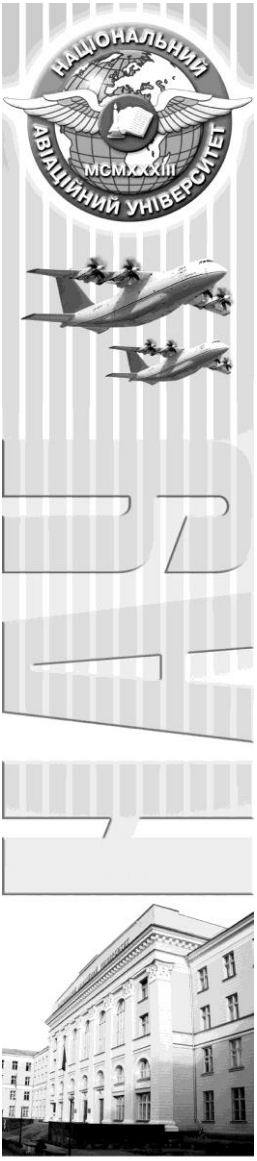


**МІНІСТЕРСТВО ОСВІТИ І НАУКИ,
МОЛОДІ ТА СПОРТУ УКРАЇНИ
Національний авіаційний університет**

**Г.Ф.Конахович, О.П. Ткаліч, В.М. Чуприн,
І.О. Мачалін**

Експлуатація телекомунікаційних систем

Підручник

Київ 2014

УДК 621.39 (075.8)
ББК з880-082я7
Е457

Рецензенти

Беркман Любов Наумівна – директор навчально-наукового інституту телекомунікацій та інформатизації, завідувач кафедри телекомунікаційних систем Державного університету інформаційно-комунікаційних технологій, доктор технічних наук, професор.

Шокало Володимир Михайлович – професор кафедри основ радіотехніки Харківського національного університету радіотехніки, доктор технічних наук, професор.

Сундучков Костянтин Станіславович – професор кафедри інформаційно-телекомунікаційних мереж Інституту телекомунікаційних систем НТУУ «КПІ», доктор технічних наук, професор.

Гриф надано Міністерством освіти і науки, молоді та спротру України
(Лист №1\11-4505 від 27.02.13р……)

Конахович Г.Ф., Чуприн В.М., Ткаліч О.П., Мачалін

Е457Експлуатація телекомунікаційних систем: Підручник. – К.: , 2014. – 800 ст.

Підручник «Експлуатація телекомунікаційних систем» присвячено експлуатації сучасних телекомунікаційних систем. Це перше україномовне видання, де у систематизованому вигляді представлено найбільш повний виклад основних понять, характеристик, методів та технологій експлуатації обладнання сучасних інформаційно-телекомунікаційних систем (ІТКС), що є гармонізованим із чинною програмою підготовки студентів. В підручнику розкрито розділи із широкого спектру проблем, що пов'язані із експлуатацією обладнання ІТКС і які складають фундамент, на якому базуються сучасні технології експлуатації ІТКС.

УДК 621.39 (075.8)
ББК з880-082я7

ЗМІСТ

Народу України,
що вже зробив суттєві кроки на
шляху побудови громадянського
суспільства, присвячуємо

ПЕРЕДМОВА

В Україні наразі вже побудовані сучасні інфраструктури глобальних телекомунікаційних мереж. Локальні мережі вмонтовані в інфраструктуру майже кожного підприємства чи установи і знаходять усе більше використання у повсякденному побуті. На більшості українських підприємств вже створені та широко використовуються локальні та глобальні корпоративні телекомунікаційні системи різноманітного призначення. Телекомунікаційні послуги, що надаються на основі використання ресурсів цих систем та мереж, користуються невпинно зростаючим попитом. Тому підготовка фахівців, що будуть у змозі кваліфіковано експлуатувати телекомунікаційні системи та мережі, сьогодні є актуальною.

Ця книга - є підручником із експлуатації телекомунікаційних систем. Він повністю відповідає паспорту навчальної дисципліни „Експлуатація телекомунікаційних систем" за напрямом 0924 („Телекомунікації"), спеціальності 7.092401 („Телекомунікаційні системи та мережі"), кваліфікації спеціалістів 2144.2 („Інженер електрозв'язку"). Робоча навчальна програма цієї дисципліни побудована за кредитно-модульною системою і передбачає необхідність проведення 35 годин лекційних, 35 годин лабораторних занять та 162 години самостійної роботи студентів. На думку авторів, цього замало, щоб отримати фундаментальні знання щодо експлуатації телекомунікаційних систем. Тому у текст підручника включено також і факультативний матеріал, котрий не є обов'язковим для вивчення, якщо мати на увазі формальні вимоги до підготовки студентів за спеціальністю 7.092401, проте ознайомлення із цим факультативним матеріалом є вкрай важливою справою з точки зору формування цілісного погляду на проблеми експлуатації телекомунікаційних систем.

Приступаючи до роботи над підручником, автори усвідомлювали, що функціональні можливості та технічні

характеристики сучасного телекомунікаційного обладнання (надалі ТЛК-обладнання), а також інші аспекти, що пов'язані з особливостями їхньої побудови та функціонування, в достатній мірі висвітлені у відповідній учбовій літературі. От же, студенти – майбутні фахівці з експлуатації телекомунікаційних систем - все це мали вивчити до початку роботи над матеріалом цього підручника. У той же час перелік публікацій, що присвячені проблемам раціонального використання можливостей ТЛК-обладнання, є досить обмеженим і не відповідає у кількісному і якісному вимірах потребам фахівців, котрі забезпечують його працездатність та надання телекомунікаційних послуг (надалі ТЛК-послуг). Зокрема, сфера організації експлуатації сучасного ТЛК-обладнання висвітлена, на наш погляд, недостатньо, а бібліографія з проблематики забезпечення якісного надання ТЛК-послуг взагалі майже відсутня. Відчувається нагальна потреба у підручнику із вищеназваної тематики, котрий у доступній та стислій формі надавав для студентів, що навчаються за напрямом 0924 („Телекомунікації"), вичерпні відповіді на весь комплекс питань, котрі повинні бути висвітлені у рамках навчальної дисципліни „Експлуатація телекомунікаційних систем".

Автори цієї книги мали за мету усунути цю прогалину та надати студентам надійний підручник з експлуатації сучасних телекомунікаційних систем, котрий у повній мірі відповідав би паспорту вищеназваної навчальної дисципліни.

Структура викладу матеріалу у підручнику відображає модульний принцип побудови навчальної дисципліни „Експлуатація телекомунікаційних систем". Увесь навчальний матеріал, котрий має бути викладений студентам у рамках 17 лекційних занять (35 учбових годин), розбито на п'ять тематично незалежних модулів. Спочатку чотири лекції (що складають модуль №1) присвячено загальній характеристиці систем експлуатації ТЛК-обладнання. Розглянуто цілі та основні функціональні групи задач експлуатації. Із множини цих задач відокремлено задачі технічної експлуатації (ТЕ). Проаналізовано основні характеристики існуючих систем ТЕ та види забезпечення цих систем (інформаційного, організаційного, технічного та метрологічного). Окрема лекція присвячена аналізу основних

характеристик систем надання телекомунікаційних послуг (ТЛК-послуг), у рамках якої розглянуто характеристики ТЛК-послуг як об'єктів споживчого попиту. Розглянуто основні характеристики транспортних послуг та послуг комутованого і некомутованого доступу, зокрема структура середовища транспортування даних, існуючі види послуг та точки доступу до них. Розглянуто також види систем обслуговування, що базуються на використанні ресурсів ТЛК-обладнання (обслуговування із максимальними зусиллями, пріоритетне обслуговування і т.ін.). Остання лекція першого модулю присвячена основним характеристикам систем керування (адміністрування) ТЛК-обладнанням. Розглянуто TMN-архітектуру побудови систем керування, схему взаємодії „менеджер – агент", бази MIB і RMON та протокол керування SNMP.

Чотири лекції модулю №2 присвячено технологіям вимірювань експлуатаційних параметрів ТЛК-обладнання. Детально пояснено основні методи та базові схеми вимірювань параметрів обслуговування для технологій канального та мережного рівнів інформаційної взаємодії (відповідно до класифікації, що прийнята у семирівневій моделі OSI ISO). Мова йде, в першу чергу, про технології передавання пакетних даних, що функціонують за специфікаціями *IP, Frame Relay, xDSL* та *Optical Ethernet*. Технології вимірювань фізичного рівня, на думку авторів, мають більш високий ступінь стандартизації. Вони більш широко висвітлені в учбовій літературі. Тому цим технологіям у підручнику приділено менше уваги. Проте надано усі необхідні посилання на матеріали інших авторів.

Чотири лекції модулю №3 присвячено технологіям підтримки працездатного стану ТЛК-обладнання. Надана характеристика основним процедурам підтримки працездатності. Детально розглянуто технологію контролю відповідності, у т.ч. механізми тестування ТЛК-обладнання, моніторингу та аудиту мережних ресурсів. Висвітлено методи вирішення проблем невідповідності параметрів ТЛК-обладнання прийнятим нормам обслуговування, у т.ч. аналізу телекомунікаційних протоколів. Окрема лекція присвячена адмініструванню ресурсами телекомунікаційного обладнання: конфігурування характеристик обладнання,

адміністрування вузлу мережі, систем сигналізації тощо. Остання лекція модулю №3 присвячена методам і механізмам підтримки надійності функціонування ТЛК-обладнання.

Модуль №4 складається із чотирьох лекцій, що присвячені технологіям управління трафіком та наданням ТЛК-послуг. У першій лекції цього модулю розглянуто характеристики навантаження на ТЛК-обладнання, надано розрахунки навантаження та методи вимірювань його параметрів. Окремі лекції присвячені відповідно організаційному та інформаційному забезпеченню надання послуг. Положення підручника поширюються, в першу чергу, на сферу організації надання послуг транспортними мережами передачі даних (МПД), зокрема: магістральними МПД, що побудовані на основі використання телекомунікаційної технології асинхронного режиму переносу (*Asynchronous Transfer Mode, ATM*) та протоколу Інтернет (*Internet Protocol, IP*); каналами та мережами абонентського доступу, що створені на основі використання телекомунікаційних технологій *FRAME RELAY (FR), IP, xDSL* та *Optical Ethernet*; мережами та окремими вузлами управління транспортними мережами. До складу інформаційного забезпечення віднесені моделі процедур обслуговування, що структуровані згідно рекомендації Е.800 МСЕ-Т. Ці моделі відображають функціонально самодостатні технологічні ланцюги, що реалізують прийняту технологію обслуговування відповідно до систем, що використовуються на практиці, перш за все, мається на увазі система диференційованого обслуговування з гарантованим сервісом (система ДОГС).

У рамках модулю №4 розглянуто задачі технічного забезпечення якості обслуговування (*QoS*). Пояснено структуру та механізми функціонування служби *QoS*. Значна увага приділена інженерії трафіку, зокрема детально розглянуто методи керування навантаженням. Наведено класифікацію та визначення усіх основних показників функціональності та якості надання транспортних послуг. Детально пояснено базові схеми та методи вимірювань параметрів якості обслуговування**.** У заключній лекції модулю №4 фактично викладено основні аспекти сучасної технології оцінки якості обслуговування: класифікація рівнів якості обслуговування, нормативні значення показників якості

обслуговування, контроль параметрів послуг, дії обслуговуючого персоналу у разі виникнення проблем в процесі обслуговування тощо. Зокрема, в книзі наведено нормативи якості обслуговування при наданні транспортних послуг на основі використання найбільш поширених телекомунікаційних технологій передавання даних. Ці нормативи слід розглядати як продукт узагальнення практичного досвіду провідних сервіс-провайдерів та операторів електрозв'язку України. Вони є гармонізованими із відповідними рекомендаціями МСЕ-Т, що розглянуті далі. Технологія забезпечення і оцінювання рівня надання послуг із транспортування даних, що висвітлена у даній книзі, широко застосовується сервіс-провайдерами та операторами електрозв'язку на глобальних мережах передачі даних.

Заключний п'ятий модуль підручника (складається із двох лекцій, одна із котрих є факультативною) присвячено викладу стандартної технології створення підсистем захисту інформаційних ресурсів ТЛК-обладнання та їх підтримки в актуальному стані. Факультативно викладена прийнята в Україні стандартизована технологія оцінювання ефективності та гарантованості захисту інформації у ТЛК-системах.

Слід зауважити, що у підручнику міститься конкретна інформація про сучасні методи та процедури вимірювань параметрів ТЛК-обладнання, вирішення проблем невідповідності цих параметрів прийнятим нормативним значенням, інженерії пакетного трафіку та оцінювання якості мережного обслуговування. Книга буде корисною не тільки для студентів, а і для фахівців, які безпосередньо займаються експлуатацією ТЛК-обладнання та технічним забезпеченням обслуговування споживачів ТЛК-послуг, а також, ймовірно, для «вдумливих» споживачів ресурсів телекомунікаційних мереж (надалі ТЛК-мереж), котрі бажають заощадити свої кошти шляхом оптимізації параметрів ТЛК-послуг, що ними замовляються у рамках сервісних угод з постачальниками цих послуг.

Вивчення змісту підручника передбачає підготовку читача на рівні базових вузівських курсів інформатики, теорії зв'язку та телекомунікаційної техніки.

Підручник написано на основі лекцій, що читаються протягом

останніх п’яти років на кафедрі телекомунікаційних систем Національного авіаційного університету (Україна, м.Київ) для студентів, які навчаються за напрямом «Телекомунікації».

ПОЗНАЧЕННЯ ТА СКОРОЧЕННЯ

Україномовні:

АЦ – адміністративний центр

ВД – вузол доступу

ДСТУ – державний стандарт України

ЗАКТМ – загальнодержавна телефонна мережа з автоматичною комутацією

ЛОМ – локальна обчислювальна мережа

МПД – мережа передачі даних

МСЕ-Т – міжнародний союз електрозв'язку – телекомунікації

НД – нормативні документи

ПВ – периферійний вузол

ПД – передача даних

ПОД – пристрій обслуговування даних

ПОК - пристрій обслуговування каналів

РВ – регіональний вузол

РТВ – регіонально-транзитний вузол

ТВ - територіальний вузол

ТЕ – технічна експлуатація

ТО – технічне обслуговування

ТОР - технічне обслуговування і ремонт

ЦВ – центральний вузол

ЦК – центр керування

ЦСУ – централізована система управління

Англомовні:

DCE – Data Circuit Terminating Equipment (апаратура передавання даних)

DTE – Data Terminal Equipment (прикінцеве обладнання даних)

FR – Frame Relay (Фрейм Рілей)

FRAD – Frame Relay Access Device (пристрій доступу FR)

IP – Internet Protocol (протокол Інтернет)

ISO - International Standartization Organization (Міжнародна організація зі стандартизації)

LAN – Local Area Network (локальна обчислювальна мережа, ЛОМ)

NMS – Network Management System (система мережного

керування)

OSI – Open System Interconnection (взаємозв’язок відкритих систем)

PDU – Protocol Data Unit (протокольний блок даних)

PVC – Permanent Virtual Circuit (постійний віртуальнй канал)

SLA – Service Level Agreement (угода щодо рівня надання послуг або рівня обслуговування)

SMTP – Simple Management Telecommunication Protocol (телекомунікаційний протокол спрощеного керування)

TDM – Time Division Multiplexing (часове мультиплексування)

TMN – Telecommunication Management Network (мережа управління телекомунікаціями)

МОДУЛЬ №1. ЗАГАЛЬНІ ПОЛОЖЕННЯ ЩОДО ПОБУДОВИ ТА ХАРАКТЕРИСТИК СИСТЕМ ЕКСПЛУАТАЦІЇ ТЕЛЕКОМУНІКАЦІЙНОГО ОБЛАДНАННЯ

ЛЕКЦІЯ №1. ЗАГАЛЬНА ХАРАКТЕРИСТИКА СИСТЕМ ЕКСПЛУАТАЦІЇ

Розглядаються наступні питання:

1.1. Пояснення щодо термінів „експлуатація”, „технічна експлуатація” та „об’єкт експлуатації”

1.2. Цілі експлуатації телекомунікаційного обладнання (ТЛК-обладнання)

1.3. Функціональні групи задач експлуатації ТЛК-обладнання.

1.1. Пояснення щодо термінів „експлуатація”, „технічна експлуатація” та „об’єкт експлуатації”

Перш за все, необхідно згадати, що означає термін „експлуатація”, і уяснити, чим це поняття відрізняється від поняття „технічна експлуатація”.

Під узагальненим терміном “експлуатація” розуміється одна із стадій життєвого циклу об’єкта експлуатації, впродовж котрої організується функціонування цього об’єкту за основним призначенням та реалізується множина експлуатаційних процесів із підтримки і поновлення його якості.

Під терміном “технічна експлуатація” розуміється лише та частина із усієї множини процесів експлуатації, що включає у себе безпосередньо технічне обслуговування об’єкта експлуатації, його ремонт, транспортування та зберігання.

Як бачимо із наведених визначень, „експлуатація” – це значно ширше поняття, ніж „технічна експлуатація”. Уся сукупність задач технічної експлуатації будь-якого об’єкту – це лише одна із складових множини задач експлуатації цього об’єкту. Зокрема, сукупність дій персоналу, що спрямована на підтримку та поновлення якості об’єкту експлуатації, визначається терміном „технічна експлуатація”. У той час як дії персоналу із використання досягнутого рівня якості об’єкту експлуатації у будь-яких корисних для власників цього об’єкту цілях (зокрема, із

використання його якісних характеристик з метою одержання бізнесового прибутку) терміном „технічна експлуатація” не охоплюються. Наприклад, ремонт та обслуговування обладнання – це задачі технічної експлуатації, а обслуговування клієнтів з використанням ресурсів цього обладнання не є задачами технічної експлуатації. Цілеспрямоване використання об’єкту експлуатації за його функціональним призначенням – це відокремлений від технічної експлуатації вид експлуатаційної діяльності.

У якості об’єктів експлуатації у рамках цього підручника розглядається обладнання телекомунікаційних систем та комплексів. ТЛК-система, як правило, створюється на базі ТЛК-обладнання для надання послуг із транспортування інформації (а також для надання доступу до інших інформаційних сервісів) суб’єктам та об’єктам прикладних систем, що розосереджені за територіальною ознакою. У свою чергу, ТЛК-комплекс утворюється шляхом інтеграції кількох ТЛК-систем.

Примітка 1. Нагадаємо, що телекомунікаційними мережами (ТЛК-мережами) називають ТЛК-системи, котрі складаються із територіально розосереджених вузлів, з’єднаних між собою каналами інформаційної взаємодії. Наприклад, якщо якась ТЛК-система складається більше ніж із двох вузлів, що з’єднані між собою каналами інформаційної взаємодії, то таку систему вже можна назвати ТЛК-мережею.

Розглядається ТЛК-обладнання - від найпростішого, локально інстальованого на автономних комп’ютерах, до високопродуктивного багатофункціонального мультисервісного обладнання глобальних телекомунікаційних мереж. Основне призначення такого обладнання – слугувати технічним ресурсом, що використовується його власниками для організації надання різноманітних телекомунікаційних послуг та доступу до різноманітних інформаційних сервісів. Чим вища якість цього технічного ресурсу, тим більш якісні ТЛК-послуги можливо надавати шляхом його використання. З іншого боку, оскільки придбання програмно-апаратних засобів ТЛК-обладнання, а також підтримка його коректної експлуатації, зокрема територіально розгалужених ТЛК-мереж, потребують великих коштів, то підвищення завантаження цього обладнання клієнтським (а не службовим або технологічним) інформаційним трафіком сприяє

його економному використанню і є актуальною експлуатаційною задачею. Тому у даній сфері під використанням якості об'єкту експлуатації розуміють не тільки діяльність, що пов'язана із наданням ТЛК-послуг (та доступу до інформаційних сервісів) і, отже, може приносити прибуток, але і діяльність, що спрямована на підвищення завантаженості ТЛК-обладнання і, отже, має на меті економію капіталовкладень.

Організаційні структури більшості постачальників ТЛК-послуг (зокрема, операторів електрозв'язку та інтернет-провайдерів) передбачають розділення функцій служб підтримки надання ТЛК-послуг та служб керування трафіковим навантаженням від служб, що здійснюють технічну експлуатацію ТЛК-обладнання.

1.2. Цілі експлуатації ТЛК-обладнання

Програмні та (або) апаратні засоби ТЛК-обладнання – це, здебільшого, капіталоємні ресурси. Ці ресурси експлуатують шляхом надання ТЛК-послуг користувачам ТЛК-систем. У якості користувачів ТЛК-ресурсів розглядаються як фізичні особи, так і певним чином активізовані (тобто, запущені у роботу) фізичні процеси або комп'ютерні програми, що реалізуються, зокрема, термінальним обладнанням, серверним обладнанням або засобами прикладних систем. Вважається, що кінцеві корисні функції у тій чи іншій сфері людської діяльності реалізують так звані прикладні системи, зокрема прикладні програмні системи. Наприклад, комплекс бухгалтерських комп'ютерних програм, інстальованих на різних вузлах локальної або глобальної ТЛК-мережі, являє яскравий приклад прикладної системи. Цей комплекс програм називають також бухгалтерським прикладним застосуванням або бухгалтерською прикладною задачею. Якщо ж це прикладне застосування ще і пристосовано для продажу (зокрема, отримало сертифікат якості та інші необхідні дозвільні документи, що легалізують процес продажу), то його можливо також назвати бухгалтерським прикладним продуктом. **Прикладні застосування (прикладні задачі, прикладні продукти) можуть реалізовуватися у локальному або мережному варіантах.** Локальний варіант прикладного застосування інсталюється в межах одного вузлу ТЛК-мережі або на одній окремо розташованій

комп’ютерній системі. Під час експлуатації локально розташованої прикладної системи ТЛК-обладнання не використовується. Мережний варіант прикладного застосування передбачає інсталювання його програмних та (або) апаратних модулів відразу на (де)кількох вузлах ТЛК-мережі і, отже, можливість обміну інформацією між частинами прикладної системи, що розташовані на різних вузлах цієї мережі. Зрозуміло, що здатність прикладної системи функціонувати у мережному варіанті надає її користувачам суттєві якісні переваги і нові більш досконалі функціональні можливості. Мережний варіант бухгалтерської прикладної системи, зокрема, надає можливість організувати спільну роботу бухгалтерських служб підприємства, що розосереджені по всій зоні діяльності цього підприємства, організувати обмін бухгалтерською інформацією із податковими службами, фінансовими установами тощо. Іншим прикладом прикладної задачі є програмно-технічний комплекс засобів визначення координат місцезнаходження наземних об’єктів з використанням систем супутникового та стільникового зв’язку. Ця прикладна задача (тобто, задача визначення координат) передбачає застосування ТЛК-обладнання для здійснення транспортування навігаційної інформації між окремими її елементами, розосереджиними на великих відстанях у просторі: між мобільним терміналом користувача цієї задачі та базовою станцією стільникового зв’язку, між обладнанням підсистеми пакетної комутації стільникової мережі та регіональними наземними коригувальними станціями, між коригувальними станціями та відповідним супутниковим обладнанням тощо. Подібних прикладів прикладних задач – безліч, практично у всіх сферах людської діяльності. Важливою особливістю використання ТЛК-обладнання для вирішення прикладних задач є те, що це обладнання кінцевих корисних функцій безпосередньо не виконує: воно лише сприяє успішному вирішенню цих задач, а у багатьох випадках її застосування є безальтернативною умовою функціонування прикладної системи. Тому навряд чи доцільно у якості можливої цілі експлуатації ТЛК-обладнання обирати досягнення екстремальних значень показників якості його функціонування (зокрема, максимізацію швидкості передавання або обробки

інформації у прикладній системі, мінімізацію виникнення помилок або мінімізацію часу реакції системи на надіслані запити). Більш раціональною ціллю експлуатації такого обладнання є гармонізація (узгодження) бажаних значень показників якості його функціонування із оптимальними значеннями показників якості функціонування безпосередньо самої прикладної системи. Якщо, наприклад, проміжок часу у 1,5 секунди для реакції прикладної системи на запити, що надходять до неї каналами ТЛК-мережі, є достатнім для її якісного застосування, то навряд чи є доцільними намагання експлуатаційного персоналу покращити реактивність ТЛК-обладнання, що функціонує у складі такої прикладної системи. Вартість експлуатації у цьому випадку суттєво зросте, а рівень корисності прикладної системи не підвищиться. Таким чином, **досягнення відповідності між показниками якості функціонування прикладних систем та показниками якості функціонування ТЛК-обладнання, що надає ТЛК-послуги цим прикладним системам, є узагальненою ціллю експлуатації ТЛК-обладнання.** Оскільки у більшості випадків ТЛК-обладнання використовується для одночасного обслуговування багатьох різних прикладних систем, що мають різні потреби у ТЛК-послугах, то вищезазначене узгодження показників являє нетривіальну задачу. Найбільш раціональним шляхом вирішення цієї задачі є нормування показників якості. Якщо на певну групу показників якості існують норми, то виробники ТЛК-обладнання намагаються випускати вироби, що цим нормам відповідають. З іншого боку, постачальники ТЛК-послуг намагаються організувати процес обслуговування у відповідності із цими нормами. За таких обставин розробники прикладних систем, знаючи конкретні діапазони значень показників якості ТЛК-обладнання, що надані у відповідних нормах, мають можливість задавати функціональність розроблюваних прикладних систем, яка у повній мірі використовує телекомунікаційні ресурси існуючих ТЛК-систем. З урахуванням вищезазначеного **ціль експлуатації можливо також визначити як забезпечення відповідності показників якості функціонування ТЛК-обладнання, що є об'єктом експлуатації, а також показників якості послуг, що надаються з використанням ресурсів цього обладнання, тим припустимим**

значенням, що зазначені у чинних нормативних документах (НД) та (або) в інших документах, що регламентують процеси експлуатації цього обладнання. Тобто, слід застосовувати такі експлуатаційні технології, впроваджувати такі експлуатаційні процеси та процедури, що забезпечують відповідність реально виміряних в процесі експлуатації значень показників якості існуючим регламентованим значенням цих показників.

Існують і більш конкретні визначення цілей експлуатації ТЛК-обладнання, зокрема у формі постановок оптимізаційних задач. Наприклад, в якості цілі експлуатації вибирається досягнення максимальних значень трафікового навантаження на обладнання за умов забезпечення певним чином визначених рівнів якості надання ТЛК-послуг та надійності функціонування обладнання. Однак таку ціль можливо розглядати, якщо оператор телекомунікаційної системи не відчуває дефіциту попиту на ТЛК-послуги, що надаються на основі використання ресурсів цієї системи.

1.3. Функціональні групи задач експлуатації ТЛК-обладнання

Усю багаточисельну множину різноманітних експлуатаційних задач (або, як кажуть, множину функцій експлуатації) з метою спрощення та упорядкування процесу експлуатації доцільно декомпозувати (тобто, розбити) на окремі функціональні групи. Декомпозиція здійснюється таким чином, щоб в кожну із цих груп увійшли задачі приблизно однакового функціонального призначення. Наприклад, до одної функціональної групи відносять усі експлуатаційні задачі, що пов'язані із виявом та знешкодженням збоїв та помилок у роботі ТЛК-обладнання, до іншої функціональної групи - задачі забезпечення надійності роботи обладнання і т.д. Прийнято розглядати наступні функціональні групи задач експлуатації:

1) конфігурування параметрів ТЛК-обладнання (*Configuration Maintenance*);

2) підтримка працездатного стану ТЛК-обладнання (*Fault Maintenance*);

3) забезпечення продуктивності роботи ТЛК-обладнання (*Performance Maintenance*);

4) забезпечення надійності роботи ТЛК-обладнання (*Reliability Maintenance*);

5) підтримка визначених (зокрема, у сервісних угодах з клієнтами) рівнів якості надання ТЛК-послуг (*QoS Maintenance*);

6) підтримка прийнятої політики забезпечення захисту інформаційних ресурсів ТЛК-системи (*Security Maintenance*);

7) облік використаних ресурсів ТЛК-системи на визначених інтервалах часу (*Accounting Maintenance*);

8) забезпечення взаємодії із користувачами ТЛК-ресурсів (*User Interface Maintenance, Customer Interface Management, User Feedback Control*);

9) забезпечення фінансових розрахунків з клієнтами ТЛК-системи (*Billing Maintenance*);

10) збирання, накопичення та обробка даних, необхідних для аналізу роботи ТЛК-системи та визначення шляхів її подальшого удосконалення та розвитку (*Data Collection Maintenance*);

11) підтримка параметрів середовища експлуатації ТЛК-обладнання у діапазонах припустимих значень (*Operation Environment Protection*);

12) отримання та зберігання контрольних та нових версій і модифікацій елементів програмного забезпечення ТЛК-системи (*Storage Protection*);

13) отримання та зберігання необхідних запасних апаратних компонентів обладнання та витратних матеріалів;

14) підтримка належного стану та якісного рівня інструментальних засобів супроводу експлуатаційних процесів, іншого допоміжного технологічного обладнання та методик їхнього застосування;

15) забезпечення фізичного захисту ТЛК-обладнання;

16) забезпечення зберігання документації, що супроводжує процес експлуатації ТЛК-системи.

Основна сутність кожної із перерахованих вище функціональних груп задач експлуатації полягає у наступному.

1.3.1. Configuration Maintenance (конфігурування параметрів ТЛК-обладнання)

Як правило, будь-який зразок сучасного ТЛК-обладнання

складається із великої кількості програмних та апаратних компонентів. Кожен виріб телекомунікаційної техніки, особливо той, що призначений для широкого продажу, виготовляється із таким розрахунком, щоб задовольнити потреби якомога більшої кількості прикладних застосувань та бути затребуваним у якомога ширшій області сфер і умов використання. Незручно, а з економічної точки зору і неефективно, застосовувати та створювати обладнання, яке може використовуватися лише у вузькій смузі застосувань та вирішувати дуже обмежене коло прикладних задач. Мати справу з обладнанням, що має наперед задані фіксовані значення його характеристик, обмежені та незмінні режими функціонування, невигідно, перш за все, його виробникам, оскільке таке обладнання потрібне недостатньо великій кількості потенційних покупців, а виробник не хоче мати проблем зі збутом своєї продукції. Придбання обладнання, що не здатне бути переналагоджуваним, у багатьох випадках невигідно також його потенційним користувачам, оскільки таке обладнання мало пристосовано до змін умов його застосування і, отже, існує велика ймовірність, що воно буде не придатне для використання у разі модернізації або змін напрямків діяльності його власників. Тому практично усе обладнання, що пропонується на ринках телекомунікаційної техніки, є, у той чи іншій мірі, багатофункціональним, багаторежимним та побудованим за модульним принципом – щоб надати можливість його покупцям настроїти характеристики (параметри) придбаного обладнання на конкретні умови використання. Процес настроювання параметрів обладнання з метою отримання бажаної структури його функціональних можливостей називається конфігуруванням.

Конфігуруванню підлягають як апаратні, так і програмні засоби, що входять до складу експлуатованого ТЛК-обладнання. Оскільки ці засоби складаються із більш дрібних компонентів, котрі, у свою чергу, містять іще більш дрібні компоненти (як правило, використовується ієрархічний деревоподібний принцип побудови ТЛК-обладнання), то, у принципі, задача конфігурування параметрів є актуальною щодо компонентів усіх ієрархічних рівнів. Іншими словами, конфігуруванню можуть підлягати як параметри складових компонентів обладнання, так і параметри ТЛК-

обладнання, коли воно озглядається як єдине діюче ціле.

На практиці ТЛК-обладнання потрапляє на ринок телекомунікаційної техніки у вигляді ТЛК-продуктів, котрі різняться і за призначенням, і за функціональними можливостями. Оператори різноманітних ТЛК-мереж, провайдери різноманітних інформаційних сервісів, що базуються на використанні ресурсів ТЛК-мереж (зокрема, інтернет-провайдери), та численні корпорації, котрі здійснюють свою діяльність практично у всіх галузях людської діяльності, для більш ефективного вирішення своїх прикладних задач намагаються найбільш раціональним для них шляхом придбати певним чином обрану сукупність ТЛК-продуктів, які вони інтегрують у ТЛК-системи.

Примітка 2. У сфері економіки існує точне визначення терміну „корпорація". Однак у сфері телекомунікацій, коли використовують слово „корпорація", то розуміють будь-яке підприємство або будь-яку установу, що використовує ТЛК-обладнання не для надання ТЛК-послуг стороннім організаціям або особам, тим більш за гроші, а для підвищення комфортності свого існування або для підвищення ефективності своєї діяльності за умов, коли ця діяльність не пов'язана з наданням масових послуг стороннім клієнтам на основі використання ресурсів ТЛК-обладнання.

Примітка 3. У телекомунікаційній проблематиці часто використовується термін „корпоративне застосування", котрий означає комплекс (програмний або програмно-апаратний) прикладних задач, спеціально створений для використання корпораціями безпосередньо в процесі їхньої діяльності. Будь-яке корпоративне застосування має вирішувати або сприяти вирішенню саме тих прикладних задач, що входять до складу сфер діяльності корпорації. Здебільшого, корпоративні застосування підвищують рівень автоматизації та (або) інтелектуалізації технологічних процесів та процедур, що має здійснювати корпорація. Проте нерідко впроваджене корпоративне застосування відкриває перед корпорацією нові корисні можливості, зокрема підвищує її конкурентоспроможність.

Корпоративні застосування знайшли впровадження не тільки на підприємствах – суб'єктах підприємницької діяльності, але і у бюджетних організаціях – державних установах, органах державної влади, силових структурах тощо.

Не всі корпорації мають у своєму складі висококваліфікованих спеціалістів у галузі інформаційно-телекомунікаційних технологій. Тому для побудови корпоративної ТЛК-системи (або ТЛК-комплексу, що утворюють шляхом інтеграції кількох ТЛК-систем)

зазвичай запрошують сторонні організації, котрі називаються **системними інтеграторами.**

Цілі та зміст процедур поточного конфігурування, що виконуються на стадії експлуатації ТЛК-обладнання, суттєво відрізняються від цілей та змісту первісного конфігурування параметрів, що виконується на стадії уведення обладнання в експлуатацію, а також від процесів переінсталяції конфігурації обладнання під час його модернізації.

На стадії експлуатації будь-якої ТЛК-системи середовище користувачів її послуг, як правило, постійно змінюється. Зокрема змінюється у реальному часі топологія абонентських вузлів, номенклатура, кількість і якість послуг, які заявляються абонентом, модернізується обладнання, удосконалюється організація експлуатації і т. ін. Тому існує необхідність в оперативних змінах поточної конфігурації штатних програмно-апаратних засобів ТЛК-системи з тим, щоб ця конфігурація адекватно відображала поточні вимоги користувачів і персоналу до кількості та якості послуг, що надаються системою. Поточні зміни конфігурації ТЛК-системи здійснюються експлуатаційним персоналом, головним чином, за допомогою штатних засобів оперативного керування конфігурацією цієї системи. Слід підкреслити, що процес поточного (оперативного) керування конфігурацією, як правило, не зачіпає системних компонентів обладнання і, тому, може здійснюватися у фоновому режимі роботи цього обладнання, тобто без презупинки його функціонування за основним призначенням.

На стадії уведення обладнання в експлуатацію, як правило, здійснюється первісна інсталяція програмних та апаратних засобів ТЛК-системи.

Примітка 4. У вітчизняній практиці процес інсталяції апаратних та інших технічних засобів (тобто, не програмних засобів) часто називають монтажем. Щодо програмного забезпечення термін „інсталяція" є загальноприйнятим і розуміється як комплекс дій із розміщення виконавчих модулів певної програмної системи, що є об'єктом інсталяції, у заданому комп'ютерному середовищі та з настроювання параметрів цих модулів таким чином, щоб вони були здатними виконувати покладені на них функції.

Під час первісної інсталяції конфігуруються параметри ТЛК-системи – об'єкта інсталяції з метою їхнього узгодження як із

параметрами заданого комп'ютерного середовища, так і з цілями, задачами та умовами застосування цієї системи за її основним призначенням. Іншими словами, апаратні та програмні компоненти ТЛК-системи (і вся ТЛК-система у цілому) конфігурується таким чином, щоб її характеристики повністю відповідали положенням та умовам проектної документації на цю систему і враховували конкретні умови її використання на площах розгортання системи.

На стадії експлуатації ТЛК-обладнання час від часу може підлягати модернізації. Під час модернізації зазвичай виконується переінсталяція обладнання і, отже, виникає потреба у його реконфігуруванні. У випадках, коли реконфігуруванню підлягають і системні компоненти ТЛК-системи, то доводиться призупиняти її роботу за основним призначенням.

Зміст задач із конфігурування ТЛК-систем не вичерпується тільки маніпулюванням їхніми параметрами. До цієї групи задач експлуатації належать також задачі визначення мережних адрес та ідентифікаторів (імен) об'єктів, що входять до складу ТЛК-системи, побудова таблиць комутації та маршрутизації, побудова мап (карт) міжвузлових зв'язків ТЛК-мережі, настроювання комутаторів та маршрутизаторів на підтримку маршрутів і логічних віртуальних каналів і т.д і т.п.

Найбільш важливі із цих задач, а також основні механізми їхнього вирішення, розглянуто у лекції №11.

1.3.2. Fault Maintenance (підтримка працездатного стану ТЛК-обладнання)

Fault Maintenance, тобто підтримка працездатного стану ТЛК-обладнання – одна із найважливіших груп задач, котрі мають вирішуватися персоналом, що займається технічною експлуатацією (ТЕ) цього обладнання.

До складу цієї групи відносяться наступні три типові види задач ТЕ:

1) контроль відповідності параметрів обладнання;

2) діагностування обладнання;

3) відновлення роботи обладнання.

Контроль відповідності параметрів обладнання здійснюється

на стадії його експлуатації з метою визначення стану цього обладнання з точки зору його працездатності. Зазвичай, необхідно отримати упевненість, що обладнання на момент контролю було у працездатному стані. Або, у гіршому випадку, виявити сам факт існування невідповідності в роботі обладнання. Під невідповідністю розуміється невідповідність виміряних значень контрольованих параметрів обладнання їхнім припустимим значенням, що задаються стандартами, корпоративними нормами, технічними умовами і т. ін.

Необхідність здійснення контролю відповідності обумовлена тим, що робота будь-якого фізично існуючого обладнання в реальних умовах його використання не може бути абсолютно надійною. Із самих різних причин час від часу виникають аномалії, збої та помилки в роботі апаратних засобів обладнання або логічні конфлікти та некоректності в роботі програмних засобів. Якщо активно не займатися протидією виникненню логічних конфліктів, аномалій, збоїв та помилок, то вони можуть призвести до деградації якості роботи обладнання, а згодом і до виникнення відмов в його роботі.

Примітка 5. Нижче надане визначення основних понять, що пов'язані із підтримкою працездатності обладнання.

Аномалія (*Anomaly*) – відхилення дійсного значення певної характеристики контрольованого обладнання від очікуваного значення цієї характеристики. Аномалія може впливати або не впливати на здатність обладнання виконувати штатні функції.

Збій (*Failure*) – відхилення процесу функціонування обладнання від штатних характеристик цього процесу. Збій може впливати або не впливати на здатність обладнання виконувати штатні функції. Слід пам'ятати, що англійське слово ***Failure*** може означати не тільки збій, але і відмову.

Помилка (*Error*) – невірний результат виконання певної операції в процесі виконання певної процедури, що може призвести або не призвести до виникнення дефекту.

Дефект (*Defect*) – певне обмеження у здатності обладнання виконувати потрібну функцію. Визначення – у ДСТУ 2860-94.

Відмова (*Disrepair, Failure*) – виникнення обмежень (зокрема,

переривань) в спроможності телекомунікаційного обладнання виконувати штатні функції. Визначення - у ДСТУ 2860-94. Несправність обладнання в багатьох випадках є наслідком відмов в його роботі.

Деградація (*Degradation***)** – виникнення аномалій, збоїв або дефектів в роботі обладнання, що не призвели до порушень його працездатності.

Ушкодження (*Impairment***)** – виникнення аномалії або дефекту, але не відмови в роботі обладнання (тобто, це деградація якості ресурсу, що не призвела до переривань в його використанні).

Несправність (*Fault***)** – стан неспроможності обладнання виконувати потрібні функції. Визначення – у ДСТУ 2860-94.

На базі ресурсів ТЛК-обладнання створюються та експлуатуються величезні за своїми масштабами мережі масового обслуговування. Поряд з ними та (або) на їхній основі функціонує велика кількість корпоративних критично важливих для держави і бізнесу ТЛК-систем (наприклад, у банківській сфері, у сфері національної оборони, у податковій системі тощо). Тому навіть нетривала відмова в роботі таких мереж і систем призводить до величезних збитків, а у деяких випадках і до катастрофічних (форс-мажорних) наслідків. Отже, для того, щоб забезпечити можливість завчасного попередження відмов в роботі обладнання, в процесі його експлуатації необхідно постійно займатися рішенням задач із виявлення логічних конфліктів, аномалій, збоїв і помилок в роботі цього обладнання. Процедури, що здійснюються персоналом під час контролю відповідності, як раз і спрямовані на виявлення цих невідповідностей або, як кажуть, на виявлення проблем в роботі обладнання.

Проблема виявлення невідповідності реально виміряних значень параметрів об’єкта експлуатації тим припустимим значенням цих параметрів, котрі регламентовані відповідними документами, що є чинними на момент вимірювань, - центральна проблема, що вирішується у рамках групи задач *Fault Maintenance*. Під відповідними документами розуміються: державні стандарти України (ДСТУ), перш за все ті, що регламентують діяльність у сфері телекомунікацій на території України; міжнародні та міждержавні стандарти, що набули своєї легітимності в Україні

шляхом їх затвердження уповноваженими державними органами; галузеві стандарти Мінтрансзв'язку (зараз - Мінінфраструктури) України; корпоративні стандарти організацій, що є власниками об'єктів експлуатації; накінець, технічні завдання (ТЗ), технічні вимоги (ТВ), технічні умови (ТУ) або технічні сертифікати (ТС) на об'єкти експлуатації. В якості об'єкта експлуатації може бути: безпосередньо ТЛК-обладнання (без урахування прикладних систем, що використовують ресурси цього обладнання); ТЛК-система (зокрема, ТЛК-мережа), що реалізована на базі певним чином визначеного ТЛК-обладнання; ТЛК-комплекс, що інтегрує у собі (де)кілька ТЛК-систем.

Чому проблема невідповідності відноситься до групи задач *Fault Maintenanc*e? Тому що ця проблема безпосередньо пов'язана із виявом логічних конфліктів, аномалій, помилок та збоїв в роботі об'єкта експлуатації. Дійсно, якщо реально виміряні значення хоча б одного із параметрів виходять за межі припустимих норм, то логічно припустити, що нормальний стан функціонування об'єкта експлуатації із якихось причин порушився. Наслідком такого негативного зсуву у стані обладнання може бути поява аномалій, збоїв та помилок в його роботі, що, зокрема, може призвести до погіршення якості надаваних ТЛК-послуг або навіть до відмов в роботі обладнання. У свою чергу, відмови обладнання унеможливлюють процес нормального обслуговування користувачів об'єкта експлуатації.

Зрозуміло, що не всі параметри об'єкта експлуатації є визначальними з точки зору попередження відмов. Наприклад, параметри підсистеми обліку використаних ресурсів або підсистеми захисту інформації не мають відношення до виникнення відмов обладнання. Тому контроль відповідності виконується, головним чином, щодо тих параметрів, що безпосередньо або опосередковано впливають на рівень працездатності обладнання або залежать від нього. Ці параметри називають визначальними.

Для того, щоб успішно вирішувати проблему невідповідності необхідно, перш за все, мати можливість здійснювати вимірювання визначальних параметрів об'єкта експлуатації. Для здійснення вимірювань необхідно: володіти методами та процедурами

вимірювань визначальних параметрів об'єкта експлуатації; мати апробовані методики вимірювань, що допущені до використання уповноваженими особами або організаціями; знати чинні норми на діапазони припустимих значень визначальних параметрів; мати інструментальні засоби вимірювань. Технологіям вимірювань експлуатаційних параметрів ТЛК-обладнання присвячені лекції №5, №6, №7 та №8 та додатковий матеріал до них.

Результати вимірювань, як правило, проходять відповідну обробку і на основі оброблених даних здійснюють оцінювання стану обладнання, зокрема отримують відповідь на питання, чи було на момент вимірювань обладнання працездатним.

Якщо ж обладнання виявиться працездатним, то шукають відповідь на питання, чи перебувало обладнання на момент вимірювань у нормальному стані або якість його функціонування з якихось причин погіршилась. Зрозуміло, що в останньому випадку шукають причину погіршення якості функціонування обладнання з метою, щоб якнайшвидше цю причину усунути.

Якщо обладнання виявиться не працездатним, то реєструється факт виникнення відмови в роботі обладнання і починаються роботи із діагностування обладнання, тобто пошуку елементів, що вийшли з ладу, та причин виникнення відмови.

Примітка 6. У сучасному ТЛК-обладнанні широко застосовуються всілякі методи, засоби та процедури його резервування. Тому відмова, що виникла в роботі обладнання, зазвичай не призводить до призупинки надання ТЛК-послуг користувачам. У більшості випадків штатні засоби, що функціонують у складі обладнання, відмову одразу ж виявляють та швидко локалізують, після чого виявлений несправний модуль обладнання у реальному часі без презупинки в обслуговуванні замінюється на резервний. Однак ці дії проблему виявлення причини відмови та ремонту несправного модулю не знімають.

Діагностування обладнання. Вирішенням проблеми невідповідності не вичерпується група задач *Fault Maintenance*. До цієї групи належить також широке коло інших важливих задач, що називають діагностуванням обладнання. Діагностування – це задача локалізації проблеми невідповідності, тобто пошуку місця розташування та причин виникнення проблеми невідповідності в роботі обладнання. Словосполучення „місце розташування" розуміють у широкому сенсі: місце розташування апаратного елемента у конструктиві обладнання, місце виникнення логічного

конфлікту на трасі протоколу, місце розташування команди у тексті комп'ютерної програми тощо.

Діагностування – складний процес, що потребує зусиль досвідчених фахівців та задіяння різноманітних інструментальних механізмів, що полегшують процес діагностування, як от: реєстрація помилок, повідомлення про помилки, класифікація повідомлень за ступенем важливості, фільтрація повідомлень, що надсилаються засобами обладнання на адресу адміністраторів ТЛК-системи (наприклад, відображаються тільки найбільш важливі повідомлення), кореляційний аналіз з метою виявлення причин помилок на основі певним чином вибраної кореляційної моделі та багато інших.

Відновлення роботи обладнання. До групи задач *Fault Maintenance* відносяться також задачі відновлення роботи обладнання, тобто усунення (знешкодження, нейтралізація) проявів невідповідності в роботі обладнання. **Відновлення (*Clear*)** – усунення несправності. Шляхи вирішення цих задач будуть розглянуті у подальших лекціях.

1.3.3. Performance Maintenance (забезпечення продуктивності роботи ТЛК-обладнання)

ТЛК-обладнання у багатьох випадках потенційно може бути здатним працювати з високою ефективністю, але реально функціонує з низькою продуктивністю. Наприклад, потенційні можливості обладнання дозволяють передавати трафік безперервно, цілодобово і з високою інтенсивністю. Однак на практиці внаслідок різних причин (головним чином, через неоптимально обрані режими та методи експлуатації) цей трафік реально передається з переривами та (або) з низькою інтенсивністю. Тобто, потенційні можливості обладнання щодо його продуктивності використовуються не у повній мірі, що, звичайно, не є бажаним для власників обладнання. Тому у процесі експлуатації слід здійснювати заходи, що спрямовані на забезпечення максимально можливих значень параметрів продуктивності роботи обладнання. Ці заходи і складають зміст функціональної групи задач ***Performance Maintenance*.**

У телекомунікаціях в якості основного показника

продуктивності прийнято застосовувати так званий коефіцієнт використання (або коефіцієнт навантаження) обладнання $K_в$ – відношення реально досягнутої продуктивності функціонування обладнання на визначеному проміжку часу до максимально можливої продуктивності, на яку потенційно спроможно це обладнання. Під продуктивністю зазвичай розуміють пропускну здатність обладнання. Пропускну здатність комутаційного обладнання вимірюють у кількості виконаних з'єднань (виконаних комутацій) за одиницю часу або у сумарній кількості інформації, що просувається із увідних портів комутаційного обладнання до його вивідних портів за одиницю часу. У свою чергу, кількість інформації в залежності від конкретного змісту експлуатаційних задач вимірюється у бітах, байтах, блоках, кадрах, пакетах, фреймах і т.ін. Пропускну здатність канального обладнання вимірюють у кількості інформації, що передається через це канальне обладнання за одиницю часу, або іноді у ширині смуги його пропускання. Пропускну здатність серверного обладнання вимірюють у кількості оброблюваних запитів на обслуговування за одиницю часу, а обчислювального обладнання (процесорів, комп'ютерів, інтелектуальних терміналів і т. ін.) – у кількості елементарних обчислювальних операцій за одиницю часу.

Чим більш високих значень коефіцієнту $K_в$ вдається досягти за допомогою засобів впровадженої системи експлуатації, тим більш досконалою вона вважається. В ідеалі значення $K_в$ має дорівнювати одиниці. Однак на практиці через низку об'єктивних і суб'єктивних причин (котрі будуть розглянуті на лекції №13) діапазон реально досягнутих значень цього коефіцієнту для більшості типів ТЛК-обладнання знаходиться в межах від 0,2 до 0,8. Не вдаючись до деталізації, слід звернути увагу на одну фундаментальну закономірність: якщо за рахунок певним чином визначених експлуатаційних заходів у рамках якоїсь коректно експлуатованої ТЛК-системи комусь вдається підвищити коефіцієнт використання обладнання, то у цьому випадку слід очікувати зниження рівня якості ТЛК-послуг, що надаються на основі використання ресурсів цієї системи, і навпаки. Тому в процесі експлуатації слід шукати „золоту середину", тобто визначитися з необхідними рівнями якості надання ТЛК-послуг і, використовуючи методи інженерії

трафіка, намагатися підвищувати продуктивність використання обладнання до тих пір, поки буде досягнуто визначені рівні якості обслуговування. Іноді має сенс і зворотня задача: намагаються підвищувати якість надання ТЛК-послуг до тих пір, поки реальні значення коефіцієнту використання обладнання наблизяться до наперед визначеної величини.

1.3.4. Reliability Maintenance (забезпечення надійності роботи ТЛК-обладнання)

Надійність функціонування обладнання напряму пов'язана із проблемою виникнення відмов. А відмови ТЛК-обладнання, як вже вказувалось раніше, є вкрай небажані події, які слід у будь-якому разі намагатися уникать. Задачі попередження виникнення відмов займають чільне місце у функкціональній групі задач забезпечення надійності роботи ТЛК-обладнання. Якщо все ж таки відмова сталася, то необхідно задіяти усі доступні методи та засоби для якнайшвидшого відновлення працездатності обладнання. Резервування обладнання та (або) його окремих компонентів, у тому числі і програмного забезпечення – один із основних напрямків у вирішенні задач відновлення працездатності.

Методи та механізми підтримки надійності функціонування ТЛК-обладнання розглянуто у лекції №12.

1.3.5. QoS Maintenance (підтримка заданих рівнів якості надання ТЛК-послуг)

ТЛК-послуги можуть надаватися із різними рівнями якості. Існує прямий зв'язок між якістю та вартістю послуг. Зрозуміло, що більш якісна послуга надається за більш високим тарифом. Тому споживач намагається мінімізувати свої витрати на ТЛК-послугу, замовляючи саме той рівень її якості, котрий є достатнім (а не більшим) для нормального функціонування його прикладного застосування. Споживач може запустити в одночасну роботу (тобто, активізувати) кілька своїх прикладних застосувань, вимоги котрих до необхідних рівнів якості можуть бути різними. Наприклад, цифрова передача мовних повідомлень не висуває жорстких вимог до рівня помилок та втрат інформації у каналі зв'язку, оскільки людській мові властива висока надлишковість, що

сприяє відновленню сигналів – носіїв мовних повідомлень на приймальній стороні каналу. Однак людська мова дуже чутлива до неоднаковості часу затримки сигналів в каналі. Тому за цим параметром якості передачі мовне застосування висуває дуже жорсткі вимоги до ТЛК-обладнання. У сучасних ТЛК-системах забезпеченням необхідних рівнів якості надання послуг займається спеціалізована служба підтримки якості обслуговування, що називається службою ***QoS (Quality of Services).***

Методи та механізми підтримки якості надання послуг розглянуто у лекціях №14, №15 та №16.

1.3.6. Security Maintenance (підтримка прийнятої політики забезпечення захисту інформаційних ресурсів ТЛК-системи)

Підсистема підтримки прийнятої оператором ТЛК-системи політики забезпечення захисту її інформаційних ресурсів являє собою певний технічний комплекс програмних та апаратних засобів захисту інформації, котрий у сукупності із прийнятим комплексом заходів адміністративно-організаційного характеру має забезпечувати визначений політикою безпеки рівень ефективності та гарантованості захисту. Нормативні документи Державної служби спеціального зв'язку та захисту інформації (ДССЗЗІ) України визначають специфікації щодо стандартних рівнів ефективності та гарантованості захисту інформації щодо різноманітних видів ТЛК-систем. Більшість (але не всі) існуючих ТЛК-систем, що реально експлуатуються на практиці, мають відповідати цим специфікаціям.

Слід підкреслити, що на стадії експлуатації ТЛК-систем не займаються створенням нових систем або механізмів захисту інформації, а займаються експлуатацією вже створених і вмонтованих у ТЛК-систему механізмів захисту. Шляхом маніпулювання параметрами вмонтованих механізмів захисту експлуатаційний персонал намагається забезпечити рівень ефективності та гарантованості захисту інформації у системі, що визначений прийнятою політикою безпеки.

До завдань *Security Maintenance*, що має вирішувати персонал ТЛК-систем відноситься: контроль доступу до інформаційних ресурсів системи або до підсистеми керування системою;

забезпечення конфіденційності баз даних; зберігання цілісності даних та програмного забезпечення; автентифікація, ідентифікація та авторизація користувачів ресурсами системи; шифрування та тунелювання інформації; розподіл парольної інформації; настроювання міжмережних екранів тощо.

Технологія забезпечення захищеності інформаційних ресурсів сучасних ТЛК-систем на стадії їхньої експлуатації висвітлена у лекціях №17 та №18.

1.3.7. Accounting Maintenance (облік використаних ресурсів ТЛК-системи)

Підсистема обліку ресурсів ТЛК-обладнання, що були використані його користувачами на визначених інтервалах часу його роботи, з економічної точки зору є однією із найважливіших, оскільки результати роботи цієї підсистеми - отримані облікові дані - є вихідними даними для нарахування платні за витрачені ресурси. Ширина смуги частот каналів зв'язку, пропускна здатність каналоутворюючого та комутаційного обладнання (зокрема, мультиплексорів, комутаторів та маршрутизаторів), пропускна здатність обладнання мереж доступу до глобальних ТЛК-ресурсів, ємність запам'ятовуючих пристроїв, що зберігають інформацію користувачів та (або) для користувачів, продуктивність процесорних пристроїв, що розділяється між прикладними системами користувачів, продуктивність серверного та шлюзового обладнання – усе це ресурси ТЛК-обладнання, які не є безмежними і, тому, мають бути розподілені між тими користувачами, котрі у кожен конкретний момент користуються послугами цього обладнання. Зрозуміло, якщо якомусь привілейованому користувачеві на будь-якому інтервалі часу дістається, наприклад, більша частка ширини смуги каналу, то усі інші користувачі на цьому часовому інтервалі вимушені користуватися меншою часткою цього каналу. Це означає, що прикладне застосування привілейованого користувача буде мати можливість передавати інформацію через цей канал набагато швидше, ніж прикладні застосування звичайних користувачів. Отже, ширина смуги канала – це цінний ресурс, який може бути об'єктом продажу, а цінний ресурс необхідно обліковувати як за параметрами кількості, так і за

параметрами якості для того, щоб мати можливість обгрунтувати його ціну. Те ж саме слід сказати і про інші ТЛК-ресурси – усі вони являють цінність і мають бути облікованими.

