Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
дипломної роботи

бакалавра
(назва освітнього рівня)

галузь знань *17 Електроніка та телекомунікації*
(шифр і назва галузі знань)

спеціальність *172 Телекомунікації та радіотехніка*
(код і назва спеціальності)

освітній рівень *бакалавр*
(назва освітнього рівня)

кваліфікація *бакалавр із телекомунікацій та радіотехніки*
(код і назва кваліфікації)

На тему: «Розробка алгоритму обробки сигнальних повідомлень ОКС № 7 в мережах NGN на базі технології SIGTRAN»

Виконавець: студент *3* **курсу, групи** *172-17зск-2*

(підпис) **Вигонюк** Вадим Ігорович
(прізвище ім'я по-батькові)

Керівники	Прізвище, ініціали	Оцінка	Підпис
проекту	Проф. Гусєв О.Ю.		
розділів:			
спеціальний	Проф. Гусєв О.Ю.		
економічний	Доц. Романюк Н.М.		
Рецензент			
Нормоконтроль	Проф. Гусєв О.Ю.		

Дніпро
2020

Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
д.т.н., професор_____Корнієнко В.І.
«_____»_____20___року

ЗАВДАННЯ
на дипломну роботу бакалавра

спеціальність *172 Телекомунікації та радіотехніка*
(код і назва спеціальності)

студента 172-17зск-2 **Вигонюк** Вадим Ігорович
(група) (прізвище ім'я по-батькові)

Тема дипломного проекту «Розробка алгоритму обробки сигнальних повідомлень ЗКС7 в мережах NGN на базі технології SIGTRAN»

Наказ ректора НТУ "ДП" від _____№_____

Розділ	Зміст	Термін виконання
Стан питання. Постановка задачі	Аналітичний обзор лиітературы по темеі проекту Постановка задачі	Квітень 2020
Спеціальна частина	Розробка алгоритму обробки сигнальних повідомлень ОКС № 7 в мережах NGN на базі технології SIGTRAN	Травень 2020
Економічний розділ	Розрахунок капітальных витрат	Травень 2020

Завдання видав _____ Гусєв О.Ю.
(підпис) (прізвище, ініціали)

Завдання прийняв до виконання _____ Вигонюк В.І.
(підпис) (прізвище, ініціали)

Дата видачі завдання: 15 березня 2020 р.

Строк подання дипломного проекту до ДЕК:

РЕФЕРАТ

Пояснювальна записка: с. , рис. , табл. , додатків , джерел .

Об'єкт розробки: мережі NGN.

Предмет розробки: алгоритми обробки сигнальних повідомлень ОКС № 7.

Мета дипломної роботи: розробка алгоритму обробки сигнальних повідомлень ОКС № 7 в мережах NGN на базі технології SIGTRAN.

В першому розділі виконаний аналітичний огляд літературних джерел по темі дипломної роботи. Здійснено постановку задачі роботи.

У другому розділі розроблено алгоритм обробки сигнальних повідомлень ОКС № 7 в мережах NGN на базі технології SIGTRAN. Виконано аналіз результатів.

У третьому розділі виконано розрахунок капітальних витрат на розробку моделі системи передачі даних.

МЕРЕЖІ NGN, МЕДІА-ШЛЮЗ, SOFTSWITCH, ТМЗК, ЗКС7, ПРОПУСКНА ЗДАТНІСТЬ, ТЕХНОЛОГІЯ SIGTRAN

РЕФЕРАТ

Пояснительная записка с. , рис. , табл. , приложений , источников .

Объект разработки: сети NGN.

Предмет разработки: алгоритмы обработки сигнальных сообщений ОКС № 7.

Цель дипломной работы: разработка алгоритма обработки сигнальных сообщений ОКС № 7 в сетях NGN на базе технологии SIGTRAN.

В первом разделе выполнен аналитический обзор литературных источников по теме дипломной работы. Осуществлена постановка задачи работы.

Во втором разделе разработан алгоритм обработки сигнальных сообщений ОКС № 7 в сетях NGN на базе технологии SIGTRAN. Выполнен анализ результатов.

В третьем разделе выполнен расчет капитальных затрат на разработку модели системы передачи данных.

СЕТИ NGN, МЕДИА-ШЛЮЗ, SOFTSWITCH, ТфОП, ОКС7, ПРОПУСКНАЯ СПОСОБНОСТЬ, ТЕХНОЛОГИЯ SIGTRAN

ABSTRACT

Explanatory note p. , fig. , tab. , applications , sources .

Object of development: NGN networks.

Subject of development: signal processing algorithms for ACS No. 7.

The purpose of the thesis: development of an algorithm for processing signal messages ACS No. 7 in NGN networks based on SIGTRAN technology.

The first section contains an analytical review of literary sources on the topic of thesis. The statement of the problem of work is carried out.

In the second section, an algorithm for processing signal messages of ACS No. 7 in NGN networks based on SIGTRAN technology is developed. An analysis of the results.

In the third section, the calculation of capital costs for the development of a model of a data transmission system is performed.

NGN NETWORKS, MEDIA-GATEWAY, SOFTSWITCH, PSTN, SS No. 7, ACCESSIBILITY, SIGTRAN TECHNOLOGY

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ЗКС7 - Система сигналізації № 7. Набір сигнальних телефонних протоколів, використовуваних для налаштування більшості телефонних станцій (PSTN та PLMN) по всьому світу на основі мереж з канальним поділом за часом.

TDM-канали - Канали з часовим мультиплексуванням

Мережі NGN - Мережі наступного покоління

ІКМ - імпульсно-кодова модуляція

ІС - інтелектуальні мережі

ТМЗК - Телефонні мережі загального користування

API - Відкриті протоколи та інтерфейси прикладного програмування

SIP - Протокол прикладного рівня, за допомогою якого здійснюються такі операції, як встановлення, зміна та завершення мультимедійних сесій або викликів по IP-мережі

SCTP - Протокол, який відповідає за надійну передачу сигнальної інформації, що здійснює управління сигнальним трафіком, що забезпечує безпеку

SIGTRAN - Набір протоколів для передачі сигнальної інформації по IP-мережам

ЛОМ – Локальні обчислювальні мережі

ЗМІСТ

ВСТУП

На даний час модернізація телекомунікаційних мереж обумовлена головним чином зростанням трафіку, а також необхідністю розробки нових послуг і досягнень. Таким чином, світовий трафік Інтернет збільшується в світі в останні роки на 60-80% щорічно, а кількість абонентів широкосмугових мереж збільшується з середньою швидкістю 60%.

Головна мета ринкової політики найбільших телекомунікаційних операторів полягає в зменшенні капітальних і експлуатаційних витрат при збільшенні прибутковості послуг. Основними перешкодами на шляху до призначеної мети, як правило, стає устаріваюча мережева інфраструктура і концептуальна невизначеність в питаннях мережевого розвитку. Зараз перед розробниками стоїть завдання вибору такого рішення, яке повинно врахувати перспективи розвитку телефонної мережі і в технологічному, і в територіальному плані. Це дозволило б зберегти абонентську базу, при моральній зношеності обладнання, а також запропонувати на ринок нові послуги зв'язку і посилити свої конкурентні переваги. Економічна ефективність інвестицій повинна бути забезпечена за рахунок широкого використання послуг. Зазначені особливості [1] відрізняють мережі NGN від звичайних телефонних і IP-мереж, найбільш широко поширених в світі телекомунікацій. Найістотніша проблема мережі нового покоління міститься в постачанні взаємодії наявних і останніх телекомунікаційних мереж, підтримуваних цілісною інфраструктурою для трансляції різних типів інформації (голос, дані, відео).

Головна архітектурна особливість NGN полягає в тому, що передача та маршрутизація пакетів і базові елементи транспортної інфраструктури (канали, маршрутизатори, комутатори, шлюзи) фізично і логічно відокремлені від пристроїв і механізмів управління викликами та доступом до послуг [2]. Мережі наступного покоління (NGN) представляють собою нову концепцію мережі, що комбінує в собі голосові функції, якість обслуговування (QoS) і комутовані мережі з перевагами та ефективністю пакетної мережі. Мережі

NGN означають еволюцію існуючих телекомунікаційних мереж, що відображається в злитті мереж та технологій. Завдяки цьому забезпечуються широкий набір послуг, починаючи з класичних послуг телефонії та закінчуючи різними послугами передачі даних або їх комбінацією. При цьому вважається, що в результаті визначення точок розміщення обладнання шлюзів доступу і закріплення за шлюзами доступу зон обслуговування була отримана конфігурація, коли між будь-якими двома навантаженнями повідомлення буде передаватися через третій комутатор без збільшення втрат. Тобто транспортний ресурс та продуктивність комутаторів повинні розраховуватися виходячи із забезпечення резервування. Крім того, комутатори на рівні шлюзів не реалізуються і замикання навантаження між будь-якими двома об'єктами, підключеними до одного шлюзу, здійснюється через магістральний комутатор. Крім всіх переваг, які дає перехід на NGN мережі, пропоновані рішення забезпечують:

1. Низьку вартість передачі інформації з розрахунку на одиницю об'єму.
2. Високий рівень масштабованості.
3. Простоту монтажу, налаштування та подальшого обслуговування мережі.
4. Швидкість доступу по діючих телефонних лініях 100 і більше Мбіт/с.

Концепція NGN передбачає конвергенцію мереж IP-телефонії з ТМЗК, цифровою мережею з інтеграцією служб (ISDN), інтелектуальними мережами (IN), мережами мобільного зв'язку та мережею Інтернет. До основних типів сигналізації відносяться сигналізація для управління з'єднаннями (протоколи -SIP, SIP-T, ЗКС7, H.323), сигналізація для взаємодії різних програмних комутаторів Softswitch між собою (протоколи -SIP, SIP-T) та сигналізація для управління шлюзами (SG - шлюз сигналізації, MG - транспортний шлюз, AG - шлюз доступу, протоколи - Sigtran, MGCP, Megaco / H.248). Модифікований протокол SIP-T (SIP forTelephony) дозволяє інтегрувати протокол ЗКС7 з протоколом SIP. Вузол взаємодії SIP-мережі з мережею сигналізації ЗКС7 инкапсулює повідомлення ISUP в SIP-повідомлення і транслює частину

інформації з повідомлень ISUP в заголовки повідомлень SIP, щоб забезпечити їх транспортування в пакетній IP-мережі.

Мережа сигналізації ЗКС7, що працює по протоколам загальноканальної сигналізації, відноситься до спеціалізованої мережі с коммутацією пакетів, логічно відділена від інформаційних мереж і забезпечує транспортування повідомлень управління з'єднаннями в мережах, а також запитів виконання операцій у віддалених вузлах мережі. В мережі зв'язку сигнальні повідомлення передаються по загальному каналу сигналізації ЗКС7 (CCS №7, CommonChannelSignaling-сигналізація по загальному каналу). Система сигналізації SS No 7 (SignalingSystemNo7, система сигналізації по загальному каналу сигналізації) забезпечує взаємодію всіх мережевих функціональних компонент і визначає зміст та формат сигнальних повідомлень, необхідних для пересилання мережевої керуючої інформації. Сістема сигналізації SS-7 (міжнародна, міжміська, внутрішньозонова та місцева) дозволяє передавати сигнальну інформацію між системами комутації не для одного конкретного розмовного каналу, а для цілого пучка розмовних каналів по одному CCS-7. Система сигналізації є обов'язковим елементом телефонної мережі загального користування (ТМЗК), цифровий мережі з інтеграцією служб (ЦМІС), мережі зв'язку з рухомими системами (МЗРС), інтелектуальної мережі (ІМ) та інших цифрових мереж зв'язку. Взаємодія даних мереж здійснюється по ЗКС7 з використанням протоколів TUP, ISUP, MAP, INAP.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Архітектура мереж NGN та її переваги

1.1.1 Традиційні телефонні мережі

Мережі з комутацією каналів мають багату історію, вони походять від перших телефонних мереж. Мережі з комутацією пакетів порівняно молоді, вони з'явилися в кінці 60-х років як результат експериментів з першими глобальними комп'ютерними мережами. Кожна з цих схем має свої переваги і недоліки, але за довгостроковими прогнозами багатьох фахівців, майбутнє належить технології комутації пакетів, як більш гнучкій та універсальній.

При комутації каналів комутаційна мережа утворює між кінцевими вузлами безперервний складений фізичний канал з послідовно з'єднаних комутаторами проміжних канальних ділянок. Умовою того, що кілька фізичних каналів при послідовному з'єднанні утворюють єдиний фізичний канал, є рівність швидкостей передачі даних в кожному зі складових фізичних каналів. Рівність швидкостей означає, що комутатори такої мережі не повинні буферизувати передані дані.

У мережі з комутацією каналів перед передачею даних завжди необхідно виконати процедуру встановлення з'єднання, в процесі якої і створюється складений канал. І тільки після цього можна починати передавати дані.

Можна виділити наступні переваги комутації каналів:

- Постійна і відома швидкість передачі даних за встановленим між кінцевими вузлами каналу. Це дає користувачеві мережі можливості на основі заздалегідь виробленої оцінки, необхідної для якісної передачі даних пропускної здатності, встановити в мережі канал потрібної швидкості.

- Низький і постійний рівень затримки передачі даних через мережу. Це дозволяє якісно передавати дані, чутливі до затримок (звані також трафіком реального часу) - голос, відео, різну технологічну інформацію.

Поряд з достоїнствами, мережі з комутацією каналів мають ряд недоліків, які в умовах сучасного ринку поступово відсувають їх на задній план.

1.1.2 Недоліки TDM мереж і необхідність переходу до NGN

Впровадженню систем IP-сигналізації сприяє цілий ряд факторів. Це і архітектурні обмеження існуючих мереж ЗКС7, і необхідність операторів зв'язку знижувати експлуатаційні витрати, і конвергенція мереж передачі мови та даних, і прискорення процесу розгортання нових послуг зв'язку.

Властива IP-технологіям висока ефективність використання смуги пропускання дозволяє операторам зв'язку істотно економити кошти. Канали з тимчасовим мультиплексуванням (TDM) в традиційних телефонних мережах проектуються з урахуванням найбільш несприятливої ситуації - пікового навантаження. Протоколи ЗКС7 вимагають, щоб в штатній ситуації завантаженість TDM-каналів не перевищувала 40%. Це призводить до того, що на практиці їх середнє завантаження становить 20-30%. Значить, 70-80% канальних ресурсів постійно простоюють. Технології IP забезпечують динамічне виділення смуги пропускання на вимогу, при цьому її вартість виявляється найчастіше на 75% нижче вартості смуги пропускання TDM-мережі з комутацією каналів.

Обмеження, які накладаються технологією TDM на смугу пропускання, негативно впливають і на роботу інших елементів мережі: серверів додатків, регістрів положення, блоків контролю послуг. Навіть якщо потужності зазначених елементів цілком достатньо для обробки великих обсягів трафіку, обмеження протоколів ЗКС7 на TDM-канали, які з'єднують ці елементи з іншою мережею, не дають їм "розігнатися". Тому для підвищення продуктивності мережі операторам доводиться докуповувати додаткові пристрої, притому, що ресурси наявних ще далеко не вичерпані. Треба також

мати на увазі таку обставину: додавання кожного нового елементу вимагає організації каналу "точка-точка" та поновлення маршрутних таблиць, а значить, додаткових капітальних і експлуатаційних витрат. Вірне масштабування смуги пропускання в IP-мережах дозволяє справлятися з флуктуаціями трафіку, спростити архітектуру мережі, а різним базам даних працювати з максимально можливою продуктивністю.

На додаток до тієї економії, яка забезпечується за рахунок ефективного використання смуги пропускання та інших ресурсів, IP-технології дозволяють операторам більш економічно розвивати мережі. Вони можуть "віртуалізувати" велике число серверів, які будуть "виглядати" для мережі ЗКС7 як єдиний об'єкт, який працює під управлінням шлюзу сигналізації. У разі необхідності додати в мережу ще один сервер, досить буде всього лише підключити його до локальних обчислювальних мереж (ЛОМ) і, можливо, зробити відповідні зміни в налаштуваннях шлюзу сигналізації. Така схема розвитку означає відсутність будь-яких змін (або їх мінімізацію) в решті частини мережі, отже, знову-таки зниження витрат.

Як уже зазначалося, технології IP гарантують добре масштабування смуги пропускання, а це як можна краще підходить для служб, що генерують "вибуховий" трафік, обсяг якого може сильно змінюватися в часі. До таких служб відноситься SMS (Short Message Service), яка використовується сьогодні для самих різних додатків, таких, як електронна пошта та отримання інформації з Web-серверів. Оператори мобільних мереж відзначають значні сплески SMS-трафіку в святкові і вихідні дні. Підготувати мережу до подібних сплесків в рамках класичної архітектури ЗКС7 складно і дорого через статичне виділення смуги пропускання в TDM-мережах. Ефективним вирішенням проблеми є переведення SMS-трафіку з мереж ЗКС7 в мережі з сигналізацією на базі IP-сигналізації, що відкриває широкі можливості для оперативного впровадження нових послуг. Технології IP сильні своїм "інтелектуальним потенціалом": багато фахівців добре розбираються в цих

технологіях і здатні створювати програмне забезпечення для підтримки нових послуг. IP-мережі, засновані на розподіленій моделі, за своєю природою є відкритими системами, готовими до розгортання додатків, що розробляються третіми фірмами.

1.3 Загальні принципи побудови мереж NGN

Для мереж NGN можна виділити п'ять характерних особливостей:

- використання в транспортній мережі пакетних технологій для передачі всіх видів інформації;

- застосування систем комутації з розподіленою архітектурою, які відрізняються від традиційних (функціонально орієнтованих) телефонних станцій;

- відділення функцій, що стосуються підтримки послуг, від комутації та передачі;

- забезпечення можливості широкосмугового доступу для будь-якого користувача;

- реалізація функцій експлуатаційного управління (в тому числі делегованим користувачам) за рахунок Web-технології.

Примітно, що для обладнання розподілу інформації не зроблений такий же категоричний висновок про використання пакетних технологій, як для транспортної мережі. Деякі фахівці не виключають можливість появи якоїсь нової технології розподілу інформації. Можливо, що вона буде найбільше схожа на технологію «комутація каналів».

Стандартизацією NGN займаються кілька міжнародних організацій. Певний внесок вносять МСЕ і ETSI (Європейський інститут телекомунікаційних стандартів). Активно розробляє свої стандарти Міжнародний консорціум пакетного зв'язку - IPCC.

Нижче представлена архітектура NGN, запропонована МСЕ в рекомендації Y.1001 (рис. 1.1).

Медіа-шлюз виконує досить прості функції перетворення інформаційних потоків. Зліва від медіа-шлюзу показаний RTP-потік, який формується при використанні транспортного протоколу реального часу (Real-Time Transport Protocol), а праворуч - потік, утворений системою передачі з імпульсно-кодовою модуляцією (ІКМ). Медіа-шлюз виконує досить прості процедури, але у великій мережі він повинен володіти великою продуктивністю.

Медіа-шлюз керується відповідним контролером - MGC (Softswitch). Контролери можуть бути пов'язані між собою, що показано на рис.1 пунктирною лінією з надписом MGC/MGC. Контролер взаємодіє також з інтелектуальною базою даних (Intelligent Database ID).

Над контролером MGC показаний шлюз сигналізації (SG). В сторону ТМЗК (або сотової мережі) шлюз сигналізації передає і приймає інформацію по мережі загальних каналів сигналізації (ЗКС). У мережі ЗКС застосовується підсистема користувача ЦСІО - ISUP. Взаємодія з контролером MGC здійснюється через інтерфейс, позначений як SG/MGC. Для зв'язку з інтелектуальної базою даних визначено інтерфейс ID/SG. Для підтримки послуг ІС використовується прикладний протокол інтелектуальної мережі - INAP.

