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

Інститут електроенергетики
(інститут)
факультет інформаційних технологій
(факультет)
Кафедра безпеки інформації та телекомунікацій
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи ступеня магістра
(бакалавра, спеціаліста, магістра)

Студента Проценко Кирило Віталійовича
(ПІБ)
академічної групи 172м-21-1
(шифр)
спеціальності 172 «*Телекомунікації та радіотехніка*»
(код і назва спеціальності)
за освітньо-професійною програмою
Телекомунікації та радіотехніка

(офіційна назва)

на тему **Вдосконалення системи тестування платформи потокового мовлення на основі мікросервісної архітектури**

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	Доц..Магро. В. І			
розділів:				
Спеціальний	к.ф.-м.н.,доц, каф. БІТ Горєв В. М.			
Економічний	Доц. Романюк Н.М			

Рецензент	доц. Хом'як Т.В			

Нормоконтролер	Проф. Гусєв. О.Ю			

ДНІПРО
2022

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
д.т.н., проф. Корнієнко В.І.
«_____»__грудня_____2022року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра

студенту _____Проценко К.В._____ **академічної групи** _____172м-21-1____
(прізвище та ініціали) (шифр)

спеціальності _____*172 Телекомунікації та радіотехніка*

за освітньою-професійною програмою *Телекомунікації та радіотехніка*

на тему_____**Вдосконалення системи тестування платформи потокового мовлення на основі мікросервісної архітектури**

затверджену наказом ректора НТУ «Дніпровська політехніка» від 31.10.2022. № 1200-с

Розділ	**Зміст**	**Термін виконання**
Розділ 1	Проаналізувати типи реалізації системи тестування та моніторингу	01.11.22-07.11.2
Розділ 2	Виконати аналіз технічної реалізації та принципу роботи розробленої мультисервісної системи та її компонентів	08.11.22-28.11.22
Розділ 3	Провести розрахунок вартості розробки системи тестування потокового мовлення на основі мікросервісної архітектури та очікуваний час розробки цієї системи	29.11.22-07.12.22

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі _____

Дата подання до екзаменаційної комісії ___11.12.2022р._____

Прийнято до виконання _____ _____Проценко К.В____
(підпис студента) (прізвище, ініціали)

ДНІПРО
2022

РЕФЕРАТ

Пояснювальна записка: 86 с., 26 рис., 3 табл., 4 додаток, 10 джерел.

Об'єктом дослідження є процеси, що забезпечують підвищення завадозахищеності телекомунікаційних систем з багатопозиційними сигналами.

Предметом дослідження є методики та засоби підвищення завадозахищеності телекомунікаційних систем з багатопозиційними сигналами.

Метою роботи є підвищення завадозахищеності ТКС з багатопозиційними сигналами.

Методи дослідження: методи статистичної радіотехніки, теорії ймовірності, математичного моделювання.

В першому розділі кваліфікаційної роботи наведено аналіз с типів реалізацій систем тестування та моніторингу

В спеціальній частині визначено вплив видів модуляції сигналу на енергетику радіолінії. Досліджено транспортну, городську та сільску мультісервісні системи і наведено Принципи використання коммутаторів Softswitch для створення мультисервісних мереж

В економічній частині проведено розрахунок вартості розробки удосконаленого методу обробки сигналів та очікуваний час розробки методу.

Технічним результатом отриманим в кваліфікаційній роботі є дослідження використання ФМ-4 сигналу, який суттєво зменшує необхідну потужність передавачі порівняно з іншими методами модуляції.

ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА, ЗАВАДОЗАХИЩЕНІСТЬ, БАГАТОПОЗИЦІЙНИЙ СИГНАЛ, СИГНАЛЬНА КОНСТРУКЦІЯ, АМПЛІТУДНОМОДУЛЬОВАНИЙ СИГНАЛ.

ДНІПРО
2022

ABSTRACT

Explanatory note: 86 pp., 26 fig., 3 tab., 4 appendix, 10 sources.

The object of research is the processes that provide increased noise immunity of telecommunication systems with multi-position signals.

The subject of the research is methods and means of increasing the noise immunity of telecommunication systems with multi-position signals.

The aim of the work is to increase the noise immunity of TCS with multi-position signals.

Research methods: methods of statistical radio engineering, probability theory, mathematical modeling.

The first section of the qualification work provides an analysis of the types of implementations of testing and monitoring systems

In a special part, the influence of types of signal modulation on the energy of the radio line is defined. Transport, urban and rural multi-service systems are studied and the principles of using Softswitches for creating multi-service networks are given

In the economic part, the cost of developing an improved signal processing method and the expected development time of the method were calculated.

The technical result obtained in the qualification work is to study the use of the FM-4 signal, which significantly reduces the necessary transmitter power compared to other modulation methods.

TELECOMMUNICATION SYSTEMS, INTERFERENCE PROTECTION, MULTI-POSITION SIGNAL, SIGNAL STRUCTURES, AMPLITUDE MODULATED SIGNAL.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

3GPP – (3rd Generation Partnership Project) партнерська асоціація груп телекомунікаційних компаній;

DMPSK – відносна багатофазова модуляція;

DVB – (Digital Video Broadcasting) сімейство міжнародних відкритих стандартів цифрового телебачення;

LTE – (Long Term Evolution) назва мобільного протоколу передавання даних;

MIMO – (Multiple Input Multiple Output) метод просторового кодування сигналу;

MPEG – (Moving Picture Experts Group) міжнародний стандарт, що використовується переважно для зшивання цифрового аудіо та відео;

SDN – (Software-defined Networking) програмно-конфігурована мережа;

UMTS – (Universal Mobile Telecommunications System) технологія стільникового зв'язку;

VSB – (Vestigial Side Band) технологія цифрового телебачення з частково пригніченою бічною смугою;

WI-FI – (Wireless Fidelity) назва для стандарту IEEE 802.11 передачі цифрових потоків даних по радіоканалах;

АМ (ASK) – амплітудна модуляція;

ЗММ – значущий момент модуляції;

ІКМ – імпульсно-кодова модуляція;

КАМ – (QAM, Quadrature Amplitude Modulation) квадратурно-амплітудна модуляція;

ТКС – телекомунікаційна система;

ТСК – таймерні сигнальні конструкції;

ФМ (PSK) – фазова модуляція;

ЧМ (FSK) – частотна модуляція.

Зміст

ВСТУП 7

1. Проаналізувати типи реалізації системи тестування та моніторингу 8

1.1. Типи реалізації системи тестування 8

1.2. Системне тестування, приймально-здавальні та сертифікаційні випробування при розробці сертифицируемого програмного забезпечення 14

1.3 Інтеграційне тестування 20

1.3.1. Завдання і цілі інтеграційного тестування 21

1.4. Фундаментальний процес тестування 24

1.4.1. Планування та управління 25

1.4.2 Аналіз та проектування 26

1.4.3 Впровадження та реалізація 26

1.4.4 Оцінка критеріїв виходу і написання звітів 26

1.4.5 Дії після завершення тестування 27

1.5. Конфігураційне тестування 27

1.6 Тестування надійності і відновлення після збоїв 28

1.7. Системи моніторінгу та управління безпекою 37

2. Виконати аналіз технічної реалізації та принципу роботи розробленої мультисервісної системи та її компонентів 38

2.1. Архітектура мультисервісних мереж передачі даних 38

2.1.1. Інфраструктура 41

2.2. Принципу роботи розробленої мультисервісної системи 53

2.2.1. Транспортні мережі в містах 53

2.2.2. Транспортні мережі в сільскій місцевості 55

2.2.3. Загальні тенденції розвитку місцевих транспортних мереж 57

2.3. Принципи модернізації місцевих телекоммунікаційних мереж 58

2.3.1 Городські телефоні мережі 61

2.3.1. Інтернет (Аспекти доступу) 68

2.4 Принципи використання коммутаторів Softswitch для створення мультисервісних мереж 69

2.4.1 Системи сигналізації в NGN 71

2.4.2 Рекомендації щодо переходу до NGN 72

ВСТУП

Принцип максимально ефективного використання ресурсів мереж зв'язку має на увазі можливість якісної і кількісної адаптації продуктивності, найбільш повне використання всіх ресурсів і сервісів, надійність, доступність, безпеку. Основними характеристиками телекомунікаційної системи (ТКС), які в різній формі враховуються при розрахунку і проектуванні мережевих структур, є помилка приймання сигналу та пропускна здатність системи. Помилка приймання сигналу повністю визначається відношенням сигнал/шум на вході вирішуючого пристрою.

Ефективним методом підвищення пропускної здатності ТКС є використання багатопозиційних сигналів. Однак при цьому погіршується відношення сигнал/шум і відповідно збільшується помилка приймання сигналу. Впродовж останніх десятиліть вчені займаються дослідженням завадозахищеності телекомунікаційних систем при різних методах модуляції та кодуванні сигналу. Аналіз науково-технічної літератури показує, що проблемі забезпечення завадозахищеності ТКС та мереж присвячено цілий ряд наукових досліджень вітчизняних та закордонних вчених: Б. Скляр, Іпатов В.П., В. Столінгс, Беркман Л.Н., Захарченко М.В., Гепко І.О., Климаш М.М. та інші. Однак, в їх роботах недостатньо повно розглянута можливість підвищення завадозахищеності телекомунікаційних систем з багатопозиційними сигналами.

Актуальність обраної теми кваліфікаційної роботи підтверджується необхідністю дослідження та розробки методик підвищення завадозахищеності ТКС з багатопозиційними сигналами.

Зазначене вище й зумовило вибір теми кваліфікаційної роботи, її мету та завдання для кваліфікаційної роботи.

1. Проаналізувати типи реалізації системи тестування та моніторингу

1.1. Типи реалізації системи тестування

По завершенню інтеграційного тестування всі модулі системи узгоджені за інтерфейсами та функціональністю. Починаючи з цього моменту, можна переходити до тестування системи в цілому як єдиного об'єкта тестування – до системного тестування. На рівні інтеграційного тестування тестувальника цікавили переважно структурні аспекти системи, лише на рівні системного тестування цікавлять поведінкові аспекти системи. Як правило, для системного тестування застосовується підхід чорного ящика, при цьому як вхідні та вихідні дані використовуються реальні дані, з якими працює система, або подібні їм дані.

Системне тестування – один із найскладніших видів тестування. На цьому етапі проводиться не лише функціональне тестування, а й оцінка характеристик якості системи – її стійкості, надійності, безпеки та продуктивності. На цьому етапі виявляється багато проблем зовнішніх інтерфейсів системи, пов'язані з неправильною взаємодією з іншими системами, апаратним забезпеченням, неправильним розподілом пам'яті, відсутністю коректного звільнення ресурсів і т.п.

Після завершення системного тестування розробка переходить у фазу приймально-здавальних випробувань (для програмних систем, що розробляються на замовлення) або у фазу альфа- та бета-тестування (для програмних систем загального застосування).

Оскільки системне тестування – процес, потребує значних ресурсів, щодо його проведення часто виділяють окремий колектив тестувальників, а часто системне тестування виконується організацією, не що з колективом розробників і тестувальників, виконували роботи на попередніх етапах тестування. При цьому необхідно відзначити, що при розробці деяких типів програмного забезпечення (наприклад авіаційного бортового) вимога незалежного тестування на всіх етапах розробки обов'язково.

Системне тестування проводиться у кілька фаз, кожної з яких перевіряється одне із аспектів поведінки системи, тобто. проводиться один із типів системного тестування. Усі ці фази можуть протікати одночасно чи послідовно. Наступний розділ присвячений розгляду особливостей кожного із типів системного тестування на кожній фазі.

Види системного тестування

Прийнято виділяти такі види системного тестування:

- Функціональне тестування;
- Тестування продуктивності;
- Навантажувальний або стресове тестування;
- Тестування конфігурації;
- *Тестування безпеки*;
- Тестування надійності і відновлення після збоїв;
- *Тестування зручності використання*.

У ході системного тестування виробляються далеко не всі з перерахованих видів тестування – конкретний їх набір залежить від системи, що тестується.

Вихідною інформацією щодо перелічених видів тестування є два класу вимог: функціональні і нефункциональные. Функціональні вимоги явно описують, що система повинна робити і які перетворення вхідних значень у вихідні. Нефункціональні вимоги визначають властивості системи, які безпосередньо не пов'язані з її функціональністю. Прикладом таких властивостей може бути час відгуку на запит користувача (наприклад, не більше 2 секунд), час безперебійної роботи (наприклад, не менше 10000 годин між двома збоями), кількість помилок, що допускаються початківцем за перший тиждень роботи (не більше 100), і т.п.

Розглянемо кожен вид тестування докладніше:

Функціональне випробування. Даний вид тестування призначений для доказу того, що вся система загалом поводиться відповідно до очікувань користувача, формалізованими у вигляді системних вимог. Під час цього виду тестування перевіряються всі функції системи з погляду її користувачів (як користувачів-людей, і "користувачів" – інших програмних систем). Система при функціональному тестуванні розглядається як чорна скринька, тому в даному випадку корисно використовувати класи. еквівалентності.Критерієм повноти тестування в даному випадку буде

повнота покриття тестами системних функціональних вимог (або системних тест-вимог) і повнота тестування класів еквівалентності, а саме:

- Всі функціональні вимоги повинні бути протестован ;
- Всі класи допустимих вхідних даних повинні коректно оброблятися системою;
- Всі класи неприпустимих вхідних даних повинні бути відкинуті системою, при цьому не повинна порушуватися стабільність її роботи;
- В тестових прикладах повинні генеруватися всі можливі класи вихідних даних системи;
- Під час тестування система повинна побувати у всіх своїх внутрішніх станах, пройшовши при цьому по всіх можливих переходах між станами.

Результати системного тестування протоколюються і аналізуються абсолютно аналогічно тому, як це робиться для модульного та інтеграційного тестування. Основна складність тут полягає в локалізації дефектів у програмному коді системи та визначенні залежностей одних дефектів від інших (ефект "парного числа помилок").

Тестування продуктивності. Даний вид тестування спрямовано визначення того, що система забезпечує належний рівень продуктивності при обробці запитів користувача. Тестування продуктивності виконується за різних рівнів навантаження на систему, різних конфігураціях устаткування. Виділяють три основні фактори, що впливають на продуктивність системи: кількість підтримуваних системою потоків (наприклад, сесій користувачів), кількість вільних системних ресурсів, кількість вільних апаратних ресурсів.

Тестування продуктивності дозволяє виявляти вузькі місця у системі, які у умовах підвищеного навантаження чи відсутності системних ресурсів. В цьому випадку за результатами тестування проводиться доопрацювання системи, змінюються алгоритми виділення та розподілу ресурсів системи.

Всі вимоги, що пред'являються до продуктивності системи, повинні бути чітко визначені і обов'язково повинні включати числові оцінки параметрів продуктивності. Тобто, наприклад, вимога "Система повинна мати прийнятний час відгуку на запит користувача" непридатна для тестування. Навпаки, вимога "Час відгуку на запит користувача не повинен перевищувати 2 секунд" може бути протестована.

Те саме стосується і результатів тестування продуктивності. У звітах з цього виду тестування зберігаються такі показники як завантаження апаратного та системного програмного забезпечення (кількість циклів процесора, виділеної пам'яті, кількість вільних системних ресурсів тощо). Також важливі швидкісні характеристики системи (кількість оброблених в одиницю години запитів, часові інтервали між початком обробки кожного наступного запиту, рівномірність години відкликання в різні моменти години і т.п.).

Для проведення тестування продуктивності потрібна наявність генератора запитів, що подає на вхід системи потік даних, типових для сеансу роботи з нею. Тестове оточення повинне включати в себе крім програмної компоненти ще й апаратну, причому на такому тестовому стенді має існувати можливість моделювання різного рівня доступних ресурсів

Стресове тестування. Стресове тестування має багато спільного з тестуванням продуктивності, проте його основне завдання – не визначити продуктивність системи, а оцінити продуктивність та стійкість системи у разі, коли для своєї роботи вона виділяє максимальну кількість ресурсів або коли вона працює в умовах критичної нестачі. Основна мета стресового тестування – вивести систему озброєння, визначити умови, за яких вона зможе далі нормально функціонувати. Для проведення стресового тестування використовуються самі інструменти, що й для тестування продуктивності. Однак, наприклад, генератор навантаження при стресовому тестуванні повинен генерувати запити користувачів з максимально можливою швидкістю або генерувати дані запитів таким чином, щоб вони були максимально можливими за обсягом обробки.

Стресове тестування дуже важливе при тестуванні web-систем та систем з відкритим доступом, рівень навантаження на які дуже складно прогнозувати.

Тестування конфігурації. Більшість програмних систем масового призначення призначені для використання на різному устаткуванні. Незважаючи на те, що в даний час особливості реалізації периферійних пристроїв ховаються драйверами операційних систем, що мають уніфікований з точки зору прикладних систем інтерфейс, проблеми сумісності (програмної, так і апаратної) все одно існують.

При тестуванні конфігурації перевіряється, що програмна система правильно працює по всьому підтримуваному апаратному забезпеченні разом із іншими програмними системами. Необхідно також перевіряти, що система продовжує стабільно працювати при гарячій заміні будь-якого підтримуваного пристрою аналогічним. При цьому система не винна давати

збоїв ні в момент заміни пристрою, ні після початку роботи з новим пристроєм.

Також необхідно перевіряти, що система коректно обробляє проблеми, що виникають в обладнанні, як штатні (наприклад, сигнал кінця паперу в принтері), так і позаштатні (збій харчування).

Тестування безпеки. Якщо програмна система призначена для зберігання або обробки даних, вміст яких є таємницею певного роду (особисту, комерційну, державну тощо), то властивостям системи, що забезпечує збереження цієї таємниці, будуть пред'являтися підвищені вимоги. Ці вимоги мають бути перевірені під час тестування системи безпеки. У ході цього тестування перевіряється, що інформація не втрачається, не пошкоджується, її неможливо підмінити, а також до неї неможливо отримати несанкціонований доступ, у тому числі за допомогою вразливостей у програмній системі.

У вітчизняній практиці прийнято проводити сертифікацію програмних систем, призначених для зберігання даних для службового користування, секретних, таємних і таємних особливої важливості. Існує ряд вітчизняних стандартів Федеральної служби з технічного та експортного контролю (ФСТЭК), що регламентують властивості програмних систем із забезпечення необхідного рівня безпеки та відсутність недокументованих можливостей ("закладок"), які можуть бути використані зловмисником для несанкціонованого доступу до даних. Крім того, існує міжнародний стандарт Common Criteria, що також регламентує питання захисту інформації в програмних системах.

Незважаючи на те, що сертифікація – процес, який слідує за верифікацією, вимоги цих стандартів можуть бути використані і під час тестування системи. Так, стандарт ФСТЭК, традиційно скорочено званий РД СВТ, виділяє такі групи властивостей програмної системи, що підлягають перевірці (деякі групи властивостей укрупнені для скорочення списку):

- розмежування і контроль доступу - запобігання доступу до "чужої" інформації;
- очищення та захист пам'яті - запобігання доступу до залишкової інформації після
- видалення об'єктів з пам'яті;
- маркування і захист інформації, переданої у зовнішній світ - збереження рівня

- секретності навіть поза системою;
- ідентифікація та аутентифікація - надання доступу тільки санкціонованим
- користувачам і відмова в доступі всім іншим;
- реєстрація (аудит подій) - реєстрація в спеціальному журналі всіх подій системи,
- пов'язаних з безпекою для подальшого аналізу;
- гарантії проектування та архітектури - система повинна бути спроектована таким чином, щоб гарантувати захищеність інформації з певним рівнем впевненості;
  тестування - всі функції щодо забезпечення безпеки повинні бути протестовані у всіх режимах;
- цілісність і відновлення засобів захисту - система повинна мати засоби контролю коректності всіх правил розмежування доступу та системи безпеки в цілому, а також засоби їх відновлення при збої;
- документація розробника, адміністратора і користувача - всі засоби системи із забезпечення безпеки повинні бути описані у відповідних посібниках.

При розробці та верифікації програмної системи, яка буде піддаватися подальшої сертифікації, роботи з сертифікації повинні включати в себе перевірку всіх перерахованих властивостей.

Тестування надійності та відновлення після збоїв . Для коректної роботи системи в будь-якій ситуації необхідно переконатися, що вона відновлює свою функціональність і продовжує коректно працювати після будь-якої проблеми, що перервала її 7 роботу. , викликані зовнішніми факторами При аналізі поведінки системи в цьому випадку необхідно звертати увагу на два фактори - мінімізацію втрат даних в результаті збою та мінімізацію часу між збоєм та продовженням нормального функціонування системи

Тестування зручності використання. Окрема група нефункціональних вимог - вимоги до зручності використання

користувальницького інтерфейсу системи. Цей вид тестування буде розглянуто в наступній лекції.

В результаті виконання всіх розглянутих вище видів тестування робиться висновок про функціональність і властивостях системи, після чого вузькі місця системи допрацьовуються до реалізації необхідної функціональності або до досягнення системою необхідних

1.2. Системне тестування, приймально-здавальні та сертифікаційні випробування при розробці сертифицируемого програмного забезпечення

При розробці масового ("коробкового", COTS) програмного забезпечення після проведення системного тестування система проходить етапи альфа-і бета-тестування, під час якого роботу системи перевіряють потенційні користувачі (або спеціально виділені фокус-групи користувачів, або всі бажаючі). На цьому етапі в програмну систему вносяться останні незначні зміни, які не впливають на суть системи. Після завершення цієї стадії система надходить у продаж кінцевим користувачам.