Власники ТЛК-ресурсів зацікавлені в організації обліку не тільки задля отримання прибутків від їхнього продажу, але і для оптимізації витрат, що йдуть на закупівлю та утримання ТЛК-обладнання. Підсистема обліку реєструє, зокрема, час використання кожного ресурсу, що дає змогу визначити коефіцієнт використання встановленого обладнання, усереднений на будь-яких періодах експлуатації. Оскільки коефіцієнт використання обладнання характеризує ступінь його завантаженості, то знання цього коефіцієнту дозволяє власникам ТЛК-ресурсів планувати свої витрати на придбання нового обладнання. Поки обладнання має недовантажені ресурси, витрати на збільшення цих ресурсів, зокрема придбання нового обладнання, не є актуальними. Якщо ж навантаження на обладнання збільшується, то зростає і значення коефіцієнту його використання. Перетин реально обчислених значень цього коефіцієнту певного заздалегідь визначеного порогового значення свідчить про те, що навантаження на обладнання досягло тієї межі, коли настав час розпочати дії з нарощування його ресурсів.

1.3.8. User Interface Maintenance (забезпечення взаємодії із користувачами ТЛК-ресурсів)

Сучасні методи організації обслуговування клієнтів забезпечують можливість отримання ними у реальному часі будь-якої інформації щодо обслуговування у будь-який зручний для них час. Оператор електрозв'язку або провайдер ТЛК-послуг надає своїм клієнтам інформацію, що стосується обсягу використаних ними ТЛК-ресурсів, встановлених тарифів на послуги, прийнятих правил та умов надання послуг, довідкової інформації щодо стану обслуговування на момент запиту тощо. З метою реалізації такої можливості у складі ТЛК-систем організують службу інформаційної взаємодії з клієнтами. Бажано, щоб ця служба функціонувала у режимі реального часу. Бажано також, щоб вона була дуплексною, тобто не тільки клієнт мав доступ до відповідних довідкових служб, баз даних та відповідальних працівників

експлуатаційних підрозділів оператора ТЛК-системи, але і адміністратори системи мали доступ до термінального обладнання клієнтів.

1.3.9. Billing Maintenance (забезпечення фінансових розрахунків з клієнтами ТЛК-системи)

Забезпечення фінансових розрахунків оператора електрозв'язку або провайдера послуг з клієнтами за використані ресурси називається **білінгом**, а відповідні програмно-апаратні засоби, що автоматизують та інтелектуалізують процес фінансових розрахунків називаються білінговими системами. Основні вихідні дані, що є необхідними для здійснення розрахунків, надходять від підсистем обліку використаних ресурсів. Це, перш за все, дані щодо кожного клієнта про кількість і якість використаних ним ТЛК-ресурсів. У базі даних будь-якої білінгової системи зберігаються так звані тарифні плани, тобто тарифні розцінки на кожний ресурс (зокрема, на кожну ТЛК-послугу), що може бути наданий у розпорядження клієнтів. Зрозуміло, що у тарифах враховано різні рівні якості ресурсів. Один і той же ресурс може надаватися з різними рівнями якості. Чим більша якість ресурсу, тим вища його вартість. На основі прийнятих тарифних планів і даних, що надходять від підсистем обліку використаних ресурсів білінгова система виконує підрахунок величини плати, яку має сплатити кожен клієнт за отримані ним ТЛК-послуги. Сучасна білінгова система – це високопродуктивна і досить складна програмно –апаратна система, що має функціонувати у реальному часі і одночасно обслуговувати сотні тисяч клієнтів.

1.3.10. Data Collection Maintenance (збирання, накопичення та обробка даних)

Важливою функціональною групою задач експлуатації вважають задачі, що пов'язані із збором та накопиченням всіляких даних, що характеризують різні аспекти функціонування ТЛК-обладнання в процесі його експлуатації. Інтерес представляють не тільки обсяги використаних клієнтами ТЛК-ресурсів, але і дані, що є необхідними для аналізу роботи ТЛК-системи та визначення шляхів її подальшого удосконалення та розвитку. Наприклад, дані

про „поведінку” потоків інформації після їхньої відповідної обробки використовують для визначення шляхів підвищення коефіцієнту використання обладнання та планування розвитку ТЛК-системи. Дані про інтенсивності виникнення збоїв та помилок в роботі обладнання (також після їхньої відповідної обробки) використовують для визначення шляхів підвищення завадостійкості ТЛК-систем. Дані про простої та відмови обладнання необхідні для вибору раціональних методів його ремонту та резервування. У сучасному обладнанні функції збору, накопичення, зберігання та первісної обробки зібраних даних виконуються у реальному часі штатними програмно-апаратними засобами цього обладнання. У складі обладнання знайшли широке застосування всілякі програмні фільтри, лічильники, таймери та класифікатори, що дозволяють експлуатаційному персоналу із величезних масивів накопичених даних швидко відбирати саме ті дані, котрі у даний момент потрібні для вирішення тої чи іншої експлуатаційної задачі.

1.3.11. Operation Environment Protection (підтримка параметрів середовища експлуатації ТЛК-обладнання у діапазонах припустимих значень)

ТЛК-обладнання у більшості випадків розраховано на експлуатацію у стаціонарних приміщеннях (за винятком, можливо, термінальних пристроїв систем мобільного зв’язку), де температура та вологість повітря повинні підтримуватися у визначених відповідними нормами діапазонах припустимих значень. Енергозабезпечення та заземлення обладнання, електромагнітні, електростатичні та вібраційні впливи на обладнання також повинні бути у визначених відповідними нормами діапазонах припустимих значень. Для контролю та підтримки припустимих значень параметрів середовища експлуатації ТЛК-обладнання використовують відповідні прилади та системи, які мають певними чином утримуватися. Роботи із підтримки параметрів середовища експлуатації, зазвичай, покладається на персонал, що здійснює експлуатацію ТЛК-обладнання. Цей персонал повинен вміти коректно користуватися вищеназваними приладами та системами, знати і неухильно

додержуватися правил та інструкцій з їхнього утримання у належному стані.

1.3.12. Storage Protection (отримання та зберігання контрольних та нових версій і модифікацій елементів програмного забезпечення ТЛК-системи)

Програмне забезпечення (ПЗ) ТЛК-систем, що знаходяться в експлуатації, може у будь-який момент вийти з ладу. З іншого боку, виробники ПЗ, що інстальовано на сучасному ТЛК-обладнанні, як правило, постійно здійснюють його модифікацію, намагаючись його удосконалити, наприклад додати нові функціональні можливості. Тому у власників ТЛК-обладнання виникає постійна потреба в отриманні та зберіганні контрольних та нових версій і модифікацій елементів ПЗ, що інстальовано на їхньому обладнанні. Щодо цього існують відповідні правила та інструкції. Експлуатаційний персонал повинен знати і неухильно їх виконувати.

1.3.13.Отримання та зберігання необхідних запасних апаратних компонентів обладнання та витратних матеріалів

Роботи з отримання та зберігання запасних апаратних компонентів обладнання та витратних матеріалів, у більшості випадків, покладається на експлуатаційний персонал. Цей персонал повинен знати і неухильно виконувати відповідні правила та інструкції щодо порядку отримання та зберігання запасних частин та витратних матеріалів.

1.3.14. Підтримка належного стану та якості інструментальних засобів супровіду експлуатаційних процесів, іншого допоміжного технологічного обладнання та методик їхнього застосування

Для ефективного вирішення більшості експлуатаційних задач бажано мати і постійно розвивати належну інструментальну базу – аналізатори протоколів, імітатори тестових послідовностей сигналів, тестери, рефлектометри, комплекси тестових програм тощо. Перелік сучасних інструментальних засобів – різноманітний та широкий.

Має бути забезпечена метрологічна підтримка вимірювальних засобів, зокрема організована повірка цих засобів відповідно до стандартів, що є чинними в Україні.

1.3.15. Phizical Protection (забезпечення фізичного захисту ТЛК-обладнання)

Для захисту ТЛК-обладнання від розкрадання та вандалізму його слід розміщати у межах так званого фізичного контуру безпеки, роль котрого відіграють стіни закритих будівель, окремих приміщень, всілякі короби, кожухи, огорожі, стінки металевих шкафів і т.ін. Контур безпеки має бути фізично укріпленим та цілісним. Фізичні отвори у контурі безпеки мають закриватися надійними засувами або дверима із спеціальними замковими пристроями. Має бути забезпечена охорона контуру безпеки, у т.ч. і з використанням спеціальних систем охоронної сигналізації. У залежності від призначення ТЛК-системи, характеру потенційних загроз ТЛК-обладнанню, що очікуються з боку зловмисників та вандалів, коштовності обладнання та важливості прикладних задач, що вирішуються засобами ТЛК-системи, визначаються необхідні рівні стійкості фізичного контуру безпеки та гарантованості захисту. Специфікації цих рівнів у нашій країні є нормованими, тобто у відповідних нормативних документах надано критерії віднесення експлуатаційних приміщень до тієї чи іншої категорії важливості, а також визначено вимоги до засобів фізичного укріплення у залежності від умов експлуатації обладнання. Побудова систем фізичного захисту здійснюється відповідно до існуючих норм та правил ліцензованими фахівцями із спеціальною підготовкою. Зокрема, розробка політики забезпечення фізичного захисту обладнання та інсталяція відповідних систем охоронної сигналізації не входять до функціональних обов'язків фахівців з телекомунікацій, однак контролювання роботи засобів сигналізації, їх включення та виключення, а також загальний нагляд за цілісністю контуру фізичної безпеки в процесі експлуатації ТЛК-обладнання, як правило, покладається на лінійний персонал ТЛК-систем.

Примітка 7. Історично так склалося, що та частина експлуатаційного персоналу, яка безпосередньо контактує з обладнанням і постійно знаходиться

біля обладнання, зокрема внутрі фізичного контуру безпеки, називається лінійним персоналом.

Персонал ТЛК-систем повинен знати та сумлінно дотримуватися встановлених інструкцій та правил із забезпечення фізичного захисту обладнання.

1.3.16. Забезпечення зберігання документації, що супроводжує процес експлуатації ТЛК-системи

Щоб успішно вирішувати експлуатаційні задачі, необхідно мати і належним чином зберігати відповідну експлуатаційну документацію. Це - перш за все, технічна документація на ТЛК-обладнання (ТЛК-системи або ТЛК-комплекси), що призначена для користування експлуатаційним персоналом – опис принципів, порядку та умов функціонування обладнання, опис експлуатаційних процесів, починаючи від інсталяції та закінчуючи утилізацією обладнання, опис різного роду методік, регламентів, інструкцій з експлуатації та правил користування ресурсами обладнання тощо.

Примітка 8. Слід зауважити, що окрім експлуатаційної документації існує також конструкторьска документація на обладнання, яка не завжди поставляється експлуатаційним організаціям. Зрозуміло, що в конструкторській документації викладено, як виготовляти обладнання, а в експлуатаційній документації – як його експлуатувати.

Необхідно також забезпечити належне зберігання організаційно-розпорядчої документації, що підтримує організаційну структуру та легитимність функціонування експлуатаційних підрозділів підприємства – власника ТЛК-ресурсів.

Накінець, необхідно забезпечити коректне генерування та зберігання звітних документів, що необхідні для контролю роботи і оцінювання діяльності експлуатаційних підрозділів підприємства.

Контрольні питання до першої лекції:

1. Перерахуйте усі шістнадцять груп задач експлуатації ТЛК-обладнання.
2. Надайде англомовні названня основних груп задач експлуатації.
3. Охарактеризуйте групу Configuration Maintenance

4. Охарактеризуйте групу Fault Maintenance
5. Охарактеризуйте групу Performance Maintenance
6. Охарактеризуйте групу Reliability Maintenance
7. Охарактеризуйте групу QoS Maintenance
8. Охарактеризуйте групу Security Maintenance
9. Охарактеризуйте групу Accounting Maintenance
10. Охарактеризуйте групу User Interface Maintenance
11. Охарактеризуйте групу Billing Maintenance
12. Охарактеризуйте групу Data Collection Maintenance.

Література до першої лекції

1) В.Г. Оліфер, Н. А.Оліфер. Комп'ютерні мережі. Принципи, технології, протоколи: Посібник для вузів. Друге видання – СПб.: Питер, 2003. Розділ 19, стор. 776 – 790.

ЛЕКЦІЯ №2. ОСНОВНІ ХАРАКТЕРИСТИКИ СИСТЕМ ТЕХНІЧНОЇ ЕКСПЛУАТАЦІЇ

Розглядаються наступні питання:

2.1. Уточнене визначення понять „технічна експлуатація”, „технічне обслуговування” та „ремонт”

2.2. Основна ціль та функції технічної експлуатації

2.3. Принципи побудови систем технічної експлуатації

2.4. Організаційне забезпечення технічної експлуатації

2.5. Технічне забезпечення технічної експлуатації

2.6. Інформаційне забезпечення технічної експлуатації

2.7. Метрологічне забезпечення технічної експлуатації

2.1. Уточнене визначення понять „технічна експлуатація”, „технічне обслуговування” та „ремонт”

На попередній лекції надане узагальнене визначення поняття „технічна експлуатація”. Показано, що технічна експлуатація охоплює лише частину задач, що мають вирішуватися на стадії експлуатації будь-якої технічної системи. Стосовно сфери телекомунікацій технічну експлуатацію (ТЕ) ТЛК-обладнання (ТЛК-системи або ТЛК-комплексу) визначають як сукупність всіх технічних та відповідних адміністративних дій, включаючи спостереження за станом обладнання, з метою підтримки або відновлення його стану, при якому воно може виконувати визначену сукупність корисних функцій.

Основними функціями технічної експлуатації будь-якого ТЛК-обладнання є технічне обслуговування та ремонт (ТОР).

Технічне обслуговування - це комплекс операцій з підтримки працездатності об’єкта експлуатації, що здійснюється під час використання цього об’єкта відповідно до його призначення, а також під час його зберігання та транспортування.

Ремонт визначається як комплекс операцій з відновлення працездатності об’єкта експлуатації, його ресурсів або ресурсів його складових частин.

Примітка 1. Визначення термінів “технічне обслуговування” та “ремонт” надане згідно ГОСТ 18322 – 78, що є чинним в Україні.

2.2. Основна ціль та функції технічної експлуатації

Основною ціллю ТЕ є забезпечення відповідності параметрів та характеристик об'єкта експлуатації тим їхнім припустимим значенням, що наведені у чинних в Україні нормативних документах (зокрема, в ДСТУ або корпоративних стандартах) та (або) в інших документах, які регламентують процеси ТЕ цього об'єкта експлуатації (зокрема, в ТЗ, ТВ, ТУ або ТС на об'єкт експлуатації). У якості об'єктів експлуатації у рамках цього підручника, як вже зазначалось, розглядається обладнання ТЛК-систем та (або) ТЛК-комплексів.

Із всієї множини функцій (задач) експлуатації, що були розглянуті на попередній лекції, безпосередньо до функцій ТЕ обладнання будь-якої ТЛК-системи слід віднести наступне:

1) оперативне (поточне) керування конфігурацією програмно-апаратних засобів ТЛК-системи;

2) спостереження за характеристиками навантаження на обладнання, контроль неперевищень навантаження певним чином вибраних порогових значень;

3) технічне обслуговування (ТО) та ремонт ТЛК-обладнання;

4) ТО і ремонт додаткових (до штатних) засобів технічного захисту інформації;

5) контроль конфігурації середовища експлуатації ТЛК-обладнання;

6) контроль стану обладнання захисту від фізичних ушкоджень та розкрадань;

7) контроль стану засобів захисту довкілля;

8) отримання і зберігання запасних частин, комплектуючих та витратних матеріалів;

9) здавання відходів в утиль;

10) ремонт із залученням сторонніх організацій;

11) планування запасів матеріальних ресурсів;

12) ведення обліку та виконання правил документообігу.

Примітка 2. Слід зауважити, що такі функції як керування маршрутизацією, тарифікацією, абонентськими лініями (уведення, відміна і т. ін.), надання додаткових послуг, адміністрування службами та сервісами Інтернет не є функціями ТЕ, а є функціями експлуатації, що забезпечують використання ТЛК-обладнання за його основним призначенням відповідно до вимог ТУ на це

обладнання.

Стисла характеристика вищеперерахованих функцій ТЕ надана у попередній лекції. До того слід додати наступне.

На стадії експлуатації середовище користувачів ТЛК-ресурсів, як правило, постійно змінюється. Зокрема змінюється у реальному часі топологія абонентських вузлів, номенклатура, кількість і бажана якість послуг, які заявляються клієнтами оператора електрозв'язку або провайдера інформаційних сервісів. Окрім цього, постійно модернізується обладнання, удосконалюється організація експлуатації і т. ін. Тому існує необхідність в оперативних змінах поточної конфігурації штатних програмно-апаратних засобів ТЛК-обладнання з тим, щоб ця конфігурація адекватно відображала поточні вимоги клієнтів і експлуатаційного персоналу до кількості та якості послуг, що надаються ТЛК-системою.

Примітка 3. Експлуатаційний персонал також вважається користувачем ресурсів ТЛК-системи, яку цей персонал обслуговує і використовує у своїй діяльності. Вважається, що ТЛК-система надає послуги не тільки клієнтам, але і персоналу. ТЛК-послуги, що надаються персоналу, мають за мету підвищити продуктивність їхньої праці. Зокрема, використовуючи ці послуги, адміністратори обладнання мають змогу зручним для себе способом управляти його ресурсами, контролювати стан обладнання, отримувати або забороняти доступ до управління обладнанням і т. ін.

Поточні зміни конфігурації програмно-апаратних засобів ТЛК-обладнання, як правило, здійснюються експлуатаційним персоналом за допомогою штатних засобів оперативного керування конфігурацією цього обладнання.

Зазначимо, що в процесі експлуатації контролюється не тільки конфігурація програмно-апаратних засобів ТЛК-обладнання, але і конфігурація усієї інфраструктури середовища експлуатації ТЛК-системи. Зокрема, конфігурація допоміжних засобів електропостачання, технологічного інструменту, засобів захисту довкілля, меблів, носіїв інформації, матеріалів та запасних частин, засобів оргтехніки та ін. Такий контроль здійснюється з метою запобігання реалізації загроз щодо порушень конфіденційності, цілісності та доступності інформаційних ресурсів об'єкта експлуатації, а також підтримки цілісності ТЛК-обладнання.

Така функція ТЕ як спостереження і контроль мережного навантаження є специфічною і важливою для комунікаційних систем, оскільки своєчасне запобігання перенавантаженню ділянок мережі циркулюючим через них трафіком є найважливішою передумовою надійного функціонування мережного обладнання і дотримання угод з користувачами щодо якості надаваних мережних послуг.

У більшості експлуатаційних організацій ТОР засобів захисту від фізичних ушкоджень та розкрадань (замкових та зачиняючих пристроїв, охоронної сигналізації, дверей, вікон і т. ін.), а також ТОР засобів захисту довкілля (зокрема, вологоміри, градусники, радіометри, кондиціонери, вентилятори і т. ін.) не входять до вищенаведеного переліку безпосередніх функцій ТЕ, але контроль стану вищезазначеного обладнання має здійснюватися персоналом в процесі ТЕ об'єктів експлуатації.

2.3. Принципи побудови систем технічної експлуатації

Для вивчення принципів побудови систем ТЕ в якості моделі об'єкта експлуатації будемо розглядати глобальну ТЛК-систему із мережною структурою, архітектура котрої узята за основу більшістю сучасних українських операторів великих територіально розгалужених ТЛК-систем. Системи ТЕ більш простих ТЛК-систем будемо вважати окремими спрощеними випадками вищеназваної типової моделі.

Узагальнена архітектура моделі об'єкта експлуатації відображена на рис. 2.1 і являє собою трьохшарову багаторівневу ієрархічно побудовану структуру. Внутрішній шар представляє первинну мережу систем передачі фізичних сигналів: обладнання каналоутворення (зокрема, цифрові системи передачі PDH, SDH, DWDM тощо), фізичні канали розповсюдження сигналів (оптоволоконні, електричні, радіоканали тощо), обладнання ущільнення каналів передачі (з частотним FDM, часовим TDM або кодовим CDM ущільненням), обладнання мультиплексування /демультиплексування та регенерації сигналів, що передаються фізичними каналами. (Цей шар на рис.2.1 не показано).

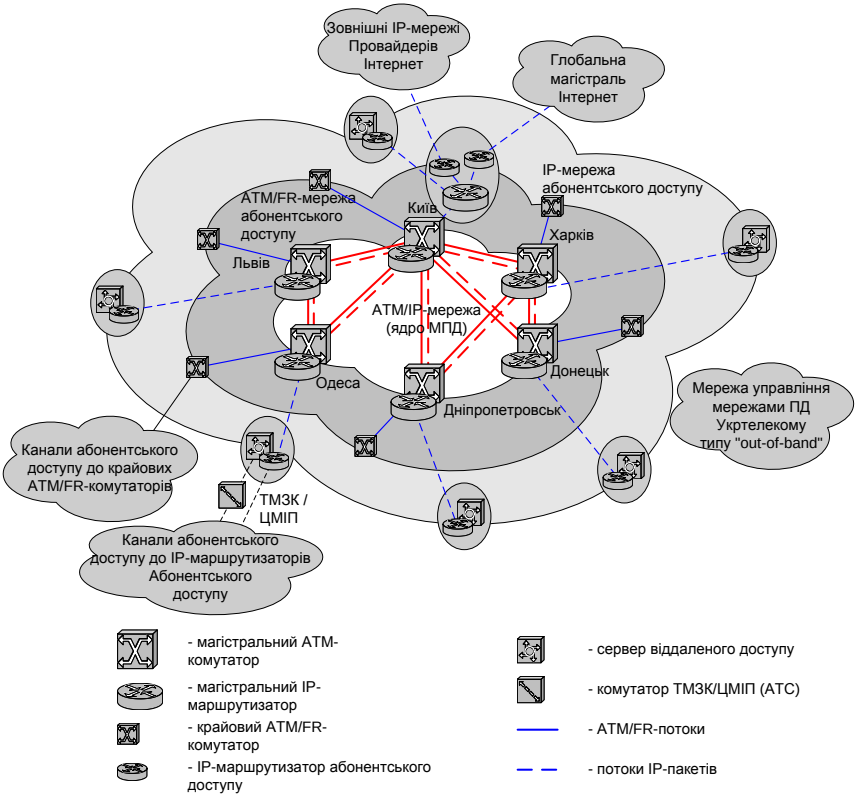


Рис. 2.1. Узагальнена архітектура моделі об’єкта експлуатації (обладнання первинної мережі на рисунку не відображено)

Проміжний шар в архітектурі моделі представляє магістральну транспортну мережу, що побудована на базі технологій ATM та IP, а зовнішній шар – мережі абонентського доступу ATM/FR та IP.

Будемо вважати, що мережі абонентського доступу на базі IP використовуються для надання інтернет-послуг, включаючи забезпечення доступу до глобальної магістралі Інтернет. А мережі абонентського доступу на базі ATM/FR використовуються у двох основних напрямках застосування – для забезпечення транспорту IP-пакетів від абонентських вузлів до вузлів IP-мереж і для надання послуг оренди каналів ATM/FR, включаючи організацію

підключень до магістральної транспортної мережі з використанням HDLC-подібних протоколів.

Ядро транспортної мережі (проміжний шар в архітектурі моделі об'єкта експлуатації) являє собою магістральну ATM/IP-мережу, вузли котрої (що розташовані, наприклад, у найбільших містах України) з'єднуються між собою високошвидкісними магістральними каналами передачі даних (ПД) за схемою "із резервуванням напрямків". Міжвузлові з'єднання у магістральній мережі здійснюються за технологією ATM. Будемо вважати, що пропускна спроможність кожного магістрального каналу ПД у цій мережі – 155 Мбіт/с. Через неї циркулюють мультиплексовані потоки даних від магістральних ATM-комутаторів та IP-маршрутизаторів, а також комутаторів та (або) маршрутизаторів мереж доступу (до магістральної транспортної мережі). У склад магістральної транспортної мережі включена лінійка серверів різного функціонального призначення.

Зовнішній (по відношенню до ядра) шар в архітектурі моделі розтинається на два прошарки. Перший прошарок – це ATM/FR-мережа абонентського доступу. Вузли цієї мережі приєднуються до ATM-комутаторів магістральної мережі через високошвидкісні канали ПД. В цих вузлах розташовані крайові (граничні) ATM/FR-комутатори, до портів котрих під'єднуються користувачі через канали абонентського доступу. Будемо рахувати, що пропускна спроможність кожного такого абонентського каналу доступу у ATM/FR-мережу – до 2,048 Мбіт/с. Через них циркулюють мультиплексовані потоки даних від пристроїв доступу до FR-вузлів, які називають пристроями FRAD (Frame Relay Access Device), або від абонентських ATM-систем (зокрема, ATM-LAN, Private ATM-switch, IAD і т. ін.) до крайових ATM/FR-комутаторів. Будемо вважати, що для передавання даних в ATM/FR-мережі абонентського доступу використовується технологія постійних віртуальних каналів (PVC).

Примітка 4. Мережі абонентського ATM/FR-доступу. Послуги мереж абонентського ATM/FR-доступу використовуються, здебільшого, для об'єднання корпоративних локальних мереж між собою. Ці мережі абонентського доступу підключаються до магістральної транспортної ATM-мережі через крайові ATM/FR-маршрутизатори/мультиплексори.

Якщо для підключення до магістральної транспортної мережі використовується технологія FR, то до складу обладнання мереж абонентського доступу повинен входити спеціальний пристрій доступу – FRAD. Найчастіше пристрій FRAD є невід'ємною частиною IP-маршрутизаторів, але він, також, може бути конструктивно оформлений у вигляді окремого пристрою. В цьому випадку для його підключення до маршрутизотора використовуються інтерфейси 10BaseT/100BaseTX, V.24, V.35, V.36, V.11. Для зв'язку FRAD з крайовими ATM/FR-комутаторами/мультиплексорами використовуються цифрові та (або) аналогові виділені канали тощо. Каналоутворююче обладнання (ПОД/ПОК, синхронні/асинхронні аналогові модеми) може входити до складу FRAD (маршрутизатора) або бути конструктивно оформленим у вигляді окремих пристроїв.

В деяких випадках крайові ATM/FR-комутатори можуть під'єднуватися до магістральних ATM-комутаторів за технологією FR, тобто через інтерфейс NNI FR із швидкістю 2,048 Мбіт/с.

Схема абонентського доступу до магістральної транспортної мережі з використанням технології FR зображена на рис.2.2.

Між абонентськими пристроями FRAD через комутатори транспортної мережі встановлюються постійні віртуальні канали. Послуги комутованих віртуальних каналів на практиці через відсутність попиту практично не надаються. При встановленні постійного віртуального каналу задається його узгоджена швидкість (CIR) та додаткова максимальна швидкість (EIR).

Другий прошарок зовнішнього шару в структурі моделі об'єкта експлуатації – це IP-мережа абонентського доступу, що призначена, головним чином, для надання послуг Інтернет. Вузли цієї мережі приєднуються до IP-маршрутизаторів магістральної ATM/IP-мережі із використанням цифрових потоків типу E1 (із швидкістю 2,048 Мбіт/с), що утворюються за допомогою обладнання первинної мережі.

Користувачі IP-мережі підключаються до вузлів доступу мережі IP, тобто до IP-маршрутизаторів абонентського доступу, за допомогою синхронних та (або) асинхронних некомутованих ліній, TDM-каналів, FR-каналів, а також комутованих каналів телефонних мереж загального користування (аналогових - ЗАКТМ

і цифрових – ЦМІП). Через IP-мережу користувачі мають доступ до глобальної мережі Інтернет.

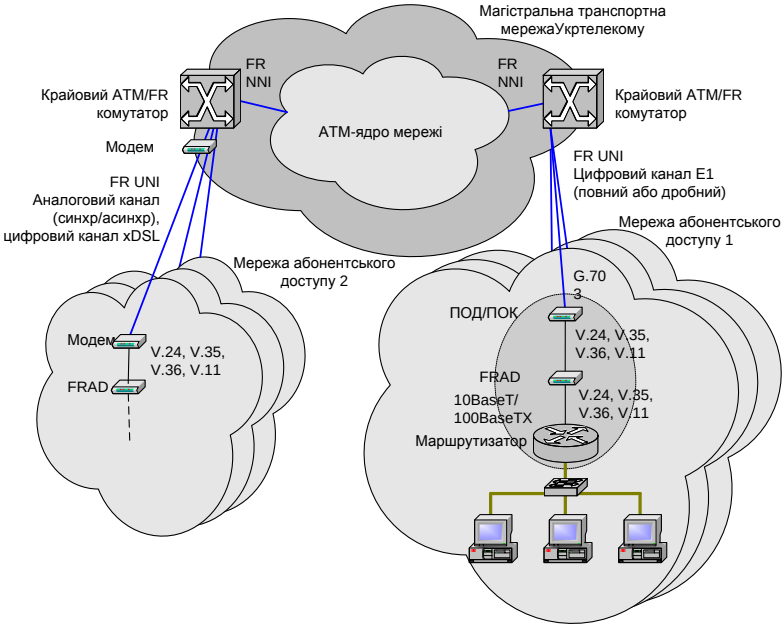


Рис. 2.2. Схема абонентського *FR* -доступу до магістральної транспортної мережі

Примітка 5. Мережі абонентського IP-доступу. Мережі абонентського доступу підключаються до транспортної IP-мережі через вузли доступу (ВД). До складу основного обладнання типового ВД входить маршрутизатор абонентського доступу, сервери віддаленого доступу (RAS), сервери DNS RESOLVER та RADIUS PROXY. Обладнання ВД з'єднується між собою через локальну обчислювальну мережу (ЛОМ), поділену міжмережним екраном на окремі зони захисту. Поділ об'єктів ЛОМ за зонами захисту здійснюється відповідно до прийнятої політики забезпечення захисту інформаційних ресурсів ВД. Функції міжмережного екрану може здійснювати маршрутизатор абонентського доступу або окремий програмно-апаратний засіб.

Типова конфігурація апаратних засобів ВД зображена на рис. 2.3. Поряд з ВД до транспортної IP-мережі розміщуються вузли доступу до прикладних служб Інтернету, типова конфігурація яких також показана на рис. 2.3.

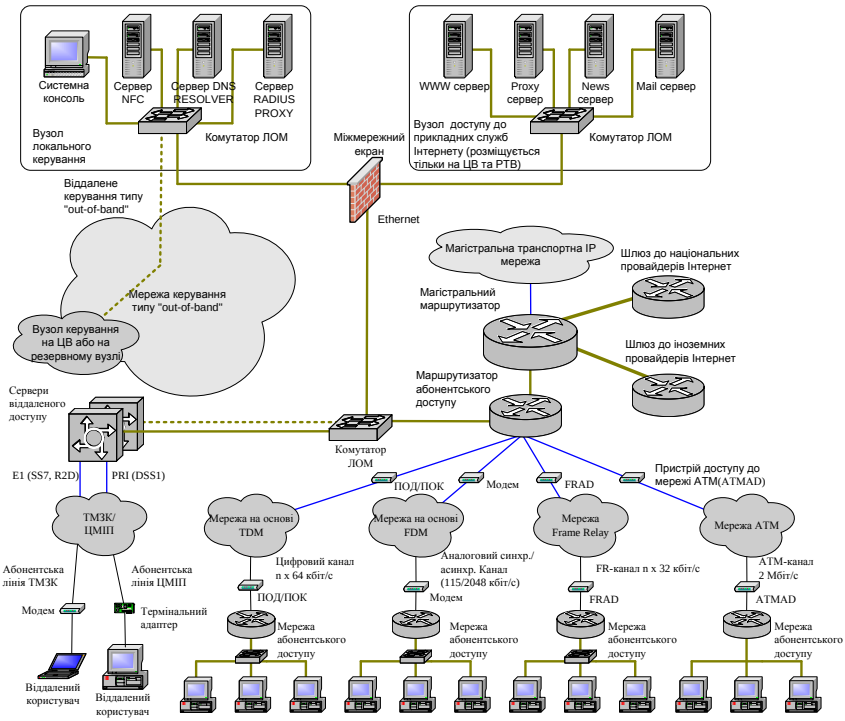


Рис. 2.3. Типова конфігурація апаратних засобів вузла доступу до *IP*-мережі

Мережі абонентського доступу підключаються до ВД через комутовані та (або) виділені канали зв'язку. У минулому використовувались, здебільшого, аналогові комутовані канали. Але є можливим застосування цифрових комутованих каналів. Аналогові комутовані канали – це, як правило, канали телефонної мережі загального користування ЗАКТМ із смугою пропускання 3,1 кГц. Цифрові комутовані канали, якщо вони використовуються, то це – канали BRI цифрової мережі з інтеграцією послуг (ЦМІП). Для організації каналів абонентського доступу через канали ЗАКТМ/ЦМІП використовуються відповідно аналогові модеми/термінальні адаптери (ТА).

В якості шлюзів між мережами з комутацією каналів, через які здійснюють доступ користувачі послуг МПД, та транспортною IP-

мережею використовуються сервери віддаленого доступу (СВД). СВД підключаються до ЗАКТМ через інтерфейси Е1. Обмін службовою інформацією з комутаторами ЗАКТМ (тобто, з АТС) відбувається за допомогою систем сигналізації СКС7, R2D та інших. Для підключення СВД до мережі ЦМІП використовуються інтерфейси PRI. Обмін службовою інформацією з комутаторами ЦМІП здійснюється за допомогою системи сигналізації DSS1.

На деяких периферійних вузлах з невеликою кількістю абонентів в якості СВД іноді використовуються персональні комп'ютери (ПК) із встановленим спеціальним програмним забезпеченням (ПЗ). До цих ПК через мультипортові плати з інтерфейсами RS-232C/V.24 підключені аналогові модеми. Модеми, в свою чергу, підключені до абонентських ліній ТМЗК.

Перед отриманням доступу через комутовані канали до транспортної IP-мережі виконуються процедури ідентифікації та автентифікації користувачів. Для цього використовується програмне забезпечення СВД та сервера RADIUS PROXY.

Обладнання та ПЗ, яке є необхідним для виконання безпосередніх функцій сервера RADIUS PROXY, входить до складу будь-якого ВД. Але спеціалізоване ПЗ та обладнання сервера RADIUS, яке виконує функції керування, входить до складу тільки вузла керування мережею, що розташований на ЦВ або на регіонально-транзитному вузлі, який виконує функції резервного вузла керування. До складу цих вузлів керування (тобто, основного і резервного) входить, крім того, спеціалізоване ПЗ та обладнання СВД із використанням ЗЗК, а також ПЗ, що здійснює функції управління ресурсами модемного пулу. ПЗ серверів СВД та RADIUS забезпечує облік обсягів наданих послуг комутованого доступу.

Крім комутованих аналогових і цифрових каналів для доступу до глобальної транспортної IP-мережі наразі використовуються виділені канали. Виділені канали також можуть бути аналоговими та (або) цифровими.

Аналогові виділені канали – це ненавантажені двох або чотирьох проводові канали (тобто, фізичні лінії), що з'єднують абонентське обладнання з маршрутизаторами вузлів доступу, або навантажені аналогові канали, що входять до складу первинних

мереж з частотним ущільненням каналів (FDM). В якості каналоутворюючого обладнання в цих випадках використовуються аналогові модеми. Допускається використання асинхронних (з максимальною швидкістю передачі даних 115,2 кбіт/с) та синхронних (з максимальною швидкістю передачі даних 2048 кбіт/с) аналогових модемів.

Цифрові виділені канали – це канали цифрових первинних мереж з ущільненням каналів за часом (*TDM*). В якості каналоутворюючого обладнання для підключення мереж абонентського доступу до транспортної *IP*-мережі через виділені цифрові канали мереж *TDM* використовуються пристрої обслуговування даних/пристрої обслуговування каналу ПОД/ПОК (DSU/CSU). Швидкість передачі даних виділених цифрових каналів є кратною 64 кбіт/с.

Крім того, для доступу до магістральної *IP*-мережі є можливим використання постійних віртуальних каналів транспортних мереж *ATM/FR*. Мережі абонентського доступу підключаються до мережі *FR* за допомогою спеціального обладнання доступу – пристрою *FRAD* (*Frame Relay Access Device*). Один із портів маршрутизатора ВД також підключений до мережі *FR*. При замовленні абонентом послуги доступу до магістральної *IP*-мережі між абонентським пристроєм *FRAD* та пристроєм *FRAD*, що підключений до порту *IP*-маршрутизатора, встановлюється постійний віртуальний *FR*-канал, через який абонентська мережа отримує доступ до транспортної мережі.

Для вирішення задач керування ТЛК-системою та контролю її працездатності у рамках прийнятої моделі об’єкта експлуатації створена відповідна мережа управління. Реалізується управління типу “*out-of-band*” (тобто, позасмугове керування). Такий тип управління передбачає створення потоків сигналів управління та іншої технологічної інформації через фізично відокремлені канали зв’язку, що сприяє підвищенню живучості та надійності функціонування мереж. На відміну від керування типу “*out-of-band*” у більш простих та менш відповідальних ТЛК-системах нерідко використовується керування типу “*in-band*” (тобто, внутрішньосмугове керування), коли потоки сигналів управління просуваються тими ж каналами, що і абонентська інформація.

Примітка 6. Системи керування. Керування ТЛК-системами здійснюється як за допомогою спеціалізованих програмно-апаратних систем керування, що встановлені у виділених центрах керування (ЦК) (як правило, основний – на центральному вузлі ЦВ ТЛК-системи та резервний – на одному із регіонально-транзитних вузлів РТВ) і дозволяють виконувати централізоване управління територіально розгалуженим ТЛК-обладнанням та всією ТЛК-системою у цілому, так і шляхом використання штатного ПЗ окремих елементів ТЛК-системи (комутаторів, маршрутизаторів, серверів тощо).

Зазвичай керування ядром магістральної транспортної мережі IP/ATM/FR (тобто, центральним вузлом, регіонально-транзитними та регіональними вузлами РВ) здійснюється централізовано персоналом виділених ЦК. На практиці використовуються системи керування ядром транспортної мережі ATM/FR та ядром мережі IP, що є повністю незалежними одна від одної. У багатьох випадках керування територіальними та периферійними вузлами (ПВ) IP-мережі здійснюється локально персоналом відповідних вузлів. Крім того, персонал всіх вузлів IP-мережі здійснює локальне керування серверами інтернет-сервісів IP-мережі (DNS, SMTP тощо).

Керування магістральною транспортною мережею ATM/FR здійснюється, як правило, централізовано за допомогою програмно-апаратних засобів ЦК. ЦК здійснюється контроль та керування комутаторами транспортної мережі, які розміщені на центральному вузлі, регіонально-транзитних та регіональних вузлах ТЛК-системи. Зокрема, виконується керування конфігурацією комутаторів, збір статистичної інформації і генерація звітів, обробка збоїв і відмов у роботі обладнання тощо.

В якості програмної платформи ЦК транспортної мережі як один із можливих варіантів може використовуватися ПЗ Network Management System (NMS). За допомогою NMS системні адміністратори центра керування повністю контролюють комутатори ядра транспортної мережі ATM/FR.

ПЗ NMS працює під керуванням операційної системи Sun Solaris. В основі ПЗ NMS лежить архітектура клієнт/сервер. ПЗ користувачів взаємодіє з ПЗ сервера NMS через відокремлену від магістральної мережі IP-мережу управління (тобто, використовує тип управління “out-of-band”). Для взаємодії серверного ПЗ NMS з магістральними комутаторами, як правило, використовуються

фірмові технології виробника АТМ-комутаторів.

До складу ПЗ NMS входить кілька окремих модулів. Центральним модулем NMS є InfoCenter. Він створює спільне операційне середовище для інших модулів NMS. Завдяки використанню InfoCenter системні адміністратори мають можливість візуально контролювати ресурси мережі, спостерігати її фізичну та логічну топології тощо.

Модуль OmniView забезпечує послуги зі збору статистичної інформації про роботу як мережі в цілому та її підмереж, так і окремих портів мережного обладнання, її обробки та генерації звітів. Цей модуль здатний взаємодіяти з будь-яким обладнанням, що сумісне із специфікацією MIB II (RFC 1213, ISO 8824:1987, МСЕ-Т X.208). (Ця специфікація буде розглянута у лекції № 4). Інформація, яка зібрана OmniView, відображається на екрані графічного інтерфейсу системного адміністратора у вигляді діаграм, графіків та/або таблиць.

Модуль Path Trace призначений для обслуговування зв’язків між вузлами мережі. За допомогою цього модулю забезпечується діагностика серверного, клієнтського та іншого мережного обладнання та каналів зв’язку між ними. Інформація про стан обладнання відображається у графічній формі.

Модуль Fault Summary призначений для збору інформації про збої, відмови та помилки в роботі обладнання та її обробки. Зібрана інформація відображається на екрані графічного інтерфейсу користувача модуля Fault Summary разом з рекомендаціями щодо усунення виниклих проблем. Засобами цього модулю системні адміністратори повідомляються про виникнення нештатних ситуацій в мережі (електронною поштою та/або через мережі персонального радіовиклику).

Модуль Expanded View відображає на екрані графічного інтерфейсу користувача інформацію про поточний стан конкретних мережних пристроїв, дозволяє їх моніторинг, конфігурування, збір статистики тощо.

Керування магістральною мережею IP виконується централізовано за допомогою програмно-апаратних засобів відповідних ЦК (основного – на ЦВ ТЛК-системи та резервного – на РТВ). За допомогою засобів цих ЦК здійснюється контроль та

керування маршрутизаторами ядра IP-мережі. Зокрема, виконується керування конфігурацією обладнання та маршрутизацією трафіку, збір статистичної інформації і генерація звітів, обробка збоїв і відмов у роботі обладнання тощо.

За допомогою спеціалізованого ПЗ системні адміністратори центрів керування контролюють маршрутизатори ядра IP-мережі.

У глобальних розгалужених ТЛК-системах, як правило, використовуються централізовані та децентралізовані (локальні) схеми ТЕ ТЛК-обладнання. Під час побудови схем ТЕ мають на увазі, що трудовитрати при централізованому обслуговуванні у середньому не перевищують 0,05 людино/годин на одне еквівалентне PVC-з'єднання на рік, у той час як при локальній схемі обслуговування цей показник може зрости до 0,4 людино/годин на одне еквівалентне PVC-з'єднання на рік. Тому, щонайменше, функції контролю стану та конфігурування ТЛК-обладнання, що розміщується на вузлах мережі, здійснюється централізованим способом. Для цього використовується окрема фізично або логічно виділена мережа керування. В центрі керування інсталюється спеціалізована програмна або програмно-апаратна система, що виконує функції головного менеджера усієї ТЛК-системи. Іншими словами, робоче місце головного адміністратора об'єкту експлуатації (ТЛК-системи) знаходиться за терміналом центра керування. Саме із цього робочого місця головний адміністратор реалізує функції контролю стану та конфігурування обладнання, що розташовано на всіх вузлах ТЛК-системи. Паралельно ці ж, а також усі інші функції ТЕ можуть здійснюватися персоналом безпосередньо на вузлах за допомогою локальних систем керування ТЛК-обладнанням. У разі порушення зв'язку із центром керування локальні системи керування забезпечують накопичення і збереження тарифної, аварійної, діагностичної та статистичної інформації, а також інших важливих даних.

В останній час в глобальних мережах національного рівню намітилась тенденція до повної централізації функцій керування так, щоби усі ці функції здійснювались засобами центру керування. Це дозволяє суттєво скоротити персонал вузлового обладнання та підвищити рівень керованості мережі.

Штатне обладнання ТЛК-систем для забезпечення функцій ТЕ у більшості випадків спроможне, щонайменше, реалізовувати наступні системні функції:

1) видача повідомлень про стан обладнання підсистем керування;
2) видача аварійних повідомлень;
3) локалізація пошкоджень;
4) функціональне тестування після відновлювальних робіт;
5) перевірка несуперечності даних;
6) ініціювання перезапуску;
7) заміна вмісту пам'яті;
8) видача дампу пам'яті в цілях техобслуговування;
9) управління параметрами навантаження;
10) обмеження обслуговування низькопріоритетних користувачів.

Експлуатаційний персонал, як правило, має можливість запитувати стан елементів обладнання. У відповідь на запити видається вже оброблена засобами ТЛК-системи узагальнена інформація. Існує також можливість шляхом ініціювання додаткових запитів отримувати більш детальну інформацію щодо стану обладнання.

Забезпечується обробка та відповідь на принаймні наступні запити:

1) конфігураційна інформація;
2) узагальнений стан контрольованого обладнання (включаючи аварійну та попереджувальну інформацію);
3) діагностична інформація (детальний стан функціонального модулю, підсистеми керування тощо);
4) детальний стан каналів та портів обладнання;
5) параметри якості обслуговування;
6) параметри навантаження;
7) тарифікаційна інформація;
8) підтвердження виконання команд управління.

Система діагностики ТЛК-обладнання здійснює виявлення та локалізацію проблем в експлуатації цього обладнання, його тестування після ремонту. Наприклад, сучасне ТЛК-обладнання за допомогою засобів системи діагностики забезпечує можливість

автоматичного виявлення проблем при несправностях в одному ТЕЗі з ймовірністю 0,75, а при несправностях одночасно від одного до трьох ТЕЗів з ймовірністю 0,95. В інших 5% випадків місце несправності має визначатися експлуатаційним персоналом.

Вище вказувалось, що прийнята модель об'єкту експлуатації (тобто, ТЛК-мережі) має ієрархічну функціонально-організаційну структуру. Як приклад на рис. 2.4 зображена ієрархія вузлів моделі.

Як бачимо, в залежності від виконуваних функцій, типу обладнання, його ємності та умов використання всі вузли моделі поділені на шість рівнів.

Роботи з технічного обслуговування та ремонту (ТОР) ТЛК-обладнання доцільно структурувати згідно рис. 2.4, тобто організаційна структура системи ТЕ має відображати функціональну (та топологічну) структуру об'єкта експлуатації. Проте розподіл обов'язків між персоналом центру керування мережею та персоналом вузлів залежить від ступеню централізації функцій керування. Із рис. 2.1 та 2.4 витікає, що конкретний зміст задач ТОР, а також вибір методів та процедур їхнього вирішення напряму залежить від:

1) організаційної структури кадрового ресурсу, що забезпечує експлуатацію обладнання ТЛК-системи;

2) виду телекомунікаційної технології, яка реалізується ТЛК-обладнанням;

3) виду технічного обслуговування та ремонту, що виконується експлуатаційним персоналом (поточне, планово-періодичне і т. ін.);

4) рівня вузлу в ієрархічній структурі багаторівневих ТЛК-систем;

5) методу експлуатації, що використовуються для вирішення задач ТОР;

6) виду процедури, що застосовується для реалізації обраного методу експлуатації.

Структуризація робіт з ТОР ТЛК-обладнання у типовій моделі ТЛК-системи надана на рис. 2.5.

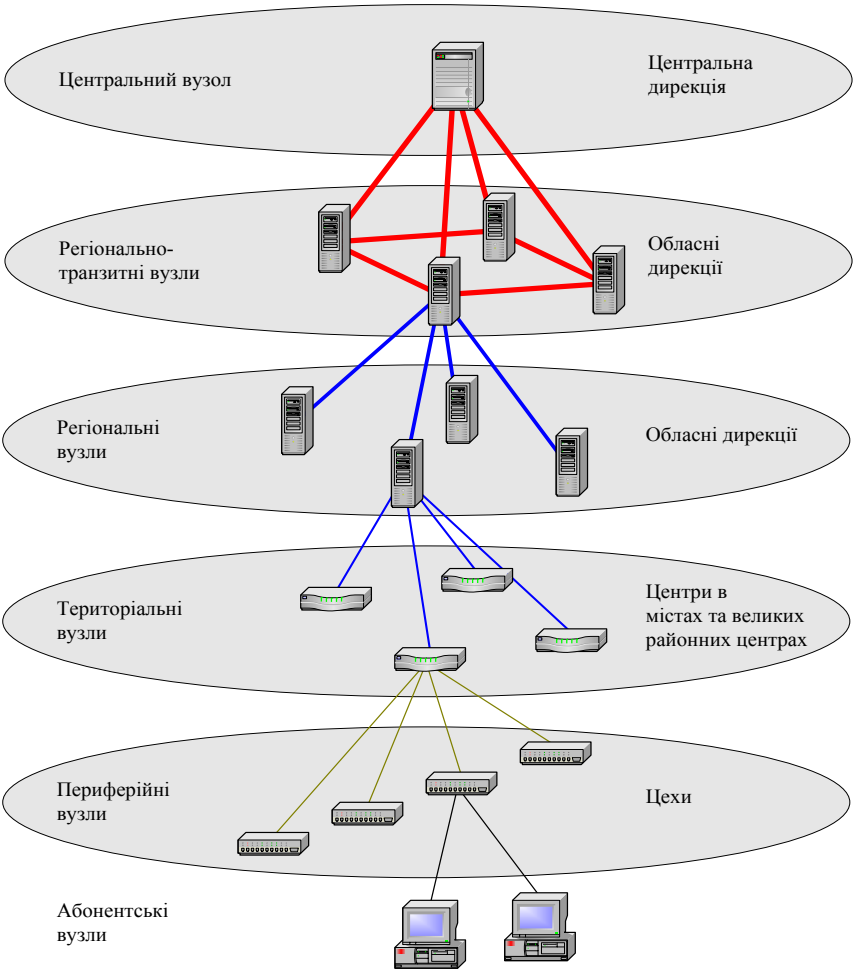


Рис. 2.4. Ієрархія вузлів моделі об’єкту експлуатації

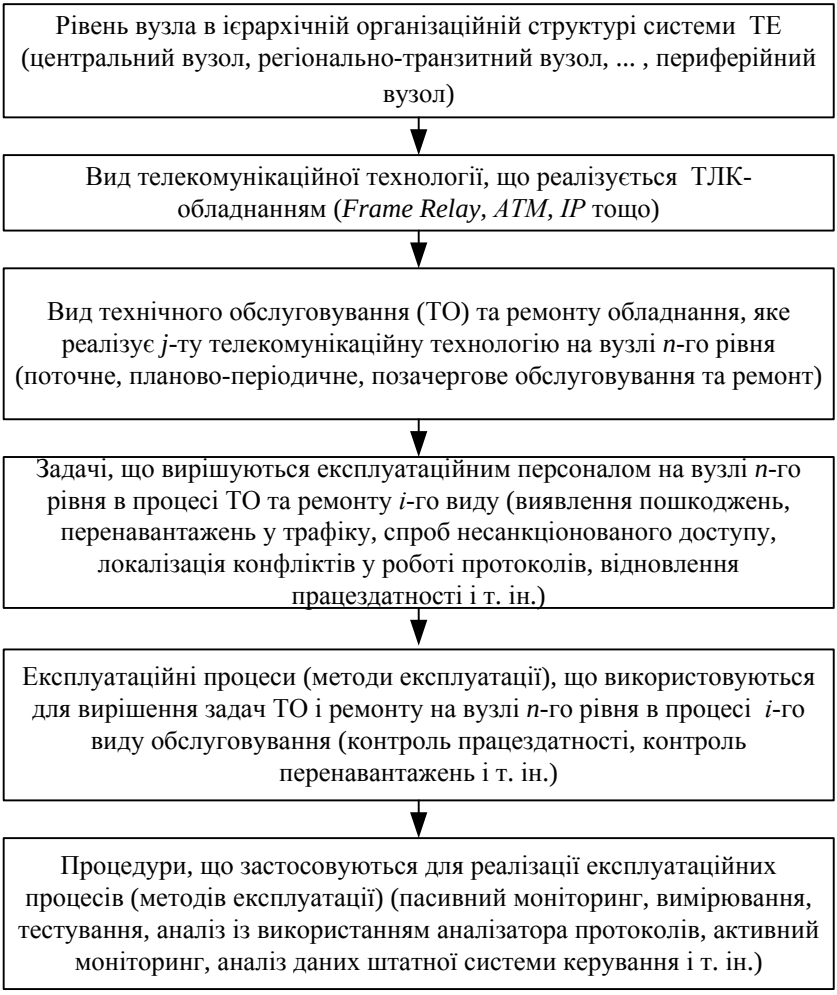


Рис. 2.5. Структуризація робіт з технічного обслуговування та ремонту обладнання у типовій моделі ТЛК-системи

2.4. Організаційне забезпечення технічної експлуатації

Система ТЕ ТЛК-систем складається із спеціально підготовленого адміністративно-технічного персоналу, спеціально підібраних інструментальних програмно-апаратних засобів

технічного забезпечення ТЕ (включаючи тестове забезпечення), відповідної технічної експлуатаційної документації та організаційно-розпорядницької документації, що необхідна для підтримки та відновлювання обладнання.

Організаційна структура експлуатаційних підрозділів повторює ієрархічну функціональну структуру вузлів моделі експлуатації (див. рис.2.4).

В процесі ТЕ адміністративно-технічний персонал (надалі - експлуатаційний персонал) здійснює наступні функції:

1) технічне обслуговування (ТО) обладнання ТЛК-систем;
2) ремонт обладнання ТЛК-систем;
3) утримання та поновлення комплектів запасних частин, інструментів, приладів та матеріалів (надалі – ЗІП);
4) роботи із запровадження нової техніки;
5) рекламаційна робота;
6) ведення експлуатаційно-технічної та облікової документації;
7) збір та узагальнення статистичних даних щодо технічного стану та ушкодження обладнання, а також щодо витрат ЗІП;
8) облік та аналіз показників ТЕ, розробка та впровадження пропозицій щодо її удосконалення.

Персонал, що здійснює ТЕ обладнання транспортування інформації, взаємодіє із експлуатаційними підрозділами первинних ТЛК-мереж з питань:

- зміни структури ТЛК-систем (підключення нових каналів або їх відключення, введення в дію нових вузлів і т. ін.);
- зміни режимів функціонування обладнання;
- узгодження планів виконання ремонтних робіт;
- обміну інформацією щодо стану обладнання, якості обслуговування користувачів (особливо, під час вирішення виниклих проблем щодо працездатності обладнання).

Більшість глобальних ТЛК-систем має ієрархічну мережну структуру, тобто існує центр керування системою, що розташований, як правило, на центральному вузлі цієї системи, та підпорядковані центру сукупності вузлів більш нижчих рівнів ієрархії. Організаційна структура взаємодії підрозділів, що здійснюють надання ТЛК-послуг, адміністративне та технічне

обслуговування ТЛК-систем, відображає структуру цих систем та побудована, як правило, за принципами спеціалізації та подвійної підпорядкованості. Це сприяє раціональному використанню кадрового потенціалу оператора електрозв'язку, зменшенню експлуатаційних витрат, підвищенню надійності функціонування обладнання та якості надання послуг користувачам, спрощенню вирішення питань щодо захисту ТЛК-систем від несанкціонованого доступу і т. ін.

Подвійна підпорядкованість передбачає, що функції безпосереднього адміністрування експлуатаційним персоналом здійснює керівництво вузлів ТЛК-системи, в той час як у сфері забезпечення технологічної дисципліни і здійснення процесів ТЕ цей персонал підпорядковується відповідним підрозділам центру керування ТЛК-системою.

Персонал верхніх рівнів організаційної структури, окрім забезпечення виконання експлуатаційних функцій на своїх рівнях організаційної структури, виконують також функції оперативного управління вузлами більш нижчого ієрархічного рівня, які до них приєднані.

З метою зменшення запасного майна і приладів (ЗІП) та експлуатаційних витрат здійснення функцій ТЕ зосереджується з максимально можливим ступенем централізації. На периферійних вузлах нижнього рівня штат експлуатаційного персоналу є мінімізованим – лише для забезпечення нормативу на середній час відновлення працездатності обладнання цих вузлів та мережного обладнання користувачів.