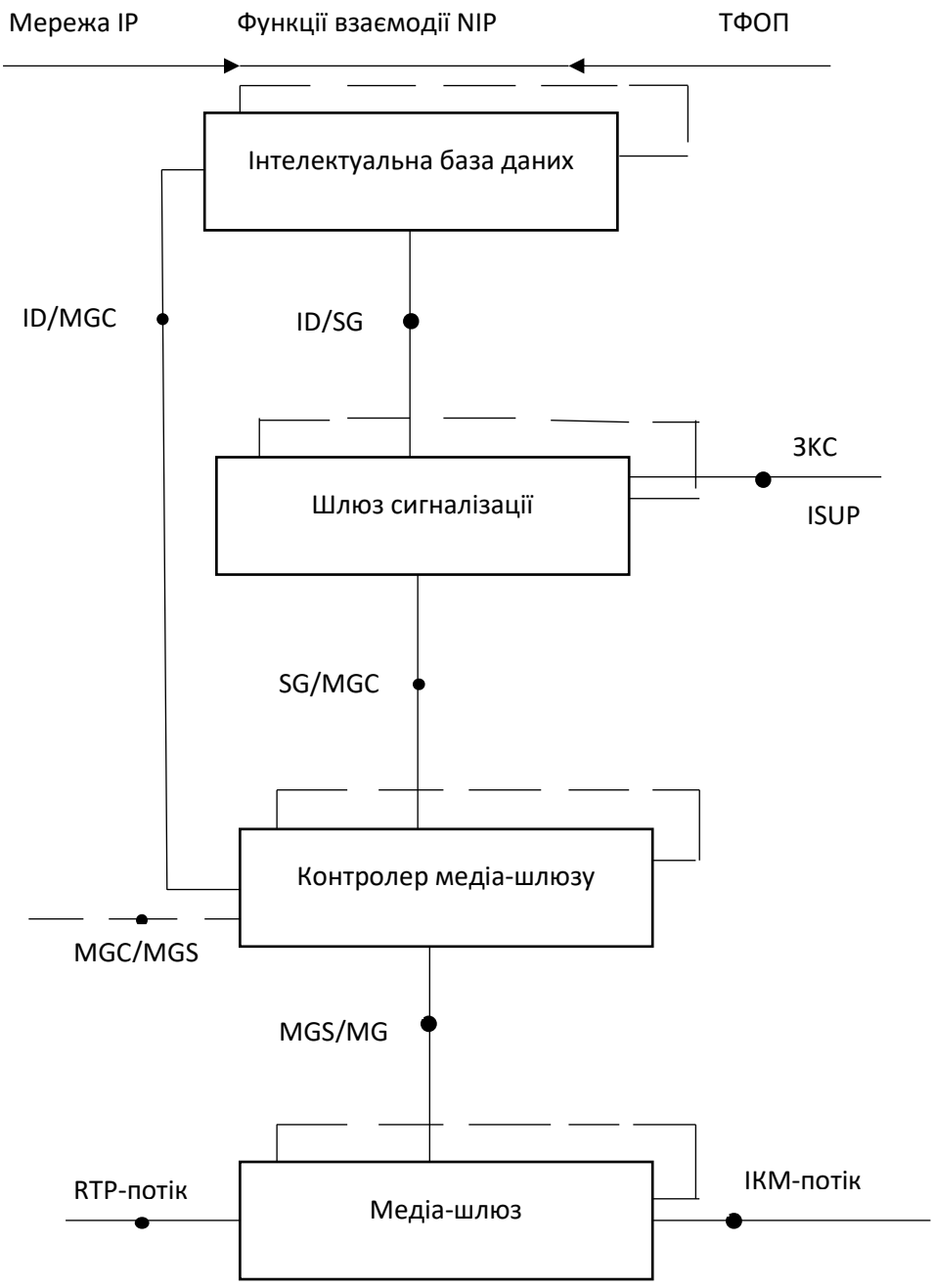


Рисунок 1.1 – Архітектура NGN

На рис. 1.2 приведена рівнева архітектура [4], запропонована компанією Lucent Technologies для пояснення концепції NGN. Ця архітектура відрізняється від аналогічних моделей, які використовуються в мережах телефонного зв'язку і обміну даними.

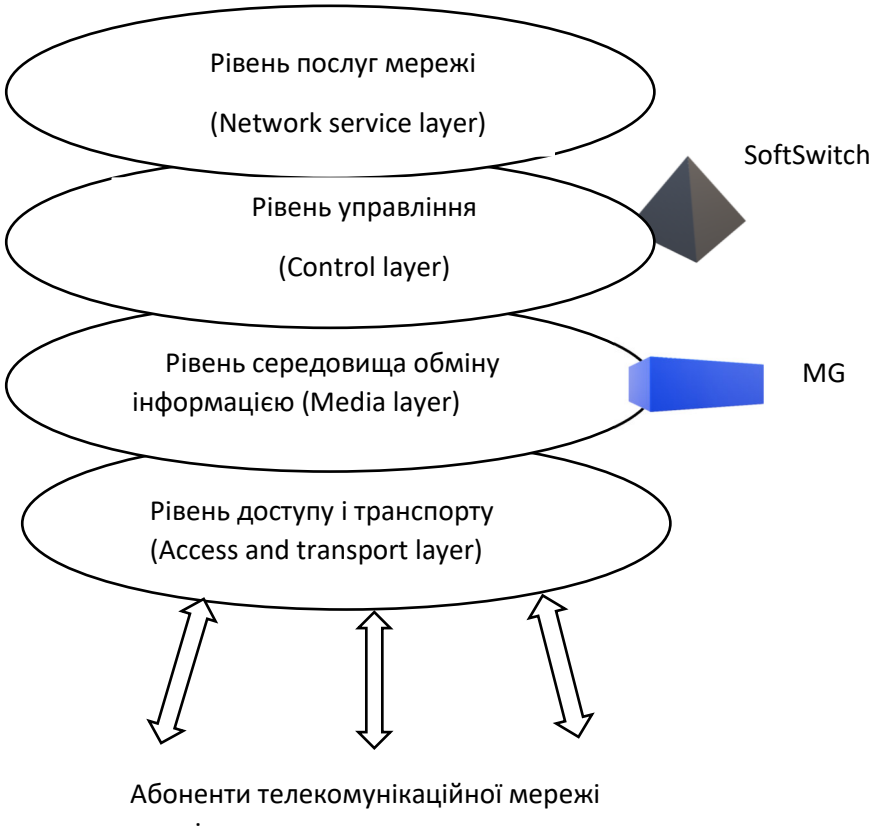


Рисунок 1.2 – Рівнева архітектура NGN

Рівень послуг виділяється в самостійний елемент архітектури мережі. Він займає верхню площину в даній моделі. В якійсь мірі, виділення самостійного рівня послуг подібно рішенню, яке запропоновано в концепції інтелектуальної мережі (IC).

Рівень управління розташовується на другій площині. У моделі NGN цей рівень включає сукупність функцій з управління всіма процесами в телекомунікаційній системі, а також нарахування плати за послуги зв'язку та технічну експлуатацію. Для реалізації функцій, які виконує цей рівень,

виробники телекомунікаційного обладнання розробили апаратно-програмні засоби, іменовані Softswitch [5].

Рівень середовища обміну інформацією знаходиться на третій площині. Функції, що виконуються цим рівнем, включають процедури встановлення з'єднань між користувачами мережі і міжмережеву взаємодію. Типовим прикладом обладнання, яке реалізує ці функції в мережі NGN, служать апаратно-програмні засоби Media Gateway (медіа-шлюзу).

Рівень доступу і транспорту розташовується на четвертій площині. Основні функції цього рівня - перенесення інформації між кінцевими користувачами мережі NGN. В якості засобів доступу в концепції мережі NGN розглядаються практично всі використовувані в даний час варіанти, засновані на різних технологіях.

Термін «Softswitch» можна перевести на російську мову як «комутатор з програмним управлінням», що не відображає його функціонального призначення, тому, щоб більш точно визначити цей термін, краще скористатися несуворим перекладом «Інтелектуальний комутатор».

У мережі NGN передбачається застосовувати тільки відкриті (стандартні) протоколи, які дозволяють при необхідності легко змінювати їх функції. Особливість комутаційних станцій ТМЗК полягає в тому, що вони, як правило, мають стандартні інтерфейси на вході і виході. Практично всі внутрішні процеси в комутаційної станції, як у «чорному ящику», підтримувалися фірмовими (нестандартними) протоколами, розробка яких здійснювалася виробником відповідних апаратно-програмних засобів.

Рис. 1.3 ілюструє відмінності в архітектурі комутаційних станцій ТМЗК і Softswitch (NGN). Відкриті протоколи та інтерфейси прикладного програмування (API) - невід'ємна особливість архітектури Softswitch (NGN).

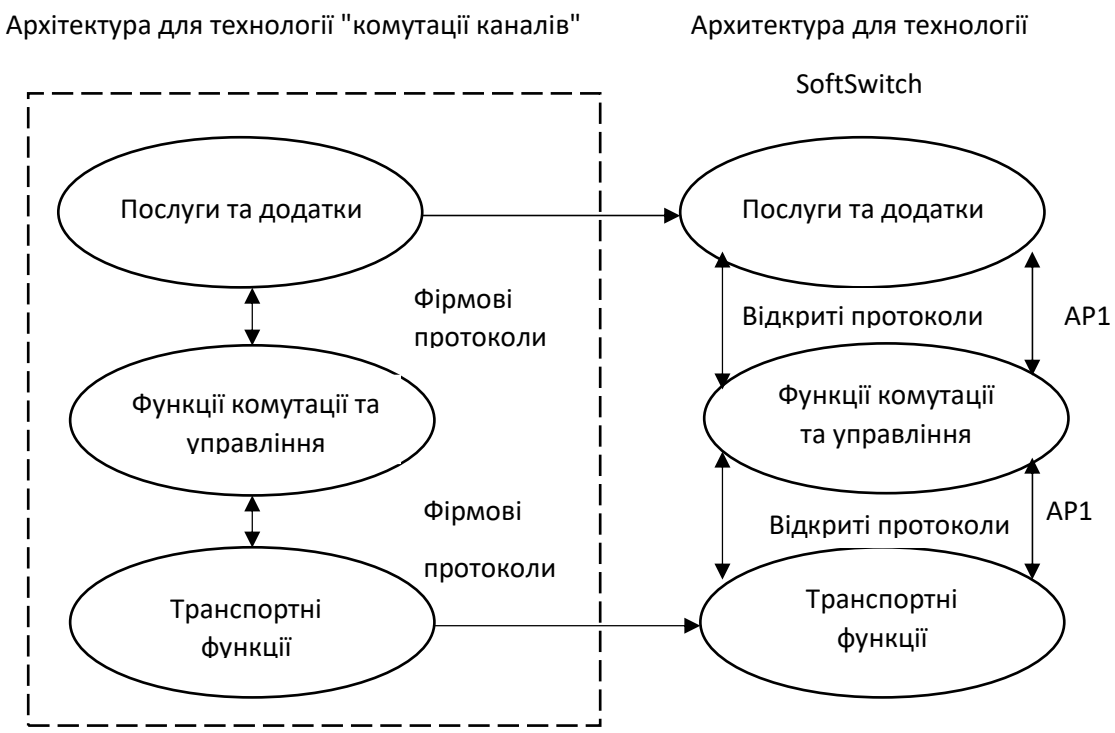


Рисунок 1.3 – Архітектура комутаційних станцій ТМЗК та Softswitch

Для мережі NGN визначено ряд нових протоколів, частина з яких була розроблена раніше. Доцільно виділити п'ять наступних протоколів:

1 Протокол H.323. Рекомендація MCE H.323 була розроблена для забезпечення встановлення з'єднання і передачі голосового та відео трафіку по пакетним мережам, зокрема Інтернет і intranet, які не гарантують якості обслуговування (QoS). Використовується протокол RTP, розроблений IETF (інженерна група з проблем Інтернет), а також стандартні кодеки, що відповідають вимогам MCE, які викладені в рекомендаціях серії G. Протокол H.323 був першим в технології IP-телефонії, але зараз він почав поступатися позиціями розробленого IETF протоколу SIP (ініціювання сеансів зв'язку), який виявився простіше і краще зі зміненим розміром.

2 Session Initiation Protocol. Це протокол прикладного рівня, за допомогою якого здійснюються такі операції, як встановлення, зміна і

завершення мультимедійних сесій або викликів по IP-мережі. В мультисервісних мережах SIP виконує функції, аналогічні тим, які реалізовані в протоколі H.323. Сесії SIP можуть включати мультимедійні конференції, дистанційне навчання, Інтернет-телефонію і інші подібні програми. Сьогодні SIP розглядається багатьма учасниками инфокомуникаційного ринку як міжнародний стандарт.

3 Media Gateway Control Protocol. Протокол MGCP використовується для управління шлюзами MG. Він розроблений для архітектури, в якій вся логіка обробки викликів розташовується поза шлюзами, і управління виконується зовнішніми пристроями, такими, як MGC або агенти викликів. Модель викликів MGCP розглядає медіа-шлюзи як набір кінцевих точок, які можна з'єднати одну з одною.

4 MEGACO/H.248. Цей протокол, скоріше всього, замінить MGCP в якості стандарту для управління медіа-шлюзами. MEGACO служить загальною платформою для шлюзів, пристроїв управління багатоточковими з'єднаннями, а також пристроїв інтерактивного голосової відповіді.

5Протокол Signalling Transport (SIGTRAN). Це набір протоколів для передачі сигнальної інформації по IP-мережах. Він використовується як в обох видах шлюзів, так і в Softswitch. SIGTRAN реалізує функції протоколу SCTP (Simple ControlTransport Protocol) і рівнів адаптації (Adaptation Layers). SCTP відповідає за надійну передачу сигнальної інформації, здійснює управління сигнальним трафіком, забезпечує безпеку. У функції Adaptation Layers входить передача сигнальної інформації від відповідних сигнальних рівнів, що використовують послуги SCTP. Ці протоколи відповідальні за сегментацію і пакетування призначених для користувача даних, захист від імітації законного користувача, зміни сенсу переданої інформації і ряд інших функцій.

Нижче, на рис. 1.4 представлений приклад узагальненої схеми побудови мережі NGN:

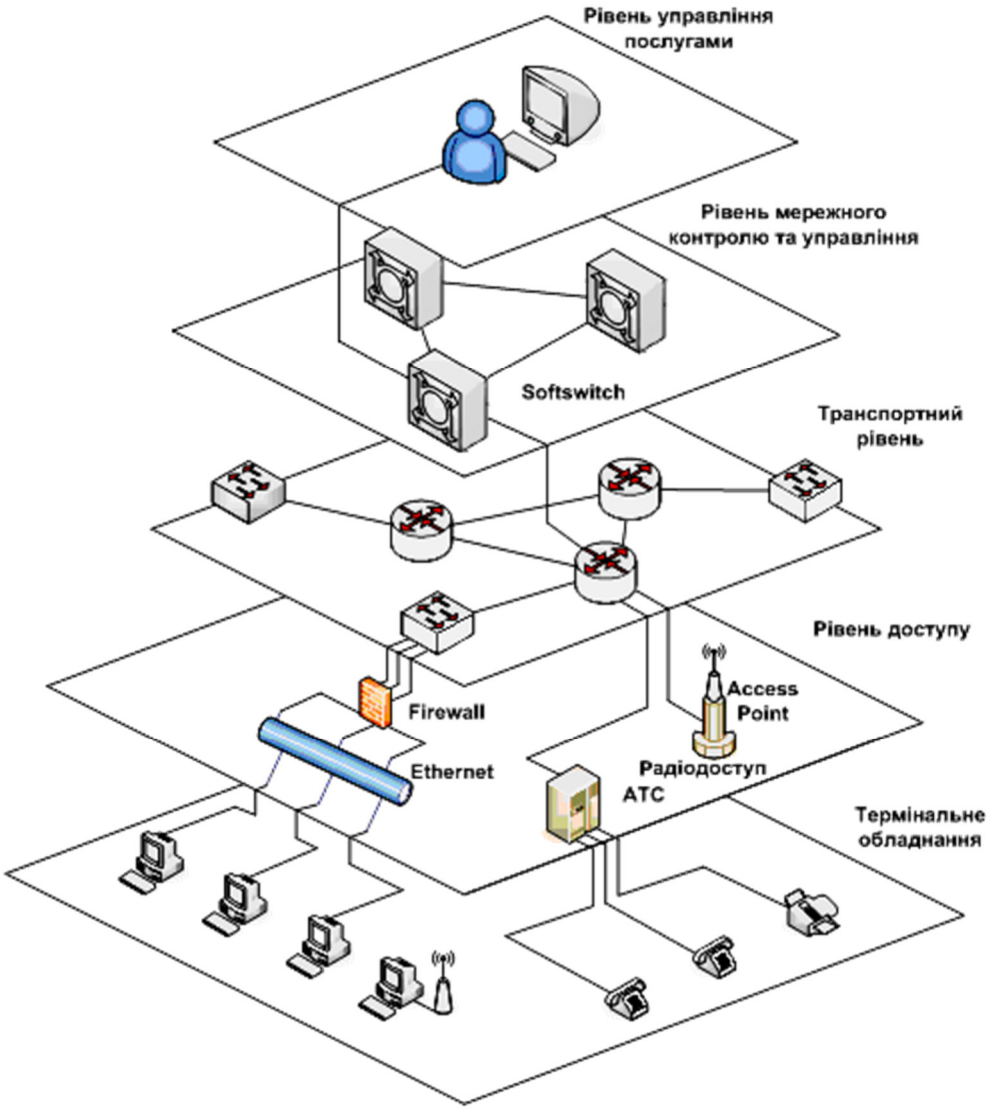


Рисунок 1.4 – Чотирирівнева архітектура мережі наступного покоління

NGN в Україні. Відповідно до положень «Концепції конвергенції телефонних мереж і мереж з пакетною комутацією в Україні» визначена функціональна архітектура та складові NGN, зображені на рис. 1.5, а її фізична реалізація — на рис. 1.6.

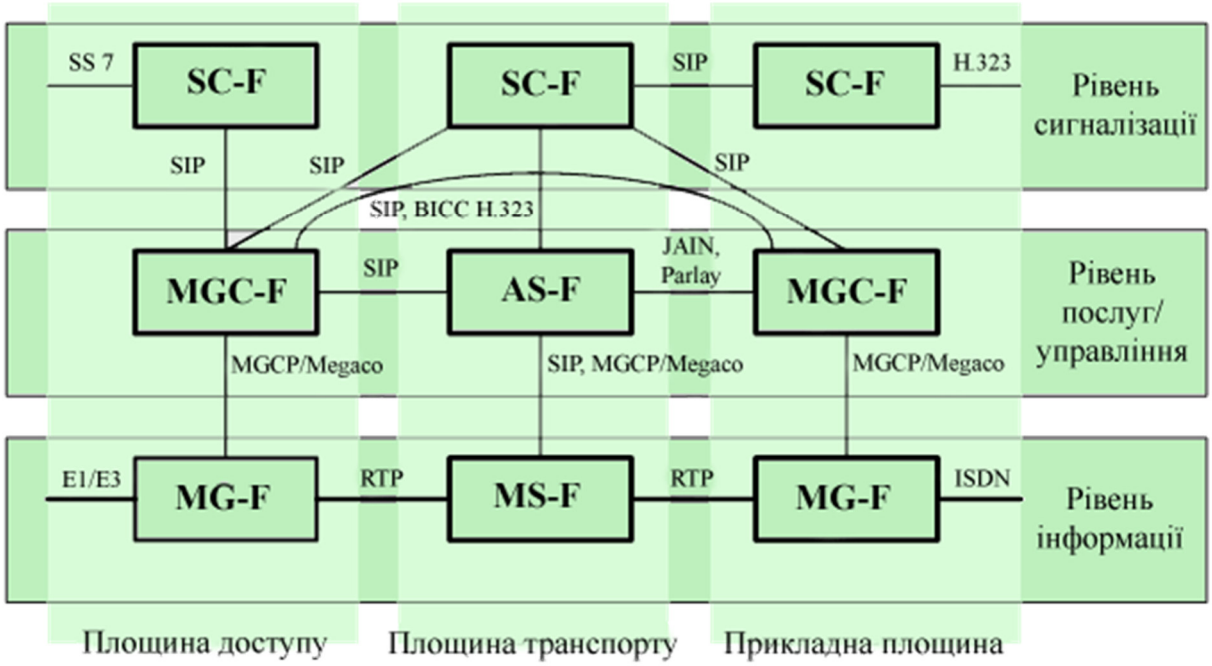


Рисунок 1.5 – Функціональна архітектура NGN:

SS7 — система загальноканальної сигналізації (ЗКС7); MGC-F — функція контролера медіашлюзів; AS-F — функція сервера прикладних програм; MGCP/Megaco — протоколи управління медіашлюзами; BICC — незалежний від середовища протокол виклику; MG-F — функція медіашлюзу; E1/E3 — тип потоку, який визначає швидкість; MS-F — функція медіасервера; ISDN — цифрова мережа з інтеграцією послуг; RTP — протокол передавання в реальному часі; SC-F — функція перетворення сигналів; JAIN, Parlay — відкриті інтерфейси прикладного програмування; SIP — протокол управління з’єднанням.

