90 = 10889$ біт/с

$V_{2\ V5} = (70 \cdot 28 \cdot 50 \cdot 10)/90 = 10889$ біт/с

$V_{3\ V5} = (70 \cdot 11 \cdot 50 \cdot 10)/90 = 4278$ біт/с

$$V_{PBX} = (P_{PBX} \cdot N_{PBX} \cdot L_{IUA} \cdot N_{IUA})/90 \text{ біт/с} \quad (4.14)$$

$V_{PBX1} = (70 \cdot 4 \cdot 50 \cdot 10)/90 = 1556$ біт/с

$V_{PBX2} = (70 \cdot 7 \cdot 50 \cdot 10)/90 = 2722$ біт/с

$V_{PBX3} = (70 \cdot 7 \cdot 50 \cdot 10)/90 = 2722$ біт/с

Крім того, у шлюзі необхідно передбачити транспортний ресурс для обміну сигнальними повідомленнями протоколу MGCP, який використовується для керування шлюзами. Обсяг цього ресурсу визначається відповідною розрахунковою формулою.

$$V_{MGCP} = [(P_{PSTN} \cdot N_{PSTN} + P_{ISDN} \cdot N_{ISDN} + P_{V5} \cdot N_{V5} + P_{PBX} \cdot N_{PBX}) \cdot \cdot L_{MGCP} \cdot N_{MGCP}]/90 \text{ біт/с} \quad (4.15)$$

$V_{MGCP1} = [(10 \cdot 1000 + 20 \cdot 50 + 70 \cdot 28 + 70 \cdot 4) \cdot 50 \cdot 10]/90 = 73556$ біт/с.

$V_{MGCP2} = [(10 \cdot 500 + 20 \cdot 200 + 70 \cdot 28 + 70 \cdot 4) \cdot 50 \cdot 10]/90 = 62444$ біт/с.

$V_{MGCP3} = [(10 \cdot 800 + 20 \cdot 100 + 70 \cdot 11 + 70 \cdot 7) \cdot 50 \cdot 10]/90 = 62556$ біт/с.

Таким чином загальний транспортний ресурс шлюзу визначений, як сума всіх складових:

$$V_{GW} = V_{GW_{LSRR}} + V_{PSTN} + V_{ISDN} + V_{V5} + V_{PBX} + V_{MGCP} \qquad (4.16)$$

$$V_{GW1} = 11773000 + 55556 + 5556 + 10889 + 1556 + 73556 = 11920 \text{ Кбіт/с} = 11{,}920 \text{ Мбіт/с}$$

$$V_{GW2} = 10178000 + 27778 + 22222 + 10889 + 2722 + 62444 = 10304 \text{ Кбіт/с} = 10{,}304 \text{ Мбіт/с}$$

$$V_{GW3} = 9867000 + 44445 + 11111 + 4278 + 2722 + 62556 = 9992 \text{ Кбіт/с} = 9{,}992 \text{ Мбіт/с}$$

*Розрахунок обладнання транспортної пакетної мережі:*

Кількість комутаторів пакетної мережі та їх топологія визначаються з урахуванням наявної топології первинної мережі, передбачуваної продуктивності використовуваного обладнання, а також вимог до забезпечення надійності пакетної мережі.

Визначення необхідної продуктивності комутаторів пакетної мережі.

Введемо наступні позначення.

$L_{IP}$ – середня довжина пакету IP, який використовуємо при передачі інформації (як сигнальної так і даних)

$M_{GW}$ – частина потоку користувацьких даних, що замикається на рівні шлюзу доступу.

1 - $M_{GW}$ – частина потоку користувацьких даних, що потрапляє в пакетну мережу.

В пакетну мережу потрапляють частина користувацьких даних від шлюзів доступу та інформація сигналізації в напрямку гнучкого комутатора.

$$P_{SW} = \left[\sum_{i=1}^{L}\left(1 - M_{l_{GW}}\right) \cdot V_{l_{GM}} + V_{SX}\right] \cdot L_{IP}\left(\frac{\text{пак}}{\text{с}}\right) \qquad (4.17)$$

Де $P_{SW}$ – мінімальна продуктивність обладнання комутаторів пакетної мережі

l – номер шлюзу

Якщо на рівні шлюзів доступну здійснюється замикання користувацького навантаження, то такий шлюз повинен мати власний комутатор, продуктивність ($P_{GW}$) якого може бути оцінена по формулі:

$$P_{GW} = M_{GW} \cdot \frac{V_{GW}}{L_{IP}} \left(\frac{\text{пак}}{\text{с}}\right) \qquad (4.18)$$

Ємнісні параметри комутаторів пакетної мережі визначаються топологією мережі та типами інтерфейсів підключення шлюзів і гнучкого комутатора. Місця розміщення обладнання розподіленого абонентського комутатора обираються з урахуванням граничної довжини абонентської лінії, топології первинної мережі, технічних можливостей обладнання та наявності приміщень для його встановлення.

Логічну топологію мережі наведено в графічній частині магістерської кваліфікаційної роботи.

# 5 СПЕЦІАЛЬНА ЧАСТИНА

## 5.1. Особливості протоколу SIP

Session Initiation Protocol (SIP) розроблено для встановлення, керування та завершення сеансів зв’язку між пристроями незалежно від їхнього місця розташування та часу підключення. На відміну від протоколів HTTP і SMTP, які не були орієнтовані на ініціацію мультимедійних сеансів у реальному часі, SIP заповнив цю функціональну прогалину, запозичивши від HTTP текстову модель обміну повідомленнями, формат і кодування, а від SMTP — механізм адресації на основі URI [23-26].

SIP-функціонування реалізується в розподіленому середовищі, що включає такі основні елементи: User Agents**,** Proxy Servers**,** Redirect Servers**,** Registrar Servers та Back-to-Back User Agents (B2BUA)**.** Клієнтами SIP є програмні компоненти, що працюють на кінцевих пристроях (ПК, сервери, спеціалізоване обладнання) та забезпечують встановлення з’єднань і обмін інформацією.

User Agent (UA) може функціонувати у двох режимах:

- User Agent Client (UAC) — формує та надсилає SIP-запити до серверів і отримує відповіді;
- User Agent Server (UAS) — приймає запити, обробляє їх і формує відповідні відповіді.

SIP-повідомлення поділяються на два основні типи:

- запити, що ініціюються клієнтом і визначають необхідну операцію;
- відповіді, які надсилаються сервером та інформують про стан обробки запиту.