На мережах передачі даних (МПД) оперативно-технічне керівництво роботами під час аварій, у тому числі непроходженні сигналів через канали зв'язку, а також під час уведення або виведення каналів, здійснюється так званими керівними вузлами. Центральний вузол МПД є керівним вузлом на прямих зв'язках з будь-якими іншими вузлами, які під'єднані до його портів. Вузол більш високого рівня здійснює оперативне керівництво вузлами більш низького рівнів, що під'єднані до його портів.

Обов'язки експлуатаційного персоналу

На кожному вузлі існують посадові інструкції для експлуатаційного персоналу, що розроблені з урахуванням

організаційної структури підприємства. З метою безперебійного поточного обслуговування обладнання протягом доби може бути організовано чергування персоналу. У цьому випадку персонал розподіляється за трьома робочими змінами. Між взаємодіючими службами вузлів і посадовими особами змін організується службовий зв'язок. Основні аспекти такої взаємодії документуються.

Старший технічний керівник зміни вузла повинний:

а) здійснювати оперативно-технічне керівництво роботою персоналу зміни всіх технічних підрозділів вузла;

б) контролювати роботу чергового персоналу, надавати йому необхідну допомогу у вирішенні виникаючих проблем; у разі тривалих порушень працездатності обладнання особисто брати участь у відновленні його дії;

в) забезпечувати своєчасну організацію обхідних напрямків за умов ушкодження основних;

г) повідомляти головного інженера або начальника вузлу про всі аварії, тривалі порушення працездатності обладнання і прийняті заходи щодо його відновлення;

д) вести запис всіх повідомлень, що відносяться до аварійних ситуацій, у робочому журналі, а після ліквідації аварії або відновлення роботи обладнання оповіщати керівництво про час відновлення і виявлені причини порушень працездатності ТЛК-системи;

е) виявляти нестійкі працюючі з'єднання і вносити пропозиції керівництву вузла щодо поліпшення їхньої роботи;

ж) забезпечувати правильне розміщення персоналу відповідно до його службових обов’язків, стежити за виробничою дисципліною в зміні;

з) удосконалювати свої технічні знання і ділові якості, сприяти підвищенню кваліфікації працівників;

і) сприяти впровадженню й удосконалюванню прогресивних методів праці і поширенню передового досвіду.

Персонал вузла зобов'язаний:

а) добре знати побудову, принцип дії і методи ТЕ устаткування на ділянці, що обслуговується;

б) постійно вести спостереження за роботою дорученого устаткування, своєчасно і у повному обсязі проводити відповідні

профілактичні заходи;

в) у випадку порушення нормальної роботи обладнання із технічних причин уживати негайних заходів до швидшого усунення виниклих проблем;

г) виконувати вимоги правил і інструкцій із технічної експлуатації, правила техніки безпеки, промсанітарії і протипожежних заходів, сумлінно виконувати свої обов'язки відповідно до посадової інструкції.

У випадку зникнення або невідповідності нормам живлячих напруг на устаткуванні вузла персонал, що здійснює його технічну експлуатацію, повинний негайно сповістити про це відповідну службу, а також старшого технічного керівника зміни вузла.

Про виниклі несправності в обладнанні службового зв’язку експлуатаційний персонал повинний негайно повідомляти про це службу, що здійснює обслуговування і ремонт обладнання службового зв’язку, а про несправності вимірювальної апаратури — персонал метрологічної служби.

Черговий персонал зобов'язаний безвідлучно знаходитися на своїй ділянці, безупинно спостерігати за процесом функціонування обладнання, а у разі необхідності втручатися у цей процес, намагаючись забезпечити роботу обладнання із заданою якістю. Черговий працівник може залишити своє робоче місце тільки з дозволу свого керівника.

До часу здавання чергування черговий працівник повинен перевірити наявність і стан резервної апаратури, інструмента, запасних частин, приладів, матеріалів, схем і інструкцій, виконати усі дії, які регламентовані правилами документообігу та упорядкувати робоче місце.

Під час здавання зміни черговий працівник зобов'язаний інформувати працівника, що приймає чергування, про стан устаткування і його роботу за час чергування, про одержані оперативні вказівки і розпорядження, що стосуються організації й експлуатації обладнання, яке є об’єктом контролю.

Працівник, що приймає чергування, зобов'язаний:

а) перевірити наявність і стан резервної апаратури, інструмента, запасних частин, приладів, матеріалів, документації (схем і інструкцій і ін.), санітарний стан робочих місць;

б) ознайомитися із записами у технічних журналах з метою виявлення можливих невідповідностей у цих записах.

Працівники оформляють здавання і приймання чергування шляхом накладення власноручних підписів у технічному журналі або в іншому документі, який призначений для цієї мети. Про результати прийому чергування працівник доповідає старшому технічному керівнику, після чого приймає зміну.

Кваліфікація експлуатаційного персоналу

Кваліфікація працівників, які здійснюють ТЕ, має бути достатньою для виконання ними своїх службових обов'язків, що зафіксовані у відповідних внутрішньокорпоративних документах.

Експлуатаційний персонал повинен проходити спеціалізоване навчання за учбовими програмами, що структуровані відповідно до організаційної структури системи ТЕ. Працівники допускаються до роботи з обладнанням тільки при позитивних результатах атестації їхніх знань після навчання.

2.5. Технічне забезпечення технічної експлуатації

Увесь широкий спектр робіт з експлуатації різноманітного ТЛК-обладнання (якщо мова йде про оператора чи провайдера телекомунікаційних послуг національного масштабу) майже неможливо охопити у рамках однієї організаційної структури експлуатаційного персоналу. Тому експлуатаційні організації спеціалізуються за видами ТЛК-обладнання. В основі спеціалізації лежить семирівнева модель взаємодії відкритих інформаційних систем згідно з ГОСТ 28906, що стандартизована ISO (ИСО 7498). На практиці експлуатаційні організації, що спеціалізуються на експлуатації обладнання фізичного рівня (згідно семирівневої моделі), виділяються в окрему групу – операторів первинних мереж та систем передачі (наприклад, Дирекція первинних мереж Укртелекому). Засоби технічного забезпечення ТЕ обладнання фізичного рівня будуть розглянуті у подальших лекціях. Другу групу складають телекомунікаційні оператори та провайдери, що спеціалізуються на експлуатації обладнання транспортування інформації (це обладнання реалізує інтерфейси і протоколи від канального до сеансового рівнів). Третя група складається із провайдерів інформаційних сервісів, що експлуатують обладнання

від сеансового до прикладного рівнів.

Розглянемо технічне забезпечення експлуатації обладнання транспортування інформації. Для здійснення функцій ТЕ цього обладнання експлуатаційні підрозділи ТЛК-оператора використовують наступні групи технічних (у т.ч., програмно-технічних) засобів:

1) засоби технічного обслуговування і ремонту (ТОР) основного технологічного обладнання ТЛК-систем;

2) засоби спостереження і контролю навантаження (тобто, засоби контролю трафіка);

3) засоби оперативного керування конфігурацією програмно-апаратних компонентів та ТЛК-систем у цілому;

4) засоби контролю стана обладнання захисту від фізичних ушкоджень та розкрадань;

5) засоби отримання і зберігання запасних частин, матеріалів та комплектуючих;

6) засоби планування запасів матеріальних ресурсів;

7) засоби обліку та виконання правил документообігу.

Примітка 7. Слід мати на увазі, що більшість провайдерів не забезпечує свої експлуатаційні підрозділи спеціалізованими технічними засобами виконання таких видів робіт як:

- ТО і ремонт засобів технічного захисту інформації (ТЗІ);
- контроль конфігурації середовища експлуатації ТЛК-систем;
- контроль стану засобів довкілля;
- здавання відходів в утиль;
- ремонт із залученням сторонніх організацій.

Для виконання перерахованих вище робіт вважається за доцільне користуватися послугами сторонніх спеціалізованих організацій.

Група технічних засобів ТОР основного технологічного обладнання складається із:

1) програмних і апаратних модулів, що входять у штатні комплекти поставок обладнання спеціалізованих систем централізованого керування ТЛК-системами;

2) програмних і апаратних модулів, що входять у штатні комплекти поставок обладнання вузлів локального керування (зокрема, серверів віддаленого доступу (*RAS*), серверів *RADIUS PROXY* та *NFC* тощо);

3) програмних і, можливо, апаратних модулів, що входять у штатні комплекти поставок міжмережних екранів (файєрволів);

4) програмних і апаратних модулів, що входять у штатні комплекти поставок магістральних і крайових *Ethernet/ATM/FR*-комутаторів;

5) програмних і апаратних модулів, що входять у штатні комплекти поставок магістральних *IP*-маршрутизаторів та *IP*-маршрутизаторів абонентського доступу;

6) програмних і апаратних модулів, що входять у штатні комплекти поставок шлюзового обладнання;

7) спеціалізованого багатофункціонального програмно-апаратного пристрою для аналізу телекомунікаційних протоколів типа *HPJ2300D* (*HP Internet Advisor*) виробництва компанії *Agilent Techologies* (США).

Вищеназване обладнання використовується в процесах ТЕ мереж передачі даних (МПД) у якості засобів вимірювань, тестування, моніторингу, логічного аналізу, обробки даних, експертного аналізу, а також для автоматизації процесів ТЕ МПД.

Група технічних засобів спостереження і контролю навантаження має склад обладнання, що співпадає із складом попередньої групи технічних засобів.

Група засобів оперативного керування конфігурацією складається із програмних і апаратних модулів, що входять у штатні комплекти поставок обладнання централізованої і локальних систем керування.

Група технічних засобів контролю стану обладнання захисту від фізичних ушкоджень та розкрадань складається із: елементів системи охоронно-пожежної сигналізації, що контролюють стан цих систем; засобів відеонагляду; допоміжних спеціалізованих систем проводового та радіозв'язку для оснащення працівників служби охорони.

Група технічних засобів отримання і зберігання запасних частин, матеріалів та комплектуючих складається із транспортних засобів для перевезення вантажів та спеціалізованих засобів зберігання запасного майна (сейфи, шкафи, холодильники, кондиціонери і т. ін.).

До складу технічних засобів контролю конфігурації середовища

експлуатації МПД, засобів планування запасів матеріальних ресурсів і засобів обліку та виконання правил документообігу відноситься комп'ютерна та інша оргтехніка, а також відповідне спеціалізоване ПЗ.

2.6. Інформаційне забезпечення технічної експлуатації

ТЕ телекомунікаційних систем пов'язана не тільки із особливостями використання програмно-технічних засобів та із задіяними адміністративно-організаційними заходами, що спрямовані на досягнення визначених цілей експлуатації. Необхідно мати чітке уявлення про множину експлуатаційних процесів та процедур, які необхідно здійснювати на стадії експлуатації цих систем. Іншими словами, необхідно мати моделі експлуатаційних процесів, реалізація котрих на практиці дозволить досягти визначені цілі експлуатації. Окрім того, необхідно знати структуру взаємозв'язків між службами та процесами обслуговування, множину параметрів, що впливають на працездатність обладнання, а також норми на припустимі діапазони значень цих параметрів. Вищенаведені дані складають зміст інформаційного забезпечення прийнятих технологій ТЕ.

Основні характеристики інформаційного забезпечення експлуатації ТЛК-систем, зокрема моделі експлуатаційних процесів та процедур, що набули широкого застосування на практиці, детально висвітлені в лекції №15.

2.7. Метрологічне забезпечення технічної експлуатації

Технічна експлуатація ТЛК-обладнання передбачає необхідність широкого застосування інструментальних засобів випробувань, вимірювань та контролю (надалі – засобів вимірювань або інструментальних засобів). Ці засоби повинні не тільки справно виконувати покладені на них функції, але і протягом періоду їхньої експлуатації не погіршувати свої технічні характеристики, зокрема характеристики точності. Внаслідок об'єктивних причин (зокрема, через природнє старіння компонентів вимірювальних систем, схованих відмов, нештатних ситуацій у середовищі експлуатації і т.ін.) характеристики будь-якого інструментального засобу рано чи пізно, але можуть відхилитися від номінальних значень, що вказані

у його технічному паспорті. І якщо не уживати відповідних заходів із метрологічного забезпечення експлуатаційних робіт, то може так трапитися, що події відхилення характеристик вимірювальних приладів від номінальних значень, зокрема характеристик точності, будуть не помічені експлуатаційним персоналом. Зрозуміло, що користування приладами, які неадекватно відображають реальність, може призвести до негативних наслідків. Тому необхідно мати гарантії, що характеристики усіх засобів вимірювань, що застосовуються під час експлуатаційних робіт, своєчасно атестовані, тобто перевірені (метрологи кажуть: „повірені") кваліфікованими спеціалістами за допомогою надійних методик, а результати атестації відповідають номінальним значенням. Зміст робіт із метрологічного забезпечення як раз і полягає у періодичних повірках і, у разі необхідності, відповідних настройках інструментальних засобів ТЕ.

В Україні, як і в багатьох інших країнах, проблема підтримки коректного функціонування засобів вимірювань, враховуючи її важливість, вирішується на державному рівні. Створена національна мережа метрологічних служб, що надає послуги з атестації засобів вимірювань згідно заявок клієнтів. Розроблені (і розроблюються) нормативні документи (НД), зокрема Держстандартом України, що регламентують усі аспекти метрологічних робіт.

Метрологічне забезпечення ТЕ ТЛК-обладнання має відповідати вимогам НД, чинним в Україні, а засоби вимірювань мають пройти метрологічну атестацію згідно з ДСТУ 3215 та повірку згідно з ДСТУ 2708. Забороняється використання засобів вимірювань, що не пройшли атестацію (повірку) у встановлені строки.

Відповідно до чинного законодавства уся множина параметрів ТЛК-обладнання розділена на три групи:

1) група параметрів, для вимірювання котрих в умовах експлуатації ТЛК-обладнання мають використовуватися засоби вимірювань, які підлягають обов'язковому державному метрологічному контролю та нагляду;

2) група об'єктів телекомунікаційної галузі, параметри та характеристики котрих не підпадають під сферу розповсюдження державного метрологічного контролю та нагляду (а серед них –

більшість параметрів та характеристик, що пов'язані із якістю функціонування ТЛК-обладнання), проте правила та умови вимірювань цих параметрів та характеристик визначаються органами відомчого метрологічного контролю та нагляду;

3) група всіх інших об'єктів телекомунікаційної галузі, правила та умови вимірювань параметрів котрих визначаються власниками об'єктів експлуатації.

До номенклатури параметрів, для вимірювання котрих мають використовуватися засоби вимірювань, які підлягають обов'язковому державному метрологічному контролю та нагляду, входять:

1) параметри каналів ТЧ і аналогових трактів первинної мережі (залишкове затухання або підсилення, нерівномірність амплітудно-частотної характеристики (АЧХ) залишкового затухання, параметри завадостійкості тощо);

2) параметри цифрових каналів та трактів (швидкість передавання цифрових сигналів, параметри імпульсів, показники помилок тощо);

3) параметри металічних кабелів зв'язку (електричний опір ізоляції, випробувальна напруга, перехідне затухання або захищеність, частотна характеристика, відстань до обривів та неоднорідностей);

4) параметри волоконно-оптичних систем передачі (довжина хвилі оптичного випромінювання; рівень середньої потужності оптичного сигналу; чутливість оптичного приймача; затухання регенераційної секції оптичного кабелю; дисперсія; відстань до обривів та неоднорідностей);

5) деякі параметри систем обліку обсягів надання клієнтам мережних послуг.

Примітка 8. Обов'язковому державному контролю та нагляду підлягають засоби вимірювань параметрів також деяких інших систем та каналів передачі, які використовуються у якості транспортного або синхронізуючого середовища на мережах передачі даних (зокрема, параметри апаратури радіорелейних та супутникових систем передачі, параметри тактової мережної сигналізації та ін.).

До номенклатури параметрів, для вимірювання котрих в умовах експлуатації ТЛК-обладнання мають використовуватися засоби вимірювань, які підлягають відомчому метрологічному контролю

та нагляду, входять:

1) параметри обладнання *Frame Relay*;

2) параметри обладнання *ATM*:

параметри обладнання *IP*.

Це дуже широкий перелік параметрів, з котрим корисно ознайомитись, зокрема, звернувшись до сайтів Мінінфраструктури. Наприклад, відомчому метрологічному контролю підлягають наступні параметри IP-обладнання:

– кількість октетів, що прийняті портом за час спостереження [байт];

– кількість пакетів із індивідуальними (*unicast*) *IP*-адресами одержувачів, які надійшли до порту і були доставлені протоколам верхніх рівнів за час спостереження [пакетів];

– кількість пакетів із широкомовними (*broadcast*) та груповими (*multicast*) *IP*-адресами одержувачів, які надійшли до порту і були доставлені протоколам верхніх рівнів за час спостереження [пакетів];

– кількість пакетів, які надійшли до порту і були відкинуті (дискартовані) за час спостереження [пакетів];

– кількість пакетів, які мали помилки, що завадили доставці даних цих пакетів протоколам верхніх рівнів за час спостереження [пакетів];

– кількість пакетів, які надійшли до порту і були відкинуті (дискартовані) через те, що програмно-апаратним засобам контрольованого *IP*-обладнання, які реалізують стек протоколів TCP/IP, не вдалося визначити протокол верхнього рівня, якому необхідно доставити дані цього пакета [пакетів];

– кількість октетів, що були передані портом за час спостереження [байт];

– кількість пакетів із індивідуальними (*unicast*) IP-адресами одержувачів, які були відправлені портом за час спостереження [пакетів];

– кількість пакетів із широкомовними (broadcast) та груповими (multicast) IP-адресами одержувачів, які були відправлені портом за час спостереження [пакетів];

– кількість пакетів, які були відкинуті (дискартовані) за час

спостереження [пакетів];

– кількість пакетів, які мали помилки, що завадили відправці цих пакетів за час спостереження [пакетів];

– середній час затримки передачі пакетів, варіація часу затримки [с];

– продуктивність інтерфейсу в байтах, тобто число октетів, які були передані та прийняті інтерфейсом за одиницю часу [байт/с];

– продуктивність інтерфейсу в протокольних блоках даних, тобто число протокольних блоків даних, переданих та прийнятих інтерфейсом за одиницю часу [пакетів/с];

– коефіцієнт використання пропускної здатності інтерфейсу, тобто відношення числа октетів, що були передані та прийняті інтерфейсом за час спостереження, до максимальної пропускної здатності цього інтерфейсу [%];

– загальна кількість помилкових пакетів, тобто загальна кількість протокольних блоків даних, які не були доставлені протоколу вищого рівня [пакетів];

– коефіцієнт помилкових пакетів, тобто відношення кількості помилкових пакетів до загальної кількості пакетів, що були передані та прийняті інтерфейсом за час спостереження [%];

– довжина вихідної черги пакетів [пакетів].

Усі перераховані вище параметри фіксуються, як правило, штатними засобами будь-якого сучасного магістрального маршрутизатора.

Засоби вимірювань будь-якого оператора електрозв'язку або провайдера інформаційних сервісів повинні підлягати випробуванням з метою затвердження типу засобу вимірювань, який дозволено використовувати для вимірювань, мати відповідні сертифікати Держстандарту та проходити періодичні перевірки. Процес перевірки засобів вимірювань виконується згідно з вимогами регламентуючих документів Держстандарту України. Результатом перевірки є підтвердження придатності засобу вимірювань до використання (у цьому разі на засіб або на його технічний паспорт наноситься відповідне клеймо і видається "Свідоцтво про перевірку") або визнання його непридатним до використання.

Слід наголосити, що в експлуатаційній практиці трапляються ситуації, коли вимірювання одних тих самих параметрів за допомогою двох різних методик дають неоднакові результати. Виробники вимірювальної техніки, як правило, намагаються застосовувати методики, що рекомендуються Держстандартом. Щоб уникнути можливих похибок, експлуатаційникам теж слід намагатися користуватися методиками вимірювань, що рекомендовані Держстандартом. Тому фахівці, що професійно займаються експлуатацією ТЛК-обладнання, повинні постійно відвідувати відповідні сайти Держстандарту та Мінінфраструктури з тим, щоб своєчасно отримувати інформацію щодо змін у нормативній базі з питань метрологічного забезпечення.

Контрольні питання до другої лекції:

1. Чим відрізняється поняття „технічна експлуатація" від поняття „технічне обслуговування" ?
2. Що таке „ремонт обладнання" ?
3. Яка основна ціль технічної експлуатації ?
4. У чому полягають функції технічної експлуатації ?
5. Назвіть основні принципи побудови систем технічної експлуатації.
6. Назвіть основні функції адміністративно-технічного персоналу ТЛК-систем.
7. Які основні обов"язки експлуатаційного персоналу ТЛК-систем ?
8. Які основні вимоги щодо кваліфікації персоналу ?
9. Яким чином здійснюється технічне забезпечення експлуатації обладнання транспортування інформації ?
10. Що таке метрологічне забезпечення експлуатації ТЛК-систем ?
11. У чому полягає зміст робіт із метрологічного забезпечення експлуатації ?
12. Які параметри ТЛК-систем підлягають обов'язковому державному метрологічному контролю та нагляду ?
13. Які параметри ТЛК-систем підлягають відомчому

метрологічному контролю та нагляду ?

Література до другої лекції

1) Рекомендація МСЕ-Т М.20. Концепція технічної експлуатації мереж електрозв'язку.

2) Рекомендація МСЕ-Т М.60. Терміни та визначення, що відносяться до технічної експлуатації.

ЛЕКЦІЯ №3 ОСНОВНІ ХАРАКТЕРИСТИКИ СИСТЕМ НАДАННЯ ПОСЛУГ

Розглядаються наступні питання:

3.1. Телекомунікаційна послуга як об'єкт споживчого попиту

3.2. Якість послуги, якість обслуговування, показники та рівні якості, їхній взаємо зв'язок

3.3. Класи послуги, класи обслуговування, їхній взаємозв'язок

3.4. Види систем надання ТЛК-послуг

3.1. Телекомунікаційна послуга як об'єкт споживчого попиту

У загальному випадку телекомунікаційна послуга (надалі, послуга) характеризується багатьма властивостями, але в системах надання послуг вона розглядається, в першу чергу, як об'єкт споживчого попиту. Під цим кутом зору інтерес викликає функціональність послуги, споживчі властивості послуги, якість надання та її ціна.

Функціональність послуги (інакше, - функціональний профіль послуги), тобто доступний та потенційно корисний для споживача набір взаємопов'язаних функцій, який здатний під час надання послуги задовольнити його потреби в телекомунікаційних застосуваннях, є однією із її основних характеристик.

Необхідна функціональність послуги безпосередньо визначається тонкою структурою потреб прикладних застосувань користувача. Тому оцінка функціональності здійснюється диференційовано, з урахуванням конкретних умов використання застосувань. Однак безумовно одне: чим більша повнота функціональності послуги (іншими словами, чим більше корисних функцій може виконуватися в процесі надання послуги), тим із більшою ймовірністю і в більшій мірі вона в змозі задовольнити споживчий попит користувачів.

Споживчі властивості послуги – це ті її властивості, котрі враховуються споживачами підчас прийняття ними рішень щодо ступеню корисності цієї послуги у їхніх застосуваннях та (або) доцільності користування цією послугою.

Щодо телекомунікаційних технологій існує рекомендація

Міжнародного Союзу Електрозв'язку МСЕ-Т Е.800, у якій визначено наступні чотири споживчі властивості послуги: забезпеченість (Service Support Performance), зручність використання (Service Operability Performance), дієвість (Serve Ability) та безпечність користування (Service Security Performance). У свою чергу, дієвість – найбільш важлива споживча властивість послуги характеризується такими ознаками як доступність (Service Accessibility Performance), безперервність (Service Retain Ability Performance) та цілісність (Service Integrity Performance). Визначення цих властивостей надано далі у цьому підручнику.

Реалізація перелічених властивостей напряму залежить від здатності мережі обробляти трафікове навантаження (Traffic Ability Performance), тобто від якості функціонування мережі (Network Performance, NP).

Примітка 1. Слово „Performance" означає у прямому перекладі „якість" або „досконалість". Тому у дослівному перекладі, наприклад, „Network Performance" означає „мережна досконалість", а „Service Accessibility Performance" – „якість доступності послуги".

Властивості мережної досконалості – це ті властивості мережі, які характеризують ступінь її досконалості. За звичайних умов вони не є об'єктом споживчого інтересу з боку кінцевих користувачів мережних послуг. Але саме ці властивості, в першу чергу, враховуються сервіс-провайдерами в процесі надання послуг. Властивості мережної досконалості визначені у Рекомендації МСЕ-Т Е.800, згідно якої слід розрізняти: ресурсні можливості мережі щодо її використання (Resources and Facilities), її надійність (Dependability) та якість передавання (Transmission Performance). Основна характеристика досконалості мережі - надійність, що визначається готовністю її ресурсів до використання (Availability Performance). У свою чергу, готовність характеризується такими трьома складовими: безвідмовність (Reliability Performance), ремонтопридатність (Maintainability Performance) та забезпеченість технічного обслуговування і ремонту (Maintenance Support Performance).

Для кількісного оцінювання кожної із властивостей уводяться відповідні показники. Наприклад, показниками доступності є ймовірність відмови у доступі, середня затримка доступу і т. ін.

Якість надання послуги (якість послуги, Quality of Service, QoS) – інтегральний корисний ефект від надання послуги, що визначається ступенем задоволення потреб користувача цієї послуги.

Оскільки користувач оцінює якість послуг у метриці їхніх властивостей, то і критерії якості надання послуг повинні мати вигляд певних функцій та (або) функціоналів від показників властивостей послуг. Однак на практиці найчастіше в цілях спрощення можливими функціональними взаємозв'язками між показниками властивостей нехтують, а в ролі критерію якості надання певної послуги використовують визначений набір (зокрема, упорядковану послідовність) показників властивостей такої послуги. В цьому випадку показники властивостей звичайно називають показниками або параметрами якості надання послуги, а критерій якості – узагальненим або інтегральним показником якості надання послуги.

Наприклад, інтегральний показник якості надання послуги із транспортування через мережу пакетів у форматі IP, що переносять голосовий трафік, на практиці у більшості випадків визначають наступним чином. Такі властивості послуги як її забезпеченість та безпечність користування (див. Рекомендацію МСЕ-Т Е.800) не враховують. Зручність використання враховують шляхом введення такого показника як інтервал звітування (тобто, періодичність представлення покупцю послуг звітів про поточний стан обслуговування). Щодо дієвості враховують усі три її ознаки, тобто уводять показники доступності, безперервності та цілісності. В результаті отримують наступні показники якості надання вищезазначеної послуги:

1) часовий інтервал забезпечення параметрів обслуговування $T_о$;

2) коефіцієнт доступності послуги $K_д$, тобто співвідношення між сумою проміжків часу, протягом котрих послуга є доступною для користування, і часовим інтервалом забезпечення параметрів обслуговування $T_о$;

3) максимальна величина затримки голосових пакетів τ;

4) максимальна величина варіації затримки голосових пакетів $\tau_в$;

5) ймовірність того, що на визначеному часовому інтервалі буде забезпечена передача пакетів із затримками, котрі не перевищують визначену максимальну величину затримки голосових пакетів $P_з$;

6) ймовірність того, що на визначеному часовому інтервалі буде забезпечено передавання пакетів із варіаціями затримок, котрі не перевищують визначену максимальну величину варіації затримки голосових пакетів $P_{вз}$.

У вищенаведеному прикладі ознака доступності (тобто, властивість послуги бути наданою саме тоді, коли у цьому існує потреба) врахована шляхом введення таких параметрів як *Кд* і *То* . Параметр *То* характеризує також і таку ознаку дієвості послуги як безперервність її надання, оскільки значення усіх інших вищенаведених показників якості повинні безперервно забезпечуватися протягом часу *То*. На кінець, останні чотири показника із вищевказаних (тобто, τ, $\tau_в$, $P_з$ та $P_{вз}$) характеризують цілісність послуги, оскільки саме вони визначають ту припустиму межу у погіршенні якості, що є прийнятною для користувача послуги.

Якість обслуговування (Quality of Services, QoS`) – інтегральний корисний ефект від обслуговування, що визначається ступенем задоволення користувача як від отриманої послуги, так і від самої системи обслуговування.

Примітка 2. Зверніть увагу на те, що англійська скорочена позначка якості обслуговування пишеться з апострофом після букви Q , тобто QoS`.

Згідно з Рекомендацією Міжнародної організації із стандартизації ISO 9004-3, п.02 під контролем необхідно тримати усі технічні, адміністративні і людські ресурси, що впливають на якість обслуговування. Стосовно до умов надання послуг на основі використання мережних ресурсів критерій якості обслуговування (котрий за звичайних умов називають коротко "якість обслуговування") доцільно представити у вигляді певного інтегрального показника досконалості обслуговування, що враховує не тільки якість надання послуги, але і здатність мережі обробляти навантаження. Тому критерій якості обслуговування у телекомунікаційному бізнесі за звичайних умов визначається набором (зокрема, упорядкованою послідовністю) показників

властивостей як телекомунікаційної послуги, що надається, так і мережних ресурсів, що використовуються. Показники якості надання послуги називають параметрами QoS послуги, а показники якості мережних ресурсів - параметрами NP мережі. Конкатенацію параметрів QoS та NP називають параметрами якості обслуговування, тобто QoS`. У вищенаведених визначеннях слово "параметр" є синонімом слова "показник".

Стосовно вищенаведеного прикладу щодо якості надання послуги із транспортування через мережу IP пакетів з голосовим трафіком: у разі необхідності визначення якості обслуговування QoS` слід показники якості надання цієї послуги QoS об'єднати із показниками NP, які характеризують властивості мережної досконалості, тобто об'єднати параметри QoS із такими параметрами NP як показники ресурсних можливостей IP-мережі щодо її використання, показники надійності та показники якості передавання (див. Рекомендацію МСЕ-Т Е.800).

На практиці під час визначення набору показників мережної досконалості NP також йдуть на певні спрощення, враховуючи тільки найбільш суттєві щодо даних конкретних умов показники. За умов, що відображені у вищенаведеному прикладі, доцільно враховувати лише такі показники безвідмовності:

1) відсоток втрачених пакетів по відношенню до загальної кількості транспортованих пакетів, визначених на проміжку часу, що дорівнює 1 с;

2) відсоток пакетів із помилковими даними по відношенню до загальної кількості транспортованих пакетів, визначених на проміжку часу, що дорівнює 1 с;

3) коефіцієнт навантаження обладнання, розташованого уздовж маршруту потоку пакетів;

4) період усереднення швидкостей потоків пакетів під час визначення коефіцієнта навантаження обладнання.

Усі чотири показника характеризують безвідмовність, що є згідно з Рекомендацією МСЕ-Т Е.800 складовою надійності, яка, в свою чергу, визначається готовністю ресурсів мережі до використання (Availability Performance). Інші властивості мережної досконалості у наведеному прикладі не враховані.

Ціна послуги має вирішальне значення для її покупця підчас

прийняття ним рішення щодо доцільності користування цією послугою. Визначення ціни на послугу залежить від багатьох різнорідних факторів і в цьому підручнику не розглядається. Не є предметом розгляду у рамках цього підручнику і безумовно важливі з точки зору організації надання послуг проблеми, що пов'язані із формуванням тарифної політики та організацією розрахунків з покупцями послуги.

3.2. Якість послуги, якість обслуговування, показники та рівні якості, їхній взаємозв'язок

Якість послуги. Будь-яка телекомунікаційна послуга характеризується тим набором властивостей, що є суттєвими для користувачів. У свою чергу, кожна із властивостей характеризується набором показників цієї властивості. Із всієї множини показників властивостей послуги у площині взаємовідносин між покупцем і продавцем послуги, тобто на інтерфейсі "покупець послуги – провайдер послуги" (Customer – SP Interface), доцільно розглядати підмножину показників властивостей, що дозволяє оцінити на кількісному рівні якість надання послуги. Елементи цієї підмножини називають показниками або визначальними параметрами якості послуги (а також параметрами QoS послуги). Таким чином, узагальнений (інтегральний) показник якості надання послуги (або, коротко, - якість послуги) – це набір функціонально пов'язаних між собою або незалежних один від одного параметрів якості послуги (набір визначальних параметрів якості послуги).

Якість більшості послуг, що можуть надаватися на основі використання ресурсів ТЛК-мереж, розуміється із статистичної точки зору. Зокрема щодо пакетних мереж: прикладні застосування користувачів здебільшого на практиці генерують в мережу пакети у випадкові моменти часу. Тому і черги у пристроях буферної пам'яті портів комунікаційних пристроїв (надалі, - буфери) являють собою випадкові процеси. Це призводить до того, що миттєва швидкість потоків пакетів та їхні затримки в елементах мережі також мають випадковий характер. Як наслідок, більшість визначальних параметрів, що використовуються для вимірювань якості послуг на мережах пакетної комутації, розглядаються як

статистичні.

Наприклад, у якості показника швидкості потоку пакетів за звичайних умов вибирають середнє значення (математичне чекання) цієї швидкості, у якості показника характеру пульсацій трафіка - варіації (дисперсії) швидкості потоку відносно середнього значення, у якості показника чутливості прикладних застосувань (задач) користувачів до затримок пакетів – варіації затримок відносно середньої затримки (котрі іноді ще називають джитером затримок пакетів) і т. ін. Немає сенсу вимірювати затримку будь-якого одного окремого пакету або швидкість потоку на дуже малих проміжках часу, близьких до часу передавання одного пакету. Більш доцільно вимірювати якість послуг шляхом усереднення відповідних параметрів протягом певним чином попередньо обумовлених проміжків часу.

Рівні якості послуги. Як правило, послуга може надаватися із різним рівнем якості. Рівень якості послуги узгоджується між сервіс-провайдером та його клієнтом і включається до тексту відповідної сервісної угоди (що називається також Service Level Agreement або SLA).

Рівень якості послуги визначається шляхом надання конкретних кількісних значень показникам якості, що входять до складу узагальненого показника якості надання послуги. Якщо ці показники розглядаються як незалежні один від одного, то рівень якості послуги задається упорядкованим набором (множиною) значень визначальних параметрів якості послуги. У геометричній інтерпретації рівень якості послуги – це вектор, що задається у n - мірному просторі визначальних параметрів, де n – кількість визначальних параметрів якості послуги. Згідно такої інтерпретації рівень якості послуги не може асоціюватися із суб'єктивними уявленнями типу "більш якісна або менш якісна послуга", а задається конкретним набором значень визначальних параметрів якості послуги.

Бажаний рівень послуги (бажаний рівень QoS) – це той рівень якості послуги, що найбільш точно задовольняє вимогам прикладних застосувань користувача цієї послуги.

Наприклад, якщо потенційний покупець ТЛК- послуги в процесі укладання сервісної угоди SLA прагне сформулювати бажаний для

нього рівень якості послуги, то він, після визначення набору визначальних параметрів, що впливають на якість функціонування його застосувань, має задатися конкретними значеннями (або діапазонами значень) щодо кожного із визначених параметрів. Тоді бажаний рівень якості послуги буде визначатися набором вибраних значень (або діапазонів значень) визначальних параметрів якості цієї послуги.

Скільки комбінацій із припустимих значень визначальних параметрів є можливим утворити, стільки рівнів якості послуги буде можливим задати. Так що, структуруючи вимоги до бажаної якості послуги у термінах та метриці "рівня якості послуги", будь-який потенційний покупець послуги має змогу формалізувати тонку структуру своїх потреб до якості надання цієї послуги з урахуванням конкретних умов функціонування його прикладних застосувань.

Гарантований рівень послуги (гарантована якість послуги, гарантована QoS) - розрахований та заявлений провайдером рівень якості послуги, який він в змозі і згодний гарантовано підтримувати на основі сервісної угоди щодо рівнів надаваних послуг, тобто на основі SLA. Гарантована QoS – це сукупність заявлених провайдером значень (або діапазонів значень) технічних параметрів, що характеризують відповідність засобів служби підтримки якості провайдера послуги очікуванням покупця цієї послуги щодо якості обробки його застосувань. Гарантована QoS – пороговий критерій якості, з яким порівнюються досягнуті в процесі надання послуги поточні значення параметрів QoS.

Виміряний рівень послуги (виміряний рівень QoS) – це значення оцінки рівня якості наданої послуги, що отримане на основі оцінок її визначальних параметрів шляхом усереднення виміряних в процесі контролю відповідності поточних значень цих параметрів. Якщо усереднення здійснюється на інтервалі поточного збору даних, то таким чином виміряний рівень послуги називають поточним рівнем послуги.

Трафарети сервісної угоди щодо рівня надаваних послуг, темплети SLA (Service Level Agreement Templates) – визначення стандартних ступенів якості послуги (тобто, стандартних рівнів послуги), які можуть бути запропоновані покупцям послуги у

рамках SLA. Наприклад, трафарети, що визначають характеристики так званої “золотої послуги” або “срібної послуги” і т. ін.

Якість обслуговування. Поняття “якість обслуговування” відрізняється від поняття “якість послуги” тим, що при визначенні якості обслуговування враховуються не тільки параметри QoS послуги, але і параметри NP мережі, на основі використання ресурсів котрої ця послуга надається.

В залежності від прийнятої системи надання послуг використовують різні підходи до визначення якості обслуговування.

В системах пріоритетного обслуговування, а також в системах диференційованого обслуговування з гарантованим сервісом використовується термін “якість обслуговування”, що позначається абревіатурою “QoS` ”. Під якістю обслуговування в цих системах розуміють здатність мережних ресурсів забезпечити потрібний сервіс для визначених класів потоків даних у визначеному мережному середовищі (мережне середовище - це середовище передавання даних, що побудовано на основі використання обладнання ATM, FR, IP, Optical Ethernet тощо). А під класом потоку даних (класом трафіку) розуміють тип даних, що транспортуються каналами мережі: голосові пакети, відео, HTTP, FTP, трафік баз даних і т. ін.

В системі диференційованого обслуговування з гарантованим сервісом, як правило, визначаються гарантовані рівні QoS`.

Рівні якості обслуговування. Обслуговування також може надаватися із різним рівнем якості. Рівень якості обслуговування може бути об’єктом узгодження між сервіс-провайдером та його клієнтом і вимоги до цього рівня можуть уводитись до тексту відповідної сервісної угоди SLA.

За аналогією із визначеннями основних різновидів “рівнів якості послуги” уводяться подібні різновиди поняття “рівень якості обслуговування”, а саме:

Бажаний рівень обслуговування (бажаний рівень QoS`) – це той рівень якості обслуговування, що найбільш точно задовольняє вимогам прикладних застосувань суб’єкта обслуговування.

Гарантований рівень обслуговування (гарантована якість

обслуговування, гарантована QoS`) - розрахований та заявлений провайдером рівень якості обслуговування, який він в змозі і згодний гарантовано підтримувати на основі сервісної угоди. Гарантована QoS` – це сукупність заявлених провайдером значень (або діапазонів значень) технічних параметрів, що характеризують відповідність засобів служби підтримки якості сервіс-провайдера та задіяних мережних ресурсів очікуванням суб'єкта обслуговування щодо якості обробки його застосувань. Гарантована QoS` – пороговий критерій якості, з яким порівнюються досягнуті в процесі надання послуги поточні значення характеристик QoS`.

Виміряний рівень обслуговування (виміряний рівень QoS`) – це значення оцінки рівня якості обслуговування, що отримане на основі оцінок її визначальних параметрів шляхом усереднення виміряних в процесі контролю відповідності поточних значень цих параметрів. Якщо усереднення здійснюється на інтервалі поточного збору даних, то таким чином виміряний рівень обслуговування називають поточним рівнем обслуговування.

Параметри якості обслуговування. Під час вирішення проблем забезпечення якісного надання ТЛК-послуг дотримуються наступної класифікації параметрів якості обслуговування.

По-перше, множину параметрів QoS`, що визначає рівень якості обслуговування, розбивають на три категорії параметрів:

1) сервіс-орієнтовані параметри, що безпосередньо пов'язані із визначенням якості послуги, тобто параметри QoS ;

2) мережно-орієнтовані параметри, що безпосередньо пов'язані із визначенням мережної досконалості, тобто параметри NP;

3) сервіс/мережно-незалежні параметри, тобто параметри, які не пов'язані із визначенням якості послуги QoS або мережної досконалості NP.

Примітка 3. Окрім параметрів якості обслуговування покупця послуги, зазвичай, цікавлять також параметри функціональності цієї послуги (наприклад, припустима середня швидкість потоку пакетів, що генерується прикладними застосуваннями, припустимі пульсації цього потоку і т. ін..) та, можливо, параметри функціональності мережного обладнання (наприклад, надана пропускна здатність, ширина смуги тощо).

По-друге, множину видів послуг розподіляють на наступні два види послуг:

1) диференційовані послуги, які орієнтовані на обслуговування користувачів із урахуванням конкретної структури їхніх вимог щодо якості обслуговування;

2) стандартні (інакше, - базові, агреговані, масові) послуги, що надаються шляхом використання уніфікованих механізмів і орієнтовані на потреби широкої групи користувачів з приблизно однаковими характеристиками вимог щодо обслуговування.

Як результат, отримують класифікатор параметрів QoS, типові приклади використання котрого наведено у вигляді таблиць 3.1 та 3.2. Прийняті позначення параметрів будуть розглядатися далі у наступних лекціях.

Таблиця 3.1

Приклад класифікації параметрів *QoS` при наданні послуги із транспортування пакетів IP через канал абонентського DSL-доступу*

Види послуг	Категорії параметрів обслуговування		
	мережно-орієнтовані	сервіс-орієнтовані	мережно/сервіс-незалежні
диференційовані	*IPER*, *IPLR*, коефіцієнт готовності обладнання	*IPTD*, *IPDV*, коефіцієнт доступності послуги	максимальний час відновлення, максимальний час ремонту
стандартні	середні значення *IPER*, *IPLR* та коефіцієнту готовності обладнання	розподіл затримок та девіацій затримок між потоками трафіка	*MTBF*, *MTTR*, *MTRS*

Таблиця 3.2

Приклад класифікації параметрів якості обслуговування при наданні послуги транспортування *ATM*-вічок

Види послуг	Категорії параметрів обслуговування		
	мережно-орієнтовані	сервіс-орієнтовані	мережно/сервіс-незалежні

диференційовані	максимальні значення параметрів *CER, CLR, CTD, CDV*	максимальний час відновлення, максимальний час ремонту
стандартні	усереднені значення параметрів *CER, CLR, CTD, CDV*	*MTTR, MTRS*

Як видно із вищенаведених таблиць, певні параметри деяких послуг вважаються одночасно сервіс- і мережно-орієнтованими. Так що вищенаведена класифікація є в деякій мірі умовною.

Примітка 4. Класифікатори параметрів якості обслуговування QoS` відрізняються від класифікаторів параметрів якості послуги QoS двома додатковими стовпцями: в один додатковий стовпець вносяться дані щодо параметрів мережної досконалості, а в інший – дані щодо сервіс/мережно-незалежних параметрів обслуговування .

Загальна структура взаємозв'язків між об'єктами системи управління якістю обслуговування надана на рис.3.1.

3.3. Класи послуги, класи обслуговування, їхній взаємозв'язок

Класи послуги. Досвід надання послуг, набутий провідними сервіс-провайдерами в Україні, свідчить, що внаслідок широкої

різноманітності прикладних застосувань кількість показників, які цікавлять покупців в різних реальних ситуаціях стосовно більшості мережних послуг, що надаються на основі використання сучасних ТЛК-технологій, перевищує п'ятдесят найменувань. При цьому, потрібні значення кожного із показників, як правило, вибираються із широких діапазонів припустимих значень. Тому і простори потенційно запитуваних покупцями рівнів будь-якої послуги є великорозмірними. Це, з одного боку, забезпечує широкий діапазон можливостей для покупця послуги в оптимізації заявленого ним рівня послуги відносно його реальних потреб з урахуванням тонкої структури вимог до якості послуги, що висувають його прикладні застосування. Але, з другого боку, надання персоніфікованих послуг із забезпеченням будь-якого бажаного для покупця рівня послуги суттєво підвищує вартість такого обслуговування, яка за існуючих умов у неприпустимій мірі звужує платоспроможний попит на нього. Тому на практиці щодо кожної послуги обмежуються лише кількома стандартизованими рівнями та (або) вузькими діапазонами рівнів її надання. Це спрощує обслуговування (зокрема, планування мережі та інженерію її ресурсів), дозволяє більш економно використовувати мережні ресурси і, як наслідок, знизити вартість послуги.

Раціональний вибір стандартизованих рівнів послуги є відповідальною задачею, оскільки намагання щодо зменшення кількості цих рівнів повинні при цьому не призводити до суттєвого зменшення потенційної клієнтської бази. Кожний запропонований рівень послуги повинен мати сталий попит з боку потенційних користувачів.

Множину ТЛК-послуг, що надаються із використанням ресурсів мереж передачі даних (МПД), доцільно розподілити (класифікувати) за видами телекомунікаційних технологій транспортування протокольних блоків даних (PDU) канального та (або) мережного рівнів (за моделлю OSI ISO). Це, зокрема, такі технології як ATM, FR, IP, xDSL, Optical Ethernet тощо. Вони утворюють мережне середовище надання послуг. З іншого боку, усі найбільш популярні види потоків, що транспортуються каналами МПД завдяки використанню транспортних технологій канального та мережного рівнів, групуються за загальними для них ознаками в

так звані класи трафіків. Розрізняють такі класи трафіків як голосові пакети, відео, HTTP, FTP, трафік баз даних і т. ін. І далі для кожної послуги в рамках кожної ТЛК-технології, що має застосування на МПД, визначається кілька стандартизованих рівнів (діапазонів рівнів) її надання з урахуванням характеристик класів трафіків, тобто характеристик найбільш популярних видів потоків PDU, що наразі генеруються основною масою прикладних застосувань реальних і потенційних користувачів. Визначені таким чином рівні (діапазони рівнів) послуги називаються класами послуги (або класами QoS).

Класи обслуговування. Будь-який клас будь-якої послуги характеризується лише сукупністю значень показників якості послуги QoS і не враховує показники мережної досконалості NP. Тому за аналогією із визначенням рівнів обслуговування доцільно увести поняття "класи обслуговування".

Класи обслуговування (класи QoS`) – це певним чином визначені рівні обслуговування щодо кожної послуги в рамках кожної телекомунікаційної технології з урахуванням характеристик найбільш популярних видів трафіку.

Кожному класу обслуговування відповідає певний клас послуги із доповненням - визначеної для цього класу обслуговування певної множини показників мережної досконалості NP та множини сервіс/мережно-незалежних параметрів обслуговування. Множина показників мережної досконалості характеризує рівні мережної досконалості тієї мережі, на основі використання ресурсів котрої надається послуга. Вищезазначені множини показників визначаються окремо в рамках кожної телекомунікаційної технології, що має застосування на МПД. Отже, клас обслуговування – це конкатенація певного класу послуги із певним рівнем мережної досконалості з урахуванням значень сервіс/мережно-незалежних параметрів обслуговування.

Кожний клас обслуговування характеризується певним набором стандартизованих значень (або діапазонів значень) визначених показників якості послуги (тобто, сервіс-орієнтованих параметрів), мережної досконалості (тобто, мережно-орієнтованих параметрів) та сервіс/мережно-незалежних параметрів обслуговування (див. таблицю 3.3).

Таблиця 3.3

Типовий приклад визначення класів обслуговування

Параметри обслугов.	Характеристика параметра	Клас 0	Клас 1	Клас 2	Клас 3	Клас 4	Клас 5
Сервіс/мережно-незал. параметри							
1. *MTBF*	Середній час між відмовами, годин	500	400	400	200	н/в	н/в
2. *MTTR*	Середній час ремонту	300 с	600 с	3600 с	н/в	н/в	н/в
3. *MTRS*	Середній час відновлення працездатності	600 с	1600 с	7200 с	н/в	н/в	н/в
Сервіс-орієнтовані параметри							
1. *mean IPDV*	Гарантоване на проміжку 1с середнє значення варіації затримок	100 мс	100 мс	н/в	н/в	н/в	н/в
2. *mean IPTD*	Гарантоване на проміжку 1с середнє значення величини затримки при передачі пакетів	200 мс	800 мс	200 мс	800 мс	2 с	н/в
3. *mean*	Гарантоване	$5x10^{-4}$	$5x10^{-}$	$5x10^{-}$	$5x10^{-}$	$5x10^{-}$	н/в

IPLR	на проміжку 1с середнє значення кількості втрачених пакетів		^{4}	^{4}	^{4}	^{4}	
4. *mean IPER*	Гарантоване на проміжку 1с середнє значення кількості пакетів із помилками	$3x10^{-6}$	$3x10^{-6}$	$3x10^{-6}$	$3x10^{-6}$	$3x10^{-6}$	н/в
Мережно-орієнтовані параметри							
1. *max IPDV*	Межа щодо варіації затримок	50 мс	50 мс	н/в	н/в	н/в	н/в
2. *max IPTD*	Межа щодо величини затримки при передачі пакетів	100 мс	400 мс	100 мс	400 мс	1 с	н/в
3. *max IPLR*	Верхня межа ймовірності втрат пакетів	$1x10^{-4}$	$1x10^{-4}$	$1x10^{-4}$	$1x10^{-4}$	$1x10^{-4}$	н/в
4. *max IPER*	Верхня межа щодо кількості пакетів із помилками	$1x10^{-6}$	$1x10^{-6}$	$1x10^{-6}$	$1x10^{-6}$	$1x10^{-6}$	н/в

Примітка: позначка “н/в” означає “не визначений”.

Визначення класів транспортних послуг і відповідних ним показників у рамках найбільш поширених телекомунікаційних

технологій, що мають застосування на МПД в Україні, буде наведено у подальших лекціях за цією навчальною дисципліною.

3.4. Види систем надання ТЛК-послуг

Системи надання телекомунікаційних послуг в залежності від можливостей сервіс-провайдера, попиту покупців та умов конкуренції можуть враховувати або не враховувати тонку структуру потреб застосувань споживачів щодо параметрів якості послуг. З цієї точки зору доцільно розрізняти наступні три типи систем:

1) система обслуговування з максимальними зусиллями (сервіс типу "максимум можливого" або "best effort");

2) система обслуговування з наданням переваги (пріоритетне обслуговування, "м'який" сервіс QoS);

3) система диференційованого обслуговування з гарантованим сервісом ("жорсткий" або "істинний" сервіс QoS).

Система обслуговування з максимальними зусиллями не передбачає будь-яку оцінку (а, тим більш, використання) механізмів регулювання якості обслуговування в процесі надання послуг. Зокрема, за цією системою обробка та просування протокольних блоків даних (PDU) каналами пакетної мережі здійснюється без надання будь-яких гарантій щодо часових, швидкісних або інших характеристик оброблюваного трафіку. Термін "з максимальними зусиллями" означає лише тільки те, що сервіс-провайдер зобов'язується задіяти для надання послуг усі наявні ресурси, не надавати переваг в обслуговуванні будь-якому покупцю послуг, що обслуговується за цією системою, та намагатися обслуговувати потоки пакетів за принципом FIFO („First in – First out", тобто „перший прийшов – перший отримав обслуговування").

Система обслуговування з наданням переваги (інші назви, - система пріоритетного обслуговування, система диференційованого обслуговування) надає переваги щодо якості обслуговування певним типам потоків даних. Під перевагами розуміється, наприклад, забезпечення більш швидкісної обробки

пакетів або менших втрат даних, надання більшої частки пропускної спроможності каналу транспортування даних тощо. Проте за цією системою будь-які кількісні значення показників якості обслуговування не гарантуються. Більш того, ці показники в процесі надання послуг навіть не контролюються, а надання переваг фактично забезпечується шляхом пріоритезації одних типів потоків над іншими. Зокрема, якщо більш пріоритетний потік пакетів в певний проміжок часу генерується з низькою інтенсивністю, то в цей час менш пріоритетному потоку може бути надана більша частка ресурсів ТЛК-мережі. Як наслідок, менш пріоритетний потік отримає високоякісне обслуговування – з малими затримками і втратами пакетів. Але якщо ситуація зміниться так, що більш пріоритетний потік почне нарощувати свою інтенсивність, то через це менш пріоритетний потік може взагалі деякий час не обслуговуватися.

Система диференційованого обслуговування з гарантованим сервісом (система ДОГС) забезпечує надання гарантій якості обслуговування на кількісному рівні з урахуванням тонкої структури вимог окремо кожного із покупців послуг до параметрів якості обслуговування. За цією системою кожний потік пакетів, що обслуговується на умовах "істинного" сервісу QoS, гарантовано отримує саме ті параметри якості послуг, які визначені для нього у числовому вигляді (за умов, зрозуміло, якщо покупці послуг не порушують узгоджені із сервіс-провайдером умови щодо характеристик цих потоків пакетів і не генерують їх більше, ніж те, що передбачено в сервісних угодах). Гарантується, наприклад, що певне застосування буде користуватися обумовленою часткою пропускної здатності наскрізного з'єднання за будь-яких обставин, навіть за умов, коли всі інші застосування миттєво почнуть генерувати потоки пакетів з максимальною інтенсивністю.

Комбіноване застосування систем обслуговування. На практиці, зазвичай, здійснюється комбіноване застосування усіх трьох вищенаведених систем обслуговування. Це дозволяє враховувати широкий спектр умов функціонування телекомунікаційних мереж та різноманітні вимоги прикладних застосувань користувачів.

Зокрема, певні застосування, такі, наприклад, як електронна пошта, достатньо обслуговувати з максимальними зусиллями. Для

деяких інших застосувань, таких як інтернет-служби FTP або HTTP, параметри якості обслуговування не є абсолютно важливими, тобто користувачі цих застосувань можуть миритися з певними нетривалими погіршеннями реактивності мережі. В цих випадках може бути доцільним використати систему обслуговування з наданням переваги. На кінець, існують застосування, такі як відеоконференцзв'язок або передача сигналів широкосмугової вимірювальної системи реального часу, котрі можуть бути втілені на пакетних мережах тільки за умов використання системи диференційованого обслуговування з гарантованим сервісом.

Як приклад, схема комбінованого застосування систем обслуговування за умов одночасного функціонування наведених вище типів потоків може бути запропонована така. Для трафіка відеоконференцзв'язку попередньо резервується певна частка пропускної спроможності мережі, щоб мати можливість гарантовано обслужити цей трафік з визначеними на кількісному рівні параметрами якості послуг. Ресурси мережі, що залишилися після резервування, диференційовано розподіляються між такими пріоритетними класами трафіка як служби FTP (з нижчим пріоритетом в обслуговуванні) та HTTP (з вищим пріоритетом). Тоді, якщо службі HTTP на певний проміжок часу знадобиться висока пропускна спроможність, то ця потреба задовольняється за рахунок служби електронної пошти, що обслуговується за системою "best effort" . Якщо цього виявиться недостатньо, то збільшення пропускної спроможності для служби HTTP буде здійснюватися за рахунок служби FTP, що має менший пріоритет. Зрозуміло, що за цією схемою комбінованого обслуговування трафік електронної пошти буде обслуговуватися за залишковим принципом, тобто на рівні "максимум можливого".

Контрольні питання до третьої лекції

1. Що таке функціональність послуги?
2. Що таке споживчі властивості послуги?
3. Які чотири споживчі властивості послуги, що визначені

рекомендацією Е.800 МСЕ-Т, Ви знаєте?

4. Які властивості мережної досконалості розглянуто у рекомендації Е.800?

5. Що таке якість послуги? Чим це поняття відрізняється від поняття ”якість обслуговування”?

6. Надайте визначення понять „рівень послуги”, „гарантований рівень послуги” та „виміряний рівень послуги”.

7. Що таке темплета *SLA*?

8. Які три категорії параметрів якості обслуговування Ви знаєте?

9. Що таке диференційована послуга?

10. Що таке клас послуги? Чим це поняття відрізняється від поняття „клас обслуговування?

11. Які види систем надання послуг Ви знаєте?

12. Чим пріоритетне обслуговування відрізняється від обслуговування типу “*best effort*” ?

13. Які основні переваги системи диференційованого обслуговування з гарантованим сервісом?

14. Надайте приклад комбінованого застосування систем обслуговування.