Функціональна архітектура NGN [Поповський В.В. та ін. Телекомунікаційні системи та мережі. Том 1. Структура й основні функції. ТОВ «Компанія СМІТ», 2018] поділяється на три функціональні площини та чотири функціональні шари. Функціональними площинами NGN є: площина транспорту, площина доступу та прикладна площина. У цій градації втілено основний принцип NGN — впровадження послуг, що не залежать від систем доступу до них, і відокремлення транспорту від систем доступу й обслуговування.

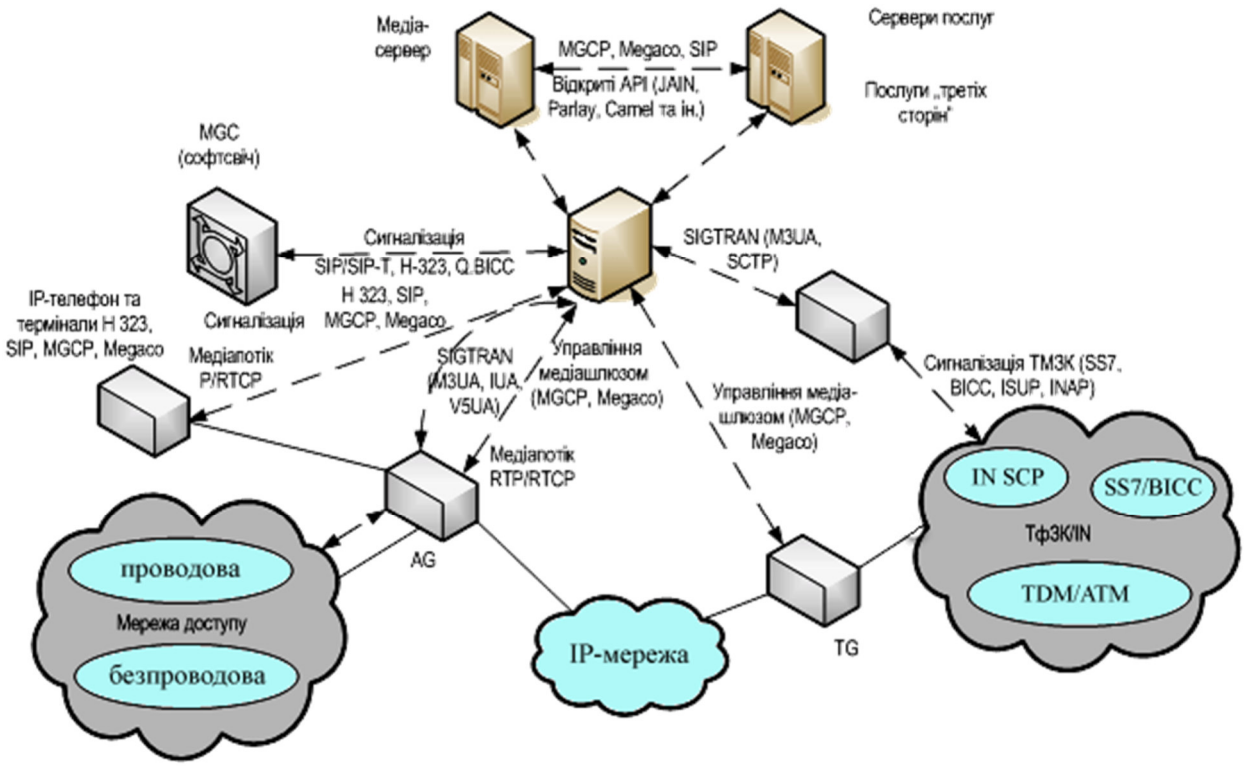


Рисунок 1.6 – Фізична реалізація архітектури NGN:AG — шлюз доступу:

RTP/RTCP — протоколи передавання в реальному часі; BICC — сигнальний протокол управління викликом; SG — шлюз сигналізації; INAP — прикладна частина протоколу сигналізації № 7 інтелектуальної мережі; SIGTRAN — протокол транспортування сигналізації; ISUP — частина

протоколу сигналізації ЗКС7 користувача; SCP — вузол управління послугами; MGC — контролер медіашлюзу; TG — транзитний медіашлюз.

У площині доступу здійснюється адаптація різноманітних технологій перенесення інформації для передавання через транспортну площину. У цій площині, зокрема, здійснюється конвертація потоків з часовим розподілом сигналів у пакетний формат і перетворення сигналізації ТМЗК у сигналізацію транспортної мережі.

Прикладна площина відповідає за надання користувачам послуг шляхом маніпулювання інформаційними та сигнальними потоками у мережі.

За типом інформації, що передається, функціональні об’єкти NGN поділяються на чотири рівні: сигналізації, послуг/управління, інформації та мережного управління. Компонентами функціональних рівнів є функції, основними з яких є: функція медіашлюзу, функція контролера медіашлюзів, функція сервера прикладних програм, функція медіасервера, функція перетворення сигналізації та функція тарифікації. Ці функції можуть бути фізично реалізовані як окремі пристрої, або ж один пристрій може поєднувати декілька функцій.

Рівень послуг/управління здійснює управління послугами та виконанням сервісної логіки, забезпечуючи обробку викликів та надання різних за складністю послуг. До пристроїв цього рівня належать так званий софтсвіч — Softswitch (або контролер медіашлюзів — MGC) та сервер прикладних програм AS. Для реалізації послуг ці пристрої взаємодіють з пристроями рівнів інформації та сигналізації. Взаємодія між шлюзом і контролером здійснюється через протокол Megaco (H.248) або MGCP.

Контролер медіашлюзів управляє роботою одного або кількох медіашлюзів, що забезпечують взаємодію мереж на нижчих рівнях, і

зосереджує у собі інтелект пари «шлюз — контролер», яка виконує функції місцевої або міжміської АТС.

1.4 Технологія SIGTRAN

1.4.1 Опис технології

Архітектура SIGTRAN описує взаємовідносини між функціональними і фізичними об'єктами, які обмінюються сигнальною інформацією, наприклад, шлюзами сигналізації (Signaling Gateways, SG) і контролерами транспортних шлюзів (Media Gateway Controllers, MGC) і визначає інтерфейси, на яких може використовуватися транспортування інформації сигналізації, а також функціональні та якісні вимоги, які пред'являються існуючими сигнальними протоколами мережі з комутацією каналів (Switched Circuit Network, SCN).

Транспортування сигнальної інформації забезпечує прозору передачу повідомлень протоколів сигналізації через мережі IP.

Функції транспортування сигнальної інформації повинні використовуватися для передачі інформації сигналізації ТМЗК між блоком шлюзу сигналізації (Signaling Gateway Unit) і блоком контролера транспортного шлюзу (Media Gateway Controller Unit). Транспортування сигнальної інформації може також використовуватися при передачі повідомлень сигналізації між блоком транспортного шлюзу (Media Gateway Unit) і блоком контролера транспортного шлюзу (Media Gateway Controller Unit), між розосередженими блоками контролерів транспортних шлюзів і між двома блоками шлюзів сигналізації (Signaling Gateway Unit), що з'єднують кінцеві точки сигналізації або STP в мережі з комутацією каналів.

Транспортування сигнальної інформації визначається таким чином, щоб підтримувати інкапсуляцію і передачу різноманітних протоколів SCN, а також забезпечувати незалежність від функцій транслювання (перетворення) будь-

яких протоколів SCN, що діють на кінцевих точках перенесення сигнальної інформації, оскільки його функція обмежена транспортуванням протоколу SCN.

Загальна функціональна модель [5], яка розділяє функції SG, MGC і MG, може бути реалізована різними способами з функціями, реалізованими в окремих пристроях або об'єднаними в єдині фізичні блоки (рис.1.7).

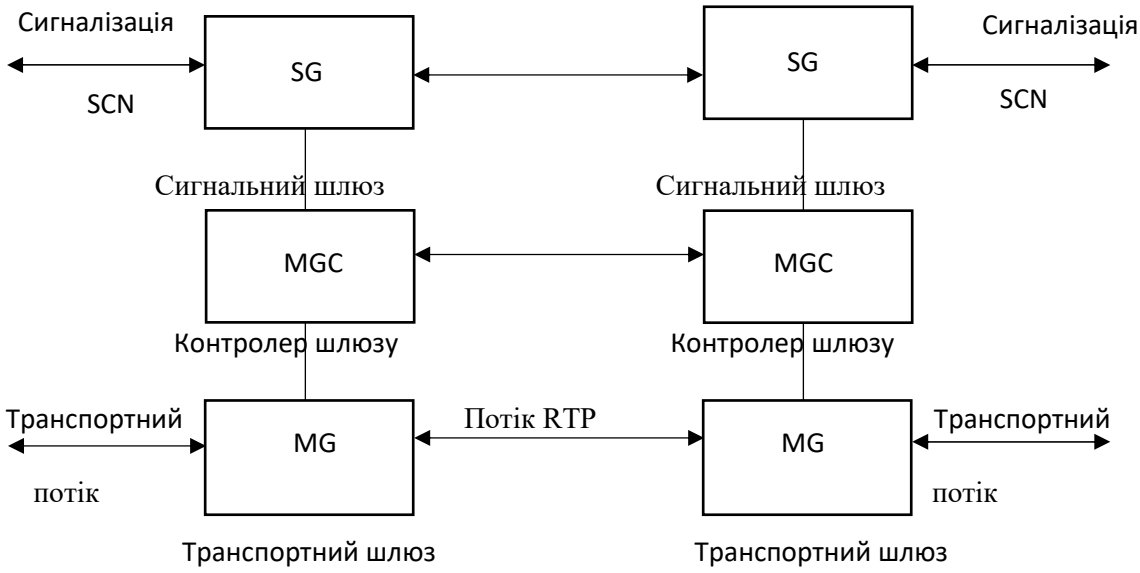


Рисунок 1.7 – Функціональна модель SIGTRAN

Інтерфейси транспортування сигнальної інформації: SG-MGC, SG SG і, можливо, MGC-MGC або MG-MGC - в залежності від вимог до транспортування відповідного протоколу.

1.4.2 Архітектура SIGTRAN

Технологія SIGTRAN має на увазі під собою наявність наступних трьох рівнів, згідно RFC 2719 (рис. 1.8):

1 Internet protocol (IP-протокол).

2 Протокол передачі інформації для управління потоками SCTP (Stream Control Transmission Protocol), який підтримує перенесення сигнальних повідомлень між кінцевими пунктами сигналізації SP в IP-мережі. Для організації сигнального зв'язку один кінцевий пункт надає іншому перелік своїх транспортних адрес (IP- адреси в поєднанні з портом SCTP). Протокол SCTP дозволяє незалежно впорядковувати сигнальні повідомлення в різних потоках і забезпечує перенесення сигнальної інформації з підтвердженням прийому, без помилок і дублювання, доставку повідомлень кожного потоку зі збереженням черговості їх проходження, можливість об'єднання декількох повідомлень в один пакет SCTP, фрагментацію даних у міру необхідності, стійкість до перевантажень і т.п.

3 Рівень адаптації, що забезпечує інтерфейс з протоколами і додатками верхнього рівня, так що ці програми не відчувають, що нижчеприведене транспортування здійснюється в IP-середовищі, а не за традиційними протоколами перенесення повідомлень MTP стека ЗКС7, наприклад.

Протокол SCTP надає можливість використовувати його для надійної доставки сигнального трафіку інших типів, що не входить в стек ЗКС7. В область інтересів Sigtran включені також адаптаційні рівні різних протоколів, що дає можливість пересилати по SCTP сигнальні повідомлення не тільки ЗКС7, а наприклад, Q.931 ISDN або V5.2.

Використання в якості транспортного протоколу саме SCTP пояснюється тим, що UDP і TCP не відповідають суворим вимогам ЗКС7 до параметрів втрат повідомлень і до дотримання черговості проходження повідомлень. Ці вимоги не дозволяють всерйоз використовувати UDP, оскільки він ненадійний в своїй основі. Протокол TCP ближчий до вимог, але і він не підходить за своїми часовими характеристиками: хоча TCP може гарантувати сувору черговість доставки повідомлень, доставка відбувається недостатньо швидко. Це пов'язано з тим, що блокування даних, що прийшли несвоєчасно, яке пропоновано протоколом TCP, вносить непотрібну затримку.

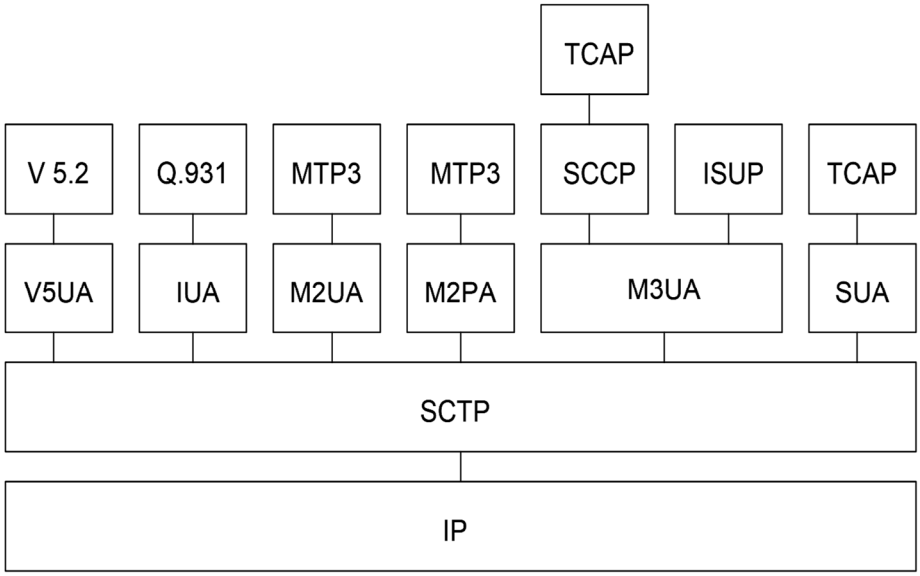


Рисунок 1.8 – Архітектура SIGTRAN

Протокол TCP відстежує передані байти і підтверджує прийняті байти. Цей характер протоколу TCP, орієнтований на передачу байтів, часто заважає, коли додаток бажає відстежувати надіслані повідомлення в цілому.

Обмежена область дії TCP-портів ускладнює завдання перенесення даних з множинною адресацією - дуже важливу обставину. Ще один аспект, що говорить на користь SCTP, це вразливість TCP до атак зловмисників, що призводить до відмови в обслуговуванні.

Рівні адаптації забезпечують сполучення SCTP з протоколами верхнього рівня. Більшість з них орієнтовано на ОКС7, в першу чергу, на протокол ISUP, але два відносяться до сигналізації інших типів. У число працюючих поверх SCTP модулів адаптації входять наступні:

M2UA (MTP2-User Adaptation Layer) забезпечує адаптацію SCTP до MTP3 таким чином, щоб стандартний протокол MTP3 міг використовуватися в мережі IP, реалізуючи транспортування повідомлень через SCTP і IP замість MTP2. Наприклад, реалізований в Softswitch стандартний додаток MTP3 може обмінюватися керуючими повідомленнями мережевої сигналізації із зовнішньою мережею ЗКС7. Таким же чином, як в мережі ЗКС7 MTP2 надає

свої послуги MTP3, M2UA надає свої послуги MTP3 в мережі IP. M2UA має зареєстрований номер порту 2904.

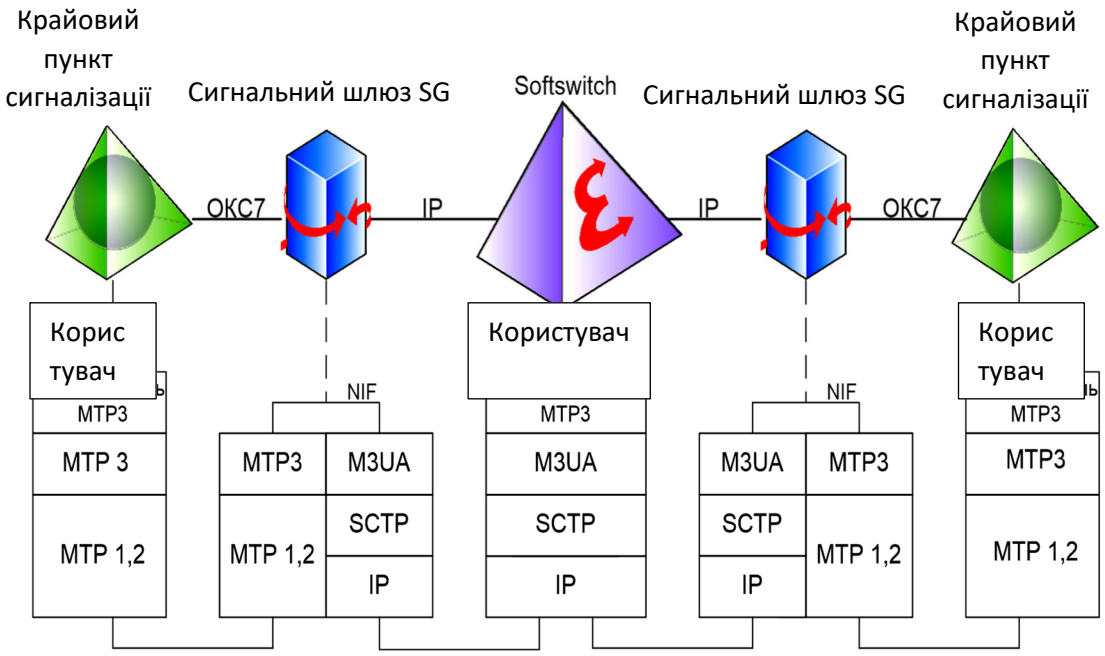


Рисунок 1.9 – Структура m2ua

M2PA (MTP2 Peer-to-Peer Adaptation Layer) також забезпечує адаптацію SCTP до MTP3, але вже в іншій області. Аналогічно до випадку з M2UA, рівень MTP3 в вузлі мережі IP обмінюється інформацією з M2PA, як якщо б він був звичайним MTP2. Відмінності між M2UA і M2PA визначаються їх ролями в мережевій архітектурі: якщо Softswitch з'єднується з мережею ЗКС7 просто на правах терміналу сигналізації ЗКС7, то досить застосування M2UA. Шлюз SG, який використовує M2PA, сам фактично є транзитним пунктом сигналізації STP на базі IP, у нього є власний код пункту сигналізації, він може також виконувати функції сигналізації верхнього рівня, такі як функції SCCP.

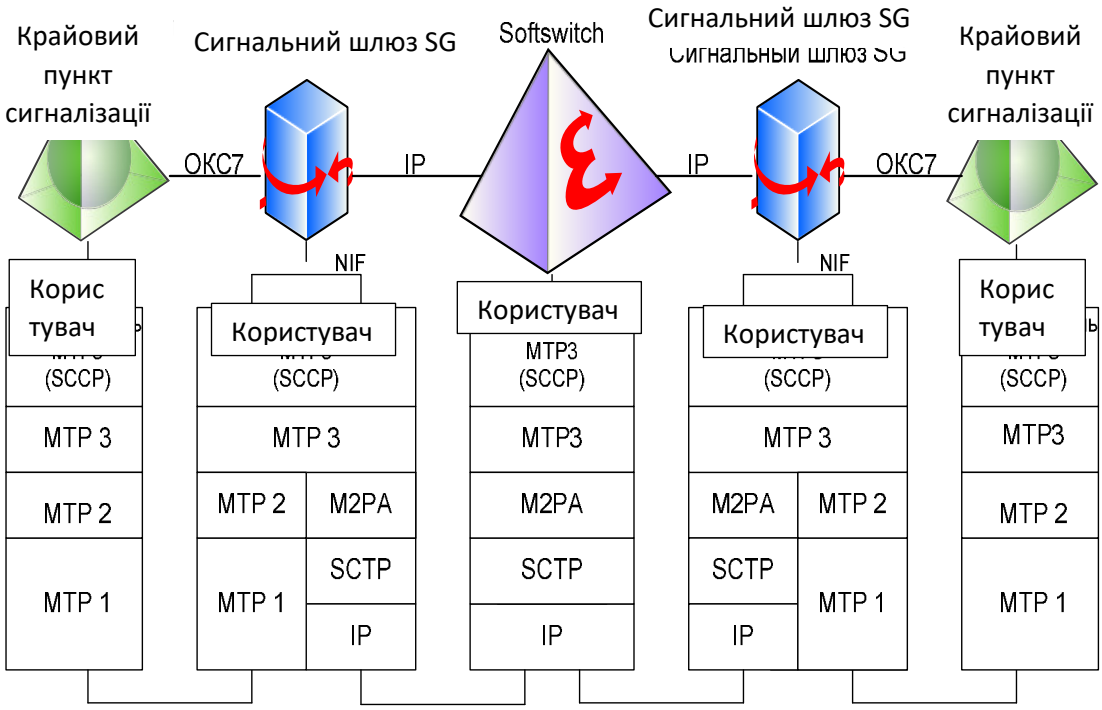


Рисунок 1.10 – Структура m2pa

M3UA (MTP3-User Adaptation Layer) забезпечує інтерфейс між SCTP і тими протоколами ЗКС7, які використовують послуги MTP3, наприклад, ISUP і SCCP. Завдяки M3UA ці протоколи не відчувають, що замість типового транспортування MTP3 використовується транспортування SCTP поверх IP.