Табл. 5.1. Методи протоколу SIP

| **Метод** | **Опис** |
|---|---|
| Invite | використовується для ініціювання SIP-сесії та передавання параметрів сеансу |
| Register | забезпечує автентифікацію користувацького агента та інформує мережу про поточне місцезнаходження об’єкта |
| Bye | призначений для завершення вже встановленої SIP-сесії |
| Ack | підтверджує успішне отримання кінцевої відповіді на запит INVITE |
| Cancel | відхиляє раніше надісланий запит; для коректного завершення активної сесії використовується метод BYE |
| Options | застосовується для запиту можливостей та параметрів взаємодії кореспондентів. |
| **Методи розширення** | |
| Info | Забезпечує відповідну інформацію протягом встановленої сесії. Використовується рідко. |
| Message | Використовується для надсилання миттєвих повідомлень |
| Notify | Публікує результат подій. Використовується в поєднанні з запитами Subscribe. |
| PRack | Попереднє підтвердження відповіді (A Provisional Response ACKnowledgment). Підтверджує отримання попередньої відповіді. |
| Publish | Публікує інформацію про стан з’єднання. Використовується для служби миттєвих повідомлень. |
| Refer | Механізм передачі запиту на більш підходящий об’єкт. |
| Subscribe | Використовується для отримання запиту майбутніх Notify або Publish запитів. |
| Update | Змінює параметри сеансу в середині обміну. |

SIP-запити характеризуються набором методів, концептуально подібних до методів HTTP. Для реалізації основних функцій протоколу використовуються ключові слова (методи), які інтерпретуються користувацькими агентами та серверами. Стандарт RFC 3261 визначає шість базових SIP-методів, а також механізм розширення протоколу додатковими методами (зокрема INFO та іншими), що вводяться підлеглими стандартами.

SIP-відповіді завжди передаються у відповідь на відповідний запит і призначені для інформування ініціатора (UAC) про поточний стан обробки, підтвердження виконання операції, можливі перенаправлення або помилки. Відповіді поділяються на попередні та остаточні і ідентифікуються тризначними кодами стану.

У протоколі SIP визначено шість класів відповідей, які класифікуються за першою цифрою тризначного коду. П’ять із них успадковані з HTTP, тоді як шостий клас є специфічним для SIP і був введений спеціально для підтримки його функціональних особливостей..

Табл. 5.2. Класи повідомлень «відповідей»

| **Клас** | **Опис** |
|---|---|
| 1xx Попередній | підтверджують отримання запиту та інформують про продовження його обробки; попередні відповіді на запит **INVITE** не є повідомленнями **ACK** |
| 2xx Успіх | свідчать про те, що запит отримано, коректно оброблено та успішно виконано |
| 3xx Перенаправлення | надають інформацію про нове розміщення запитуваного ресурсу або пропонують альтернативні сервіси |
| 4xx Помилка запиту | вказують на наявність помилки у запиті або неможливість його обробки на стороні сервера |
| 5xx Помилка серверу | означають, що сервер не може обробити коректний запит через внутрішню помилку |
| 6xx Глобальна помилка | повідомляють про відсутність сервісу або неможливість обробки запиту будь-яким сервером |

Поле Warning у SIP-заголовку використовується для передавання додаткової інформації про стан відповіді та містить тризначний код у діапазоні 300–399, ім’я хоста та текст попередження.

Кожне SIP-повідомлення починається з Start-Line, за якою слідує набір заголовків; від тіла повідомлення вони відокремлюються порожнім рядком (CRLF).

Start-Line визначає тип повідомлення та версію протоколу і має два варіанти:

- Request-Line — використовується для запитів і містить метод, URI та версію протоколу (*SIP/2.0*);
- Status-Line — застосовується для відповідей, починається з версії протоколу, після чого наводиться числовий код стану та короткий текстовий опис.

Заголовки (Headers) передають додаткові атрибути повідомлення та мають формат, аналогічний HTTP: ім’я заголовка, двокрапка і значення. Заголовки можуть містити один або кілька параметрів, розділених комами, а також переноситися на кілька рядків із використанням CRLF і пробілів.

Між заголовками та тілом повідомлення розташовується роздільний рядок (Separator Line).

Тіло повідомлення (Body) містить корисне навантаження у текстовій або двійковій формі, найчастіше у вигляді опису сеансу за протоколом SDP.

Формування SIP-запитів і відповідей може бути реалізоване мовою **C#** з використанням SIP .NET SDK**.** Процес створення повідомлення запиту передбачає виконання таких основних етапів:

1. формування рядка запиту (Request-Line) з указанням типу повідомлення INVITE та URI «SIP: stepler@opengamer.com.ua»;
2. додавання заголовка Via, який визначає зворотний маршрут передавання відповіді;
3. задання адрес відправника і отримувача у вигляді SIP URI, що можуть містити IP-адреси або повні доменні імена (рекомендовано); за потреби допускається відображення імен та використання анонімного відправника з міркувань безпеки;
4. генерація унікальних ідентифікаторів сесії, зокрема Call-ID, який разом з адресами відправника і отримувача формує унікальний ключ виклику;
5. додавання альтернативної контактної інформації відправника;

6. визначення типу та параметрів контенту, що передається у тілі повідомлення.

Тестування програми, яка ініціює встановлення з’єднання та надсилає повідомлення ACK у відповідь на отриманий статус, наведено в додатках.

Створення SIP-відповіді включає такі дії:

1. формування рядка стану (Status-Line) із зазначенням результату обробки запиту та ідентифікацією відповідного запиту;
2. додавання контактної інформації;
3. визначення параметрів контенту повідомлення.

Приклад програмного коду, що реалізує формування відповіді на запит встановлення з’єднання, подано в додатках.

## 5.2. Програмне забезпечення

Konnetic Unity SIP .NET SDK — це бібліотека класів, реалізована мовою C#, яка працює на платформі Microsoft CLR або Mono та надає об’єктно-орієнтовану модель для розроблення SIP-додатків і сервісів відповідно до стандарту IETF RFC 3261. Бібліотека сумісна з .NET Framework 2.0 і новішими версіями.

Основні вимоги SIP значною мірою абстраговані, що дозволяє розробнику зосередитися на логіці прикладного рівня. Водночас SDK зберігає можливість низькорівневого налаштування та детального контролю потоків SIP-повідомлень за допомогою поведінкової моделі.

Бібліотека підтримує розширене багатопотокове керування з’єднаннями, що забезпечує ефективне використання багатоядерних і багатопроцесорних апаратних платформ та досягнення високої продуктивності. Реалізована підтримка транспортних протоколів TCP і UDP, а також механізмів аутентифікації та шифрування на основі TLS, що підвищує надійність і безпеку передавання даних.

Реалізація SIP у Konnetic Unity орієнтована переважно на клієнтські застосунки, однак може використовуватися і в серверних рішеннях, що робить її універсальною платформою для побудови різних типів SIP-додатків і сервісів:

- рішень класу **Media over IP**;
- інструментів для **спільної роботи** користувачів;
- модульних компонентів для розроблення широкого спектра застосунків — від мобільних до масштабованих корпоративних сервісів;
- комплексних рішень для керованих платформ **.NET**, що використовують функціональність рівнів викликів, повідомлень і транзакцій.

### 5.3. Особливості програмування SIP

Компоненти SIP-стеку реалізовані відповідно до специфікацій RFC 3261 та низки внутрішніх SIP-розширень. Стек підтримує базові методи SIP, зокрема INVITE (re-INVITE), ACK, BYE, CANCEL, OPTIONS, REGISTER, а також розширені методи INFO, UPDATE та MESSAGE.

Бібліотека SIP забезпечує можливість приймання та обробки нестандартних параметрів повідомлень, які не входять до базової специфікації, включаючи додаткові методи, коди відповідей, заголовки та параметри заголовків. Підтримується стандарт RFC 3263, що визначає механізми пошуку SIP-серверів із використанням записів DNS NAPTR, SRV, A та AAAA, а також методики тестування відповідно до рекомендацій ETSI.