Література до третьої лекції

1)Г.Ф.Конахович, В.М.Чуприн. Мережі передавання пакетних даних. -К.: «МК-Прес», 2006. Розділи 2 та 3

ЛЕКЦІЯ №4. ОСНОВНІ ХАРАКТЕРИСТИКИ СИСТЕМ КЕРУВАННЯ ТЕЛЕКОМУНІКАЦІЙНИМ ОБЛАДНАННЯМ

Розглядаються наступні питання:

4.1. Загальна характеристика систем керування
4.2. Багаторівневе представлення задач керування
4.3. Архітектура систем керування
4.4. Стандарти протоколу *SNMP*
4.5. Недоліки протоколу *SNMP*

4.1. Загальна характеристика систем керування

Будь-яка ТЛК-система, а тим більш складна та територіально розгалужена програмно-апаратна система, що функціонує у режимі реального часу, потребує керування. Тобто, має існувати система керування ТЛК-системою, яка була б здатна забезпечити її нормальне функціонування. Якщо така система керування реалізована штатними засобами керованої ТЛК-системи, то її логічно назвати підсистемою керування, що функціонує у складі ТЛК-системи. Проте на практиці функціонують також системи керування, що є фізично відокремленими від штатних засобів керованої ТЛК-системи. У цьому випадку основну частину спеціалізованого обладнання, що здійснює функції керування, розміщають на спеціально виділеному вузлі керування, а інші частини цього обладнання інсталюють безпосередньо на вузлах керованої ТЛК-системи. Такі системи керування називають централізованими. Розосереджений характер будь-якої великої глобальної мережі робить неможливою її підтримку без централізованої системи керування (яка має англомовну назву *NMS – Network Management System*). Використовуються також і комбіновані системи керування, коли частина управлінських функцій виконуються штатними (як, іноді, кажуть – локальними) засобами керування, а інша частина управлінських функцій реалізуються централізованою системою керування.

Локальні механізми керування (тобто, ті механізми, що функціонують у складі штатного обладнання окремих активних елементів ТЛК-системи - комутаторів, маршрутизаторів, шлюзів тощо), як правило, реалізуються засобами операційних систем

(ОС), що інстальовані локально на цих складових елементах обладнання ТЛК-системи.

Примітка 1. Наразі практично будь-який окремий активний елемент, що входить до складу сучасних ТЛК-мереж, являє собою комп'ютеризовану систему із власним програмним забезпеченням (ПЗ), що знаходиться під керуванням спеціалізованої або широкорозповсюдженої ОС (типу Unix, Windows і т. ін.).

Використовуються також окремі локально інстальовані програми керування. Цим програмам притаманний більш високий рівень функціональності щодо вирішення задач керування у порівнянні із функціональністю штатних засобів ОС, проте і він (тобто, рівень) у багатьох випадках не є достатнім, щоб здійснювати ефективне керування глобальною багатовузловою ТЛК-системою.

Зазвичай кожний активний елемент ТЛК-системи має власну штатну підсистему керування. Наприклад, якщо розглядати структуру типової мережі стільникового зв'язку, то неважко упевнитись, що, зокрема, кожна із базових станцій має власну підсистему керування, контролери базових станцій також мають власні підсистеми керування, вузли комутації каналів мають свої штатні підсистеми керування і т.д. щодо кожного активного елементу цієї мережі. І якщо ТЛК-система складається із невеликої кількості вузлів, то на практиці зазвичай обмежуються застосуванням лише локальних засобів керування, а узгодження сумісної роботи цих вузлів здійснюється адміністраторами за допомогою звичайного телефонного зв'язку. Однак щоб керувати ТЛК-системою більш-менш значних розмірів як єдиним діючим цілим, необхідно використовувати централізоване керування.

Обладнання ядра централізованої системи керування однорідною мережею (що, як вже вказувалось, зазвичай розташоване на окремо виділеному вузлі керування) являє собою більш-менш просту програмно-апаратну систему. Однак для керування великими неоднорідними ТЛК-мережами, на вузлах котрих інстальовані неоднотипні локальні засоби керування (такі мережі іноді називають гетерогенними), доводиться застосовувати складні програмно-апаратні комплекси засобів, що у сукупності утворюють так звані інтегровані системи керування.

Система керування має бути здатною одночасно вирішувати

багато різнорідних задач та підкоряться певній загальній для усіх вузлів меті керування, наприклад досягненню відповідності між показниками якості функціонування прикладних систем, що запускаються у роботу користувачами ресурсів ТЛК-системи, та параметрами ТЛК-обладнання, що надає ТЛК-послуги цим прикладним системам.

Зазвичай NMS функціонує в автоматизованому режимі, виконуючи типові однозначно визначені управлінські дії автоматично, у той час як логічно більш складні завдання, що потребують застосування інтелекту людини, мають вирішувати адміністратори ТЛК-системи. Адміністратори усієї ТЛК-системи здійснюють керування системою за допомогою системних терміналів вузлу керування. На цьому вузлі в автоматичному режимі у реальному часі збираються різнорідні дані про стан обладнання у кожному вузлі ТЛК-системи та стан трафіку у кожному каналі. Усі ці дані проходять обробку на вузлі керування (і не тільки на ньому) та в узагальненому вигляді надаються адміністраторам мережі. (Зрозуміло, що адміністратори при потребі можуть отримувати і детальну інформацію щодо кожного параметру системи, що їх цікавить).

4.2. Багаторівневе представлення задач керування

Керування сучасними ТЛК-системами – одна з основних груп технологічних процесів, що впроваджені в експлуатаційну практику завдяки зусиллям як багатьох провідних ТЛК-корпорацій, так і міжнародних організацій, що регламентують діяльність у сфері телекомунікацій. Запропоновано кілька моделей систем керування ТЛК-системами, щодо котрих інтерес викликають, перш за все, такі категорії як архітектура та протоколи системи керування.

Одна з основних моделей керування складними ТЛК-системами є модель TMN (Telecommunication Management Network), що розроблена спільними зусиллями ITU-T (телекомунікаційне відділення Міжнародного союзу електрозв'язку, MCE-T), ISO (міжнародна організація із стандартизації), ANSI (американський інститут із стандартизації) та ETSI (європейський інститут із стандартизації) і прийнята в якості міжнародного стандарту у сфері

управління телекомунікаційним обладнанням. Модель керування TMN створена у рамках концепції інформаційної взаємодії відкритих систем (OSI), що підтримується ISO. Модель TMN відображає складну інтегровану багаторівневу ієрархічну систему керування, що має мережну структуру. Проте її не завжди доцільно використовувати на практиці (вона є дуже складною та громіздкою, оскільки охоплює усю можливу множину архітектур ТЛК-систем). Тим не менш, концепція цієї моделі знайшла використання в задачах аналізу функціонування тих чи інших засобів та механізмів керування в телекомунікаціях. Тому вона має бути розглянута у рамках цієї навчальної дисципліни.

У рамках моделі TMN розроблено Рекомендацію ITU-T X.700 та міжнародний стандарт ISO 7498-4, згідно з якими уся сукупність задач керування поділена, перш за все, на п’ять функціональних груп. Декомпозиція функціональності керування виконана таким чином, що в кожну із цих груп увійшли задачі керування приблизно однакового функціонального призначення, а саме:

1) Керування конфігурацією параметрів ТЛК-обладнання та найменуванням (Configuration Management).

Конфігуруються параметри як окремих компонентів, так і ТЛК-системи у цілому. Визначаються мережні адреси, ідентифікатори (імена) об’єктів керування, їх географічне розташування тощо. Якщо ТЛК-система має мережну структуру, то вирішується задача побудови так званої мапи (карти) мережі, тобто відображення реальних зв’язків між елементами мережі, відображення на карті фізичних та логічних каналів, побудова таблиць комутації та маршрутизації. Побудова та підтримка у реальному часі мапи мережі вважається складною та відповідальною задачею. Її вирішення може здійснюватися у ручному, автоматичному (шляхом зондажу) та напівавтоматичному режимах. Методи побудови мапи зв’язків мережі – це фірмові розробки, які не знайшли широкого висвітлення у спеціалізованій літературі. Налаштування (настройка) комутаторів та маршрутизаторів на підтримку маршрутів та логічних віртуальних каналів – це те ж задача, що відноситься до функціональної групи Configuration Management.

2) Вияв та знешкодження збоїв та помилок у роботі ТЛК-

обладнання (Fault Management).

У рамках цієї функціональної групи задач виконується реєстрація помилок, повідомлення про помилки, фільтрація повідомлень (наприклад, надсилаються на адресу адміністратора тільки найбільш важливі повідомлення), маршрутизація повідомлень до необхідних підсистем системи керування, кореляційний аналіз виявлених помилок на основі певним чином вибраної кореляційної моделі з метою виявлення причин помилок. Вирішуються також проблеми невідповідності параметрів нормам, аналіз телекомунікаційних протоколів, діагностика та ремонт ТЛК-обладнання і т. ін..

3) Забезпечення продуктивності та надійності роботи ТЛК-обладнання (Performance Management).

Вирішуються задачі інженерії трафіка з метою підтримки заданих значень параметрів якості надання послуг (параметри QoS) та параметрів мережної досконалості (параметри NP), зокрема коефіцієнту готовності обладнання (інтегральний показник надійності обладнання) та коефіцієнту використання обладнання (інтегральний показник ефективності використання обладнання). До групи Performance Management відносяться також задачі побудови процедур резервування обладнання та задачі поточного контролю виконання положень укладених сервісних угод (SLA) і оперативного усунення виявлених порушень цих угод.

У процесі експлуатації ТЛК-системи накоплюється статистика щодо таких параметрів як час реакції системи, затримки у передаванні інформації, інтенсивність трафіку, коефіцієнт готовності обладнання тощо. Ці статистичні дані потрібні для прогнозування роботи системи та підготовки необхідних управлінських рішень щодо оптимізації її параметрів. Збір статистичних даних та їхня обробка також здійснюються у рамках вирішення задач Performance Management.

4) Підтримка прийнятої політики забезпечення захисту інформаційних ресурсів ТЛК-системи (Security Management).

До цієї функціональної групи відносяться, перш за все, задачі розмежування доступу до ресурсів ТЛК-системи, забезпечення цілісності даних, ідентифікації, автентифікації та авторизації суб’єктів та об’єктів доступу, фільтрації, тунелювання та

шифрування інформації, розподілу ключів шифрів.

Примітка 2. Для конкретних умов використання ТЛК-системи зазвичай розроблюється стратегія (політика) забезпечення захисту її інформаційних ресурсів. Однак на практиці трапляється, що штатні функції захисту інформації, котрі реалізовані у складі підсистеми керування не дозволяють забезпечити у повній мірі прийняту політику інформаційної безпеки. У цьому випадку ТЛК-обладнання дооснащується закупними спеціалізованими продуктами захисту інформації.

5) Облік використаних ресурсів ТЛК-системи на визначених інтервалах часу *(Accounting Management).*

Реєстрація часу використання ресурсів мережі: каналів, маршрутизаторів, комутаторів тощо. Визначення плати за використані ресурси - **Білінг.**

Примітка 3. Якщо порівняти вищенаведений класифікатор функціональності керування (в котрому маємо п'ять функціональних груп) із класифікатором функціональності експлуатації, що був наданий у лекції №1 (де маємо 16 функціональних груп), то слід зробити висновок: задачі керування з точки зору їхньої функціональності є підмножиною задач експлуатації.

По-друге, у склад моделі TMN входить ще один класифікатор задач керування, однак вже не за ознакою функціональності, а за ступенем агрегованості (деталізації) елементів об'єкту керування. Зокрема, за цією ознакою прийнято наступне ієрархічне п'ятирівневе представлення задач керування: рівень елементів мережі, рівень управління елементами мережі, рівень керування всією мережею, рівень керування мережними послугами та рівень бізнес-керування. Як бачимо, в якості самого дрібного рівня агрегованості ТЛК-системи узято рівень її складових елементів (це можуть бути задачі підтримки найбільш дрібних елементів обладнання ТЛК-системи - наприклад індикаторних та (або) виконавчих механізмів, що інстальовані у складі комутатора, маршрутизатора, шлюзу тощо або задачі підтримки більш агрегованих елементів обладнання – комутаторів, маршрутизаторів, шлюзів тощо або, навіть, усього обладнання окремого вузлу ТЛК-мережі), а в якості найбільш агрегованого об'єкту керування пропонується розглядати бізнес-керування ТЛК-системою. Проміжні рівні агрегованості згідно цієї моделі керування – рівень управління елементом системи (це – задачі

управління механізмами комутатора або маршрутизатора або шлюзу або вузлового обладнання і т.ін.), рівень керування всією ТЛК-системою (це, як правило, задачі централізованого керування) та рівень керування наданням послуг (це – задачі служби QoS). Тобто, маємо розбивку (декомпозицію) усіх задач керування на п’ять функціональних груп, а для кожної групи - на п’ять рівнів агрегованості представлення елементів об’єкту керування. Візуально взаємозв’язок задач керування згідно з моделлю TMN нагадує піраміду, що представлена на рис. 4.1.

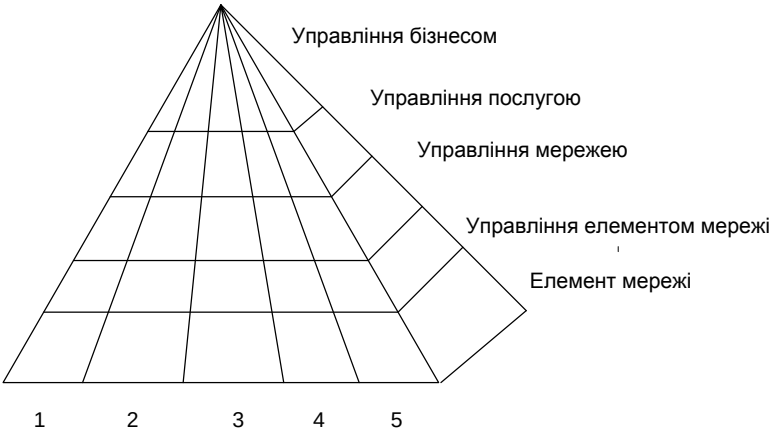


Рис. 4.1. Взаємозв’язок задач керування згідно з моделлю *TMN*

На рис.4.1 прийняті наступні позначки: 1 – управління конфігурацією; 2 – управління усуненням недоліків; 3 – управління якістю передавання; 4 – управління розрахунками; 5 – управління захистом інформації.

4.3. Архітектура систем керування

В основі архітектури систем керування сучасними ТЛК-системами, як правило, лежить так звана схема «менеджер - агент». Використання цієї схеми, а також відповідним чином побудованої моделі керованого об’єкту (МКО) дозволяє автоматизувати процес

керування.

Схема керування виду «менеджер - агент». Найбільш простий варіант архітектури автоматизованої системи керування представляється у вигляді сукупності двох підсистем – керуючої та керованої, що знаходяться між собою у стані постійної інформаційної взаємодії. Об'єкт, що підлягає керуванню, знаходиться у складі керованої підсистеми, а менеджер, тобто суб'єкт (людина) або об'єкт (автомат), що повинен приймати управлінські рішення та ініціювати команди відповідно до цілей керування, знаходиться у складі керуючої підсистеми. В якості керованого об'єкту може розглядатися будь-який елемент ТЛК-системи будь-якого рівня агрегованості. Цілеспрямоване керування може здійснюватися лише на основі певних знань про стан керованого об'єкту. Ці знання черпаються менеджером із моделі керованого об'єкту (МКО). МКО є спрощеним (точніше, - утисненим) відображенням реального об'єкту, що підлягає керуванню, оскільки у цій моделі відображаються лише ті і саме ті характеристики (параметри) реального об'єкту, що мають безпосереднє відношення до ефективності процесу керування. Характеристики керованого об'єкту у реальному масштабі часу, як правило, змінюються. Для того, щоб ці зміни адекватно відображалися у МКО, необхідно вимірювати показники характеристик керованого об'єкту і на основі отриманих результатів змінювати МКО синхронно із змінами його стану. В якості організатора вищеназваних процесів у реальному часі виступає представник менеджера, тобто його агент, котрий безпосередньо знаходиться у місці розташування керованого об'єкту і має змогу, з одного боку, підтримувати актуальність МКО, а з другого боку, виконувати команди, що надходять від менеджера. Таким чином, у складі керуючої підсистеми знаходиться менеджер, що у реальному часі отримує інформацію із МКО про стан керованого об'єкту і на основі цієї інформації приймає управлінські рішення. А інформацію для менеджера на стороні керованої підсистеми добуває (також у реальному часі) агент. Агент безпосередньо взаємодіє із всілякими фізичними давальниками та лічильниками, обчислювачами визначальних параметрів якості функціонування ТЛК-обладнання та якості

надання послуг, вимірювачами трафікових навантажень, виявлячами та фільтрувальниками системних подій, пороговими схемами та виконавчими механізмами, будь-якими іншими контролюючими та виконавчими механізмами, що здатні напряму контролювати роботу керованого об'єкту та змінювати його стан у бажаному напрямі згідно із цілями керування.

Більш конкретно принцип взаємодії менеджера з агентом під час керування будь-яким елементом ТЛК-системи будь-якого рівня агрегованості (іншими словами, під час керування будь-яким ресурсом ТЛК-системи) пояснюється за допомогою схеми, що відображена рис.4.2.

Як бачимо, поряд з агентом та менеджером у схему взаємодії включена також модель керованого об'єкту (МКО). МКО присутня на схемі як на стороні керованої підсистеми, так і на стороні керуючої підсистеми. Тобто, і менеджер і агент працюють із відображеннями однієї і тієї ж моделі керованого об'єкту. Проте у відображенні цієї моделі на різних сторонах схеми „менеджер – агент ", а також у використанні цієї моделі менеджером і агентом існують суттєві відмінності.

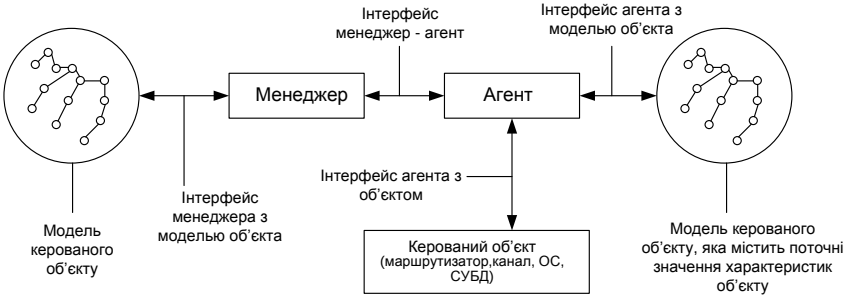


Рис.4.2. Схема взаємодії менеджера, агента та керованого об'єкту

Перш за все, важливо підкреслити, що у рамках архітектури керування за схемою „менеджер – агент " відображенням моделі керованого об'єкту є так звана база даних керуючої інформації (Management Information Base, MIB).

Відображення МКО на стороні керованої підсистеми назвемо базою MIB агента, а відображення МКО на стороні керуючої

підсистеми назвемо базою MIB менеджера. База MIB агента являє собою сукупності поточних значень показників характеристик керованого об'єкту, що були виміряні та, можливо, пройшли попередню обробку у реальному часі за допомогою спеціалізованих інструментальних засобів на стороні керованої підсистеми. Іншими словами, поточний стан керованого об'єкту відображається у базі MIB агента у вигляді сукупностей поточних значень показників характеристик цього об'єкту. Саме тих показників, що використовуються у якості вихідних даних у задачах керування. Якщо керований об'єкт внаслідок будь-яких причин у реальному часі постійно змінює свій стан, то і база MIB агента має знаходитись у стані постійного оновлення. Інформація щодо змін у стані керованого об'єкту заноситься у базу MIB агента під безпосереднім керуванням цього агента з тим чи іншим інтервалом оновлення даних. Менеджеру же для ефективного керування у реальному масштабі часу (у відповідності із прийнятою стратегією або метою керування) необхідно володіти не усією поточною інформацією, що накопичується у базі MIB агента, а тільки тою її частиною, що відображає реальний стан керованого об'єкту у моменти прийняття управлінських рішень. Тому база MIB менеджера не є точною копією бази MIB агента. Як правило, база MIB менеджера – більш компактна, у ній зосереджується лише та інформація, що безпосередньо використовується для формування управлінських рішень. Зрозуміло, що ця інформація має бути якомога достовірнішою і не запізнілою з урахуванням швидкості змін характеристик керованого об'єкту. Нюанс полягає у тому, що дані у MIB оновлюються агентом на стороні керованої підсистеми, в той час як менеджер користується даними MIB на стороні керуючої підсистеми. Тому одне із завдань, що вирішується системою керування, - це синхронізація стану баз MIB на обох сторонах схеми „менеджер – агент". Вкрай бажано, щоб дані бази MIB, якою користується менеджер, були у моменти прийняття управлінських рішень ідентичними даним бази MIB, яка оновлюється на стороні агента. Проте зрозуміло, що досягнення ідеальної синхронізації стану вищеназваних баз даних не є можливим хоча б тому, що потрібен деякий час на їхню синхронізацію.

Таким чином, керування за схемою „менеджер – агент” полягає у наступному (див. рис. 4.2). Агент наповнює MIB керованого об’єкту поточними значеннями його характеристик, а менеджер витягує із MIB, що розташована на керуючій стороні, дані, що дозволяють йому приймати обгрунтовані управлінські рішення. Окрім того, менеджер може запитувати через агента значення параметрів, що знаходяться у MIB агента, і передавати агенту інформацію, на основі котрої цей агент повинен безпосередньо керувати об’єктом. Отже, агент може розглядатися як посередник між керованим об’єктом та менеджером. Зрозуміло, що агент може поставляти менеджеру лише ті дані, що зберігаються у MIB.

Менеджер та агент взаємодіють відповідно до стандартних протоколів, що називаються протоколами керування. Менеджер розміщується, зазвичай, на окремому комп’ютері (консолі адміністратора). Цей комп’ютер приєднується до обладнання, що потребує керування. Менеджер (зокрема, той, що функціонує у складі вузлу централізованого керування) може взаємодіяти одночасно з декількома агентами. Проте у загальному випадку у складі однієї системи керування може існувати кілька керуючих підсистем та декілька керованих підсистем. Малоймовірний, але можливий випадок, коли кілька керуючих підсистем взаємодіють з однією керованою підсистемою. Більш реалістичною виглядає ситуація, коли одна керуюча підсистема одночасно взаємодіє з декількома керованими підсистемами. У будь-якому разі взаємодія здійснюється відповідно до схеми „менеджер – агент”.

Наразі в експлуатації знаходиться широкий спектр різноманітного ТЛК-обладнання, що використовується у різноманітних умовах застосування. Тому і функціональні та інтелектуальні можливості агентів, що функціонують у рамках створених систем керування, можуть бути самими різними. Наприклад, примітивний агент здатний лише підраховувати кількість інформаційних блоків, що перетинають визначену точку контролю. У той час як інтелектуально розвинений агент здатний виконувати складні логічні дії, що пов’язані із автоматизацією побудови мапи мережі, оптимізацією маршрутів просування протокольних блоків даних, прогнозуванням поведінки трафікового навантаження, фільтрацією системних подій,

класифікацією виниклих помилок під час роботи обладнання і т.ін. Інтерфейси між агентами та керованим обладнанням – не стандартизовані (через велику кількість та різноманітність типів об'єктів, що потребують керування). Це суттєво утруднює створення універсальних засобів керування.

У більшості випадків на практиці агенти вбудовують напряму в апаратні та (або) програмні елементи керованого обладнання. Зрозуміло, що у цьому разі агентам необхідно присвоїти окремі мережні адреси та (або) забезпечити їх фізично або логічно виділеними портами, через котрі має здійснюватися їхня інформаційна взаємодія із менеджерами. Щодо менеджерів то вони реалізуються як програмними, так і спеціалізованими апаратними засобами. У разі централізованого керування вони входять до складу окремо виділених вузлів керування. Менеджери також можуть входити до складу засобів локального керування яким-небуть елементом ТЛК-мережі.

У випадках, коли безперервна робота системи керування не передбачається, агенти разом із управляючою програмою (тобто, менеджером) можуть інсталюватися локально на окремому переносному комп'ютері. У разі потреби цей комп'ютер приєднується до обладнання, що потребує керування.

Мережі внутрішньосмугового та позасмугового керування. Інформаційна взаємодія менеджерів з агентами може здійснюватися як через окремо виділені канали зв'язку, так і в загальному потоці інформаційних сигналів, спільних для користувацьких даних та сигналів керування. У цьому контексті розрізняють внутрішньосмугове керування (або керування типу In-band) та позасмугове керування (або керування типу Out-of-band). Якщо керуючі сигнали проходять через той же канал, що і користувацькі дані (наприклад, повідомлення протоколу керування, згідно з котрим взаємодіють агенти з менеджером, транспортуються тими ж каналами IP-мережі, що і пакети користувачів цієї мережі), то маємо справу із внутрішньосмуговим керуванням. Якщо ж менеджер вузлу керування контролює IP-маршрутизатор і взаємодіє із своїми агентами, що в нього вбудовані, через канали окремої спеціально виділеної мережі керування, то маємо справу із позасмуговим керуванням.

Зрозуміло, що на створення окремої мережі керування потрібні значні фінансові ресурси. Проте позасмугове керування є набагато більш надійнішим і захищеним від несанкціонованого доступу.

Схема „менеджер – агент” має застосування також і у тих випадках, коли необхідно побудувати розподілені системи керування. Наприклад такі, що відображені на рис.4.3 – 4.5.

Кожний агент, що відображений на цих рисунках, керує певним мережним елементом (NE, Network Element).

Виміряні поточні значення параметрів контрольованого NE агент поміщає у свою базу MIB (на рисунках ці бази не відображені). Менеджери вилучають дані із баз MIB своїх агентів, відповідним чином оброблюють їх і оброблені дані поміщають у свої бази даних, тобто у бази MIB менеджерів. На основі цих даних менеджери у відповідності із своїми управляючими програмами, що закладені у їхню пам’ять, здійснюють процес автоматичного керування (і контролю) тими NE, що їм підпорядковані.

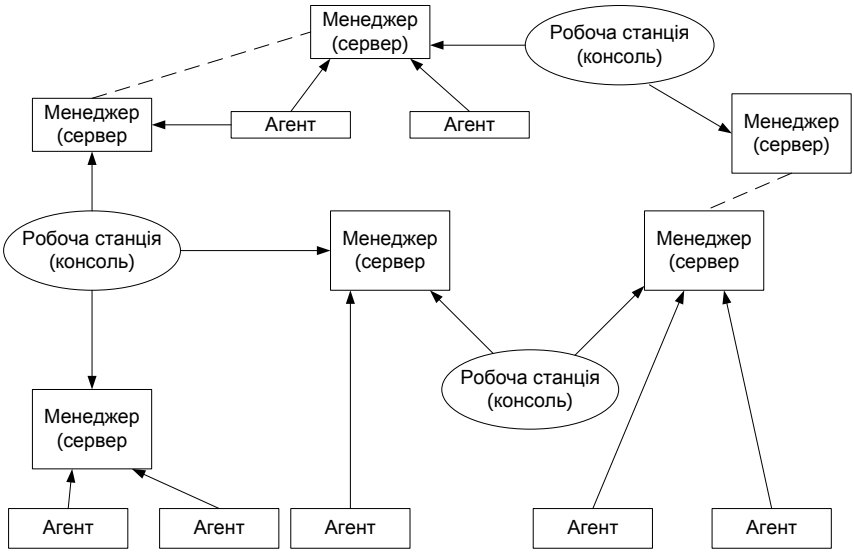


Рис.4.3. Розподілена система керування на базі кількох менеджерів та робочих станцій

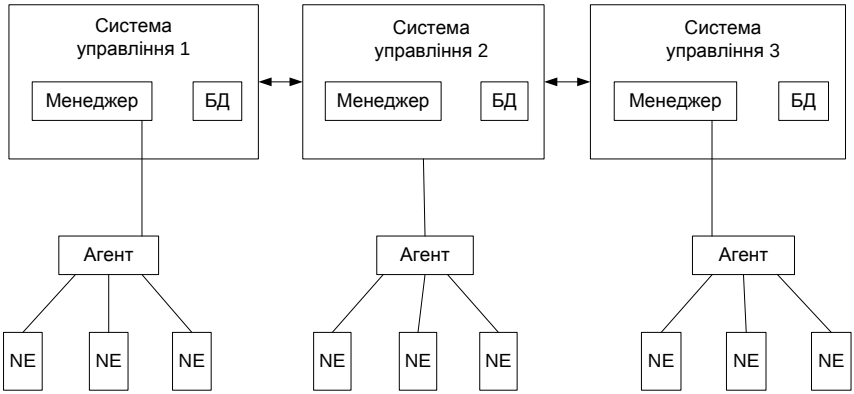


Рис.4.4. Однорангові зв'язки між менеджерами

Адміністратори ТЛК-системи, що працюють за клавіатурами робочих станцій, мають можливість підключитися до будь-якого менеджера (або до кількох менеджерів одразу) і за допомогою графічного інтерфейсу оглянути дані щодо поточного стану об'єкту керування, а також видати менеджерам певні директиви з метою оптимізації роботи цього об'єкту або його окремих елементів. Включення у систему керування кількох менеджерів дозволяє розділити між ними навантаження із обробки даних керування та забезпечити масштабованість системи. Здебільшого використовуються два типи зв'язків між менеджерами – одноранговий та ієрархічний.

У випадку однорангових зв'язків (див. рис.4.4) маємо децентралізовану систему керування. Кожен із менеджерів вирішує свою групу управлінських завдань і користується інформацією тільки від тих агентів, що йому підпорядковані. Менеджери є незалежними один від одного, а координація їхньої роботи досягається за рахунок обміну інформацією між базами даних менеджерів.

Ієрархічна структура зв'язків між менеджерами, що відображена на рис. 4.5, є більш гнучкою. Гнучкість забезпечується тим, що кожен менеджер більш низького рівня у той же час виконує функції агента для менеджера більш вищого рівня. Як наслідок, у бази MIB менеджерів більш вищих рівнів заноситься тільки та інформація, котра вже цілеспрямовано оброблена менеджерами

більш низьких рівнів. Це підвищує якість та гнучкість керування, а також суттєво скорочує обсяги інформації, що циркулює між різними рівнями системи керування.

Система управління мережею. Схема „менеджер – агент" лежить в основі найбільш поширених стандартів мережного керування на основі протоколів SNMP та CMIP. Міжнародні організації ISO та ITU-T у рамках моделі TMN підтримують протокол керування CMIP (Common Management Information Protocol), що придатний для використання при побудові системи керування ТЛК-системою будь-якого ступеню складності. CMIP – це повнофункціональний спеціалізований протокол, орієнтований на керування великими територіально розгалуженими ТЛК-системами (тобто, ТЛК-мережами). Проте протокол CMIP є дуже складним у реалізації. Тому для керування не дуже складними і не дуже великорозмірними ТЛК-системами застосовують більш прості протоколи. Одним із таких простих протоколів, що широко використовуються для керування мережами Інтернет є протокол SNMP (Simple Network Management Protocol).

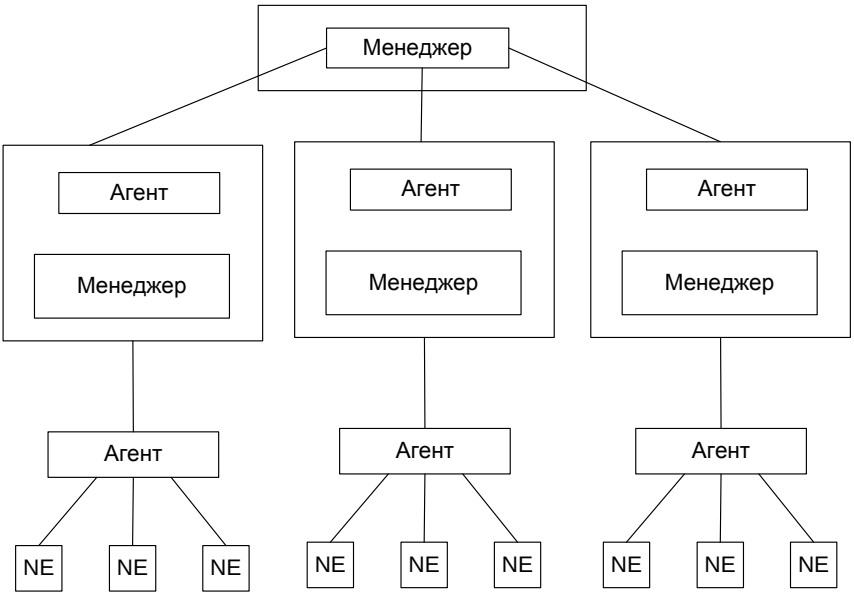


Рис.4.5. Ієрархічні зв'язки між менеджерами

4.4.Стандарти протоколу керування SNMP

Основна перевага протоколу керування SNMP – це його простота. Що і обумовило його поширеність, популярність та довготривалість застосування, особливо в мережах, що побудовані на стеку протоколів TCP/IP.

Примітиви протоколу SNMP. SNMP – це протокол прикладного рівня, що реалізує схему керування типу „менеджер – агент", тобто на кожний запит, що надійшов від менеджера у формі команди, агент має сформувати та передати відповідь. Протокол дозволяє оперувати менеджеру та агенту усього із кількома командами, а саме:

1) команда Get-request («отримай запит») використовується менеджером для отримання від агента значень показників певного об'єкту за його іменем;

2) команда GetNext-request («отримай наступний запит») використовується менеджером для отримання від агента відповіді щодо значень показників наступного об'єкту у випадках, коли здійснюється послідовний перегляд таблиці об'єктів;

3) команда Get-response («отримай відповідь») – відповідь агента, що надсилається на адресу менеджера, як реакція на команду Get-request або GetNext-request;

4) команда Set («установити») дозволяє менеджеру встановлювати або змінювати значення показника якогось об'єкту, а також задавати умови, у разі виконання котрих агент повинен надіслати менеджеру відповідне повідомлення (зокрема, за допомогою цієї команди менеджер може отримати інформацію про такі системні події, як втрата зв'язку, відновлення зв'язку, некоректна автентифікація, рестарт агента, розірвання віртуального каналу тощо: якщо виникає будь-яка із названих подій, то агент ініціалізує відповідне переривання процесу функціонування обладнання, яке фіксується менеджером);

5) команда Trap («зловлено») використовується агентом для повідомлення на адресу менеджера про виникнення особливої події;

6) команда GetBulk дозволяє менеджеру запитувати кілька значень показника певного об'єкту або кількох об'єктів (ця команда у першій версії протоколу SNMP – відсутня).

Зрозуміло, що у будь-якому разі агент повинен „розуміти” імена об’єктів, що він отримує від менеджера, і на основі цих даних здійснювати реальні керуючі впливи – переключати порти, активізовувати канали, запускати процеси авторизації і т.ін.

У загальному випадку бажано формалізувати наступні аспекти функціонування схеми «менеджер - агент»:

- протокол взаємодії агента з менеджером;
- інтерфейс «агент-керований ресурс»;
- інтерфейс «агент-модель керованого ресурсу»;
- інтерфейс «менеджер-модель керованого ресурсу»;
- довідкова служба щодо розташування агентів та менеджерів;
- мова опису моделей керованих ресурсів, тобто мова опису бази *MIB*;
- дерево наступництва, що дозволяє будувати нові моделі на основі більш узагальнених моделей;
- дерево включення, що відображає взаємозв’язок між елементами реальної системи.

Однак із усіх цих аспектів функціонування схеми «менеджер - агент» у рамках протоколу SNMP стандартизовано лише необхідний мінімум: протокол взаємодії «агент-менеджер», абстрактну мову опису бази MIB (так звану мову абстрактної синтаксичної нотації ASN.1, що підтримується рекомендацією MCE-T X.208) та конкретні версії наступних чотирьох моделей бази MIB – MIB-1, MIB-2, RMON та RMON2. Щодо цих моделей то стандарти визначають лише структуру баз MIB, набір типів та імен їхніх об’єктів, а також дозволені операції над ними. Усе інше – не стандартизовано, і, отже, має розроблюватися виготовлювачами засобів SNMP за власним розсудом.

Структура SNMP MIB. У рамках протоколу керування SNMP наразі стандартизовано наступні моделі бази MIB:

1) MIB1 та MIB2 – для використання в задачах локального керування за схемою „менеджер – агент”;

2) RMON та RMON2 для використання в задачах віддаленого керування;

3) спеціалізовані MIB для ТЛК-обладнання конкретного типу (для концентраторів, для модемів і т. ін.);

4) бази MIB конкретних постачальників ТЛК-обладнання.

Модель бази MIB1 – це найбільш спрощена модель бази MIB. Вона припускає користування лише командами Get-request та Get-response. Ця модель розроблювалася з метою її використання для керування пакетними комутаторами та маршрутизаторами, що реалізують стек протоколів TCP/IP. Специфікація MIB1 (в інтерпретації Комісії із регулювання зв'язку США RFC 1156) визначає 114 стандартних об'єктів, що поділені на наступні вісім груп:

1) група System – загальні дані про обладнання, що підлягає керуванню (наприклад, ідентифікатор постачальника обладнання, номер версії ПЗ, момент останньої ініціалізації тощо).

2) група Interfaces – характеристики інтерфейсів обладнання (зокрема, їхня кількість, назва, типи, інтенсивність та інші параметри інформаційних потоків, що через них проходять, тощо).

3) група Address Translation Table – ідентифікація параметрів відповідності між мережними та фізичними адресами, зокрема згідно з протоколом ARP.

4) група Internet Protocol – дані протоколу IP (IP-адреси шлюзів, хостів, серверів, статистичні дані проходження пакетів IP через ту чи іншу точку контролю тощо).

5) група ICMP – дані протоколу обміну керуючими повідомленнями ICMP.

6) група TCP – дані про TCP-з'єднання.

7) група UDP – дані про UDP–дейтаграми (їх кількість, що прийнята з помилками, що втрачена і т.ін.).

8) група EGP – дані протоколу EGP.

Модель бази MIB2 – є подальшим удосконаленням моделі MIB1. Специфікація MIB2 (в інтерпретації RFC 1213) визначає 185 стандартних об'єктів, що поділені на 10 груп.

Як база MIB1, так і база MIB2 мають деревоподібну структуру. Для прикладу на рис. 4.6 показана деревоподібна структура двох (із 10 можливих) груп стандартних об'єктів бази MIB2, а саме: група об'єктів System та група об'єктів Interfaces. Імена об'єктів групи System починаються із префікса Sys, а групи Interfaces - із префікса If .

Розглянемо значення стандартних об'єктів, що показані на рис.4.6. Об'єкт SysUpTime із групи System містить значення

тривалості часу роботи керованої системи, починаючи із моменту останнього перезавантаження. Об'єкт SysDescr містить опис керованої системи. Об'єкт SysObjectID - це ідентифікатор одного із керованих пристроїв (наприклад, шлюзу). Група об'єктів Interfaces представлена двома підгрупами об'єктів: IfTable та IfNumber. Об'єкт IfTable визначає усі стандартні об'єкти одного із конкретних інтерфейсів керованої системи, що представляються у табличній формі. Об'єкт IfEntry визначає вхід до множини цих таблиць, тобто є вершиною піддерева таблиць, що описують цей інтерфейс.

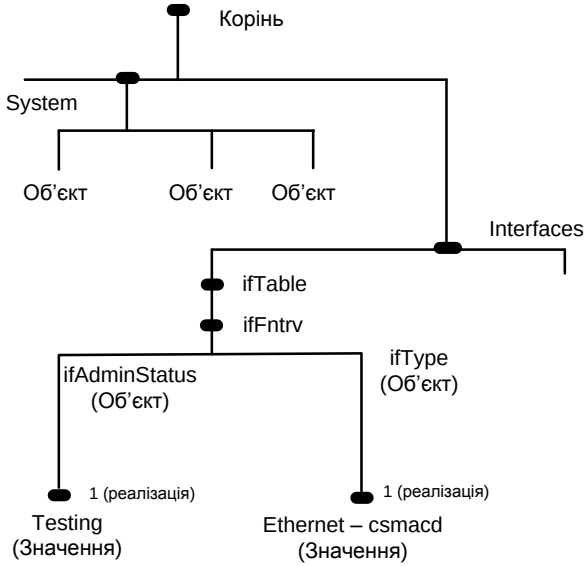


Рис.4.6. Стандартне дерево об'єктів бази *MIB2*

Піддерево IfTable складається із двох гілок: IfAdminStatus та IfType, котрі визначають відповідно стан та тип у даному випадку інтерфейса Ethernet. Стандартні об'єкти, що входять до складу цих гілок, мають наступні значення:

IfType – визначає тип протоколу, що підтримується інтерфейсом (у даному випадку інтерфейсом Ethernet). Цей об'єкт може приймати значення будь-якого із інтерфейсів канального рівня, наприклад Ethernet-csmacd, rfc877-x25, iso88025-tocenRing і т. ін.;

IfMtu – визначає максимальний розмір мережного пакету, що може бути переданий через цей інтерфейс;

IfSpeed – пропускна здатність інтерфейса, що вимірюється у мегабітах за секунду;

IfPhyzAddress – фізична адреса порта (для протоколів Ethernet – це MAC-адреса);

IfAdminStatus – визначає стан порта щодо готовності функціонувати у штатних режимах (up - готов передавати пакети, down - не готов передавати пакети, testing - знаходиться у режимі тестування);

IfOperStatus – визначає поточний стан порта та має ті ж самі значення параметрів, що і об'єкт IfAdminStatus;

IfInOctets – загальна кількість байтів (включаючи службові), що прийнята портом з моменту останньої ініціалізації SNMP-агента;

IfInUcasPkts – кількість пакетів з індивідуальною адресою порта даного інтерфейсу, що були доставлені протоколу верхнього рівня;

IfInNUcasPkts – кількість пакетів з груповою або широкомовною адресою порта даного інтерфейсу, що були доставлені протоколу верхнього рівня;

IfInDiscards – кількість коректно прийнятих пакетів, але не доставлених протоколу верхнього рівня (зокрема, через переповнення буферу пакетів);

IfInErrors – кількість пакетів, що були прийняті з помилками і тому не переданих протоколу верхнього рівня.

Підкреслимо, що поряд з об'єктами, що відображають статистику роботи контрольованого інтерфейсу щодо вхідних пакетів структура бази MIB2 передбачає також стандартизацію аналогічних об'єктів щодо вихідних пакетів.

Аналізуючи структуру бази MIB2, можливо стверджувати, що вона за багатьма аспектами не дає детального опису контрольованого об'єкту. Зокрема, вона не дає детальної статистики щодо помилок у кадрах Ethernet (що вкрай важливо для системного адміністратора). Окрім цього, вона не відображає у наглядній формі зміни у параметрах контрольованого об'єкту у реальному часі. Ці недоліки були усунені завдяки уведенню в дію стандарта RMON MIB, котрий спеціально був орієнтований на збирання детальної статистики про роботу протоколу Ethernet.

Зокрема можливості RMON MIB передбачають побудову часових залежностей значень параметрів протоколу Ethernet.

Для ідентифікації об'єктів бази RMON MIB та визначення формату їхнього представлення уведена специфікація структури керуючої інформації, що називається SMI (Structure of Management Information). Наприклад, для найменування адреси IP обрано ім'я IpAddress, а формат цього стандартного об'єкту визначено як рядок довжиною 4 байти. Різного роду лічильники іменуються як Counter, для котрих задається формат у вигляді цілого числа у діапазоні від 0 до 232 -1. Імена змінних можуть представлятися як у символьних, так і у числових форматах. Наприклад, символьному імені SysDescr відповідває складове число (тобто, число, що складається через крапки із певної кількості цілих чисел) 1.3.6.1.2.1.1.1. Символьний формат використовується для представлення змінних у текстових документах та на екранах моніторів, а числовий формат – у повідомленнях протоколу SNMP. Корисно знати, що розробники протоколу SNMP зареєстрували стандартні об'єкти MIB не в якості стандартів Інтернет (котрі публікуються як документи RFC), а в якості стандартів ISO. Складове числове ім'я об'єкту MIB SNMP відповідає імені цього об'єкту у так званому всесвітньому дереві реєстрації об'єктів, що стандартизоване ISO. Це дерево показане на рис.4.7. DoD?

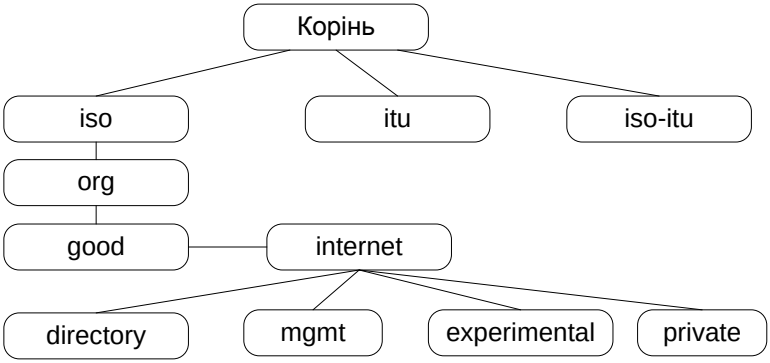


Рис. 4.7. Простір імен стандартизованих об'єктів *ISO*

На рис. 4.7 відображена лише частина верхнньої частини

всесвітнього дерева стандартних імен ISO. Однак це дозволяє визначити повне числове ім'я об'єкту MIB. Як бачимо на рис. 4.7, від кореня дерева відходять три гілки, що відповідають стандартам ISO, ITU та спільним стандартам ISO/ITU. У свою чергу, організація ISO створила гілку org для стандартів, що розроблені національними та іншими (окрім ISO) міжнародними організаціями із стандартизації. У цю гілку входить підгілка DoD – стандартів, що створювались під егідою Міністерства оборони США (Department of Defence, DoD). Стандарти Інтернет розроблювались під егідою цього міністерства. Тому група стандартів керування мережами Інтернет має повне символьне ім'я ISO.org.DoD.Internet.mgmt, а повне символьне ім'я об'єкту MIB - ISO.org.DoD.Internet.mgmt.MIB. Символьні імена об'єктів надаються у стандартах ISO. Проте у повідомленнях протоколу SNMP використовуються не символьні імена, а числова форма їхнього представлення. Для знаходження відповідності між символьними та числовими формами представлення імен слід пам'ятати, що у дереві імен ISO кожна гілка нумерується цілими числами зліва направо. Якщо б на рис.4.7 було представлено у повній мірі дерево стандартних імен, то було б легко визначити, що повному символьному імені об'єкта MIB відповідає повне числове ім'я 1.3.6.1.2.1.

Група об'єктів private зареєстрована за стандартами недержавних корпорацій, таких як Cisco, Nortel і т.п.

Важливо знати, що це ж саме дерево реєстрації імен ISO використано для найменування стандартних об'єктів протоколів CMIP та TMN.

Формат SNMP-повідомлень. Протокол SNMP, що обслуговує процес передавання повідомлень між агентами та менеджерами, використовує ненадійний дейтаграмний спосіб транспортування службових пакетів, заснований на протоколі UDP. Керуюча інформація, що передається каналами IP у вигляді дейтаграмних повідомлень, може легко загубитися або бути перехопленою чи модифікованою несанкціонованою особою, що не має повноважень на право керування ТЛК-системою. З іншого боку, в умовах такого простого способу передавання ресурси керованого об'єкту не завантажуються необхідністю обробки великої кількості службової

інформації, що мало б місце, якщо б для транспортування службових пакетів використовувався стек протоколів TCP/IP. У кінці 80-х років минулого сторіччя (коли розроблювалися протоколи SNMP) ТЛК-обладнання було не таке продуктивне, як зараз, і застосування протоколу TCP для цих цілей з економічної точки зору було невиправданим.

Формат SNMP-повідомлень не передбачає заголовків із фіксованими полями та складається із довільної кількості службових полів. Кожне поле починається із опису його типу та розміру. Будь-яке SNMP-повідомлення розбивається на три частини: версії протоколу, ідентифікатора спільності та області даних.

Ідентифікатор спільності (community string) використовується для групування пристроїв, що мають керуватися певним менеджером. Цей ідентифікатор фактично є аналогом паролю, оскільки для того, щоб певна група пристроїв мала можливість взаємодіяти згідно з протоколом SNMP, усі ці пристрої повинні мати одне і те ж значення ідентифікатора спільності. За умовчанням цей ідентифікатор має значення public.

Область даних (data) містить інформацію про команди протоколу SNMP (ті, що були розглянуті вище), зокрема імена їхніх об'єктів (із бази MIB) та конкретні значення параметрів цих об'єктів. В області data містяться один або кілька протокольних блоків даних (protocol data unit, PDU). Кожний із цих PDU може відноситися до одного із п'яти можливих типів PDU. У свою чергу, кожен тип PDU узгоджений за форматом із відповідною командою протоколу SNMP: Get-request-PDU, GetNext-request-PDU, Get-response-PDU, Set-PDU, Trap-PDU. Наприклад, формат блоку Get-request-PDU включає у себе такі поля як ідентифікатор запиту, статус помилки (вона є чи її немає), індекс помилки (тобто, тип помилки, якщо вона виникла), список імен об'єктів MIB SNMP, що включені до запиту.

На рис.4.8 в якості прикладу показано повідомлення протоколу SNMP, що представляє собою запит про значення об'єкту SysDescr (його повне числове ім'я – 1.3.6.1.2.1.1.1).

1	30	22	02	01	00			
	SEQUENCE	lon=41	INTEGER	lon =1	vers =0			
2	04	06	70	75	62	60	69	63
	string	lon=6	P	u	b	l	i	c
3	A0	1C	02	04	05	AE	56	02
	getreq	lon=26	INTEGER	lon =4	----	requested ID	---	---
4	02	01	00	02	01	00		
	INTEGER	lon=1	Status	INTEGER	lon=1	emor	index	
5	30	OE	30	OC	08	08		
	SEQUENCE	lon=14	SEQUENCE	lon =12	objectid	lon=8		
6	28	06	01	02	01	01	01	00
	1,3	6	1	2	1	1	1	0
7	05	00						
	null	lon=0						

Рис.4.8. Приклад повідомлення протоколу *SNMP*

Як бачимо із рис. 4.8, це повідомлення складається із семи рядків кодових слів. Під кожним кодовим словом наведений його символьний аналог (так що на рис.4.8 усього маємо чотирнадцять рядків). Повідомлення слід читати зліва направо (спочатку перший рядок, потім другий рядок і т.д.). Повідомлення починається із кодового слова 30 (усі коди – шістьнадцятирічні), що відповідає ключовому слову SEQUENCE (послідовність). Це означає, що повідомлення складається не з одного поля, а з певної послідовності полів. Довжина послідовності вказується у наступному байті. Це кодове слово 22 (бачимо, що ця довжина дорівнює 41 байту). Далі вказується версія протоколу SNMP, тобто використовується специфікація MIB1 чи MIB2. Для цього спочатку наводиться код (02) слова INTEGER (тобто, далі буде ціле число). Вказується (01), що цьому числу виділяється один байт. І далі безпосередньо вказується версія MIB протоколу SNMP: якщо

vers=0 (як вказано у таблиці), то маємо справу із MIB1; якщо було б вказано vers=1, то ми мали б справу із MIB2. Далі читаємо другий рядок повідомлення. Код 04 означає, що поле ідентифікатора спільності має тип string (тобто, рядок) довжиною (код 06) 6 байт з ключовим словом public. Далі читаємо третій рядок повідомлення. З нього починається протокольний блок даних типу Get-request-PDU. Те, що маємо справу саме із командою Get-request говорить код A0 (його символьний аналог вказаний у таблиці безпосередньо знизу цього коду, тобто слово getreq). Далі бачимо, що довжина цього PDU складає 28 байтів (якщо рахувати також перші два байти заголовка цього PDU). Далі йдуть два кодових слова 02 та 04, що означає виділення чотирьох байтів для цілого числа. Це ціле 4-х байтове число має значення 05 AE 56 02. Символьна розшифровка цього числа означає поле ідентифікатору запиту. Далі у четвертому рядку повідомлення бачимо два однобайтових цілих числа, що означають відповідно статус та індекс помилки. Вони встановлені у нуль. Це значить, що помилка не виявлена. Починаючи з п'ятого рядка, маємо список імен об'єктів, значення котрих запитуються командою Get-request. Цей список у даному випадку складається із однієї змінної, що має числове ім'я 1.3.6.1.2.1.1.1.0, що відповідає символьному імені групи об'єктів SysDescr. Ознака null (якій відповідає числове ім'я 05) означає кінець повідомлення.

Модель бази ***RMON MIB.*** До появи специфікацій бази RMON MIB протокол SNMP використовувався лише у цілях локального адміністрування ТЛК-обладнання, що підтримувало протоколи стеку TCP/IP. Специфікації RMON (Remote Maintenance and Operation Network) розширили функціональні можливості протоколу SNMP, дозволяючи здійснювати віддалену взаємодію з базою MIB і не тільки в мережах TCP/IP. База RMON MIB містить агреговану інформацію щодо керованого пристрою і тому не потребує передавання через мережу великих обсягів службової інформації. Специфікації RMON MIB у порівнянні із MIB1 або MIB2 визначають додаткові стандартні об'єкти. Зокрема, такі як додаткові лічильники помилок у пакетах, більш гнучкі засоби аналізу трендів і статистичних даних, більш продуктивні засоби фільтрації для захоплення та аналізу окремих пакетів, а також

більш деталізовані умови встановлення порогів для формування сигналів тривожної сигналізації. Агенти RMON у порівнянні із агентами MIB1 або MIB2 мають більш високий рівень інтелектуальних можливостей, що дозволяє їм брати на себе значний обсяг обчислювальних робіт і, тим самим, розвантажувати ресурси менеджерів. На практиці обладнання агентів монтується у складі керованих об'єктів (комутаторів, маршрутизаторів, шлюзів тощо) або виконується у вигляді окремих програмних модулів, що завантажуються у ПК або ноутбуки.

Стандартному об'єкту RMON у наборі об'єктів MIB присвоєно номер 16, котрий, у свою чергу, об'єднує близько 200 об'єктів, котрі об'єднані у 10 груп об'єктів більш низького рівня у деревоподібній структурі об'єктів цієї бази. Специфікації цих груп об'єктів відрізняються від розглянутих вище специфікацій груп об'єктів бази MIB2 і виглядають наступним чином:

1) Statistics (1) – поточні накопичені поточні дані про характеристики пакетів, кількості колізій і т. ін.;

2) History (2) – статистичні дані, що зібрані через визначені проміжки часу і зберігаються для наступного аналізу тенденцій у їхніх змінах;

3) Alarms (3) – порогові значення статистичних показників, при перевищенні котрих агенти мають надсилати відповідні повідомлення на адресу менеджерів;

4) Hosts (4) – дані про мережні хости та їхні MAC-адреси;

5) Host TopN (5) – таблиця найбільш завантажених хостів мережі;

6) Traffic Matrix (6) – матриця завантаженості каналів між кожною парою хостів у мережі;

7) Filter (7) – умови фільтрації пакетів;

8) Packet Capture (8) – умови захоплення пакетів;

9) Event (9) – умови реєстрації та генерації подій;

10) Token Ring (10) - спеціальні об'єкти протоколу Token Ring.

Порядок визначення числових імен об'єктів MIB розглядався раніше. Наприклад, числове ім'я групи Hosts має вигляд 1.3.6.1.2.1.16.4.

Специфікації RMON MIB зафіксовані у двох документах: RFC 1271 (для мереж Ethernet) та RFC 1513 (для мереж Token Ring).

Розглянемо більш детально групу Statistics, що визначає, яку саме інформацію здатний предоставити агент RMON щодо кадрів Ethernet (у специфікаціях RFC ці кадри називаються пакетами). Звернемо увагу, що група History заснована на об'єктах групи Statistics, оскільки об'єкти групи History призначені для побудови часових рядів об'єктів групи Statistics.