При розробці програмного забезпечення на фазу альфа-і бета-тестування замінюють приймально-здавальні випробування. Під час цих випробувань замовник засвідчується, що система працює відповідно до його потреб (як зафіксованими в технічному завданні на систему, так і не зафіксованими). Замовник може проводити такі випробування самостійно, виконуючи заздалегідь підготовлені тести системи, або проводити їх спільно з представниками колективу розробників. У цьому випадку тестові приклади також готуються розробниками, наприклад, на основі тестових прикладів, що використовувалися на етапі системного тестування

Завершуються приймально-здавальні випробування або підписанням акта приймання, або видачею замовником додаткових вимог до системи, які повинні бути виправлені до приймання системи. Після усунення всіх недоліків системи приймальноздавальні випробування повторюються (можливо, за скороченою програмою). Після успішного підписання акта система надходить в експлуатацію замовнику.

Існує спеціальний вид програмних систем, до властивостей яких пред'являються особливі вимогами. Прикладом таких систем можуть служити бортові авіаційні програмні системи, для яких особлива увага приділяється питанням безпеки, надійності та відмовостійкості. Незважаючи на те, що більша частина таких систем може бути віднесена до категорії замовленого програмного забезпечення, для отримання дозволу на установку системи на борт потрібне отримання сертифіката на льотну придатність.

Таким чином, після проведення системного тестування та приймально-здавальних випробувань проводяться сертифікаційні випробування. *Сертифікація* програмного забезпечення - процес встановлення і офіційного визнання того, що розробка ПОпроводилася відповідно до певних вимог. У процесі сертифікації відбувається взаємодія заявника, органа, що сертифікує і наглядового органу.

Заявник - це організація, що подає заявку у відповідний сертифікуючий орган на отримання сертифіката (відповідності, якості, придатності і т.п.) вироби.

Сертифікуючий орган - організація, яка розглядає заявку заявника про проведення сертифікації ПО і або самостійно, або шляхом формування спеціальної комісії проводить набір процедур, спрямованих на проведення процесу сертифікації ПО заявника.

Наглядова орган - комісія фахівців, що спостерігають за процесами розробки заявником сертифікується інформаційної системи і дають висновок про відповідність даного процесу певним вимогам, яке передається на розгляд до сертифікуючий орган.

Основний *об'єкт* перевірки в ході сертифікаційних випробувань - чи задовольняє процес розробки програмної системи регламентом і рекомендаціям стандарту, на відповідність якому проводиться сертифікація. Така відповідність визначається за допомогою аналізу життєвого циклу сертифікується системи та документів, що створюються на ключових його етапах. Весь процес аналізу й ті властивості системи, які піддаються сертифікації, описується в плані сертифікаційних випробувань, який затверджується спільно заявником та сертифікуючим органом.

У разі сертифікації бортової системи за стандартом DO-178B (або його аналогам КТ-178, JB-12 і т.п.) план додатково визначає рівень впливу відмови програмної системи на безпеку польоту (рівень отказобезопасность) за яким буде проводитися *сертифікація*. Будь-які питання, які виникають у сертифікує органу щодо змісту плану сертифікаційних випробувань, повинні бути дозволені до початку самих випробувань.

Згідно вимог DO-178B план сертифікаційних випробувань (план програмних аспектів сертифікації) повинен включати:

Огляд системи. Цей розділ описує систему, включаючи опис її функцій та їх розміщення в програмне і апаратне забезпечення, її архітектуру, використовуваний процесор (процесори), апаратно-програмний інтерфейс, і особливості отказобезопасность;

Огляд програмного забезпечення. Цей розділ коротко описує функції програмного забезпечення з акцентом на концепцію забезпечення отказобезопасность і поділу на відокремлені частини, наприклад, розподіл ресурсів, резервування, несиметрично резервувати програмне забезпечення, стійкість до відмов, стратегії таймування і діспетчерізірованія;

Сертифікаційні міркування. Цей розділ містить зведення сертифікаційного базису, включаючи засоби підтвердження відповідності, як це визначається програмними аспектами сертифікації. У цьому розділі також заявляється запропонований рівень (рівні) програмного забезпечення та наводяться підтвердження правильності цього рівня, отримані в процесі оцінки отказобезопасность системи, включаючи потенційний внесок програмного забезпечення в відмовні ситуації;

Життєвий цикл програмного забезпечення. Цей розділ визначає життєвий цикл програмного забезпечення, який буде використовуватися, а також включає зведення його процесів, детальна інформація про яких визначається у відповідних планах програмного забезпечення. У зведенні роз'яснюється, як будуть задовольнятися цілі кожного процесу життєвого циклу, вказуються залучаємо організації, організаційна відповідальність, а також відповідальність за процеси життєвого циклу системи та за процес підтримки контактів в ході сертифікації;

Дані життєвого циклу програмного забезпечення. Цей розділ визначає дані життєвого циклу, які будуть випущені і контролюватимуться в процесах життєвого циклу програмного забезпечення. Цей розділ також описує взаємозв'язок даних між собою або з іншими даними, що визначають систему, дані життєвого циклу програмного забезпечення, що подаються сертифікуючим владі, форму даних і засоби, за допомогою яких дані життєвого циклу програмного забезпечення можуть бути зроблені доступними для сертифікуючих влади;

План-графік. Цей розділ описує засоби, які заявник буде використовувати для того, щоб забезпечити для сертифікуючих влади обозримость діяльності в процесах життєвого циклу програмного забезпечення і, отже, можливість планування перевірок;

Додаткові міркування. Цей розділ описує особливості, які можуть вплинути на процес сертифікації, наприклад, альтернативні методи підтвердження відповідності, кваліфікацію інструментальних засобів, раніше розроблене програмне забезпечення, вариантное програмне забезпечення, яке може бути вибрано за бажанням, програмне забезпечення, доступне для модифікації користувачем, готове програмне забезпечення COTS, використовуване без модифікацій, програмне забезпечення, завантажуване в

польових умовах, несиметрично резервувати програмне забезпечення або використання історії експлуатації продукту.

У процесі самих сертифікаційних випробувань заявник надає свідчення того, що *процеси життєвого циклу* програмного забезпечення задовольняють планам програмного забезпечення. Заявник організовує доступ органа, що сертифікує до даних життєвого *циклу* програмного забезпечення. При цьому мінімальний перелік цих даних включає в себе:

- План сертифікаційних випробувань (план програмних аспектів сертифікації);

- Індекс зміни програмного забезпечення - документ, який повинен однозначно ідентифікувати кожен компонент проекту (включаючи вимоги, вихідні коди, об'єктний і виконуваний код), середу реалізації системи, інструкції з компіляції системи, апаратне та програмне забезпечення для роботи системи, апаратне і програмне забезпечення для проведення сертифікації.

- Підсумковий висновок про програмне забезпечення.

Підсумкове висновок з програмного забезпечення є основним документом для демонстрації відповідності програмного забезпечення Плану програмних аспектів сертифікації. Підсумкове висновок повинен включати:

огляд системи. Цей розділ містить огляд системи, включаючи опис її функцій і їх розміщення в апаратному та програмному забезпеченні, архітектуру, використовуваний процесор (процесори), апаратно-програмний інтерфейс, засоби забезпечення отказобезопасность. У цьому розділі також описуються всі відмінності від опису системи, раніше поміщеного в план програмних аспектів сертифікації;

Огляд програмного забезпечення. Цей розділ коротко описує функції програмного забезпечення (особлива увага приділяється використовуваної концепції отказобезопасность і поділу на відокремлені частини), а також роз'яснює відмінності від огляду програмного забезпечення, раніше поміщеного в план програмних аспектів сертифікації;

Сертифікаційні міркування. Цей розділ повторно формулює сертифікаційні міркування, наведені в плані програмних аспектів сертифікації, а також описує будь-які відмінності від раніше наведених міркувань;

Характеристики програмного забезпечення. Цей розділ констатує дані про розмір виконуваного коду, запасах за часом і пам'яті, обмеженнях ресурсів, а також описує засоби для вимірювання кожної характеристики;

Життєвий цикл програмного забезпечення. Цей розділ підсумовує реальний життєвий цикл (цикли) програмного забезпечення і роз'яснює відмінності від життєвого циклу програмного забезпечення і процесів життєвого циклу, раніше запропонованих в плані програмних аспектів сертифікації;

Дані життєвого циклу програмного забезпечення. Цей розділ дає посилання на дані життєвого циклу програмного забезпечення, віднайдені в процесах розробки програмного забезпечення та процесах забезпечення цілісності. Він описує взаємозв'язок даних між собою та з іншими даними, що визначають систему, і засоби, за допомогою яких до даних життєвого циклу програмного забезпечення може бути забезпечений доступ з боку сертифікуючих влади. Цей розділ також описує будь-які відмінності від опису даних життєвого циклу, раніше поміщеного в плані програмних аспектів сертифікації;

Додаткові міркування. Цей розділ підсумовує питання, які можуть привернути увагу сертифікуючих влади, і дає посилання на дані, застосовні до цих питань, такі, як випущені документи або спеціальні умови;

Ідентифікація програмного забезпечення. Цей розділ ідентифікує конфігурацію програмного забезпечення по номенклатурному номеру або версії;

Історія змін. Цей розділ, якщо це доречно, включає зведення змін програмного забезпечення. Особлива увага приділяється змінам, які зроблені для виправлення помилок, що впливають на отказобезопасность, а також ідентифікацію змін у процесах життєвого циклу програмного забезпечення з часу попередньої сертифікації;

Статус програмного забезпечення. Цей розділ містить зведення повідомлень про проблеми, не дозволених на момент сертифікації, включаючи заяви про функціональні обмеженнях;

Заяву про відповідність. Цей розділ включає заяву про відповідність програмного забезпечення з цим документом, а також зведення методів, використаних для демонстрації відповідності із зазначенням критеріїв, які специфіковані в планах програмного забезпечення. У цьому розділі також зазначаються додаткові, по відношенню до планів програмного забезпечення, стандартам і цьому документу, використані правила і відхилення від планів, стандартів і цього документа.

Повний перелік даних життєвого циклу, які можуть знадобитися при сертифікації, включає в себе:

план програмних аспектів сертифікації;

- план розробки програмного забезпечення;
- план верифікації програмного забезпечення;
- план управління конфігурацією програмного забезпечення;
- план гарантії якості програмного забезпечення;
- стандарти на вимоги до програмного забезпечення;
- стандарти проектування програмного забезпечення;
- стандарти на код програмного забезпечення;
- дані вимог на програмне забезпечення;
- опис проекту;
- вихідний текст;
- виконуваний об'єктний код;
- тестові приклади і тестові процедури верифікації програмного забезпечення;
- звіт за результатами верифікації програмного забезпечення;
- індекс зміни навколишнього середовища життєвого циклу програмного забезпечення;
- індекс зміни програмного забезпечення;
- повідомлення про проблеми;
- документи з управління конфігурацією програмного забезпечення;
- документи по гарантії якості програмного забезпечення;
- підсумковий висновок з програмного забезпечення.

Сертифікуючий орган встановлює т.зв. сертифікаційний базис для системи в ході консультацій із заявником. Сертифікаційний *базис* визначає конкретні правила разом з будь-якими спеціальними умовами, які можуть доповнювати опубліковані правила сертифікації, регламентовані стандартом.

Для програмного забезпечення установка базису проводиться з розгляду підсумкового висновку про програмне забезпечення та свідоцтв відповідності.

В ході сертифікації сертифікуючий орган оцінює план програмних аспектів сертифікації на повноту і узгодженість з критеріями оцінки отказобезопасность системи й іншими даними життєвого *циклу* програмного забезпечення. Якщо вірні всі дані життєвого циклу, що є доказом того, що в ході проекту були активні всі необхідні процеси розробки та верифікації, то сертифікуючий орган видає позитивне рішення про видачу сертифіката.

Сертифікати на *програмне забезпечення* можна віднести до двох типів: сертифікати відповідності та сертифікати якості.

- **Сертифікат якості** - свідоцтво, що засвідчує якість фактично поставленого товару та його відповідність умовам договору. У сертифікаті якості дається характеристика товару або підтверджується відповідність товару певним стандартам чи технічним умовам замовлення. Сертифікат якості видається компетентними організаціями, торговими палатами, спеціальними лабораторіями як у країні експорту, так і імпорту. Сторони договору купівлі-продажу можуть домовитися про надання сертифікатів різних контрольних і перевірочних установ.

- **Сертифікат відповідності** - результат дій третьої сторони (документ), що підтверджує впевненість у тому, що належним чином ідентифікована продукція, процес або послуга відповідають конкретному стандарту чи іншому нормативному документу

Сертифікат на льотну придатність в розглянутому прикладі поєднує в собі властивості обох типів сертифікатів. З одного боку, він засвідчує, що розроблена система має певний рівень якості реалізації, а з іншого - що процеси з її розробки відповідають міжнародному авіаційному галузевому стандарту.

1.3 Інтеграційне тестування

Результатом тестування та верифікації окремих модулів, що складають програмну систему, є висновок про те, що ці модулі є внутрішньо несуперечливими і відповідають вимогам. Однак окремі модулі рідко функціонують самі по собі, тому наступна задача після тестування окремих модулів - тестування коректності взаємодії декількох модулів, об'єднаних в єдине ціле. Таке тестування називають інтеграційним. Його мета - упевнитися в коректності спільної роботи компонент системи.

Інтеграційне тестування називають ще тестуванням архітектури системи. З одного боку, це назва пояснюється тим, що, інтеграційні тести містять у собі перевірки всіх можливих видів взаємодій між програмними модулями і елементами, які визначаються в архітектурі системи, - таким чином, інтеграційні тести перевіряють повноту взаємодій в тестованої реалізації системи. З іншого боку, результати виконання інтеграційних тестів - один з основних джерел інформації для процесу поліпшення та уточнення архітектури системи, міжмодульних і межкомпонентних інтерфейсів. Тобто з цієї точки зору інтеграційні тести перевіряють коректність взаємодії компонент системи.

У результаті проведення інтеграційного тестування та усунення всіх виявлених дефектів виходить погоджена та цілісна архітектура програмної системи, тобто можна вважати, що інтеграційне тестування - це тестування архітектури та низькорівневих функціональних вимог.

Інтеграційне тестування, як правило, являє собою ітеративний процес, при якому перевіряється функціональність все більш і більш збільшується в розмірах сукупності модулів

1.3.1. Завдання і цілі інтеграційного тестування

1.3.1.1. Структурна класифікація методів інтеграційного тестування

Як правило, інтеграційне тестування проводиться вже по завершенні модульного тестування для всіх інтегровних модулів. Однак це далеко не завжди так. Існує кілька методів проведення інтеграційного тестування:

Висхідне тестування. При використанні цього методу мається на увазі, що спочатку тестуються всі програмні модулі, що входять до складу системи, і тільки потім вони об'єднуються для інтеграційного тестування. При такому підході значно спрощується локалізація помилок: якщо модулі протестовані окремо, то помилка при їх спільній роботі є проблема їх інтерфейсу. Тоді область пошуку проблем у тестувальника стає досить вузькою, а тому набагато вища ймовірність правильно ідентифікувати дефект.

Однак у *висхідного методу* тестування є істотний недолік - необхідність у розробці драйвера і заглушок для модульного тестування перед проведенням інтеграційного тестування і необхідність у розробці драйвера і заглушок при інтеграційному тестуванні частини модулів системи.

З одного боку, драйвери і заглушки - потужний інструмент тестування, з іншого - їх розробка потребує значних ресурсів, особливо при зміні складу інтегруються модулів. Тобто може знадобитися один набір драйверів для модульного тестування кожного модуля, окремий драйвер і заглушки для

тестування інтеграції двох модулів з набору, окремий - для тестування інтеграції трьох модулів і т.п.У першу чергу, причина в тому, що при інтеграції модулів відпадає необхідність у деяких заглушках, а також потрібна зміна драйвера, яка підтримуватиме нові тести, що зачіпають кілька модулів.

Монолітне тестування передбачає, що окремі компоненти системи серйозного тестування не проходили. Основна перевага даного методу - відсутність необхідності в розробці тестового оточення, драйверів і заглушок. Після розробки всіх модулів виконується їх інтеграція, потім система перевіряється вся в цілому, як вона є. Цей підхід не слід плутати з системним тестуванням.Незважаючи на те, що при монолітному тестуванні перевіряється робота всієї системи в цілому, основне завдання 16 цього тестування - визначити проблеми взаємодії окремих модулів системи. Завданням же системного тестування є оцінка якісних і кількісних характеристик системи з точки зору їх прийнятності для кінцевого користувача.

Проте, *монолітне тестування* має низку серйозних недоліків:

- дуже важко виявити джерело помилки (ідентифікувати помилковий фрагмент коду);
- важко організувати виправлення помилок;
- процес тестування погано автоматизується.

Спадний тестування передбачає, що процес інтеграційного тестування рухається слідом за розробкою. Спочатку при низхідному підході тестують тільки самий верхній керуючий рівень системи, без модулів більш низького рівня. Потім поступово з більш високорівневими модулями інтегруються більш низькорівневі. В результаті застосування такого методу відпадає необхідність в драйверах (роль драйвера виконує більше високорівнева модуль системи), проте зберігається потреба в заглушках.

1.3.1.2. **Тимчасова класифікація методів інтеграційного тестування**

На практиці найчастіше в різних частинах проекту застосовуються всі розглянуті в попередньому розділі методи в сукупності. Кожен модуль тестують по мірі готовності окремо, а потім включають у вже готову композицію. Для одних частин тестування виходить низхідним, для інших - висхідним. У зв'язку з цим видається корисним розглянути ще один тип класифікації типів інтеграційного тестування - класифікацію за частотою інтеграції:

- тестування з пізньої інтеграцією;

- тестування з постійною інтеграцією;
- тестування з регулярною або пошаровим інтеграцією.

Тестування з пізньої інтеграцією - практично повний аналог монолітного тестування. Інтеграційне тестування при такій схемі відкладається на якомога більш пізні терміни проекту. Цей підхід виправдовує себе в тому випадку, якщо система являє собою 17 конгломерат слабко пов'язаних між собою модулів, які взаємодіють з якого-небудь стандартного інтерфейсу, визначеним поза проекту (наприклад, у випадку, якщо система складається з окремих Web-сервісів).

Схематично тестування з пізньої інтеграцією може бути зображено у вигляді ланцюжка RCVRCVRCVIRCVRCVI, де R - розробка вимог на окремий модуль, C - розробка програмного коду, V - тестування модуля, I - інтеграційне тестування всього, що було зроблено раніше.

Тестування з постійною інтеграцією увазі, що як тільки розробляється новий модуль системи, він відразу ж інтегрується з усією іншою системою. Тести для цього модуля перевіряють як суто його внутрішню функціональність, так і його взаємодію з іншими модулями системи. Таким чином, цей підхід поєднує в собі модульне тестування та інтеграційне. Розробки заглушок при такому підході не потрібно, але може знадобитися розробка драйверів. В даний час саме цей підхід називають unit testing, незважаючи на те, що на відміну від класичного модульного тестування тут не перевіряється функціональність ізольованого модуля. Локалізація помилок міжмодульних інтерфейсів при такому підході дещо ускладнена, але все ж значно нижче, ніж при монолітному тестуванні.Велика частина таких помилок виявляється досить рано саме за рахунок частоти інтеграції і за рахунок того, що за одну ітерацію тестування перевіряється порівняно невелике число міжмодульних інтер фейсом.

Схематично тестування з постійною інтеграцією може бути зображено у вигляді ланцюжка RCIRCIRCI, в якій *фаза тестування модуля* навмисно опущена і замінена на тестування інтеграції.

При **тестуванні з регулярною або пошаровим інтеграцією** інтеграційному тестуванню підлягають сильно пов'язані між собою групи модулів (шари), які потім також інтегруються між собою. Такий вид інтеграційного тестування називають також ієрархічним інтеграційним тестуванням, оскільки укрупнення інтегрованих частин системи, як правило, відбувається за ієрархічним принципом.Однак, на відміну від спадного або висхідного тестування, напрямок проходу по ієрархії в цьому підході не задано.

	Висхідний	Спадний	Моноліт не	Пізня інтеграція	Постійна інтеграція	Регулярна інтеграція
Час інтеграції	пізно (після тестування модулів)	рано (паралельно з розробкою	пізно (після розробки всіх модулів)	пізно (після розробки всіх модулів)	рано (паралельно з розробкою)	рано (паралельно з розробкою)
Частота інтеграції	Рідко	часто	рідко	рідко	часто	часто
Чи потрібні драйвери	Так	немає	немає	немає	да	да
Чи потрібні заглушки	Так	да	немає	немає	немає	да

Таблиця 1.1 представляє основні характеристики розглянутих вище видів інтеграційного тестування. Час інтеграції характеризує момент часу, коли проводиться перша інтеграційне тестування і всі наступні, частота інтеграції - наскільки часто при розробці виконується інтеграція. Необхідність в драйверах і заглушках визначена в останніх двох рядках таблиці.

1.4. Фундаментальний процес тестування

Як ми побачили, виконання тестів необхідно, але не менш важливі і супроводжуючі дії – планування і документування процесу. В обов'язки тестувальників входить розробка тестових сценаріїв, а також підготовка тестування і оцінка його результатів. Становлення ідеї фундаментального тестового процесу на всіх рівнях тестування зайняло роки. У рамках цього процесу можна виділити ключові кроки:

- Планування та управління;
- Аналіз та проектування;
- Впровадження та реалізація;
- Оцінка критеріїв виходу і написання звітів;

- Дії по завершенню тестування.