Обробка вхідних SIP-повідомлень реалізується за допомогою ефективного механізму детермінованого скінченного автомата (Deterministic Finite Automaton), який забезпечує коректний аналіз і керування заголовками повідомлень. Для транспортування підтримуються протоколи UDP, TCP та

TLS, при цьому TLS забезпечує змішану модель автентифікації, включаючи режим client-only.

SIP-стек реалізує механізми перевірки автентичності запитів відповідно до стандарту SIP, підтримуючи автентифікацію клієнта, сервера та змішану модель, а також контроль цілісності повідомлень (Auth-Int). Бібліотека функціонує у багатопотоковому режимі та забезпечує потокобезпечну роботу як для однопотокових, так і для багатопотокових застосунків за рахунок механізмів синхронізації на рівні окремих об’єктів (діалогів, транзакцій) і транспортного рівня..

### 5.4. Конфігурування створюваних програм

У цьому розділі наведено опис основних параметрів конфігурації програмних застосунків.

**SIP-адреса** користувача за замовчуванням визначається елементом defaultUserSipAddress, який містить єдиний атрибут URI з SIP-адресою користувача. Це значення використовується бібліотекою SIP під час формування стандартних запитів і відповідей. За відсутності параметра фабричні методи автоматично підставляють анонімну адресу в поле From (наприклад, sip:anonymous@anonymous.invalid).

**Контактні адреси** користувача застосовуються для задання альтернативних шляхів зв’язку та підтримують виключно SIP URI. Конфігураційний розділ userContacts не містить атрибутів і формується як набір дочірніх елементів add з атрибутом uri. У разі відсутності цього розділу альтернативні контактні адреси не використовуються.

**Проксі-сервери** налаштовуються в розділі ProxyServers, який дозволяє клієнтському застосунку визначити вихідний проксі-сервер для передавання SIP-запитів. Поряд із цим підтримуються альтернативні механізми обслуговування проксі, зокрема через модуль SipCore. Проксі-сервери

використовуються під час формування маршрутів вихідних повідомлень, а адреса призначення визначається відповідно до стандартів RFC 3261 та RFC 3263.

**Паролі.** З міркувань безпеки зберігання паролів у конфігураційних файлах не рекомендується, навіть якщо вони є спільними. Модуль **SipCore** надає механізми для додавання, редагування та видалення проксі-серверів без збереження облікових даних у відкритому вигляді.

**Захищені проксі-сервери.** Для забезпечення захищеної передачі вихідного трафіку передбачено окрему конфігурацію проксі-серверів із підтримкою захищених SIP URI.

**User Agent.** Протокол SIP дозволяє клієнту вказувати тип програмного або апаратного агента в заголовку User-Agent. Відповідний конфігураційний елемент UserAgent містить атрибут *value* (UTF-8 рядок). За відсутності цього елемента заголовок не додається.

**Підтримувані методи.** Перелік SIP-методів, що підтримуються клієнтом, задається елементом supportedMethods з атрибутом *methods* (список методів, розділених комами). Якщо параметр не визначено, використовується мінімальний набір відповідно до RFC 3261: *INVITE, BYE, OPTIONS, REGISTER, CANCEL, ACK*.

**Підтримувані схеми.** Конфігураційний елемент supportedScheme визначає допустимі схеми адресації. За замовчуванням використовуються *sip* та *sips*.

**Підтримувані розширення.** За допомогою елемента supportedExtensions клієнт може вказувати підтримувані SIP-розширення через заголовок *Supported*. Якщо розділ відсутній, розширення не використовуються.

**Кодування вмісту.** Елемент defaultEncodings визначає підтримувані кодування тіла повідомлення (заголовок *Content-Encoding*) у вигляді списку

IANA-зареєстрованих значень. За замовчуванням кодування не застосовується.

**Типи вмісту.** Підтримувані медіа-типи задаються в розділі supportedMediaTypes за допомогою дочірніх елементів *add* з атрибутом *media*. За відсутності цього розділу типи вмісту не визначаються.

**Обов'язкові розширення.** Елемент requiredExtensions використовується для задання SIP-розширень, підтримка яких є обов'язковою для іншої сторони (заголовок *Require*). За замовчуванням такі розширення відсутні.

**Транспортний протокол за замовчуванням.** Елемент defaultTransportProtocol визначає транспорт для заголовка *Via* та SIP URI. Підтримуються значення UDP, TCP, TLS**;** за відсутності параметра використовується **UDP**.

**Обмеження на повідомлення.** На транспортному рівні встановлюються граничні значення внутрішніх параметрів SIP-повідомлень з метою запобігання некоректному або шкідливому трафіку та підвищення загального рівня безпеки. Відповідні обмеження наведені в табл. 5.3.

Табл. 5.3. Межі повідомлень протоколу SIP

| **Ліміт** | **Блок** | **Значення** | **Опис** |
|---|---|---|---|
| maximumContentSize | Ціле | 5242880 | Максимальне число байтів, що дозволяються використовувати в тілі повідомлення |
| maximumHeaderCount | Ціле | 256 | Максимальне число полів заголовку SIP у повідомленні. |
| maximumHeaderCount | Байт | 1024 | Максимальне число байтів, що дозволяються використовувати у імені заголовку |
| maximumHeaderValueSize | Байт | 65537 | Максимальне число байтів, що дозволяється використовувати в заголовку |
| maximumParameterCount | Ціле | 32 | Максимальне число байтів, що |

| | | | |
|---|---|---|---|
| | | | дозволяється використовувати в полях заголовків |
| maximumWhitespaceSize | Байт | 1024 | Максимальне число байтів, що дозволяються використовувати для пропусків в полях заголовку |

Розділ конфігурації MessageLimits визначає значення за замовчуванням. Ім'я елемента messageLimits. Існує один атрибут per limit. Атрибут ціле число.

*Таймери*

Транспортний рівень задіює таймери, щоб контролювати поведінку процесу відправки повідомлення. Ці таймери можуть бути налаштовані.

Основне завдання полягає в оптимізації бібліотеки, так щоб вона задовольняла умови, які відчуває середовище передачі.

Таймери і конфігураційні імена наведені в наступній таблиці:

Табл. 5.4. Таймери і конфігураційні імена

| **Таймер** | **Конфігураційне ім'я** | **Стандартне значення** | **Опис** |
|---|---|---|---|
| T1 | TimerT1 | 500 мс | Оцінка RTT |
| T2 | TimerT2 | 4 с | Максимальний інтервал повтору для НЕ-INVITE запитів і відповідей на запит |
| T3 | TimerT3 | 5 с | Максимальна тривалість часу поки повідомлення буде залишатися в мережі |
| Timer A | TimerA | T1 | INVITE інтервал угоди між перечею, тільки для UDP |
| Timer B | TimerB | $64 \cdot T1$ | Таймаут таймер INVITE транзакції |
| Timer C | TimerC | > 3 хв | Таймаут проксі INVITE транзакції |
| Timer D | TimerDUdp/ TimerDTcp | > 32 с для UDP | Очікування відповіді, 0с для пересилання TCP/SCTP |
| Timer E | TimerE | T1 | Generic INVITE інтервал повтору транзакції, тільки UDP |
| Timer F | TimerF | $64 \cdot T1$ | Generic INVITE транзакції таймер таймаута |

| | | | |
|---|---|---|---|
| Timer G | TimerG | T1 | інтервал повторної передачі відповіді INVITE |
| Timer H | TimerH | $64 \cdot T1$ | Час очікування 0c для отримання ACK |
| Timer I | TimerIUdp/ TimerITcp | T4 для UDP | Час очікування 0c для повторного надсилання TCP / ACK SCTP. |
| Timer J | TimerJUdp/ TimerJTcp | $64 \cdot T1$ для UDP | Час очікування 0s для повторної передачі TCP / SCTP HE-INVITE запиту |
| Timer K | TimerKUdp/ TimerKTcp | T4 для UDP | Час очікування 0s для пересилання TCP / SCTP відповіді |

Елемент timers не містить власних атрибутів і використовується як контейнер для дочірніх елементів. Налаштування таймерів здійснюється за допомогою елемента add з атрибутом key, який визначає назву таймера, та відповідним значенням, що задається у мілісекундах і використовується як значення за замовчуванням.