У групу Statistics входять наступні об'єкти:

- etherStatsDropEvents – загальна кількість подій, коли пакети були проігноровані агентом через дефіцит його ресурсів (при цьому самі ці пакети, можливо, коректно просунулись через інтерфейс);
- etherStatsOctets – загальна кількість прийнятих байтів (тобто, усіх байтів, що пройшли через визначену точку контролю, за виключенням преамбули; байти полів контрольних сум та помилкових пакетів враховуються);
- etherStatsPkts – загальна кількість отриманих пакетів (у т.ч., помилкових);
- etherStatsBroadcastPkts – загальна кількість коректно прийнятих широкомовних пакетів;
- etherStatsMulticastPkts – загальна кількість коректно прийнятих пакетів за груповою адресою;
- etherStatsCRCAlignErrors – загальна кількість отриманих пакетів, що мали невірну контрольну суму;
- etherStatsUndersizePkts – загальна кількість отриманих пакетів, що мали неприпустимо малу довжину (тобто, були меншими, ніж 64 байти);
- etherStatsOversizePkts – загальна кількість отриманих пакетів, що мали неприпустимо велику довжину (тобто, були довшими, ніж 1518 байтів);
- etherStatsFragments – загальна кількість невірно отриманих пакетів (тобто, вони або складалися не із цілого числа байтів, або мали невірну контрольну суму, або мали неприпустимо малу довжину);
- etherStatsJabbers – загальна кількість невірно отриманих пакетів (тобто, вони або складалися не із цілого числа байтів, або мали невірну контрольну суму, або мали неприпустимо велику довжину);

- etherStatsColizions – найбільш ймовірна кількість колізій, що мали місце у контрольованому сегменті Ethernet;

- etherStatsPkts64Octets – загальна кількість отриманих пакетів (у т.ч., помилкових) розміром 64 байти;

- etherStatsPkts65to127Octets – загальна кількість отриманих пакетів (у т.ч., помилкових) розміром від 65 до 127 байтів;

- etherStatsPkts128to255Octets – загальна кількість отриманих пакетів (у т.ч., помилкових) розміром від 128 до 255 байтів;

- etherStats256to511Octets – загальна кількість отриманих пакетів (у т.ч., помилкових) розміром від 256 до 511 байтів;

- etherStats512to1023Octets – загальна кількість отриманих пакетів (у т.ч., помилкових) розміром від 512 до 1023 байтів;

- etherStats1024to1518Octets – загальна кількість отриманих пакетів (у т.ч., помилкових) розміром від 1024 до 1518 байтів.

Як бачимо із вищенаведеного, за допомогою агента RMON, вбудованого у будь-який засіб пакетної комутації, існує можливість здійснити тонкий аналіз роботи сегменту Ethernet. Спочатку можливо отримати дані щодо типів виниклих помилок у кадрах. Потім побудувати залежності інтенсивності цих помилок у часі (для цього використати об’єкти групи History). За результатами аналізу часових залежностей з’явиться можливість зробити певні попередні висновки щодо подальших дій із пошуку джерела виниклої проблеми і сформулювати більш тонкі і деталізовані умови захоплення кадрів. Специфічні ознаки цих умов є можливим задати за допомогою об’єктів групи Filters. Після відповідної фільтрації кадрів відкривається можливість провести ще більш тонкий аналіз проблеми шляхом вивчення захоплених (за допомогою групи Packets Capture) кадрів.

Таким чином, застосування моделі RMON MIB дозволяє вирішувати широкий спектр задач керування об’єктами телекомунікаційної техніки. Проте слід зазначити, що на сьогодняшній день стандартизовано удосконалений варіант цієї моделі під назвою RMON2. Удосконалення дозволили розповсюдити функціональність RMON MIB на протоколи верхніх рівнів (тобто, не тільки на кадри Ethernet,). От же обладнання, що реалізує специфікації RMON2, є здатним виконувати функції сучасних аналізаторів протоколів.

4.5. Недоліки протоколу SNMP

Протокол знайшов широке застосування у сучасних системах керування ТЛК-обладнанням. Проте через притаманні йому принципові недоліки він не є основним засобом керування об'єктами телекомунікаційної техніки. Слід вказати на два основних недоліки цього протоколу: орієнтованість на використання ненадійного транспортного протоколу UDP (на що вже зверталась увага) та відсутність засобів взаємної автентифікації агентів із менеджерами.

Єдиним стандартизованим механізмом протоколу SNMP будь-яких версій, котрий лише умовно можливо віднести до засобу автентифікації, слід вважати так званий рядок спільності (community string) у форматі повідомлень SNMP. Цей ідентифікатор, як вже вказувалось, слугує основою для об'єднання агентів і менеджерів: агент взаємодіє лише з тими менеджерами, що мають із ним однаковий рядок спільності. На жаль, цей рядок передається каналами мережі у відкритій формі і, отже, не забезпечує прийнятний рівень інформаційної безпеки. Деякі розробники засобів SNMP MIB2 доповнили функціональність цього протоколу додатковими механізмами автентифікації, проте вони не є стандартизованими і тому не обов'язкові для реалізації.

Щодо роботи через ненадійний протокол UDP, то, на жаль, він є джерелом неякісного адміністрування ТЛК-обладнання, зокрема його застосування призводить до загублень службових пакетів в каналах взаємодії агентів з менеджерами, не говорячи вже про те, що ці пакети являються легкою здобиччю всілякого роду зловмисників та хакерів. Протокол SNMP є дуже простий у реалізації, на його основі розроблено безліч різноманітних агентів. Тому від цього протоколу ТЛК-оператори не поспішають відмовлятися. Робляться спроби його удосконалення таким чином, щоб ці удосконалення не торкались роботи агентів. Зокрема у системі керування HP OV Telecom DM TMN (це одна із основних сучасних платформ, що використовується для створення багаторівневих систем адміністрування у рамках стандартів ISO) механізми протоколу SNMP удосконалені таким чином, що загублені службові пакети відновлюються за рахунок їхньої повторної передачі. Однак в багатьох випадках використання ТЛК-

обладнання функціональність протоколу SNMP не є достатньою. Тому за допомогою протоколу SNMP у сучасних телекомунікаціях вирішується лише обмежене коло локальних завдань адміністрування. У відповідальних випадках транспортування службових пакетів із керуючою інформацією здійснюють за допомогою більш надійних транспортних протоколів із установленням з'єднань. Зокрема, використовують протокол TCP. Якщо ж виникає потреба забезпечити не тільки надійність передавання службових пакетів, але ще і їхню захищеність від нексанкціонованого доступу (НСД) з боку неавторизованих осіб або процесів, то між агентами та менеджерами утворюють так звані захищені канали (фізичні або логічні), а самі службові пакети шифрують за допомогою сучасних методів криптографії.

Контрольні питання до четвертої лекції

1. Які системи керування називають централізованими ?
2. Що таке локальні механізми керування ?
3. Що таке вузол керування ?
4. Надайте узагальнену характеристику моделі керування TMN?
5. Як структурується сукупність задач керування згідно стандарту ISO 7498-4 ?
6. Надайте характеристику групі задач Configuration Management.
7. Надайте характеристику групі задач Fault Management.
8. Надайте характеристику групі задач Performance Management.
9. Надайте характеристику групі задач Security Management.
10. Надайте характеристику групі задач Accounting Management.
11. Що таке білінг ?
12. Надайте характеристику схемі керування типу «менеджер - агент».
13. Що таке модель керованого об'єкту у схемі «менеджер - агент» ?
14. Що таке база MIB у схемі «менеджер - агент» ?
15. Чим відрізняються мережі внутрішньосмугового керування від мереж позасмугового керування ?
16. Чим відрізняється одноранговий тип зв'язків між

менеджерами від ієрархічного ?

17. Які протоколи керування підтримує ISO/ITU-T у рамках моделі TMN?

18. Яка основна перевага протоколу керування SNMP ?

19. Назвіть примітиви протоколу SNMP.

20. Надайте характеристику структурі SNMP MIB.

21. Надайте характеристику моделі бази MIB1.

22. Надайте характеристику моделі бази MIB2.

23. Який формат SNMP-повідомлень ?

24. Надайте характеристику моделі бази MIB RMON.

25. Назвіть недоліки протоколу SNMP ?

Література до четвертої лекції

1) Рекомендація МСЕ-Т М.60. Терміни та визначення, що відносяться до технічної експлуатації.

2) В.Г. Оліфер, Н. А.Оліфер. Комп'ютерні мережі. Принципи, технології, протоколи: Посібник для вузів. Друге видання – СПб.: Питер, 2003. Розділ 20, стор. 791 – 815.

3) Рекомендація МСЕ-Т М.3010. Принципи організації мережі керування електрозв'язком (TMN).

4) Рекомендація МСЕ-Т М.3200. Огляд послуг керування мережі TMN.

5) Рекомендація МСЕ-Т М.3400. Функції керування мережею TMN.

МОДУЛЬ №2. ТЕХНОЛОГІЇ ВИМІРЮВАНЬ ЕКСПЛУАТАЦІЙНИХ ПАРАМЕТРІВ ТЛК-ОБЛАДНАННЯ

ЛЕКЦІЯ №5. ЗАГАЛЬНІ ПОЛОЖЕННЯ ЩОДО ВИМІРЮВАНЬ ЕКСПЛУАТАЦІЙНИХ ПАРАМЕТРІВ ТЛК-ОБЛАДНАННЯ

Розглядаються наступні питання:

5.1. Загальна характеристика технологій вимірювань параметрів обладнання

5.2. Вибір технології вимірювань для вирішення експлуатаційних завдань

5.3. Класифікатор технологій вимірювань

5.4. Методики вимірювань

5.5. Обробка, оформлення та подання результатів вимірювань

Самостійне заняття. Методи представлення сигналів у системах зв'язку

5.6. Спектральні методи представлення сигналів

5.7. Окові діаграми

5.8. Діаграми станів

5.9. Деревоподібні діаграми

5.10. Решітчасті діаграми Треліса

5.1. Загальна характеристика технологій вимірювань параметрів обладнання

Вимірювання параметрів обладнання телекомунікаційних систем відноситься до найважливіших процедур, що здійснюються майже на усіх стадіях життєвого циклу цього обладнання. На стадії виготовлення, а також в багатьох випадках під час увіду ТЛК-обладнання в експлуатацію здійснюють так звані системні вимірювання із використанням спеціалізованих системних вимірювальних засобів. Цим засобам притаманні широкі функціональні можливості, висока точність та ступінь автоматизації вимірювань, а також підвищені можливості щодо їхньої інтеграції у вимірювальні комплекси. Проте системне інструментальне обладнання, нерідко унікальне, є високовартісним. Воно не розраховано на оперативний режим

застосування та має використовуватися у стаціонарних умовах роботи. На стадії експлуатації ТЛК-обладнання здійснюють експлуатаційні вимірювання. І використовують для цього, як правило, недорогі портативні прилади. Завдяки цим вимірюванням експлуатаційний персонал має змогу отримати об'єктивну відповідь на широкий спектр питань, що виникають в процесі експлуатації, зокрема визначити: чи знаходиться обладнання у працездатному стані; чи відповідає якість обслуговування положенням сервісних угод з клієнтами; чи вийшли які-небудь параметри за межі припустимих норм; якщо вийшли, то які саме елементи обладнання спричинили або зможуть причинити збій або відмову у роботі обладнання; чи загрожує фрагменту мережі перенавантаження трафіком і т.д. і т.п. Цілі, заради яких здійснюються вимірювання, витікають із широкого кола розглянутих у лекції №2 експлуатаційних завдань, вирішення котрих потребує застосування різноманітних методів, схем та технологій вимірювань.

Проте щодо телекомунікацій існує одна найбільш узагальнена модель процедури вимірювань, яка лежить в основі переважної більшості вимірювальних технологій, що використовуються на практиці. Коротко, сутність її полягає у наступному. Виходячи із змісту експлуатаційних завдань, визначають множину параметрів об'єкту експлуатації, що потребують вимірювань. Для кожного із визначених параметрів розроблюють методику вимірювань (якщо вона відсутня) та обирають норму на діапазон припустимих значень цього параметру. І далі згідно розроблених методик проводять вимірювання параметрів, а отримані в результаті вимірювань значення параметрів порівнюють із нормами. Якщо виміряні значення параметрів знаходяться в межах діапазонів припустимих значень, то робиться висновок про нормальне функціонування обладнання та (або) про нормальний рівень якості обслуговування. Якщо ж виміряні значення будь-якого із параметрів вийшли за межі припустимих значень, то це говорить про виникнення невідповідностей в роботі обладнання, що у більшості випадків потребує певної реакції з боку системи експлуатації, інакше можуть мати місце негативні наслідки, зокрема погіршення якості обслуговування або, навіть, відмови в

роботі обладнання. Добре, коли у складі експлуатаційної документації на об'єкт експлуатації містяться усі необхідні методики вимірювань, а інструментальна база експлуатаційної організації дозволяє втілити ці методики у життя. У протилежних випадках, експлуатаційному персоналу доводиться самостійно розроблювати необхідні методики, виходячи із конкретних умов використання обладнання та обмежень існуючої інструментальної бази. Слід пам'ятати, що в основі будь-якої методики лежить певним чином обраний метод вимірювань, що реалізується згідно із певною схемою вимірювань. Тому практично у всіх базових навчальних дисциплінах за напрямком „телекомунікації" значна увага приділяється визначенню множини параметрів, котрі за типових умов використання тієї чи іншої ТЛК-технології потребують вимірювань, та вивченню відповідних методів та схем вимірювань. Вважається, що на момент вивчення матеріалу цього підручника студент вже обізнаний з основними аспектами вимірювальних технологій, що є типовими для більшості сучасних ТЛК-технологій. Матеріал цієї лекції лише систематизує раніш набуті знання та містить відповідні посилання на основні публікації у рамках розглянутих питань. Щодо визначення норм на припустимі значення параметрів, то ці норми обираються на основі аналізу відповідних стандартів, технічних вимог та умов, а також інших нормативних документів, що мають чинність на території України і можуть бути коректно застосовані саме у тих умовах, в яких використовується об'єкт експлуатації.

5.2. Вибір технології вимірювань для вирішення експлуатаційних завдань

Вибір тієї чи іншої технології вимірювань напряму залежить від цілей та змісту вимірювань. Зрозуміло, що будь-які вимірювання виконуються із певними цілями. Наприклад, ціллю вимірювань може бути отримання відповіді на питання, чи може узятий зі складу відрізок нового оптичного кабелю бути використаний для заміни відрізку старого оптичного кабелю, що втратив свої властивості через фізичну деградацію оптоволокна. Можна навести багато інших прикладів щодо можливих цілей вимірювань. Проте усі вони витікають із цілей поставлених експлуатаційних завдань.

Цілі експлуатаційних завдань, у свою чергу, формулюються, головним чином, виходячи із положень прийнятої політики (стратегії) експлуатації ТЛК-обладнання. Зміст вимірювань визначається властивостями та логікою роботи конкретного набору засобів телекомунікаційної техніки, що реалізує визначену множину технологій і функціонує в конкретних умовах експлуатації. Тобто, на зміст вимірювань впливають як характеристики об'єкту експлуатації (в якості котрого розглядається ТЛК-обладнання), так і характеристики середовища експлуатації. Усе вищезазначене має бути враховано під час планування експлуатаційних завдань і, отже, при організації вимірювальних робіт.

5.3. Прийнятий класифікатор технологій вимірювань

Загальноприйнятої унормованої класифікації технологій вимірювань параметрів телекомунікаційного обладнання поки що не створено. Напевно через те, що параметри сучасного ТЛК-обладнання, які потребують вимірювань, характеризуються великою кількістю та різнорідністю.

Тим не менш, з метою упорядкування викладу щодо вимірювань параметрів ТЛК-обладнання будемо керуватися наступними міркуваннями. Основне призначення ТЛК-обладнання, як вже раніш зазначалось, полягає у технічному забезпеченні транспортування інформації. Процеси транспортування інформації майже повністю специфікуються чотирма нижніми рівнями семирівневої моделі інформаційної взаємодії відкритих систем OSI ISO, а саме фізичним, канальним, мережним та сеансовим рівнями цієї моделі. Тому множину технологій вимірювань параметрів ТЛК-обладнання також доцільно розглядати у розрізі чотирьох нижніх рівнів семирівневої моделі.

Примітка 1. Слід мати на увазі, що на практиці часто класифікація процесів інформаційної взаємодії у ТЛК-системах здійснюється не на основі семірівневої моделі OSI (Open System Interconnection) міжнародної організації із стандартізації ISO (International Standartization Organization), а на основі моделі Інтернет. Мережному рівню Інтернет відповідають два рівня моделі OSI - мережний та сеансовий.

В якості прикладу розглянемо структуру сучасної глобальної

транспортної IP-мережі (див. рис.5.1), що реалізується наразі більшістю операторів електрозв'язку. Вона, як бачимо із рис.5.1, будується за чотирьохрівневою схемою.

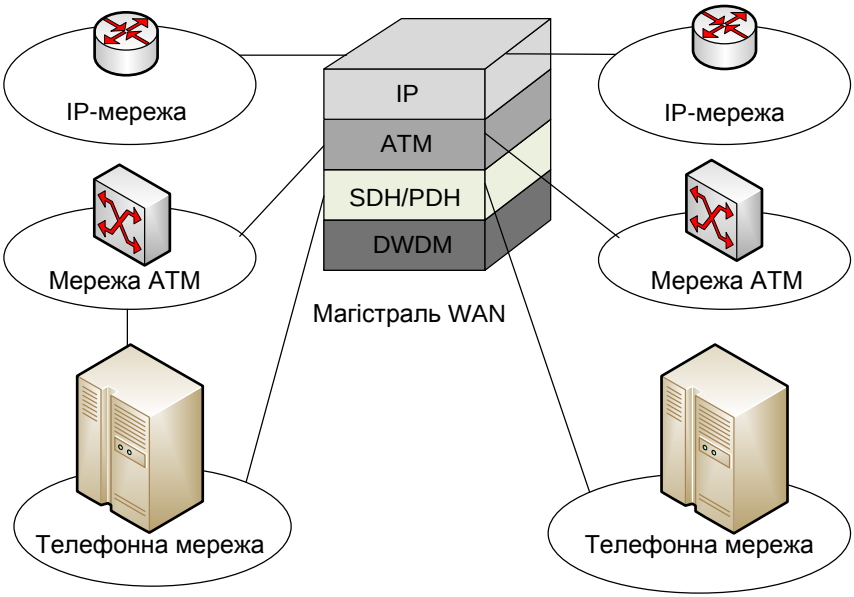


Рис.5.1. Чотирьохрівнева структура сучасної пакетної мережі

Проте рівні цієї схеми не співпадають із рівнями моделі взаємодії відкритих інформаційних систем (*OSI*) *ISO*. Нижньому (фізичному) рівню моделі *ISO* відповідають два нижніх рівня схеми рис.5.1, тобто мережа широкосмугових оптоволоконних каналів з пропускною здатністю 10 Гбіт/с і вище, що зараз будується на основі технології *DWDM*, та накладена поверх неї система передавання цифрової синхронної ієрархії (*SDH*) з мережами доступу, що створюються на базі плезіохронних цифрових систем передавання (*PDH*). Як відомо, за допомогою обладнання *SDH/PDH* оптичні спектральні канали *DWDM* діляться на більш дрібні субканали *TDM*, кінці котрих з'єднуються з портами комутаторів мережі канального рівню (на рис.5.1 – це комутатори *ATM*). Обладнання двох нижніх рівнів схеми рис.5.1

(тобто, обладнання *DWDM* разом із обладнанням *SDH/PDH*) утворюють так звану первинну мережу електрозв'язку. Зверху на первинну мережу накладаються вторинні мережі канального рівню (згідно класифікації *ISO*) – пакетні або телефонні (з комутацією каналів). На рис.5.1 в якості вторинної вибрана пакетна мережа *ATM*, що має у порівнянні з іншими пакетними мережами найбільш гнучкі механізми керування потоками пакетного трафіку. Замість *ATM* на третьому рівні структури, відображеної на рис.5.1, могла бути використана будь-яка інша пакетна технологія канального рівню - *Frame Relay, X.25* (дуже застаріла технологія, яка практично вже не застосовується), *Optical Ethernet* тощо. Накінець, на четвертому (верхньому) рівні структури рис.5.1 показана мережа *IP*, що відповідає згідно семирівневій моделі *ISO* мережному та сеансовому рівням цієї моделі. Обладнання мережі *IP* функціонує, як правило, за специфікаціями стеку протоколів *TCP/IP*.

Логічно розгляд технологій вимірювань почати із технологій вимірювань параметрів ТЛК-обладнання на фізичному рівні взаємодії інформаційних систем, що і буде зроблено на наступній лекції.

5.4. Методики вимірювань

5.4.1. Загальна характеристика методик вимірювань

Оцінку поточних значень контрольованих параметрів здійснюють, як правило, шляхом вимірювання. Для вимірювань використовують відповідні методики. За звичайних умов використовують методики вимірювань, що засновані на :

- прямих вимірюваннях значень контрольованого параметру, у т.ч. із використанням тестового трафіку. Приклад: вимірювання часу передачі *IP*-пакетів від відправника цих пакетів до їх одержувача та у зворотному напрямку (*Round-Trip Time, RTT*) для пакетів заданого розміру;

- обчислені значення контрольованого параметру шляхом прямих вимірювань інших параметрів, що пов'язані із контрольованим певною функціональною залежністю. Приклад: визначення затримки у передаванні пакетів заданого розміру на

маршруті від відправника до одержувача шляхом безпосереднього вимірювання затримок передачі пакетів на кожній із ділянок маршруту передавання;

- статистичному визначенні значення контрольованого оцінюваного параметру на певний момент часу за умов, коли є звісними статистичний закон розподілу значень цього параметру та представницький набір його значень, що отримані експериментальним шляхом. У цьому разі мова йде не про виміряне значення параметру, а про оцінювання можливого його значення та про рівень достовірності отриманої оцінки. Приклад: оцінювання поточного значення пропускної здатності каналу, якщо є звісними значення пропускної здатності у попередні проміжки часу, попередні та поточні значення затримок у передаванні пакетів, а також модель потоку таких пакетів.

5.4.2. Загальні вимоги щодо методик вимірювань

Для того, щоб результати вимірювань були коректними, необхідно дотримуватися ряду умов, що пов'язані не тільки із організацією процесу вимірювань, але і з методиками вимірювань (або методиками оцінки) параметрів. Зокрема, вимірювання та оцінювання параметрів має здійснюватися у відповідності із науково обгрунтованими та всебічно апробованими методиками. Вимірювання повинні за ідентичних умов проведення вимірювань давати однакові результати, тобто забезпечувати відтворюваність результатів вимірювань. Також у більшості випадків має виконуватися принцип неперервності, який полягає у наступному: для незначних змін умов проведення вимірювань повинні спостерігатись незначні відхилення результатів вимірювань.

Під час розробки методик вимірювань необхідно на кількісному рівні оцінити можливі похибки вимірювань. На основі результатів аналізу похибок мають бути сформульовані вимоги до інструментальних вимірювальних засобів та умов проведення вимірювань, дотримання яких дозволить знизити похибки або тримати їх у припустимих межах.

5.4.3. Вимірювання проміжків часу

Значна кількість методик визначення параметрів ТЛК-

обладнання ґрунтується на вимірюванні часу. З огляду на цей факт необхідно враховувати похибки вимірювань та недостовірності в оцінках, які можуть бути пов'язані з пристроями для вимірювання часу.

У *RFC 1305* (*RFC* – комісія з радіочастот, регуляторна установа США) визначені характеристики вимірювачів проміжків часу (тобто, таймерів), які можуть бути використані для оцінювання якості їхнього функціонування. Зокрема похибка (*offset*) таймера у певний момент часу визначається як різниця між зареєстрованим часом та «дійсним» (*true*) часом (в якості котрого розглядають так званий загальний скоординований час, *Universal Coordinated Time, UCT*). Тобто, якщо зареєстрований таймером час дорівнює T_c, а «дійсний» час дорівнює T_t, то похибка таймера буде визначатись як $T_c - T_t$. Точність (*accuracy*) таймера у даний момент часу визначається тим, на скільки абсолютне значення його похибки буде відмінним від нуля.

Розфазування (*skew*) таймера (перша похідна від абсолютної похибки) – це різниця між частотами опорних сигналів досліджуваного та еталонного таймерів. Величина розфазування може змінюватись у часі. Тобто, у загальному випадку друга похідна від похибки показань таймера по відношенню до «дійсного» часу не дорівнює нулю. Цей процес, відповідно до *RFC 1305*, називається дрейфом (*drift*) таймера.

Розділювальна здатність (*resolution, разрешающая способность*) таймера – це найменша одиниця часу, на яку змінюються показання таймера. Розділювальною здатністю встановлюється нижня межа невизначеності показань таймера. Слід мати на увазі, що таймер може мати високу роздільну здатність та водночас низьку точність.

Існують випадки, коли методики вимірювань включають порівняння показань двох таймерів. Прикладом є безпосереднє вимірювання затримки у передаванні протокольних блоків даних на шляху від їх відправника до одержувача без утворення зворотного каналу (*one-way delay*). У цьому випадку значення затримки одержують шляхом порівняння показань таймера на одному із кінців маршруту передавання з показаннями таймера на іншому кінці. У даному випадку на точність вимірювань

впливають, головним чином, не абсолютні значення похибки, розфазування та дрейфу таймерів, а відносні значення цих показників. Відносна похибка таймера А у деякий момент часу визначається як різниця між показаннями таймера А та показаннями таймера В у цей момент часу. Тобто, якщо зареєстрований час у відповідності із таймером А дорівнює T_a, а цей же момент часу за таймером В дорівнює $T_в$, то відносна похибка таймера А буде визначатись як $T_a - T_в$. Відносне розфазування та дрейф таймерів визначають аналогічно.

Якщо таймер є точним щодо іншого таймеру (тобто, його відносна похибка дорівнює нулю), то такий таймер вважається синхронізованим (*synchronized*). Слід мати на увазі, що таймери можуть бути синхронізованими та водночас мати низьку точність. Під час вимірювання багатьох параметрів ТЛК-обладнання синхронність таймерів має більший вплив на точність вимірювань, ніж абсолютні похибки таймерів. Те саме стосується і розфазування: доки абсолютне значення розфазування не є надто великим, відсутність відносного розфазування двох таймерів є більш важливим фактором.

5.4.4. Апаратні засоби та програмне забезпечення (ПЗ) вузлів телекомунікаційної мережі, які задіяні у процесі вимірювань, також можуть впливати на результати вимірювань. Особливо це стосується випадків, коли реєстрація часу настання мережних подій здійснюється засобами прикладного ПЗ вузла мережі, а не засобами операційної системи. Тому у випадку, коли необхідно вимірювати параметри затримок пакетів у каналах зв'язку між вузлами мережі, доцільно розглянути можливість використання замість штатних засобів вузла мережі в якості вимірювального обладнання спеціалізованих інструментальних засобів, наприклад, аналізатора протоколів.

5.4.5. Часто оцінки виміряних значень параметрів залежать від типу і розмірів протокольних блоків даних (*PDU*), які були використані в процесі вимірювань. Наприклад, пов'язаність (рос. – связность) транспортного каналу між двома вузлами мережі може бути різною для *IP*-пакетів різної довжини, для *IP*-пакетів, що транспортують *PDU* різних протоколів вищих рівнів (*TCP, UDP*), *IP*-пакетів з невірними контрольними сумами заголовків або

різними значеннями *TTL* і т. ін. У випадку наявності між вузлами мережі міжмережних екранів або використання протоколу *RSVP* врахування типу *PDU*, що використовуються для транспортування інформації, є особливо важливим для коректного функціонування мережного обладнання. Тому, визначаючи певний параметр або вказуючи його конкретне значення, завжди слід зазначати, *PDU* якого типу використовувались у процесі вимірювань.

5.4.6. Контрольовані параметри за способом їхнього визначення можуть бути розділені на три групи:

1) параметри, для визначення яких необхідно виконати одиничне вимірювання. Наприклад, для визначення обсягу даних, що були транспортовані між відправником даних та їхнім одержувачем протягом одного сеансу зв'язку необхідно виконати однократну процедуру вимірювання кількості PDU, що були отримані одержувачем даних протягом цього сеансу зв'язку;

2) параметри, для визначення яких необхідно виконати багатократні вимірювання. Наприклад, для визначення затримки у передаванні блоків даних може знадобитись реалізація послідовності вимірювань, виконаних протягом 1 години із проміжком часу між кожним вимірюванням, що дорівнює 1 с;

3) параметри, для оцінювання ймовірних значень яких необхідно виконати статистичну обробку результатів послідовності вимірювань. Наприклад, середню затримку у передаванні блоків даних визначають шляхом статистичної обробки результатів зазначеної вище послідовності вимірювань.

Основною метою виконання серії вимірювань під час оцінювання ймовірних значень вимірюваних параметрів є прагнення урахувати зміни у часі, яких може зазнавати оцінюваний параметр, в залежності від особливостей розташування вузла мережі, від дня тижня, години доби і т. п. Визначення необхідної кількості актів вимірювань в серії є важливою задачею, оскільки крім довготривалих флуктуацій вимірювані величини зазнають також короткочасних змін, які, зокрема, пов'язані із пульсуючим характером трафіку пакетних мереж.

5.4.7. Загальним способом організації вимірювання (або оцінювання) поточних значень контрольованих параметрів ТЛК-обладнання є проведення їх періодичних вимірювань через

фіксовані інтервали часу. Перевагою цього способу організації вимірювань є його простота. Водночас, якщо період змін вимірюваного параметра дорівнює періодові проведення вимірювань або кратний йому, то використання фіксованих інтервалів часу може стати причиною похибок у результатах вимірювань.

5.4.8. Причинами похибок можуть бути і деякі інші фактори, природа яких відображена у нижченаведеному прикладі.

У якості приклада розглянемо розповсюджений спосіб вимірювання величини затримки у передаванні *IP*-пакетів від відправника цих пакетів до їх одержувача та у зворотному напрямку (*Round-Trip Time, RTT*). Як видно із рис.5.2, процес вимірювань *RTT* полягає у надсиланні *K* тестових пакетів, що складають одну групу тестових пакетів, із інтервалом τ одиниць часу між кожним пакетом в межах групи. Надсилається багато груп тестових пакетів з часовим інтервалом між групами, що дорівнює *T* одиниць часу.? ? ? тестових, а не текстових

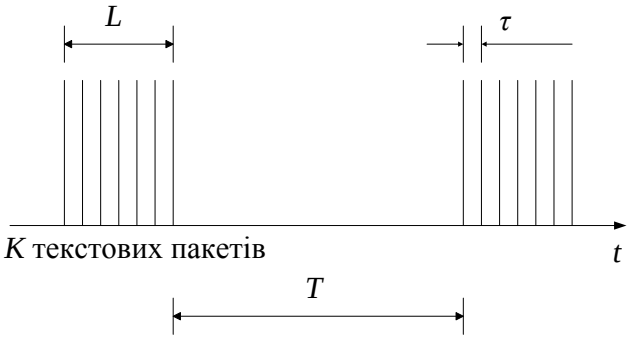


Рис.5.2. Ілюстрація структури тестового потоку пакетів для вимірювання величини параметра *RTT*

Через перенавантаження елементів мережі або непередбачених змін маршруту транспортування пакетів на шляху між відправником та одержувачем оцінка значення *RTT*, що отримується на одній групі тестових пакетів, може суттєво змінюватись. Тому оцінювання виконується не на одній групі пакетів, а на певній множині груп пакетів за умов, коли групи тестових пакетів надсилаються кожні *T* одиниць часу.

З метою зменшення часу обробки тестових пакетів у елементах мережі та часу їхнього передавання через канали зв'язку розмір цих пакетів повинен бути якнайменшим. Тому в якості тестових пакетів доцільно обрати протокольні блоки даних протоколу *ICMP*.

Якщо інтервал τ між тестовими пакетами занадто малий, то вони будуть надсилатись у мережу занадто швидко, що може викликати їхню буферизацію у вихідних чергах портів мережного обладнання. У цьому випадку виміряна величина *RTT* буде відрізнятись від реально можливого значення (для умов, коли пакети просуваються за маршрутом без затримок у чергах) на час знаходження тестових пакетів у чергах. Для уникнення буферизації необхідно визначити мінімальне значення часу τ, при якому пакети не впливають один на одного.

Час $L = K \cdot \tau$ передавання групи тестових пакетів повинен бути таким, щоб імовірність зміни маршруту пакетів між відправником та одержувачем за цей час була достатньо малою.

Для найбільш повного визначення характеру змін параметру *RTT* у часі інтервал надсилання груп тестових пакетів *T* повинен бути достатньо малим (як мінімум, у двічі меншим, ніж період зміни величини *RTT*). З іншого боку, з метою зменшення похибок вимірювання *RTT* через вплив тестового трафіку на поточну завантаженість мережних ресурсів, значення інтервалу *T* доцільно збільшувати. Тому оптимальне значення *T* слід визначати емпіричним шляхом з урахуванням конкретних цілей та умов проведення вимірювань.

*5.4.9. Недоліки проведення періодичних вимірювань значень параметрів через фіксовані інтервали***.** Як вже зазначалось, проведення періодичних вимірювань значень параметрів через фіксовані інтервали часу має ряд недоліків. Більш раціональним підходом до визначення параметрів є виконання вимірювань через випадкові інтервали часу *T*, які мають бути розподілені у відповідності із певним законом статистичного розподілу *G(t)*. Зокрема, час надсилання наступної у послідовності групи тестових пакетів носить непередбачуваний характер, якщо *G(t)* є експоненціальним розподілом (розподілом Пуасона) з коефіцієнтом λ, тобто

$$G(t) = 1 - e^{-\lambda t}. \quad (5.1)$$

Документом *RFC 2330* рекомендовано використання саме цього розподілу для генерації тестових послідовностей під час проведення вимірювань, які пов'язані із визначенням показників якості мережних послуг. Однак у деяких випадках використання такого розподілу не є виправданим. Так, зокрема, проміжок часу між здійсненням актів вимірювань у випадку використання закону Пуасона теоретично не є обмеженим. Однак у багатьох випадках може бути корисним обмежити максимальний час між вимірюваннями деякою величиною *dT*. У цьому разі для генерації тестових послідовностей реалізують рівномірний закон розподілу, а сааме:

$$G(t) = \text{Unif}\,(0, dT). \quad (5.2)$$

5.4.10. В експлуатаційній практиці знайшов застосування спосіб визначення значень вимірюваних параметрів, згідно з яким вимірювання проводяться з фіксованою імовірністю *p*. Наприклад, під час вимірювань із застосуванням аналізатора протоколів цим пристроєм реєструються усі *PDU*, що просуваються через канал зв'язку, однак до траси протоколів записується інформація щодо *PDU* лише у випадку, якщо деяке випадкове число із рівномірним законом розподілу на інтервалі від 0 до 1 є більшим, ніж *p*. Такий спосіб вимірювань має усі переваги способу вимірювань із використанням закону Пуассона.

5.4.11. Оскільки спосіб організації послідовності вимірювань із використанням закону Пуасона є рекомендованим і найбільш поширеним, далі розглядаються різні варіанти реалізації такого способу вимірювань.

Перш за все, слід визначити коефіцієнт λ (наприклад, якщо середній інтервал між одиничними вимірюваннями дорівнює T = 30 с, то λ = 1/30). Потім слід згенерувати набір експоненційно розподілених (псевдо) випадкових чисел $E_1, E_2, \ldots, E_n$. Перше вимірювання проводиться через інтервал часу E_1, друге – через інтервал E_1+E_2 і т. д. Більшість комп'ютерних систем мають штатні засоби генерації (псевдо) випадкових чисел $U_1, U_2, \ldots, U_n$, які рівномірно розподілені на інтервалі від 0 до 1. Випадкові числа E_i

отримують за формулою

$$E_i = -\frac{\log(U_i)}{\lambda}, \qquad (5.3)$$

де log (U_i) – натуральний логарифм U_i.

Існують, як мінімум, три способи виконання послідовності вимірювань із використанням закону Пуасона.

Перший спосіб є найпростішим у реалізації. Він полягає у наступному:

1) Згенерувати випадкове число E_1 і чекати протягом E_1 с.

2) Виконати процедуру вимірювання.

3) Згенерувати випадкове число E_2 і чекати протягом E_2 с.

4) Виконати процедуру вимірювання.

5) Згенерувати випадкове число E_3 і чекати протягом E_3 с.

6) Виконати процедуру вимірювання і т. д. …

Однак процедура вимірювання триває деякий час M_i. Тому вимірювання відбуваються не у моменти часу E_1, E_1+E_2…, а у інтервали E_1, $E_1+M_1+E_2$… . Якщо час M_i малий у порівнянні з 1/λ, то похибка, яка пов'язана із даним способом, є також відносно малою. У іншому випадку методичною похибкою нехтувати не можна.

У другому способі виконання послідовності вимірювань час M_i враховано. Цей спосіб полягає у наступному:

1) Згенерувати випадкове число E_1 і чекати протягом E_1 с.

2) Виконати процедуру вимірювання та визначити її тривалість M_1.

3) Згенерувати випадкове число E_2 і чекати протягом E_2-M_1 с.

4) Виконати процедуру вимірювання і т. д. …

Але цей спосіб також має недолік – його реалізація можлива лише за умови, що $E_{i+1} \geq M_i$. У іншому випадку виникає необхідність виконувати кілька вимірювань одночасно.

Третій спосіб полягає у наступному:

1) Згенерувати випадкові числа E_1, E_2, …, E_n.

2) Визначити моменти виконання вимірювань T_1, T_2, …, T_n, де $T_i=E_1+…+E_i$.

3) Виконати необхідні вимірювання.

У випадку припустимості одночасного виконання кількох

процедур вимірювання третій спосіб позбавлений недоліків, які властиві першим двом способам. Якщо виконання *i*-тої процедури вимірювання суттєво впливає на результати інших процедур, то третій спосіб не має переваг і може виявитись навіть гіршим за два попередні.

На практиці, якщо $M_i << 1/\lambda$, то можливе використання будь-якого із способів виконання послідовності вимірювань із використанням закону Пуассона. Якщо $M_i \leq 1/\lambda$, слід використовувати другий спосіб. У випадку припустимості одночасного виконання кількох процедур вимірювання використовують третій спосіб виконання вимірювань.

5.5. Обробка, оформлення та подання результатів вимірювань

5.5.1. Обробку результатів вимірювань параметрів контрольованого обладнання здійснюють з метою:

1) контролю поточного стану обладнання на відповідність вимогам експлуатаційної документації та стандартам підприємства;

2) контролю поточного стану якості надання телекомунікаційних послуг (якості обслуговування) на відповідність умовам сервісних угод з клієнтами (*SLA – Service Level Agreement*) або корпоративним стандартам;

3) інформування покупців послуг щодо поточного стану обслуговування відповідно до умов *SLA*;

4) інформування управлінських структур підприємства щодо стану обладнання і обслуговування (для забезпечення виконання ними функцій контролю та управління);

5) отримання вихідних даних для пошуку можливостей розширення номенклатури та підвищення якості послуг і обслуговування;

6) отримання вихідних даних для прогнозування стану обслуговування і планування розвитку мережі.

5.5.2. Обробку результатів вимірювань здійснюють окремо щодо кожного напряму передавання інформації на всіх рівнях ієрархії вузлів телекомунікаційної мережі.

Для послуг, що надаються на умовах гарантованої якості обслуговування, обробку результатів вимірювань здійснюють

окремо щодо кожної точки доступу до послуги (або кожної групи точок доступу до послуги).

Результати обробки вимірювань агрегують та структурують в залежності від задач, в яких ці результати використовуються, і надаються покупцям послуг, іншим підрозділам та адміністрації телекомунікаційної компанії.

5.5.3. Оброблюються результати вимірювань щодо кожного визначального параметра у розрізі кожної наданої телекомунікаційної послуги. Основна форма представлення результатів вимірювань – графіки залежності отриманих оцінок визначальних параметрів від часу з масштабом, вибір котрого залежить від виду послуги, класу обслуговування та цілей обробки результатів вимірювань.

Наприклад, для параметрів затримки або девіації затримок протокольних блоків даних в мережаж передавання даних графіки будуються з інтервалом по вісі абсцис, що дорівнює тривалості однієї серії сеансів вимірювань. Усереднені на інтервалі однієї серії сеансів вимірювань значення вищеназваних параметрів відкладаються по вісі ординат.

Для усереднення виміряних значень параметрів, що характеризують якість транспортування протокольних блоків даних (крім параметрів надійності), незалежно від класу обслуговування зазвичай передбачається необхідність здійснення 10 сеансів вимірювань протягом кожної години, тобто одна серія складається із 10 сеансів вимірювань.

Для параметра блокових помилок (мається на увазі коефіцієнт помилково прийнятих протокольних блоків даних) графік будується з інтервалом 12 годин (тобто, з інтервалом, що дорівнює тривалості однієї серії сеансів вимірювань цього параметра). Графік має охоплювати проміжок часу тривалістю 1 місяц (тобто, потрібно побудувати 12 таких графіків протягом 1 року).

Коефіцієнт доступності обладнання (або телекомунікаційної послуги) визначається із дискретністю – 1 доба. Для визначення цього параметра будується погодинна функція доступності (*AF – availability function*) – співвідношення між проміжками часу, коли обладнання або послуга є доступними для користувачів, та проміжками часу, коли вони є недоступними. Дискретність графіка

параметра *AF* – 1 година. Вибір критеріїв доступності та їх порогів буде розглянуто далі.

Параметр годин недоступності обладнання (або послуги) протягом року (*TSU – time service unavailability*) розраховується на звітному проміжку, що дорівнює одному року (тобто, усі часові інтервали, на котрих послуга визначалась як недоступна, підсумовуються протягом одного року).

Інтервал вимірювань параметрів помилок обладнання *ISDN* та *xDSL* на відповідність довгостроковим нормам - 1 місяць. Інтервал вимірювань цих же параметрів на відповідність оперативним нормам – 15 хвилин.

Параметри експлуатаційної надійності розраховуються після кожної події відновлення обладнання.

5.5.4. Побудовані графіки залежностей виміряних оцінок параметрів від часу дозволяють визначитися з поточним станом обладнання та рівнем якості обслуговування. Інформація щодо поточного стану якості обслуговування по кожному напряму передавання даних на всіх рівнях ієрархії вузлів мережі, а також щодо кожної точки доступу до послуг, які надаються на умовах гарантованої якості обслуговування, має відображатися у вигляді табл.5.1.

Таблиця 5.1

Форма представлення інформації щодо поточного стану обслуговування (інтервал обробки результатів вимірювань – 1 доба)

Напрямок передавання або точка доступу до послуги	Поточна дата (число, місяц, рік)
Найменування параметра	**Отримана середньодобова оцінка**
Вносяться тільки ті визначальні параметри якості обслуговування, які узгоджені умовами *SLA*.	

5.5.5. Агрегована інформація щодо поточного стану якості обслуговування по кожному напряму передавання даних на всіх рівнях ієрархії вузлів МПД, а також щодо кожної точки доступу до послуги, які надаються на умовах гарантованої якості обслуговування, має відображатися у вигляді табл.5.2. Інтервал

агрегації – 1 місяць.

Таблиця 5.2

Форма представлення агрегованої інформації щодо стану обслуговування

Напрямок передавання або точка доступу до послуги	1.х. хх	2.х. хх	.....	30.х. хх	Отримана середньомісячна оцінка
Найменування параметра					

5.5.6. Побудовані графіки залежностей визначальних параметрів від часу дозволяють визначитися щодо можливого перевищення нормативів на визначальні параметри.

Зокрема, інформація щодо можливого перевищення нормативів по кожному напряму передавання даних на всіх рівнях ієрархії вузлів мережі передавання даних (МПД) та щодо кожної точки доступу до послуг, які надаються на умовах гарантованої якості обслуговування, має відображатися у вигляді табл.5.3, де під *PDU(TD+DV+LR+ ... + SESR)* мається на увазі сумарний час перевищення нормативних показників визначальних параметрів у розрізі контрольованого обладнання транспортування протокольних блоків даних *PDU* (тобто, у розрізі технологій *IP, ATM, FR, xDSL* тощо). При цьому, якщо зустрічаються випадки перевищення нормативів, які перекриваються у часі, то в загальному часі перевищення нормативів враховується тривалість від початку першого в часі випадку перевищення та до закінчення останнього випадку перевищення.

Таблиця 5.3

Форма представлення інформації щодо випадків та тривалості перевищень нормативів на визначальні параметри, які мали місце протягом доби

Напрямок передавання або точка доступу до послуги	Поточна дата (тривалість перевищення, хв.)
Перевищення нормативу на $PDUTD_0$	хх (хв.)
Перевищення нормативу на $PDUDV_0$	хх (хв.)
Перевищення нормативу на $P(PDUDV_{max})$	хх (хв.)

Перевищення нормативу на $K'_{зав0}$	хх (хв.)
Перевищення нормативу на $PDULR_0$	хх (хв.)
Перевищення нормативу на $P(PDUTD_{max})$	хх (хв.)
Перевищення нормативу на *ESR*	хх (хв.)
Перевищення нормативу на *SESR*	хх (хв.)
Значення *PDU(TD+DV+LR+ …+SESR)*	хх (хв.)
Перевищення нормативу на $PDUER_0$	Виміряне значення $PDUER_0$
Кількість годин недоступності послуги від початку поточного року	хх (годин)

Примітка 1. Визначення параметрів, що в якості прикладу наведені у табл. 5..3, будуть надані далі.

Як видно із табл.5.3, у разі необхідності (наприклад, на вимогу покупця послуги) щодобово можуть надаватися дані щодо перевищення нормативу на коефіцієнт помилок $PDUER_0$.

5.5.7. Агрегована інформація щодо можливого перевищення нормативів по кожному напряму передавання даних на всіх рівнях ієрархії вузлів МПД, а також щодо кожної точки доступу до послуги, які надаються на умовах гарантованої якості обслуговування, має відображатися у вигляді табл.5.4. Інтервал агрегації даних, що поміщені в усі колонки таблиці, крім останньої колонки – 1 доба. Інтервал агрегації даних, що поміщені в останню (заключну) колонку таблиці – 1 місяць.

***Таблиця** 5.4*

Форма представлення агрегованої інформації щодо випадків та тривалості перевищень нормативів на визначальні параметри

Напрямок передавання або точка доступу до послуги	Поточна дата у ____ місяці _____р.				Загальне перевищення нормативу
Перевищення нормативу на параметр, хв. :	1.х. хх	2.х. хх	....	30.х. хх	
$PDUTD_0$					
$PDUDV_0$					
$P(PDUDV_{max})$					
$K'_{зав0}$					
$PDULR_0$					
$P(PDUTD_{max})$					
SES					

SESR					
PDU(TD+DV+LR+ …+SESR)					
$PDUER_0$*)					
Кількість годин недоступності послуги від початку поточного року					

Примітка 2. У графі "загальне перевищення нормативу" вказується сумарний час перевищення нормативу на поточний момент вимірювань протягом місяця.

Примітка 3. Значення перевищення нормованого значення коефіцієнту помилок $PDUER_0$ надається не у хвилинах, а вказується виміряне середньомісячне значення цього параметра.

5.5.8. Сервіс-провайдер із визначеною у SLA періодичністю має надсилати на адресу кожного із покупців послуг, які отримують обслуговування із гарантованим сервісом, звіти про стан обслуговування, в яких міститься інформація про поточний стан справ щодо виконання вимог SLA, про якість наданої послуги та про використані мережні ресурси.

Звіт про виконання вимог сервісної угоди надсилається покупцю послуг один раз на добу і містить інформацію згідно табл.5.3 (та, можливо, також дані щодо перевищення нормативу на $PDUER_0$).

Звіт про якість наданої послуги надсилається на адресу покупця послуг один раз на місяць і містить інформацію у розрізі наданих послуг згідно табл.5.2.

Звіт про використані мережні ресурси надсилається на адресу покупця послуг один раз на місяць. Структура цього звіту напряму залежить від умов SLA і стандартами не регламентується.

Примітка 4. В умовах SLA можуть бути визначені й інші періоди звітування, виходячи із конкретних умов функціонування прикладних застосувань покупця послуг.

Примітка 5. Усі вищезазначені звіти представляються окремо щодо кожної точки доступу до послуги (або кожної групи точок доступу до послуги).

5.5.9. Підрозділи сервіс-провайдера, які безпосередньо здійснюють експлуатацію обладнання МПД, мають надавати

інформацію щодо якості обслуговування керівництву підприємства, його регіонального вузлу дирекції та іншим підрозділам підприємства.

Експлуатаційні підрозділи МПД з періодичністю один раз на місяць мають надсилати на адресу адміністрації свого регіонального вузлу агрегований звіт про якість наданих послуг. Основу цього звіту складають дані щодо випадків та тривалості перевищень нормативів на параметри якості обслуговування за напрямами передавання даних, що оформлені згідно табл.5.4. У якості додатку до табличних даних у звіті надаються пояснення щодо суттєвих випадків перевищень нормативів якості, порушень вимог SLA, причини та наслідки їхнього виникнення, а також щодо заходів, які були проведені з метою ліквідації негативних наслідків та запобігання порушень у майбутньому.

Експлуатаційний персонал з періодичністю один раз на місяць має надсилати на адресу адміністрації свого регіонального вузлу агрегований звіт про використані мережні ресурси. Форма такого звіту - не регламентується.

У свою чергу, адміністрації центрального та регіональних вузлів МПД повинні періодично один раз на місяць надавати на адресу керівництва підприємства – оператора електрозв'язку агрегований звіт про поточний стан обслуговування. Форма цього звіту не регламентується. У звіті мають бути відображені усі найбільш суттєві події, які були пов'язані із виникненням невідповідностей у наданні послуг та у використанні мережних ресурсів, а також зміст здійснених заходів із нейтралізації негативних наслідків та запобігання виникненню таких подій у майбутньому. У додатках до цього звіту мають бути надані агреговані звіти про якість наданих послуг та агреговані звіти про використані мережні ресурси.

Контрольні питання до п'ятої лекції

1. У чому полягає сутність найбільш узагальненої моделі процедури вимірювань?

2. Якими міркуваннями слід керуватися щодо вибору технології вимірювань для вирішення експлуатаційних завдань?

3. У розрізі яких рівнів семирівневої моделі доцільно розглядати

технології вимірювань параметрів ТЛК-обладнання?

4. Надайте загальну характеристику технологій вимірювань.

5. Наведіть загальні вимоги до методики вимірювань.

6. Яким чином вимірюються проміжки часу?

7. На які групи за способом визначення можуть бути розділені контрольовані параметри?

8. Які фактори можуть бути причинами похибок вимірювань?

9. З якою метою здійснюють обробку результатів вимірювань параметрів контрольованого обладнання?

10. Яким чином здійснюється обробка результатів вимірювань?

Література до п'ятої лекції

1) І.Г. Бакланов. Технології вимірювань у сучасних телекомунікаціях. –М.: ЕКО-ТРЕНДЗ, 1998. Розділи 4, 5 та 10.2.

2) І.Г. Бакланов. Методи вимірювань у системах зв'язку. –М.: ЕКО-ТРЕНДЗ, 1999.

САМОСТІЙНЕ ЗАНЯТТЯ ЗА МАТЕРІАЛАМИ ЛЕКЦІЇ №5 МЕТОДИ ПРЕДСТАВЛЕННЯ СИГНАЛІВ У СИСТЕМАХ ЗВ'ЯЗКУ

5.6. Спектральні методи представлення сигналів

У сучасних телекомунікаціях використовуються як цифрові, так і аналогові сигнали. Звісно, що основна відмінність цифрових сигналів від аналогових криється у їхній дискретній структурі. Якщо параметри аналогових сигналів у процесі передавання у певному діапазоні їхніх можливих значень змінюються безперервно, то параметри цифрових сигналів змінюються дискретно. Ця особливість цифрових сигналів дозволяє застосовувати для їхнього аналізу ряд специфічних методів, що відрізняються високою наглядністю та простотою реалізації. Основні методи представлення цифрових сигналів розглянуто нижче.

Достатньо глибоко розроблено методи спектрального аналізу аналогових сигналів, а також аналізу аналогових сигналів з використанням осцилограм. Щодо цифрових сигналів, то широке розповсюдження отримало представлення цих сигналів у вигляді спеціальних діаграм – окових діаграм, діаграм Треліса і т.ін.

Спектральний аналіз аналогових сигналів ???

В багатьох випадках сигнали зручно представляти як $S(t), t \in T_c$, де T_c – час існування сигналу, тобто аргументом функції, що описує сигнал, є час. Подання сигналів як функції часу не є єдине з можливих. Дістав загальне визнання і спектральний спосіб опису сигналів, оскільки будь-який сигнал s(t) зі скінченною енергією, тобто сигнал, для якого виконується умова

$$\int_{-\infty}^{\infty} s^2(t)dt < \infty,$$

можна зобразити у вигляді ряду

$$s(t) = \sum_{k=0}^{\infty} c_k \phi_k(t), \qquad (5.4)$$

де c_k – певним чином визначені коефіцієнти розкладення, що у сукупності називаються спектром сигналу; ϕ_k – система ортонормованих дійсних функцій, або базис.

Формула (5.4) називається узагальненим рядом Фур'є сигналу $s(t)$ в обраному базисі $\{\phi_k\}$.

У теорії електрозв'язку широко застосовується спектральне представлення сигналів у базисах гармонічних функцій. Це передусім пояснюється прямим зв'язком, що існує між спектральним розкладенням та представленням елементів реальних ТЛК-систем у вигляді електричних чотирьохполюсників - коливальних систем. Зокрема, періодичний з періодом Т сигнал зручно зобразити математичним рядом тригонометричних функцій

$$s(t) = c_0 + \sum_{k=1}^{\infty} c_k \cos(2\pi \frac{t}{T} - \varphi_k), \qquad (5.5)$$

тобто сумою членів ряду $c_k \cos(2\pi \frac{t}{T} - \varphi_k)$, кожен з яких є косинусоїдальним коливанням з амплітудою c_k, початковою фазою φ_k і частотами $f_k = \frac{k}{T}$, кратними основній частоті. Значення c_k і φ_k визначаються так, щоб рівність (5.5) виконувалася. Частоти коливань, що складають періодичну функцію $s(t)$, створюють гармонічну послідовність. Окремі складові називають гармоніками.

Вираз (5.5) можна переписати у вигляді ряду Фур'є:

$$s(t) = c_0 + \sum_{k=1}^{\infty} (a_k \cos 2\pi k \frac{t}{T} + b_k \sin 2\pi k \frac{t}{T}),$$

де $a_k = c_k \cos\varphi_k$, $b_k = c_k \sin\varphi_k$, так що $c_k = \sqrt{a_k^2 + b_k^2}$, $tg\varphi_k = \frac{b_k}{a_k}$.

Коефіцієнти a_k і b_k визначають із формул:

$$a_k = \frac{2}{T}\int_{-\frac{T}{2}}^{\frac{T}{2}} s(t)\cos 2\pi k\frac{t}{T}\,dt \qquad b_k = \frac{2}{T}\int_{-\frac{T}{2}}^{\frac{T}{2}} s(t)\sin 2\pi k\frac{t}{T}\,dt$$

$$c_0 = \frac{1}{T}\int_{-\frac{T}{2}}^{\frac{T}{2}} s(t)dt$$

Ряд Фур'є можна також записати у комплексній формі:

$$s(t) = \sum_{k=-\infty}^{\infty} \dot{C}\cdot e^{j2\pi k(\frac{t}{T})}, \qquad (5.6)$$

де $2\dot{C} = c_k e^{-j\varphi_k} = a_k - jb_k$ – комплексна амплітуда, що визначається за формулою:

$$\dot{C}_k = \frac{1}{T}\int_{-\frac{T}{2}}^{\frac{T}{2}} s(t)\cdot e^{-j2\pi k(\frac{t}{T})}dt\ . \qquad (5.7)$$

Ряд Фур'є, як бачимо, розкладає періодичну функцію за тригонометричними функціями. Це розкладання можна узагальнити і на випадок неперіодичної функції, яку можна розглядати як граничний випадок періодичної функції за умови необмежено зростаючого періоду $T\to\infty$.