Тут дії описані в логічній послідовності, але в умовах реального проекту вони можуть накладатися, відбуватися одночасно або навіть повторюватися. Зазвичай, відбувається адаптація цих кроків під потреби конкретної системи або проекту. Розглянемо їх:

1.4.1. Планування та управління

Планування тестування включає дії, спрямовані на визначення основних цілей тестування і завдань, виконання яких необхідне для досягнення цих цілей.

У процесі планування ми переконуємося в тому, що ми правильно зрозуміли цілі та побажання замовника і об'єктивно оцінили рівень ризику для проекту, після чого ставимо цілі і завдання для, власне, тестування.

Для більш ясного опису цілей і завдань тестування складаються такі документи як тест-політика, тест-стратегія і тест-план.

Тест-політика – високорівневий документ, що описує принципи, підходи і основні цілі компанії в сфері тестування.

Тест-стратегія – високорівневий документ, що містить опис рівнів тестування і підходів до тестування в межах цих рівнів. Діє на рівні компанії або програми (одного або більше проектів).

Тест-план – документ, що описує засоби, підходи, графік робіт і ресурси, необхідні для проведення тестування. Крім іншого, визначає інструменти тестування, функціональність, яку потрібно протестувати, розподіл ролей в команді, тестове оточення, техніки тест-дизайну, що використовуються, критерії початку та закінчення тестування та ризики. Тобто, це докладний опис всього процесу тестування.

У будь-якій діяльності, управління не закінчується плануванням. Нам потрібно контролювати і вимірювати прогрес. Саме тому управління тестуванням – безперервний процес.

Управління тестуванням – зіставлення поточної ситуації в процесі тестування із планом та складання звітності.

У свою чергу, дані, отримані в ході контролю над процесом, враховуються при плануванні подальших дій.

1.4.2 Аналіз та проектування

Аналіз та проектування тестів – це процес написання тестових сценаріїв і умов на основі загальних цілей тестування. У процесі аналізу і проектування ми розробляємо тестові сценарії на підставі загальних цілей тестування, визначених під час планування.

Тестовий сценарій – документ, що визначає встановлену послідовність дій при виконанні тестування.

1.4.3 Впровадження та реалізація

Під час виконання тестування відбувається написання тест-кейсів, на основі написаних раніше тестових сценаріїв, збирається необхідна для проведення тестів інформація, готується тестове оточення і запускаються тести.

Тест-кейс – документ, що містить набір вхідних значень, перед- та післяумови, а також очікуваний результат проведення тесту, розроблений для перевірки відповідності визначеної функціональності системи заданим для цієї функціональності вимогам.

Тестове оточення – апаратне і програмне забезпечення та інші засоби, необхідні для виконання тестів

1.4.4 Оцінка критеріїв виходу і написання звітів

Критерії виходу визначають, коли можна завершувати тестування. Вони необхідні для кожного рівня тестування, оскільки нам необхідно знати, чи достатньо було проведено тестів.

При оцінці критеріїв виходу необхідно:

- Перевірити, чи було проведено достатню кількість тестів, чи досягнута потрібна ступінь забезпечення якості системи;
- Переконається в тому, що немає необхідності проводити додаткові тести. Якщо все ж така необхідність є, можливо, буде потрібно змінити встановлений критерій виходу.

Після закінчення тестування відбувається написання звіту, який буде доступний всім зацікавленим сторонам. Адже не тільки тестувальники

повинні знати результати виконання тестів, – ця інформація може бути необхідна багатьом учасникам процесу створення ПЗ.

1.4.5 Дії після завершення тестування

При завершенні тестування ми збираємо, систематизуємо і аналізуємо інформацію про його результати. Вона може стати в нагоді пізніше – при випуску готового продукту. Можуть бути й інші причини для згортання тестування, наприклад, дострокове закриття проекту або завершення певного етапу розробки.

Основні цілі цього етапу:

- Переконатися, що вся запланована функціональність дійсно була реалізована;
- Перевірити, що всі звіти про помилки, подані раніше, були, так чи інакше, закриті;
- Завершення роботи тестового забезпечення, тестового оточення та інфраструктури;
- Оцінити загальні результати тестування і проаналізувати досвід, отриманий в його процесі.

1.5. Конфігураційне тестування

Даний вид тестування дозволяє перевірити працездатність програмної системи в умовах різних операційних систем, апаратних та програмних конфігурацій. Ознайомившись із визначенням, можна помітити, що конфігураційне тестування сходиться із визначенням тестування здатності до портування (portability testing), і це неспроста, оскільки дані поняття практично ідентичні.

Конфігураційне тестування – ще один із видів традиційного тестування продуктивності. У цьому випадку замість того, щоб тестувати продуктивність системи з погляду навантаження, тестується ефект впливу на продуктивність змін у конфігурації. Хорошим прикладом такого тестування можуть бути експерименти з різними методами балансування навантаження. Конфігураційне тестування також може бути поєднане з тестуванням навантаження, стрес або тестуванням стабільності.

Виходячи із визначення, можна виділити 2 мети конфігураційного тестування:

- Визначити оптимальну конфігурацію устаткування, що забезпечує необхідні характеристики продуктивності та часу реакції системи, що тестується.
- Перевірити об’єкт тестування на сумісність із обладнанням, що заявлене в специфікації, операційними системами та програмними продуктами третіх компаній.

Також, можна виділити 2 рівня проведення тестування конфігурації – клієнтський та серверний. **Клієнтський**. Додаток тестується з позиції робочого оточення кінцевого користувача. А саме:

- Кросплатформенне тестування (типи і версії ОС).
- Кросбраузерне тестування (використовується, при тестуванні веб-додатків).
- Тестування роботи при різних версіях драйверів.
- При тестуванні ігрових додатків – тестування відеоадаптера.

Якщо ж програма **клієнт-серверна**, необхідно протестувати взаємодію додатоку із оточенням:

- Апаратним (тип і кількість процесорів, обсяг пам’яті, характеристики мережі/мережевих адаптерів і т.д.).
- Програмним (ОС, драйвера та бібліотеки, стороннє ПЗ, що впливає на роботу програми і т.д.).

Безпосередньо, саме тестування проводиться таким чином:

- Визначаються всі можливі конфігурації, які необхідно протестувати.
- Дані конфігурації розподіляються у чергу за пріоритетом, так як їх кількість може бути дуже великою.
- Відповідно до встановлених пріоритетів проводиться саме тестування.

1.6 Тестування надійності і відновлення після збоїв

Тестування на відмову та відновлення (Failover and Recovery Testing) – вид тестування, основною місією якого є визначення здатності ПЗ до опору та відновленню після збоїв у роботі, які виникли як всередині програми, так і від інших програмно-незалежних факторів (апаратура, мережа і т.д.).

Тобто іншими словами, тестування на відновлення це нефункціональне тестування, яке визначає здатність програмного забезпечення відновлювати

такі збої, як збої програмного / апаратного забезпечення або будь-які збої в мережі.

Даний вид тестування має досить специфічний (порівняно з іншими видами) підхід до виконання тестів, так як об'єктами дослідження є:

- Поведінка ПЗ при перериванні обробки даних.
- При втраті мережі.
- При відключенні електроенергії (на стороні клієнта або сервера).
- При втраті підключення носіїв даних.

Отже і різні сценарії тестування розробляються спираючись на вищезгадані фактори впливу на здатність ПЗ до відновлення після збою.
Тестування на відмову та відновлення особливе актуально при розробці систем, які повинні працювати протягом тривалого часу, аж до 24/7. Від здатності такого ПЗ відновлювати працездатність після непередбаченої ситуації, а також мінімізувати втрати даних буде залежати не тільки репутація компанії-розробника, а часом і щось більше, ніж гроші.
При моделюванні ситуації збою, оцінюється як ступінь втрати даних (чи знаходиться вона в межах допустимого), так і здатність системи протоколювати всі транзакції та статус їх виконання.
Виконання тестування відновлення програмно-апаратних засобів не вдалося

перевірити

- Якщо відновлення успішне чи ні.
- Чи можна виконувати подальші операції з програмним забезпеченням

  чи ні.
- Тривалість, необхідна для відновлення операцій.
- Втрачені дані можна відновити повністю або ні.
- Відсоток сценаріїв, за яких система може повернутися назад.

Перед тим, як це тестування буде виконано, резервна копія знімається та зберігається у захищеному місці, щоб уникнути втрати даних, якщо дані не будуть відновлені успішно.

Поширені збої, які слід перевірити на відновлення:

1. Проблема мережі
2. Збій живлення
3. Зовнішній сервер недоступний
4. Сервер не відповідає
5. dll файл відсутній
6. Перевантаження бази даних
7. Припинені послуги
8. Фізичні умови
9. Зовнішній пристрій не відповідає
10. Втрата сигналу бездротової мережі

Життєвий цикл тестування на відновлення
Життєвий цикл включає:

Рис 1. Життєвий цикл тестування на відновлення

1) Стандартні операції

Стандартні операції системи - це спосіб роботи системи. Це система, налаштована зі всім необхідним обладнанням / програмним забезпеченням, щоб система могла працювати належним чином.

2) Подія катастрофи та аварії

Збій або катастрофа системи може статися з різних причин, таких як фізичні умови, збій живлення, недоступність сервера, відмова обладнання та багато іншого.

3) Переривання стандартного процесу

Коли відбувається переривання стандартних процесів, це може призвести до збитків з точки зору бізнесу, відносин з клієнтом, грошових коштів, репутації на ринку тощо.

4) Процес відновлення

Щоб уникнути великих збитків у компаній, створіть резервні плани, щоб мінімальний вплив на систему спричинив переривання.

5) Процес відновлення

Процес відновлення включає вже визначені документи та процеси, яких слід дотримуватися. Усі папки та файли конфігурації перебудовуються для отримання втрачених даних.

Приклад тестування на відновлення

- Завантажуючи дані у свою систему, вимкніть з'єднання Wi-Fi і через деякий час увімкніть його знову і спостерігайте, чи продовжують завантажуватися дані, чи дані втрачаються.
- Нехай браузер працює більше одного сеансу та перезапустить систему. Після перезапуску системи переконайтеся, що всі сеанси перезавантажені знову.

- Коли програма отримує дані з мережі, щоб відмовити у сценарії, від'єднайте кабель. Через деякий час знову підключіть кабель і відстежуйте, чи відновлені дані, і програма продовжує отримувати дані з місця, де втратила зв’язок

Кроки до плану відновлення

- Правильний аналіз слід зробити, щоб перевірити можливість одужання. Потрібно проаналізувати збої, які можуть виникнути, способи їх усунення, вплив несправностей, спосіб їх запуску. Слід проаналізувати здатність системи розподіляти додаткові ресурси, такі як центральний процесор та сервер у разі критичних збоїв.
- План випробувань - Випробувальні випадки повинні бути розроблені відповідно до результатів аналізу (згаданих у пункті вище)
- Тестове середовище слід будувати на основі результатів, отриманих в результаті аналізу, проведеного для відновлення.
- Резервне копіювання даних слід постійно підтримувати, наприклад, стан програмного забезпечення, дані бази даних тощо. Залежно від критичності, дані можна створити за допомогою наступних стратегій:
    - Одинарне резервне копіювання / Кілька резервних копій
    - Резервне копіювання в режимі онлайн / офлайн
    - Кілька резервних копій в одному або декількох місцях.
    - Автоматичне налаштування для резервного копіювання кожну 'n' хвилину, скажімо, 15 хвилин.

    - Мати окрему команду для виконання та відстеження резервних копій.
- Виділення ресурсів для тестування відновлення.
- План відновлення повинен бути задокументований та оновлювати документ, коли і коли вносяться зміни.

Передовий досвід тестування на аварійне відновлення:

- Щоб розпочати це тестування, найпершим кроком є підготовка тестового середовища, яке має бути копією виробничого / реального середовища. Інтерфейс, апаратне забезпечення, програмне забезпечення, код, прошивка повинні бути повною копією діючої системи. Результати якості можна отримати, якщо налаштування тестового середовища наближається до реального / виробничого середовища.
- Під час проведення випробувань на відновлення слід використовувати обладнання, яке виділено для виробничого середовища для відновлення.
- Тестери можуть використовувати для тестування систему резервного копіювання в Інтернеті, але в той же час потрібно забезпечити легке отримання даних та відсутність проблем із безпекою.

Переваги / недоліки

Переваги:

- Це допомагає зробити систему більш стабільною та без помилок та покращує якість продукту.

- Система стає більш надійною, оскільки помилки видаляються до їх запуску та покращують продуктивність системи.
- Резервне копіювання завжди підтримується для відновлення даних у разі будь-якої помилки.

Недоліки:

- Для проведення цього тестування необхідний навчений ресурс. Тестер, який виконує те саме, повинен мати усі дані для тестування, тобто дані та файли резервних копій.
- Тестування відновлення вимагає декількох кроків, які слід виконати перед тестуванням, і багато кроків під час виконання, що робить це трудомістким процесом.
- Тестування відновлення - дорогий процес.
- Не всі потенційні помилки можна знайти в декількох випадках.

Різниця між тестуванням на відновлення та тестуванням на надійність

Тестування відновлення та перевірку надійності часто плутають і вважають однаковим. Тоді як обидва пов'язані між собою, але різні.

Давайте перевіримо різницю між ними в таблиці нижче:

№	Тестування на відновлення	Перевірка надійності
1	Тестування на відновлення проводиться, щоб перевірити, наскільки добре система відновлюється після відмови або катастрофи	Перевірка надійності проводиться, щоб виявити несправність у конкретному місці, де вона виникає.
2	Дізнається, чи здатна система продовжувати роботу після катастрофи.	Помилки виявляються та виправляються до розгортання.
3	Тестування відновлення визначає його здатність відновлювати дані після відмов живлення, проблем з мережею тощо.	Додаток тестується протягом певного періоду часу та навколишнього середовища. Якщо результати тестів

		незмінно однакові, то лише це вважається надійним додатком.

Шаблон для тестування на аварійне відновлення

Шаблон, тобто попередньо відформатований документ, використовується для планування відновлення від будь-якої катастрофи. Компанії можуть мати шаблони відповідно до їх вимог та відповідно до їх потреб. Але мало елементів є обов'язковими, щоб бути частиною цього.

Давайте перевіримо ті елементи, які повинні бути частиною шаблону:

1. **Визначення катастрофи**, тобто ситуація / стан, коли це буде вважатися катастрофою.
2. **Список групи реагування на надзвичайні ситуації** з їх повними даними, такими як ім'я / роль / електронна адреса / номер телефону
3. **Детальна інформація про команду з питань аварії**
4. **Список зовнішніх контактів**: Список ресурсів, які можуть знадобитися під час аварійного відновлення.
5. **Управління ризиками**: Для покриття потенційних ризиків та рішення документально підтверджено.
6. **Огляд плану**
7. **Оповіщення про надзвичайні ситуації**, **ескалація та активація**: Кроки під час надзвичайної ситуації.
8. **Інформація про страхування**

9. **Фінансово-правова інформація**

10. **План відновлення** / стратегія резервного копіювання

1.7. Системи моніторінгу та управління безпекою

З кожним днем зростає складність і кількість різних загроз інформаційної безпеки. Разом з цим збільшується і число систем, покликаних захистити бізнес від цих загроз. У 99% великих компаній функціонує міжмережевий екран, антивірусне рішення і система виявлення вторгнення — це сьогодні необхідний мінімум. Крім того, в мережі працюють бази даних, операційні системи та програмне забезпечення власної розробки. Всі ці підсистеми генерують реєстраційні журнали і різні події.

У підсумку адміністратори отримують сотні тисяч повідомлень від безлічі різноманітних підсистем кожен день. Функціонування кожної з підсистем окремо критично для бізнесу в цілому, тому фахівці змушені аналізувати весь цей потік інформації. Виділити важливі повідомлення стає все складніше, і в результаті цінність окремих рішень для забезпечення безпеки прагне до нуля, а час відновлення інформаційної системи після збоїв катастрофічно зростає.

Максимально ефективно використовувати дані, одержані від сенсорів (серверів) виявлення атак і від міжмережевих екранів атаках (про відображених ними атаках) дозволяє використання системи моніторингу інформаційної безпеки. Система моніторингу ІБ дозволяє звести всі події та інциденти ІБ в єдиній консолі, виконує інтелектуальний аналіз атак та їх наслідків і допомагає адміністраторам виробити контрзаходи. Крім цього, система моніторингу ІБ виконує реєстрацію та зберігання всіх подій інформаційної безпеки, що робить можливим використання отриманого матеріалу в якості доказового при виконанні розслідувань інцидентів та судочинстві

Основні можливості SIEM-систем:

- Збір інформації про події з різних пристроїв забезпечення інформаційної безпеки і мережевих пристроїв;
- Візуалізацію подій в режимі реального часу;
- Підтримку сигнатурних і «поведінкових» методів виявлення аномалій і атак;
- Можливість створення власних правил кореляції;
- Можливість управління активними мережевими пристроями з метою блокування шкідливого трафіку;
- Прогнозування результатів атаки;
- Аналіз ризику захищаємої системи;
- Автоматичне визначення статусу події (атака, сканування тощо);
- Можливість обробки та аналізу інцидентів безпеки;
- Фокусування уваги на пріоритетних захищаємих вузлах;
- Вбудована система роботи з інцидентами, можливість інтеграції з існуючою;
- Автоматична реакція на інциденти.
- забезпечити централізоване управління подіями і інцидентами ІБ
- збільшити швидкість виявлення, розслідування та реагування на інциденти
- управляти інцидентами ІБ
- підвищити ефективність управління ризиками ІБ
- підвищити рівень відповідності політикам і нормативним вимогам

2. Виконати аналіз технічної реалізації та принципу роботи розробленої мультисервісної системи та її компонентів

2.1. Архітектура мультисервісних мереж передачі даних

Основа побудови мультисервісних мереж – архітектура Cisco Architecture for Voice Video and Integrated Data [6, 24, 26]. Це всеосяжна архітектура, що складається з трьох основних блоків (рис. 2):

1. Інтелектуальна мережева інфраструктура на базі протоколу IP, що включає в себе маршрутизатори, комутатори, шлюзи та інше мережеве обладнання. IP інфраструктура є основою для подальшого впровадження користувацьких додатків і повинна забезпечувати підтримку таких життєво важливих для мережі сервісів, як безпека, мережеве управління та механізми гарантії якості

сервісу (QoS, - Quality of Service).
2. Інтелектуальні клієнтські місця із підтримкою протоколу IP, зокрема цифрові IP телефони, персональні комп'ютери зі спеціалізованим програмним забезпеченням забезпеченням для вирішення різних бізнес-завдань, програмні емулятори телефонів, відео клієнти і таке інше.

3. Службові серверні програми, у тому числі сервери Cisco CallManager, що забезпечують управління корпоративною системою IP телефонії, корпоративна система директорій, відео сервери і т.д.

Рис 2. – Архітектура Cisco AVVID

Мультисервісні мережі можуть містити такі компоненти (рис. 3)

1. IP Phones
2. Gatekeeper
3. Gateway
4. Multipoint control unit (MCU)
5. Call agent
6. Application servers
7. Інші компоненти, голосові програми, системи автоматичної відповіді (Interactive Voice Response)

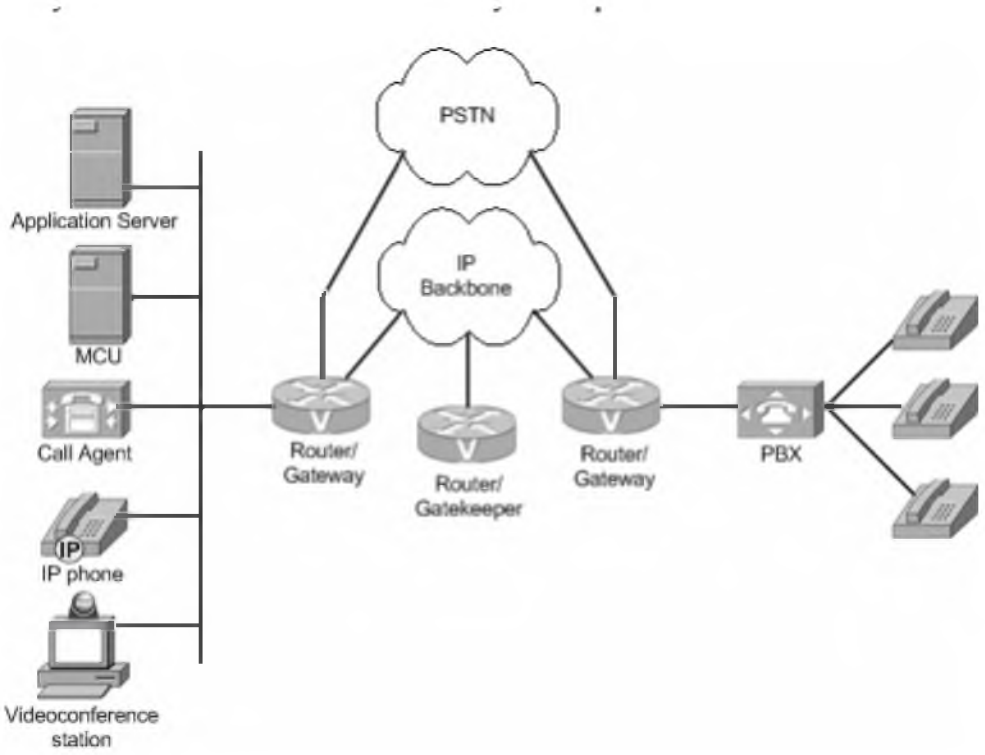

Рис 3. – Основні компоненти мультісервісної мережі

Характерною рисою архітектури, що розглядається, є її розподілена природа, завдяки якій система легко масштабується. Мережа на базі архітектури Cisco AVVID може охоплювати одну будівлю або кілька будівель, об'єднаних кампусною мережею. Можна забезпечити сервіси телефонії, відео та даних для користувачів віддалених офісів та підрозділів, об'єднаних корпоративною IP мережею.