У разі відсутності цього розділу застосовуються стандартні значення таймерів, наведені в таблиці вище.

### 5.5. Алгоритм програми встановлення сесії зв’язку

Session Initiation Protocol (SIP) призначений для встановлення з’єднань між пристроями та організації обміну інформацією. Реалізація цієї функції ґрунтується на моделі запит–відповідь, яка передбачає ініціювання запиту та його прийняття або відхилення. Нижче наведено алгоритм роботи консольного застосунку, що здійснює ініціювання SIP-сесії, очікує відповідь та, за необхідності, підтверджує її отримання.

У середовищі C# створюється новий проєкт, до якого підключаються розширення бібліотеки Konnetic, після чого виконується налаштування параметрів програми шляхом редагування конфігураційного файлу. Далі до тіла програми додаються необхідні класи та ініціалізується ядро SIP-бібліотеки, що забезпечує базові механізми керування протоколом. На етапі

ініціалізації також задається ключ, необхідний для використання програмних розширень.

Програма формує SIP-запит INVITE, у якому зазначається адреса об’єкта, з яким встановлюється з’єднання. Запит реєструється для отримання відповідних повідомлень-відповідей і передається у мережу, після чого застосунок переходить у режим очікування відповіді. Отримання повідомлення типу Trying свідчить про процес встановлення з’єднання, тоді як повідомлення Ringing означає доставлення запиту адресату та очікування його відповіді. У разі надходження позитивної відповіді програма надсилає підтвердження, завершуючи процедуру встановлення з’єднання. Якщо ж відповідь відсутня, користувача інформують про неуспішну спробу ініціювання сеансу.

### 5.6. Алгоритм програми прийняття, або відхилення запиту сесії

На відміну від протоколів HTTP і SMTP, Session Initiation Protocol (SIP) забезпечує ініціювання сеансів обміну даними в мережі Інтернет. При цьому кінцевий пристрій має можливість прийняти або відхилити пропозицію встановлення з’єднання. Реалізація такого механізму ґрунтується на моделі пропозиції–відповіді, яка виходить за межі простого обміну запитами та відповідями. У межах цієї моделі використовуються повідомлення підтвердження (OK) або відхилення (Decline).

Розглянуто алгоритм роботи простого консольного застосунку, що здійснює прослуховування вхідних SIP-повідомлень, аналізує запити для ідентифікації відправника та, залежно від результату перевірки, приймає або відхиляє запрошення на встановлення сеансу.

Після створення нового проєкту в середовищі C# до нього підключається бібліотека Konnetic, формується та налаштовується файл конфігурації відповідно до функціональних вимог програмного забезпечення.

У програмі ініціалізується ядро SIP-середовища та визначається клас, відповідальний за взаємодію з SIP-елементами. Далі встановлюється ліцензійний ключ, конфігурується модуль прослуховування мережевих портів і транспортних протоколів для приймання вхідних повідомлень.

Отримані SIP-повідомлення реєструються та підлягають подальшому опрацюванню. Залежно від типу повідомлення виконується перевірка: якщо повідомлення не є запитом INVITE, формується відповідь Decline. У разі отримання запиту INVITE здійснюється порівняння адреси відправника з попередньо визначеними SIP-адресами. За умови їх збігу формується підтвердження OK, у протилежному випадку — повідомлення Decline.

Крім того, система формує візуальні повідомлення для інформування оператора та накопичує статистичні дані, які можуть бути використані для аналізу функціонування мережі, а також її подальшої оптимізації та розвитку.

# 6 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

## 6.1. Тривалість робочого часу на підприємстві, тривалість відпочинку

Нормальна тривалість робочого часу працівників не може перевищувати 40 годин на тиждень (ст. 40 КЗпП України). Підприємства і організації при укладенні колективного договору можуть встановлювати меншу норму тривалості робочого часу, ніж передбачено в частині першої цієї статті.

Скорочена тривалість робочого часу встановлюється: для працівника віком від 16 до 18 років - 36 годин на тиждень, для осіб віком від 15 до 16 років (учні віком від 14 до 15 років, які працюють в період канікул) - 24 години на тиждень.

Тривалість робочого часу учнів, які працюють протягом навчального року у вільний від навчання час, не може перевищувати половини максимальної тривалості робочого часу, не більше 20 годин.

Для працівників, зайнятих на роботах з шкідливими умовами праці, не більше як 36 голин на тиждень.

Крім того, законодавством встановлено скорочена тривалість робочого асу для окремих категорій працівників (учителів, лікарів та інших).

Скорочена тривалість робочого часу може встановлюватись за рахунок власних коштів на підприємствах і в організаціях для жінок, які мають дітей віком до 14 років або дитину-інваліда.

При роботі в нічний час встановлена тривалість роботи (зміни) скорочується на годину. Це правило не поширюється на працівників, для яких уже передбачено скорочення робочого часу.

Тривалість нічної роботи зрівнюється з денною в тих випадках, коли це необхідно за умовами виробництва, зокрема у безперервних виробництвах, а

також на змінних роботах при шестиденному робочому тижні з одним вихідним днем. Нічним вважається час з 10 години вечора до 6 години ранку.

Забороняється залучення до роботи в нічний час:

- вагітних жінок і жінок, що мають дітей віком до трьох років;
- осіб молодших 18 років;
- інших категорій працівників, передбачених законодавством.

При змінних роботах працівники чергуються в змінах рівномірно в порядку, встановленому правилами внутрішнього трудового розпорядку. Тривалість перерви в роботі між змінами має бути не меншою подвійної тривалості часу роботи в попередній зміні (включаючи і час перерви на обід). Призначення працівника на роботу протягом двох змін підряд забороняється (ст..59 КЗпП України). Надурочні роботи, як правило, не допускаються.

Власник або уповноважений ним орган може застосовувати надурочні роботи тільки у таких випадках:

- при проведенні робіт, необхідних для оборони країни, а також відвернення громадського або стихійного лиха, виробничої аварії і негайного усунення їх наслідків;
- при проведенні громадсько-необхідних робіт по водопостачанню, газопостачанню, опаленню, освітленню, каналізації, транспорту, зв'язку – для усунення випадкових або несподіваних обставин, які порушують правильне їх функціонування;
- при необхідності закінчити почату роботу, яка внаслідок непередбачених обставин чи випадкової затримки з технічних умов виробництва не могла бути закінчена в нормальний робочий час, коли припинення її може призвести до псування або загибелі державного чи громадського майна, а також необхідності невідкладного ремонту машин, верстаків або іншого устаткування, коли несправність їх викликає зупинення робіт для значної кількості трудящих;

- при необхідності виконання вантажно-розвантажувальних робіт з метою недопущення або усунення простою рухомого складу чи скупчення вантажів у пунктах відправлення і призначення;
- для продовження роботи при нез'явленні працівника, який заступає,коли робота не допускає перерви; в цих випадках власник зобов'язаний негайно вжити заходів до заміни іншим працівником.