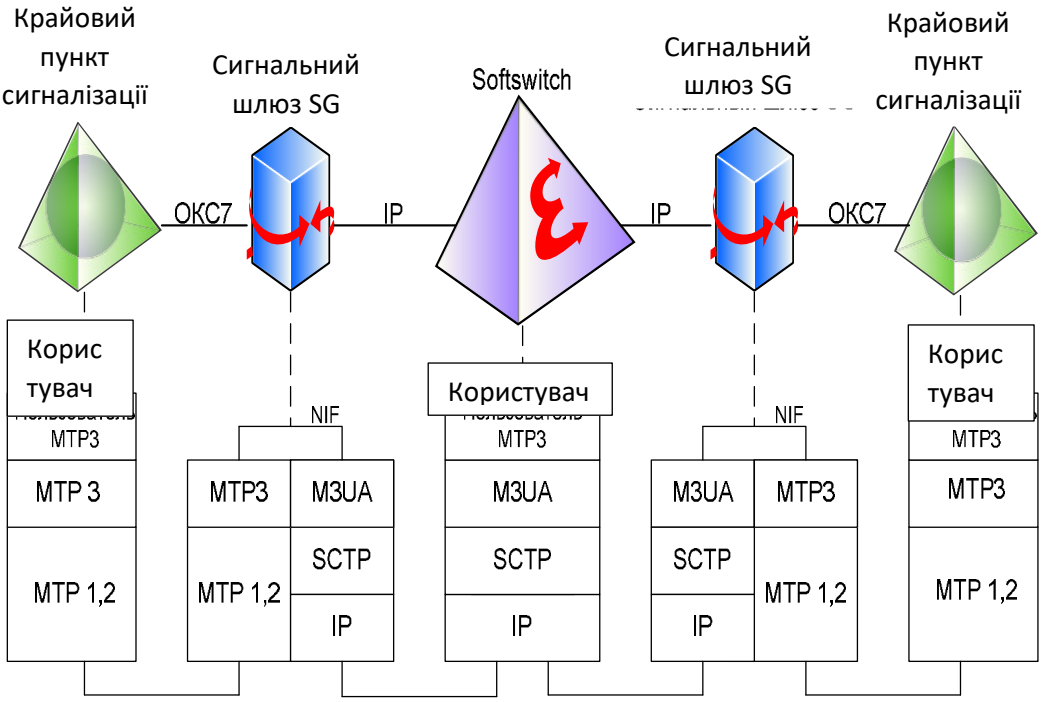


Рисунок 1.11 – Структура m3ua

SUA (SCCP-UserAdaptation Layer) - забезпечує інтерфейс між протоколом SCCP стека ЗКС7 і SCTP, завдяки чому такі прикладні підсистеми-користувачі SCCP як TCAP використовують послуги SUA точно так, як вони використовують послуги SCCP в мережі ЗКС7, навіть не підозрюючи, що все це відбувається в IP-мережі.

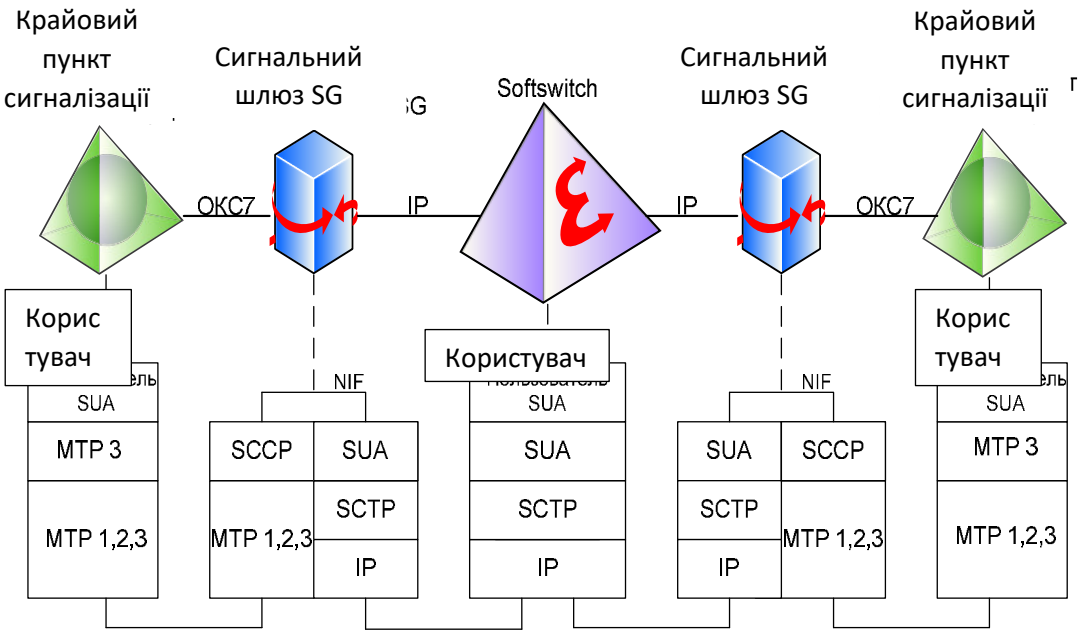


Рисунок 1.12 – Структура SUA

IUA (ISDN Q.921-User Adaptation Layer) теж працює поверх SCTP і забезпечує для сигналізації DSS1 за рекомендацією Q.931 прозоре транспортування повідомлень по мережі IP точно так, як вони передаються рівнем ланки даних Q.921 в мережі ISDN.

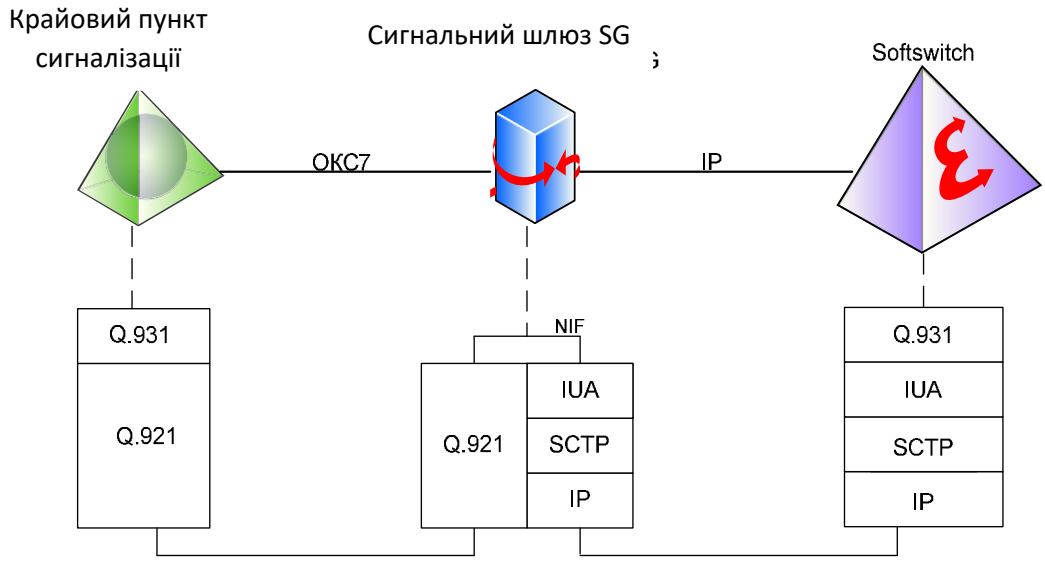


Рисунок 1.13 – Структура IUA

UA (V5-User Adaptation Layer) є рівнем адаптації для протоколу V5.2, також працює поверх SCTP.

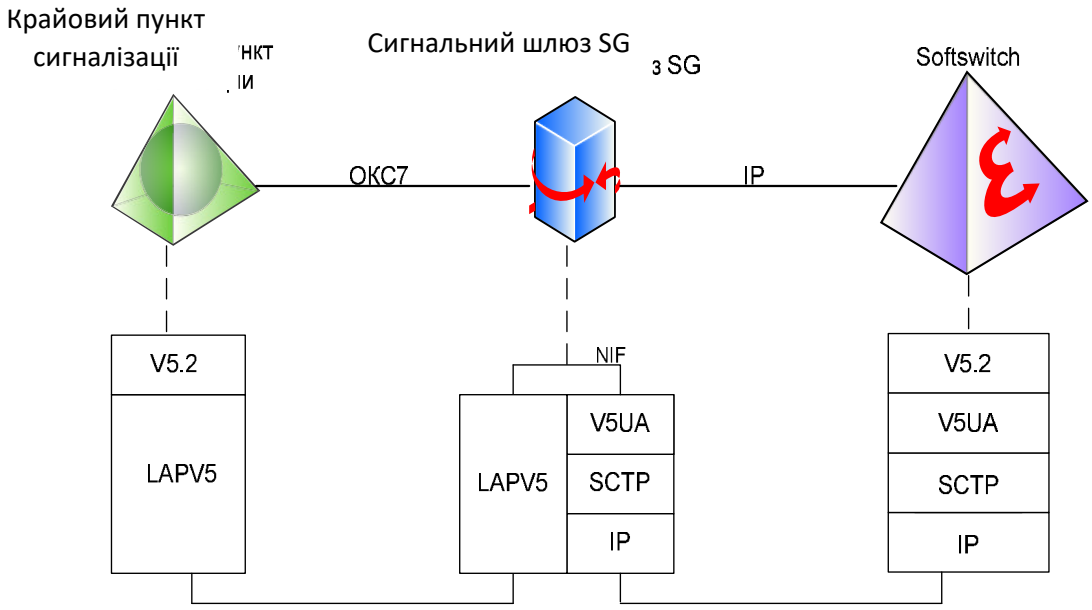


Рисунок 1.14 – Структура v5ua

1.4.3 Аналіз протоколу SCTP

У зв'язку з нездатністю UDP і TCP забезпечити необхідні вимоги ЗКС7, за транспортну основу взято протокол передачі з керуванням потоками SCTP (Stream Control Transmission Protocol), специфікований в документі RFC 2960.

Протокол SCTP реалізує такі принципи:

· підтверджуване, достовірне, вільне від помилок і не дубльоване пересилання призначених для користувача даних в потоках повідомлень (message streams), при якому усувається необхідність в забезпеченні суворого порядку проходження повідомлень, і повідомлення пересилаються на вищерозміщений рівень, як тільки вони отримані;

· сегментація даних для адаптації до розміру максимального блоку даних, що пересилається, що, втім, є обов'язковою умовою в світі IP і передбачає складання блоків даних в повідомлення на дальньому кінці;

· відсутність обов'язкового мультиплексування повідомлень в SCTP-дейтаграми;

· відмовостійкість на мережевому рівні;

· виключення перевантажень і протидію лавинам повідомлень та нелегальним проникненням в систему, що викликають перевантаження;

· функції експлуатаційного управління трактом передачі, що дозволяють встановити доступність адресата в режимі реального часу за допомогою періодичних контрольних повідомлень, і якщо виявляється, що поточний транспортний адрес одержувача недоступний, вибирається інша адреса зі списку можливих транспортних адрес цього одержувача.

Кінцевим пунктом SCTP є логічний передавач або приймач пакетів SCTP і являє собою комбінацію одного або кількох адрес і номера порту, причому SCTP дозволяє кінцевому пункту мати кілька IP-адрес і бути, таким чином, multihomed - розподіленим по декільком фізичним платформам, забезпечуючи тим самим стійкість до пошкоджень. Навіть маючи кілька IP-адрес, кінцевий пункт SCTP може використовувати тільки один номер порту. Таким чином, якщо у кінцевого пункту кілька IP-адрес, до кожного з них застосовується один і той же номер порту SCTP.

Коли активна транспортна адреса (комбінація IP-адреси і номера порту) недоступна, пробуються інші адреси віддаленого порту зі списку можливих транспортних адрес. Будь-яка транспортна адреса може застосовуватися тільки до одного кінцевого пункту SCTP, хоча кінцевий пункт може мати кілька транспортних адрес, працює шляхом встановлення зв'язків між кінцевими пунктами SCTP. Такий зв'язок називається асоціацією, причому вона визначається кінцевими пунктами SCTP, що беруть в ній участь, і поточним станом протоколу. Таким чином, SCTP-з'єднання (SCTP association) - це протокольний зв'язок між двома SCTP-портами, що містить протокольну інформацію про стан, включаючи теги верифікації і активний в даний момент

набір порядкових номерів передачі TSN. Два SCTP-порту в будь-який момент часу не повинні мати між собою більше одного SCTP-з'єднання. Перш ніж додатки двох кінцевих пунктів зможуть обмінюватися інформацією, необхідно встановити з'єднання. Коли комунікація закінчена, з'єднання можна припинити. Протоколи верхнього рівня ISUP, SCCP, TCAP та інші не інформовані про такі з'єднання, більш того, вони не виявляють того факту, що сигнальні повідомлення переносяться не стандартною MTP, а чимось іншим.

У кожному потоці SCTP проводиться упорядкування даних. Якщо фрагмент пакета, що належить деякому потоку, втрачений, то фрагменти цього пакета, наступні за втраченим, будуть зберігатися в буфері приймача потоку, поки втрачений фрагмент не буде переданий джерелом повторно.

Однак фрагменти пакетів з інших потоків можуть, як і раніше, проходити в додаток верхнього рівня, інакше кажучи, кожен потік обробляється окремо, так що доставка повідомлень одного потоку не затримується через очікування наступного по порядку повідомлення іншого потоку.

Пакет SCTP складається із загального заголовка і кількох фрагментів (chunks), як показано на рис. 1.15.

0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
Номер порту джерела																Номер порту адресата															
Тег верикації																															
Контрольна сума (Adler-32)																															
ID фрагменту								Прапор								Довжина фрагменту															
Значення фрагменту																															
ID фрагменту								Прапор								Довжина фрагменту															
Значення фрагменту																															
…																															
ID фрагменту								Прапор								Довжина фрагменту															
Значення фрагменту																															

Рисунок 1.15 – Загальний заголовок SCTP

Існують чотири основні категорії ідентифікаторів:

· Ідентифікатори перенесення даних користувача SCTP;

· Ідентифікатори перенесення керуючої інформації SCTP;

· Ідентифікатори, які резервовані IETF;

· Ідентифікатори перенесення розширень, визначених IETF.

1.4.4 Рівень адаптації M3UA

Завданням M3UA є забезпечення надання додатків в мережі IP послуг, аналогічних тим, які MTP3 надає додаткам таким як ISUP в мережі ЗКС7. Більш детально це видно з рис. 1.11 (наведеному вище), де показаний Softswitch, якому необхідно запустити додаток типу ISUP. Softswitch в загальному випадку може зробити це декількома способами. Наприклад, він може запустити ISUP поверх MTP3 поверх M2UA (або M2PA) поверх SCTP або ж Softswitch може реалізувати ISUP поверх M3UA поверх SCTP. Різниця

між цими двома способами визначається тим, де реально розташована функція MTP3. У сценарії, який показаний на рис. 1.11, звичайний протокол MTP3 присутній в шлюзах SG, а M3UA просто забезпечує додатку ISUP в Softswitch віддалений доступ до функції MTP3 в SG без відчуття додатком ISUP того, що функція MTP3 не є локальною, в даному випадку може мати код пункту сигналізації, відмінний від коду, який має SG. В цьому випадку SG працює подібно STP і сприймається зовнішньою мережею ЗКС7 як STP. Зовнішня мережа ЗКС7 розглядає Softswitch як звичайний кінцевий пункт сигналізації ЗКС7, доступ до якого досягається через один або кілька пунктів SG STP.

Для того щоб краще зрозуміти подальшу інформацію, слід відразу привести кілька визначень:

Під сервером додатків AS розуміється логічний об'єкт, який обробляє сигналізацію (наприклад, ISUP) в певній галузі (наприклад, для конкретного діапазону ЗКС7 DCP / OPC / CIC).

Процес сервера додатків ASP (Application Server Process] являє собою екземпляр AS. Сервер AS містить набір процесів сервера додатків. Фактично, AS можна розглядати як список процесів ASP, частина яких активна, а частина знаходиться в резерві.

Ключ маршрутизації (Routing Key) являє собою набір таких параметрів ЗКС7, як SLS, DPC, OPC або діапазон CIC, які визначають сигналізацію для деякого AS. Наприклад, якщо якийсь AS повинен обробляти сигналізацію ISUP для певної комбінації OPC/DPC/діапазон CIC, то ця комбінація і є ключем маршрутизації для такого AS. В межах SG кожен ключ маршрутизації зазвичай вказує на один певний AS. Інакше кажучи, між ключами маршрутизації і AS, як правило, існує однозначна відповідність.

Відображення мережі (Network Appearance) - це таке її уявлення, яке дозволяє відокремити частину сигнального трафіку, потрібного для зв'язку між SG і ASP, від всього трафіку, що використовує одне й те ж з'єднання SCTP,

наприклад, потік з національним кодом пункту сигналізації від потоку з міжнародним.

Кожен ASP необхідно асоціювати з кодом пункту сигналізації. Однак призначення кодів пунктів для процесів ASP є абсолютно гнучким. Наприклад, всі ASP, під'єднані до певного SG, можуть спільно використовувати той же код пункту, що і цей SG. В такому випадку комбінацію SG і процесів ASP видно мережі ЗКС7 як єдиний кінцевий пункт сигналізації. Або ж все ASP, під'єднані до одного SG, можуть мати один і той же код пункту, який відрізняється від коду пункту сигналізації, присвоєного цьому SG. В такому випадку SG буде видно мережі ЗКС7 як STP, а об'єднані загальним кодом ASP - як єдиний кінцевий пункт сигналізації, розташований за цим STP.

Ще одним варіантом призначення кодів може бути присвоєння кожному ASP свого коду пункту, або групам ASP - різних загальних кодів, відмінних від коду, присвоєного SG. В цьому випадку SG видно як STP, а кожен ASP (або група процесів ASP) - як один кінцевий пункт сигналізації. Справа в тому, що якщо якийсь ASP або якась група ASP може зв'язуватися з мережею ЗКС7 не через один, а через два SG, то цей ASP або ця група ASP повинні мати код пункту, який відрізняється від кодів цих двох SG. У такому сценарії шлюзи SG працюють як транзитні пункти сигналізації STP.

Щоб надавати послуги верхнього рівня прозоро (так, щоб додаток не відчував факт використання функцій MTP3, вбудованих в SG, замість функцій локальної MTP), M3UA повинен надавати верхньому рівню ті ж самі примітиви, які надає MTP3. Це такі примітиви:

· MTP-Transfer request передається з верхнього рівня в M3UA, щоб запросити перенесення повідомлення в певний пункт призначення.

· MTP-Transfer indication використовується M3UA, щоб пропустити вхідне повідомлення у верхній рівень.

· MTP-Pause indication передається M3UA в верхній рівень, щоб вказати, що передача сигналів у певний пункт призначення повинна бути припинена. Цей примітив використовується, наприклад, коли пункт призначення недосяжний.

· MTP-Resume indication передається M3UA в верхній рівень, щоб вказати, що передачу сигналів в пункт призначення можна відновити.

· MTP-Status indication передається M3UA в верхній рівень, щоб інформувати цей рівень про деякі зміни, що виникли в мережі ЗКС7, таких як перевантаження або недоступність підсистеми-користувача в пункті призначення.

1.4.5 Структура повідомлень рівня адаптації M3UA

Загальний заголовок повідомлення (рис. 1.16):

0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
версія								резерв								клас								тип							
Довжина повідомлення																															
тіло повідомлення																															

Рисунок 1.16 – Загальний заголовок M3UA

1 Поле версії містить версію рівня адаптації M3UA.

2 Наступні 8 біт зарезервовані для подальшого використання.