Інша відмінна риса архітектури Cisco AVVID - це її відкритість, - орієнтація на використання відкритих стандартів (зокрема, стандартних протоколів H.323, SIP та MGCP для передачі голосу та відео в мережах IP). Це дозволяє забезпечити поєднання з цілим рядом інших систем, як традиційної, так і пакетної телефонії, а також із системами передачі даних та відео додатками, що підтримують ці стандарти.

Підтримка відкритих стандартних протоколів та відкритих інтерфейсів для розробки додатків (таких як TAPI та JTAPI), забезпечує можливість написання нових програм, що інтегруються в системи на базі Cisco AVVID, а також можливість інтеграції додатків, написаних сторонніми виробниками (рис. 4)

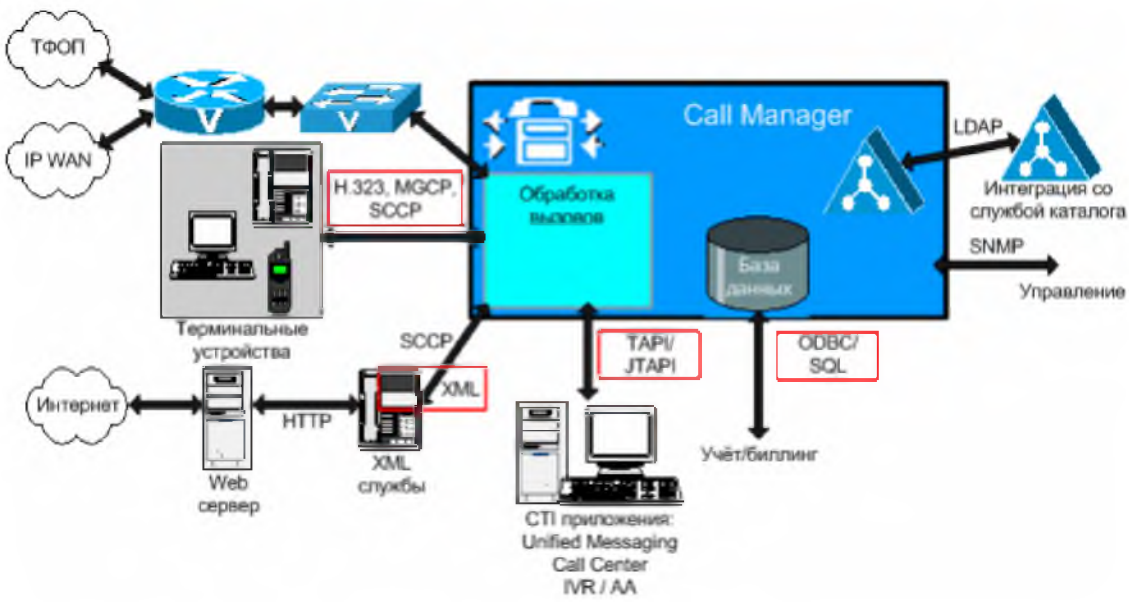

Рис 4. – Інтеграція з додатками на основі відкритих протоколів та інтерфейсів

2.1.1. Інфраструктура

Як і будь-яка архітектура, Cisco AVVID має стійку основу у вигляді трирівневої моделі побудови мереж. Трирівнева модель побудови мережі. Більшість сучасних мереж побудовано на основі трирівневої моделі [24, 26].

Як видно із рис. 5, модель визначає три рівні: рівень ядра, рівень розподілу та рівень доступу. Кожен рівень відповідає за певних функцій. Однак ці рівні є логічними та не обов'язково узгоджені з фізичними пристроями

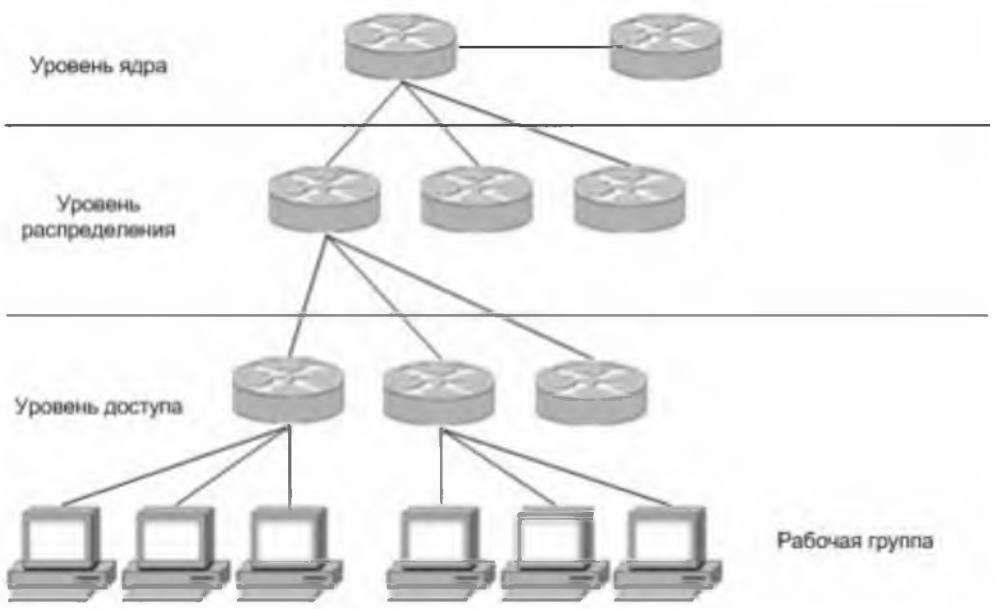

Рис. 5 – Дизайн мережі: трьохрівнева модель

Дотримання даної моделі дозволяє значно спростити побудову мережі та пошук несправностей, а також забезпечує передбачуваність та кращу керованість мережі. Переваги трирівневої побудови, що відповідають вимогам до дизайну мережі, або недосяжні в інших моделях, або вимагають значних зусиль для втілення:

Масштабованість. Поділ функціональності по шарах дозволяє створити природні точки розширення мережі, не надаючи негативного впливу на інші характеристики.

Легкість реалізації. Оскільки ієрархічна модель поділяє мережу на логічну та фізичну складову, з'являється можливість поступової побудови та введення в експлуатацію окремих ділянок мережі

Легкість пошуку несправності. Як правило, ієрархічна побудова мережі полегшує завдання пошуку несправності, знижуючи кількість можливих циклів.

Передбачуваність. Планування пропускної спроможності істотно полегшується в ієрархічної моделі, потреба у пропускній спроможності зростають при наближення до ядра.

Керованість. Передбачуваність потоків даних, масштабованість, незалежність продажі та легкість пошуку несправності значно полегшують управління мережею.

Рівень ядра. На самому верху ієрархії цей рівень відповідає за швидку та надійне пересилання великих обсягів трафіку. Єдиним призначенням базового рівня є швидка комутація трафіку.

Якщо відбувається помилка лише на рівні ядра, вона впливає всіх користувачів. Отже, дуже важливо забезпечити високу надійність цьому рівні. На цьому рівні обробляються великі обсяги трафіку, тому не менш важливо враховувати швидкість та затримки.

Із зазначених функцій рівня ядра, випливають особливості його реалізації:

- Ніщо не повинно уповільнювати трафік, у тому числі списки доступу, маршрутизація між віртуальними локальними мережами VLAN та фільтрація пакетів;
- Не слід реалізовувати функції доступу для робочої групи;
- Слід уникати розширення рівня ядра при зростанні розмірів об'єднаної мережі(наприклад, при додаванні маршрутизаторів). У разі нестачі продуктивності даного рівня, більш кращим виходом є модернізація, а чи не розширення.

Рівень розподілу. Рівень розподілу іноді називають рівнем робітників груп. Він розташований між рівнем ядра та рівнем доступу. Основні функції рівня розподіли полягають у маршрутизації, фільтрації та доступі до регіональних мереж, а також (якщо необхідно) для визначення правил доступу пакетів до рівня ядра. Рівень розподілу повинен встановлювати найшвидший спосіб обробки запитів до службам (наприклад, метод файлового звернення до сервера). Після визначення на цьому рівні найкращого шляху доступу, запит може бути переданий на рівень ядра, де реалізовано швидкісний транспорт запиту до необхідної службе. На рівні розподілу встановлюється політика мережі, а також забезпечуються можливості гнучкого опису мережевих операцій. На рівні розподілу виконується кілька функцій:

- Реалізація інструментів, подібних до списків доступу, фільтрації пакетів або механізму запитів;
- Реалізація системи безпеки та мережевих політик, включаючи трансляцію адрес та встановлення брандмауерів;
- Перерозподіл між протоколами маршрутизації, включаючи використання
- статичних шляхів;

- Маршрутизація між мережами VLAN та іншими функціями підтримки робочих груп;
- Визначення доменів широкомовних та багатоадресних розсилок.

Рівень доступу. На рівні доступу реалізовано управління користувачами та робочими групами під час звернення до ресурсів об'єднаної мережі. Іноді рівень доступу називають рівнем настільних систем. Найбільша частина необхідних користувачам мережевих ресурсів має бути доступна локально – для невеликих мереж пропонується збереження відношення трафік локального сегмента/зовнішній трафік на рівні 80/20, для великих корпоративних мереж існує тенденція до збільшення обсягу зовнішнього трафіку – до співвідношення 20/80. На рівні розподілу виконується перенапрямок трафіку до віддалених служб. Для рівня доступу характерні такі функції:

- Постійний контроль (з рівня розподілу) за доступом та політиками;
- Формування незалежних колізійних доменів (сегментація);
- З'єднання робочих груп із рівнем розподілу.

Забезпечення необхідної якості обслуговування

Для переходу від традиційної телефонії до мультисервісних мереж повинні бути забезпечені відмовостійкість, якість обслуговування (QoS) та пропускна спроможність, необхідні для підтримки програм мультисервісної мережі, таких як передача потокових голоси та відео [17, 18].Наприклад, мають виконуватися такі вимоги:

• Стандартний кодек G.729 для відсутності помилок відтворення вимагає, щоб втрата пакетів, була значно меншою за 1 відсоток;

• Специфікація ITU G.114 рекомендує, щоб затримка при VoIP пакеті при пересилання від абонента до абонента не перевищувало 150 мілісекунд (ms). Для міжнародних дзвінків прийнятною вважається затримка до 300 мілісекунд, особливо у разі використання супутникових каналів. При обчисленні цієї затримки також враховується час поширення сигналу вздовж тракту передачі;

• Повинні бути мінімізовані коливання тривалості затримки (jitter), для чого використовують буферизацію даних. Це рішення збільшує затримку передачі даних між абонентами та є ефективним тільки при коливаннях, не що перевищують 100 мілісекунд.

Тому однією з необхідних умов для впровадження IP телефонії є заміна широкомовного середовища передачі даних на комутовану, однак, ця проблема не актуальна зараз, що обумовлено суттєвим падінням цін на

відповідне обладнання та практично стовідсотковим переходом на комутоване середовище передачі (рис. 6).

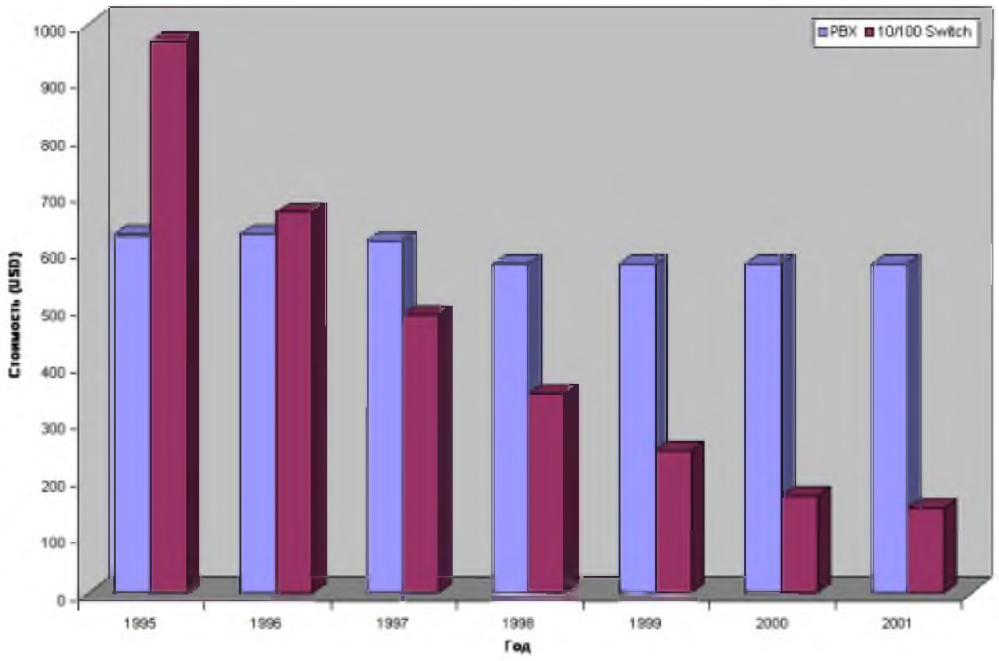

Рис 6 – Порівняльний графік середьої вартості обладнання в разрахунках на один порт

Крім цього для надійного транспортування голосу та відео потрібна підтримка розширеної пріорітизації трафіку, багатоадресних розсилок, буферизації та компресії.

Для забезпечення високої якості передачі голосу потрібно, щоб пакети VoIP (як сигнального, так і аудіо каналу) мали пріоритет щодо інших типів трафіку. Необхідне задоволення вимог щодо відмовостійкості, пропускної здібності, затримки та коливань величини затримки в мережі.

Забезпечення високої відмовостійкості

Традиційна телефонія забезпечує надійне функціонування системи 99.999% часу, це відповідає 5.25 протоколу простою на рік. Багато мереж передачі даних не забезпечують такий рівень надійності. Тому однією з основних вимог при впровадження VoIP є висока надійність і доступність мережі.

Заходи, спрямовані на забезпечення стійкості до відмов, можуть включати:

• придбання обладнання та програмного забезпечення з високим показником MTBF (mean time between failures) – середній час між збоями;

• встановлення дублюючого обладнання;

• прокладання дублюючих ліній зв'язку;

• забезпечення безперебійного електроживлення мережного обладнання, включаючи обладнання кінцевих користувачів;

• попереджувальне управління мережею та вирішення проблем до їхнього прояву.

Для повної стійкості до відмов потрібне дублювання наступних компонентів:

• сервери та CallManager-и;

• пристрої рівня розподілу, такі як маршрутизатори та багаторівневі комутатори;

• пристрої рівня ядра, такі як багаторівневі комутатори;

• з'єднання з оператором телефонного зв'язку, WAN, можливо навіть через різні провайдерів; голосові шлюзи;

• джерела електроживлення та UPS.

Забезпечення гарантованої пропускної спроможності

При переході до мультисервісної мережі потрібно забезпечити необхідну пропускну здатність для потокового голосового та відео трафіку. Це накладає обмеження на канал передачі даних та мережеве обладнання. Необхідна пропускна спроможність визначається технологією стиснення аудіо або відео даних,

Пропускна здатність – це реальний обсяг корисних даних, переданий від джерела до отримувача. Об'єм, що віддається, збільшується за рахунок накладних витрат – заголовків протокольних блоків даних різних рівнів Дані також схильні помилок передачі. Обсяг даних, що передаються обмежений пропускною здатністю каналу, при перевантаженні мережі можливі втрати пакетів, що може призвести до необхідності повторної передачі.

Для забезпечення необхідної пропускної спроможності застосовуються такі техніки:

а. **Використання черг**: ґрунтується на передачі пакетів через конкретний

інтерфейс відповідно до заданих пріоритетів, дозволяє обробляти

інтенсивні потоки, керувати навантаженням мережі, пріоритизувати трафік,

резервувати пропускну спроможність;

b. **Стиснення заголовків**: в IP мережах голос передається за допомогою протоколу реального часу Real-Time Transport Protocol (RTP), який переноситься протоколом UDP, датаграми UDP інкапсулюються у пакети IP. Таким чином, складовий заголовок RTP/UDP/IP досягає 40 байт. Це досить велика величина, оскільки обсяг даних, що надаються в одному пакеті, в більшості випадків становить 20 байт. Застосування стиснення заголовків (CRTP) зменшує розмір заголовка до 2-4 байт.

c. **Контроль встановлення виклику**: цей механізм розширює можливості забезпечення якості обслуговування, забезпечуючи захист голосового трафіку від негативного впливу іншого голосового трафіку шляхом обмеження кількості одночасно встановлених дзвінків.

d. **Фрагментація та чергування**: при фрагментації великі пакети розбиваються на дрібніші, між якими передаються голосові пакети, що дозволяє уникнути затримок, пов'язаних із виведенням великих пакетів в інтерфейс.

Класифікація пакетів. В основі забезпечення якості обслуговування лежить можливість мережних пристроїв розпізнавати та групувати специфічні пакети. Процес розпізнавання отримав назву "класифікація пакетів". Після класифікації пакет має бути помічений відповідним чином, для чого виставляються відповідні прапори в IP заголовку.

Для розпізнавання пакетів VoIP мережні пристрої використовують адреси джерела і одержувача в заголовку IP та номери портів UDP джерела та одержувача в заголовку UDP.

Крім статичної класифікації, заснованої на заголовках протокольних блоків даних 3 і 4 рівнів, може бути використаний механізм динамічної класифікації, такий як Resource Reservation Protocol (RSVP).

Класифікація пакетів - досить ресурсомісткий процес, тому класифікація має відбуватися якомога ближче до краю мережі. У ядрі класифікація має бути максимально спрощена, це досягається рахунок маркування пакетів - установки байта типу сервісу (Type of Service) у заголовку IP.

Три старші біти байта (ToS) називаються бітами старшинства IP (IP Precedence). У даний час більшість додатків та виробників обладнання підтримують встановлення та розпізнавання бітів старшинства IP. Часто для визначення диференційованих класів сервісу (Differentiated Services classes) використовуються шість старших бітів, званих Differentiated Services Code Point.

Маркування пакетів може здійснюватися установкою наступних прапорів:

• Три біти IP Precedence байта ToS заголовка IP пакета;

• Шість бітів DSCP байта ToS заголовка IP пакета;

• Три біти MPLS Experimental (EXP);

• Три біти Class of Service Ethernet 802.1p;

• Один біт Cell Loss Probability (CLP) ATM.

У більшості IP мереж маркування здійснюється установкою IP Precedence або DSCP, що цілком достатньо для ідентифікації трафіку VoIP.

Класифікація та маркування Voice Dial Peers
Дана техніка дозволяє класифікувати пакети VoIP в залежності від номера, з яким здійснюється з'єднання.

Класифікація та маркування Committed Access Rate (CAR)
Committed access rate (CAR) – техніка, що використовує лімітування максимального значення рівня пропускної спроможності, що використовується трафіком. CAR дозволяє виставляти різні біти IP Precedence або DSCP залежно від того, чи перевищено. встановлений ліміт. Однак техніка класифікації CAR найчастіше використовується для пакетів даних, ніж для пакетів VoIP.

Застосування політик маршрутизації (Policy-Based Routing)
Дана техніка дозволяє маршрутизувати трафік, ґрунтуючись на списках доступу (ACL), використовуваному протоколі, номері порту-джерела і так далі. Оскільки дана технологія дозволяє змінювати широке коло полів пакета або кадру, її застосування також можливо для класифікації та маркування пакетів

Модульний інтерфейс командного рядка QoS (Mod QoS CLI або MQC)

Даний метод, заснований на застосуванні шаблонів, є найбільш кращим способом класифікації та маркування пакетів. Він дозволяє відокремити класифікацію від політик, забезпечуючи можливість конфігурування різних засобів забезпечення якості обслуговування різних класів трафіку. Для класифікації трафіку застосовується class map, а визначення необхідних дій для кожного класу - policy map, яка застосовується до вхідного або вихідного трафіку конкретного інтерфейсу.

Організація черг. Коли мережні пристрої можуть ідентифікувати VoIP пакети, з'являється можливість забезпечення необхідного рівня обслуговування (QoS). Для цього можуть застосовуватися різні способи організації черг пакетів на передачу в вузлах мережі (таблиця 1).

Таблиця 1. Способи організації черг пакетів

Способи організації черг	Опис	Переваги	Обмеження
FIFO	Порядок передачі пакетів збігається з порядком, якому вони були отримані.	Простота конфігурування та висока швидкість роботи.	Не забезпечується пріоритетне обслуговування або гарантована смуга пропускання.
WFQ	Потоки розподіляються в різні черги, де ваги використовуються для визначення того, скільки пакетів із цієї черги передається поспіль. Ваги встановлюються при допомоги IP Precedence та DSCP.	Простота конфігурації. за замовчуванням використовується на з'єднаннях з швидкістю до 2 Mbps.	Не забезпечується пріоритетне обслуговування або гарантована смуга пропускання.
Custom Queueing (CQ)	Трафік розподіляється в різні черги, змінної довжини. Довжина черги визначається на основі середньої довжини пакета, максимального розміру пакета (MTU) та відсотка резервованої смуги пропускання. Таким чином, реалізується статистичне резервування смуги пропускання.	можливо наближене резервування смуги пропускання для різних черг.	Не забезпечується пріоритетне обслуговування. можливо наближене резервування смуги пропускання, але обмежена кількість черг. Складність конфігурування.
Priority Queueing (PQ)	Трафік розподіляться по чергам з високим, середнім, нормальним та низьким пріоритетом. Обслуговування трафіку здійснюється в порядку	Забезпечується обслуговування по пріоритетів.	Можливе блокування низькопріоритетного трафіку високопріоритетним. Не забезпечується гарантована смуга пропускання.