Підставивши у формулу (5.6) значення $\dot{C}_k$ з виразу (5.7), отримаємо:

$$s(t) = \sum_{k=-\infty}^{\infty} e^{j2\pi k(\frac{t}{T})}\int_{-\frac{T}{2}}^{\frac{T}{2}} s(t)\cdot e^{-j2\pi k(\frac{t}{T})}dt \qquad (5.8)$$

Замість $\frac{1}{T}$ уведемо кругову частоту $\omega_1 = \frac{2\pi}{t}$ – частотний інтервал між сусідніми гармоніками, частоти яких дорівнюють

$2\pi\frac{k}{T}$. За умови граничного переходу заміна відбувається за схемою:

$$T \to \infty,\ \omega \to d\omega,\ 2\pi\frac{k}{T} = \omega,$$

де ω – поточна частота, що змінюється безперервно; $d\omega$ – її приріст. Звідси сума у виразі (5.8) перейде в інтеграл, і тоді:

$$s(t) = \frac{1}{2\pi}\int_{-\infty}^{\infty} e^{j\omega t}d\omega \int_{-\infty}^{\infty} s(t)\cdot e^{-j\omega t}dt,$$

або

$$s(t) = \frac{1}{2\pi}\int_{-\infty}^{\infty} \dot{F}(\omega)\cdot e^{j\omega t}d\omega, \qquad (5.9)$$

де $\overset{*}{F}(\varpi)$ - спектральна щільність сигналу *s(t)* та розраховується

$$\dot{F}(\omega) = \int_{-\infty}^{\infty} s(t)\cdot e^{-j\omega t}dt \qquad (5.10)$$

Формули (5.9) та (5.10) - основні в теорії спектрів. Формулу (5.10) можна записати у дійсній формі, тоді інтегрування виконується тільки за дійсними частотами. Зокрема, якщо увести позначення $\dot{F}(\omega) = A(\omega) + jB(\omega)$, тоді маємо:

$$s(t) = \frac{1}{\pi}\int_{0}^{\infty}\left[A(\omega)\cos\omega t - B(\omega)\sin\omega t\right]d\omega.$$

Для багатьох застосувань достатньо знати спектр амплітуд. Амплітудний спектр є модулем спектральної щільності. Його використовують настільки часто, що коли кажуть «спектр», то розуміють саме амплітудний спектр.

Спектр періодичної функції має вигляд дискретного спектра, який називають також лінійчастим. Це означає, що він складається з рівновіддалених спектральних ліній, тобто частоти гармонік перебувають у простих кратних співвідношеннях.

Дискретний спектр мають не лише періодичні функції. Наприклад коливання, що утворене шляхом складання двох синусоїдних коливань з нерівними і некратними частотами, мають спектр, що складається з двох спектральних ліній.

Спектр неперіодичних сигналів є суцільним, оскільки унаслідок граничного переходу від ряду до інтегралу Фур'є відстані між окремими спектральними лініями необмежено зменшуються, і замість дискретних точок зображується неперервною послідовністю точок, тобто неперервною кривою.

Розглянемо математичні моделі найпростіших типових сигналів, а також їхні спектральні зображення.

Гармонічний сигнал

Гармонічний сигнал називають ще тригонометричним. Математична модель такого сигналу визначається формулою:

$$x(t) = A\cos(\omega_0 t + \varphi_0),$$

а типова осцилограма і амплітудний спектр зображено на рис.5.3.

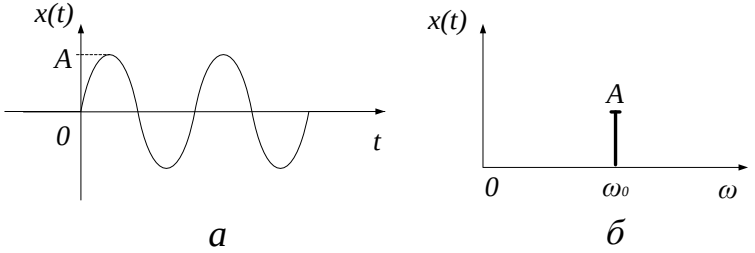


Рис.5.3. Гармонічний сигнал (*а*) і його амплітудний спектр (*б*)

Прямокутний відеоімпульс

Математична модель $s(t)$ одиничного прямокутного відео імпульсу, симетрично розміщеного відносно початку відліку часу (рис.5.4) не є періодичною функцією і задається співвідношенням:

$$s(t) = \begin{cases} U, & -\tau/2 \le t \le \tau/2, \\ 0, & |t| > \tau/2. \end{cases}$$

Амплітудна спектральна щільність такого сигналу є дійсною функцією і обчислюється за формулою:

$$S(\omega) = 2\int_0^{\infty} s(t)\cos(\omega t)dt\,. \qquad (5.11)$$

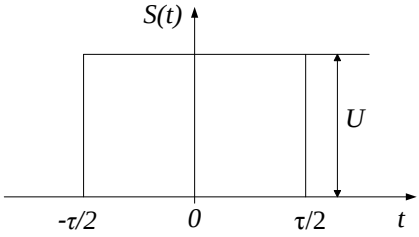


Рис.5.4. Зображення прямокутного відеоімпульсу як функції часу

Оскільки поза межами $|t| > \tau/2$ сигнал дорівнює нулеві, то вираз (5.11) набуває вигляду:

$$S(\omega) = 2U\int_0^{\frac{\tau}{2}} \cos(\omega t)dt = \frac{2U}{\omega}\sin\frac{\omega\tau}{2}\,.$$

Якщо увести безрозмірну змінну $\xi = \omega\tau/2$, то остаточно можна записати вираз для амплітудного спектру (що у даному випадку називають спектральною щільністю) у наступному вигляді:

$$S(\xi) = U\tau\frac{\sin\xi}{\xi}\,.$$

Значення спектральної щільності на нульовій частоті дорівнює площі імпульсу:

$$S(0) = U\tau\,.$$

Отже, нормований амплітудний спектр (рис.5.5) цього імпульсу можна записати як:

$$A(\xi) = \frac{|S(\xi)|}{S(0)}\,.$$

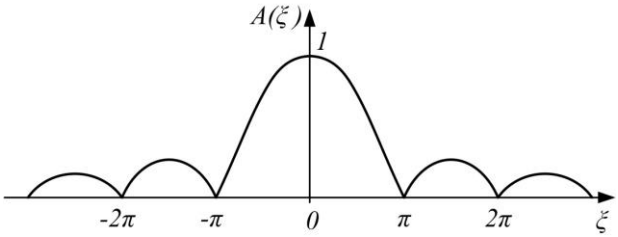


Рис.5.5. Амплітудний спектр одиничного прямокутного відеоімпульсу

Як бачимо, що важливо, ширина спектра одиничного прямокутного відеоімпульсу обернено пропорційна його тривалості, тобто чим коротший імпульс, тим ширший його спектр, і навпаки.

Періодична послідовність прямокутних відеоімпульсів

Така послідовність має аналогічну математичну модель як і одиничний відеоімпульс, з тією різницею, що імпульси повторюються з періодом T (рис.5.6).

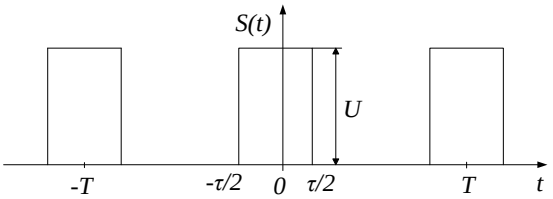


Рис.5.6. Зображення послідовності прямокутних відео імпульсів

Оскільки послідовність - періодична, то можна знайти коефіцієнти ряду Фур'є, а саме:

$$a_0 = \frac{2U}{T}\int_{-\frac{\tau}{2}}^{\frac{\tau}{2}} dt = \frac{2U\tau}{T}$$

$$a_k = \frac{2U}{T}\int_{-\frac{\tau}{2}}^{\frac{\tau}{2}} \cos(k\omega_1 t)dt = \frac{2U\tau}{T}\frac{\sin(k\omega_1\tau/2)}{k\omega_1\tau/2}$$

$$b_k = \frac{2U}{T}\int_{-\frac{\tau}{2}}^{\frac{\tau}{2}} \sin(k\omega_1 t)dt = 0$$

Введемо означення шпаруватості послідовності імпульсів як відношення періоду проходження імпульсів *T* до їхньої тривалості τ:

$$q = \frac{T}{\tau}.$$

Тоді систему коефіцієнтів можна зобразити у наступному вигляді:

$$a_0 = \frac{2U}{q}, \quad a_k = \frac{2U}{q}\frac{\sin(k\pi/q)}{k\pi/q}, \quad b_k = 0.$$

Тепер запишемо ряд Фур'є для періодичної послідовності прямокутних відео імпульсів як

$$s(t) = \frac{U}{q}\left(1 + 2\sum_{k=1}^{\infty}\frac{\sin(k\pi/q)}{k\pi/q}\cdot\cos(k\omega_1 t)\right). \qquad (5.12)$$

Відповідно до виразу (5.12) розглянутий періодичний сигнал можна зобразити як суму сталої складової

$$A_0 = \frac{a_0}{2} = \frac{U}{q}$$

і нескінченної сукупності гармонічних коливань на частотах $\omega_k = k\omega_1$ з амплітудами, які визначаються як модуль величини, що є співмножником гармонічного коливання $\cos(k\omega_1 t)$, тобто

$$A_k = \frac{2U}{q}\left|\frac{\sin(k\pi/q)}{k\pi/q}\right|, \; k = 1,2...$$

Із співвідношення (5.12) випливає, що амплітудний спектр періодичної послідовності прямокутних відео імпульсів є дискретним (рис.5.7).

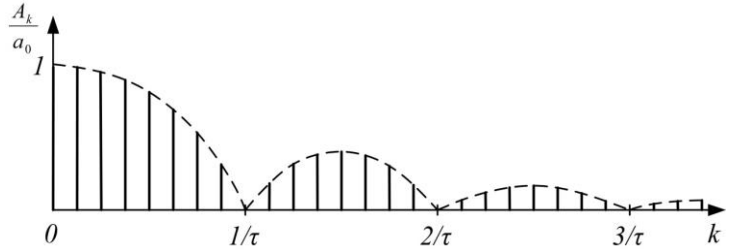


Рис.5.7. Спектр періодичної послідовності прямокутних відео імпульсів

Як бачимо, чим більшою є шпаруватість періодичної послідовності відео імпульсів, тим більше гармонік спектра міститься в кожній пелюстці. При фіксованому періоді проходження імпульсів зі зменшенням тривалості імпульсів збільшується ширина основної пелюстки спектра, і навпаки.

Трикутний відеоімпульс

Математична модель $s(t)$ одиничного трикутного сигналу описується наступною системою рівностей:

$$s(t) = \begin{cases} U(1 + \dfrac{t}{\tau/2}), & -\tau/2 \le t \le 0, \\ U(1 - \dfrac{t}{\frac{\tau}{2}}), & 0 \le t \le \tau/2, \\ 0, & |t| > \tau/2, \end{cases}$$

Графічне відображення цього імпульсу показане на рис.5.8.

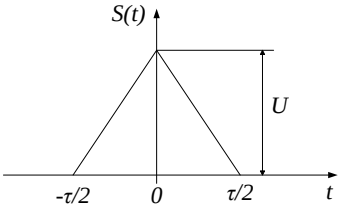


Рис.5.8. Зображення одиничного трикутного відео імпульсу

Вираз для спектру амплітуд трикутного відео імпульсу є наступним:

$$S(\xi) = \frac{U\tau}{2} \cdot \left(\frac{\sin \xi}{\xi} \right)^2, \qquad \text{де } \xi = \omega\tau / 4 .$$

Як бачимо, нормований спектр трикутного імпульсу має такий самий вигляд як і прямокутного, але ширина спектру трикутного відео імпульсу є удвічі більшою при однаковій довжині цих імпульсів.

Періодична послідовність трикутних відео імпульсів

Періодичну послідовність трикутних імпульсів зображено на рис.5.9.

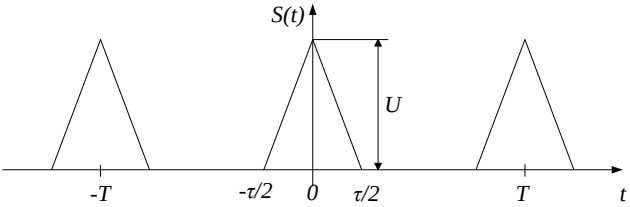


Рис.5.9. Послідовність трикутних відео імпульсів

Математичне представлення такої послідовності має наступний вигляд:

$$s(t) = \frac{U}{2q} \left(1 + 2 \sum_{k=1}^{\infty} \left(\frac{\sin(k\pi / 2q)}{k\pi / 2q} \right)^2 \cdot \cos(k\omega_1 t) \right). \qquad (5.13)$$

Амплітудний спектр послідовності трикутних імпульсів показано на рис.5.10.

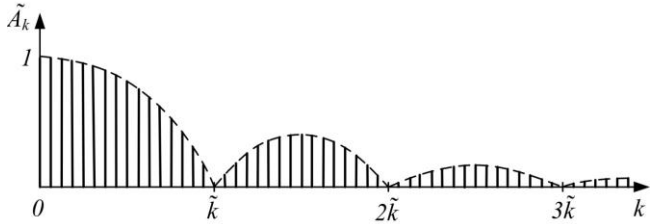


Рис.5.10. Спектр амплітуд послідовності трикутних відео імпульсів

При однаковій шпаруватості кількість гармонік, що містяться в пелюстці спектра амплітуд періодичної послідовності трикутних сигналів, удвічі більше відповідної кількості гармонік періодичної послідовності прямокутних сигналів.

Гаусівський відеоімпульс

Гаусівський сигнал описується аналітичним виразом:

$$s(t) = U \cdot e^{-\frac{t^2}{2\tau^2}},\ -\infty < t < \infty. \qquad (5.14)$$

Цей імпульс (див.рис.5.11) збігається за формою з графіком нормального (гаусівського) закону розподілу ймовірності.

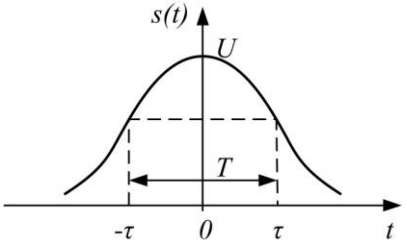


Рис.5.11. Зображення форми гаусівського відео імпульсу

Параметр τ у формулі (5.14) має значення половини тривалості імпульсу, що визначається на рівні $e^{-1/2}$ від амплітуди імпульсу, тобто повна тривалість гаусівського імпульсу згідно рис.5.11 дорівнює 2τ.

Перетворення Фур'є такого імпульсу у загальній формі має наступний вигляд:

$$S(\omega) = U \int_{-\infty}^{\infty} e^{-\frac{t^2}{2\tau^2}} \cdot e^{-j\omega t} dt = U \int_{-\infty}^{\infty} e^{-(\frac{t^2}{2\tau^2} + j\omega t)} dt.$$

Після математичних перетворень та інтегрування вищенаведеного виразу будемо мати наступний вираз для спектральної щільності спектру гаусівського відео імпульсу:

$$S(\omega) = U\tau\sqrt{\frac{2}{\pi}} \cdot e^{-\frac{(\omega\tau)^2}{2}}. \qquad (5.15)$$

Із зіставлення формул (5.14) і (5.15) випливає, що гаусівський імпульс і його спектр відображаються однаковими функціями і мають властивість симетрії. Підкреслимо, що гаусівський сигнал – це єдиний сигнал, для якого форми його часової функції і спектральної щільності є однаковими.

Однобічний експоненціальний відеоімпульс

Розглянемо сигнал (форма якого представлена на рис.5.12,а), що описується наступною формулою:

$$s(t) = U \cdot e^{-\alpha \cdot t},\ t \geq 0.$$

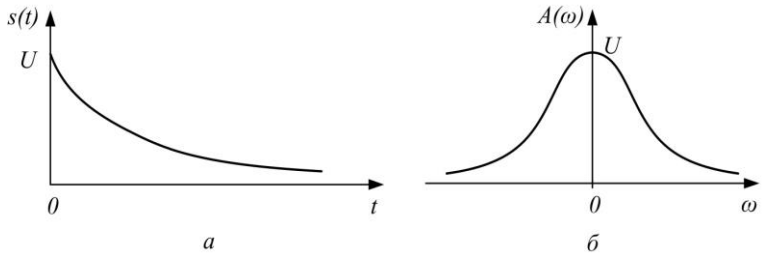
Такий сигнал лише умовно можна назвати імпульсом через його нескінченність при $t \to \infty$.

Спектральна щільність такого імпульсу є комплексною функцією виду

$$\dot{S}(\omega) = \frac{U}{\alpha + j\omega}.$$

Амплітудний спектр є модулем спектральної щільності:

$$A(\omega) = \frac{U}{\sqrt{\alpha^2 + \omega^2}}.$$



а *б*

Рис.5.11. Однобічний експоненціальний імпульс (*а*) і його амплітудний спектр (*б*)

Двобічний експоненціальний відео імпульс

Математична модель двобічного експоненціального імпульсу має наступний вигляд:

$$s(t) = U \cdot e^{-\alpha \cdot |t|},\ t \in (-\infty; \infty).$$

Форма цього імпульсу показана на рис.5.12.

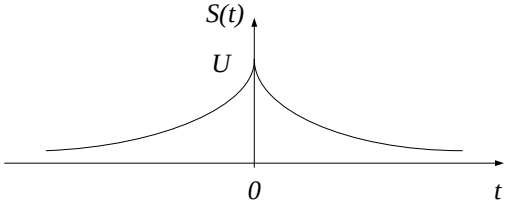


Рис.5.12. Зображення форми двобічного експоненціального імпульсу

Спектральна щільність двобічного експоненціального імпульсу є дійсною функцією (оскільки функція є парною) і дорівнює його амплітудному спектру:

$$A(\omega) = S(\omega) = \frac{2\alpha U}{\alpha^2 + \omega^2}.$$

Форма спектра двобічного експоненціального імпульсу така ж, як і в однобічного, з точністю до масштабного коефіцієнту.

Дельта-функція

Дельта-функція або функція Дірака, або одиничний імпульс $\delta(t)$ можна визначити наступним чином:

$$\delta(t) = \begin{cases} \infty, & t = 0, \\ 0, & t \neq 0, \end{cases}$$

причому такий імпульс має одиничну площу, тобто:

$$\int_{-\infty}^{\infty} \delta(t)dt = 1.$$

Застосовуючи пряме перетворення Фур'є до сигналу $\delta(t)$, маємо

$$\dot{S}(\omega) = \int_{-\infty}^{\infty} \delta(t) \cdot e^{-j\omega t} dt = 1, \ -\infty < \omega < \infty .$$

Отже, спектральна щільність дельта-функції є дійсною функцією і дорівнює одиниці для всіх частот, тобто

$$S(\omega) = 1, \ -\infty < \omega < \infty .$$

Таким чином, спектр одиничного імпульсу $\delta(t)$ має щільність, що дорівнює одиниці на всій нескінченній осі частот, тобто внески всіх спектральних складових дельта-функції підсумовуються в момент $t=0$, утворюючи нескінченно великий пік, а в момент $t \neq 0$, внески цих самих складових взаємно компенсуються.

Незмінний у часі сигнал

Математичну модель незмінного в часі сигналу можна записати у вигляді

$$s(t) = U_0, \ -\infty < t < \infty . \qquad (5.16)$$

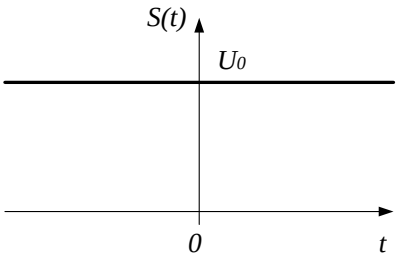


Рис.5.13. Форма незмінного у часі сигналу

Спектральна щільність незмінного у часі сигналу не обчислюється за класичною формулою прямого перетворення Фур'є, оскільки інтеграл

$$\int_{-\infty}^{\infty} U_0 \cdot e^{-j\omega t} dt$$

не є невизначеним. Тому сигнал (5.16) зручно зобразити за допомогою оберненого перетворення Фур'є:

$$U_0 = \frac{1}{2\pi}\int_{-\infty}^{\infty} \dot{S}(\omega)\cdot e^{j\omega t} d\omega .$$

Використовуючи фільтрувальні властивості дельта-функції

$$\dot{S}(\omega) = 2\pi \cdot U_0 \cdot \delta(\omega)$$

можна встановити наступну відповідність:

$$U_0 \leftrightarrow 2\pi \cdot U_0 \cdot \delta(\omega) .$$

Фізичний зміст отриманого результату: незмінний у часі сигнал має спектральну компоненту тільки на нульовій частоті, тобто містить тільки нульову гармоніку.

Східчастий сигнал

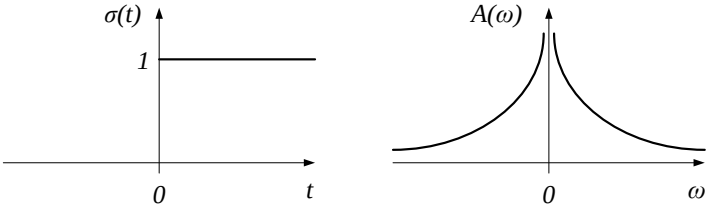
Математична модель східчастого сигналу (рис.5.14, *а*), який іноді називають функцією включення, є наступною:

$$\sigma(t) = \begin{cases} 1, & t \geq 0, \\ 0, & t < 0, \end{cases}$$

Спектральний аналіз даного сигналу досить складний, однак після ряду відповідних перетворень остаточний вираз для амплітудного спектру цього сигналу буде мати наступний вигляд:

$$\mathrm{A}(\omega) = \begin{cases} \infty, & \omega = 0, \\ 1/|\omega|, & \omega \neq 0, \end{cases}$$

Амплітудний спектр східчастого сигналу зображено на рис.5.14.



а *б*

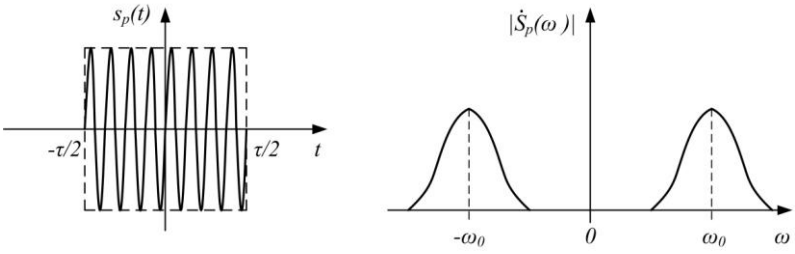
Рис.5.14. Східчастий сигнал (*а*) і його амплітудний спектр (*б*)

Аналізуючи функцію включення, можна зробити висновок, що амплітуда її спектру прагне до нескінченності при наближенні до точки ω=0, а при віддалені від неї спадає за гіперболічним законом.

Радіоімпульс

Радіоімпульс (рис.5.15,*а*) у математичному вигляді задається добутком деякого відео імпульсу, що відіграє роль обвідної, і деякого гармонічного коливання:

$$s_p(\mathrm{t}) = s_в \cdot \cos\omega_0 t\,.$$



а *б*

Рис.5.15. Зображення форми радіоімпульсу (*а*) та його спектру (*б*)

Для знаходження спектральної щільності радіоімпульсу вважатимемо відомою функцію $\dot{S}_в(\omega)$ – спектральну щільність обвідної радіоімпульсу.

Спектр косинусоїдального коливання визначається за формулою:

$$\cos\omega_0 t \leftrightarrow \pi[\delta(\omega-\omega_0)+\delta(\omega+\omega_0)].$$

Спектр радіоімпульсу з точністю до множника 1/2π є згорткою спектрів двох сигналів: відео імпульсу і гармонічного коливання, тобто з урахуванням фільтрувальних властивостей дельта-функції будемо мати:

$$\dot{S}_p(\omega) = \frac{1}{2}\dot{S}_в(\omega-\omega_0) + \frac{1}{2}\dot{S}_в(\omega+\omega_0)\,.$$

Отже, перехід від відео до радіоімпульсу в спектральному відображенні означає перенесення спектра відео імпульсу в область високих частот: замість єдиного максимуму спектральної щільності відео імпульсу при $\omega=0$ спостерігається два максимуми на частотах $\pm\omega_0$.

Амплітудно-модульований сигнал

Модуляція – процес зміни одного або декількох параметрів високочастотного модульованого коливання відповідно до закону зміни низькочастотного інформаційного сигналу.

Амплітудна модуляція (АМ) – процес зміни амплітуди високочастотного (несучого) сигналу за законом низькочастотного (інформаційного).

Математично АМ-сигнал записується як

$$U_{AM}(t) = U_m\left[1 + m \cdot F(t)\right]\sin(\omega_0 t + \varphi_0) \qquad (5.17)$$

де U_m – амплітуда несучого сигналу, $F(t)$–функція, що здійснює модулювання, m–коефіцієнт модуляції, ω_0 – частота несучого сигналу, φ_0– фаза несучого сигналу.

Коефіцієнт модуляції характеризує ступінь впливу інформаційного сигналу на несучу і лежить у межах $0<m<1$.

Розглянемо простий випадок – синусоїдної модуляції (рис.5.16), тобто коли

$$F(t) = \sin\Omega t \,. \qquad (5.18)$$

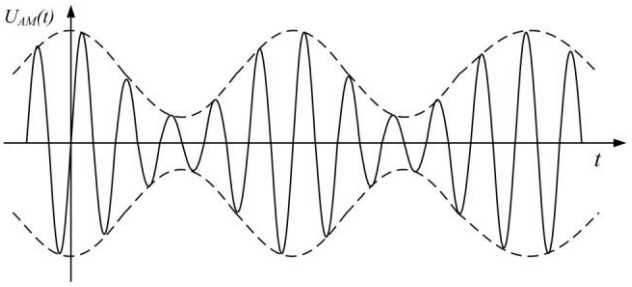


Рис.5.16. Вигляд амплітудно-модульованого сигналу

Підставивши рівняння (5.18) в (5.17) і розкривши дужки, отримаємо:

$$U_{AM}(t) = U_m[\sin(\omega_0 t + \varphi_0) + m \cdot \sin(\omega_0 t + \varphi_0)\sin\Omega t] =$$
$$= U_m \sin(\omega_0 t + \varphi_0) + \frac{U_m \cdot m}{2}\cos[(\omega_0 - \Omega)t + \varphi_0] -$$
$$- \frac{U_m \cdot m}{2}\cos[(\omega_0 t + \Omega)t + \varphi_0]$$

Отже, коливання, яке модульоване синусоїдним сигналом, має дискретний спектр, що складається з трьох спектральних ліній (рис.5.17). Додаткові частоти, що винили внаслідок модуляції ω_0-Ω і ω_0+Ω називають бічними.

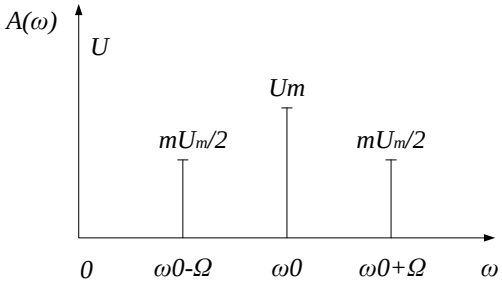


Рис.5.17. Спектр АМ сигналу

Слід додати, що при модуляції більш складними сигналами, замість спектральних ліній на бокових частотах, містяться бокові смуги, що відображають спектральний склад корисного сигналу. Також слід пам'ятати, що існує велика множина різних підвидів амплітудної модуляції (односмугова, балансна та ін.).

Частотно-модульований сигнал

Частотна модуляція – це процес, коли частота несучого коливання змінюється за законом корисного сигналу. Припустимо, що частота модулюється за косинусоїдальним законом (див. рис.5.18):

$$\omega(t) = \omega_0 + \Delta\omega \cdot \cos\Omega t = \omega_0 (1 + \frac{\Delta\omega}{\omega_0} \cos\Omega t)$$

,

де $\Delta\omega$ – відхилення частоти несучого коливання, $\Delta\omega/\omega_0$ – відносне змінювання частоти, тобто глибина модуляції частоти.

Колова частота є похідною за часом від аргументу тригонометричної функції, що описує коливання. Тому вираз для частотно-модульованого (ЧМ) коливання за синусоїдним законом записується наступним чином:

$$U_{чм}(t) = U_m \sin\left[\int_0^t \omega(t)dt\right] = U_m \sin\left[\omega_0 t + \frac{\Delta\omega}{\Omega}\sin\Omega t\right] =$$

$$= U_m \left[\sin\omega_0 t \cos(\beta \sin\Omega t) + \cos\omega_0 t \sin(\beta \sin\Omega t)\right]$$

,

де $\beta=\Delta\omega/\Omega$ – індекс модуляції.

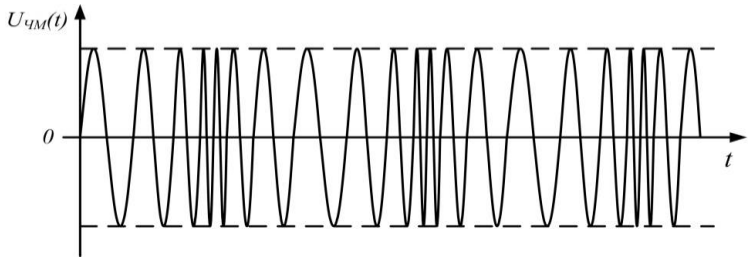


Рис.5.18. Вигляд частотно-модульованого сигналу

Розглянемо ЧМ з малим індексом ($\beta<<1$). Знаючи, що косинус та синус малого аргументу можна замінити відповідно на одиницю та самий аргумент, отримаємо:

$$U_{чм}(t) = U_m \left[\sin\omega_0 t + \beta \sin\Omega t \cos\omega_0 t\right],$$

тобто маємо вираз, що принципово не відрізняється від виразу для АМ-коливання.

Тому спектр ЧМ-коливання за синусоїдної модуляції з малим

індексом, так само як і спектр АМ-коливання, складається з несучої та двох бокових частот.

За довільного значення β, застосовуючи відомі формули теорії бесселевих функцій, одержуємо:

$$U_{чм}(t) = U_m \left\{ J_0(\beta) \sin \omega_0 t + \sum_{k=1}^{\infty} J_k(\beta) \left[\sin(\omega_0 + k\Omega t) + (-1)^k \sin(\omega_0 t + k\Omega) t \right] \right\},$$

де $J_k(\cdot)$– функція Бесселя першого роду k-го порядку.

Отже, маємо коливання з лінійчатим спектром. На відміну від АМ тут за синусоїдної модуляції виникає безмежний спектр. Проте на практиці він є обмеженим, оскільки амплітуди гармонік пропорційні $J_k(\beta)$, а ці функції характеризуються тим, що набувають дуже малих значень при високих значеннях порядку k.

Отже, спектр ЧМ-сигналу при великих індексах модуляції значно ширший, ніж спектр АМ-сигналу.

Фазо-модульований сигнал

У цьому випадку фаза сигналу несучої частоти змінюється за законом інформаційного сигналу, а сам ФМ сигнал записується як:

$$U_{фм}(t) = U_m \sin[\omega_0 t + \varphi_0 + \Delta\varphi s(t)],$$

де $\Delta\varphi$ – девіація фази сигналу несучої частоти; $s(t)$ –інформаційний сигнал.

По суті ФМ і ЧМ утворюють сигнали одного виду. Відмінність полягає лише в тому, що у разі ФМ в аргумент синусоїдної функції входить сам інформаційний сигнал,а в разі ЧМ – його інтеграл. У разі синусоїдної модуляції розбіжність у формі модульованих коливань та їхніх спектрів узагалі помітити неможливо, оскільки інтеграл від синусоїди є косинусоїда, тобто знову ж таки синусоїда, але зсунута за фазою на $\pi/2$.

Методи представлення дискретних сигналів у вигляді спеціальних діаграм.

Основне розповсюдження отримали два класи спеціальних діаграм:

1) діаграми представлення фізичних параметрів послідовностей

дискретних сигналів, до котрих відносяться окові діаграми та діаграми стану;

2) алгоритмічні діаграми представлення послідовностей дискретних сигналів, до котрих відносяться деревоподібні діаграми та різноманітні види діаграм Треліса.

Діаграми представлення фізичних параметрів послідовностей дискретних сигналів використовуються для аналізу послідовностей як простих бінарних цифрових сигналів, так і складних модульованих сигналів, що знайшли застосування у радіотехнічних системах передачі і системах радіозв'язку.

5.7 Окові діаграми

5.7.1. Сутність методу окових діаграм

Основна перевага методу представлення послідовностей дискретних сигналів у вигляді так званих окових діаграм – це наглядність представлення результатів аналіза сигналів на екрані осцилографа та простота реалізації, оскільки для представлення досліджуваних послідовностей сигналів потрібен лише осцилограф. Виявилось: якщо подавати досліджувані послідовності дискретних сигналів (з кінцевим та, бажано, не вельми великим числом розрізнюваних станів цих сигналів) на вхід осцилографа, то на екрані осцилографа можливо спостерігати сталі характерні „картинки", котрі візуально демонструють характер та величину спотворень досліджуваних сигналів (або, навпаки, засвідчують, що вони були сформовані та передані через канал без спотворень). Однак при цьому необхідно коректно здійснювати синхронізацію досліджуваних послідовностей сигналів з періодом розгортки осцилографа (тобто, правильно обирати синхронізуючі послідовності сигналів, котрі подаються на вхід зовнішньої розгортки осцилографа). У даному випадку мова йде про дослідження послідовностей сигналів (не обов'язково періодичних, але обов'язково дискретних, з кінцевим числом станів), оскільки, як правило, одиничний сигнал на екрані осцилографа практично неможливо побачити. Простіше за усе за допомогою осцилографа досліджувати періодичні сигнали, наприклад синусоїду або періодичну послідовність однакових за формою відеоімпульсів,

коли існує можливість „засинхронізувати” період досліджуваних сигналів з періодом розгортки осцилографа. Проте послідовності однакових за формою сигналів не переносять інформацію користувачів систем зв’язку. Тому періодичні „однакові” сигнали у системах зв’язку мають вузьке коло застосувань, головним чином для технологічних цілей – синхронізації, тестування або налагодження елементів обладнання.

За допомогою окових діаграм можливо здійснювати дослідження: як періодичних, так і не періодичних послідовностей дискретних сигналів; як однакових, так і не однакових (але відносно близьких за формою) сигналів. Головне, щоб кількість можливих станів елементарних сигналів, що входять до складу досліджуваних послідовностей і подаються на вхід осцилографа, була кінцевою та однаковою для усіх сигналів. Важливо також, щоб тривалість елементарних сигналів була кратною періоду розгортки осцилографа. Інакше не отримаєш сталу „картинку” на осцилографі. Слід звернути увагу: якщо форма елементарних сигналів, що складають періодичні послідовності, змінюється у часі у певних розумних межах (можливо, випадковим чином), то це візуально на екрані сприймається як спотворення сигналів. Чим більше змінюється форма сигналів на екрані, тим вище рівень спотворень.

Розглянемо простий випадок застосування окової діаграми, коли на вхід осцилографа подається потік двійкових сигналів, що розбитий на тріади. Потрібно за допомогою окової діаграми на екрані осцилографа оцінити вигляд усіх можливих бітових тріад сигналів, тобто вигляд тріади „000”, потім вигляд тріади „001”, потім „010” і т.д. аж до останньої тріади „111”. При цьому оцінювання вигляду тріад необхідно здійснювати для двох можливих випадків: перший випадок – коли тріади просуваються через канал зв’язку за умов відсутності спотворень (це ідеальний випадок, котрий фактично ілюструє вигляд сигналів на виході джерела двійкового потоку сигналів ще до моменту їхнього проходження через канал); другий випадок – коли канал зв’язку спотворює форму сигналів тріади, що проходять через нього (це реальний випадок, котрий ілюструє вигляд реальних сигналів на виході канала зв’язку). Блок-схема вимірювальної установки, що

дозволяє побачити окові діаграми тріад для вищеназваних випадків, показана на рис.5.19.

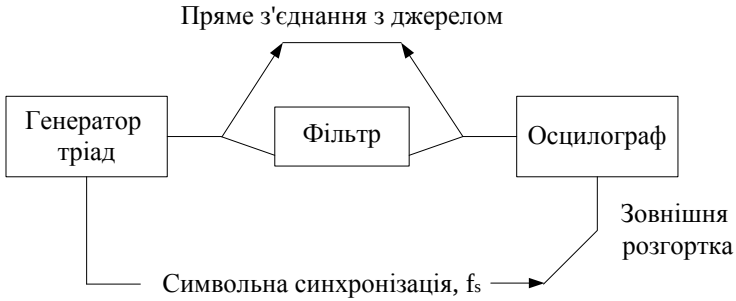


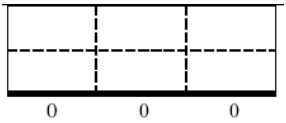
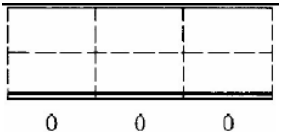
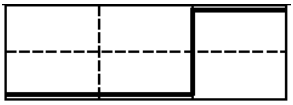
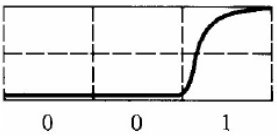
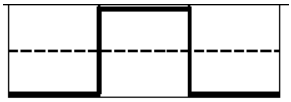
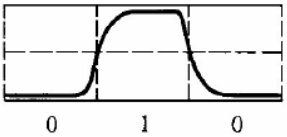
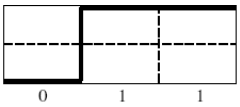
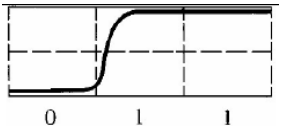
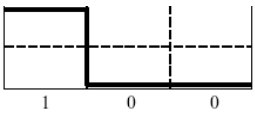
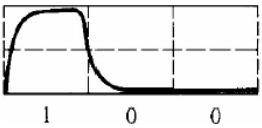
Рис.5.19. Блок-схема вимірювальної установки для отримання окових діаграм регулярних бітових тріад виду 000, 001, ……, 011, 111

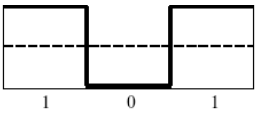
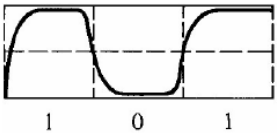
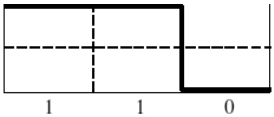
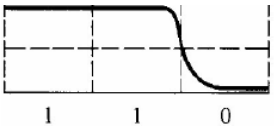
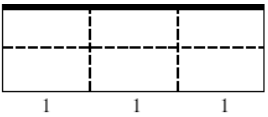
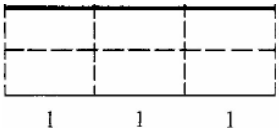
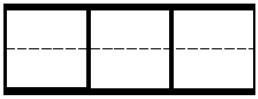
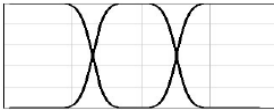
Відповідно до рис.5.19 регулярні періодичні послідовності, що формуються генератором тріад, подаються на вхід осцилографа або напряму (моделюється ідеальний випадок передавання тріад без спотворень), або через смуговий фільтр (котрий моделює спотворюючий вплив реального каналу, оскільки спектри сигналів, що проходять через фільтр, не „влізають” у смугу пропускання фільтру). Тріади в осцилографі потрібно коректно засинхронізувати. Наприклад так, щоб на екрані поміщалася лише одна тріада. Тоді частота синхропослідовності, що подається на зовнішню розгортку осцилографа, має бути утроє менше за частоту бітового потоку. Тріада бітів являє собою певний символ, що визначається у десятковій системі від 0 до 7. Тому ланцюг синхронізації осцилографа на схемі рис.5.19 називається ланцюгом символьної синхронізації.

Окові діаграми тріад, що сформовані генератором і подаються у вигляді бітового потоку сигналів, показані у табл.5.5. Показано приклад формування окової діаграми безпосередньо на виході джерела тріад та на виході смугового фільтра, що моделює фізичний канал зв’язку.

Таблиця 5.5

Окові діаграми тріад, що складені із двійкових сигналів

Бітова послідовність елементарних сигналів, що розбита на тріади		
Двійковий код тріади	Окова діаграма тріади безпосередньо на виході генератора тріад	Окова діаграма тріади на виході смугового фільтра
000		
001		
010		
011		
100		

101		
110		
111		
Супер-позиція		

Якщо на рис.5.19 замість генератора детермінованих послідовностей тріад використати генератор псевдовипадкових бітових послідовностей (ГПВП), то на вхід осцилографа будуть надходити випадковим чином різноманітні комбінації тріад та „картинка” ускладниться (вона буде виглядати так, як це показано в останньому рядку табл.5.5 з назвою „суперпозиція”). Тобто, у цьому випадку реальна осцилограма бітового потоку „розрізається” посимвольно у відповідності із тактовими імпульсами синхронізуючого генератора, а потім окова діаграма „складається” із отриманих шматків. Як результат такого складання в ідеальному випадку без фільтру сформується квадрат („квадратне око”). У той час як окова діаграма тріад на виході смугового фільтра буде суттєво відрізнятися від квадрата, оскільки буде містити складові зростання фронту сигнала та спадання його фронту. Прямокутний

імпульс буде мати форму колоколу. Як результат, сформується діаграма більш схожа на око.

Таким чином, окова діаграма являє собою результат багатократного накладання одна на одну бітових послідовностей, що надходять від генератора ПВП і відображаються на екрані осцилографа у вигляді діаграми розподілу амплітуди сигналу у часі. По формі „ока" можливо робити висновки щодо ступеню зростання або спадання фронтів елементарних сигналів, що складають тріаду, і, отже, можливо робити висновки щодо ступеню негативного впливу характеристик каналу на якість проходження сигналів через канал.

Дослідження око-діаграм дозволяє провести детальний аналіз послідовностей дискретних сигналів за параметрами, що безпосередньо пов'язані із формою хвилевого фронту: параметром міжсимвольної інтерференції, джитером передавання даних, джитером синхронізації і т.ін.

Розглянемо параметри окової діаграми, по величині котрих можливо оцінювати на кількісному рівні ступень спотворення дискретних сигналів, що подаються на вхід осцилографа. Припустимо, на вхід осцилографа подається бітовий потік реальних відеоімпульсів, де логічному „0" відповідає негативний відеоімпульс з амплітудою E0, а логічній „1" – позитивний відеоімпульс з амплітудою E1. Окова діаграма такого потоку відеоімпульсів показана на рис.5.20. Як бачимо, через спотворення у каналі реальні відеоімпульси не будуть мати строго прямокутну форму: фронти відеоімпульсів будуть задовжені, самі імпульси будуть розповзатися або звужуватися або навіть „тремтіти" у часі, з'являться коливальні складові і т.ін. Ефекти розширення імпульсу, а також фазове тремтіння сигналу викликають появу взаємних спотворень між символами, що призводить до перетину око-діаграми із часовою віссю у різні проміжки часу. На око-діаграмі рис.5.20 показані її основні параметри (згідно даних книги И.Г.Бакланова «Методы измерений в системах связи»).

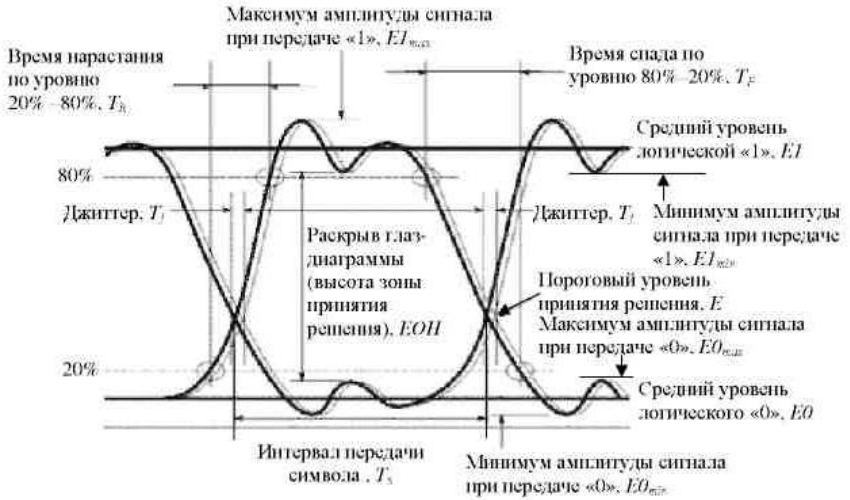


Рис.5.20. Ідентифікація параметрів око-діаграми

До цих параметрів відноситься, перш за все, розкрив око-діаграми *E0H*, від котрого залежить поріг прийняття рішення *E* в задачах розрізнення сигналів. Важливе значення має час зростання, а також і час спадання сигналів за певним рівнем, що характеризує ступінь лінійних спотворень у каналі.

Максимальна ширина області перетину із часовою віссю визначається як пікове фазове тремтіння або джитер передачі даних *Tj*. Джитер вимірюється зазвичай в одиницях часу або як відношення до інтервалу передачі символу *Tj/Ts*.

За допомогою окових діаграм можливо представити не тільки послідовності двійкових сигналів, але і багаторівневих сигналів, що важливо під час досліджень процесів лінійного кодування у цифрових каналах типу DSL або ISDN, котрі розглядаються у наступних лекціях.

У випадку побудови багаторівневих діаграм блок-схема вимірювальної установки (див.рис.5.21) має включати до свого складу, поряд з іншим, ще і багаторівневий конвертор, що моделює процес лінійного кодування відповідно до досліджуваного багаторівневого коду (наприклад, HDB3, 2B1Q і т.ін.).

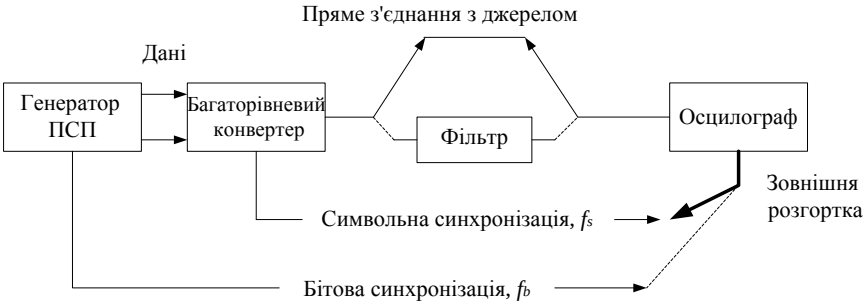


Рис.5.21. Блок-схема вимірювальної установки для отримання окових діаграм багаторівневих сигналів

Сигнал із виходу двійкового генератора ПВП має проходити через багаторівневий конвертор, а синхронізація здійснюватися від символьного потоку з частотою f_s. Під час калібрування окової діаграми сигнал зазвичай подають в обхід смугового фільтра, що обмежує спектр сигналу. Фільтр, що обмежує смугу сигналу, вносить суттєві зміни у форму імпульсу, у результаті чого отримується діаграма у вигляді „стандартного ока”.

Як вже зазначалось, окові діаграми використовують періодичну структуру дискретних сигналів. За рахунок підбору періоду сигнала зовнішньої синхронізації розгортки осцилографу, отримувані осцилограми „шматків” сигнальних послідовностей, що дорівнюють періоду спостерігаємої послідовності, накладаються один на одний. Як результат на екрані осцилографа ми бачимо окову діаграму, при цьому на вісі ординат відкладається амплітуда сигнальних послідовностей, а на вісі абсцис – час, відповідно.

Дослідження окових діаграм дозволяє провести детальний аналіз сигналів як за амплітудними, так і за часовими параметрами око-діаграм.

5.7.2. Вимірювання амплітудних параметрів око-діаграми

Досліджуваний сигнал, у той чи іншій мірі, характеризують наступні амплітудні параметри око-діаграми:

- оковий рівень;
- амплітуда ока;
- рівень окового перетину;

- висота ока;
- окове відношення сигнал-шум;
- добротність ока.

Для визначення будь-якого із вищеперерахованих параметрів розглядають окову діаграму уздовж вертикалі.

Оковий рівень (*Eye Level*). Оковий рівень – це певний амплітудний рівень вертикальної шкали відображення сигналу на оковій діаграмі, що розглядається з тією чи іншою метою у даний момент часу. Вимірюється в одиницях амплітуди (AU). Сигнали на оковій діаграмі відображаються у вигляді ліній. Але слово «лінія відображення сигналу» не слід розуміти буквально. З цього приводу слід зазначити наступне. На певних окових рівнях спостерігаються відповідні лінії, що візуально відображають структуру досліджуваних послідовностей дискретних сигналів. Через спотворення сигналів, як правило, лінії, що спостерігаються на око-діаграмах, представляються „розмазаними" (розмитими). Ступінь розмитості лінії по вертикалі характеризується параметром σ, що називається дисперсією розкиду амплітуди досліджуваних сигналів. На практиці застосовують трьохкратне значення 3σ, що називається стандартна девіація, тобто вважають, що краї розмитої лінії по вертикалі знаходяться на відстані 3σ від середньої величини функції розподілу амплітуд PDF (probability distribution function: функція розподілу ймовірностей) цієї лінії.

Аналіз особливостей представлення окових рівнів має враховувати „розмазаність" цих рівнів як за вертикальною, так і за горизонтальною вісями. Якщо спостерігати окову діаграму по горизонталі (тобто, уздовж вісі часу), то окові рівні теж слід визначати не для якогось одного моменту часу, а розглядати їх протягом певного часового інтервалу розмитості лінії. Наприклад, на рис.5.22 інтервал спостереження розмитості окових рівнів обмежується вікном, утвореним двома вертикальними лініями в районі часового моменту $10x10^{-3}$ с. Відстань по горизонталі між цими вертикальними лініями - це є інтервал розмитості лінії відображення сигналу по горизонталі.

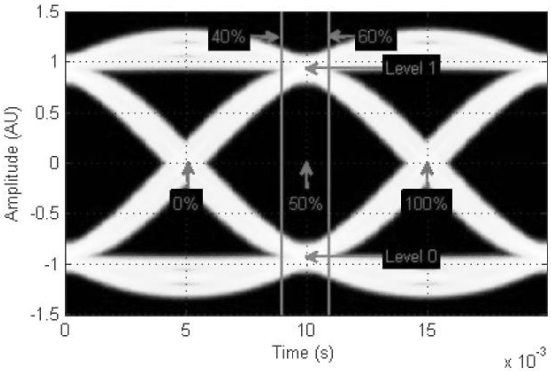


Рис. 5.22. Вікно, у рамках котрого аналізуються окові рівні

На цьому інтервалі спостереження для ідеального NRZ-сигнала, що відображений на рис.5.22, існує два окових рівня: +1AU та -1AU. Розмазаність окових рівнів по вертикалі характеризується за допомогою вертикальних гистограм розподілу їхніх амплітуд. Зокрема, для окових рівнів NRZ-сигнала (тобто, для рівнів +AU та –AU) вертикальна гистограма розподілу амплітуд показана на рис.5.23.

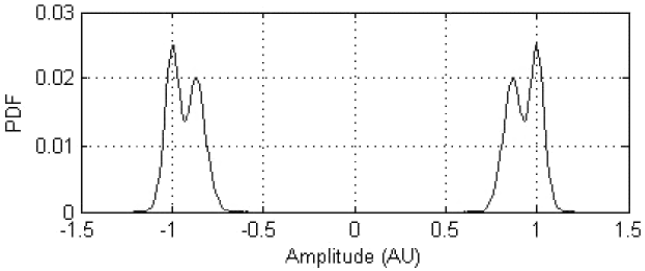


Рис. 5.23. Вертикальна гістограма розподілу амплітуд окових рівнів

Ця гистограма будується наступним чином. Ширина вікна (див.рис.5.22) розбивається на десять більш дрібних часових інтервалів. На краях цих дрібних інтервалів визначаються індивідуальні вертикальні гистограми розподілу амплітуд окових рівнів. Потім ці індивідуальні гистограми усереднюються в межах окових рівнів. Так що, на рис.5.23 показано усереднений розподіл окових рівнів NRZ-сигнала.

Амплітуда ока (*Eye Amplitude*). Амплітуда ока може визначатися у будь-яких зручних для вимірювань одиницях (так званих амплітудних одиницях, *Amplitude Unit, AU*) і являє собою відстань по вертикалі між двома сусідніми оковими рівнями (див.рис.5.24).

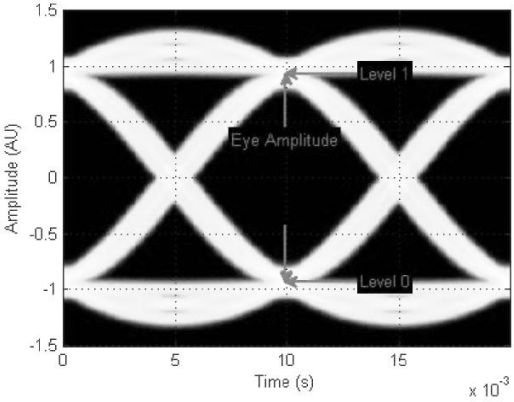


Рис. 5.24. Визначення величини амплітуди ока

Наприклад, для NRZ-сигналу існує лише два рівня: високий рівень (рівень 1, на рис.5.24 він дорівнює 1AU) та низький рівень (рівень 0, на рис.5.24 він дорівнює мінус 1 AU). Окові рівні на око-діаграмі рис.5.24 виглядають „розмазаними". Тому потрібно умовитися, як саме визначати відстань між оковими рівнями. Якщо для визначення окового рівня брати приблизно середнє значення розмазаної лінії, то амплітуда ока на рис.5.24 – це різниця між середніми значеннями сусідніх окових рівнів, тобто 1 – (-1) = 2 AU.

Рівень окового перетину (*Eye Crossing Level, ECL*). Рівень окового перетину – це рівень амплітуди на оковій діаграмі, на котрому виник перетин досліджуваної частини лінії відображення сигналу з певним чином визначеним оковим рівнем. Вимірюється в одиницях амплітуди (AU). На рис.5.25 показано два часові моменти окового перетину – A1 (в момент $5x10^{-3}$ сек) та A2 (в момент $15x10^{-3}$ сек).

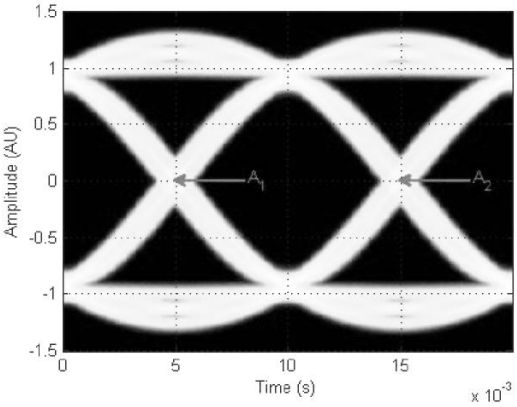


Рис. 5.25. Визначення рівнів окового перетину для двох моментів A_1 та A_2

Як бачимо, лінії, що утворюють окові перетини, також „розмазані". Для моменту A_1 на рис 5.25 маємо три рівні окового перетину – верхній рівень (середнє значення цього рівню – трохи більше за плюс 1AU), середній рівень (середнє значення цього рівню дорівнює 0AU), нижній рівень (середнє значення цього рівню – трохи менше за мінус 1AU). В якості значення ECL на будь-якому рівні окового перетину використовують середнє амплітудне значення цього рівню.

Для обчислень меж окового перетину на будь-якому із рівнів зручно користуватися вертикальною гистограмою розподілу амплітуд для конкретно визначеного часового моменту цього окового перетину. Зокрема, на рис.5.26 показана вертикальна гистограма розподілу амплітуд PDF (probability distribution function: функція розподілу ймовірностей) у момент A_1.

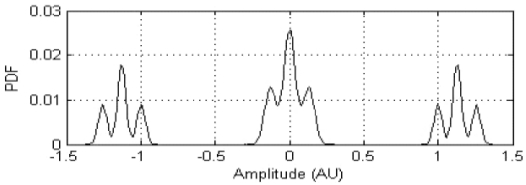


Рис. 5.26. Вертикальна гистограма розподілу амплітуд у момент A_1

Як бачимо, ECL верхнього рівню дорівнює плюс 1,15 AU, ECL середнього рівню дорівнює 0 AU, а ECL нижнього рівню дорівнює мінус 0,85 AU.