3 Всі повідомлення M3UA поділяються за такими класами:

· 00000000- MGMT (повідомлення управління);

· 00000001- повідомлення перенесення інформації;

· 00000010 - SSNM (повідомлення експлуатаційного управління мережею SS7);

· 00000011 - ASPSM (повідомлення експлуатаційного управління станом ASP);

· 00000100 - ASPTM (повідомлення експлуатаційного управління трафіком ASP);

· 00000101 - резерв для класу повідомлень, що відносяться до IUA;

· 00000110 - резерв для класу повідомлень адаптації користувача, що відносяться до M2UA;

· 00000111- резерв для класу повідомлень без встановлення з'єднання, що відносяться до SUA;

· 00001000 - резерв для класу повідомлень, що орієнтовані на з'єднання та відносяться до SUA;

· 00001001- RKM (повідомлення експлуатаційного управління ключем маршрутизації);

· 00001010 - резерв для класу повідомлень експлуатаційного управління ідентифікатором інтерфейсу M2UA;

· 00001011- резерв для класу повідомлень M2PA;

· 00001100 - 01111111- зарезервовані комітетом IETF;

· 10000000 - 11111111- зарезервовані для визначених IETF розширень класу повідомлень.

4 Кожен клас повідомлень має на увазі під собою такі типи:

- Для MGMT:

· 00000000 - помилка (ERR);

· 00000001 - повідомлення (NTFY);

· 00000010 - 01111111- зарезервовані комітетом IETF;

· 10000000 - 11111111- зарезервовані для визначених IETF розширень класу повідомлень.

- Для повідомлень перенесення інформації:

· 00000000 - резерв;

· 00000001 - дані (DATA);

· 00000010 – 01111111 - зарезервовані комітетом IETF;

· 10000000 – 11111111 - зарезервовані для IETF для розширень.

- Для SSNM:

· 00000000- резерв;

· 00000001 - адресат недоступний (DUNA);

· 00000010 - адресат доступний (DAVA);

· 00000011 - перевірка стану пункту призначення (DAUD);

· 00000100 - повідомлення перенавантаження мережі (SCON);

· 00000101 - підсистема-користувач в пункті призначення недоступна (DUPU);

· 00000110 - доступ до пункту призначення обмежений (DRST);

· 00000111 – 01111111 - зарезервовані комітетом IETF;

· 10000000 – 11111111 - зарезервовані для визначених IETF розширень класу повідомлень.

- Для ASPSM:

· 00000000 - резерв;

· 00000001 - включення ASP (ASPUP);

· 00000010 - виключення ASP (ASPDN);

· 00000011 - повідомлення про працездатність (BEAT);

· 00000100 - підтвердження включення ASP (ASPUP ACK);

· 00000101 - підтвердження виключення ASP (ASPDN ACK);

· 00000110 - підтвердження працездатності (BEAT ACK);

· 00000111 – 01111111 - зарезервовані комітетом IETF;

· 10000000 – 11111111 - зарезервовані для визначених IETF розширень класу повідомлень.

- Для ASPTM:

· 00000000 - резерв;

· 00000001 - активний стан ASP (ASPAC);

· 00000010 - неактивний стан ASP (ASPIA);

· 00000011 - підтвердження активного стану ASP (ASPAC ACK);

· 00000100 - підтвердження неактивного стану ASP (ASPIA ACK);

· 00000101 - 01111111 - зарезервовані комітетом IETF;

· 10000000 - 11111111- зарезервовані для визначених IETF розширень класу повідомлень.

- Для RKM:

· 00000000 - резерв;

· 00000001 - запит реєстрації (REG REQ);

· 00000010 - підтвердження реєстрації (REG RSP);

· 00000011 - запит скасування реєстрації (DEREG REQ);

· 00000100 - підтвердження скасування реєстрації (DEREG RSP);

· 00000101 - 01111111- зарезервовані комітетом IETF;

· 10000000 - 11111111- зарезервовані для визначених IETF розширень класу повідомлень.

5 Поле “довжина повідомлення” визначає довжину повідомлення в октетах, включаючи загальний заголовок і додаткові параметри.

Нижче наведена зведена таблиця всіх повідомлень M3UA.

Таблиця 1.1 Перелік всіх повідомлень M3UA

Им’я повідомлення	Клас повідомлення	Код класу повідомлення	Код типу повідомлення
Error (ERR)	MGMT	00000000	00000000
Notify (NTFY)	MGMT	00000000	00000001
Data	Transfer	00000001	00000001
Destination Unavailable (DUNA)	SSNM	00000010	00000001
Destination Available (DAVA)	SSNM	00000010	00000010
Destination State Audit (DAUA)	SSNM	00000010	00000011
SS7 Network Congestion State {SCON)	SSNM	00000010	00000100
Destination User Part Unavailable (DUPU)	SSNM	00000010	00000101
Destination Restricted (DRST)	SSNM	00000010	00000110
ASPUp(ASPUP)	ASPSM	00000011	00000001
ASP Down (ASPDN)	ASPSM	00000011	00000010
Heartbeat (BEAT)	ASPSM	00000011	00000011
ASP Up Acknowledgment (ASPUP ACK)	ASPSM	00000011	00000100
ASP Down Acknowledgment (ASPDN ACK)	ASPSM	00000011	00000101
Heartbeat Acknowledgment (BEAT ACK)	ASPSM	00000011	00000110
ASP Active (ASPAC)	ASPTM	00000100	00000001
ASP Inactive (ASPIA)	ASPTM	00000100	00000010
ASP Active Acknowledgment (ASPAC ACK)	ASPTM	00000100	00000001
ASP Inactive Acknowledgment (ASPIA ACK)	ASPTM	00000100	00000010
Registration Request (REG REQ)	RKM	00001001	00000001
Registration Response (REG RSP)	RKM	00001001	00000010
Deregistration Request (DEREG REQ)	RKM	00001001	00000011

De registration Response (DEREG RSP)	RKM	00001001	00000100

1.5 Постановка задачі

Метою даної дипломної роботи є розробка алгоритму обробки сигнальних повідомлень ЗКС7 в мережах NGN на базі технології SIGTRAN.

Для реалізації поставленої мети необхідно вирішити такі завдання:

1. Виконати аналітичний огляд літератури за темою дипломної роботи.
2. Розробити алгоритми обробки сигнальних повідомлень ЗКС7 в мережах NGN на базі технології SIGTRAN.
3. Розрахувати капітальні витрати на розробку алгоритмів.
4. Виконати аналіз отриманих результатів.

1.6 Висновки

Протоколи в мережі сигналізації ЗКС7 визначаються в залежності від мережі зв'язку. У аналогової ТМЗК застосовується протокол TUP, в цифровій ТМЗК застосовується протокол ISUP цифрової мережі з інтеграцією служб ISDN, протокол INAP інтелектуальної мережі IN. В аналоговій системі рухомого зв'язку NMT-450 застосовувався протокол MUP. З переходом на цифрові системи зв'язку необхідно уточнити склад протоколів четвертого рівня моделі ЗКС7.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальний опис ЗКС7

Основними підсистемами ЗКС7 є:

- Підсистема перенесення повідомлень (MTP - Message Transfer Part).

- Підсистеми-користувачі послугами MTP:

· SCCP - підсистема управління з'єднанням сигналізації;

· TUP - підсистема користувача телефонії;

· ISUP - підсистема користувача ISDN;

· MUP - підсистема користувача рухомого зв'язку (NMT);

· HUP - підсистема естафетної передачі сигналів управління в процесі розмови (NMT);

· TCAP - підсистема можливостей транзакцій;

· MAP - прикладна підсистема користувача рухомого зв'язку (GSM);

· INAP - прикладна підсистема інтелектуальної мережі;

· OMAP - підсистема технічного обслуговування і експлуатації. формує та надає послуги перенесення сигнальної інформації (у вигляді сигнальних повідомлень) від пункту-відправника через мережу ЗКС7 до пункту-адресату.

Користувачі послугами MTP - це підсистеми, які надають свої послуги або підсистемам, розташованим вище (як це робить SCCP), або (як це робить ISUP) прямо користувачам системи ЗКС7, якими є різноманітні прикладні процеси (це, зокрема, процес управління комутацією, процеси управління наданням тих чи інших додаткових послуг, процеси експлуатаційного управління та ін.).

На рис. 2.1 представлена архітектура протоколів ЗКС7.

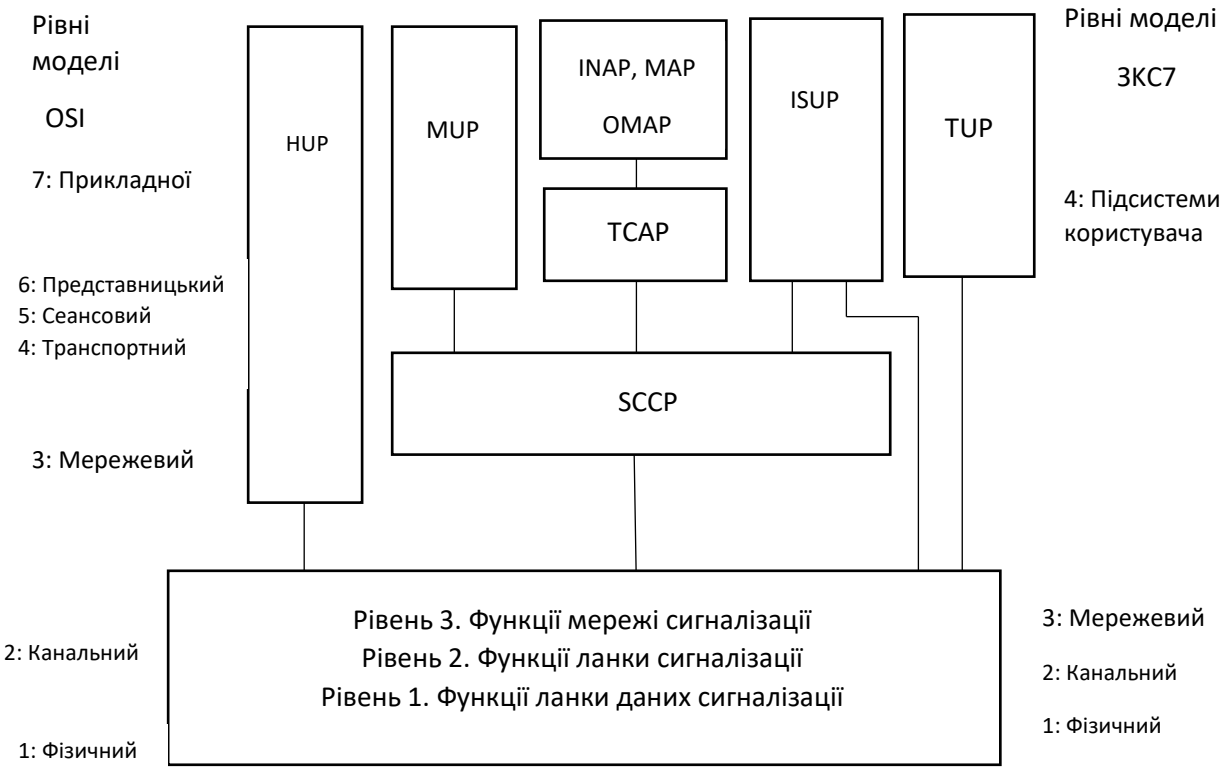


Рисунок 2.1 – Архітектура протоколів ЗКС7

Мережа зв'язку, що використовує ЗКС7, складається з безлічі вузлів комутації, пов'язаних між собою цифровими ІКМ-трактами.

Для використання послуг ЗКС7, кожен з вузлів комутації повинен містити вбудовані засоби, що дозволяють виконувати функції пункту сигналізації (SP - Signalling Point). Пункт сигналізації здатний формувати, надсилати, отримувати та інтерпретувати сигнальну інформацію.

Кожному пункту сигналізації присвоюється своя унікальниа адреса в мережі ЗКС7- код пункту сигналізації (SPC, signalling point code).

Пункти сигналізації SP повинні бути пов'язані між собою цифровими каналами, які виконують функції сигнальних ланок.

Сукупність пунктів сигналізації і ланок сигналізації утворюють мережу загальноканальної сигналізації - мережа ЗКС7.

В якості основних понять слід виділити наступні:

Пункти сигналізації (SP-signalling point) - вузли мережі зв'язку, що використовують ЗКС7, які можуть передавати і/або приймати сигнальний трафік, тобто генерувати та/або обробляти сигнальні повідомлення. Транзитний пункт сигналізації (STP-signalling transfer point) - пункт сигналізації, який передає прийняті сигнали на інший SP або STP, що не обробляючи при цьому сигнальні повідомлення.

Код пункту сигналізації (SPC - Signalling Point Code) - це унікальний номер пункту сигналізації в мережі ЗКС7.

Ланка сигналізації (signalling link) - ланка сигналізації в системі ЗКС7 використовується для передачі сигнальних повідомлень між двома пунктами сигналізації.

Пучок ланок сигналізації (signalling link set) - являє собою кілька ланок сигналізації між двома з'єднаними безпосередньо пунктами сигналізації.

Група ланок сигналізації (group of links) - це група сигнальних ланок в пучку, що мають ідентичні характеристики. Пучок ланок може включати одну або більше груп ланок.

У ЗКС7 сигнальна інформація організовується у вигляді пакетів, які передаються між пунктами сигналізації у вигляді повідомлень змінної довжини, які називаються сигнальними одиницями. Існує три типи сигнальних одиниць:

· Значуща сигнальна одиниця (MSU) - використовується для передачі сигнальної інформації, що формується підсистемами-користувачами або SCCP; повторюється в разі помилки;

· Сигнальна одиниця стану ланки (LSSU) - використовується для контролю стану ланки сигналізації; не повторюється в разі помилки;

· Заповнююча сигнальна одиниця (FISU) - використовується для забезпечення фазування ланки при відсутності сигнального трафіку; не повторюється в разі помилки.

8	16	8n,n>2	8	2	6	1	7	1	7	8
F	CK	SIF	SIO		LI	FIB	FSN	BIB	BSN	F

Рисунок 2.2 – Структура MSU

8	16	8або16	2	6	1	7	1	7	8
F	CK	SF		LI	FIB	FSN	BIB	BSN	F

Рисунок 2.3 – Структура LSSU

8	16	2	6	1	7	1	7	8
F	CK		LI	FIB	FSN	BIB	BSN	F

Рисунок 2.4 – Структура FISU

Прапор - обмежувач сигнальних одиниць - 8-бітова послідовність виду: 01111110. Зазвичай закриваючий прапор однієї сигнальної одиниці є відкриваючим прапором наступної сигнальної одиниці.

Індикатор довжини вказує на число октетів між полем LI та полем CK. Тип сигнальної одиниці ідентифікується індикатором довжини (LI) наступним чином: = 0 (FISU), що заповнює сигнальна одиниця = 1 або 2 (LSSU), сигнальна одиниця стану ланки > 2 (MSU), значуща сигнальна одиниця.

Індикатор довжини може приймати значення в інтервалі від 0 до 63.

Прямий порядковий номер (FSN) - це порядковий номер сигнальної одиниці, в складі якої він передається на протилежний пункт сигналізації.

Зворотний порядковий номер (BSN) - це номер підтверджуваної сигнальної одиниці. Прямий і зворотний порядкові номери - це двійкові числа в послідовності від 0 до 127, що циклічно повторюється.

Біти індикації прямого (FIB) і зворотного (BIB) напрямку разом з прямим і зворотним порядковими номерами використовуються в базовому методі виправлення помилок, для здійснення контролю послідовності сигнальних одиниць і функцій підтвердження.

Перевірочні біти (СК) формуються пунктом сигналізації, що передає сигнальну одиницю. Кожна сигнальна одиниця містить 16 перевірочних бітів для виявлення помилок.

Байт службової інформації (SIO):

7	6	5	4	3	2	1	0
поле подвида службы (SSF)				индикатор службы (SI)			

Рисунок 2.5 – Структура SIO

- Індикатор служби (SI):

· 0000 - управління мережею сигналізації;

· 0001 - тест ланки сигналізації;

· 0010 - резерв;

· 0011 - підсистема SCCP;

· 0100 - підсистема TUP;

· 010 1- підсистема ISUP;

· 0110 - підсистема DUP (виклики / канали);

· 0111 - підсистема DUP (реєстрація / дерегістрація);

· інші - резерв.

- Поле підвиду служби (SSF):

· 00xx - міжнародна мережа;

· 01xx - резерв (для міжнародного застосування);

· 10xx - національна мережа;

· 11xx - резерв (для національного застосування).

Індикатор служби SI займає 4 старших біта SIO, міститься тільки в значущих сигнальних одиницях MSU і вказує, до якої підсистемі користувача відноситься повідомлення.

Поле підвиду служби SSF займає 4 молодших біта SIO і містить індикатор мережі NI і два резервних біта. Індикатор мережі дозволяє відрізнити, який мережі належать повідомлення: міжнародній чи національній.

Поле сигнальної інформації (SIF) призначене для передачі корисної інформації по мережі сигналізації і може складатися максимум з 272 байтів, формати і коди яких визначаються підсистемою користувачів. Поле SIF містить інформацію, яка повинна передаватися між підсистемами користувачів двох пунктів сигналізації. Поле SIF містить етикетку, яка дозволяє:

· здійснювати маршрутизацію повідомлень за допомогою функцій рівня 3 MTP по мережі сигналізації до певного пункту призначення; ця частина етикетки називається етикеткою маршрутизації.

· асоціювати повідомлення на приймальній стороні конкретної підсистеми користувача з певним каналом, викликом, управлінням або іншими транзакціями, до яких відноситься повідомлення.

MTP не розпізнає вміст SIF, крім етикетки маршрутизації, тобто прозоро передає інформацію, що міститься в SIF, від рівня 4 одного пункту сигналізації до рівня 4 іншого.

Структура поля SIF в загальному випадку:

8n	32
Інформація управління MTP або сигнальна інформація	Етикетка маршрутизації

Рисунок 2.6 – Структура поля SIF

Для деяких підсистем користувача, крім етикетки маршрутизації, до складу етикетки входить додаткова інформація, при цьому поле SIF буде виглядати наступним чином:

Структура поля SIF для повідомлень ISUP (етикетка типу C):

8n	16	8	14	14
Сигнальна інформація	CIC	SLS	OPC	DPC

Рисунок 2.7 – Етикетка типу C

Структура поля SIF для повідомлень управління MTP (етикетка типу A):

8n	8	14	14
Інформація управління MTP	SLC	OPC	DPC

Рисунок 2.8 – Етикетка типу A

Код пункту призначення (DPC) вказує пункт призначення повідомлення.

Код вихідного пункту (OPC) визначає вихідний пункт повідомлення. Поле вибору ланки сигналізації (SLS) використовується, в разі необхідності, для здійснення поділу навантаження. Це поле існує у всіх типах повідомлень і завжди в одному і тому ж місці. Єдиний виняток з цього правила стосується деяких повідомлень підсистеми передачі повідомлень рівня 3 (наприклад, команда переходу на резерв), для яких функція маршрутизації повідомлень в вихідному пункті сигналізації не залежить від поля SLC: в цьому випадку поля, як такого, не існує, воно замінено іншою інформацією (наприклад, в разі команди переходу на резерв, ідентифікація ланки сигналізації, що відмовила). Код ідентифікації каналу (CIC) використовується в якості етикетки для повідомлень сигналізації, орієнтованих на з'єднання.

Поле інформацією управління MTP виглядає наступним чином

8n	7	6	5	4	3	2	1	0
Інформація	Заголовок H1 (тип повідомлення)				Заголовок H0 (группа повідомлень)			

Рисунок 2.9 – Структура поля інформації управління MTP

Поле стану (SF) не розглядається, тому що воно знаходиться тільки в сигнальних одиницях стану ланки (LSSU) і інтересу в даному випадку не представляє.

2.2 Повідомлення підсистеми MTP3

Всі повідомлення MTP3 поділяються за такими групами (H0 = xxxx):

- 0001 - повідомлення переходу на резерв і назад (група CHM);
- 0010 - повідомлення аварійного переходу на резерв (група ECM);

· 0011 - повідомлення керованої передачі і перенавантаження пучка маршрутів сигналізації (група FCM);

· 0100 - повідомлення заборони і дозволу передачі (група TFM);

· 0101- повідомлення тестування пучка маршрутів сигналізації (група RSM);

· 0110 - повідомлення заборони ланки системою управління (група MIM);

· 0111 - повідомлення дозволу відновлення трафіку сигналізації (група TRM);

· 1000 - повідомлення з'єднання ланки даних сигналізації (група DLM);

· 1010 - повідомлення управління потоком сигнального трафіку від підсистем користувача (група UFC);

Кожна група повідомлень ділиться на наступні типи (H1 = xxxx):

- Для CHM:

· 0001 - повідомлення переведення трафіку на резервну ланку (COO - Changeover order);

· 0010 - підтвердження переведення трафіку на резервну ланку (COA - Changeover acknowledgement);

· 0101 - повідомлення про повернення трафіку на вихідну ланку (CBD - Changeback Declaration);

· 0110 - підтвердження повернення трафіку на вихідну ланку (CBA - Changeback Acknowlegement).