	спадання пріоритетів.		
Class-Based WFQ (CBWFQ)	Для класифікації трафіку використовується MQC. Трафік міститься в черзі з зарезервованою смугою пропускання чи черга "за замовчуванням". Планувальник обслуговує черги відповідно до вагами, враховуючи зарезервовану смугу пропускання.	Спосіб схожий з LLQ за винятком відсутності пріоритетною черги. Простота конфігурації та можливість резервування смуги пропускання.	Не забезпечується пріоритетне обслуговування.
Priority Queue WFQ (PQWFQ)	Пріоритет набувають UDP пакети призначені для будь-якого з портів всередині задається інтервалу.	Простота конфігурації. Пріоритетне обслуговування пакетів RTP.	Решта трафік використовує WFQ. RTCP трафік не є пріоритетним. Не забезпечується гарантована смуга пропускання.
LLQ (PQCBWFQ)	Для класифікації трафіку використовується MQC. Трафік міститься в черзі з зарезервованою пропускною здатністю, пріоритетну чергу, або чергу "за умовчанням". Планувальник обслуговує черги відповідно до вагами, при цьому пріоритетний трафік посилається першим і враховується зарезервована смуга пропускання.	Простота конфігурації. Можливість забезпечувати пріоритетну обробку певним класам трафіку та ставити максимальну використовувану смугу пропускання. Є можливість ставити класи трафіку з гарантованою смугою пропускання.	Поки що не підтримуються різні рівні пріоритету – весь пріоритетний трафік використовує одну чергу. Різні класи пріоритету можуть резервувати різні смуги пропускання. Однак загальна пріоритетна черга, що поділяється всіма додатками, може викликати коливання тривалість затримки.

Продовження Таблиці 1. Способи організації черг пакетів

Черга з низькою затримкою (Low Latency Queueing)

Для VoIP потрібна організація пріоритетних черг у вузлах мережі. Допускається використання будь-якого способу організації черг, що надає високий пріоритет пакетам VoIP, але через найбільшу гнучкість і простоту конфігурування рекомендується використання LLQ. LLQ використовує метод конфігурування MQC та дозволяє забезпечити пріоритет певному

класу трафіку, та гарантовану мінімальну пропускну спроможність інших класів. При перевантаженні мережі пріоритетний трафік утримується в межах заданого рівня, що дозволяє уникнути блокування менш пріоритетного трафіку.

LLQ дозволяє вказати довжину черги, при перевищенні якої маршрутизатор відкидає пакети, що надходять. Також є клас "за замовчуванням", що використовується для обробки всього некласифікованого іншими класами трафіку. Цей клас може бути налаштований на основі справедливої черги (fair-queue), це означає, що кожен з некласифікованих потоків отримає приблизно рівну частку від решти пропускну здатність.

Як показано на рис. 7, весь трафік ідучий через інтерфейс або під-інтерфейс (для Frame Relay та ATM) спочатку класифікується з використанням MQC. Існує чотири класу трафіку: один пріоритетний, два з гарантованою пропускною спроможністю та один клас "за замовчуванням". Трафік пріоритетного класу поміщається у пріоритетну черга, класів із гарантованою смугою пропускання в черзі із зарезервованою смугою пропускання. Трафік класу “за умовчанням” може використовувати чергу “за замовчуванням”, де кожен із некласифікованих потоків отримає приблизно рівну частку від смуги пропускання, що залишилася, або може бути створена черга з зарезервованою смугою пропускання. Планувальник обслуговує черги таким чином, що спочатку виводиться пріоритетний трафік, доки не буде досягнуто встановлена межа використовуваної даним трафіком пропускної спроможності, якщо дана пропускна здатність затребувана трафіком із зарезервованих черг (тобто. має місце навантаження мережі). При переповненні пріоритетної черги на момент перевантаження мережі, пріоритетні пакети, що знову надходять, будуть відкидатися.

Зарезервовані черги обслуговуються відповідно до запитаної смуги пропускання, що планувальник використовує для обчислення ваги. Вага визначає, як часто обслуговується черга та скільки байт передається за одне обслуговування. Робота планувальника заснована на алгоритмі weighted fair queueing (WFQ).

Рис 7 – Схема роботи LLQ

Контролює встановлення дзвінка. Call Admission Control (CAC) застосовується до голосового та відео трафіку. Якщо мережне з'єднання перевантажене пакетами даних, виходом може стати застосування черг, буферизація та відкидання пакетів. Трафік затримується до звільнення інтерфейсу або відкидається, а надалі користувач або протокол вимагають повторну передачу.

Для трафіку реального часу, чутливого до затримки та втрати пакетів, такий спосіб вирішення проблеми призведе до падіння якості обслуговування. В даному випадку воліють обмежити можливість доступу до мережі, ніж втратити якість.

CAC є інформованим способом прийняття рішення про достатність вільних ресурсів задля забезпечення необхідної якості передачі голоса. Існує декілька різних механізмів контролю встановлення виклику:

- локальні – рішення про встановлення виклику приймається на основі стану вихідного LAN чи WAN інтерфейсу. Дані механізми мають можливість статично обмежити максимальну кількість одночасно встановлених викликів;
- засновані на вимірах – рішення приймається на основі поточного вимірювання стану мережі, що проводиться посилкою пробних пакетів за заданим IP адресою (зазвичай це голосовий шлюз адресата). Одержувач повертає пакети, на підставі чого стоїть деяка статистика (зазвичай затримка та відсоток втрати пробних пакетів), що характеризує стан мережі зараз;
- засновані на ресурсах – вони поділяються на два класи: визначальна кількість запитуваних та/або вільних ресурсів та резервуючі ресурси.

Ресурси що представляють інтерес включають пропускну здатність з'єднання, завантаження ЦП, кількість пам'яті.

2.2. Принципу роботи розробленої мультисервісної системи

2.2.1. Транспортні мережі в містах

Більшість міських транспортних мереж у Україні є сукупність трьох компонентів:

- Кільця SDH, що поєднують цифрові комутаційні станції;
- Фрагменти PDH, створені раніше для з'єднання аналогових та цифрових АТС;
- аналогові лінії передачі, які використовуються тільки для зв'язку аналогових АТС.

На рівні мережі доступу основним способом підключення терміналів поки що залишається двопровідна абонентська лінія (АЛ). Слід підкреслити, що модернізація мережі доступу є найскладнішим завданням з точки зору економічних показників відповідного проекту

Вибір структури міської транспортної мережі та технологій, які будуть оптимальні для конкретного проекту – складне завдання. Її рішення не входить до переліку питань, що розглядаються в даному РТМ. Проте, можна уявити фінальну фазу модернізації міської транспортної мережі. На малюнку **2.2.1.1** показано її рекомендовану структуру на ділянці зв'язку комутаційних станцій між собою.

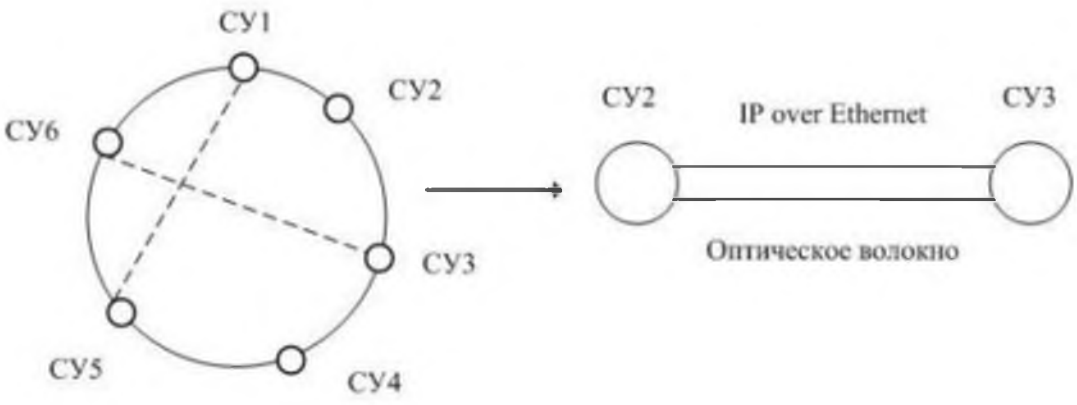

Рис 2.2.1.1– Модель міської транспортної мережі. Міжстанцева ділянка

У лівій частині моделі показано кільцеву структуру, в якій проведено дві хорди – пунктирні лінії між СУ1 та СУ5, а також СУ3 та СУ6. Хорди

дозволяють суттєво підвищити надійність транспортної мережі та пропускну здатність окремих ліній передачі. У правій частині моделі представлений фрагмент транспортної мережі – лінія передачі між СУ2 та СУ3 із зазначенням використовуваних технологій. Для вибраного прикладу використовуються технології "IP over Ethernet", а середовищем передачі служить ВВ. На малюнку **2.2.1.2** зображено модель доступу мережі. Передбачається, що у межах пристанційної ділянки створено чотири кільця - структура типу "ромашка".

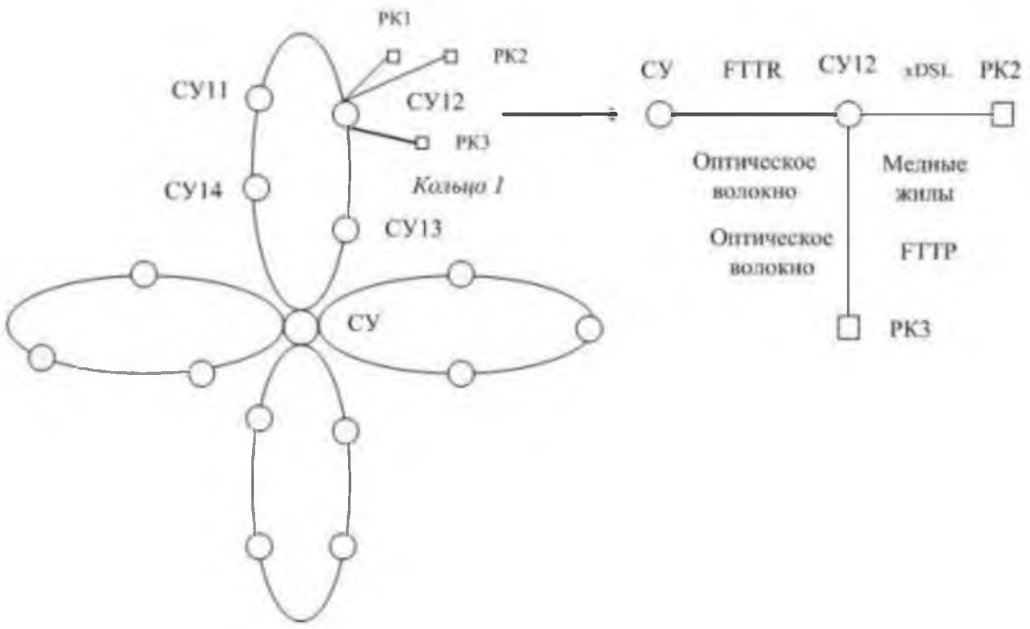

Рис 2.2.1.2– Модель міської транспортної мережі. Ділянка доступу

Для аналізу моделі досить докладно розглянути одне кільце. Для першого кільця показано включення чотирьох СУ, які використовуються для включення різних виносних модулів – УВАТС, концентраторів та інших. Для СУ12 вказано три напрямки, для організації яких використовуються кабелі з мідними жилами. Ці кабелі прокладаються за безшафною системою. і закінчуються у розподільчих коробках (РК).

У правій частині моделі показаний тракт обміну інформацією між СУ та двома РК. Він складається із двох ділянок. На першій ділянці як середовище поширення сигналів завжди використовується ВВ. Така концепція застосування кабелю з ОВ відома по абревіатурі FTTR (доведення ОВ до виносного модуля). До РК2 прокладено кабель із мідними жилами. Якщо мідні жили використовуються для обміну даними за допомогою обладнання xDSL, то на схемі зазвичай вказується назва однойменної технології. Для РК3 показаний варіант доведення кабелю з ОВ. Така

концепція застосування кабелю з ВВ відома в технічній літературі з абревіатури FTTP (доведення ВВ до приміщення користувача).

Рішення, які приймаються у процесі планування міської транспортної мережі, можна розділити на дві групи. Перша група включає рішення, які інваріантні до можливих змін принципів Операторської діяльності. До таких рішень відносяться всі заходи, що стосуються заміни існуючих лінійних споруд на кабелі з ОВ. У другу групу слід включити ті рішення, які критичні як зміни принципів Операторської діяльності, так і до технологічних новинок, що періодично з'являється на ринку телекомунікаційного обладнання.

2.2.2. Транспортні мережі в сільскій місцевості

Одна з особливостей сільських транспортних мереж – наявність застарілих ліній передачі (середовище поширення сигналів, яке не підходить для NGN) та систем передачі (аналогових або цифрових, але нестандартних з точки зору рекомендацій МСЕ). Для модернізації всієї системи сільського зв'язку необхідно провести суттєву реконструкцію транспортних мереж. Ця реконструкція стосується і середовища поширення сигналів та систем передачі. На малюнку ? показана модель сучасної сільської транспортної мережі, якою використовуються практично всі можливі технології. Ця модель ілюструє принципи побудови міжстанційного зв'язку.

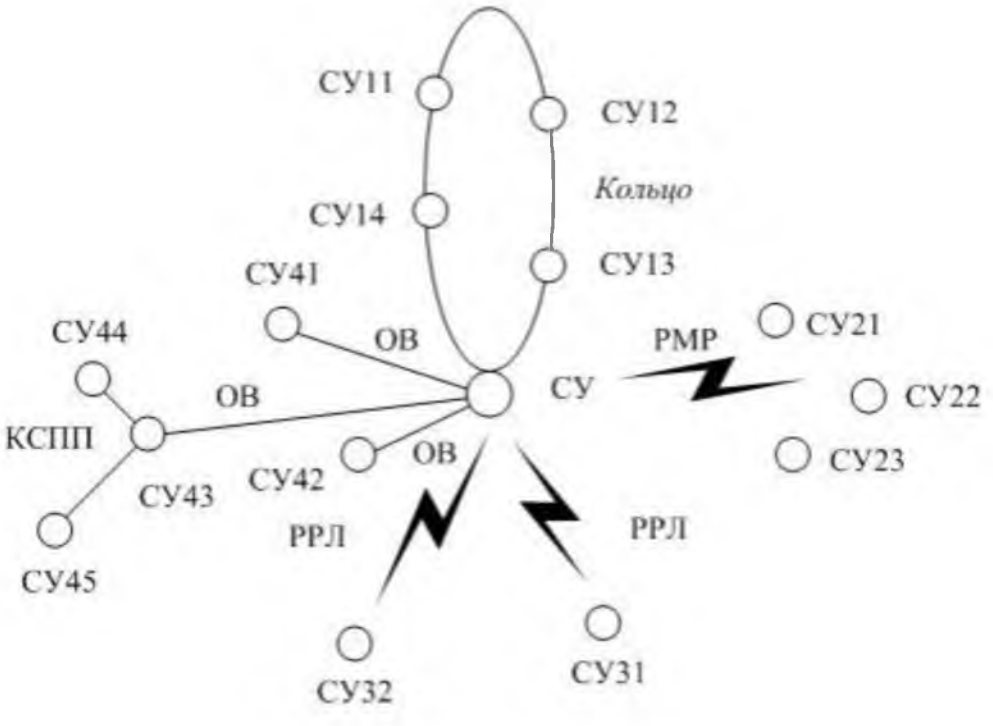

Рис 2.2.1.3 – Модель сільскої транспортної мережі. Міжстанцева ділянка

Обладнання СУ розташоване в одному приміщенні з центральною станцією (ЦС). У напрямку "Північ" розташовані чотири СУ, нумерація яких починається із цифри "1". Ці СУ об'єднані в кільце, реалізоване за рахунок прокладання кабелю з ОВ. Усі чотири СУ призначені для створення транспортних ресурсів між ЦС та кінцевими станціями (ОС). Даний варіант побудови сільської транспортної мережі слід вважати оптимальним, якщо використання кабельних ліній можливе та економічно виправдане.

У напрямку "Схід" лежать три СУ. Їхній зв'язок з СУ, який розташований в одному будинку з ЦС здійснюється за рахунок використання системи бездротового зв'язку, відомого по абревіатурі РМР ("точка - безліч точок"), присвоєної системам множинного доступу. Такий спосіб організації транспортних ресурсів стає все більш популярним, оскільки спрямований на заміну кабельних ліній, що у ряді випадків стає самим ефективним варіантом модернізації системи сільського зв'язку.

У напрямку "Південь" знаходяться два СУ. Транспортні ресурси у цьому напрямі організовані за допомогою двох РРЛ. Таке рішення використовується в сільських транспортних мережах, коли прокладка кабелю неможлива або недоцільна з економічних міркувань. Відмінність від попереднього рішення полягає в тому, що РРЛ стають економічно вигідними, якщо для СУ31 та СУ32 необхідні суттєві транспортні ресурси.

У напрямку "Захід" транспортні ресурси організовані на базі комбінованих провідних засобів. До СУ41, СУ42 та СУ43 прокладено кабель з ВВ. До СУ44 та СУ45 використовується кабель типу КСПП. Це означає, що структура транспортної мережі представляє деревоподібну топологію, тобто має низьку надійність, але для своєї реалізації вимагає мінімальної довжина кабельних ліній.

У принципі, у сільській транспортній мережі можуть використовуватись і тракти супутникового зв'язку. Однак включення цих каналів здійснюється не в той СУ, де розміщується ЦС, а вузол на вищому рівні ієрархії.

Розглянута модель свідчить, що технології можуть застосовуватися в сільських транспортних мережах, утворюють ширший ряд, ніж використовувані у містах. На малюнку ? наведено приклад тих основних технологій, які будуть використовуватись у сільських транспортних мережах.

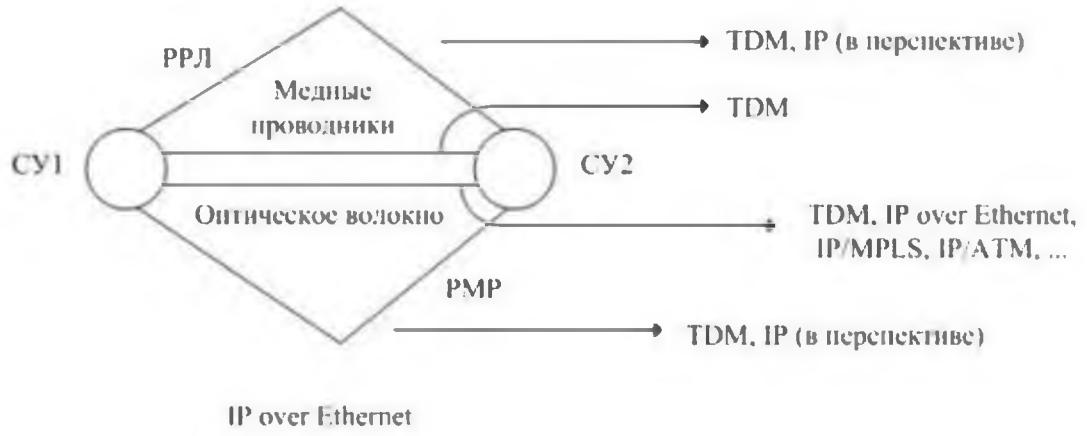

Рис 2.2.1.4– Перспективні технології для сільскої транспортної мережі

РРЛ та системи типу РМР в даний час використовують технологію TDM – тимчасовий поділ каналів. У перспективі обидва ці бездротові типи обладнання транспортної мережі зможуть підтримувати технологію IP. Мова йдеться про широкосмугові варіанти обох систем. Кабелі з ОВ, звичайно, здатні підтримувати будь-які види технологій, які необхідні Операторам та їх клієнтам. Кабелі з мідними провідниками, розраховані на обмежену смугу пропускання, швидше за все, будуть і надалі використовуватись лише для технології TDM.

Це означає, що з погляду технологій перспективними варіантами модернізації сільських транспортних мереж слід вважати кабелі з ВВ та бездротові технології.

На рівні доступу у сільській місцевості також можливі різні рішення. Крім варіантів, показаних у правій частині малюнка 2.2.1.3 застосовуватися вузькосмугові та широкосмугові бездротові засоби доступу. Окрім того, очікується розширення ринку технології PLC – зв'язок по лініях електроживлення. У віддалених пунктах будуть застосовуватись засоби доступу на основі систем супутникового зв'язку. Сектор розвитку МСЕ у результаті проведення серйозних досліджень дійшов висновку, що перспективним рішенням для віддалених пунктів слід вважати технологію бездротового (wireless) IP доступу.

2.2.3. Загальні тенденції розвитку місцевих транспортних мереж

Принципи розвитку місцевих транспортних мереж визначаються трьома групами факторів – організаційних, економічних та технічних.