Для відновлення фізичного, психофізіологічного стану людини, енергетичних витрат і т.п. працівником згідно законодавчих і інших нормативних актів передбачений час відпочинку.

Працівникам надається перерва для відпочинку і харчування тривалістю не більше 2 годин. Перерва не включається в робочий час. Перерва для відпочинку і харчування повинна надаватись, як правило, через 4 години після початку роботи.

Працівники використовують час перерви на свій розсуд. На цей час вони можуть відлучатися з місця роботи.

На тих роботах, де через умови виробництва перерву встановити не можна, власник за узгодженням з представником профспілки надає можливість прийняття їжі протягом робочого часу.

При шестиденному робочому тижні працівникам надається один вихідний день, а при п'ятиденному робочому тижні - два вихідних дні. Загальним вихідним днем є неділя.

Другий вихідний день при п'ятиденному робочому тижні, якщо він невизначений законодавством, визначається графіком роботи підприємства, установи, організації за погодженням з представником профспілки і , як правило, має надаватися підряд з загальним вихідним днем.

На підприємствах, в установах, організаціях, де робота не може бути перервана в загальний вихідний день у зв'язку з необхідністю

обслуговування населення, вихідні дні встановлюються місцевими Радами народних депутатів.

В інших обставинах, коли роботу перервати неможливо з виробничо-технічних умов або через необхідність безперервного обслуговування населення, а також на вантажно-розвантажувальних роботах, пов'язаних з роботою транспорту, вихідні дні надаються в різні дні тижня почергово кожній групі працівників згідно з графіком змінності, що затверджується власником(керівником) за погодженням з профспілковим працівником підприємства,установи, організації.

Тривалість щотижневого безперервного відпочинку повинна бути неменше як сорок дві години.

Робота у вихідні дні забороняється. Залучення окремих працівників до роботи у ці дні допускається тільки з дозволу виборчого органу первинної профспілкової організації підприємства, організації, установи і лише у виняткових випадках, що визначаються законодавством, а саме:

- для відвернення або ліквідації наслідків стихійного лиха, епідемій, епізоотій, виробничих аварій і негайного усунення їх наслідків;
- для відвернення нещасних випадків, які ставлять або можуть поставити під загрозу життя чи нормальні життєві умови людей, загибелі або псування майна;
- для виконання невідкладних, насамперед непередбачених робіт, від негайного виконання яких залежить у подальшому нормальна робота підприємства, установи, організації в цілому або їх окремих підрозділів;
- для виконання невідкладних вантажно-розвантажувальних робіт з метою запобігання або усунення простою рухомого складу чи скупчення вантажів у пунктах відправлення і призначення.

Залучення працівників до роботи у вихідні дні проводиться за письмовим наказом (розпорядженням) роботодавця (керівника).

Усім працівникам надаються щорічні відпустки із збереженням на їх період місця роботи (посади) і заробітної плати.

### 6.2. Заходи та засоби нормалізації параметрів мікроклімату

На мікроклімат у приміщенні впливають:

- Температура повітря.
- Вологість повітря.
- Потоки повітря.
- Шум від руху потоків повітря.
- Тепло-фізіологічні чинники, наприклад, температура навколишніх стін, вікон і підлоги.
- Якість повітря (частки пилу та речовин, що мають запах).
- Отруйні речовини з меблів, а також шкідливі випари з внутрішніх оздоблюваль-них будівельних матеріалів.

Для мережевого обладнання в першу чергу грають роль температура, вологість, та потоки повітря.

Мікроклімат технічних площадок забезпечується промисловими кондиціонерами (температура 16-18°С, відносна вологість повітря в межах 40-45% при діапазоні відхилень ± 1%). Кондиціонери оснащені системою очищення та фільтрації повітря (ступінь очищення складає не менше 95%).

Промислові кондиціонери мають додаткові функції, завдяки яким вони не лише охолоджують, але і зволожують або осушують (залежно від заданої програми), очищають повітря. Серед промислових кондиціонерів поширені такі типи: мультизональні, системи чиллер-фанкойл, дахові, центральні та ін.

Промислові кондиціонери допомагають з успіхом вирішити завдання ефективного кондиціонування та створення сприятливого мікроклімату завдяки великій мірі гнучкості при роботі в значній кількості приміщень,

дозволяючи збільшувати як потужність самого промислового кондиціонера, так і обсяг обслуговується простору, наближаючись по характеристикам прокачується до систем вентиляції. Одна з їх унікальних особливостей — можливість зміни витрати хладагента і, як наслідок, можливість індивідуального регулювання параметрів повітря.

Система охолодження обладнання побудована по системі “холодний-гарячий коридор” з можливістю направлення потоків повітря на обладнання, яке потребує більшого охолодження.

Дана система забезпечує ізоляцію холодних і гарячих проходів, що дозволяє збільшити ефективність системи охолодження і зменшити витрату електроенергії на охолодження.

Конструкція такої системи, модульна, модернізована, розширювана, та піддається масштабуванню.

Переваги виконання даної системи охолодження:

- Більша ефективність, ніж при традиційній центральній системі кондиціонування - до 50% економії електроенергії;
- Конструкція модульна, та піддається масштабуванню;
- Здатність охолодження до 10 кВт на стійку;
- Green IT;
- Повне системне рішення: моніторинг, охолодження, безпека;
- Ефективне управління живленням.

### 6.3. Вимоги до режимів праці і відпочинку при роботі з ВДТ

При організації праці, пов'язаної з використанням ВДТ ЕОМ і ПЕОМ, для збереження здоров'я працюючих, запобігання професійним захворюванням і підтримки працездатності передбачаються внутрішньо змінні регламентовані перерви для відпочинку.

Внутрішньо змінні режими праці і відпочинку містять додаткові нетривалі перерви в періоди, що передують появі об'єктивних і суб'єктивних ознак стомлення і зниження працездатності.

При виконанні робіт, що належать до різних видів трудової діяльності, за основну роботу з ВДТ слід вважати таку, що займає не менше 50% робочого часу. Впродовж робочої зміни мають передбачатися:

- перерви для відпочинку і вживання їжі (обідні перерви);
- перерви для відпочинку і особистих потреб (згідно з трудовими нормами);
- додаткові перерви, що вводяться для окремих професій з урахуванням особливостей трудової діяльності.