- Для ECM:

· 0001 - повідомлення аварійного переведення трафіку на резервну ланку (ECO - Emergency Changeover Order);

· 0010- підтвердження аварійного переведення трафіку на резервну ланку (ECA - Emergency Changeover Acknowledgement);

- Для FCM:

· 0001 - повідомлення тестування рівня перенавантаження пучка сигнальних маршрутів (RCT - Signalling-route-set-congestion-test signal);

· 0010 - повідомлення управління перенесенням (TFC - Transfer control);

- Для TFM:

· 0001 - повідомлення про заборону перенесення (TFP - Transfer prohibited);

· 0011 - повідомлення обмеження перенесення (TFR - Transfer restricted);

· 0101 - повідомлення про дозвіл перенесення (TFA - Transfer allowed);

- Для RSM:

· 000 1- повідомлення тестування пучка маршрутів для пункту призначення, перенесення сигнальної інформації до якого заборонений (RST - Signalling-route-set-test signal for prohibited destination);

· 0010 - повідомлення тестування пучка маршрутів для пункту призначення, перенесення сигнальної інформації до якого обмежений (RSR - Signalling-route-set-test signal for restricted destination);

- Для MIM:

· 0001 - заборона доступу до ланки (LIN - link inhibit);

· 0010 - скасування заборони доступу до ланки (LUN - link uninhibit);

· 0011 - підтвердження заборони (LIA- link inhibited ack.);

· 0100 - підтвердження скасування заборони (LUA - link uninhibited ack.);

· 0101 - відхилення заборони (LID - link inhibit denied);

· 0110 - примусове скасування заборони (LFU - link force uninhibit);

· 0111 - перевірка стану заборони з ближнього кінця (LLT - link local inhibit test);

· 1000 - перевірка стану заборони з далекого кінця (LRT - link remote inhibit test).

- Для TRM:

· 0001 - повідомлення про дозвіл перезапуску трафіку (TRA - Traffic restart allowed).

- Для DLM:

· 0001 - повідомлення про підключення ланки передачі даних (DLC - Signalling data link connection order);

· 0010 - підключення зроблено (CSS - Connection-successful);

· 0101- підключення не зроблено (CNS - Connection-not-successful);

· 0110 - підключення неможливе (CNP - Connection-not-possible).

- Для UFC:

· 0010 - повідомлення про те, що підсистема-користувач є недоступною (UPU).

2.3 Функції та процедури MTP3

Функції підсистеми MTP3

Функції мережі сигналізації складають частину будь-якого пункту сигналізації, але на відміну від функцій рівня 2 MTP, виконуваних індивідуально для кожної ланки, функції рівня 3 MTP відносяться до мережі ЗКС7 в цілому.

Головним завданням цієї групи функцій є забезпечення гарантованої доставки повідомлень, що надходять від підсистеми користувача вихідного пункту сигналізації до відповідної підсистеми користувача в пункті сигналізації призначення, в умовах можливих відмов елементів мережі.

Аналогічно повідомленням, що надходять на рівень 3 МТР від підсистем користувачів, проводиться перенесення по мережі повідомлень, які генеруються самим рівнем 3 МТР.

Функції мережі сигналізації:

· Обробка сигнальних повідомлень

· Управління мережею сигналізації

Обробка сигнальних повідомлень має на увазі виконання функцій маршрутизації, відбору і розподілу повідомлень в кожному пункті сигналізації.

Управління сигнальною мережею включає управління сигнальним трафіком, сигнальними шляхами і ланками сигналізації. Ці функції потрібні для переконфігурування сигнальної мережі в разі виникнення відмов ланок або пунктів сигналізації, а також для управління трафіком при перенавантаженнях або блокуванні.

Обробка сигнальних повідомлень:

· Відбір повідомлень

Відбір повідомлень (прийнятих від рівня 2 МТР) використовується в пункті сигналізації для визначення на основі аналізу коду пункту призначення DPC, призначене чи ні прийняте повідомлення даного пункту.

· Розподіл повідомлень

Використовується в кожному пункті сигналізації для доставки прийнятих повідомлень, призначених цим пунктом, відповідній підсистемі користувача (або рівню 3 МТР).

· Маршрутизація повідомлень

Використовується в кожному пункті сигналізації для визначення на основі аналізу етикетки маршрутизації вихідної сигнальної ланки, за яким повідомлення повинно бути надіслано до відповідного пункту призначення.

Управління мережею сигналізації:

· Функція управління ланками сигналізації

· Функція управління сигнальним трафіком

· Функція управління маршрутами сигналізації

Функції управління мережею сигналізації забезпечують дії і процедури, необхідні для підтримки працездатності системи сигналізації і для відновлення нормальних умов при відмовах в мережі, ланках або пунктах сигналізації.

Повідомлення управління мережею сигналізації передаються по ланці сигналізації в значущих сигнальних одиницях.

Ланка сигналізації.

Може розглядатися рівнем 3 МТР як доступне або недоступне для перенесення сигнального трафіку.

Сигнальний маршрут.

Може розглядатися рівнем 3 МТР як доступний, обмежено доступний або недоступний.

Пункт сигналізації.

Може бути доступним/недоступним та досяжним/недосяжним.

Пучок маршрутів, що веде до пункту сигналізації, може бути в стані перевантаження або відсутності перевантаження.

Функція управління ланками сигналізації використовується для:

· Відновлення ланок сигналізації, що відмовили.

· Для включення в роботу недіючих ланок сигналізації.

· Для виведення ланок сигналізації з роботи.

Функція управління ланками сигналізації надає кошти для створення та технічної експлуатації пучків сигнальних ланок.

Автоматичне призначення ланок даних сигналізації, тобто виконання процедур включення і відновлення сигнальних ланок, здійснюється за допомогою команди на з'єднання ланки даних сигналізації DLC.

Формат даного повідомлення:

H0=1000; H1=0001

4	12	4	4	32
	Ідентифікатор ланки даних сигналізації	Код заголовку H1	Код заголовку H0	Етикетка

Рисунок 2.10 – Повідомлення DLC

У відповідь на повідомлення DLC зустрічний пункт сигналізації посилає повідомлення про результат спроби проведення з'єднання ланки даних сигналізації, яке містить в своєму складі один з трьох можливих сигналів:

4	4	32
Код заголовку H1	Код заголовку H0	Етикетка

Рисунок 2.11 – Структура відповідних повідомлень на DLC

· сигнал успішного з'єднання (CSS), H0 = 1000; H1 = 0010;

· сигнал неуспішного з'єднання (CNS), H0 = 1000; H1 = 0011;

· сигнал неможливості з'єднання (CNP), H0 = 1000; H1 = 0100.

Функція управління сигнальним трафіком включає в себе наступні процедури:

· перехід на резерв;

· відновлення вихідного стану;

· вимушена ремаршрутізація;

· керована ремаршрутізація;

· перезапуск MTP;

· заборона від системи управління;

· управління потоком сигнального трафіку.

Зміна шляху проходження сигнального трафіку у випадках недоступності або обмеженої доступності ланок або маршрутів проводиться за допомогою вищеперерахованих процедур:

недоступність сигнальної ланки (відмова, деактивація, блокування або заборона): використовується процедура переходу на резерв для перекладу сигнального трафіку на одну або декілька альтернативних ланок.

При цьому використовується зв'язка повідомлень команди переходу на резерв COO (H0 = 0001; H1 = 0001) і підтвердження переходу на резерв COA (H0 = 0001; H1 = 0010). Нижче представлений формат даних повідомлень:

1	7	4	4	32
	FSN останньої прийнятої MSU	Код заголовку H1	Код заголовку H0	Етикетка

Рисунок 2.12 – Повідомлення COO, COA

Також в разі, коли неможливо буде визначити прямий порядковий номер (FSN) останньої сигнальної одиниці (MSU), прийнятої по недоступній ланці, застосовується процедура аварійного переходу на резерв з використанням повідомлень ECO (H0 = 0010; H1 = 0001) і ECA (H0 = 0010 ; H1 = 0010).

4	4	32
Код заголовку H1	Код заголовку H0	Етикетка

Рисунок 2.13 – Повідомлення ECO, ECA

Доступність сигнальної ланки (відновлення, активація, розблокування або дозвіл): використовується процедура повернення на вихідну ланку для перекладу сигнального трафіку назад на ланку, що стала знову доступною. Для даної процедури існують повідомлення відновлення вихідного стану CBD (H0 = 0001; H1 = 0101) і підтвердження відновлення роботи CBA (H0 = 0001; H1 = 0110). Формат аналогічний ECO.

Недоступність сигнального маршруту: застосовується процедура вимушеної ремаршрутізації для перекладу сигнального трафіку на резервний

маршрут. Процедура ініціюється в SP в момент прийому повідомлення про заборону передачі TFP (H0 = 0100; H1 = 0001), з боку суміжного STP, за допомогою якого STP вказує на неможливість доставки повідомлення до пункту призначення, тобто на недоступність сигнального маршруту.

2	14	4	4	32
	Адреса пункту призначення, до якого відноситься повідомлення	Код заголовку H1	Код заголовку H0	Етикетка

Рисунок 2.14 – Повідомлення TFP

Доступність сигнального маршруту: застосовується процедура керованої ремаршрутізації для перекладу сигнального трафіку на маршрут, який став знову доступним. Процедура ініціюється в SP в момент прийому повідомлення про дозвіл передачі TFA (H0 = 0100; H1 = 0101) з боку суміжного STP, за допомогою якого він вказує на відновлення можливості доставки повідомлень до SP призначення, тобто на доступність сигнального маршруту. Формат аналогічний TFP.

Обмежена доступність сигнального маршруту: використовується процедура керованої ремаршрутізації для перекладу сигнального трафіку на маршрут, який був недоступним і став обмежено доступним.

Доступність пункту сигналізації: використовується процедура перезапуску MTP для перекладу сигнального трафіку в напрямку пункту сигналізації, який став доступним, для поновлення в ньому динамічних маршрутних даних. Процедура використовує повідомлення про дозвіл перезапуску трафіку TRA. Кожен суміжний SP після завершення передачі всіх необхідних повідомлень про заборону передачі в сторону SP, яка провадить перезапуск MTP, посилає повідомлення TRA (H0 = 0111; H1 = 0001), яке вказує, що вся інформація про недоступні напрямки передана. За кількістю

прийнятих повідомлень TRA система управління перезапускаючого SP оцінює ступінь завершеності процесу оновлення даних маршрутизації.

4	4	32
Код заголовку H1	Код заголовку H0	Етикетка

Рисунок 2.15 – Повідомлення TRA

Процедура заборони сигнальної ланки системою управління.

Мета процедури заборони ланки сигналізації з боку системи експлуатаційного управління - обмежити сигнальний трафік від підсистем користувачів за допомогою оголошення сигнальної ланки недоступною саме для цього виду трафіку. Процедура може застосовуватися для вирішення завдань технічної експлуатації ланок або для проведення тестування ланки. В результаті дій процедури не відбувається зміни стану ланки сигналізації на рівні MTP2, а ланка лише позначається як "заборонена" системою управління, що дозволяє передавати по ньому спеціальні повідомлення тестування. Дана процедура здійснюється за допомогою повідомлень групи MIM. Формат аналогічний TRA.

Процедура управління потоком сигнального трафіку.

Мета процедури управління потоком сигнального трафіку - обмеження трафіку на стороні його джерела, коли мережа сигналізації не здатна передати весь обсяг трафіку, що надходить від підсистеми користувача через відмови елементів мережі або їх тимчасове перенавантаження.

Операції управління потоком можуть застосовуватися при наступних подіях:

· Відмови в мережі сигналізації (в ланках або пунктах), що призвели до недоступності пучка маршрутів сигналізації.

· Перенавантаження ланки або пункту привело до ситуації, при якій здійснення реконфігурації не доцільно.

· Підсистема користувача через відмову не здатна обробляти повідомлення, що доставляються підсистемою MTP.

При недоступності підсистеми користувача застосовується повідомлення UPU (H0 = 1010; H1 = 0001):

4	4	2	14	4	4	32
Причина недоступності	Ідентифікатор підсистеми користувача	00	Адреса пункту призначення, до якого відноситься повідомлення	Код заголовку H1	Код заголовку H0	Етикетка

Рисунок 2.16 – Повідомлення UPU

Функція управління сигнальними шляхами.

Призначена для обміну інформацією між SP про доступність сигнальних маршрутів і включає в себе наступні процедури:

· Процедура керованої передачі;

· Процедура заборони передачі;

· Процедура дозволу передачі;

· Процедура обмеження передачі;

· Процедура випробування пучка маршрутів;

· Процедура перевірки перенавантаження пучка сигнальних маршрутів.

Мета функції управління маршрутами - відхилення сигнального трафіку від проблемного маршруту. Мета досягається посилкою повідомлень управління передачею, що ідентифікують проблемний напрямок за значенням коду SP призначення.

Відновлення інформації про стан маршруту проводиться процедурою випробування пучка маршрутів, а інформації про перенавантаження пучка маршрутів - в рамках процедури перевірки стану перенавантаження пучка.

Процедура керованої передачі.

На міжнародній мережі процедура керованої передачі використовується з однією метою: за допомогою повідомлення управління передачею (TFC) доставити індикацію про перенавантаження від SP, де виявлено перенавантаження, до вихідного SP.

У національних мережах, які використовують призначення пріоритетів в разі перенавантаження, обмежується прийом повідомлень з пріоритетом рівним або нижче заданого.

У національній мережі, де не використовується призначення пріоритетів, процедура керованої передачі служить для доставки за допомогою повідомлення TFC індикації про перенавантаження від SP, де виявлено перенавантаження, до вихідного SP.

У національних мережах, що використовують кілька статусів перенавантаження (до 4) і які не застосовують призначення пріоритетів, резервні біти, що містяться в повідомленні TFC, використовуються для позначення поточного рівня перенавантаження ланки.

Формат повідомлення TFC (H0 = 0011; H1 = 0010) представлений нижче

2	14	4	4	32
	Адреса пункту призначення, до якого відноситься повідомлення	Код заголовку H1	Код заголовку H0	Етикетка

Рисунок 2.17 – Повідомлення TFC

Процедура заборони передачі.

Виконується в STP, коли цей пункт повинен сповістити один або кілька суміжних SP про те, що через нього сигнальні повідомлення більше передаватися не повинні.

Процедура є наслідком повної відмови найкоротшого маршруту до пункту призначення. Процедура використовує повідомлення заборони передачі TFP. По прийому повідомлення TFP суміжний SP починає процедуру вимушеної ремаршрутизации, і при необхідності сам формує повідомлення TFP до інших пунктів.

Процедура дозволу передачі.

Процедура здійснюється у STP, коли цей STP повинен повідомити одному або кількома суміжним SP про можливості передавати через нього повідомлення, адресовані певним SP призначення, при цьому використовується повідомлення TFA. Дії суміжного SP аналогічні, як при забороні передачі.

Процедура обмеження передачі.

Процедура виконується в STP для повідомлень, призначених певному SP, коли цей STP повинен вказати суміжним SP про припинення, по-можливості, маршрутизації повідомлень через цей STP. Застосування

процедури допомагає уникнути подальшого перенавантаження вже перенавантаженої ділянки мережі.

Процедура застосовується тільки в національних мережах, при цьому використовується повідомлення обмеження передачі (TFR) (H0=0011; H1=0100). Формат даного повідомлення аналогічний TFC.

Процедура випробування пучка маршрутів.

Процедура випробування пучка маршрутів сигналізації дозволяє SP визначити можливість передачі сигнального трафіку до певного SP через суміжний STP.

Процедура використовує групу повідомлень тестування пучка маршрутів сигналізації (RSM) і процедури дозволу і заборони передачі. Процедура застосовується для відновлення інформації про досяжності напрямків, яка потенційно могла бути втрачена внаслідок відмов у мережі сигналізації.

Повідомлення тестування пучка маршрутів для обмеженого призначення (RSR) (H0 = 0101; H1 = 0010), або забороненого призначення (RST) (H0 = 0101; H1 = 0001) передаються SP, що виходить, після прийому повідомлень TFR або TFP, відповідно, щодо SP призначення з боку суміжного STP.

Повідомлення RSR і RST надсилаються з періодичністю T10 (30-60 с) до прийому повідомлення TFA, що вказує на знову виниклу досяжність пункту призначення.

З прийому повідомлення TFP, що означає недоступність тестованого маршруту, суміжний SP починає процедуру вимушеної ремаршрутізації, і при необхідності сам формує повідомлення TFP до інших SP.

По прийому від STP повідомлення TFA, що означає доступність тестованого маршруту, суміжний SP виконує процедуру керованої

ремаршрутізації, і при необхідності сам посилає повідомлення TFA іншим суміжним пунктам сигналізації.

Формат повідомлень RSR, RST:

2	14	4	4	32
	Адреса SP призначення, до якої відноситься повідомлення	Код заголовку H1	Код заголовку H0	Етикетка

Рисунок 2.18 – Повідомлення RSR, RST

Процедура перевірки перенавантаження пучка сигнальних маршрутів.

Процедура перевірки перенавантаження пучка сигнальних маршрутів використовується в вихідному SP для корекції рівня перенавантаження, пов'язаного з маршрутом до певного SP призначення. Процедура призначена для визначення можливості передачі до цього SP повідомлення із заданим або більш високим рівнем пріоритету перенавантаження.

У разі перезапуску MTP рівень перенавантаження всіх пучків сигнальних маршрутів в SP ініціалізується нульовим значенням. Щоб перевірити поточний стан пучків, процедура використовує повідомлення перевірки рівня перенавантаження пучка сигнальних маршрутів (RCT) (H0 = 0011; H1 = 0001).

4	4	32
Код заголовку H1	Код заголовку H0	Етикетка

Рисунок 2.19 – Повідомлення RCT

Виходячи з вище перерахованих можливостей m3ua і mtp3, можна підвести підсумок: m3ua - це тільки адаптаційний рівень між протоколами верхнього рівня і SCTP, він не є повною копією MTP3 в IP-мережі і не реалізує деякі стандартні керуючі повідомлення мережевої сигналізації mtp3.

2.4 Розрахунок пропускної здатності каналу для базового виклику.

Розрахунок обсягу трафіку в ЧНН:

Розрахунок буде проводитися для порівняння обсягу інформації, необхідної для здійснення базового виклику при використанні протоколу Sigtran (m3ua) і SIP.

Вихідні дані для розрахунку:

$N_{аб}$ = 480 (кількість абонентів);

$K_{ЧНН}$ = 3 викл / аб. (кількість викликів від одного абонента в годину);

Розраховуємо кількість викликів в ЧНН:

$$N_{ЧНН} = N_{аб} \cdot K_{ЧНН}$$

$$N_{ЧНН} = 480 \cdot 3 = 1440 \text{ викл.}$$

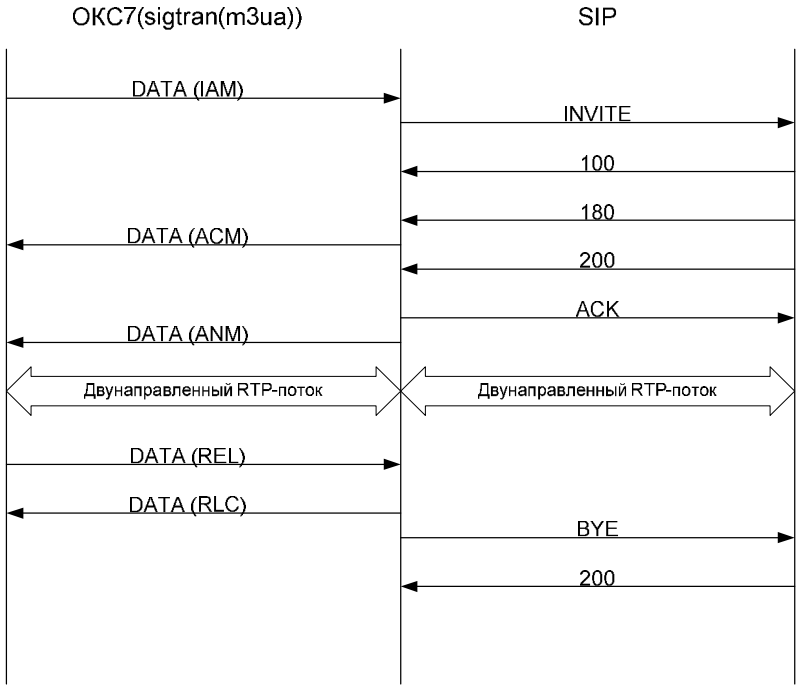


Рисунок 2.20 - Алгоритм обміну повідомленнями sigtran - SIP

- Для Sigtran (m3ua):

Для здійснення базового виклику при використанні sigtran (m3ua) потрібен обмін 5 повідомленнями (IAM, ACM, ANM, REL, RLC). При цьому дані упаковуються в пакети наступних протоколів: Ethernet, IP, SCTP, m3ua. Кожен з цих протоколів має свої заголовки.