Економічні фактори, суттєві для рішення Оператора стати учасником ринку Triple Play Service (мова, дані та відео), специфічні для міських та сільських транспортних мереж. Доходи Оператора у містах зазвичай дозволяють проводити якісну модернізацію транспортної мережі, хоча регіональні відмінності дуже помітні. Крім того, питомі витрати на міські транспортні мережі будуть меншими, ніж у сільській місцевості по ряду причин, у тому числі найважливіша – довжини ліній передачі. Положення в сільській місцевості посилюється і меншими доходами, які отримує Оператор.

До **економічних факторів** слід також віднести проблему захисту інвестицій". Справа в тому, що в останні роки тривала реконструкція місцевих транспортних мереж відповідно до концепції, розробленої для технології "комутація каналів" Нові системні рішення завжди повинні враховувати реалізовані проекти, щоб нещодавно встановлене обладнання продовжувало експлуатуватися.

Технічні фактори визначаються конкретними характеристиками тієї місцевості, де розташована мережа, що розглядається, рівнем платоспроможного попиту на нові види інфокомунікаційних послуг, станом та властивостями (потенційні можливості) основних технічних засобів, що знаходяться в комерційної експлуатації.

Аналіз всіх груп факторів є складним завданням, розв'язанням якої здійснюється у процесі проектування інфокомунікаційної системи. Виділення процесу проектування транспортної мережі в окрему (самостійне) завдання загрожує втратою будь-яких вимог з боку комутованих мереж.

2.3. Принципи модернізації місцевих телекоммунікаційних мереж

Для інших видів комутованих мереж характерні такі особливості:

- Мережа телеграфного зв'язку поступово відмирає, а її трафік плавно трансформується у факсимільні повідомлення, дані, e-mail та інші види інформації;
- мережі обміну даними займають свою нішу на ринку послуг, серед яких основна роль відводиться доступу до Інтернету;
- мережі подачі програм звукового мовлення поступово поділяється на два класи – традиційного розподілу та інтерактивного обміну (типу Sound on Demand);
- мережі подачі програм телебачення також поступово поділяється на два класи – традиційного розподілу та інтерактивного обміну (типу Video on Demand).

Мережі розподілу програм мовлення (телевізійного та звукового) можуть використовувати ресурси транспортної мережі за рахунок виділення трактів E1 (у в тому числі дробових), E3 або STM-1. За винятком мереж розподілу програм мовлення інші види трафіку, який є інтерактивним (але не завжди симетричним), можуть бути обслужені IP-мережею з підтримкою QoS. Таким чином, модернізацію комутованої мережі може розглядати як завдання оптимального поєднання всіх видів інтерактивного трафіку.

Рушійними силами цього процесу, у випадку, вважатимуться тенденції розвитку мереж далекого (міжнародного та міжміського) зв'язку та обладнання у приміщенні користувача. На малюнку 2.2.3.1 показані приклади прояви цих тенденцій.

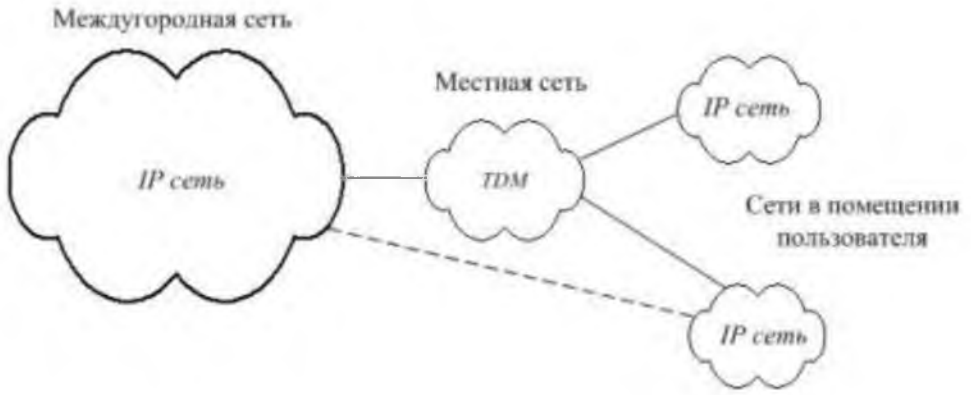

Рис 2.2.3.1 – Діючі сили, стимулючі стоверння IP мереж

Основні витрати Оператора при побудові та експлуатації мереж міжнародного та міжміського зв'язку припадають на транспортні ресурси. Це стимулювало перехід на IP технологію, що дозволяє ефективніше використовувати транспортні ресурси саме для обслуговування трафіку далі зв'язку. В результаті почалося формування так званого ядра IP-мережі. Воно показано у лівій частині малюнка 2.2.3.1.

У правій частині цього ж малюнка зображені дві IP мережі, створені в приміщенні користувачів. Такі мережі організовуються за рахунок встановлення IP-УВАТС або шлюзу, який включає звичайну УВАТС і локальну мережу (LAN). Для потенційних користувачів IP технологія, на відміну від Оператора дальньої зв'язку, приваблива з інших причин: вона дозволяє ефективно вводити послуги типу Triple Play Service, скоротити витрати на підтримку системи виробничого зв'язку, знизити витрати на міжнародні та міжміські з'єднання.

Пунктирною лінією показана можливість прямого зв'язку між IP мережами, що знаходяться на різних рівнях ієрархії. Таке рішення слід рахувати винятком, продиктованим неможливістю чи недоцільністю проходження трафіку через місцеву мережу, яка використовує технологію TDM. Зазвичай, трафік проходить місцеву мережу. Це викликає низку проблем, з яких слід виділити два дуже важливі моменти:

- Експлуатовані місцеві мережі в принципі не можуть обслуговувати мультимедійний трафік;
- Перехід з однієї технології на іншу (IP – TDM – IP) призводить до зниження якості обслуговування та надійності зв'язку.

Нездатність існуючих мереж до обслуговування мультимедійного трафіку призводить до такого виду перетворення трафіку – рисунок 2.2.3.2. У даному прикладі розглядається варіант підтримки послуг Triple Play Service в місцевих мереж.

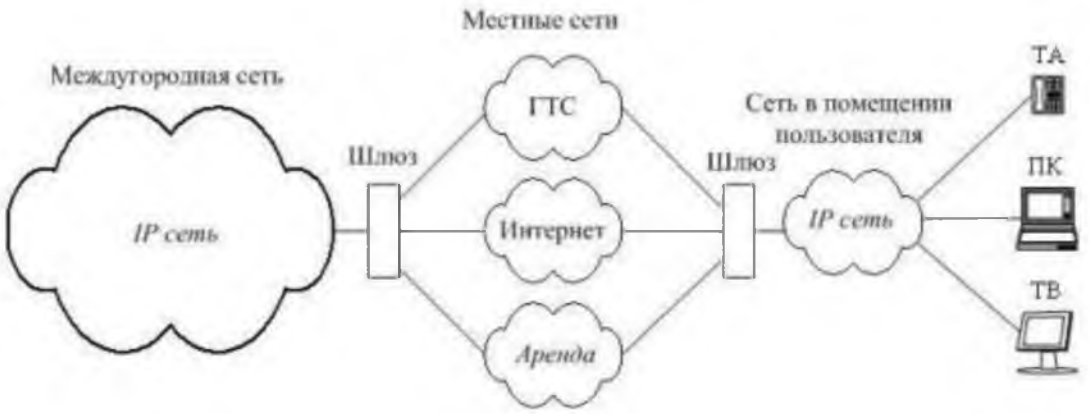

Рис 2.2.3.2 – Діючі сили, стимулюючі створення IP мереж

У правій частині малюнка показано три типи терміналів, що включаються до IP мережа. За допомогою ТА абоненти користуються телефонним та факсимільним зв'язком. ПК служить для обміну даними та виходу до Інтернету. Телевізійний термінал (ТВ) слугує для організації відеоконференції. На виході IP мережі, яка розташована в приміщенні користувача, встановлений шлюз, що виконує функції взаємодії із місцевими мережами.

Для обслуговування трафіку виду Triple Play Service необхідні три типи місцевих мереж:

- міська телефонна мережа (ГТС);

- Інтернет (мережа обміну даними);
- орендовані широкосмугові канали, необхідні передачі відеосигналів (якщо це неможливо реалізувати через Інтернет).

Після того, як усі види трафіку (Triple Play Service) будуть обслужені в місцеві мережі, для організації міжміського з'єднання вони знову будуть перетворені на IP пакети. Очевидно, що таке рішення буде суттєво гальмувати розвиток інфокомунікаційної системи загалом. Тому для місцевих телефонних мереж стає дуже актуальним завдання переходу на IP технологію. Очевидно, що заміна всіх станцій з комутацією каналів на центри обробки IP пакетів не є можливою з низки причин економічного та технічного характеру. Це означає, що мають бути розроблено сценарії поступового переходу до NGN, які дозволяють обслуговувати IP трафік на рівні місцевої мережі без переходу до технології TDM

2.3.1 Городські телефоні мережі

До аналізу можливих сценаріїв модернізації ГТС необхідно розробити оптимальне рішення – структуру моменту завершення процесу побудови NGN. На малюнку 2.2.4.1 показано модель ГТС, яку належить модернізувати. Вона є мережею з семизначною нумерацією, в якій використовуються вузли вихідного (УІС) та вхідних (УВС) повідомлень. У кожному з двох вузлових районів показано по три районні АТС (РАТС)

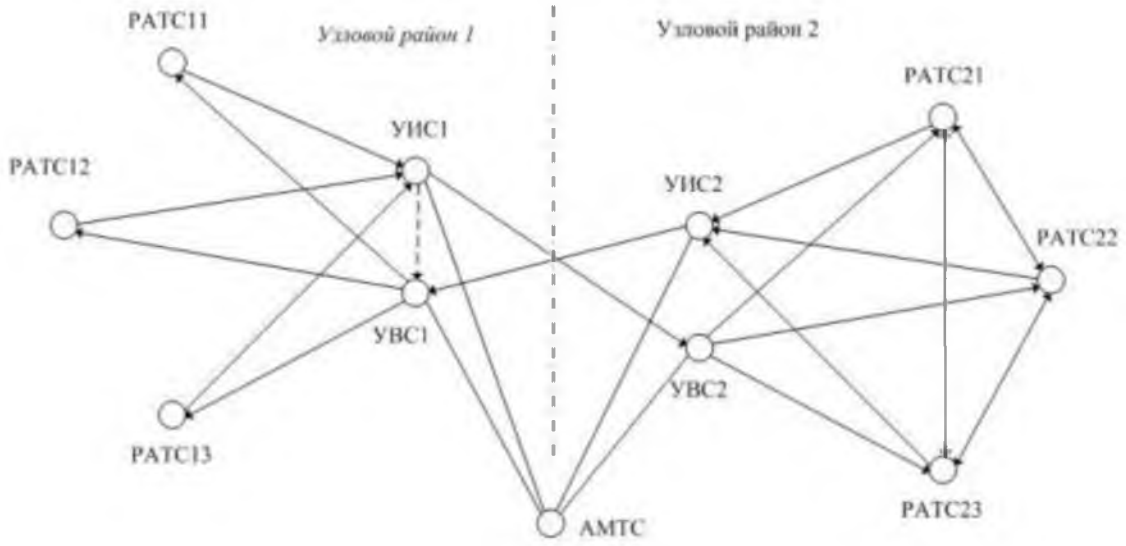

Рис 2.2.4.1 – Модель модернізуємої ГТС з вузлами

Усі РАТС першого вузлового району пов'язані між собою через свої УІВ та УВС. Пучок з'єднувальних ліній між цими вузлами показаний пунктирних

ліній. Всі РАТС другого вузлового району пов'язані між собою по принципом "кожна з кожної". Тому пучок СЛ між УІС2 та УВС не потрібен.

Передбачається, що зв'язок РАТС з автоматичним міжміським телефонним станцією (АМТС) здійснюється через УІС та УВС. Така структура ГТС характерна для великих міст, але модель, що розглядається, універсальна, то є годиться на дослідження процесів модернізації всіх типів мереж.

На малюнку 2.2.4.2 показано модель мережі, яка далі розглядається в як оптимальне рішення. Далі передбачається, що мережа NGN буде відрізнятися як технологіями передачі та комутації, а й структурою.

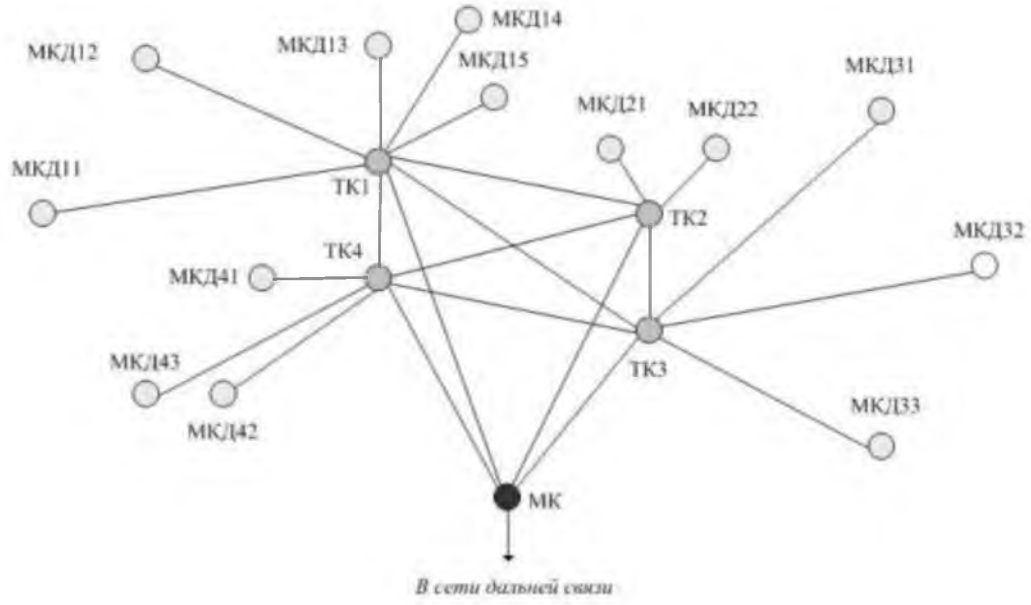

Рис 2.2.4.2 – Оптимальна структура NGN для модернізаційної мережі

Оптимальна структура мережі NGN складатиметься (для обраної моделі). з чотирьох транзитних комутаторів (ТК), пов'язаних за принципом "кожен з кожним". ТК можна розглядати як аналог транзитної станції (вузли вихідного та вхідного повідомлення) у ТФОП.

У кожен ТК включаються мультисервісні комутатори доступу (МКД), який, оперуючи термінологією ТФОП, є кінцевою (опорну) станцію місцевої телефонної мережі. На малюнку показано зіркоподібна топологія зв'язку МКД та ТК, але на рівні транспортної мережі (третій розділ цього РТМ) організуються два незалежні (у сенсі надійності) шляхи передачі інформації між цими вузлами комутації пакетів. Усі ТК пов'язані з магістральним комутатором (МК), який забезпечує вихід у мережі дальнього зв'язку для міжміських та міжнародних з'єднань, тобто є аналогом АМТС.

У результаті створюється трирівнева мережа. В принципі, можливо найбільш вигідним є перехід до дворівневої мережі. Вибір оптимальної кількості ієрархічних рівнів належить до завдань конкретного проектування. Визначення оптимального рішення – самостійне завдання, яке виходить за рамки цього РТМ. Вона може бути вирішена у різний спосіб. Не виключено метод перебору всіх практично допустимих варіантів, оскільки їх число суттєво менше теоретично можливих комбінацій.

На малюнку 2.2.4.3. показано перший етап реалізації програми модернізації існуючої ГТС. Передбачається, що вже функціонує МК, який забезпечує обслуговування IP трафіку лише на рівні мереж телекомунікації. Для підключення IP-УАТС, що з'являються у приміщеннях користувачів, має бути встановлено кілька МКД. Між IP-УАТС та МКД організуються зв'язки за рахунок ресурсів транспортної мережі. Передбачається, що на першому етапі модернізації ГТС обладнання ТК ще використовується.

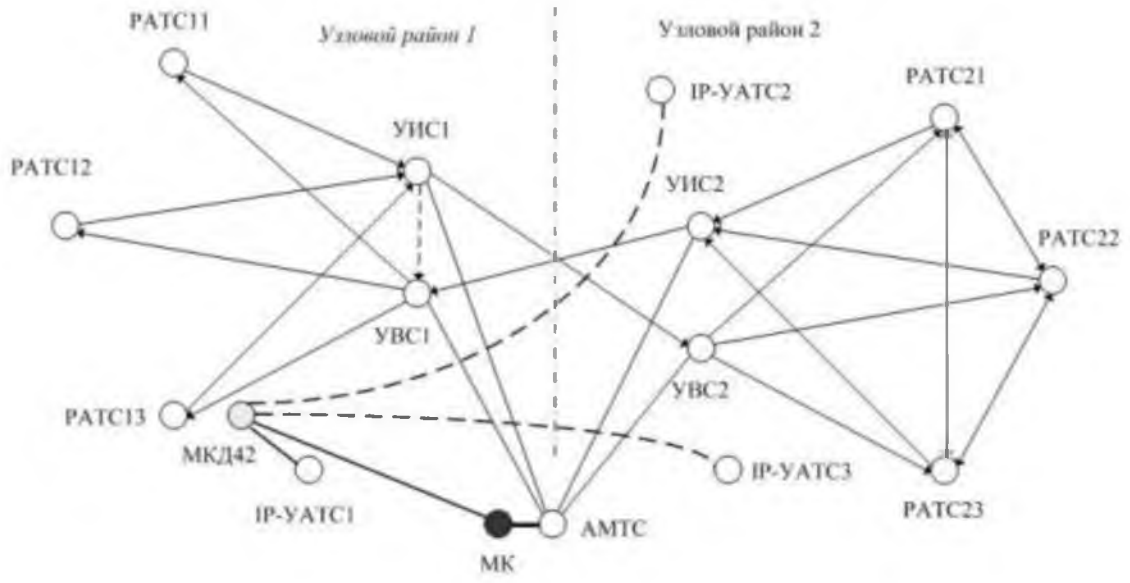

Рис 2.2.4.3 – Перший етап модернізації ГТС з вузлами

Три нововведені IP-УАТС розкидані територією місцевої мережі.

Поки що для їх підключення до IP мережі використовується лише один МКД з номером 42. У зоні його обслуговування розташована лише IP-УАТС1. Дві інші IP-УВАТС з'єднані з МКД42 за рахунок використання спеціально виділених IP ресурсів транспортної мережі. Цей факт зазначено малюнку 2.2.4.3 пунктирними лініями. При введенні інших МКД ті IP-УАТС, які входять до зони їх обслуговування, перемикатимуться. Це означає, що IP-УАТС2 та IP-УАТС3 включені в МКД42 тимчасово.

Через відсутність ТК обладнання МКД42 включається безпосередньо в МК, що забезпечує дві важливі функції. По-перше, МК грає роль транзитної станції для передачі IP пакетів, за необхідності, через мережі телекомунікації. По-друге, МК є шлюзом для зв'язку з ГТС. Така можливість може бути доповнена пристроями прямого зв'язку МКД42 з усіма УІС та УВС. Щоправда, у цьому випадку кількість необхідних шлюзів буде значно більше. Вибір оптимального способу взаємодії мереж, які використовують дві різні технології розподілу інформації, може бути зроблено після традиційних техніко-економічних розрахунків.

Другий етап модернізації ГТС передбачає розширення чисельності встановлених IP-УАТС та розвиток мережі за принципом "ядра, що розширюється".

Цей принцип означає, що ядро IP мережі, яке спочатку формується на міжнародному та міжміському рівнях, розширює свої кордони за рахунок транзитних вузлів ГТС Це означає, що необхідно розпочати заміну ДВС та УВС.

Ідеальне рішення – заміна всіх УІВ та УВС на МК. Такий підхід, що нагадує процедуру переходу з шестизначного на семизначний план нумерації (принаймні, з організаційної точки зору), спрощує процес модернізації мережі. Щоправда, він вимагає концентрації фінансових засобів, необхідних для закупівлі та монтажу обладнання МК. Якщо ж розтягнути процес заміни УІВ та УВС на деякий період часу, то для роботи ГТС знадобиться більше шлюзів за рахунок їх встановлення на ділянках між МК та УІС/УВС. У будь-якому випадку структура ГТС на другому На етапі її модернізації буде ідентичною. Вона представлена малюнку 2.2.4.4. МК у цій мережі повністю замінює АМТС. Відбувається також перемикання однієї з IP-УАТС до найближчого МКД. МКД42 перемикається у ТК4; його прямий зв'язок з МК може залишитися як резервний напрямок обміну IP пакетами.