За характером трудової діяльності розрізняють три професійні групи, згідно з діючим класифікатором професій (ДК-003-95 і Зміна N1 до ДК-003-95):

1) розробники програм (інженери-програмісти) виконують роботу переважно з відео терміналом та документацією при необхідності інтенсивного обміну інформацією з ЕОМ і високою частотою прийняття рішень. Робота характеризується інтенсивною розумовою творчою працею з підвищеним напруженням зору, концентрацією уваги на фоні нервово-емоційного напруження, вимушеною робочою позою, загальною гіподинамією, періодичним навантаженням на кисті верхніх кінцівок. Робота виконується в режимі діалогу з ЕОМ у вільному темпі з періодичним пошуком помилок в умовах дефіциту часу;

2) оператори електронно-обчислювальних машин виконують роботу, пов'язану з обліком інформації, одержаної з ВДТ за попереднім запитом, або тієї, що надходить з нього, супроводжується перервами різної тривалості, пов'язана з виконанням іншої роботи і характеризується напруженням зору,

невеликими фізичними зусиллями, нервовим напруженням середнього ступеня та виконується у вільному темпі;

3) оператор комп'ютерного набору виконує одноманітні за характером роботи з документацією та клавіатурою і нечастими нетривалими переключеннями погляду на екран дисплея, з введенням даних з високою швидкістю. Робота характеризується як фізична праця з підвищеним навантаженням на кисті верхніх кінцівок на фоні загальної гіподинамії з напруженням зору (фіксація зору переважно на документи), нервово-емоційним напруженням.

Правилами встановлюються такі внутрішньо змінні режими праці та відпочинку при роботі з ЕОМ при 8-годинній денній робочій зміні в залежності від характеру праці:

- для розробників програм із застосуванням ЕОМ слід призначати регламентовану перерву для відпочинку тривалістю 15 хвилин через кожну годину роботи за ВДТ;
- для операторів із застосуванням ЕОМ слід призначати регламентовані перерви для відпочинку тривалістю 15 хвилин через кожні дві години;
- для операторів комп'ютерного набору слід призначати регламентовані перерви для відпочинку тривалістю 10 хвилин після кожної години роботи за ВДТ.

У всіх випадках, коли виробничі обставини не дозволяють застосувати регламентовані перерви, тривалість безперервної роботи з ВДТ не повинна перевищувати 4 години.

При 12-годинній робочій зміні регламентовані перерви повинні встановлюватися в перші 8 годин роботи аналогічно перервам при 8-годинній робочій зміні, а протягом останніх 4-х годин роботи, незалежно від характеру трудової діяльності, через кожну годину тривалістю 15 хвилин.

Для зниження нервово-емоційного напруження, втомлення зорового аналізатора, поліпшення мозкового кровообігу, подолання несприятливих наслідків гіподинамії, запобігання втомі доцільно деякі перерви використовувати для виконання комплексу вправ, які наведені у Державних санітарних правилах і нормах роботи з візуальними дисплейними терміналами електронно-обчислювальних машин ДСанПІН 3.3.2.007-98.

При проведенні сеансів психофізіологічного розвантаження рекомендується використовувати деякі елементи методу аутогенного тренування, який ґрунтується на свідомому застосуванні комплексу взаємопов'язаних прийомів психічної саморегуляції й виконанні нескладних фізичних вправ із словесним самонавіюванням. Головна увага при цьому приділяється набуванню й закріпленню навичок м'язового розслаблення (релаксації).

У рекомендованому сеансі, який має проводитися в кімнаті психофізіологічного розвантаження з відповідним інтер'єром та кольоровим оформленням, виділяються три періоди, що відповідають фазам відновлювального процесу.

# ВИСНОВКИ

В роботі було виконано комплексне дослідження, проєктування та обґрунтування автоматизованого мережевого комплексу на основі технологій мереж наступного покоління (NGN), орієнтованого на використання в системах управління та сучасних телекомунікаційних інфраструктурах. Отримані результати підтверджують актуальність обраної тематики та доцільність впровадження NGN як базової платформи для розвитку мультисервісних, масштабованих і надійних мереж.

Доведено, що традиційні телекомунікаційні мережі з комутацією каналів не здатні ефективно задовольняти сучасні вимоги до передавання мультимедійного трафіку, інтеграції сервісів, мобільності та якості обслуговування. Аналіз міжнародних стандартів ITU-T, ETSI та рекомендацій серії Y.2000 дозволив систематизувати принципи побудови NGN.

Здійснено детальну класифікацію обладнання NGN за функціональними рівнями архітектури, проаналізовано роль гнучких комутаторів (softswitch), шлюзового обладнання, серверів додатків та систем експлуатаційної підтримки. Обґрунтовано, що softswitch є центральним елементом NGN Release 1, який забезпечує управління викликами, маршрутизацію, автентифікацію, тарифікацію та взаємодію з медіа- і сигнальними шлюзами. Проаналізовано основні реалізації softswitch від провідних виробників та сформовано узагальнену модель реалізації, адаптовану до потреб автоматизованих систем, із модульною архітектурою та високим рівнем відмовостійкості.

Детально розглянуто шлюзове обладнання NGN, зокрема медіа-, сигнальні, транкінгові та шлюзи доступу, а також підтримувані ними протоколи та інтерфейси. Окрему увагу приділено прикордонному контролеру сесій (SBC), який розглянуто як ключовий елемент безпеки, контролю якості та узгодження протоколів на межі мереж.

Виконано проєктування мережевої конфігурації для заданої зони автоматизації. Здійснено розрахунок навантажень, ємнісних параметрів шлюзів доступу, гнучкого комутатора та транспортної пакетної мережі. На основі заданих інтенсивностей викликів і характеристик трафіку обґрунтовано вибір кодека G.726 як компромісу між якістю мовлення, затримкою та вимогами до транспортного ресурсу. Визначено необхідну пропускну здатність для передавання як користувацького, так і сигнального трафіку, з урахуванням коефіцієнтів використання ресурсу та особливостей протоколів SIP, MGCP, MEGACO та SIGTRAN. Отримані розрахунки підтверджують можливість забезпечення заданих параметрів якості обслуговування в запропонованій NGN-архітектурі.

Детально досліджено Session Initiation Protocol (SIP) як основний механізм встановлення, керування та завершення мультимедійних сесій у NGN. Систематизовано методи SIP, класи відповідей, структуру повідомлень і механізми розширення протоколу. Практичну цінність роботи підтверджує розгляд програмної реалізації SIP-застосунків мовою C# з використанням Konnetic Unity SIP .NET SDK.

Загалом у магістерській роботі досягнуто поставленої мети — побудовано та досліджено автоматизований мережевий комплекс на основі технологій NGN, який може бути використаний у системах управління та телекомунікаційних інфраструктурах різного масштабу. Наукова новизна роботи полягає у комплексному поєднанні архітектурних принципів NGN, методів розрахунку мережевих ресурсів і практичної реалізації сигнальних протоколів у програмному середовищі. Практичне значення результатів полягає в можливості їх застосування під час проєктування, модернізації та оптимізації мереж операторського або корпоративного рівня.

# ПЕРЕЛІК ПОСИЛАНЬ

1. ETSI. (2019). Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; IP multimedia call control protocol based on SIP and SDP (3GPP TS 24.229 version 13.17.0 Release 13). European Telecommunications Standards Institute.

2. Микитишин А.Г., Митник М.М., Стухляк П.Д. Телекомунікаційні системи та мережі : навчальний посібник для студентів спеціальності 151 «Автоматизація та комп’ютерно-інтегровані технології» – Тернопіль: ТНТУ, 2017 – 384 с.

3. Баранов, Г. Л., & Шпак, О. В. (2020). Інформаційні та телекомунікаційні системи. Львів: Видавництво Львівської політехніки.

4. Конахович, Г. Ф., Корнієнко, О. В., & Гнатюк, С. О. (2016). Телекомунікаційні мережі та системи. Київ: Видавництво КПІ ім. Ігоря Сікорського.