Розміри заголовків:

Заголовок Ethernet: $l_{ethernet} = 14$ Байт;

Заголовок IP: $l_{IP} = 20$ Байт;

Заголовок SCTP: $l_{SCTP} = 44$ Байт;

Заголовок m3ua: $l_{m3ua} = 36$ Байт.

Загальний розмір заголовков:

$$l_{заг} = l_{ethernet} + l_{IP} + l_{SCTP} + l_{m3ua}$$

$$l_{заг} = 14 + 20 + 44 + 36 = 114 \text{ Байт.}$$

Розмір повідомлень:

Наведені нижче цифри є усередненими, тому що розмір повідомлень може варіюватися за рахунок необов'язкових параметрів.

Повідомлення IAM (m3ua): $l_{IAM} = 40$ байт;

Повідомлення ACM (m3ua): $l_{ACM} = 10$ байт;

Повідомлення ANM (m3ua): $l_{ANM} = 13$ байт;

Повідомлення REL (m3ua): $l_{REL} = 8$ байт;

Повідомлення RLC (m3ua): $l_{RLC} = 4$ байта.

Загальний розмір повідомлення з урахуванням заголовків:

IAM (m3ua): $l_{заг+IAM} = 114 + 40 = 154$ байта;

ACM (m3ua): $l_{заг+ACM} = 114 + 10 = 124$ байта;

ANM (m3ua): $l_{заг+ANM} = 114 + 13 = 127$ байт;

REL (m3ua): $l_{заг+REL} = 114 + 8 = 122$ байта;

RLC (m3ua): $l_{заг+RLC} = 114 + 4 = 118$ байт.

У підсумку на один базовий виклик доводиться:

$$l_{\sum} = l_{заг+IAM} + l_{заг+ACM} + l_{заг+ANM} + l_{заг+REL} + l_{заг+RLC}$$

$$l_{\sum} = 154 + 124 + 127 + 122 + 118 = 645 \text{ байт}$$

При цьому обсяг інформації з розрахунку ГНН:

$l_{ЧНН} = l_{\sum} \cdot N_{ЧНН}$

$l_{ЧНН} = 645 \cdot 1440 = 928800$ байт.

- Для SIP:

Для здійснення базового виклику при використанні протоколу SIP потрібен обмін 7 повідомленнями (INVITE, 100, 180, 200, ACK, BYE, 200). При цьому дані упаковуються в пакети наступних протоколів: Ethernet, IP, UDP. Кожен з цих протоколів має свої заголовки.

Розміри заголовків:

Заголовок Ethernet: $l_{ethernet} = 14$ байт;

Заголовок IP: $l_{IP} = 20$ байт;

Заголовок UDP: $l_{UDP} = 8$ байт;

Загальний розмір заголовків:

$l_{заг} = l_{ethernet} + l_{IP} + l_{UDP}$

$l_{заг} = 14 + 20 + 8 = 42$ байта.

Розмір повідомлень:

Наведені нижче цифри є усередненими, тому що розмір повідомлень може варіюватися за рахунок необов'язкових параметрів.

Повідомлення INVITE: $l_{INVITE} = 901$ байт;

Повідомлення 100: $l_{100} = 292$ байт;

Повідомлення 180: $l_{180} = 515$ байт;

Повідомлення 200: $_{200} = 598$ байт;

Повідомлення ACK: $l_{ACK} = 537$ байт.

Повідомлення BYE: $l_{BYE} = 331$ байт.

Загальний розмір повідомлення з урахуванням заголовків:

INVITE: $l_{заг+INVITE} = 42 + 901 = 943$ байта;

: $l_{заг+100} = 42 + 292 = 334$ байта;

: $l_{заг+180} = 42 + 515 = 557$ байт;

: $l_{заг+200} = 42 + 598 = 640$ байт;

ACK: $l_{заг+ACK} = 42 + 537 = 579$ байт.

BYE: $l_{заг+BYE} = 42 + 331 = 373$ байт.

У підсумку на один базовий виклик доводиться:

$$l_{\sum} = l_{заг+INVITE} + l_{заг+100} + l_{заг+180} + 2 \cdot l_{заг+200} + l_{заг+ACK} + l_{заг+BYE}$$

$$l_{\sum} = 943 + 334 + 557 + 2 \cdot 640 + 579 + 373 = 4066 \text{ байт}$$

При цьому об’єм інформації з розрахунку ЧНН:

$$l_{ЧНН} = l_{\sum} \cdot N_{ЧНН}$$

$$l_{ЧНН} = 4066 \cdot 1440 = 5855040 \text{ байта.}$$

Порівняльний аналіз:

Таблиця 5 – Порівняльний аналіз

Об’єм інформації в ЧНН (sigtran(m3ua))	Об’єм інформації в ЧНН (SIP)
928800 Байт	5855040 Байт

При використанні базового протоколу ISUP ОКС7 і технології Sigtran (m3ua) для використання його в IP-мережах, економія пропускної здатності - в 6 разів.

Підхід до точного розрахунку обсягу трафіку в каналі при використанні m3ua передбачає під собою наступні фактори, що впливають на підсумок обчислень:

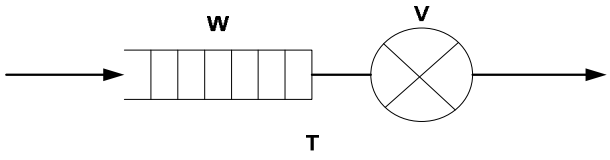
· Статистичну оцінку загальної кількості переданих повідомлень в ГНН, включаючи не тільки обсяг інформації, необхідний під процедури встановлення і руйнування з'єднання, але і трафік управління, у випадках перевантаження мережі, недоступності пунктів сигналізації і т.п.

· Розрахунок відповідно до обсягу інформації, створюваним іншими протоколами IP-мережі.

· Розрахунок з урахуванням мовного трафіку.

Розрахунок пропускної здатності каналу:

Для розрахунку необхідної пропускної здатності каналу скористаємося моделлю M/M/1. Дана система має на увазі під собою обслуговування найпростішого потоку викликів однолінійним пучком при показовому законі розподілу тривалості обслуговування і нескінченне число місць для очікування. Тобто припускаємо, що закон розподілу тривалості обслуговування близький до показового, що в більшості випадків відповідає дійсності.



T- середній час перебування в системі ($T = W + V$)

μ- середній час обслуговування (пропускна здатність)

λ- інтенсивність надходження викликів на систему

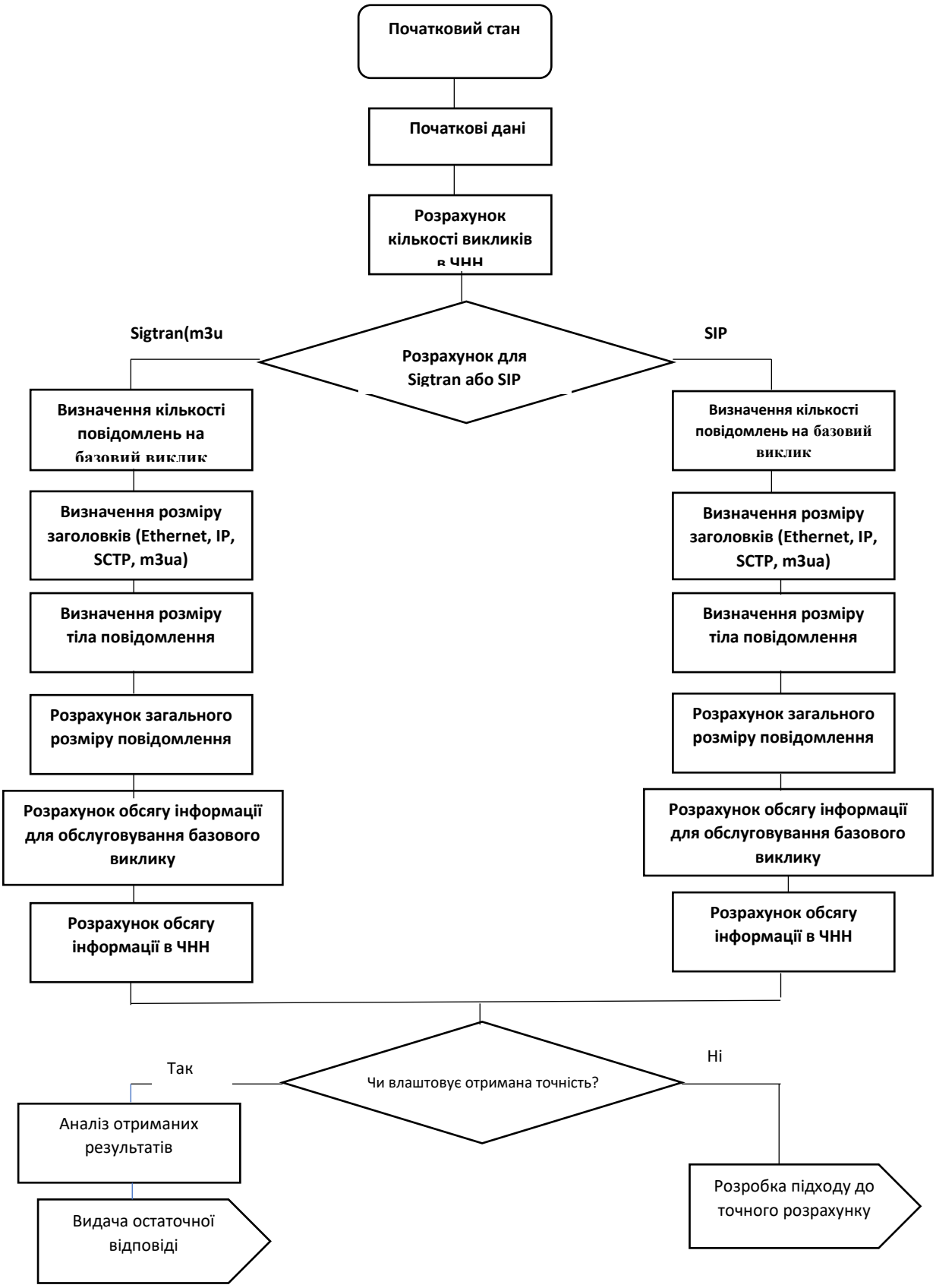


Рисунок 2.21 – SDL-діаграма порівняльного аналіза Sigtran(m3ua) – SIP

Задаємося наступними вихідними даними:

$N_{аб} = 480$ (кількість абонентів);

$K_{ЧНН} = 3$ виз/аб. (кількість викликів від одного абонента за годину);

Розраховуємо кількість викликів в ЧНН:

$$N_{ЧНН} = N_{аб} \cdot K_{ЧНН}$$

$$N_{ЧНН} = 480 \cdot 3 = 1440 \text{ выз.}$$

При цьому на кожен виклик доводиться по 5 повідомлень:

$$N_{сообщ\_ЧНН} = 1440 \cdot 5 = 7200 \text{ повідомлень /чнн}$$

$$N_{сообщ\_сек} = 7200 / 3600 = 2 \text{ повідомлень /с}$$

Розмір повідомлень розраховуємо виходячи з середнього »135 байт або 1080 біт.($N_{бит} = 1080 бит$)

Виходячи з вище розрахованих даних можна говорити про інтенсивність надходження.

$$\lambda = N_{сообщ\_сек} \cdot N_{\text{бит}} = 2 \cdot 1080 = 2160 \text{ біт/с}$$

Щоб порахувати пропускну здатність, необхідно задатися тимчасовими рамками, зокрема таймером Т1 = 0,5 с.

$$T = \frac{1/\lambda}{1-\rho}$$

$\rho = \lambda / \mu$ - коефіцієнт використання однолінійних систем.

Далі отримуємо:

$$\mu = \frac{\lambda^2 \cdot T}{1+\lambda},$$

$$\mu = \frac{2160^2 \cdot 0{,}5}{1+2160} = 1080 \text{ біт/с}$$

Для порівняння в SIP виходить:

$$N_{сообщ\_ЧНН} = 1440 \cdot 7 = 10080 \text{ повідомлень/чнн}$$

$$N_{сообщ\_сек} = 10080 / 3600 = 2{,}8 \text{ повідомлень/с}$$

$$N_{бит} = 4400 \, бит$$

$$\lambda = N_{сообщ\_сек} \cdot N_{\text{бит}} = 2{,}8 \cdot 4400 = 12320 \text{ біт/с}$$

$$\mu = \frac{12320^2 \cdot 0{,}5}{1+12320} = 6160 \text{ бит/с}$$

Дана пропускна здатність включає в себе тільки трафік сигналізації, без урахування мовного трафіку та інформації інших протоколів. Тому в якості підходу до точного розрахунку пропускної здатності каналу слід виділити наступні моменти:

· Слід привести доказ показового розподілу тривалості обслуговування;

· Для розрахунку загальної пропускної здатності каналу слід врахувати мовний трафік та трафік нижчих і рівнорівневих протоколів.

2.5 Алгоритм взаємодії NGN і ТфОП мереж при використанні Sigtran

Нижче представлені алгоритми взаємодії (ЗКС7 (ISUP) - Sigtran (ISUP)) - SIP.

Виклик з боку SIP

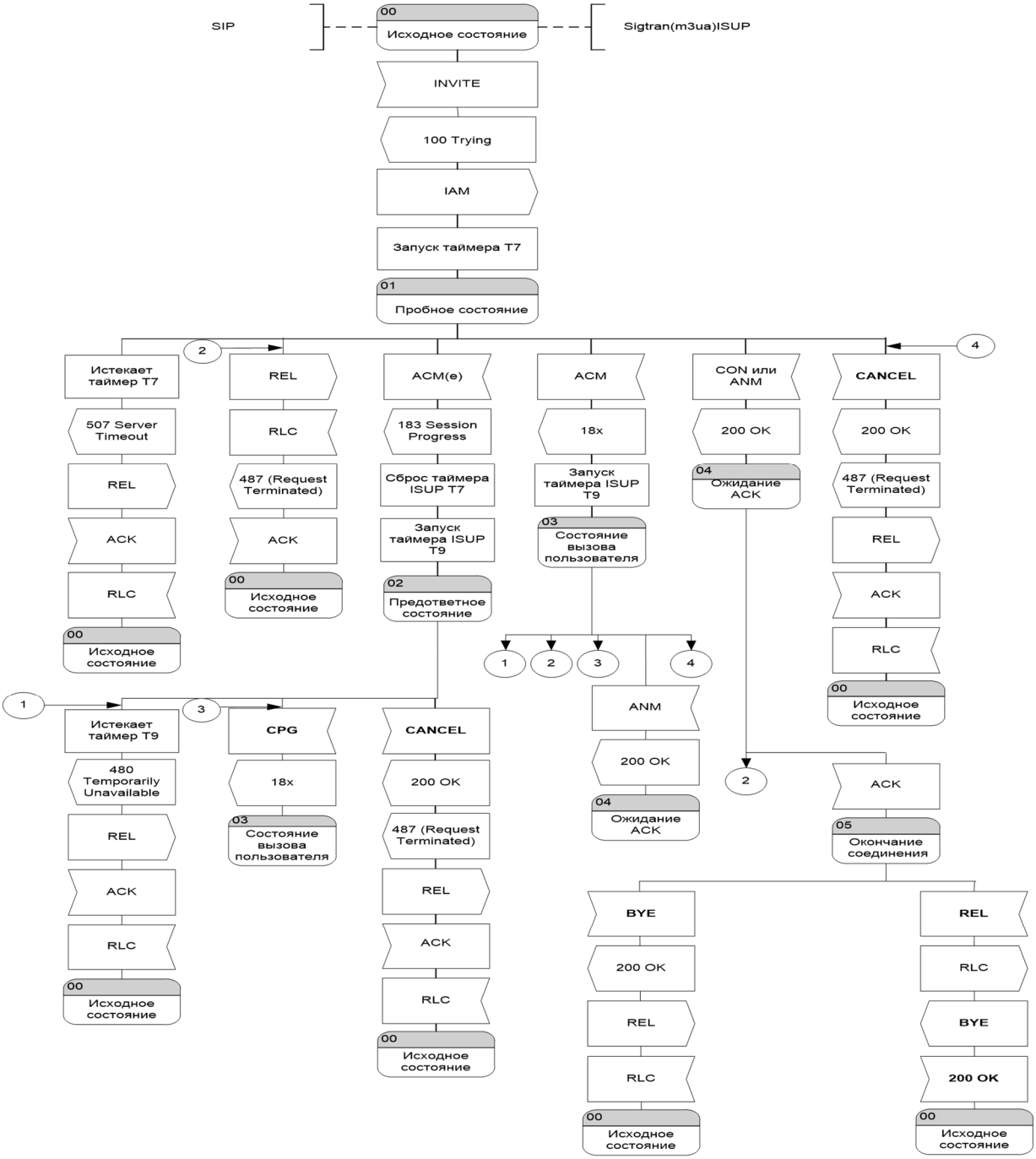


Рисунок 2.22 - SDL-діаграма взаємодії при надходженні виклику з боку SIP

Виклик з боку Sigtran (m3ua) ISUP

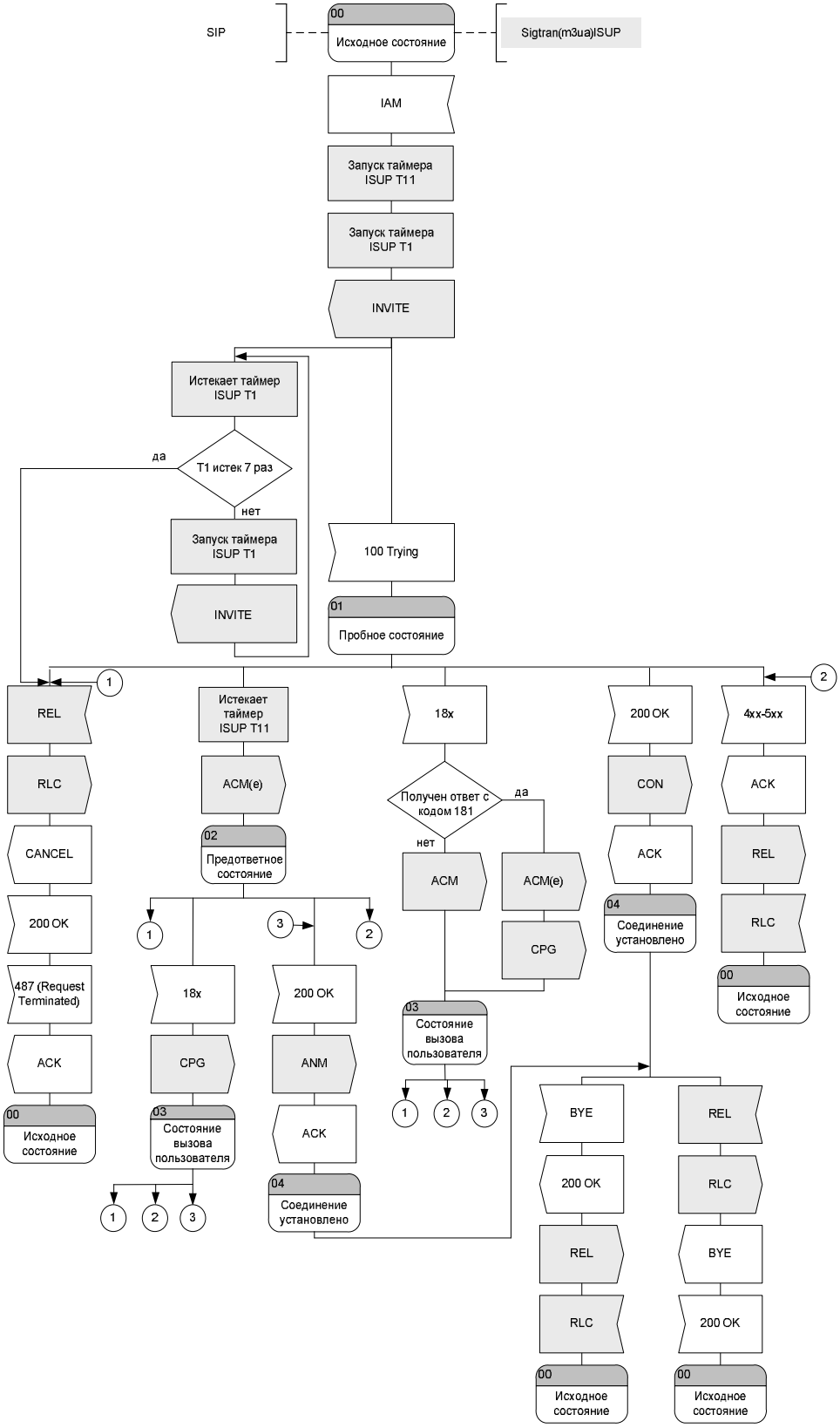


Рисунок 2.23 – SDL-діаграма взаємодії при надходженні виклику з боку мережі на базі ЗКС7