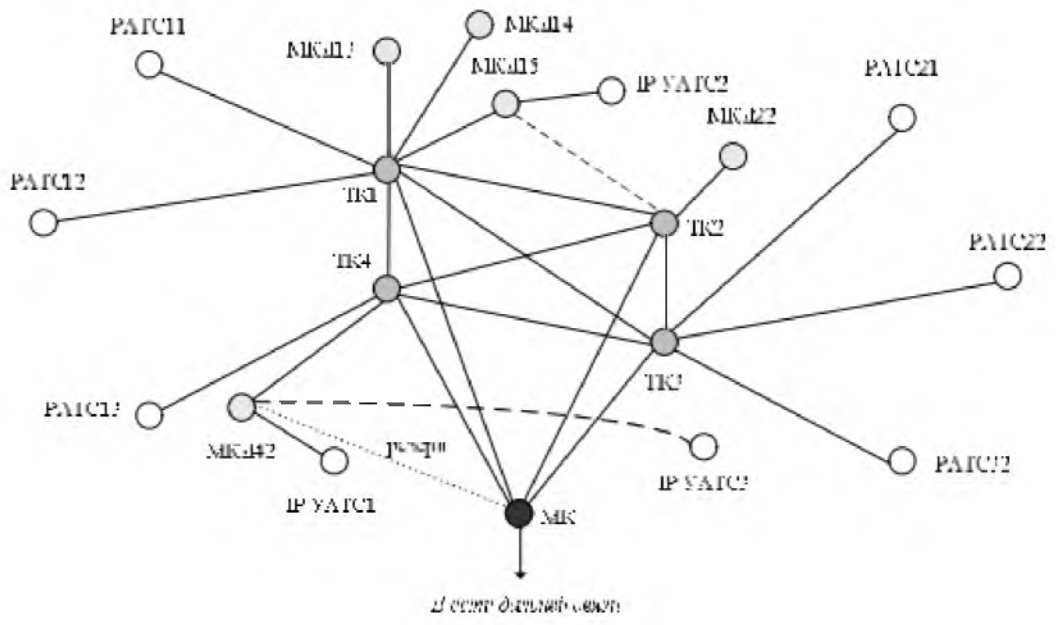

Рис 2.2.4.4 – Другий етап модернізації ГТС з вузлами

РАТС, що залишилися в експлуатації, виконують свого роду функції вузлів доступу до мережі IP. Ці станції концентрують телефонне навантаження для більш ефективної роботи IP мережі. На малюнку 2.2.4.4. показано запровадження ряду нових МКД, що дозволяють підключити до IP мережі тих користувачів, яким потрібні нові види інфокомунікаційних послуг.

Наступний етап модернізації ГТС полягає у поступовій заміні всіх РАТС. Цей процес не потребує концентрації фінансових ресурсів. Наявність деякого числа МКД дозволяє підключати всі IP-УВАТС та інші сучасні засоби, розміщені у приміщенні користувачів, до IP мережі. У результаті ГТС трансформуватиметься у мережу, показану малюнку 2.2.4.2.. Ця модель ілюструє оптимальну структуру мультисервісної мережі, відповідну ідеології NGN.

Можливі інші сценарії модернізації ГТС, які можуть виявитися більш ефективними для тієї ситуації, коли обладнання деяких РАТС вимагає якнайшвидшої заміни. Наприклад, якщо всі станції другого вузлового райони були побудовані на базі декадно-крокового обладнання, то їх слід демонтувати одночасно із заміною УІВ та УВС (другий етап модернізації ГТС, рисунок 2.2.4.4.). На майданчиках РАТС21, РАТС22 та РАТС23 доцільно встановити МКД.

Для районованої ГТС без вузлів принципи переходу до NGN будуть іншими. Необхідність встановлення обладнання ТК відсутня. У лівій частини

малюнка 2.2.4.5. показано структуру районованої ГТС, яка складається з шести РАТС. Усі комутаційні станції пов'язані між собою за принципом "Кожна з кожної". У правій частині цього ж малюнка наведено оптимальну структура NGN, що утворена трьома МКД. Для побудови мережі доступу в кожен МКД включено кілька МАК.

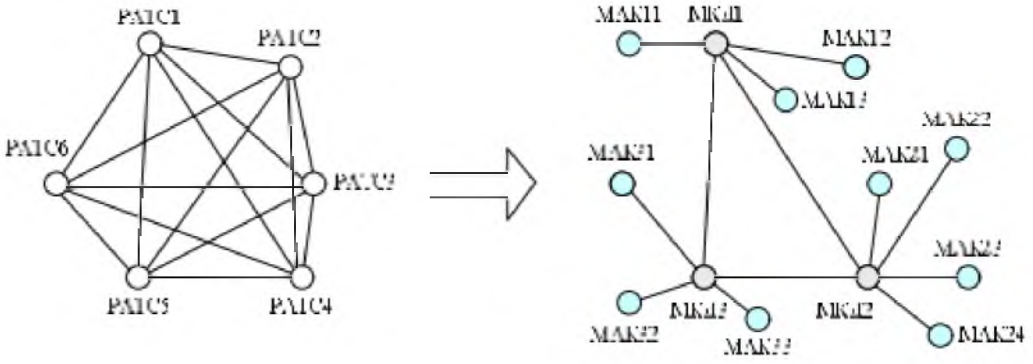

Рис 2.2.4.5 – Модель ГТС без вузлів і результат модернізації

Безліч всіх можливих варіантів переходу до оптимальної структури NGN для моделі невелика. В принципі, можна використовувати метод перебору допустимих рішень. Оператор зазвичай може визначити розумний порядок заміни РАТС.

Припустимо, що у розглянутій ГТС насамперед доцільно замінити РАТС4. На цьому місці планується встановлення МКД2, до якого будуть включені чотири концентратори. Послідовність підключення МАК22, МАК23 та МАК24 може бути будь-який. Цікаве питання про час заміни РАТС3, абонентів якої (всіх або деяку частину) буде обслуговувати Мак21. Можливі два варіанти:

- РАТС3 та РАТС4 замінюються одночасно, що мінімізує обсяг шлюзового обладнання, що встановлюється у ГТС;
- Спочатку замінюється тільки РАТС4, що має на увазі встановлення шлюзу між МКД2 та РАТС3.

Вибір оптимального рішення здійснюється за рахунок технікоекономічного аналізу двох можливих варіантів першого етапу модернізації районованої ГТС без вузлів На малюнку 2.2.4.6 показаний перший з перерахованих вище варіантів. На чотирьох напрямках (від МКД2 до РАТС1, РАТС2, РАТС5 та РАТС6) треба встановити шлюзи, що забезпечують взаємодія технологій комутації.

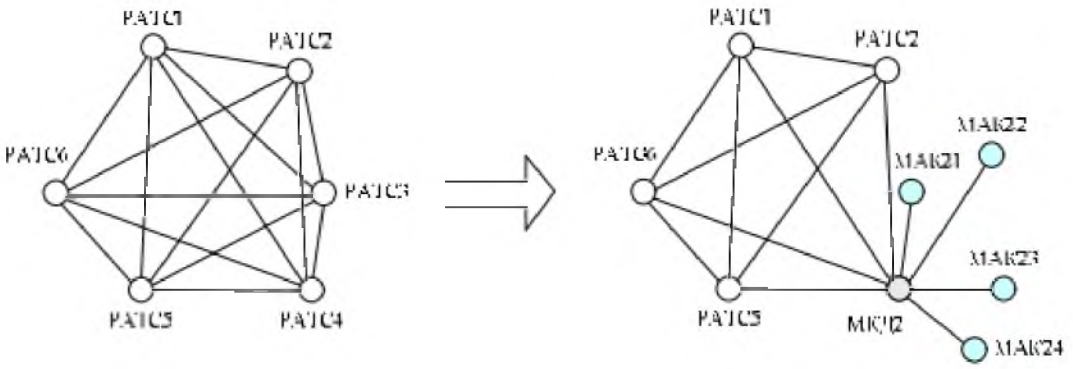

Рис 2.2.4.6 – Перший етап модернізації ГТС без вузлів

Подальша модернізація ГТС передбачає заміну інших РАТС. На малюнку 2.2.4.7, правий фрагмент, показано структуру ГТС після заміни РАТС1 та РАТС2.

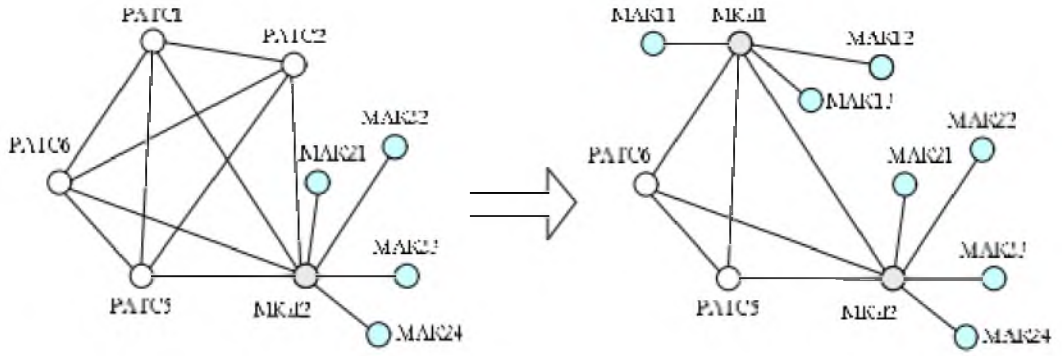

Рис 2.2.4.7 – Другий етап модернізації ГТС без вузлів

Останній етап модернізації ГТС без вузлів – заміна РАТС5 та РАТС6. У в результаті формується структура мережі, показана у правій частині малюнка 2.2.4.5. Вона була обрана як оптимальне рішення, що мінімізує витрати Оператора.

Сценарії модернізації ГТС можуть також відрізнятися темпами заміни експлуатованого комутаційного обладнання, чисельністю МКД та ТК у IP мережі та інші особливості. Для аналізу цих сценаріїв доцільно розробити пакет програм. Крім того, необхідно провести паспортизацію використовуваних технічних засобів, представивши результати роботи у вигляді файлів, які будуть використовуватись при аналізі сценаріїв модернізації ГТС.

2.3.1. Інтернет (Аспекти доступу)

В аналогових ГТС та СТС доступ до Інтернету можливий з комп'ютерів, включені через модем. Через мережу, що комутується, необхідно встановити з'єднання з модемним пулом Інтернет-провайдера (ISP). Звичайно, що швидкість обміну даними буде обмежена кількома десятками кбіт/с.

Для індивідуальних користувачів мережі Інтернет, яким потрібний високошвидкісний доступ, може бути використане обладнання ADSL – асиметрична цифрова ал. В цьому випадку в кросі комутаційної станції або концентратора встановлюється мультиплексор ліній ADSL – DSLAM. Він забезпечує високошвидкісний доступ до Інтернету. Аналогічно у процесі модернізації ГТС та СТС вирішуються і низка інших проблем, пов'язаних з підтримкою нових інфокомунікаційних послуг.

Для корпоративних користувачів мережі Інтернет практичний інтерес представляє доступ до ресурсів Інтернету через локальну мережу Ethernet

На рисунку 2.2.5.1 показаний типовий варіант підключення шкільних ПК до Інтернет. Передбачається, що всі комп'ютери об'єднані в локальну мережу Ethernet. Інші варіанти об'єднання комп'ютерів в даний час не використовуються.

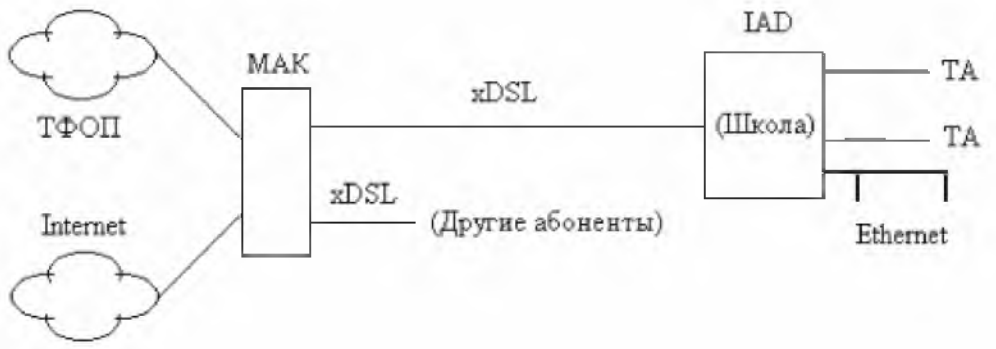

Рис 2.2.5.1 – Організація доступу в Інтернет в сільских школах

Для організації зв'язку в школі ідеально підходять інтегровані пристрої абонентського доступу IAD. Зазвичай IAD підключаються 8 ТА і одна локальна мережа Ethernet. На малюнку 4.14 показано зв'язок IAD з МАК по цифрової лінії типу xDSL. Символ х означає, що може використовуватися будь-який стандарт передачі цифрових сигналів по многопарным кабелям. устаткування МАК поділяє трафік мови та даних, спрямовуючи його до ТФОП або Інтернет.

2.4 Принципи використання коммутаторів Softswitch для створення мультисервісних мереж

Комутатор Softswitch – один із основних елементів NGN. В даний час у вітчизняній технічній літературі ще немає загальноприйнятого перекладу терміну "Softswitch" (можна знайти такі варіанти: програмний, гнучкий, інтелектуальний комутатор та інші визначення), ні точного переліку функцій, що виконують відповідні апаратно-програмні засоби.

Певна неясність у переліку тих функцій, які виконує комутатор Softswitch пояснюється тим, що концепція NGN ще тільки формується. У У процесі розвитку телефонії також існували різні думки про поділ функцій між комутаційними станціями та іншими видами обладнання (вузлами спецслужб, центрами технічної експлуатації, центрами розрахунку абонентами та іншими). Більше того, у процесі цифровізації ТФОП функції аналого-цифрового перетворення перейшли із систем передачі в абонентські комплекти комутаційних станцій

Відмінність у принципах побудови мереж з комутацією каналів та пакетів – як і однойменних технологій – не дозволяє провести просту аналогію між комутатором Softswitch та обладнанням розподілу інформації, яке використовується у ТФОП. Це пояснюється тим, що у комутаторах Softswitch часто використовується комплекс функцій, які в ТФОП розподілені між комутаційними станціями, вузлами Інтелектуальної мережі (ІВ), засобами обробки сигнальної інформації (включаючи відповідні конвертори), пристроями управління мережею електрозв'язку, а також іншими елементами інфокомунікаційної системи.

Щоправда, комутатори Softswitch іноді порівнюють із обладнанням ТФОП класу V або IV, але така відповідність справедлива, в основному, з точки зору того рівня ієрархії, що він займає у мережі. Спільність Softswitch із сучасними комутаційними станціями ТФОП полягає також у поділу функцій надання послуг (транспорт, комутація) та формування послуг (обробка дзвінків за заданими правилами). З функціональної точки зору комутатор Softswitch можна розглядати як апаратно-програмні засоби для управління викликами в тех телекомунікаційних мереж, які використовують технології IP та/або ATM.

В ідеалі Softswitch має підтримувати всі відомі протоколи IP телефонії – MGCP, H.248 (MEGACO), SIP, H.323 – та здійснювати їх конвертацію. Крім того, Softswitch, у ряді випадків, має підтримувати сімейство протоколів SIGTRAN, що використовуються для сигналізації в мережах IP телефонії. Також можуть підтримуватися різні види систем сигналізації,

використовуються у ТФОП. Для цього доводиться встановлювати спеціальні шлюзи сигналізації.

Багато операторів вже використовують апаратно-програмні засоби, що входять також до складу класичного комутатора Softswitch. Для таких Операторів велике практичне значення має розподілене (або модульне) обладнання Softswitch, яке дозволяє економічно створювати та розвивати IP мережу, набуваючи тільки відсутні апаратно-програмні кошти. Такий підхід, зокрема, був використаний НТЦ "Протей" при розроблення МКД, який може розглядатися як розподілений Softswitch – рисунок 2.3.1.

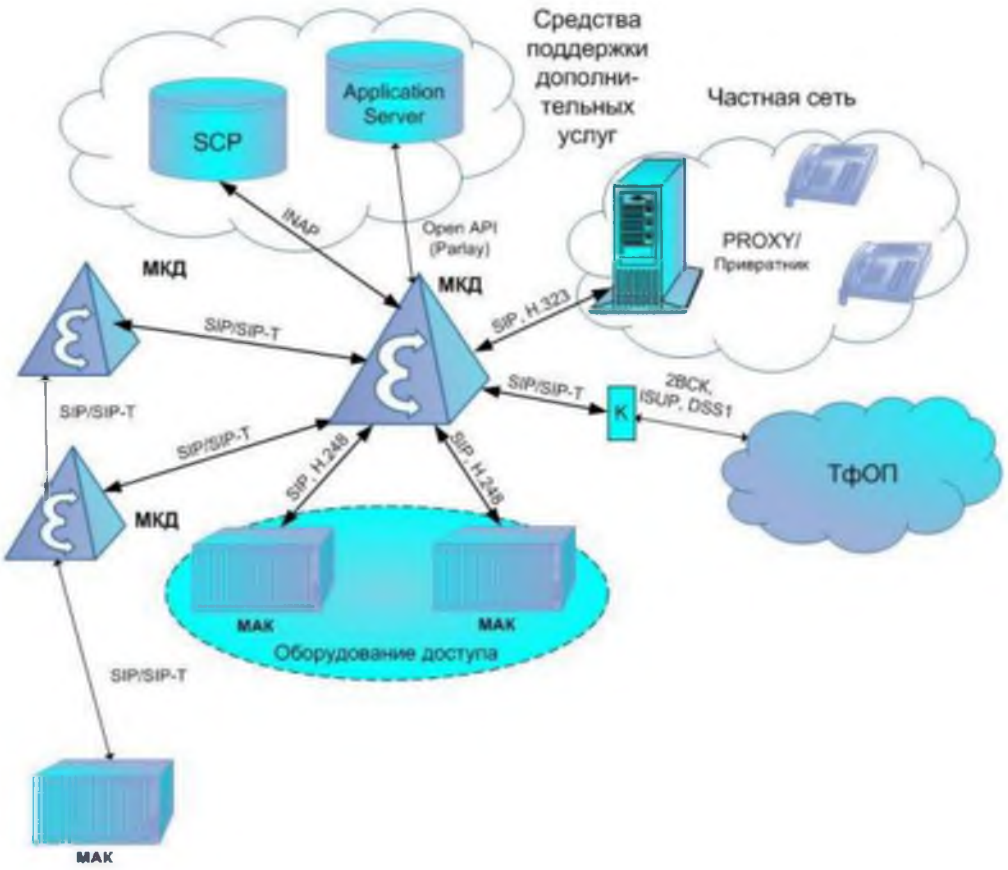

Рис 2.3.1 – Приклад використання комутатора Softswitch

У лівій нижній рисунку 2.3.1 показаний фрагмент пакетної мережі, в якій МКД забезпечують підключення МАК. Системи сигналізації, що використовуються розглядаються у наступному параграфі. МКД через конвертер сигналізації (К) взаємодіє з ТФОП. Він також може забезпечувати підключення будь-якої приватної мережі (через PROXY / Брамник, що використовує пакетні технології). Крім того, МКД здатний підтримувати додаткові послуги, надані як Інтелектуальною мережею, так і серверами додатків (Application Server)

2.4.1 Системи сигналізації в NGN

Поява кожного наступного покоління обладнання комутації супроводжується розробкою нових систем сигналізації. Наприклад, створення станцій із програмним управлінням породило системи сигналізації МСЕ №6, МСЕ №7, E-DSS та ряд інших, які не знайшли широкого застосування. Усе нові види комутаційного обладнання повинні взаємодіяти з експлуатованими станціями, які зазвичай використовують кілька систем сигналізації. З цієї причини ускладнення комутаційних взаємодій станцій (тобто зростання витрат Оператора), які відносяться до різних поколінням обладнання, визначається чисельністю застосовуваних систем сигналізації. В даний час для пакетних мереж запропоновано безліч систем сигналізації. Частина цих систем сигналізації має несуттєві відмінності. Тому реалізація в обладнанні всіх можливих видів систем сигналізації не видається доцільною.

Якщо в мережі NGN, яка базується на якісно новому поколінні систем комутації, буде мінімізовано перелік використовуваних систем сигналізації, то вирішуються дві важливі завдання:

- спрощується взаємодія NGN з мережами, що експлуатуються. зв'язку (зокрема, з ТФОП);
- зменшуються витрати Оператора створення NGN з допомогою те, що спрощуються процеси взаємодії окремих елементів мережі.

На малюнку 2.3.2 показаний фрагмент доступу мережі NGN, побудований на обладнання МАК і МКД, що використовують технологію "комутація пакетів". МАК виконує функції транспортного шлюзу (Media Gateway), а МКД – Softswitch. Взаємодія МАК з МКД здійснюється за протоколом SIP або H.248.

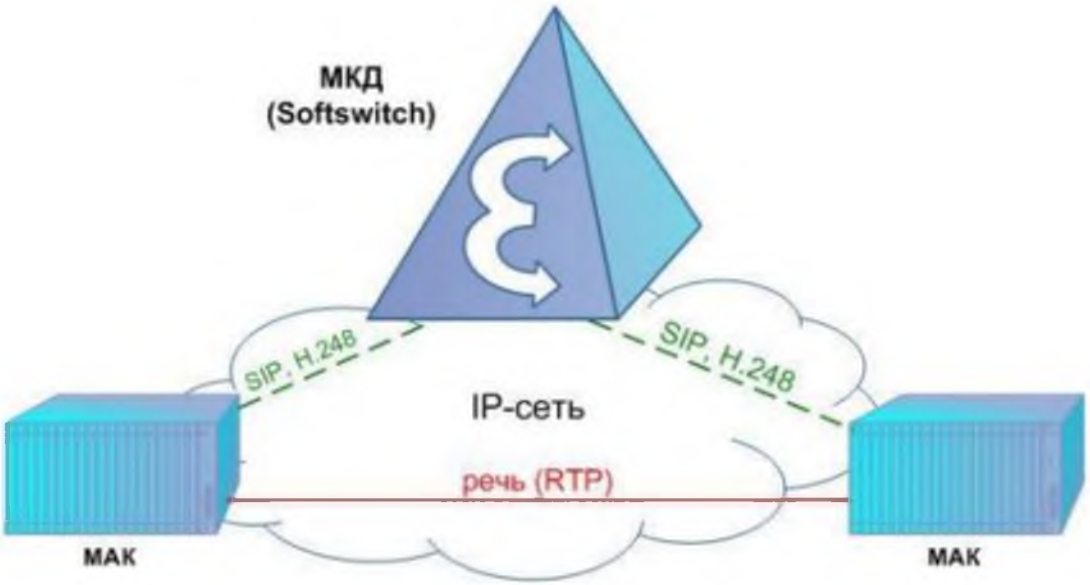

Рис 2.3.2 - Взаємодія МКД та МАК в мультисервісній системі

Під управлінням Softswitch, що входить до складу МКД, між двома МАК здійснюється сесія обміну мовними пакетами. В даному випадку обмін пакетами здійснюється за транспортним протоколом реального часу (RTP). Тракт обміну інформацією між МАК слід розглядати як логічний зв'язок концентраторів. Реальний (фізичний) шлях передачі інформації може проходити через кілька складових трактів транспортної мережі. Процес обміну мовними пакетами зазвичай називають RTP-сесією.