5. International Telecommunication Union. (2016). Signaling requirements and protocol aspects for VoIP security in NGN (Recommendation ITU-T Q.3711). ITU-T.

6. Микитишин А.Г. Програмно-апаратні пристрої у мережах наступного покоління / А.Г. Микитишин, М.М. Митник // Матеріали Міжнародної науково-технічної конференції. Фундаментальні та прикладні проблеми сучасних технологій – Тернопіль 19-21 травня 2015.– Т. : ТНТУ, 2022. — С. 57–58.

7. Рибальченко, М. В., & Кучерявий, Є. А. (2018). Мережі наступного покоління. Одеса: ОНАЗ ім. О. С. Попова.

8. Stanko, A., Wieczorek, W., Mykytyshyn, A., Holotenko, O., & Lechachenko, T. (2024). Realtime air quality management: Integrating IoT and Fog computing for effective urban monitoring. CITI, 2024, 2nd.

9. Rosenberg, J., et al. (2019). Push Notifications in the Session Initiation Protocol (SIP) (RFC 8599). IETF.

10. Campi M.C., Garatti S. Introduction to the Scenario Approach. – Society for Indus-trial and Applied Mathematics, 2018, 114 p.

11. National Institute of Standards and Technology. (2023). Guide to Operational Technology (OT) Security (NIST Special Publication 800-82, Rev. 3). NIST.

12. Cybersecurity and Infrastructure Security Agency. (2023). Zero Trust Maturity Model (Version 2.0). CISA.

13. Tong W., Zhu P. 6G: The Next Horizon: From Connected People and Things to Con-nected Intelligence. – Cambridge University Press, 2021, 490 p.

14. Tanenbaum, A. S., & Wetherall, D. J. (2021). Computer Networks (6th ed.). Pearson.

15. Maral G., Bousquet M., Sun Z. Satellite Communications Systems: Systems, Techniques and Technology. – Wiley, 2020,792 p.

16. Peterson, L. L., & Davie, B. S. (2021). Computer Networks: A Systems Approach (6th ed.). Morgan Kaufmann.

17. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп’ютерні мережі. Книга 1. - Львів, "Магнолія 2006", 2013. – 256 с.

18. Comer, D. E. (2018). Internetworking with TCP/IP: Principles, Protocols, and Architecture (6th ed.). Pearson.

19. ITU-D. Analysis of case studies on successful practices in telecommunications for rural and remote areas. Report on Quetion 10-1/2. – Geneva, 2006, 62 p.

20. D. Zhou, Zh.Yan, Y. Fu, Zh.Ya. A survey on network data collection. Journal of Network and Computer Applications, Vol. 116, Aug. 2018, pp. 9-23. DOI: 10.1016/j.jnca.2018.05.004

21. Glabowski M., Kmiecik D., Stasiak M. Overflows in Multiservice Systems. IEICE Transactions on Communications. E102B (5), 2019, pp.958-969. DOI: 10.1587/transcom.2018EUI0002

22. Kurt, S., Yildiz, H. U., Yigit, M., Tavli, B., & Gungor, V. C. (2017). Packet Size Optimization in Wireless Sensor Networks for Smart Grid

Applications. IEEE Transactions on Industrial Electronics, 64(3), 2392–2401. DOI:10.1109/tie.2016.2619319

23. Johnston, A. B. (2020). A SIP (Session Initiation Protocol) Back-to-Back User Agent (B2BUA) (RFC 8898). IETF.

24. Revsine L., Collins D.W., Johnson B., Mittelstaedt F., Soffer L. Financial Reporting and Analysis. – McGraw-Hill Education, 2014, 1152 p.

25. urose, J. F., & Ross, K. W. (2021). Computer Networking: A Top-Down Approach (8th ed.). Pearson.

26. ITU-T. Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuitswitched and packet-switched networks. Recommendation Y.1271, Geneva, 2004, 20 p.

27. Stallings, W. (2022). Data and Computer Communications (11th ed.). Pearson.

28. Микитишин А.Г. Комплексна безпека інформаційних мережевих систем: навчальний посібник для студентів спеціальності 174 «Автоматизація, комп’ютерно-інтегровані технології та робототехніка» / Укладачі: А.Г. Микитишин, М.М. Митник, О.С. Голотенко, В.В. Карташов. – Тернопіль : ФОП Паляниця В.А., 2023. – 324 с.

29. А. Станько, А. Микитишин, О. Голотенко, "Комунікаційні технології в енергосистемах," XI Міжнародна науково-практична конференція молодих учених та студентів "Актуальні задачі сучасних технологій", Тернопіль, 2022.

30. Шимчук Г. Основні проблеми та загрози хмарної безпеки / Г. Шимчук, О. Голотенко, Роман Захарійович Золотий // Матеріали X науково-технічної конференції „Інформаційні моделі, системи та технології“, 7–8 грудня 2022 року. – Т. : ТНТУ, 2022. — С. 59–60.

31. Пилипець М. І. Правила заповнення основних форм технологічних документів : навч.-метод. посіб. / Уклад. Пилипець М. І., Ткаченко І. Г., Левкович М. Г., Васильків В. В., Радик Д. Л. Тернопіль : ТДТУ, 2009. 108 с.

# ДОДАТКИ

## Додаток А

### А.1. Конфігурація файлу програми ініціації зв'язку:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
    <startup>
        <supportedRuntime version="v4.0"
sku=".NETFramework,Version=v4.5" />
    </startup>

  <configSections>
    <sectionGroup name="konneticSettings"
    type="Konnetic.KonneticConfigurationSectionGroup,
Konnetic.Signalling,
Culture=neutral, PublicKeyToken=255449bd8f8c3771" >
      <section name="sip"

type="Konnetic.Signalling.Sip.Advanced.Configuration.SipConfigurationS
ection,
Konnetic.Signalling, Culture=neutral, PublicKeyToken=255449bd8f8c3771"
      requirePermission="false"/>
    </sectionGroup>
  </configSections>
  <konneticSettings>
    <sip>
      <!--SIP URI клієнта за замовчуванням-->
      <defaultUserSipAddress uri="sip:user@opengamer.com.ua" />

      <userContacts>
        <add uri="example1@opengamer.com" />
        <add uri="example2@example2.com" />
        <add uri="example3@example3.com" />
      </userContacts>

      <supportedMethods
methods="INVITE,BYE,OPTIONS,CANCEL,ACK,MESSAGE"/>

    </sip>
  </konneticSettings>

</configuration>
```

### А.2. Текст програми ініціації зв’язку:

```
using System;
using System.Collections.Generic;
```

```
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using Konnetic.Signalling.Sip;


namespace ConsoleApplication1
{
    class InitiateASession
    {
        //Оголошення бібліотеки SIP для використання класу SIPCore
        static SipCore core;

        public static void Start()
        {   //Встановлення ліцензійного ключа і ініціалізація SipCore.
            Konnetic.Signalling.Sip.LicenseContainer.Key = "82D4-3D79-
4A58-FD9F-B6C8-2A1E-C4AC-7CC0-954B-9EF4-356A-8FB8-5EC7-5B24-BD29-473C-
ED39-74AD-51BD-A58D-D2BF-BC72-3517-9D1F";
            core = new SipCore();

          //Створення повідомлення запиту. Використовується
          узагальнений метод для виклику    //об’єкта.
          //Цей метод багато в чому залежить від конфігурації і
          забезпечує встановлення //значень для повідеомлень за
          замовчуванням.