Алгоритми обміну іінформацією в т3иа

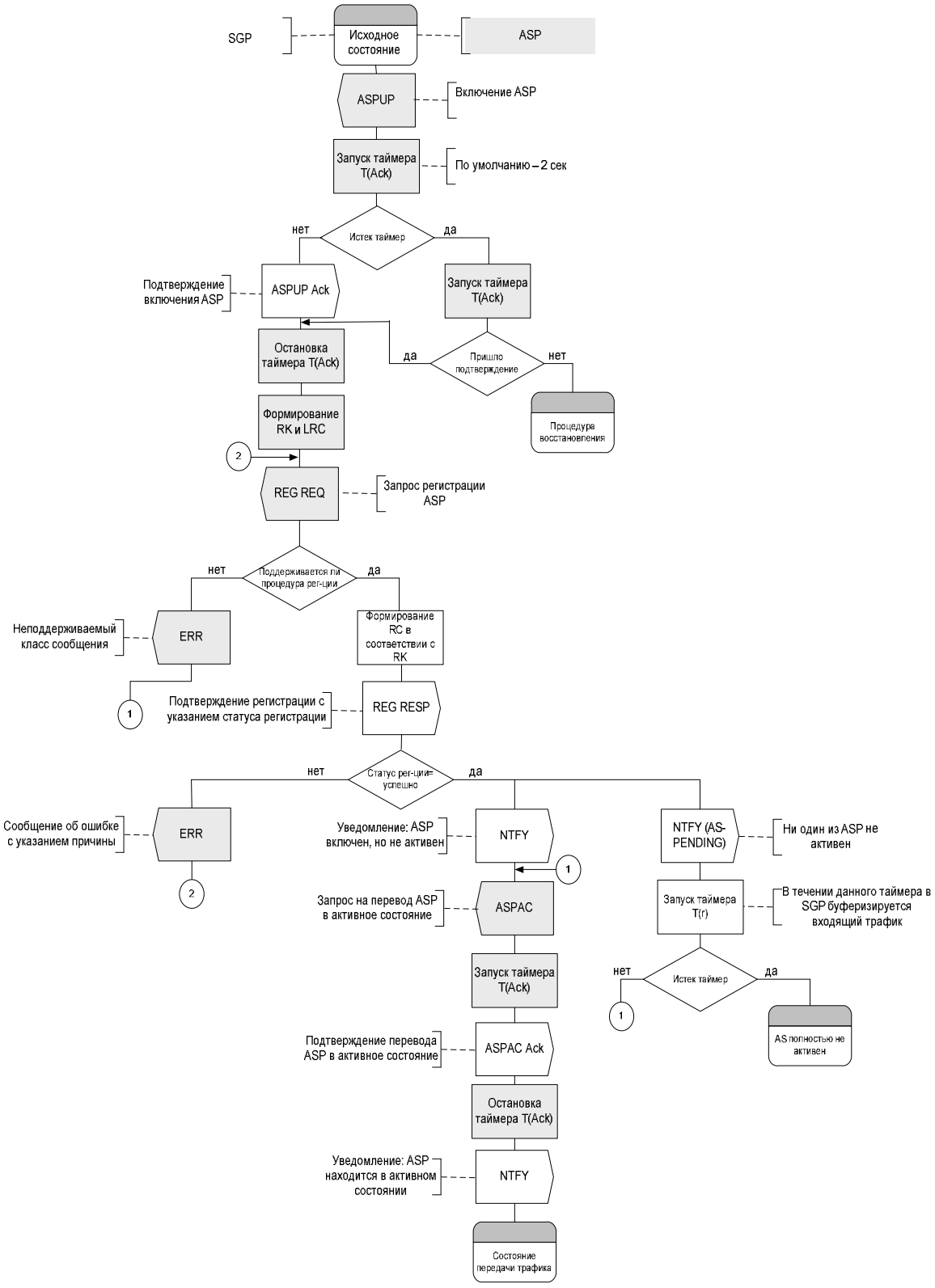


Рисунок 2.24 – SDL-діаграма включення ASP

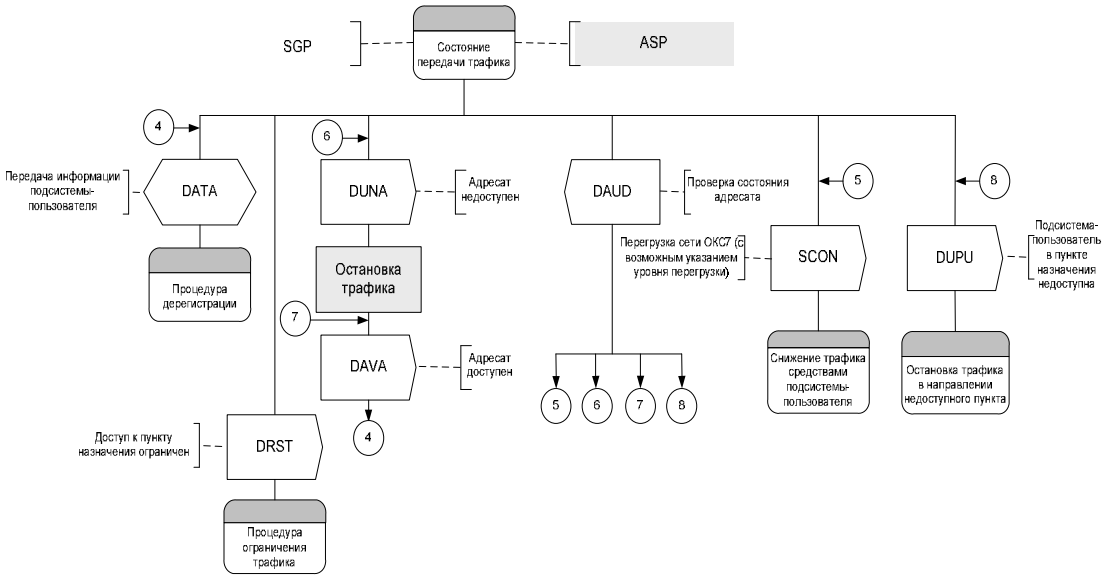


Рисунок 2.25 – SDL-діаграма обміну трафиком між ASP и SGP

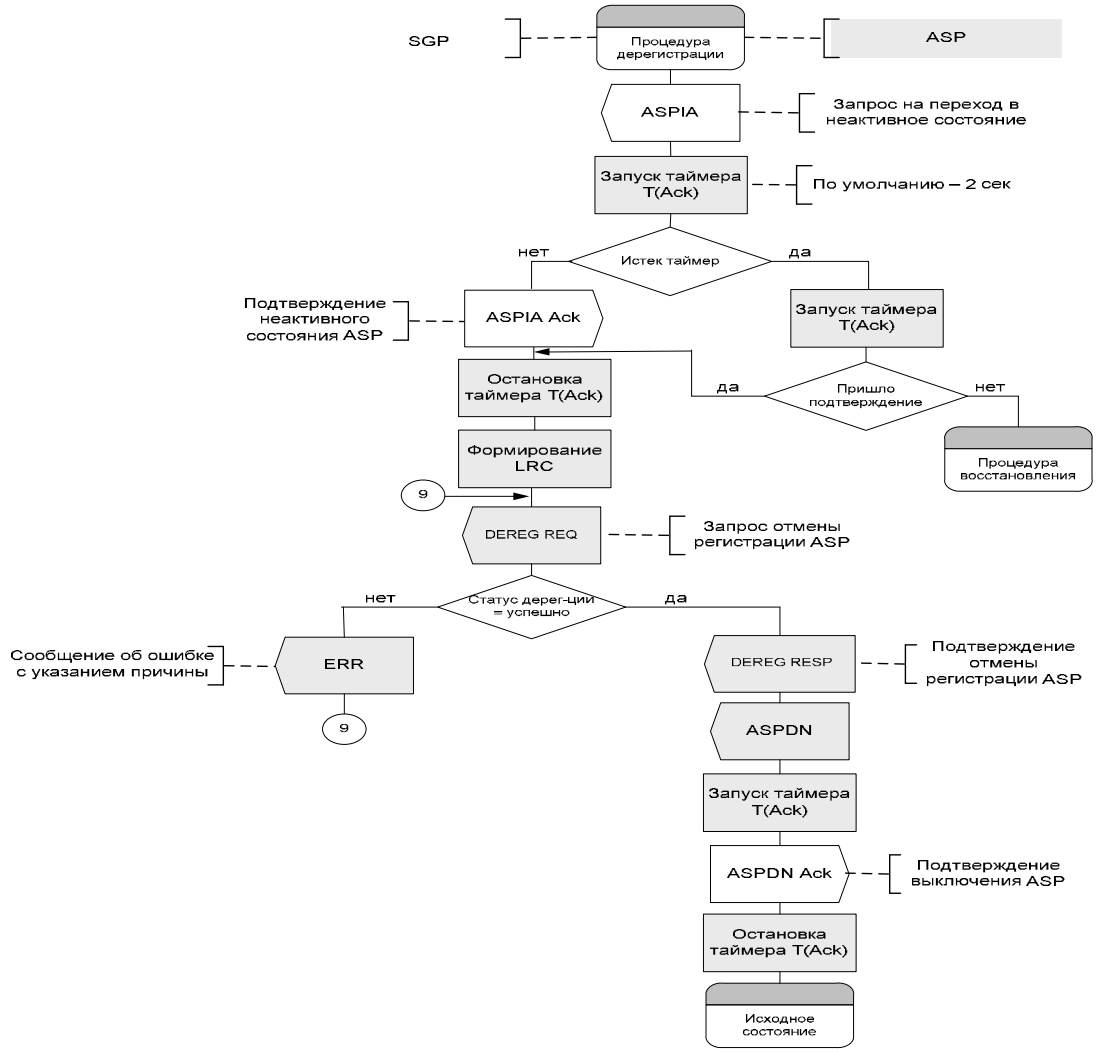


Рисунок 2.26 – SDL-діаграма виключення ASP

2.6 Висновки

У цій главі розроблений алгоритм обміну повідомленнями рівня адаптації m3ua. Дані алгоритми можуть бути застосовані на практиці для написання програмного забезпечення при реалізації m3ua, наприклад в сигнальному шлюзі SG або в SoftSwith.

3 ЕКОНОМІЧНА ЧАСТИНА

В даній дипломній роботі розроблені алгоритми обробки сигнальних повідомлень ЗКС7 в мережах NGN на базі технології SIGTRAN. У економічному розділі розраховуються одноразові капітальні витрати на їх розробку.

3.1.1 Визначення трудомісткості розробки алгоритмів

Трудомісткість створення моделі визначається тривалістю кожної робочої операції, починаючи зі складання технічного завдання й закінчуючи оформленням документації (за умови роботи одного проектувальника):

$$t = t_{mз} + t_{в} + t_{а} + t_{пр} + t_{опр} + t_{д} \text{ [год]}. \quad (3.1)$$

де $t_{mз}$ – тривалість складання технічного завдання на впровадження методу;

$t_{в}$ – тривалість вивчення технічного завдання (ТЗ) та літературних джерел за темою;

$t_{а}$ – тривалість розробки алгоритмів;

$t_{пр}$ – тривалість тестування віртуального аналога каналу зв'язку;

$t_{опр}$ – тривалість опрацювання здобутих характеристик;

$t_{д}$ – тривалість підготовки технічної документації.

Вихідні дані для визначення трудомісткості створення алгоритмів приведені в таблиці 3.1.

Таблиця 3.1 – Тривалість розробки алгоритмів

$tmз$, год	$tв$, год	$tа$, год	$tпр$, год	$tопр$, год	$tд$, год
45	48	69	19	19	29

Розрахуємо трудомісткість розробки алгоритмів за формулою (3.1):

$$t = 45+48+69+19+19+29=229 \text{ [год]}.$$

3.1.2 Розрахунок витрат на розробку алгоритмів

Витрати на розробку алгоритмів *Кпз* складаються з витрат на заробітну платню розробника *Ззп* і вартості витрат машинного часу, що необхідний для опрацювання алгоритмів мережі на ПК *Змч*:

$$К_{пз} = З_{зп} + З_{мч} \text{ [грн]} \quad (3.2)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальні потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) і визначається за формулою:

$$З_{зп} = t \cdot З_{пр} \text{ [грн]}. \quad (3.3)$$

де *t*– трудомісткість створення алгоритмів;

Зпр дорівнює 70 грн/год.

Розрахуємо заробітну платню проектувальника за формулою (3.3):

$$З_{зп} = 229 \cdot 70 = 16030{,}00 \text{ [грн]}.$$

Вартість машинного часу на ПК визначається за формулою:

$$\text{Змч} = \left(ta + tnp + tonp + td \right) \cdot \text{Смч [грн]}. \quad (3.4)$$

де $С_{мч}$– вартість 1 години машинного часу ПК, грн/година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = P_e \cdot t \cdot C_e + \frac{Ф_{перв} \cdot Н_a}{F_p} + \frac{К_{лпз} \cdot Н_{апз}}{F_p} \text{ [грн/год]}, \quad (3.5)$$

де *Ре* – встановлена потужність ПК;

t– трудомісткість створення моделі;

Се – енерговитрати;

Фперв – первісна вартість ПК на початок року;

На –річна норма амортизації на ПК;

Клпз – вартість ліцензійного програмного забезпечення;

Напз – річна норма амортизації на ліцензійне програмне забезпечення;

Fр –річний фонд робочого часу (за 40-годинного робочого тижня).

Енерговитрати розраховуються за формулою:

$$C_e = P_e \cdot C_{кВт} \text{ [грн/год]}, \quad (3.6)$$

де $C_{кВт}$ - тариф на електричну енергію.

Розрахунок витрат на розробку алгоритмів зводимо в таблицю 3.2

Таблиця 3.2 – Розрахунок витрат на розробку алгоритмів

Ре, кВт	$C_{кВт}$ кВт·год	*Фперв*, грн	*На*, частка одиниці	*Клпз*, грн	*Напз*, частка одиниці	*Fр*, год
1,4	1,60	20000	0,4	8100	0,4	1920

Тоді за формулою (3.6) отримаємо розмір енерговитрат:

$$Се = 1{,}4 \cdot 1{,}60 = 2/24 \text{ [грн/год]}.$$

Річна норма амортизації, якщо використовується метод прискорення зменшеної вартості, визначається за формулою:

$$\text{На} = \frac{2}{\text{Т}} \cdot 100\% \qquad (3.7)$$

де *Т* –строк корисного використання ПК, дорівнює 5 років.

Розрахуємо річну норму амортизації за формулою (3.7):

$$На = \frac{2}{5} \cdot 100\% = 40\% = 0{,}40 \text{ [частки одиниці]}.$$

Строк корисного використання ліцензійного програмування дорівнює 5 років.

Річна норма амортизації на ліцензійне програмне забезпечення визначається за формулою (3.7):

$$\text{Напз} = \frac{2}{5} \cdot 100\% = 40\% = 0{,}40 \text{ [частки одиниці]}.$$

Ліцензійне програмне забезпечення, яке використовується в даному випадку Microsoft Windows 7 Professional. Його вартість 8000 грн.

Вартість 1 години машинного часу ПК визначаються за формулою (3.5):

$$\text{Смч} = 1{,}4 \cdot 229 \cdot 1{,}60 + \frac{20000*0{,}40}{1920} + \frac{8100*0{,}40}{1920} = 518{,}82 \text{ [грн/год]}$$

Розрахуємо вартість машинного часу за формулою (3.4):

$$З_{мч}=(69+19+19+29)\cdot 518{,}82 = 70559{,}52 \text{ [грн]}.$$

Отже, підставивши отримані результати у формулу (3.2), отримаємо величину витрат на розробку алгоритмів:

$$К_{пз} = 16030+70559{,}52=86589{,}52 \text{ [грн]}.$$

3.1.3 Розрахунок капітальних витрат

Загальні капітальні витрати на розробку визначаються за формулою:

$$КЗ = Кпз + Кнавч + Кн \text{ [грн]}, \qquad (3.8)$$

де *Кнавч* - витрати на навчання технічних фахівців і обслуговуючого персоналу;

Кн - витрати на встановлення обладнання та налагодження системи.

Дані о витратах на розробку алгоритмів зводимо в таблицю 3.3.

Таблиця 3.3 – Витрати на розробку алгоритмів.

Кпз, грн	*Кнавч,* грн	*Кн,* грн
86589,52	5400	1300

Отже, капітальні витрати становлять:

$$КЗ =86589{,}52+5400+1300=93289{,}52 \text{ [грн]}.$$

3.2 Висновки

В економічному розділі було розраховано:

1. Трудомісткість розробки алгоритмів обробки сигнальних повідомлень ЗКС7 в мережах NGN на базі технології SIGTRAN – 229 год;
2. Заробітня платня проектувальника – 16030,00грн;
3. Витрати на розробку алгоритмів – 86589,52 грн;
4. Капітальні витрати на розробку алгоритмів – – 93289,52 грн.

ВИСНОВКИ

1. Виконано аналітичний огляд літератури по темі дипломної роботи, який дозволив сформулювати постановку задачі.

2. Розроблені алгоритми обробки сигнальних повідомлень ЗКС7 в мережах NGN на базі технології SIGTRAN.

3. Виконано порівняльний аналіз пропускної здатності каналу для базового виклику при використанні протоколу SIGTRAN (m3ua) та SIP.

4 Аналіз і розрахунки показали, що при використанні базового протоколу ISUP ЗКС7 і технології SIGTRAN (m3ua) для використання його в IP-мережах, отримуємо економію пропускної здатності в 6 разів.

ПЕРЕЛІК ПОСИЛАНЬ

1 Лубенская, С. Н. Сети NGN. Текущее состояние и перспективные пути оптимизации трафика в сетях доступа / С. Н. Лубенская. — Текст : непосредственный, электронный // Молодой ученый. — 2015. — № 23 (103). — С. 177-180. — URL: https://moluch.ru/archive/103/23570/

2 Бочаров П. П. Вишневский В. М. G-сети: развитие теории мультипликативных сетей.// Автоматика и телемеханика, 2003.

3 Гольдштейн Б.С. Стек протоколов ОКС7. Подсистема МТР. М.: Радио и связь, 2003.

4 Сети следующего поколения NGN. Под ред. А.В.Рослякова. – М.: Эко-Трендз, 2008. – 424 с.

5 Б.С. Гольдштейн. Программные коммутаторы Softswitch вчера, сегодня и… «Технология средств связи. № 2, 2005.

6 Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) - User Adaptation Layer (M3UA). Open SS7 Corporation. 2014.

ДОДАТОК А. Відомість матеріалів дипломної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат		
2	А4	Список умовних скорочень		
	А4	Зміст		
4	А4	Вступ		
5	А4	Стан питання. Постановка задачі		
6	А4	Спеціальна частина		
7	А4	Економічний розділ		
8	А4	Висновки		
9	А4	Перелік посилань		
10	А4	Додаток А		
11	А4	Додаток Б		
12	А4	Додаток В		
12		Матеріали дипломного проекту на оптичному носії		Оптичний диск

ДОДАТОК Б. Відгук керівника економічного розділу

Керівник розділу _____ Романюк Н.М.

(підпис) (прізвище, ініціали)

ДОДАТОК В Відгук керівника дипломної роботи

ВІДГУК
на дипломну роботу

Студента(ки) _____ гр.
(прізвище, ім'я)

на тему: _____

_____

Актуальність теми _____

_____

_____

Повнота розкриття теми _____

_____

_____

_____

Теоретичний рівень _____

_____

_____

Практична значущість _____

_____

_____

Самостійність виконання роботи _____

_____

_____

_____

Якість оформлення, загальна та спеціальна грамотність _____

_____

_____

Переваги та недоліки роботи _____

_____

_____

_____

Загальна оцінка роботи та висновок щодо рекомендації до захисту в ДЕК

Науковий керівник

к.ф.-м.н., професор		Гусєв О.Ю.
(посада)	**(підпис)**	**(ініціали, прізвище)**

«____»_____2020 р.