Рекомендації щодо використання протоколу SIP або H.248 для взаємодії МАК та МКД обґрунтовані результатами аналізу всіх можливі рішення. Один із суттєвих аспектів ефективного використання нового обладнання – мінімізація витрат на поєднання з засобами передачі і комутації, що залишаються в експлуатації. Показано, що це завдання може бути вирішене за рахунок вибору оптимального сценарію переходу до NGN. Такий сценарій може бути реалізований тільки в тих апаратно-програмних засобах, у яких було закладено можливість ефективного переходу до NGN, включаючи підтримку функцій розподіленого комутатора Softswitch.

2.4.2 Рекомендації щодо переходу до NGN

Ідеальна стратегія переходу до NGN може бути представлена такою послідовністю дій Оператора:

- спочатку міжнародна та міжміська телефонні мережі переводиться на технологію "комутація пакетів";
- потім усі комутаційні станції місцевих мереж замінюються комутаторами пакетів;
- після цього технологія "комутація пакетів" використовується у мережах доступу;
- в останню чергу технологія "комутація пакетів" застосовується в обладнанні користувачів.

На практиці така стратегія не є практично значущою ряду об'єктивних причин, серед яких слід виділити дві обставини. По-перше, суттєва потреба у пакетних технологіях формується саме користувачами (характерний приклад – перехід до IP УВАТС). Це означає, що потенційні абоненти не чекатимуть завершення процесів модернізації міжміської та місцевих мереж. По-друге, необхідність заміни експлуатованого комутаційного обладнання більш актуальна для місцевих мереж, включаючи ділянку доступу. До речі, більшість АМТС були встановлені нещодавно, для чого використовувалося цифрове комутаційне обладнання. Це означає, що необхідність захисту

інвестицій, зроблених Оператором стимулює використання обладнання NGN у місцевих мережах.

У таких випадках можлива низка переходів з технології "комутація" каналів" на технологію "комутація пакетів" у межах одного з'єднання. На малюнку 2.3.2.1показаний приклад з'єднання, в якому використовується чотири переходу з однієї технології в іншу. Відповідні точки відмічені квадратиками, розташованими між мережами

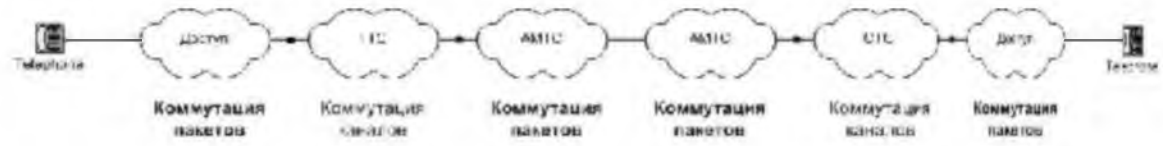

Рис 2.3.2.1 – Приклад з’єднання з чотирьма змінами технологій

Передбачається, що в обох мережах доступу, а також у міжміській мережі використовується технологія IP. Обидві місцеві мережі (ГТС та СТС) побудовані на базі цифрових АТС. Слід зазначити, що розглянута модель не представляє "найгірший" випадок з усіх можливих у національній ТФОП. Очевидно, що якість передачі мови в такій мережі буде не високою. Такий висновок можна зробити на основі простих оцінок затримки мовних сигналів, яка буде відбуватися в кожному фрагменті мережі зв'язку, який використовує технологію "Комутація пакетів".

Розумним виходом із подібних ситуацій можуть стати такі види комутаційного обладнання, які здатні ефективно працювати поза Залежно від виду технології. Характерним прикладом такого обладнання можна вважати МАК, який здатний використовувати технологію "комутація" каналів" з включенням в опорну АТС по стику V5.2 або технологію "комутація пакетів", взаємодіючи з відповідним комутатором протоколу SIP. На малюнку 2.3.2.2 показаний приклад ефективного переходу до NGN за рахунок використання обладнання МАК, МКД та сукупності шлюзів (ITG).

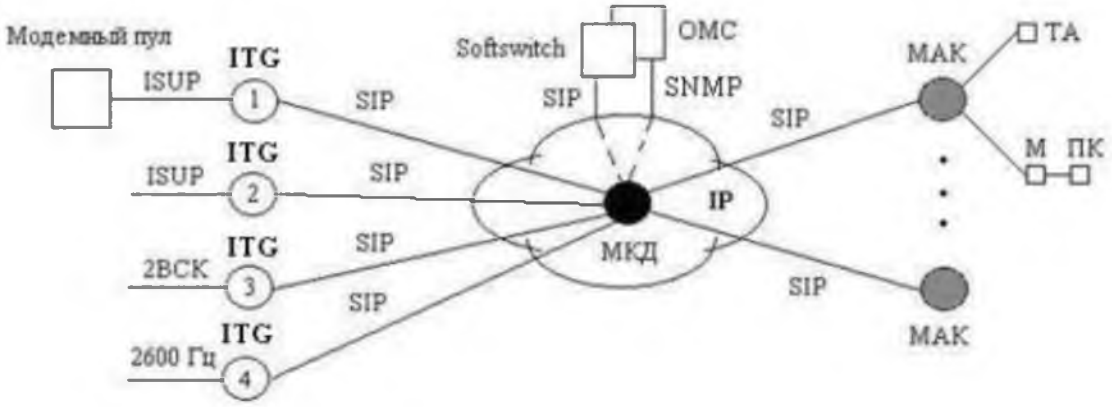

Рис 2.3.2.2 – Приклад переходу к NGN на базі МАК, МКД та шлюзів

Для взаємодії обладнання МАК та МКД застосовується стандартний протокол SIP. Устаткування технічного обслуговування (ОМС) для збору аварійних сигналів, контролю стану апаратно-програмних засобів та ведення статистики використовує SNMP – простий протокол керування мережею. Для інших завдань технічної експлуатації зазвичай використовують процедури (у тому числі протоколи), які оптимальні для конкретного виду обладнання.

Природно, подальший розвиток фрагмента місцевої мережі має здійснюватися так, щоб найближчим часом сформувалася однорідне IP середовище (хмара малюнку 2.3.2.2), що становить основу NGN. Тому для зв'язку МКД із експлуатованими комутаційними станціями доцільно встановити шлюзи (ITG). Ці шлюзи забезпечують функції взаємодії з будь-якими (за типом обладнання та за рівнем ієрархії) станціями ТФОП за рахунок підтримки сигналізації по 2ВСК, ISUP та на частоті 2600 Гц (для зв'язку з АМТС аналоговими каналами внутрішньозонової мережі).

Дуже ефективне використання шлюзів забезпечується тим, що вони складаються з тих же апаратно-програмних засобів, які застосовуються для побудови МАК та МКД – малюнок 2.3.2.3. Для наступної заміни старих комутаційних станцій на МАК в обладнання шлюзу необхідно лише додати деякі плати та відповідне програмне забезпечення.

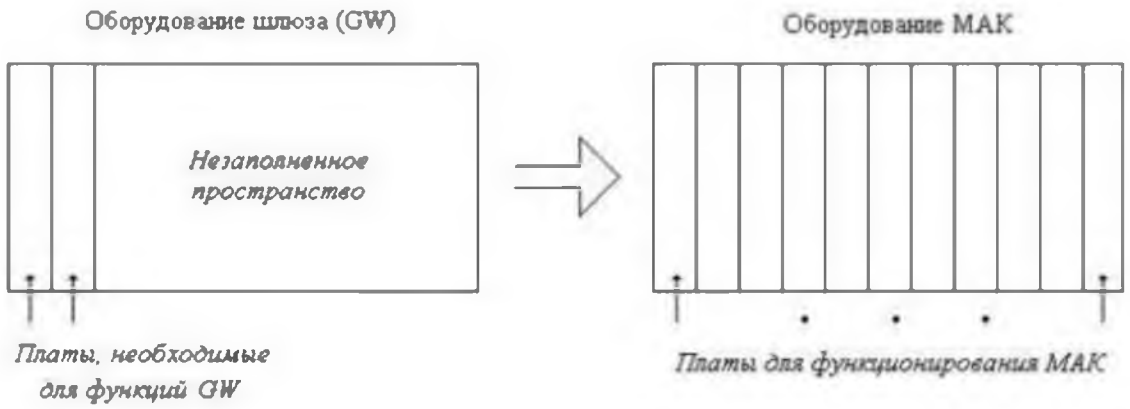

Рис 2.3.2.3 – Принципи зміни шлюза в МАК

Таке рішення означає, що шлюзи – на відміну більшості конверторів, що використовуються нині – при модернізації мережі не викидаються, а перетворюються на МАК. Це означає, що Оператор не вкладає фінансові кошти в обладнання, яке доводиться демонтувати до закінчення термін його служби. Цей підхід забезпечує зниження витрат Оператора модернізацію своєї телефонної мережі.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Метою виконання економічного розділу є визначення того, чи буде доцільним розробка методики покращення характеристик телекомунікаційних систем. На основі розрахованих показників можна буде визначити розмір капітальних витрат та експлуатаційних витрат, які необхідні для розробки та впровадження методики покращення характеристик телекомунікаційних систем, а також річний економічний ефект від впровадження даної програми. На основі розрахунків можна бути зробити висновок, чи є доцільним розробка та впровадження методики покращення характеристик телекомунікаційних систем.

3.1. Розрахунок капітальних витрат на придбання і налагодження системи ІБ або витрат, що пов'язані з виготовленням апаратури, приладів, програмного забезпечення методики покращення характеристик телекомунікаційних систем

Трудомісткість створення методики покращення характеристик телекомунікаційних систем визначається тривалістю кожної робочої операції:

$$t = t_{\text{тз}} + t_{\text{в}} + t_{\text{пр}} + t_{\text{д}}\text{, годин} \quad (3.1)$$

Де $t_{\text{тз}}$ – тривалість складання технічного завдання на розробку методики. год

$t_{\text{в}}$ – тривалість вивчення ТЗ, літературних джерел за темою, тощо . год

$t_{\text{пр}}$ – тривалість розробки методики та засобів. год

$t_{\text{д}}$ – тривалість документування та оформлення результатів. год

$$t = 30 \text{ год} + 75 \text{ год} + 160 \text{ год} + 160 \text{ год} = 425 \text{ год}$$

Витрати на розробку методики покращення характеристик телекомунікаційних систем на промисловому підприємстві $К_{пр}$ складаються з витрат на заробітну плату спеціаліста з ІБ (розробника методики) $З_{зп}$ і вартості витрат машинного часу, що необхідний для розробки методики покращення характеристик телекомунікаційних систем на підприємстві $З_{мч}$ за формулою 3.2:

$$К_{пр} = З_{зп} + З_{мч}, грн \quad (3.2)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальні потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою 3.3:

$$З_{зп} = t * З_{іб}, грн \quad (3.3)$$

де t – загальна тривалість розробки методики покращення характеристик телекомунікаційних систем на промисловому підприємстві, год;

$З_{іб}$ – средньогодинна заробітна плата спеціаліста з ІБ з нарахуваннями, грн/год.

$$З_{зп} = 400 * 210 = 84\,000 грн$$

Вартість машинного часу для розробки методики покращення характеристик телекомунікаційних систем персоналу на ПК визначається за формулою 3.4:

$$З_{мч} = t_{пр} * С_{мч} + t_{д}, год \quad (3.4)$$

де $t_{пр}$– трудомісткість методики покращення характеристик телекомунікаційних систем на ПК , год;

$t_{д}$, – тривалість документування та оформлення результатів, год;

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

Вартість 1 години машинного часу ПК визначається за формулою 3.5:

$$С_{мч} = P * t_{нал} * C_{е} + \left(Ф_{зал} * \frac{H_a}{F_p}\right) + \left(K_{лпз} * \frac{H_{апз}}{F_р}\right), грн$$

(3.5)

де P – встановлена потужність ПК, кВт;
$t_{нал}$ – кількість задіяних робочих станцій при розробці програми, год;
$C_{е}$– тариф на електричну енергію, грн/кВт*год;
$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн;
H_a– річна норма амортизації на ПК, частки одиниці;
$H_{апз}$ – річна норма амортизації на ліцензійне ПЗ, частки одиниці;
$K_{лпз}$ – вартість ліцензійного ПЗ, грн;
F_p – річний фонд робочого часу (за 40–годинного робочого тижня Fp=1920).

На промислових підприємствах середня потужність дорівнює P = 0,4, а тариф на електричну енергію становить 1,44 грн/кВт*год, отже:

$$К = К_{пр} + К_{зпз} + К_{рп} + К_{аз} + К_{дм} + К_{навч} + К_{н}$$

де $К_{пр}$ – вартість розробки програми підвищення рівня обізнаності та залучення для цього зовнішніх консультантів, тис.грн. Сторонні організації не наймалися, тому даний коефіцієнт не враховується при розрахунках;
$К_{зпз}$ – вартість закупівель ліцензійного основного та додаткового ПЗ, складає 2000 грн (програма WordPress);
$К_{рп}$ – вартість розробки програми підвищення обізнаності складає 28 500 грн;
$К_{аз}$ – вартість закупівлі апаратного забезпечення, грн. Для даної програми покупка апаратного забезпечення не потрібна;
$К_{дм}$ – вартість допоміжних матеріалів: 10 плакатів (150 грн/шт);
$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, грн. Дані витрати не враховуються під час розрахунку формули, тому що фахівці не проходили платного навчання.
$К_{н}$ – витрати на встановлення обладнання та налагодження системи ІБ, грн. Даних витрат не було, оскільки програма націлена на підвищення рівня знань у працівників підприємства.

$$К = 85\,046,5 + 2\,000 + 28\,500 + 1\,500 = 117\,046,5 \text{ грн}$$

3.2. Розрахунок витрат на розробку методики покращення характеристик телекомунікаційних систем

Річні поточні (експлуатаційні) витрати на функціонування програми підвищення обізнаності складають:

$$С = С_в + С_к + С_{ак}, грн \quad (3.7)$$

де $С_в$ – вартість відновлення й модернізації системи;
$С_к$ – витрати на курування програмою в цілому;
$С_{ак}$ – витрати, викликані активністю користувачів.

Витрати на керування програмою підвищення обізнаності персоналу складають:

$$С_к = С_н + С_а + С_з + С_{ел} + С_{єв} + С_{тос}, грн \quad (3.8)$$

Річний фонд амортизаційних відрахувань ($С_а$)

$$С_а = \frac{15 * 24\,500}{5} + \frac{50\,000}{10} = 78\,500 грн$$

Річний фонд заробітної плати персоналу, що обслуговує програму ($С_з$) складає:

$$С_з = З_{осн} + З_{дод}, грн \quad (3.9)$$

Основна заробітна плата спеціаліста з телекомунікації на місяць – 20 000 грн, додаткова заробітна плата – 8% від основної зарплати:

$$С_з = 20\,000 * 12 + 20\,000 * 12 * 0{,}08 = 259\,200 грн$$

Ставка ЄСВ для всіх категорій платників складає 22%:

$$С_{єв} = 259\,200 * 0{,}22 = 57\,024 грн$$

Вартість електроенергії, що споживається протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = P * F_p * Ц_е, грн \quad (3.10)$$

де Р – встановлена потужність ПК, кВт;
$Ц_е$, – тариф на електричну енергію, грн/кВт*год .
F – річний фонд робочого часу

$$С_{ел} = 1 * 1920 * 2{,}14 = 4\,108{,}8 грн$$

Витрати на технічне й організаційне адміністрування програми визначаються в відсотках від капітальних витрат – 2% ($С_{тос}$ = 117 046,5 * 0,02 = 2 340,9 грн).

Витрати на керування методики покращення характеристик телекомунікаційних систем ($С_к$) дорівнюють:

$$С_к = 32800 + 76100 + 259200 + 57024 + 4108{,}8 + 2340{,}9 = 431\,473{,}7 \text{ грн}$$

Таким чином, річні поточні витрати складають:

$$С = 25\,000 + 431\,573{,}7 = 456\,573{,}7 \text{ грн}$$

ВИСНОВКИ

Проведено аналіз сучасного стану розвитку безпроводових телекомунікаційних систем. Розглянуто основні характеристики телекомунікаційної системи, які в різній формі враховуються при розрахунку і проектуванні мережевих структур, а саме помилка приймання сигналу та пропускна здатність системи. Помилка приймання сигналу цілком визначається відношенням сигнал/шум на вході вирішуючого пристрою. Достовірність передачі даних оцінюється за інтенсивністю бітових помилок (Bit Error Rate), котра визначається як ймовірність спотворення переданого біта даних. Завадозахищеність системи залежить від потужності перешкод, створюваних зовнішнім середовищем або через шуми, що виникають в самій системі. Найменш завадозахищеними є радіолінії, добру завадозахищеність мають кабельні лінії, відмінну - волоконно-оптичні лінії, які не сприйнятливі до електромагнітного випромінювання. Визначено вплив видів модуляції сигналу на енергетику радіолінії.

Досліджено завадозахищеність телекомунікаційних систем з різними видами модуляції сигналу, такими як АМ-2, ФМ-2, ЧМ-2, а також з багатопозиційною амплітудною, частотною, фазовою модуляцією.

В результаті дослідження впливу видів модуляції сигналу на енергетику радіолінії було визначено, що при передачі сигналів найбільш ефективними видами модуляції є ФМ-4 та КАМ-4, які забезпечують найкращий коефіцієнт ефективності радіолінії. Найменше значення відношення сигнал/шум для помилок $P_b<10^{-3}$ забезпечує частотна модуляція ЧМ-8. При $P_b>10^{-4}$ найменше значення відношення сигнал/шум забезпечує ФМ-2.

Розроблена методика покращення визначення рівнів сигналу ТКС з використанням амплітудно-модульованих сигналів для цифрового

телебачення за технологією VSB підвищує достовірність системи, в якій завдяки автоматичному регулюванню коефіцієнта підсилення підсилювача на протязі одержаного тестового імпульсу досягається чітке приймання максимальних значень амплітудно-модульованого сигналу.

Збільшення пропускної здатності системи шляхом підвищення відношення сигнал/шум може бути досягнуто шляхом застосування сигналу амплітудно-маніпульованого сигналу та використання запропонованої моделі ТКС.

ПЕРЕЛІК ПОСИЛАНЬ

1. Системи моніторингу та управління безпекою
http://integritysys.com.ua/security/siem/

2. https://msn.khnu.km.ua/pluginfile.php/208282/mod_resource/content/2/Лекція%20№7.pdf

3. Фундаментальний процес тестування
https://qalight.ua/baza-znaniy/fundamentalnij-protses-testuvannya/

4. Конфігураційне тестування
https://qalight.ua/baza-znaniy/konfiguratsijne-testuvannya/

5. Що таке тестування відновлення при тестуванні програмного забезпечення
https://uk.myservername.com/what-is-recovery-testing-software-testing

6. Cisco Voice Over IP Version 4.2 [Электронный ресурс]: — Электрон. дан. — Cisco Systems Inc, 2004

7. http://www.inf.tsu.ru/library/DiplomaWorks/CompScience/2006/kravchenko/diplom.pdf

8. https://dut.edu.ua/uploads/l_1219_46844702.pdf

9. Odom W., Cavanaugh M. Cisco DQOS Exam Certification Guide. — Cisco Press, 2003. — 936 c

10. Voice Network Design Fundamentals [Электронный ресурс]: — Электрон. дан. — Cisco Systems Inc, 2005.
http://www.pluscom.ru/cisco_product/cc/td/doc/product/access/sc/rel9/soln/voip2

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Стан питання. Постановка задачі	15	
6	А4	Спеціальна частина	17	
7	А4	Економічний розділ	5	
8	А4	Висновки	2	
9	А4	Перелік посилань	1	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік матеріалів на оптичному носії

- Проценко К.В_172м-21-1.docx
- Проценко К.В_172м-21-1.pdf
- Проценко К.В_172м-21-1.pptx

ДОДАТОК В. Відгук керівника економічного розділу

Відгук керівника економічного розділу

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 60 б. (« задовільно »).

Керівник розділу _____ доц. Романюк Н.М.

(підпис) (ініціали, прізвище)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К
на кваліфікаційну роботу студента групи 172м-21-1
Проценко Кирила Віталійовича
на тему: «Вдосконалення системи тестування платформи потокового мовлення на основі мікросервісної архітектури»

ДНІПРО
2022