            InviteRequest invite =
InviteRequest.CreateInviteRequest(new SipUri
            ("sip:stepler@opengamer.com.ua"));

            //Створення SDP повідомлення.
            SdpMessage sdp = new SdpMessage();
            sdp.Origin = "UserA 2890844526 2890844526 IN IP4
here.com";
            sdp.SessionName = "Session SDP";
            sdp.Connection = "IN IP4 100.101.102.103";
            TimeDescriptionHeaderField td = new
TimeDescriptionHeaderField();
            td.Timings = "0 0";
            sdp.TimeDescriptions.Add(td);
            MediaDescriptionHeaderField md = new
MediaDescriptionHeaderField();
            md.MediaHeaderField = "audio 49172 RTP/AVP 0";
            md.Attributes.Add(new AttributeHeaderField("rtpmap", "0
PCMU/8000"));
            sdp.MediaDescriptions.Add(md);
            //Прив’язка SDP повідомлення до INVITE повідомлення.
            invite.Body = sdp.GetBytes();
```

```
            //Отримувати повідомлення про відповіді
            invite.ResponseReceived += new
EventHandler<ResponseReceivedEventArgs>
            (OnInviteResponseReceived);

            //Надіслати повідомлення
            core.SendRequest(invite);
            //Перевірка, що основний потік не припинився
            Console.WriteLine("Натисність будь-яку клавішу щоб
завершити.");
            Console.ReadLine();
        }

        static void WorkingWithHeaders(){
        //Використовується конструктор для встановлення значеннння URI
в поле заголовка «To»
        ToHeaderField to = new
ToHeaderField("sip:stepler@opengamer.com.ua");
        //Використовуються властивості для встановлення і отримання
параметрів полів заголовка
        to.DisplayName = "Stepler diploma maker";
        Console.WriteLine(string.Format("{0} is
at{1}",to.DisplayName,to.Uri.ToString()));
        //Використовується перетворення рядкового типу для
встановлення та отримання параметрів
      //поля заголовка
        to = "stepler <sip:stepler@lviv>";
        Console.WriteLine((string)to);
        }

        //отримання відповіді на INVITE запит
        private static void OnInviteResponseReceived(object sender,
        ResponseReceivedEventArgs e) {
        if(e.Response.StatusClass == SipStatusClass.Successful) {
        if(e.Response.StatusCode == SipStatusCode.Trying){
        //Інша сторона надсилає повідомлення про те що запит був
успішно доставлений, і що овна
      //готується до встаовлення до встановлення зв’язку.
        Console.WriteLine("===Очікування===");
        }
          if(e.Response.StatusCode == SipStatusCode.Ringing) {
        //Інша сторона надсилає повідомлення, про те що вона отримала
запит, і працює над
      //відповіддю.
        Console.WriteLine("===Встановлення з’єднання ===");
        }
        if(e.Response.StatusCode == SipStatusCode.Ok){
        //отримано повідмлення OK.
        //Надіслати відповідь Ack
```

```
        InviteClientTransaction transaction = e.Response.Transaction
as
        InviteClientTransaction;
        if(transaction!=null){
        AckRequest ack = AckRequest.CreateAck((InviteRequest)
        transaction.OriginalRequest, e.Response.To.Tag);
        core.SendRequestDirect(ack);
        Console.WriteLine("===Надіслати ACK===");
        }
        Console.WriteLine("===INVITE повідомлення успішне===");
        }
        }
        else{
        //Не вдалося встановити зв'язок.
        Console.WriteLine("===Встановлення зв’язку невдале===");
        Console.WriteLine("Reason: " +
e.Response.StatusLine.ReasonPhrase);
        }
        }
        static void Main(string[] args)
        {
        }
    }
}
```

## Додаток Б

### Б.1 Конфігурація файлу програми підтвердження, або відхилення встановлення зв'язку:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
    <startup>
        <supportedRuntime version="v4.0"
sku=".NETFramework,Version=v4.5" />
    </startup>

  <configSections>
    <sectionGroup name="konneticSettings"
    type="Konnetic.KonneticConfigurationSectionGroup,
Konnetic.Signalling,
Culture=neutral, PublicKeyToken=255449bd8f8c3771" >
      <section name="sip"

type="Konnetic.Signalling.Sip.Advanced.Configuration.SipConfigurationS
ection,
Konnetic.Signalling, Culture=neutral, PublicKeyToken=255449bd8f8c3771"
      requirePermission="false"/>
    </sectionGroup>
  </configSections>
  <konneticSettings>
    <sip>
      <!--The default SIP URI for the client-->
      <defaultUserSipAddress uri="sip:user@opengamer.com.ua" />
    </sip>
  </konneticSettings>

</configuration>
```

### Б.2. Текст програми підтвердження, або відхилення встановлення зв’язку:

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using Konnetic.Signalling.Sip;
using Konnetic.Net.Transport;

namespace ConsoleApplication2
{
```

```
    class AcceptOrDeclineInvite
    {
        //Оголошення бібліотеки SIP для використання класу SIPCore
        static SipCore core;

        public static void Start()
        {   //Встановлення ліцензійного ключа і ініціалізація SipCore.
            Konnetic.Signalling.Sip.LicenseContainer.Key = "82D4-3D79-
4A58-FD9F-B6C8-2A1E-C4AC-7CC0-954B-9EF4-356A-8FB8-5EC7-5B24-BD29-473C-
ED39-74AD-51BD-A58D-D2BF-BC72-3517-9D1F";
            core = new SipCore();

          //Прослуховування TSP повідомлень на порті 5060.
            core.StartListening( 5060, TransportProtocol.Tcp);

          //Формуєтсья повідомлення про надходження нових даних, та
          здійснюється запис    //відправника повідомлення, кількість
          полів у заголовку, і довжину контенту в //байтах
            core.TransportLayer.DataReceived += delegate(object
sender,
            DataReceivedEventArgs e) {
            Console.WriteLine("Від: " + e.Sender.HostPort);
            Console.WriteLine("Кількість полів заголовку: " +
e.Data.HeaderFields.Count);
            Console.WriteLine("Довжина контену: " +
e.Data.ContentLength);
            };


            // Реєстрація події на отримання повідомлень запиту
            core.RequestReceived +=
            new
EventHandler<RequestReceivedEventArgs>(OnRequestReceived);
            //Перевірка, що основний потік не припинився
            Console.WriteLine("Натисніть будь-яку кнопку для
завершення.");
            Console.ReadLine();
        }

        //Обробка нових повідомлень запитів
        static void OnRequestReceived(object sender,
RequestReceivedEventArgs e)
        {
            SipRequest request = e.Request;
            if (request.Method == SipMethod.Invite)
            {
                Console.WriteLine("Отримано запит");
```

```
                //прийняти повідомлення від stepler, та відхилити
решту повідомлень.
                if (request.From.Uri.UserName == "stepler")
                {
                    request.SendResponse(SipStatusCode.Ok);
                }
                else
                {
                    request.SendResponse(SipStatusCode.Decline);
                }
            }
            else
            {
                Console.WriteLine(string.Format("{0} Отримано
повідомлення запрошення", request.Method));
            }
        }

        static void Main(string[] args)
        {
        }
    }
}
```