Окова висота (*Eye Height*). Замість параметра „Амплітуда ока" іноді вимірюють параметр „Окова висота", що враховує при визначенні відстані між сусідніми ковими рівнями ступінь розмитості ліній (див.рис.5.27).

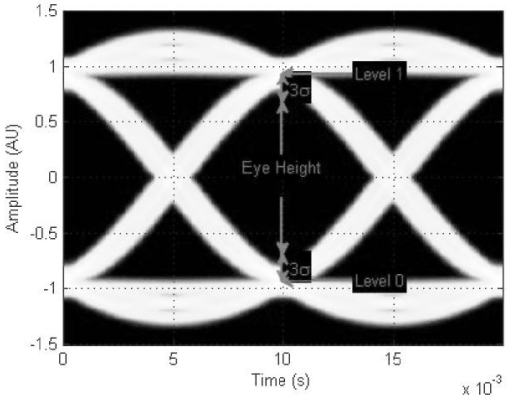


Рис. 5.27. Визначення окової висоти

Окова висота вимірюється в одиницях амплітуди (AU) і визначається як відстань між стандартними краями двох сусідніх окових рівнів, тобто краях, що віддалені від середини рівнів на відстань 3σ. Для NRZ-сигнала існує лише два рівня: високий рівень (рівень 1AU на рис.5.27) та низький рівень (рівень мінус 1AU на рис.5.27). Окова висота – це відстань між найближчими двома точками країв сусідніх окових рівнів, де краї віддалені від середини розмитих ліній на відстані 3σ (так, як це показано на рис.5.27).

Окове відношення сигнал/шум (*Eye SNR*). *Окове відношення сигнал/шум* визначається як відношення окової амплітуди до суми стандартних девіацій двох окових рівнів:

$$SNR = \frac{L_1 - L_0}{\sigma_1 - \sigma_0},$$

де L_1 та L_0 - це окові рівні - відповідно 1 и 0, а σ_1 и σ_0 – стандартні девіації окових рівнів - 1 та 0 відповідно. Для NRZ-сигнала оковий рівень 1 відповідає високому рівню, а оковий рівень 0 відповідає низькому рівню.

Добротність ока (*Quality Factor*). *Добротність* визначається таким же чином, що і окове відношення сигнал/шум. Проте використовується інше визначення девіації. А саме, добротність ока обчислюється за формулою:

$$\text{Q factor} = \frac{\text{P}_{\text{top}} - \text{P}_{\text{base}}}{\text{sigmatop} + \text{sigmabase}} \cdot 100\%,$$

де P_{top} – середній рівень максимального піка гистограми, побудованої для високого логічного рівня;

P_{base} – середній рівень максимального піка гистограми, побудованої для низького логічного рівня;

sigmatop – стандартна девіація відносно середньої величини високого логічного рівня;

sigmabase – стандартна девіація відносно середньої величини низького логічного рівня.

5.7.3. Вимірювання часових параметрів сигнальних послідовностей

Сигнали можуть досліджуватися не тільки за амплітудними характеристиками (по вертикалі око-діаграми), але і за часовими характеристиками (по горизонталі око-діаграми). Досліджуваний сигнал, у той чи іншій мірі, характеризують наступні часові параметри око-діаграми:

- повний джитер;
- детермінований джитер;
- випадковий джитер;
- середньоквадратичний джитер;
- момент та тривалість окового перетину (по горизонталі);
- окова затримка;
- тривалість окового затухання;

- тривалість окового зростання;
- ширина ока.

Для визначення будь-якого із вищеперерахованих часових параметрів слід розглядати окову діаграму по горизонталі.

Одною із основних характеристик сигналів, що досліджуються за допомогою горизонтальних розрізів око-діаграм вважається так званий джитер.

Джитер - це процес коливального відхилення уздовж часової вісі рівня сигналу від певним чином визначеного моменту часу, котрий, виходячи із тих чи інших міркувань, вважається нормальним (ідеальним). Підкреслимо, що у даному випадку розглядається коливальний рух деякого параметра сигналу (наприклад, його фази) не за амплітудою, а уздовж часової вісі. Процес коливання асоціюється із словом «тремтіння». (Це слово у перекладі на англійську звучить як джитер). Передбачається, що так званий повний джитер можливо розкласти на дві компоненти – детермінований джитер (DJ), котрий характеризує регулярну складову повного джитеру, та випадковий джитер (RJ). Найзручніше повний джитер та його компоненти характеризувати за допомогою функції розподілу ймовірностей (PDF, probability distribution function), що розглядається уздовж часової (горизонтальної) вісі окової діаграми. Функції розподілу детермінованого, випадкового та повного джитеру показані на рис.5.28. Зокрема, PDF детермінованої компоненти джитеру являє собою дві дельта-функції, що представлені на верхньому рисунку у вигляді двох ліній (μ_L та μ_R), що проходять через часові моменти мінус 10 та плюс 10. Амплітуди цих ліній можуть бути різними. PDF випадкової компоненти джитеру на середньому рисунку являє собою гаусівську функцію розподілу із нульовим середнім та певною дисперсією розкиду σ. На кінець, PDF повного джитеру *(TJ)* – це згортка двох вищезазначених PDF, що складається із двох гаусівських кривих із дисперсіями σ та середніми значеннями мінус 10 та плюс 10 (μ_L та μ_R).

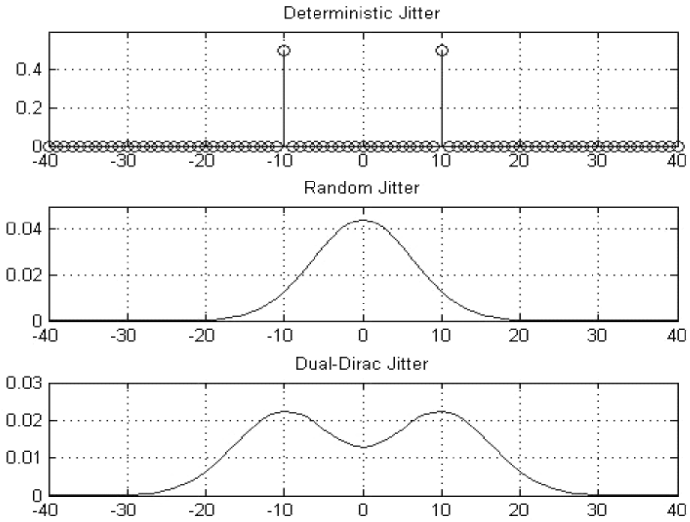


Рис.5.28. Представлення функцій розподілу детермінованого, випадкового та повного джитеру

Детермінований джитер (*Deterministic Jitter, DJ*). *Детермінований джитер* – це величина детермінованої складової коливального процесу відхилення сигналу уздовж часової вісі від його номінального значення. Вимірюється в одиницях часу. DJ визначається як усереднена за результатами вимірювань різність між величинами відхилень постійної складової джитеру від його нульового значення, тобто усереднена часова різність між стрибками дельта-функції на PDF DJ:

$$DJ = \mu_L - \mu_R,$$

де μ_L та μ_R – усереднені за результатами вимірювань часові моменти стрибків дельта-функції на часовій вісі (на верхній PDF рис.5.28 DJ складає 20 часових одиниць).

Середньоквадратичний джитер (*Jitter RMS*). *Середньоквадратичний джитер* – це стандартна девіація джитеру, що визначається за допомогою горизонтальної гистограми у межах 3σ.

Момент та тривалість окового перетину (*Eye Crossing Time, ECT*). *Момент (виникнення) окового перетину* – це часовий момент виникнення окового перетину, в який горизонтальна функція розподілу амплітуд окової діаграми має максимальне значення (див.рис.5.29).

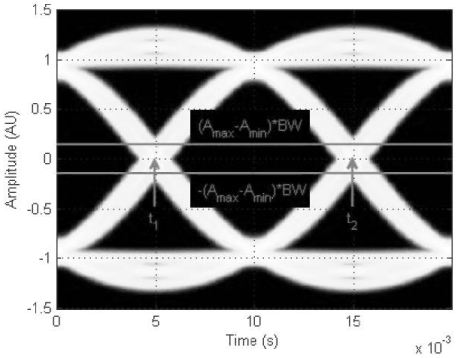


Рис. 5.29. Визначення моментів окових перетинів для нульового амплітудного рівня окової діаграми

ECT визначається шляхом побудови горизонтальної гистограми PDF. На рис.5.29 показано два моменти окового перетину - t_1 (в момент $5x10^{-3}$ сек) та t_2 (в момент $15x10^{-3}$ сек). Проте на відміну від параметра амплітудного перетину ECL у даному випадку цікавляться розподілом амплітуд у момент перетину не по висоті окової діаграми, а по її ширині.

На рис.5.30 показана усереднена горизонтальна гистограмма розподілу амплітуд для двох вищезазначених часових моментів перетину - t_1 та t_2 (див.рис.5.29).

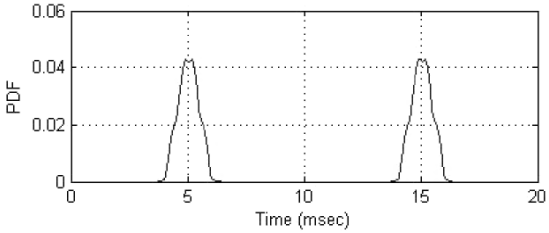


Рис. 5.30. Горизонтальна гістограмма розподілу амплітуд для двох

моментів t_1 та t_2

Як бачимо, максимальні значення амплітуд цих розподілів на гистограмі відповідають моментам 5 і 15 мсек. Ці моменти і є моментами окових перетинів ЕСТ.

Тривалість окового перетину – це часовий інтервал на око-діаграмі, впродовж котрого лінії перетину візуально зливаються, утворюючи розмиту смугу. Тривалість окового перетину визначають за допомогою горизонтальної гистограми розподілу амплітуд око-діаграми. На рис.5.30 – це ширина окового перетину .

Окова затримка (*Eye Delay*). Окова затримка – це проміжок часу між моментом окового перетину на початку ока та середньою точкою ока (див.рис.5.31). Вимірюється у секундах.

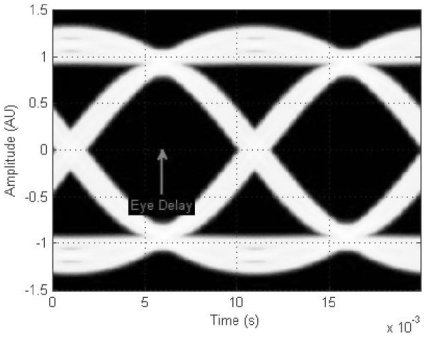


Рис. 5.31. Визначення окової затримки

Тривалість окового затухання (*Eye Fall Time, TFT*). *Тривалість окового затухання* – це усереднений часовий проміжок на спадаючий ділянці ока між високим та низьким пороговими рівнями, котрі зазвичай визначаються відповідно на рівнях 90 % та 10 % від амплітуди ока.

Тривалість окового зростання (*Eye Rise Time, ERT*). *Тривалість окового зростання* – це усереднений часовий проміжок на зростаючий ділянці ока між високим та низьким пороговими рівнями, котрі зазвичай визначаються відповідно на рівнях 90 % та 10 % від амплітуди ока.

Визначення TFT и ERT показано на рис.5.32.

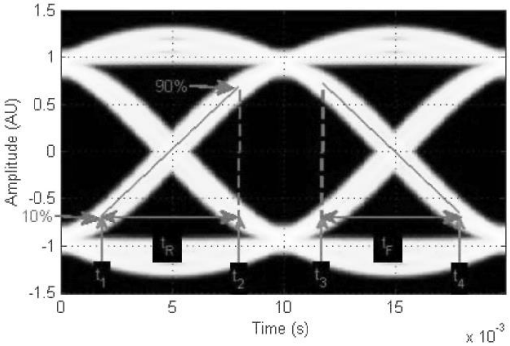


Рис. 5.32. Визначення параметрів TFT и ERT

Окова ширина (*Eye Width*). *Окова ширина* – це горизонтальна відстань між двома часовими точками, кожна із котрих віддалена від середнього моменту окового перетину у напрямку до центра ока на стандартну девіацію (тобто, на 3σ). Визначається у секундах. Визначення окової ширини показано на рис.5.33.

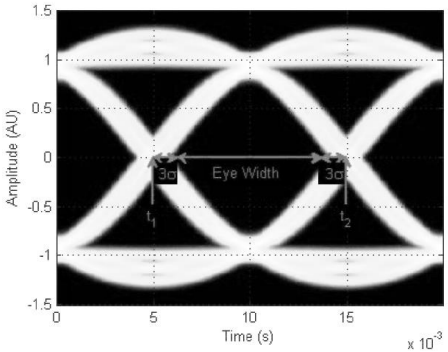


Рис. 5.33. Визначення окової ширини

5.8. Діаграми станів

У практиці сучасних телекомунікацій зустрічається клас завдань, коли для аналізу роботи цифрової системи необхідно мати представлення не про стани сигналу, а про динаміку зміни цих станів. Такі завдання зустрічаються при аналізі процесів в телекомунікаційних системах та аналізі диференціальних методів

модуляції, у яких передача цифрової інформації здійснюється не сигналом, а заміною одного сигналу іншим. Для вирішення завдань цього класу застосовуються діаграми станів, деревоподібні діаграми та діаграми Треліса. Зокрема, під час аналізу динаміки змін станів цифрового сигналу найбільш часто використається діаграма Треліса, що представляє собою одну з модифікацій діаграми станів. Основна відмінність діаграми Треліса полягає в тому, що крім станів цифрового сигналу на цій діаграмі показується ще і траєкторія змін станів. Під час алгоритмічного тестування (коли перевіряється коректність роботи алгоритму) використовуються деревоподібні діаграми, що представляють собою дерево зміни станів.

Діаграма станів (*state diagram*) визначає усі можливі стани, у яких може перебувати конкретна система, а також процес зміни станів системи як результат впливу певних подій. Фактично діаграма станів являє собою граф станів, у яких може перебувати система, і зв'язки між цими станами.

Стан (*state*) являє собою певний відрізок часу у життєвому циклі досліджуваної системи, протягом якого є істиною деяка умова, виконуються якісь строго визначені дії або очікується наперед визначена подія.

Стан може мати ієрархічну структуру. Кожний підстан (*substate*) може мати свій окремий початковий та кінцевий псевдостан. Завершення роботи всіх підстанів означає завершення активності даного стану й вихід з нього. Одиницею впливу є подія: кожна подія приводить до зміни стану одного або декількох об'єктів у системі, або до виникнення нових подій. Робота системи характеризується послідовністю подій, що відбуваються у системі.

Стан може бути вдосконалено шляхом уведення в нього послідовних підстанів зі зв'язками типу "І" або взаємовиключних підстанів зі зв'язками типу "АБО". Тільки но створена система починає функціонувати з якогось строго визначеного початкового псевдостану. Дія, що створила певний об'єкт у системі, може бути використана для ініціації переходу у початковий псевдо стан. Об'єкт, що перейшов у кінцевий псевдостан, припиняє своє існування.

Подія відбувається у деякий момент часу. Нерідко факт

виникнення події використовується для визначення відповідного моменту часу. Одна з подій може логічно передувати іншій, або випливати з іншої (якщо події мають логічно –причинний зв'язок), або вони можуть бути незалежними (якщо ці події не мають причинного зв'язку). Незалежні події не має сенсу якимось чином упорядковувати, тому що вони можуть виникати випадково або відбуватися у довільному порядку. Події передають інформацію з одного об'єкта на інший. Існують класи подій, які просто сигналізують про те, що щось відбулося або відбувається (приклади: загоряння лампочки ліфта, гудок у слухавці). Нерідко розглядаються виняткові події (іноді їх називають виключеннями), які сигналізують про порушення роботи апаратури або програмного забезпечення.

Сценарії й траси подій. Сценарієм називається послідовність подій, що може мати місце під час конкретного функціонування системи. Сценарії можуть включати всі події, що відбуваються в системі, або тільки ті події, що впливають тільки на окремі об'єкти системи. При аналізі динаміки роботи системи зазвичай складають й розглядають кілька сценаріїв, що відображають можливі варіанти її роботи.

Нижче наведено приклад сценарію користування телефонною лінією (розмова двох абонентів по телефону). Кожна подія в цьому сценарії передає якусь інформацію з одного об'єкта на інший. Перша подія, що виникає в момент підняття слухавки одним із абонентів - це довгий гудок, що передається через абонентську лінію від вузлу зв’язку до телефонного апарату користувача – ініціатора телефонної розмови. Далі виникає друга подія, третя подія і т.д.

Один із можливих сценаріїв користування телефонною лінією може бути наступним.

1) Абонент, що викликає, зняв слухавку:

починається довгий гудок.

2) Абонент, що викликає, набрав першу цифру телефонного номеру:

гудок припиняється.

3) Абонент, що викликає, набрав усі інші цифри телефонного номеру:

телефон, що викликається, починає дзвонити.

4) Абонент, що викликає, чує гудки:

абонент, що викликається, не піднімає слухавку.

5) Абонент, що викликається, піднімає слухавку:

гудки припиняються, телефони з'єднуються.

6) Один із абонентів вішає слухавку:

телефонний зв’язок розривається.

Наступним етапом після розробки та аналізу сценаріїв є визначення об'єктів, що мають генерувати і приймати кожну подію, що визначена у рамках сценарію. Послідовності подій із прив'язкою до об'єктів досліджуваної системи зручно представляти у вигляді діаграм, які часто називають трасами подій.

Приклад траси подій щодо розмов по телефону представлено на рис.5.34.

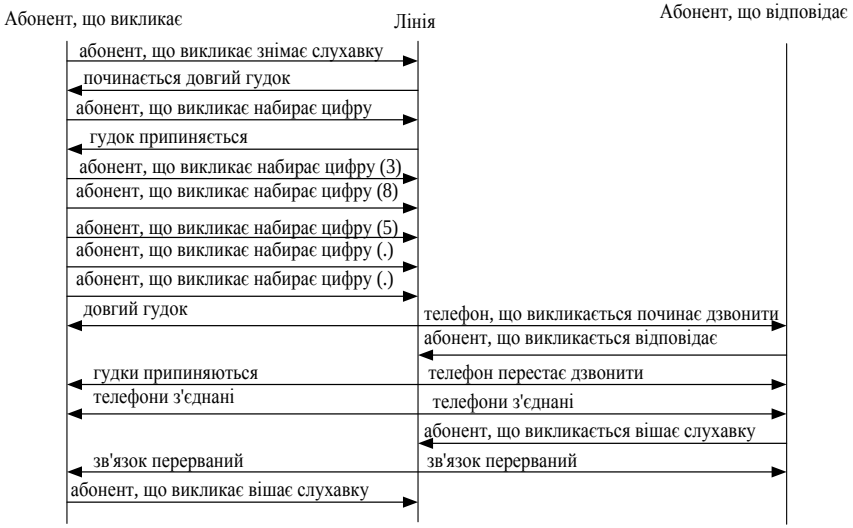


Рис. 5.34. Траса подій, що організують процес телефонної розмови

Вертикальні лінії зображують на цій трасі об'єкти, а горизонтальні стрілки - події (стрілка починається в об'єкті, що

генерує подію, і закінчується в об'єкті, що приймає подію). Події, що надійшли пізніше поміщені нижче подій, що надійшли раніше, одночасні - на одному рівні.

Стан визначає реакцію об'єкта на події, що на нього надходять. Реакція об'єкта на подію може включати деяку дію і/або перехід об'єкта у новий стан. Процес функціонування системи можливо відобразити не тільки за допомогою траси подій. Діаграму станів, що зв'язує події, об’єкти і стани, можливо ще відобразити у вигляді графа. Після прийому події наступний стан системи залежить як від її поточного стану, так і від події. Зазначимо, що зміна стану називається переходом. З урахуванням вищезазначеного діаграму станів відображають у вигляді графа, вузли якого представляють стани, а спрямовані дуги, що позначені іменами відповідних подій, представляють переходи. Діаграма станів дозволяє одержати послідовність станів по заданій послідовності подій.

На рис.5.35 наведена, як приклад, діаграма станів для процесу з’єднання двох абонентів через телефонну лінію.

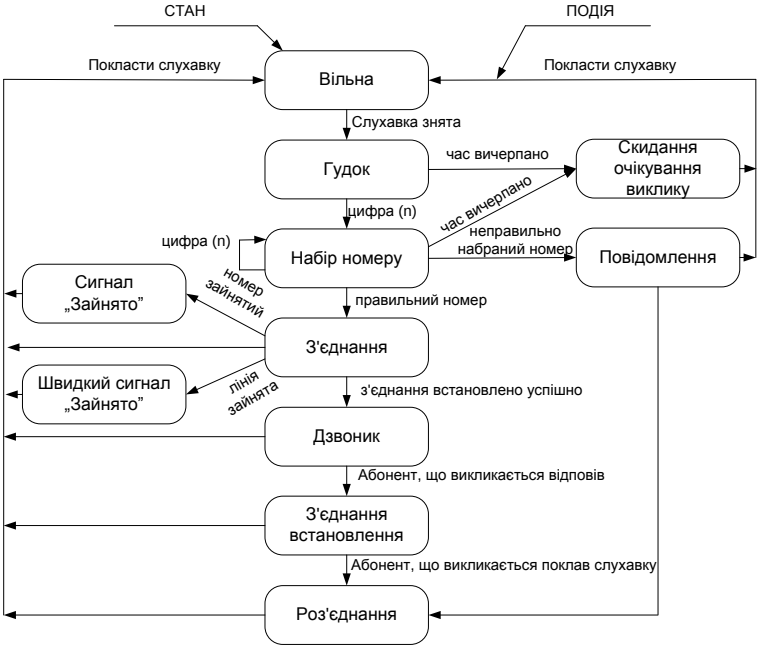


Рис. 5.35. Діаграма станів для процесу з’єднання двох абонентів

Також, як приклад, можна привести діаграму станів для згортального кодера. Робота згортального кодера із ступенем кодування ½, побудованого на трьохрозрядному регістрі зсуву (тобто, при К=3), показана на рис.5.36.

Як бачимо, розглядається шість послідовних кроків роботи цього кодеру – t_1, t_2, t_3, t_4, t_5, t_6 – коли на його вхід (зліва) послідовно надходять символи бінарної послідовності 101000 (вони фіксуються у лівому розряді регістру зсуву), а на виході підсумовуючих гілок кодера утворюються біти дворозрядного вихідного кодового слова U1, U2. Для визначення вихідних символів необхідно знати стан двох правих розрядів регістру зсуву та стан чергового одного біту, що надійшов на вхід кодера (тобто, у лівий розряд регістру зсуву).

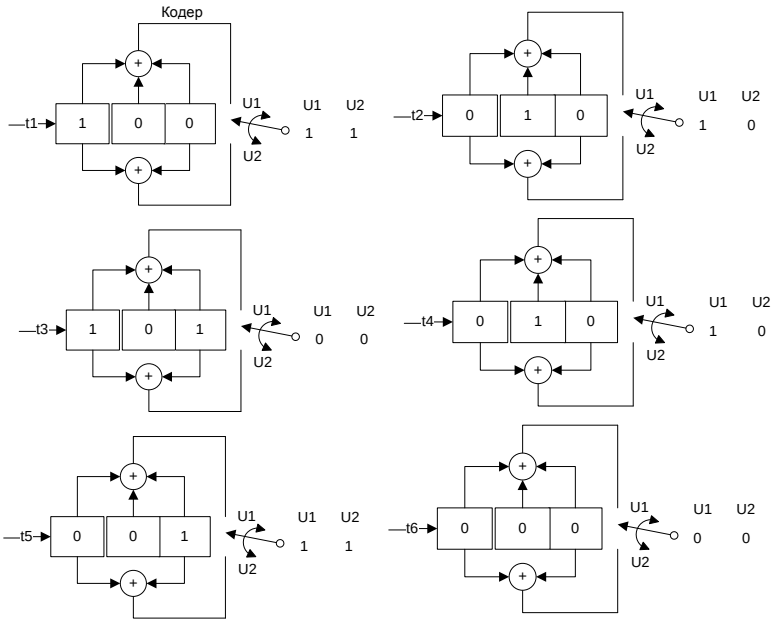


Рис.5.36. Процес кодування бінарної послідовності 101000 трьохрозрядним згортальним кодером зі ступенем кодування ½

Діаграма станів вищерозглянутого згортального кодера відображена на рис.5.37 у вигляді графа. Стани кодеру, що показані

на цій діаграмі, фізично представляють усі можливі комбінації бітів у двох крайніх правих розрядів регістра зсуву і позначаються наступним чином: a=00, b=10, c=01 й d=11.

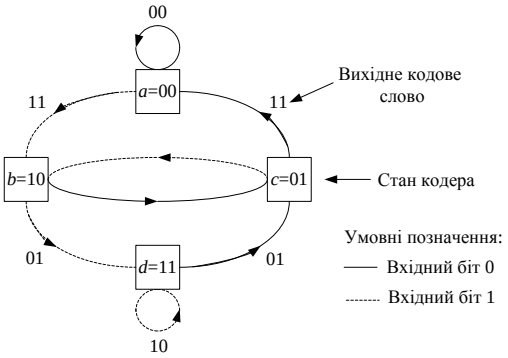


Рис. 5.37. Діаграма станів згортального кодера (ступінь кодування 1/2, K=3)

У той час як шляхи між цими станами представляють вихідні кодові слова, що утворюються на виході підсумовуючих гілок кодера. Ці слова і є результатом переходів між станами кодера. При зображенні шляхів суцільною лінією прийнято позначати шлях, пов'язаний із нульовим вхідним бітом, а пунктирною лінією - шлях, пов'язаний із одиничним вхідним бітом.

Відзначимо, що за один перехід неможливо здійснити довільний перехід із одного стану в інший. Тому що за одиницю часу переміщається тільки один біт вхідної послідовності. Існує тільки два можливих переходи між станами, у які регістр може переходити за час проходження кожного біта. Наприклад, якщо стан кодера - 00, при наступному зсуві можливе виникнення тільки станів 00 або 10.

5.9. Деревоподібні діаграми

Незважаючи на те, що діаграми станів повністю описують процес зміни станів кодера, по суті, їх не можна використати для відстеження переходів кодера залежно від часу, оскільки ці діаграми не представляють динаміку змін. Цього недоліку позбавлені деревоподібні діаграми (*tree diagram*), які до діаграм

станів додають часовий вимір. Зокрема, деревоподібна діаграма вищерозглянутого згортального кодера показана на рис.5.38.

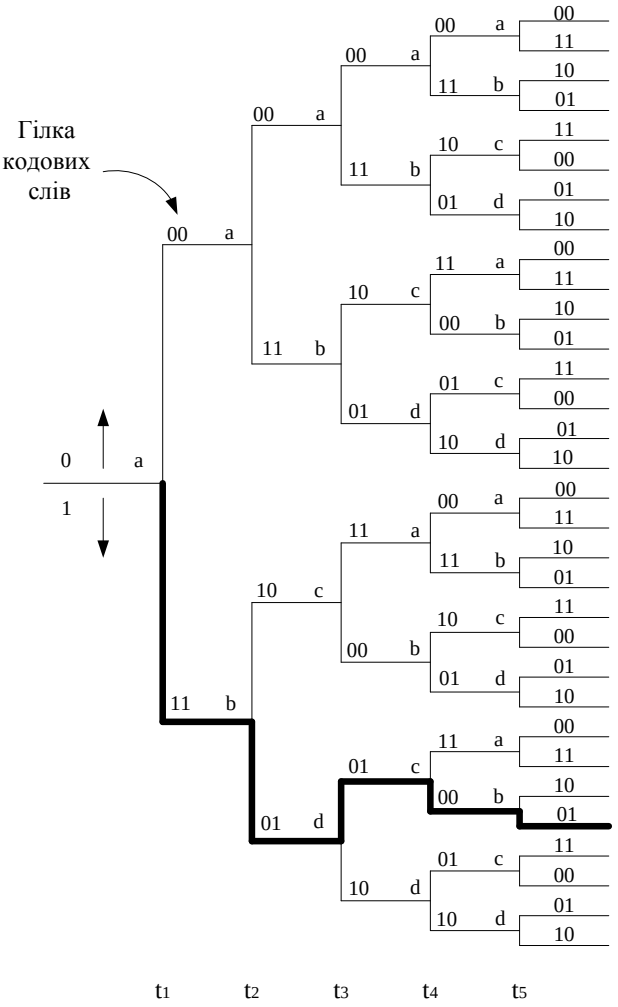


Рис.5.38. Деревоподібне представлення процесу зміни станів згортального кодера (ступінь кодування ½, K=3)

Користуватися деревоподібною діаграмою можливо наступним чином.

По-перше, слід пам’ятати, що кожна гілка дерева відображає якесь вихідне кодове слово (у нашому випадку воно – дворозрядне). У кожен наступний момент надходження чергового вхідного біта процедура кодування може бути відслідкована шляхом переміщення по цій діаграмі у напрямках „ліворуч або праворуч”. Правило розгалуження для знаходження послідовності вихідних кодових слів є наступним: якщо вхідним бітом є нуль, то він пов'язується зі словом, що знаходиться шляхом переміщення в наступну (у напрямку нагору) праву гілку; якщо вхідний біт - це одиниця, то кодове слово знаходиться шляхом переміщення в наступну (у напрямку вниз) праву гілку.

Передбачається, що спочатку кодер містив тільки нулі. Діаграма показує, що якщо першим вхідним бітом був нуль, то вихідним кодовим словом гілки буде 00, а якщо першим вхідним бітом була одиниця, то вихідним кодовим словом буде 11. Аналогічно, якщо першим вхідним бітом була одиниця, а другим - нуль, на виході другим словом гілки буде 10. Якщо першим вхідним бітом була одиниця та другий вхідний біт була одиниця, другим кодовим словом на виході буде 01. Виходячі з цієї процедурі, бачимо, що вхідна послідовність 110 11 представляється жирною лінією, намальованої на деревоподібній діаграмі (див.рис.5.38). Цей шлях відповідає вихідній послідовності кодових слів 1 10 10 10 0 0 1.

Доданий вимір часу у деревоподібній діаграмі допускає опис кодера як функції конкретної вхідної послідовності. Однак при спробі опису за допомогою деревоподібної діаграми вхідних послідовностей довільної довжини виникає проблема розмірності, оскільки число відгалужень росте як 2^L, де L - це кількість кодових слів гілок у послідовності.

5.10. Решітчасті діаграми Треліса

Дослідження деревоподібної діаграми на рис.5.38 показує, що в цьому прикладі після третього розгалуження в момент часу t_4 структура повторюється (у загальному випадку деревоподібна структура діаграми повторюється після K відгалужень, де K-

розрядність кодера). Позначимо кожен вузол у дереві на рис.5.38, ставлячи у відповідність чотири можливих стани в регістрі зсуву: a=00, b=10, c=01 й d=11. Перше розгалуження деревоподібної структури в момент часу t_1 дає пари вузлів, позначених як *a* та *b*. При кожному наступному розгалуженні кількість вузлів подвоюється. Друге розгалуження в момент часу t_2 дає в результаті чотири вузли, позначених як a, b, c та d. Після третього розгалуження всього утворилося вісім вузлів: два - a, два - b, два - c і два - d.

Можна бачити, що всі гілки виходять із двох вузлів того самого стану, створюючи ідентичні гілки послідовностей кодових слів. У цей момент дерево ділиться на ідентичні верхню й нижню частини. Зміст цього стає яснішим після розгляду кодера, зображеного на рис.5.36. Коли четвертий вхідний біт входить у кодер ліворуч, вихідний біт праворуч викидається й більше не впливає на кодові слова на виході.

Після K-го розгалуження генеруються однакові кодові слова гілок. Це означає, що будь-які стани, що мають однакову мітку в той самий момент t_i можна з'єднати, оскільки всі наступні шляхи будуть нерозрізнені. Якщо ми проробимо це для деревоподібної структури, то одержимо іншу діаграму, називану решітчастою. Решітчаста діаграма, що використовує повторювану структуру, дає більш зручний опис кодера у порівнянні з деревоподібною діаграмою.

Решітчаста діаграма для вищерозглянутого згортального кодера показана на рис.5.39.

При зображенні решітчастої діаграми ми скористалися тими ж умовними позначками, що й для діаграми станів: суцільна лінія позначає вихідні дані, що генеруються вхідним нульовим бітом, а пунктирна - вихідні дані, що генеруються вхідним одиничним бітом. Вузли решітки представляють стани кодера: перший ряд вузлів відповідає стану a=00, другий і наступні - станам b=10, c=01 та d=11. У кожен момент часу для представлення 2^{K-1} можливих станів кодера решітки необхідно мати 2^{K-1} вузлів. У нашому прикладі після досягнення глибини решітки, що дорівнює трьом (у момент часу t_4), помічаємо, що решітка має фіксовану періодичну

структуру. У загальному випадку фіксована структура реалізується після досягнення глибини K. Отже, із цього моменту в кожен стан можна увійти з кожного із двох попередніх станів. Також із кожного стану можна перейти в один із двох станів. Із двох вихідних гілок одна відповідає нульовому вхідному біту, а інша - одиничному вхідному біту. На рис.5.39 вихідні кодові слова відповідають переходам між станами, показаними як мітки на гілках решітки.

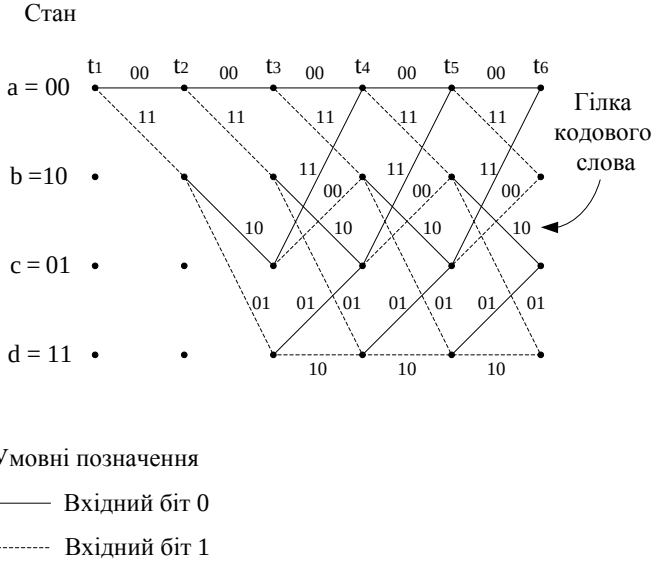


Рис.5.39. Решітчаста діаграма кодера (ступінь кодування 1/2, K=3)

Один стовпець часового інтервалу решітчастої структури кодування, що сформувалася, повністю визначає код. Кілька стовпців показані винятково для візуалізації послідовності кодових символів як функції часу. Стан згортального кодера представлено вмістом крайніх правих *K-1* розрядів у регістрі кодера.

ЛЕКЦІЯ №6 ВИМІРЮВАННЯ ПАРАМЕТРІВ ТЛК-ОБЛАДНАННЯ НА ФІЗИЧНОМУ РІВНІ ВЗАЄМОДІЇ ІНФОРМАЦІЙНИХ СИСТЕМ

Розглядаються наступні питання:

Лекційне заняття

6.1. Вимірювання параметрів електричних кабелів

6.2. Вимірювання параметрів волоконно-оптичних кабелів

6.3. Вимірювання параметрів абонентських ліній зв'язку

6.4. Вимірювання параметрів аналогових комутованих телефонних каналів

Самостійне заняття

6.5. Вимірювання параметрів обладнання цифрових систем передачі (ЦСП), що побудовані за технологіями *PDH/SDH*

6.6. Особливості вимірювання параметрів цифрових каналів, що утворені на базі аналогових ліній телефонних мереж абонентського доступу (канали *ISDN* та *xDSL*)

6.7.Особливості вимірювання параметрів обладнання систем із частотним ущільненням аналогових телефонних каналів (обладнання типу К-60, К-120 і т.ін.)

6.1. Вимірювання параметрів електричних кабелів

*6.1.1.*Загальна характеристика електричних кабелів**.** Електричні металеві кабелі використовують в якості фізичного середовища транспортування інформації. Вони є основним елементом будь-якої проводової лінії зв'язку, що входить до складу обладнання багатьох різноманітних телекомунікаційних систем, зокрема:

1) магістральних кабельних систем, призначених для передавання цифрових бітових потоків і побудованих з використанням технологій часового ущільнення каналів типу *PDH/SDH*;

2) магістральних кабельних систем, призначених для передавання аналогових широкосмугових сигналів, утворюваних шляхом частотного ущільнення стандартних аналогових телефонних каналів (так звані багатоканальні системи передачі

типу К-60, К-120 і т. ін.);

3) стандартних аналогових абонентських телефонних каналів, що використовуються у мережах абонентського доступу до телефонних комутаційних систем (АТС);

4) стандартних аналогових абонентських телефонних ліній зв'язку, що використовуються для утворення абонентських каналів *ISDN* та (або) *xDSL*;

5) структурованих кабельних систем, призначених, головним чином, для використання у складі локальних пакетних мереж.

З точки зору теорії передавання сигналів відрізок будь-якого електричного кабелю веде себе як електричний чотирьохполюсник із розосередженими параметрами незалежно від того, чи цей кабель згорнутий у бухту, чи вмонтований у ділянку якоїсь лінії проводового зв'язку.

Еквівалентна схема відрізка електричного кабелю показана на рис. 6.1. Як бачимо, реакція такого кабелю на потоки вхідних електричних сигналів повністю визначається його **первинними параметрами**: активним опором R (як щодо постійного, так і щодо змінного струму), індуктивністю L, ємністю C та провідністю ізоляції G. Визначення та фізичні пояснення щодо цих параметрів розглядати не будемо, оскільки вони надаються у будь-якому підручнику із теорії електричних ланцюгів. Наведемо лише вигляд їхніх частотних залежностей (див. рис.6.2).

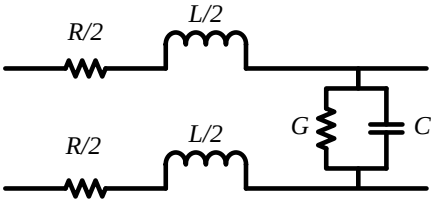


Рис. 6.1. Еквівалентна схема відрізку електричного кабелю

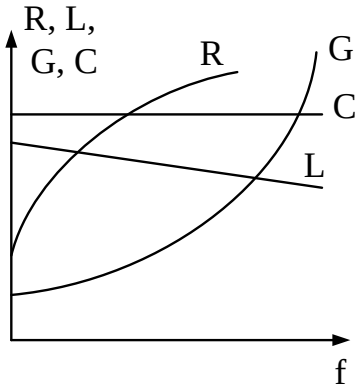


Рис. 6.2 Частотна залежність первинних параметрів симетричного електричного кабелю

На практиці для визначення фізичної цілісності кабелю за допомогою звичайного тестера (зокрема, мультиметра) здійснюють вимірювання опору цього кабелю на постійному струмі. Відрізок типового кабелю довжиною 10 метрів повинен мати опір постійному струму у діапазоні 1-2 Ома. Вимірюють також взаємну ємність між двома проводами кожної пари у багатопарному кабелі. Якщо виміряне значення цієї ємності суттєво перевищує її номінальне значення, то робиться висновок про високу ймовірність фізичного пошкодження кабелю: його намокнення, надмірну розтянутість або неякісне його термінування (неякісне з'єднання кінців кабелю з конекторами). Вимірювання індуктивності відрізка кабелю також іноді має практичну доцільність, зокрема якщо намагаються виявити факт його надмірної завитості, оскільки із збільшенням кількості витків кабелю збільшується його індуктивність. Однак в експлуатаційній практиці вимірювання первинних параметрів кабелів не є основними. Скоріш, вони носять допоміжний характер. Це пов'язано із труднощами із встановленням причинно-наслідкових зв'язків між результатами вимірювань первинних параметрів кабелю та характеристиками якості функціонування ТЛК-обладнання, в яке цей кабель вмонтовано. Труднощі виникають як на рівні теоретичних розрахунків, так і на рівні технічної реалізації експлуатаційних

процедур. Наприклад, важко знайти функціональну залежність між первинними параметрами кабелю та затримками у передаванні інформації через цей кабель або достовірністю інформації, отриманої на його вихідному кінці. Теоретично це є можливим, проте пов'язане із громіздкими інженерними розрахунками, котрі далеко не завжди вдається здійснити у замкненій математичній формі. Тому на практиці вимірюються, головним чином, так звані вторинні параметри кабелю, такі як хвильовий опір (або імпеданс, *impedans*) *z*, затухання (або згасання) *A*, перехідне затухання у двох його різновидах - перехідне затухання на ближньому кінці – *NEXT (Near End Crosstalk)* та перехідне затухання на дальньому кінці – *FEXT (Far End Crosstalk)*, захищеність від перехідних завад *ACR (Attenuation to Crosstalk Ratio)*, відносна швидкість розповсюдження сигналів *NVP (Nominal Velocity of Propagation)* (іноді цей параметр позначається як *VOP - Velocity of Propagation*), затримка проходження сигналів (параметр *delay*), розкид затримок проходження сигналів (параметр *Skew*), повернені втрати (рос., - возвратные потери) *RL (Return Loss)*, у т.ч. структурні повернені втрати *SRL (Structural Return Loss)*, опір зв'язку екрану кабеля R_k *(transfer impedans)*, параметри затухання несиметрії - на ближньому кінці *LCL (longitudinal conversion loss)* та на дальньому кінці *LCTL (longitudinal conversion transfer loss)* і параметр додаткових втрат *ILD (Insertion Loss Deviation).*

Вторинні параметри кабелю у контексті експлуатаційних задач мають ясну фізичну інтерпретацію. Вони можуть бути відносно легко виміряні за допомогою інструментальних засобів, що представлені на ринку вимірювальної техніки.

У рамках навчальної дисципліни „Лінії передачі" було детально розглянуто як первинні, так і вторинні параметри металевих кабелів (зокрема, дано формальні визначення цих параметрів, пояснено фізичні процеси у кабелі, що обумовили доцільність уведення цих параметрів в експлуатаційну практику, проаналізовано залежності уведених параметрів від параметрів фізичних процесів у кабелі, визначено норми на припустимі значення параметрів кабелю і т.ін.). Зокрема, вищеназваний матеріал міститься у розділі 2 відомої книги Семенова А.Б., Стрижакова С.К. та Сунчелея І.Р. „Структуровані кабельні

системи" (на рос. мові). –М.:ДМК Пресс, 2002. Тому ми не будемо повторювати цей матеріал, а основну увагу приділимо методам та засобам експлуатаційних вимірювань основних параметрів електричних кабелів.

6.1.2. Оцінювання якості магістральних кабелів. Якість магістрального кабелю доцільно перевіряти як безпосередньо перед його прокладкою і монтуванням у конкретну систему зв'язку (тобто, здійснювати так званий вхідний контроль кабелю), так і на етапі його експлуатації, особливо коли є сумніви щодо його нормального функціонування.

Вхідний контроль кабелю виконується не тільки для визначення його фізичної цілісності, наприклад шляхом вимірювань первинних параметрів кабелю (як вже зазначалось, такі вимірювання можливо здійснювати за допомогою звичайного мультиметру). Інтерес представляють й інші характеристики кабелю, що суттєво впливають на якість передавання сигналів через цей кабель, незважаючи на те, що ці характеристики, як правило, вказуються у паспортних даних на кабель. Кабельна продукція, а також роботи з її монтування – найбільш високовартісні складові будь-якої територіально розгалуженої системи електрозв'язку. Тому поглиблений вхідний контроль кабелю у багатьох випадках є виправданою процедурою.

Найбільш зручно вхідний контроль кабелю виконувати за допомогою пристрою, що зветься **аналізатор ланцюгів** (в англомовних публікаціях цей пристрій отримав не зовсім вдалу назву *Network Analyzer*). У склад цього пристрою входить генератор тестових сигналів та аналізатор сигнальних спектрів. Існують **скалярні та векторні аналізатори ланцюгів**. Зрозуміло, що скалярні аналізатори можуть вимірювати лише скалярні характеристики кабелю, зокрема ІЧХ кабелю, тобто залежність затухання сигналів в кабелі від частоти і т.ін. У той час як векторний аналізатор, окрім цього, здатний вимірювати фазові співвідношення між складовими сигналу у кабелі – ФЧХ, розкид затримок проходження складових сигналів, комплексні параметри кабелю тощо. Аналізатори ланцюгів розрізняються також своєю функціональністю. Зокрема, існують повнофункціональні аналізатори, котрі здатні вимірювати не лише частотні параметри

кабелів (комплексні та скалярні) та параметри відбиття (рос. – отражения) сигналів від усіляких неоднорідностей у кабелі, але і опір ізоляції кабелю. Такі аналізатори здатні подавати високу тестову напругу у ланцюг ізоляції, а потім вимірювати утворюваний цією напругою надмалий струм витоку (рос. – ток утечки). Проте існують і окремі спеціалізовані пристрої для вимірювань якості ізоляції у кабелі.

Вхідний контроль кабелю у бухтах передбачає вимірювання характеристичного імпедансу (тобто, хвилевого опору) кабелю, погонного опору кабелю, опору ізоляції, рівня повернених втрат, коефіцієнта відбиття і т. ін.

У період експлуатації вже змонтованого та укладеного у грунт кабелю найбільш актуальна проблема - виявлення факту пошкодження та знаходження (або, як кажуть, локалізація) місця пошкодження кабелю. Процес пошуку місця пошкодження іноді називають локацією точки пошкодження кабелю. Для локації використовують кабелепошукачі або металеві рефлектометри дальньої дії.

Схема використання кабелепошукача показана на рис.6.3.

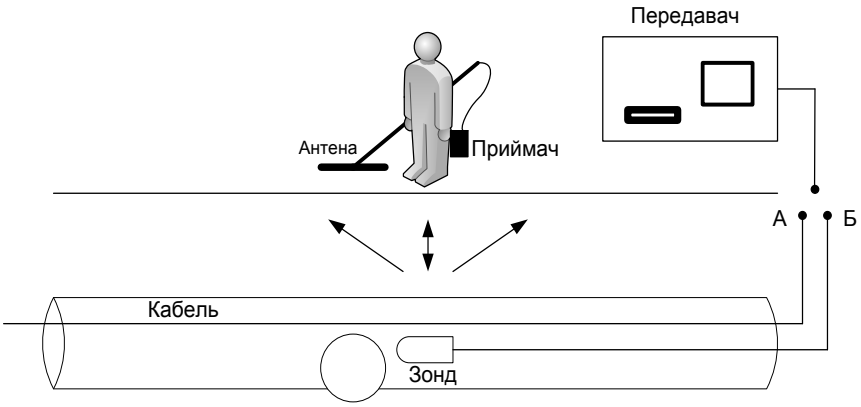


Рис.6.3. Схема використання кабелепошукача

Основними складовими елементами кабелепошукача є передавач синосоїдальних сигналів наперед визначеної частоти, що

підключається до одного із кінців визначеної пари проводів кабелю (зокрема до точки А так, як це показано на рис.6.3), та приймач-локатор із комплектом антен (індуктивних, активних, всіляких пробників і т. ін.), що вловлює та регіструє сигнали, що випромінюються кабелем через грунт. Антена закріплюється на кінці стержневого утримувача і під'єднується до приймача, що носить з собою працівник служби експлуатації. Під час локації працівник, утримуючи у руках стержень із антеною, просувається уздовж траси кабелю та, дивлячись на показання приймача-локатора, вирішує покладені на нього експлуатаційні завдання (на рис.6.3 варіант *А* підключення передавача до кабелю). В процесі роботи працівник має можливість змінювати частоту та потужність тестового сигналу, що подається на кабель, а також обирати та підключати до приймача той чи інший тип антени. Зрозуміло, що коли на кабель подається осцилюючий сигнал із наперед визначеною частотою, то впродовж нього виникає відповідне електромагнітне поле, що може бути виявлено за допомогою індуктивної антени та відфільтроване від інших радіовипромінювань засобами приймача-локатора. Енергія цього поля суттєво затухає у прошарку грунту, що знаходиться між антеною та кабелем. Тому для надійного виявлення сигналів, що випромінюються від кабелю більш глибокого залягання, необхідно збільшувати потужність передавача тестового сигналу.

Кабелепошукачі, що призначені для роботи із укладеними у грунт магістральними кабелями, виготовляються компанією *Dynatel* – модельний ряд 2210E, 2250E та 2273E. Вироби, що входять до цього модельного ряду, відрізняються один від одного своєю функціональністю. Проте усі вони здатні забезпечити вирішення наступних експлуатаційних завдань:

1) виявити шлях залягання кабелю уздовж траси;

2) визначити глибину залягання кабелю у грунті (до 4,5 м);

3) визначити характер ушкодження кабелю (коротке замикання чи розрив);

4) визначити ступінь неоднорідності параметрів кабелю у точках ушкоджень та його розгалуження (і, тим самим, визначити, чи є можливою подальша експлуатація кабелю);

5) визначити ступінь неузгодженості імпедансу навантаження із

характеристичним імпедансом кабелю;

6) виявити місця намокання кабелю;

7) виявити шлях залягання силового кабелю та інших кабелів електропостачання (у режимі відключення передавальника кабелепошукача та настроювання приймача-локатора на частоту 50Гц);

8) знаходження вузьких місць та фізичних перепон в середині труби (на рис.6.3 варіант *Б* підключення передавача до кабелю), що заважають прокладці нових кабелів у цій трубі (для цього застосовують активний зонд (міні-передавач), що просувається уздовж труби; місце знаходження перепони знаходиться там, де цей зонд не може просунутися далі).

Усі вищеназвані кабелепошукачі компанії *Dynatel* мають зручний графічний інтерфейс та звукове відображення результатів локації.

Металеві рефлектометри дальньої дії. Для локації точок пошкодження кабелю широке застосування в експлуатаційній практиці знайшли **металеві рефлектометри дальньої дії** (*Time Domain Reflectometer – TDR*). Рефлектометр являє собою сукупність засинхронізованих між собою імпульсного генератора та приймача, що забезпечує вимірювання параметрів імпульсного сигналу із одного кінця кабелю. Пристрій *TDR* діє подібно радару. У кабель надсилається короткотривалий імпульс, що розповсюджується уздовж нього із швидкістю, що майже дорівнює швидкості світла. Частина енергії імпульса відбивається від усілякого роду неоднорідностей, що можуть виникнути на шляху його розповсюдження уздовж кабелю. Під неоднорідностями кабелю розуміється коротке замикання між парами проводів у кабелі, розрив кабелю, місця з'єднань кусків кабелю, відгалуження від кабелю, місця з'єднань із конекторами, місця замокання кабелю, місця деградації метеріалів, із яких зроблено цей кабель і т. ін. Відбиті від неоднорідностей сигнали розповсюджуються уздовж кабелю у зворотному напрямі і потрапляють на вхід приймача TDR. По величині, полярності та формі відбитого сигналу є можливим визначити характер неоднорідності, а по проміжку часу між моментами надсилання імпульсу генератором та приймання відбитого сигналу – місце знаходження неоднорідності. Під час

роботи із TDR необхіно враховувати параметр *VOP* (*Velocity of Propagation*), тобто відмінність швидкості розповсюдження сигналів у кабелі від швидкості світла у вакуумі. Ця відмінність може досягати 3% і залежить від типу кабелю. Коректне користування рефлектометром неможливе без здобуття певних навичок роботи із цим приладом. Більш/менш детально прийоми роботи з *TDR* висвітлені у книзі І.Г.Бакланова „Методы измерений в системах связи» (М.: Эко-Трендз, 1999).

Металеві рефлектометри випускаються багатьма виробниками, зокрема компанією *RiserBond Instruments* (моделі 1000, 2000, 3000, 2901C та ін.).

6.2. Вимірювання параметрів волоконно-оптичних кабелів

Оптоволоконні системи передавання інформації знайшли широке розповсюдження у сучасному світі. Тому вимірювання параметрів цих систем, зокрема вимірювання параметрів оптичних кабелів, є актуальним завданням.

Розрізняють наступні категорії робіт із оптоволоконним обладнанням:

1) **Промисловий аналіз** волоконно-оптичних кабелів та вузлів оптоволоконних систем зв'язку, що, зазвичай, здійснюють під час розробки та виготовлення оптоволоконного обладнання. На цьому етапі визначають відповідність характеристик виготовленного обладнання (зокрема, оптичних кабелів у бухтах) існуючим нормам. Для цього використовують досконале системне вимірювальне обладнання, ретельно відкаліброване та повірене відповідними метрологічними службами. Виміряні значення параметрів оформлюють у вигляді паспортних даних на вироби.

Системні вимірювання оптоволоконних виробів являють окремий напрямок у телекомунікаціях, котрий у рамках навчальної дисципліни „Експлуатація ТКС" розглядатися не буде.

2) **Експлуатаційний аналіз** волоконно-оптичних кабелів та вузлів здійснюється під час або безпосередньо перед прокладкою кабеля уздовж лінії зв'язку. При цьому вимірюють, головним чином, рівні потужності оптичного випромінювання на виходах передавальних та входах приймальних оптоелектронних модулів, затухання регенераційних ділянок лінії та усієї лінії у цілому,

затухання окремих оптичних волокон, затухання на відгалуженнях кабелів, на місцях зварювання кабелів тощо. Вимірювання затухання здійснюють щодо обох напрямків передавання оптичних сигналів. За результатами цих вимірювань отримують дані щодо розподілу уздовж траси прокладки кабелю всіляких неоднорідностей в структурі кабелю, що надає змогу обрати оптимальний варіант використання волокон кабелю. Нормативні документи вимагають для кожної ділянки регенерації визначати функцію розподілу неоднорідностей уздовж лінії зв'язку, оформляти визначену функцію у вигляді графіку із доданим до нього паспортом, куди вносяться усі виміряні дані щодо параметрів ділянки регенерації. У паспорті ділянки регенерації повинно бути наведено дані щодо схеми з'єднань волокон у кожній з'єднувальній муфті, виміряні значення рівнів оптичної потужності на оптичних входах та виходах регенераторів, рівні затухання в обох напрямках передавання, а також дані щодо параметрів помилок.

3) **Експлуатаційні вимірювання** здійснюються на стадії експлуатації оптоволоконної системи зв'язку. Експлуатаційний персонал має здійснювати постійний поточний контроль апаратури волоконно-оптичних систем зв'язку (ВОЛЗ), а також регламентовані певними інструкціями процедури, що спрямовані на підтримку працездатності обладнання ВОЛЗ. Зокрема, здійснювати профілактичні, у т.ч. контрольно-вимірювальні роботи. Якщо виявлено проблему із невідповідністю параметрів обладнання встановленим нормам, необхідно, щоб персонал мав можливість швидко локалізувати точку деградації якості кабельної системи. Наприклад, у випадку розриву кабелю необхідно оперативно та з високим ступенем точності знайти точку розриву, виконати розконсервування ділянки кабелю, замінити ушкоджений шматок кабелю, здійснити зварювання та відновити кабель. Поточні вимірювання параметрів ВОЛЗ, як правило, виконуються з використанням спеціально вмонтованих у штатне обладнання контрольно-вимірювальних засобів.

На стадії експлуатації оптоволоконних систем вирішують наступні завдання:

1) вимірюють рівні оптичної потужності та затухання оптичного сигналу у кабелі;

2) вимірюють параметр перехідного затухання;

3) здійснюють пошук та усунення пошкоджень та (або) деградації якості у ВОЛЗ (зокрема, визначають місце та характер ушкодження оптоволоконного кабелю, його заміну або відновлення і т.ін.);

4) іноді здійснюють стресове тестування апаратури волоконно-оптичних систем передачі.

6.2.1. Вимірювання оптичної потужності та затухання оптичного сигналу у кабелі

Щоб виміряти потужність у *Вт* або рівень потужності у *дБм* оптичного сигналу в оптоволоконній лінії необхідно мати відповідним чином відградуйований прилад, що зветься **оптичним вимірювачем потужності** (*Optical Power Meter, OPM*). На ринку інструментальних засобів пропонується багато різних *OPM*, що відрізняються один від одного типом детектора оптичного сигналу (Si, Ge, InGaAs та ін.), робочою довжиною хвиль (380-1150нм, 750-1700нм, 750/850/1300/1550нм та ін.), припустимим діапазоном потужності вимірюваних сигналів (від -80*дБм* до +10*дБм*) та точністю вимірювань (від $\pm 0{,}1$ *дБ* до $\pm 0{,}3$ *дБ*). Серед найбільш популярних *OPM* слід назвати вимірювач *OTM-1* компанії „*Перспективные Технологии*» (РФ), E5970A компанії *Hewlett-Packard* (США), K2401 компанії *Tektronix/Siemens* (ФРН) та багато ін. До основних параметрів *OPM* відносять: тип оптичного детектора (що визначає усі найбільш важливі характеристики цього приладу), метрологічна точність вимірювань та лінійність робочої характеристики приладу, динамічний діапазон щодо потужності вимірюваних оптичних сигналів, градуювальна шкала (необхідна для калібрування приладу) та можливість підтримки різноманітних оптичних інтерфейсів. *OPM* підключається до точки вимірювань через відповідний оптичний інтерфейс.

Для того, щоб коректно обрати необхідний тип та режим роботи *OPM* у реальних умовах використання ВОЛЗ, а також правильно виконати калібрування цього приладу необхідно мати певні знання щодо характеристик оптоволоконних кабелів та інших елементів ВОЛЗ, що не є об’єктом розгляду на цій лекції. Такі знання надаються у рамках навчальної дисципліни „Системи та лінії

передачі в електрозв'язку".

Для вимірювань затухання оптичного сигналу у кабелі, окрім *OPM*, необхідно мати **стабілізоване джерело оптичного сигналу** (*Stabilized Light Source, SLS*). Оптичний сигнал *SLS* попередньо визначеної потужності на попередньо визначеній довжині світлової хвилі подається на вхід досліджуваної ділянки кабелю, а до виходу цієї ділянки під'єднується *OPM*, котрий має бути здатним виміряти рівень потужності вихідного оптичного сигналу. Якщо є довіра до стабільності роботи джерела оптичних сигналів, що функціонує у складі штатного обладнання ВОЛЗ, то під час вимірювань затухання застосовувати *SLS* немає потреби.

Промисловість випускає багато різних *SLS* (наприклад, К2501 компанії *Tektronix/Siemens* (ФРН), 774х компанії *Wavetek* (США), Е5972А компанії *Hewlett-Packard* (США) та багато ін.), що відрізняються один від одного, головним чином, типом випромінювача світла. Існують три типи *SLS*: **лазерні джерела оптичного сигналу**, **світлодіодні джерела** (*LED*) та **джерела білого світла із вольфрамовою лампою**. Ці типи *SLS* відрізняються один від одного, в основному, шириною смуги випромінювання. Зрозуміло, що чим менша ширина смуги, тим більш якісний випромінювач (але більш дорожчий за вартістю). Лазерні випромінювачі мають найвужчу смугу випромінювання, а джерела білого світла – найширшу.

Аналізатори затухання в оптичному кабелі (*Optical Loss Test Set, OLTS*) (інша назва цих пристроїв – аналізатори втрат оптичної потужності) являють собою комбінацію *OPM* та *SLS*. За допомогою цих пристроїв, зазвичай, здійснюють покроковий аналіз оптичної лінії. Вони портативні, зручні у користуванні і тому широко використовуються на практиці.

Вимірювання затухання в оптичному діапазоні мають певну специфіку, яка має враховуватися під час проведення вимірювань. Перш за все, слід мати на увазі, що результат вимірювань затухання суттєво залежить від параметрів оптичного інтерфейсу між джерелом тестового оптичного сигналу та оптичною лінією. Навіть незначні відхилення у точності юстирування випромінювача, не кажучи вже про точність виготовлення елементів оптичного інтерфейсу, призводять до значних втрат

енергії сигналу під час проходження через інтерфейс. Вплив затухання оптичних інтерфейсів лінійного обладнання ВОЛЗ має враховуватися та вимірюватися. Тому на практиці виконують безпосередні вимірювання не параметра затухання в оптичному кабелі, а так званого **внесеного затухання**, котре визначається як сума параметрів затухання у лінії та втрат потужності в оптичному інтерфейсі.

По-друге, під час вимірювань має враховуватися можлива неузгодженість за спектром джерела оптичного сигналу та його приймача. Необхідно слідкувати, щоб не виникало ситуацій, коли, наприклад, спектр випромінюваного сигналу був в районі 1310нм, а смуга пропускання приймального пристрою – в районі 1300нм.

Для оцінювання величини параметрів затухання в оптичній лінії, окрім *OLTS*, може також застосовуватися **оптичний рефлектометр** (*Optical Time Domain Reflectometer, OTDR*). Принцип дії *OTDR* практично не відрізняється від принципу дії раніш розглянутого металевого рефлектометру, лише треба мати на увазі, що *OTDR* працює в оптичному діапазоні хвиль.

Апаратна структура оптичного рефлектометра зображена на рис.6.4 і особливих пояснень не потребує.

У лінію надсилається оптичний імпульс малої тривалості, котрий розповсюджується уздовж оптичного кабеля згідно законів релеєвського розсіювання та френелєвського відбиття. Від усілякого роду неоднорідностей, що можуть існувати у кабелі, відбивається частина енергії робочого сигналу і у зворотному напрямі через направляючий відгалужувач (рос. – ответвитель) потрапляє на фотоприймач. Пристрій *OTDR*, підключений до одного із кінців досліджуваної оптичної лінії, забезпечує вимірювання відбитої потужності.

На ринку інструментальних засобів представлено два класи *OTDR*: високоточні міні-рефлектометри, що покривають відстань від 100м до 50км (деякі із них – до 100км), та оптичні рефлектометри дальньої дії, що характеризуються невисокою вирішувальною здатністю, проте здатні працювати з кабельними лініями практично будь-якої довжини.

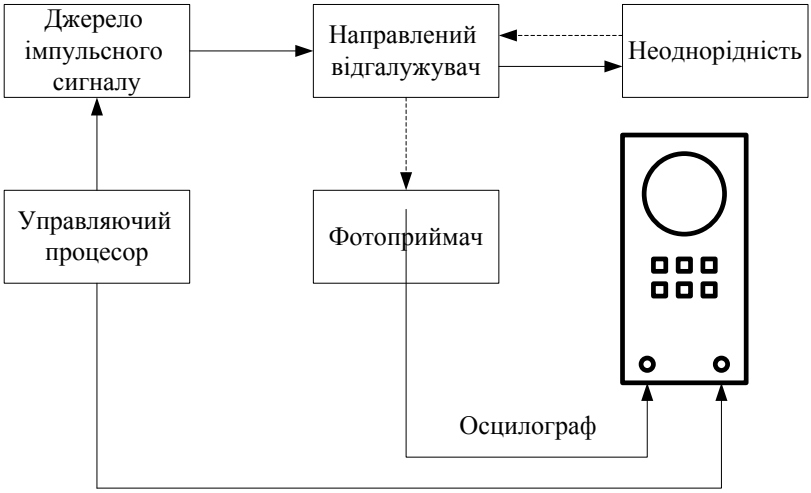


Рис.6.4. Апаратна структура оптичного рефлектометра

6.2.2. Вимірювання параметру перехідного затухання

Параметр перехідного затухання в оптоволоконних лініях вимірюється за допомогою оптичного рефлектометру (*OTDR*). При цьому застосовують наступну схему вимірювань. До одної оптоволоконної лінії підключають генератор імпульсів рефлектометра, а до іншої досліджуваної лінії підключають приймач рефлектометра. Порівнюючи потужність згенерованих імпульсів із потужністю наведених імпульсів, що фіксуються приймачем, можливо оцінити величину перехідного затухання.

6.2.3. Пошук та усунення пошкоджень обладнання оптоволоконних систем

Алгоритм пошуку пошкоджень в обладнанні ВОЛЗ надано на рис.6.5. Пошук пошкоджень слід починати із спроб визначити, до якої частини обладнання – оптичної чи електричної – відноситься виявлена несправність. Для цього за допомогою оптичного вимірювача потужності (*OPM*) вимірюється рівень потужності

оптичного сигналу у різних точках ВОЛЗ, а результати вимірювань порівнюються із нормативними та (або) паспортними даними.

Рис.6.5. Алгоритм пошуку пошкоджень в обладнанні ВОЛЗ

Якщо виміряні рівні оптичної потужності на приймальних кінцях ділянок регенерації знаходяться у межах припустимих норм, то робиться висновок про знаходження несправності у електричній частині обладнання. Якщо виміряні рівні оптичної потужності на передавальних кінцях ділянок регенерації знаходяться у межах припустимих норм у той час, коли потужності оптичних сигналів на приймальних кінцях є меншими за нормовані значення, то робиться висновок про несправність оптоволоконного кабелю.

Пошук несправності оптичного кабелю починається із аналізу його зв'язаності, тобто необхідно упевнитись, що у кабелі відсутні точки розривів або надто великого збільшення параметру затухання. Для цього, якщо кабель невеликої довжини, використовують візуальний дефектоскоп, а на великих ділянках кабелю – оптичний рефлектометр.

Основні слабкі місця оптичного кабелю: несправні конектори, зварки поганої якості, неякісні з'єднання та розриви кабелю. Дефекти у конекторах визначають візуально за допомогою **експлуатаційного мікроскопу.**

Діагностику місць зварювання, локалізацію точок розриву, місць намокнень кабелю, місць виникнення неоднорідностей у структурі кабелю і т.ін. здійснюють за допомогою оптичних рефлектометрів (*OTDR*).

Рефлектограма *OTDR* не тільки надає змогу визначити місце пошкодження кабелю, але і характер пошкодження, оскільки місця зварених вузлів, точки розсіювання енергії від неоднорідностей оптоволокна, з'єднання із конекторами, всілякі розгалуження кабелю відображаються на рефлектограмі як точки збільшення віддзеркалюваної потужності. Характер віддзеркалювання вказує на вид несправності.

6.2.4. Стресове тестування апаратури ВОЛЗ

Будь-яка ВОЛЗ проектується з урахуванням найбільш несприятливих умов її використання. У реальних умовах експлуатації показники роботи системи виявляються, зазвичай, дещо кращими. Тобто, існує певний запас між реально виміряними та гранично припустимими значеннями параметрів ВОЛЗ.

Наприклад, під час проектування ВОЛЗ здійснюють розрахунок так званого енергетичного бюджету оптичного сигналу у лінії при найгірших значеннях параметрів затухання та перехідних завад. Результати такого розрахунку вносять у проектну документацію на лінію. У той же час реально побудована лінія має дещо кращий енергетичний бюджет оптичного сигналу у порівнянні із запроектованим. Під час приймально-здавальних випробувань лінії її реально виміряні параметри вносяться у паспорт ВОЛЗ. Тому неважко визначити різницю між реально існуючими (на момент пуску в експлуатацію) та запроектованими показниками якості функціонування лінії. Ця різниця і визначає потенціальний ресурсний запас реальної лінії щодо можливостей деградації її якості. Знаючи величину цього запасу, можливо, наприклад, визначити, яке саме граничне значення затухання оптичного сигналу притаманне досліджуваній ділянці ВОЛЗ, перевищення котрого призведе до втрати її працездатності.

Для експериментального визначення реального енергетичного запасу оптоволоконної лінії здійснюють так звані **стресові випробування** шляхом імітації несприятливих умов її функціонування. Схема стресових випробувань ВОЛЗ показана на рис.6.6.

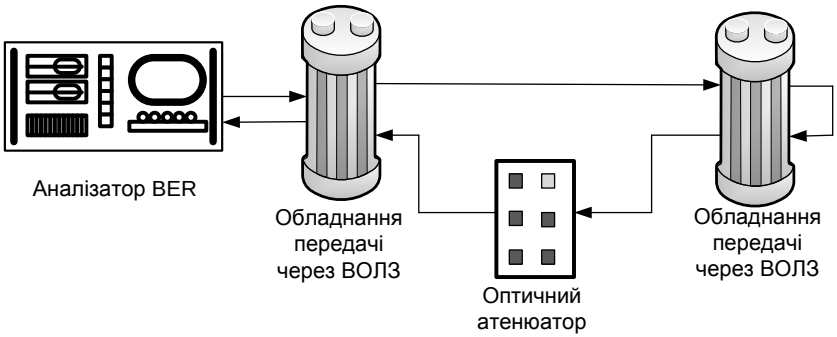


Рис.6.6. Схема стресового тестування ВОЛЗ

Як бачимо на рис.6.6, у лінію передавання оптичного сигналу включають оптичний атенюатор, що здатний вносити з певним кроком змін додаткове затухання в лінію. За допомогою

атенюатора поступово збільшуючи величину додаткового затухання, досягають ситуації, коли у лінію буде внесено гранично припустиме відповідно до технічних умов (ТУ) затухання.

Різниця між досягнутим значенням затухання та значенням затухання, виміряним у реальних умовах функціонування лінії (без атенюатора), і визначає запас лінії щодо потужності оптичного сигналу. Момент досягнення граничного значення затухання можливо визначити і по параметру бітових помилок у цифровому каналі, який неважко утворити на базі ВОЛЗ. Тобто, здійснювати оцінювання запасу потужності оптичного сигналу шляхом вимірювання параметру *BER* у цифровому каналі. На практиці широко використовуються норми на параметр *BER*. Тому за допомогою атенюатора у лінію вноситься така величина затухання, при котрій реально виміряне значення параметру *BER* буде дорівнювати нормативному значенню цього параметру.

6.3. Вимірювання параметрів абонентських ліній зв'язку

6.3.1. Вимірювання параметрів затухання сигналів в абонентській лінії**.** Як вже вказувалось, затуханням називається втрата потужності сигналу під час його проходження уздовж лінії зв'язку. Затухання вимірюють між якимись двома точками лінії, найчастіше – між її протилежними кінцями. Якщо потужності робочих сигналів, що циркулюють у лінії, задано у відносних одиницях (як правило, у *дБ* відносно потужності у 1мВт), то затухання визначають як різницю у *дБ* між відносними рівнями потужності сигналів, що виміряні у цих точках. Якщо ж потужності робочих сигналів у точках вимірювань задано у абсолютних одиницях (наприклад, у *мВт*), то затухання визначають у *дБ* як $10\lg(P_1 / P_2)$, де P_1 та P_2 – потужності сигналів в абсолютних одиницях виміру у точках, між котрими вимірюється затухання.

Існують поняття власного та робочого затухання кабелю. Власне затухання сигналу у кабелі (характеризується параметром A) – це відношення (у децібелах) потужності вхідного сигналу до потужності сигналу на виході кабелю за умови, якщо і джерело сигналів і приймач сигналів, що підключені до кінців кабелю, узгоджені із хвилєвим опором кабелю у всьому робочому діапазоні частот. Тобто, за умов, коли імпеданси (комплексні опори) джерела

та навантаження кабелю співпадають із характеристичним імпедансом цього кабелю. У цьому випадку відсутнє будь-яке відбиття енергії сигналів від кінців кабелю, що сприяє найбільш повному та якісному передаванню сигналів через кабель. Проте навіть у цьому випадку сигнал по мірі його розповсюдження через кабель поступово затухає, оскільки частина енергії сигналу розсіюється у кабелі (зокрема, перетворюється на тепло та випромінюється у зовнішнє середовище). Наприклад, якщо потужність сигналу на виході кабелю P_2 виявилась у 10 разів меншою, ніж потужність вхідного сигналу P_1, то власне затухання A буде дорівнювати $10\lg(P_1/P_2) = 10$дБ, а якщо у 100 разів меншою, то $A = 20$дБ.

Робоче затухання сигналу у кабелі A_p – це відношення (у децібелах) потужності вхідного сигналу до потужності сигналу на виході кабелю у випадках, коли характеристичний імпеданс кабелю не співпадає із імпедансом джерела сигналів або навантаження. Саме такі випадки є характерними для експлуатаційної практики. Через неспівпадіння характеристичного імпедансу лінії із імпедансами пристроїв, що під'єднані до її кінців, виникає ефект відбиття енергії сигналів від цих пристроїв, тобто від джерела вхідних сигналів та від навантаження на лінію. Внаслідок чого на вхід навантаження із лінії потрапляють послаблені сигнали, оскільки частина енергії цих сигналів пішла на утворення сигналів відбиття (що називають луно-сигналами). Тому рівень робочого затухання завжди є більшим, ніж рівень власного затухання лінії.

Примітка 1. Від неузгодженого за імпедансом навантаження у зворотному напрямку назад у лінію поступають луно-сигналами (рос. – эхо-сигналы). Потужність луно-сигналів відносно потужності робочих сигналів у лінії характеризуються параметром, що зветься повернені втрати. Цей параметр розглянуто далі.

Як виміряти параметр затухання? Для цього спочатку вимірюють значення потужності вхідного сигналу P_1, а потім – потужності сигналу на виході кабелю P_2. Якщо при цьому імпеданси джерела вхідних сигналів та навантаження на кабель дорівнюють характеристичному імпедансу кабелю, то мова йде про вимірювання власного затухання кабелю A. Якщо ж імпеданси не є

повністю узгодженими, то вимірюють робоче затухання кабелю A_p. Для вимірювань потужності вхідного сигналу здійснюють наступне. Вхід приймача сигналів, що входить до складу обладнання – навантаження на лінію зв'язку, безпосередньо підключають до виходу джерела сигналів, виключивши із утвореного таким чином ланцюга вимірюваний кабель. Потім (після вимірювань потужності вхідного сигналу) відновлюють лінію зв'язку, тобто між джерелом сигналів та приймачем навантаження включають кабель, і вимірюють потужність сигналу на виході кабелю. Накінець, узявши логарифм відношення P_1/ P_2 (із коефіцієнтом 10 за умов, що узято абсолютні одиниці вимірювання потужності), отримують у дБ шукане значення параметру A або A_p. Якщо ж узято відносні рівні потужності, то тоді параметр A або A_p визначається як різниця у дБ між цими рівнями сигналів.

Слід застерегти від спроб обчислити параметр A для вже прокладеного кабелю по параметру його погонного затухання (тобто, по затуханню, що приведене до одиниці довжини лінії) шляхом вимірювання довжини траси цього кабелю та помноження значення виміряної довжини на погонне затухання кабелю. Слід знати, що більш/менш точно виміряти довжину вже прокладеного кабелю (зокрема, рефлектометром) у типових умовах його експлуатації не є можливою справою (у рефлектометрів є так звана мертва зона). Окрім того, на параметр затухання впливає не тільки довжина кабелю, але і багато інших параметрів (ступень однорідності кабелю, наявність всіляких відводів та розгалуджень, параметри інтерфейсів і т.ін.).

6.3.2. Вимірювання імпедансо-частотної характеристики абонентської лінії

Затухання синусоїдальних сигналів у кабелі суттєво залежить від частоти коливань. У загальному випадку затухання в електричних кабелях збільшується із збільшенням частоти несучого коливання. Тому якщо спектр інформаційного сигналу займає достатньо широку смугу частот, то, скоріш за все, різні синусоїдальні складові спектру сигналу будуть не однаково затухати, що спотворить форму сигналу і негативно відіб'ється на якості передавання сигналів через кабель.

Залежність величини затухання у кабелі від частоти синусоїдальних сигналів, що через нього проходять, відображає так звана **імпедансо-частотна характеристика** (ІЧХ) кабелю на відміну від **амплітудно-частотної характеристики** (АЧХ), яка характеризує підсилюючі можливості будь-якого електричного ланцюга. Зрозуміло, що коли розглядається пасивний ланцюг, у складі якого відсутні будь-які активні підсилюючі пристрої (зокрема, абонентська лінія без регенераторів або із регенераторами, котрі підсилюють сигнал лише до його номінальних значень), більш доцільно користуватися ІЧХ, чим АЧХ.

Виміряти ІЧХ можливо різними шляхами. Один із найбільш зручних шляхів – використати будь-який **аналізатор абонентських ліній** (це - різновид аналізатора ланцюгів, *Network Analyzer*) із широкого спектру пристроїв цього типу, що існують на ринку вимірювальних засобів. Зокрема, такого роду аналізатори можуть розділятися на передавальну та приймальну частини, які під'єднуються відповідно до входу та виходу абонентської лінії. Наприклад, до входу абонентської лінії підключається генератор синусоїдальних коливань, частота котрого автоматично змінюється у наперед заданих межах (так званий, свип-генератор), а до виходу лінії підключається вимірювач рівнів прийнятих сигналів. Результати вимірювань рівнів сигналів подаються на вхід осцилографу, період розгортки котрого узгоджується із діапазоном змін частот генератора синусоїдальних коливань. Однак при цьому слід звернути увагу на робочий діапазон частот такого аналізатору. Якщо досліджується стандартний абонентський телефонний канал тональної частоти, до достатньо забезпечити розгортку ІЧХ у діапазоні від 200Гц до 4кГц. Такий діапазон розгортки може забезпечити будь-який аналізатор аналогових абонентських ліній типу *TDA-5, Line Scout, Auto-TIMS* 111 і т.п. Якщо ж досліджується якість передавання цифрових сигналів уздовж аналогової абонентської лінії (наприклад, досліджується можливість використання абонентської лінії для організації *xDSL*-лінії або *ISDN*-лінії базового доступу), то у цьому разі ІЧХ має бути розгорнута до більш високих частот (в залежності від задіяної технології утворення цифрового абонентського каналу - мінімум до

200кГц, максимум до 2мГц). До аналізаторів абонентських каналів, що забезпечують діапазон розгортки ІЧХ 2мГц (і більше), належать, наприклад, аналізатори *SunSet xDSL*, *CoBRA xDSL* та ін. На екрані індикатора аналізатору, якщо його підключити до відрізку кабелю або до реальної абонентської лінії, відображаються усі суттєві неоднорідності у їхній структурі (зокрема, паралельні відводи, котушки Пупіна, неякісні з'єднання і т.ін.), що може слугувати в якості вихідних даних для вирішення багатьох експлуатаційних завдань. Накінець, якщо ставиться завдання дослідити ІЧХ широкосмугових кабелів (коаксіалів, звитих пар категорій 3, 4, 5, 6, що застосовуються для побудови структурованих кабельних систем), то діапазон розгортки аналізатора ліній в залежності від типу широкосмугового кабелю має бути від 10мГц до 100мГц. Такий широкий діапазон здатні забезпечити аналізатори *E8505*, *965DSP* та ін.

6.3.3. Вимірювання характеристики групового часу сповільнення (ГЧС) абонентської лінії

Не тільки затухання, але і швидкість розповсюдження синусоїдальних сигналів у кабелі у той чи іншій мірі залежить від частоти коливань. Тому якщо спектр інформаційного сигналу займає достатньо широку смугу частот, то різні синусоїдальні складові спектру сигналу можуть не з однаковою швидкістю передаватися через абонентську лінію. Це спотворить форму сигналу. До того ж внаслідок нерівномірності ГЧС можуть з'явитися попереду та позаду від цього сигналу так звані луно-сигнали, які, у свою чергу, можуть мати багатократний характер. Інформаційні сигнали спотвореної форми у процесі передавання „розпливаються" у часі, накладаються один на одний. Виниклі луно-сигнали накладаються на вже спотворені інформаційні сигнали. Більше того, відбиті від кінців абонентської лінії сигнали (у разі, якщо характеристичний імпеданс лінії не співпадає із імпедансами пристроїв, що підключені до її кінців) також накладаються на інформаційні сигнали. Усе це негативно впливає на якість транспортування інформації через кабель.

Примітка 2. Реальна картина сигналів в каналі – ще більш складна. По-перше, окрім вищерозглянутих ефектів, негативний вплив на цю картину робить

нелінійність амплітудної характеристики каналу. Через цю нелінійність виникають спотворення спектрів сигналів, зокрема зникають одні складові спектрів, виникають нові інші. По-друге, на потоки вищеназваних сигналів накладаються також всілякі заважаючі наводи від зовнішніх сигналів, які, наприклад, протікають через суміжні пари проводів. По-третє, роблять суттєвий негативний вплив на сигнали в каналі і різноманітні завади, що носять ймовірнісний характер (флуктуаційні завади, імпульсні завади, широкосмугові завади, короткочасні перерви зв'язку і т. ін.). Накінець, якщо йдеться про дуплексний канал, то у ньому одночасно протікають сигнали різних напрямків передавання і, отже, існує проблема їх якісного розділення.

Залежність величини сповільнення часу передавання синусоїдальних сигналів, що проходять через абонентську лінію, від частоти цих сигналів відображає так звана **характеристика групового часу сповільнення (ГЧС)**. Ця характеристика є похідною від **фазочастотної характеристики** (ФЧХ) лінії. Проте оскільки виміряти ГЧС на практиці значно легше, ніж ФЧХ, тому саме ГЧС отримала широке застосування при вирішенні експлуатаційних завдань на абонентських лініях зв'язку. Для вимірювань ГЧС використовують векторні аналізатори ланцюгів, зокрема аналізатори абонентських ліній, які вже розглядались у цій лекції. Для вимірювання ГЧС (а також інших частотних характеристик лінії) може бути використана схема так званого тонального тестування, коли до обох кінців двопроводової лінії під'єднуються окремі аналізатори. До складу будь-якого аналізатора ліній, як було вже сказано, входить генераторний блок, що здатний посилати у досліджувану лінію послідовності синусоїдальних сигналів з поступово наростаючою частотою, та приймальний блок, що під'єднується до лінії з іншого боку у режимі високоомного підключення без відключення навантаження. У даному випадку приймальний блок вимірює не рівні прийнятих сигналів, а час їхнього проходження через абонентську лінію. Завдяки свипуванню сигналів (тобто, завдяки пилкоподібному режиму роботи генератора синусоїдальних сигналів, коли частота генерації із певним періодом поступово наростає до певного максимального значення, а потім майже миттєво спадає до мінімального значення частоти) на індикаторі приймального блоку можливо побачити розгорнуту характеристику ГЧС, наприклад таку, що зображена на рис. 6.7. Для порівняння на цьому ж рисунку

показана ФЧХ стандартного каналу ТЧ.

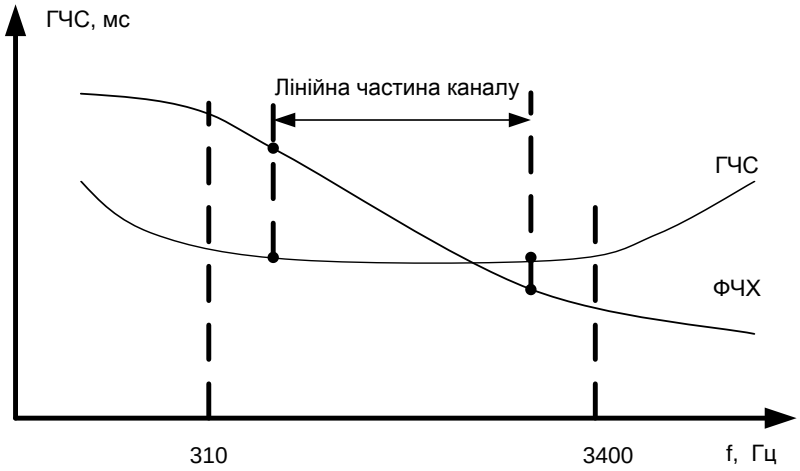


Рис.6.7. Частотні характеристики ГЧС стандартного телефонного каналу тональної частоти

Слід пам’ятати: для якісного передавання сигналів бажано, щоб ФЧХ у смузі каналу була якомога більш лінійною (нехай під певним кутом, але лінійною). Лінійній частині ФЧХ відповідає частина характеристики ГЧС, у межах котрої зберігається однаковість часу сповільнення частотних компонентів спектру сигналів, що транспортуються через канал. Тому, як бачимо на рис.6.7, у смузі пропускання стандартного каналу ТЧ (від 300Гц до 3,4кГц) ФЧХ є майже лінійною, а ГЧС – майже прямою лінією уздовж вісі абсцис. Інша картина на краях смуги пропускання каналу, а тим більш – поза смугою пропускання. Чим ближче до краю смуги, тим більше нерівномірність ГЧС (або тим більша нелінійність ФЧХ). А поза смугою пропускання вид характеристики ГЧС не має суттєвого значення.

Існують стандартизовані норми на припустиму нерівномірність характеристики ГЧС у смузі каналу та на краях цієї смуги. Перевищувати ці норми вкрай небажано, інакше спотворення сигналів в каналі досягнуть величини, коли буде неможливим забезпечити прийнятний рівень параметру помилок в каналі.

6.3.4. Вимірювання перехідного затухання на ближньому та на дальньому кінцях

У даному випадку мова йде про перехідні завади (навіди) між парами проводів у багатоканальному кабелі або між близько розташованими лініями зв'язку. В електромагнітне поле, що утворюється навколо пари провідників, через яку передаються інформаційні сигнали, можуть потрапити інші пари провідників. У цьому разі на цих провідниках виникають небажані електромагнітні навіди, які називають перехідними завадами. Перехідні завади також ще називають перехресними впливами (*crosstalk*). Інтерес представляє співвідношення потужностей: певного інформаційного сигналу, що розповсюджується уздовж одної пари провідників, та сигналу перехідної завади, що виникає на іншій, як правило, суміжній парі провідників як результат електромагнітного наводу від цього інформаційного сигналу. Перехідні завади накладаються на інформаційні сигнали в каналі, що негативно впливає на якість передавання інформації. Ще більш небажані ефекти впливу перехідних завад з'являються, коли канал має високий рівень нелінійності **амплітудної характеристики.** (Амплітудна характеристика каналу – це характеристика залежності амплітуди сигналу на виході каналу від амплітуди сигналу на його вході). У цьому разі виникає інтерференційна взаємодія між інформаційними сигналами та перехідними завадами в каналі, внаслідок чого спектри сигналів можуть кардинально змінитися.

Зрозуміло, що потужність перехідної завади майже завжди є меншою, ніж потужність сигналу, що спричинив цю заваду. Тобто, умовно кажучи, можливо вважати, що сигнал із однієї пари провідників передається на іншу суміжну пару провідників з певним затуханням. Величина цього затухання визначається у *дБ* за допомогою параметру, що називається перехідне затухання. Чим вище значення перехідного затухання, тим краще одна пара проводів ізольована від іншої пари, тим менший вплив перехідних завад на інформаційні сигнали. Величина перехідного затухання залежить від багатьох чинників – від відстані між парами провідників, від ізоляційного матеріалу, що знаходиться між провідниками та парами провідників, від геометрії розташування

провідників у просторі (наприклад, від параметру скрутки у кабелі типу „звита пара"), від неоднорідності та деградацій матеріалу провідників та ізоляції у кабелі, від якості з'єднань між кабелями та конекторами тощо. Тому одна із важливих проблем, яку вимушений вирішувати експлуатаційний персонал, - боротьба із перехідними завадами.

Розрізняють перехідне затухання на ближньому кінці лінії зв'язку (*Near End Crosstalk, NEXT*) та перехідне затухання на дальньому кінці лінії (*Far End Crosstalk, FEXT*).

Як параметр *NEXT*, так і параметр *FEXT* визначають рівень затухання потужності перехідної завади, що наведена на якусь досліджувану пару проводів, відносно рівня потужності сигналу, що проходить по іншій парі проводів. Відмінність між цими параметрами обумовлюється лише місцем знаходження точок вимірювань.

Для визначення параметрів *NEXT* та *FEXT* розглянемо рис.6.8, на котрому зображений двопарний абонентський кабель, що з'єднує приймально-передавальне обладнання двох віддалених один від одного вузлів у межах якоїсь мережі абонентського доступу.

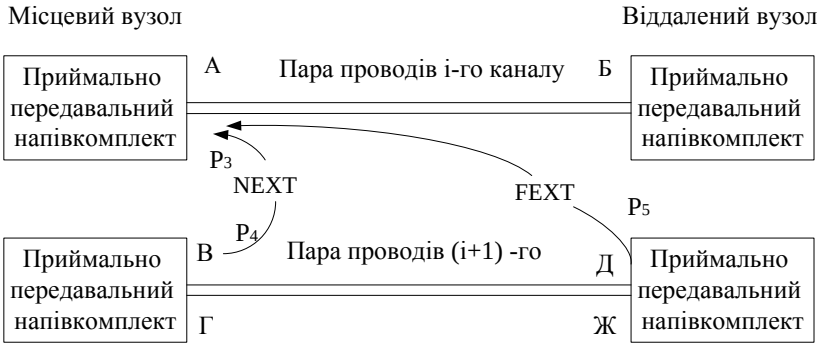


Рис.6.8. Визначення параметрів *NEXT* та *FEXT*

У випадку вимірювань параметру *NEXT* точки вимірювань беруться з одного краю кабелю, а у випадку вимірювань параметру *FEXT* – із різних країв кабелю. Спочатку розглянемо випадок, коли

досліджують перехідні завади тільки між двома парами провідників. Наприклад, вимірюється перехідна завада на парі проводів *i*-го каналу між точками вимірювань А та Б, що наведена від сигналу, котрий передається через іншу пару проводів, наприклад (*i*+*1*)-го каналу.

Різні ділянки будь-якої пари проводів, через які передаються сигнали, у загальному випадку вносять свій окремий внесок у потужність перехідної завади, що вимірюється між точками А та Б. Тому, щоб мати можливість на кількісному рівні оцінити рівень перехідного затухання між точками А та Б, необхідно визначитися із місцем розташування точок вимірювань потужності тих сигналів, що спричинили навіди (на рис.6.8 – це точки вимірювань між В та Г або між Д та Ж). Якщо точки вимірювань джерела перехідної завади обирають з того кінця кабелю, де розташована пара точок вимірювань самої перехідної завади (на рис.6.8 - це – точки між В та Г), то здійснюють вимірювання параметру *NEXT*. Якщо точки вимірювань джерела перехідної завади обирають з протилежного кінця кабелю відносно того краю, де розташована пара точок вимірювань перехідної завади (на рис.6.8 – це точки між Д та Ж), то здійснюють вимірювання параметру *FEXT*. З урахуванням вищезазначеного параметри *NEXT* та *FEXT* визначаються наступним чином:

$$NEXT = 10 \log (P_3 / P_4), [дБ];$$
$$FEXT = 10 \log (P_3 / P_5), [дБ], \qquad (6.1)$$

де P_3 - потужність перехідної завади, P_4 - потужність сигнала - джерела завади на ближньому кінці (між точками В та Г), P_5 - потужність сигнала - джерела завади на дальньому кінці (між точками Д та Ж).

Слід зазначити, що у різних системах зв'язку та за різних умов експлуатації відносний вплив параметрів *NEXT* та *FEXT* на якість передавання інформаційних сигналів може бути різним. За одних умов більш вагомий внесок у потужність перехідної завади робить параметр *FEXT*, в інших – *NEXT*. Однак на практиці здійснюють, головним чином, вимірювання параметру *NEXT*, можливо тому, що вимірювання цього параметру набагато більш легше організувати,

чим вимірювання параметру *FEXT*. Саме для параметра *NEXT* існують стандартизовані норми, що є чинними для багатьох сфер застосування кабельної продукції. Наприклад, у стандарті *TIA TSB-67* наведено стандартизовані формули та норми щодо *NEXT* для абонентських кабелів різних категорій. Зокрема, для звитої пари категорії 5 максимально припустиме значення параметру *NEXT* на частоті 1мГц визначено на рівні *60,0 дБ*, а норма на параметр *NEXT* для цього ж кабелю на частоті 100,0 мГц – *29,3 дБ*, оскільки із збільшенням частоти інформаційних сигналів їх негативний вплив на суміжні пари проводів суттєво збільшується.

Якщо маємо кабель, що містить у собі n пар провідників, то необхідно виконати (n-1) актів вимірювань параметру *NEXT*, щоб дослідити вплив навідів від усіх цих пар на якусь визначену пару провідників у кабелі. Зрозуміло, що це – вельми трудозатратна справа. Тому на практиці використовується метод інтегральної оцінки параметра *NEXT*. У цьому випадку цей параметр позначається як *PS-NEXT* та визначається дещо по іншому. А саме, потужність сумарної перехідної завади вимірюють не відносно потужності сигналу, що цю заваду спричинив, а відносно певним чином обраного номінального рівню потужності, наприклад відносно 1мВт. Тоді параметр *PS-NEXT* визначиться як $10 \log (P_н / P_\Sigma)$, [*дБ*], де P_Σ - потужність перехідних завад від усіх пар провідників у кабелі (у *мВт*), а $P_н = 1$*мВт*.

Вищенаведені визначення та методи вимірювання параметру *NEXT* використовують у випадках, коли пред'явлено підвищені вимоги до точності вимірювань. Проте в експлуатаційній практиці у більшості випадків більш важливою є простота та швидкість вимірювань, ніж їхня точність. У цих випадках параметр *NEXT* вимірюють за допомогою **портативних рефлектометрів металевих кабелів**. При цьому застосовують наступну схему вимірювань. До одної пари провідників підключають генератор імпульсів рефлектометра, а до іншої досліджуваної пари провідників підключають приймач рефлектометра. Порівнюючи потужність згенерованих імпульсів із потужністю наведених імпульсів, що фіксуються приймачем, можливо оцінити величину перехідного затухання.

Методами рефлектометрії здійснюють також так звану **локацію**

втрат *NEXT*, тобто пошук локальних точок (місць розташування) на лінії, де виявились ознаки джерела втрат енергії сигналу під час його проходження через цю лінію. Рефлектометр здатний визначити відстань між кінцем лінії та точками на лінії, де виміряні значення параметру *NEXT* будуть перевищувати максимально припустиме значення цього параметру.

6.3.5. Вимірювання параметру захищеності лінії від перехідних завад

Захищеність лінії зв'язку від перехідних завад визначається тим, наскільки перехідне затухання є більшим за власне затухання цієї лінії. Рівень захищеності конкретної лінії зв'язку із конкретним значенням рівня її затухання - власного A або робочого A_p - від перехідного затухання (рівень котрого, у свою чергу, визначається параметром *PS-NEXT* або в окремих випадках - параметром *NEXT*) характеризує параметр *ACR (Attenuation to Crosstalk Ratio). ACR* – це різниця в *дБ* між параметром *PS-NEXT*, що характеризує сумарний рівень перехідних завад в лінії, та параметром затухання цієї лінії (параметра A або параметра A_p - в залежності від того, чи є узгодженим характеристичний імпеданс лінії із імпедансом навантаження на лінію). **Захищеність лінії щодо перехідних завад** обчислюється за наступною формулою:

$$ACR\ [дБ] = PS\text{-}NEXT\ [дБ] - A_p[дБ]. \qquad (6.2)$$

Практичний інтерес являє залежність параметра *ACR* від частоти. Для визначення цієї залежності побудуємо два графіки частотних залежностей – параметра *PS-NEXT* та параметра A_p (див. рис. 6.9). Як бачимо на рис.6.9, власне (або робоче) затухання самої лінії з ростом частоти збільшується, в той час як перехідне затухання зменшується. У точці перетину графіків значення A_p буде дорівнювати значеню *PS-NEXT*, тобто захищеність лінії у цій точці (значення параметру *ACR*) має нульове значення. Зліва від точки перетину захищеність є позитивною величиною. Чим менше значення частоти, тим краще захищеність. Справа від точки перетину маємо незахищену лінію, оскільки значення параметру *ACR* в цьому випадку завжди буде негативною величиною. З

ростом частоти ситуація тільки погіршується.

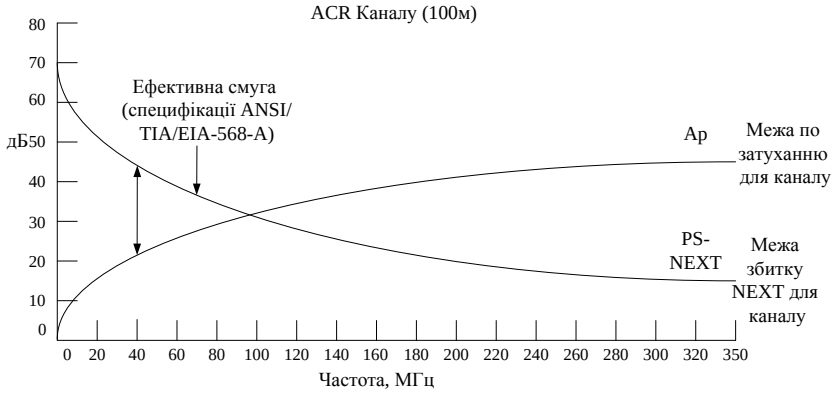


Рис.6.9. Визначення ширини робочої смуги частот лінії зв'язку по частотним залежностям параметрів *PS-NEXT* та A_p

Параметр *ACR* має суттєве практичне значення і широко застосовується на практиці для визначення реальної ширини смуги пропускання частот лінії зв'язку з урахуванням конкретних умов її використання. Треба завжди мати на увазі, що якщо у паспортних даних на кабельну продукцію вказується якась конкретна величина смуги пропускання кабелю, припустимо на рівні *400мГц*, то це зовсім не означає, що лінія зв'язку, яка побудована на основі цього кабелю, буде також мати смугу пропускання *400мГц*. Реальна робоча смуга частот лінії зв'язку буде набагато меншою. Шляхом оцінювання реального значення параметру *ACR* і визначають реальну ширину смуги пропускання частот системи зв'язку. Оцінка здійснюється наступним чином.

Припустимо, що у межах робочої смуги захищеність лінії від перехідних завад (тобто, значення параметру *ACR*), повинна бути не гірше за 10дБ. Іншими словами, той діапазон частот, в межах котрого значення параметру *ACR* не перевищують 10дБ, і є робочою смугою реальної лінії зв'язку.

На рис. 6.9, як було вже сказано, показано дві частотні залежності. Перша - залежність від частоти параметра робочого затухання лінії зв'язку A_p. Друга – частотна залежність параметру

перехідного затухання *PS-NEXT*. Якщо відступати наліво від точки перетину цих залежностей рівно настільки, щоб відстань по вертикалі у *дБ* між кривими, що відображають ці залежності, дорівнювала *10дБ*, то ми знайдемо на вісі частот **верхнє значення робочої смуги пропускання лінії**.

На рис.6.9 бачимо, що точка перетину залежностей знаходиться десь на рівні *138мГц*. Починаємо рухатись від цієї точки наліво до тих пір, поки різниця по вертикалі між двома графічними залежностями, тобто параметр *ACR*, досягне значення *10дБ*. Маємо різницю на вісі ординат між робочим затуханням A_p та параметром втрат *PS-NEXT*, що дорівнює (35 – 25) = 10 [*дБ*]. Ця різниця знаходиться на рівні *100мГц*. От же, верхній край робочої смуги лінії дорівнює *100мГц*.

6.3.6. Вимірювання параметру повернених втрат**.** Як вже вказувалось, через неспівпадіння характеристичного імпедансу лінії із імпедансами пристроїв, що приєднані до її кінців, виникає ефект відбиття енергії сигналів від точок підключення цієї лінії до джерела вхідних сигналів та до навантаження на лінію. У цьому разі в лінії виникають луно-сигнали (рос., – эхо-сигналы). Відбиття енергії сигналів відбувається не тільки від кінців неузгодженої лінії, але також і від будь-яких неоднорідностей, що можуть виникати уздовж лінії. Зрозуміло, що луно-сигнали накладаються на робочі сигнали і, таким чином, заважають нормальному прийому робочих сигналів. Щоб оцінити рівень потужності сигналу, відбитого від якогось конкретного місця неоднорідності у лінії у реальних умовах її експлуатації, вимірюють **параметр** так званих **структурних повернених втрат** (рос., - структурных возвратных потерь) *SRL (Structural Return Loss)*.

Якщо рівні основного та відбитого сигналів задано у *дБ*, то оцінюють різницю між рівнем потужності основного робочого сигналу та рівнем потужності сигналу, відбитого від конкретного місця виниклої неоднорідності. Так, наприклад, якщо рівень основного робочого сигналу у лінії дорівнює *0дБ* (завжди відносно потужності *1мВт*), а рівень відбитого сигналу дорівнює мінус *10дБ*, то різниця між ними, тобто значення параметру *SRL* у цьому випадку буде дорівнювати плюс *10дБ*.

Якщо ж потужності основного та відбитого сигналу задано в

абсолютних одиницях виміру, зокрема у *мВт*, то параметр *SRL* буде визначатися як відношення потужності основного сигналу до потужності відбитого сигналу, котре представляється у *дБ*. Тобто, візьмемо попередній приклад, якщо потужність основного сигналу – (плюс) *1мВт*, а потужність відбитого сигналу – (плюс) *0,1мВт*, то *SRL = 10 lg (1/0,1) = 10 lg (10) =* (плюс)*10 дБ*.

Найбільш часто параметр *SRL* вимірюють у місці з'єднання навантаження із вивідним кінцем лінії, оскільки у цьому випадку параметр *SRL* характеризує ступінь неузгодженості імпедансів лінії та навантаження. Зрозуміло, що чим більша неузгодженість імпедансів, тим більша потужність відбитого луно-сигналу і тим менші виміряні значення параметру *SRL*.

Якщо ставиться завдання оцінити рівень сумарної потужності луно-сигналів, що утворилися внаслідок відбиття енергії основного сигналу від усіх існуючих у лінії неоднорідностей, то тоді мова йде про вимірювання **параметру звичайних повернених втрат** (рос., - возвратных потерь) *RL (Return Loss)*. Параметр *RL* визначається таким же чином, як і параметр *SRL*, тільки у знаменнику визначальної формули береться сума потужностей усіх луно-сигналів, що утворились у лінії.

Слід зазначити, що параметри *RL* та *SRL* суттєво залежать від частоти робочого сигналу. Існуючі норми на параметри *RL* та *SRL* для різних типів та категорій кабелів (зокрема, норми TIA/EIA-568-A та ISO/IEC 1181) враховують цю частотну залежність.

Для оцінювання величини повернених втрат доцільно використати металевий рефлектометр (точніше сказати, - рефлектометр для металевих провідників).

6.3.7. Вимірювання параметрів швидкості розповсюдження сигналів

До групи параметрів, що пов'язані із вимірюваннями швидкості розповсюдження сигналів уздовж ліній зв'язку, відносять **відносну швидкість розповсюдження сигналів** *NVP (Nominal Velocity of Propagation)* (іноді цей параметр позначається як *VOP - Velocity of Propagation*) (мається на увазі відношення реальної швидкості розповсюдження сигналів в каналі відносно швидкості світла у вакуумі), **затримку** у появі сигналів на виводі із лінії відносно

моменту їхнього надходження на увід лінії (параметр *delay*), **розкид затримок** проходження сигналів по різним парам провідників багатопарного кабелю (параметр *Skew*). Усі ці параметри практично не пов'язані із прийнятими технологіями використання обладнання ліній зв'язку на стадії їхньої експлуатації. Існуючі способи вимірювання параметрів розповсюдження потребують достатньо унікальної інструментальної бази. Конкретні величини цих параметрів, як правило наведені у паспортних даних на відповідну кабельну продукцію і практично не змінюються в процесі експлуатації. Усе це обумовило незначний інтерес до експлуатаційних вимірювань цих параметрів. Тим не менш, враховувати паспортні дані на ці параметри при побудові конкретних телекомунікаційних систем (ТКС), а також під час оцінювання величин інших параметрів лінії безумовно необхідно. Наприклад, слід пам'ятати, що американський стандарт *TIA/EIA-568-A* встановлює обмеження на максимально припустиму величину затримки *delay* для звитих пар провідників. Зокрема, для будь-якої пари на частоті 10мГц параметр *delay* повинен не перевищувати *5,7нс/м*. Інакше можуть виникнути проблеми у передаванні даних з використанням технології *Fast Ethernet* навіть при відносно невеликих відстанях передачі. Крім того, слід пам'ятати, що значення параметру *NVP* змінюється приблизно у діапазоні 3% в залежності від температури зовнішнього середовища та від стану ізоляції жил кабелю і являється функцією частоти робочого сигналу в лінії. Значення параметра *NVP* враховується під час калібрування рефлектометрів.

6.3.8. Флуктуаційні та імпульсні завади у лініях зв'язку

Флуктуаційні та імпульсні завади суттєвим чином впливають на якість функціонування систем зв'язку. У межах навчальної дисципліни „Теорія електричного зв'язку" виявлена статистична природа виникнення цих завад, надана їхня класифікація, розглянуто причини та негативні наслідки їхньої появи, методи та засоби боротьби з ними і т.ін. Щодо вимірювань параметрів цих завад, то на стадії експлуатації ТЛК-обладнання вони, здебільшого, не виконуються. Визначення впливу параметрів завад ймовірнісного характеру на якість роботи каналів зв'язку

здійснюється опосередковано шляхом вимірювання параметрів помилок, які виникають внаслідок дії завад. Виняток складають флуктуаційні шуми абонентських телефонних ліній, шумові параметри котрих нормуються та вимірюються (маються на увазі псофометрічні шуми, середньо зважені шуми і т.ін.).

6.3.9. Організація вимірювань на абонентських мережах зв'язку

Наразі проводові мережі абонентського доступу будуються у вигляді структурованих кабельних систем (СКС), головним чином, на основі використання кабелів типу „звита пара" категорії 5. Такий кабель є відносно недорогим та має широку смугу пропускання частот (до *100мГц*), щоб задовольнити будь-які потреби у доступі до будь-яких глобальних транспортних мереж, у т.ч. потреби користувачів телефонних мереж, інтернет-сервісів та широкомовного телебачення.

СКС мають широке застосування. Тому експлуатаційні вимірювання їхніх параметрів являються актуальними. СКС намагаються проектувати та будувати відповідно до певних стандартів, наприклад згідно специфікаціям стандарту *TIA TSB-67,* тому що дотримання стандартизованих норм дозволяє об'єктивно на кількісному рівні оцінити якість функціонування цієї системи.

У рамках цієї лекції ми не будемо розглядати специфікації стандарту *TSB-67*. Проте зазначимо, що цей стандарт визначає стандартні моделі побудови СКС та надає стандартизовані норми на окремі елементи цих моделей. Зокрема, надаються норми на схеми розвіду кабелів, на максимально припустиму довжину цих кабелів, на параметри затухання та на параметр перехідного затухання *NEXT*. Технології експлуатаційних вимірювань СКС (у т.ч., методи тестування, інтерпретація результатів тестування, вимоги до характеристик інструментальних засобів тестування тощо) також висвітлені у стандарті *TIA TSB-67.*

У сучасній практиці знайшли застосування два основних підходи до вимірювань параметрів абонентських ліній зв'язку – тональне або імпульсне тестування. Перший, найбільш функціонально повний та точний спосіб – це вимірювання за схемою тонального тестування із використанням двох аналізаторів абонентських ліній, що приєднуються до обох кінців

двопроводової лінії. За цією схемою аналізуються АЧХ, ІЧХ, ГЧС та практично усі інші вторинні параметри лінії. До складу будь-якого аналізатора ліній входить генераторний блок, що здатний посилати у досліджувану лінію синусоїдальний свип-сигнал, та приймальний блок, що приєднується до лінії з іншого боку. Завдяки свип-сигналу на індикаторі приймального блоку можливо побачити розгорнуті частотні характеристики лінії. Проте вимірювання за цим способом потребують достатньо значних часових витрат та недешевих інструментальних ресурсів. Тому існують більш прості, але менш функціональні варіанти реалізації способу тонального тестування. Зокрема, замість одного із аналізаторів використовують більш простий та дешевий пристрій із неповними можливостями аналізатора, що називається респондером. Наприклад, респондер *TX-1D* являє собою широкосмуговий генераторний модуль, що підключається з одного боку лінії, а управляється аналізатором, що підключений до цієї лінії з іншого боку.

Другий, менш функціональний та менш точний спосіб – це аналіз та вимірювання параметрів лінії за допомогою металевих рефлектометрів, що був розглянутий вище.

6.3.10. Трасування кабелю з використанням активної антени

Роботи із прокладання, заміни або перекросування абонентських кабельних мереж часто зустрічаються в експлуатаційній практиці. Вони характеризуються великими трудовитратами. І тому технології їхнього економного виконання являють практичний інтерес. Зокрема інтерес представляють **методи трасування та кросування кабелів**. Під трасуванням розуміється комплекс вимірювальних робіт, що спрямований на визначення траси пролягання кабелю, а під кросуванням – організація здійснення безпомилкових з'єднань кабелів у кросах.

Розглянемо деякі найбільше розповсюджені методи трасування та кросування абонентських кабелів.

Для трасування кабелю, тобто визначення траси його проходження, часто застосовують в якості інструменту вимірювань вимірювальний комплекс, що складається із передавального та приймального пристроїв з активною антеною. Схема визначення

траси кабелю за допомогою такої пари пристроїв відображена на рис.6.10. Як бачимо, передавач підключається до одного із кінців досліджуваного кабелю (на рис.6.10 - до досліджуваної пари проводів на крос-панелі, що розташована зліва). Цей передавач (*transmitter, T*) генерує сигнал у кабель, а приймач (*receiver, R*) з активною антеною використовується для виявлення цього сигналу шляхом переміщення антени уздовж кабелю. Зрозуміло, у разі відхилення від траси кабелю сигнал, що сприймається антеною, буде послаблюватися. Тому по величині прийнятого сигналу завжди є можливим визначити трасу кабелю, а також його протилежний кінець на правій крос-панелі рис.6.10.

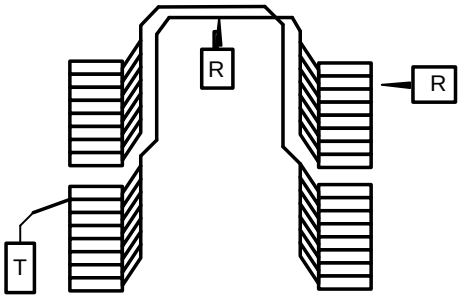


Рис. 6.10. Трасування кабелю за допомогою передавача та приймача з активною антеною

У багатьох випадках втручання у працюючий канал є неприпустимим. Тому перед початком трасування досліджуваний кабель (або пара проводів) звільняється від робочого сигналу, перевіряється відсутність робочого сигналу у цьому кабелі і лише потім до нього підключається передавач. Зрозуміло, що сигнал передавача має суттєво відрізнятися від будь-яких інших сигналів, що можуть транспортуватися через суміжні кабелі (або пари проводів), інакше його неможливо буде відрізнити від інших сигналів.

Аналогічний принцип вимірювань використовується під час визначення місцеположення кінців кабелю (або пари проводів) у шафі кросу. Наприклад, у випадках, коли загублена документація на абонентське кабельне господарство. У цьому разі передавач *T*

підключається до досліджуваної розетки (див. рис.6.11), а приймач *R* забезпечує пошук місця пари у шафі (зрозуміло, що для цього антена не потрібна). Якщо дослідити підключення усіх розеток згідно схеми рис.6.11, то можливо поновити чи перевірити усю кросову документацію.

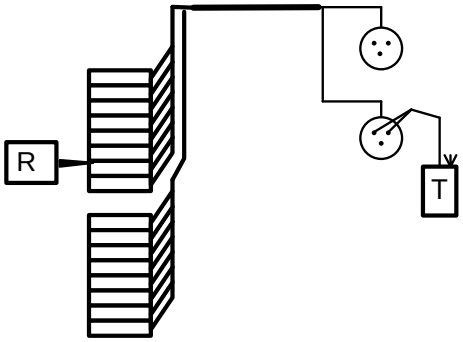


Рис.6.11. Схема пошуку кінців кабелів у кросовому шкафу

Якщо трасування кабелю необхідно здійснювати від розетки (а не від кросового шкафа, як це показано на рис.6.10), то для цього використовують індуктивний давальник, що підключається до приймача *R* замість антени (див. рис.6.12). Клеми досліджуваної розетки перемикають (тобто, організовують шлейф від розетки), а передавальник *T* послідовно по черзі підключають до кінців кабелів (пар проводів), що приєднані до роз'ємів крос-панелі або кросової шафи. При цьому послідовне підключення здійснюють до того часу, поки індуктивний датчик не буде ідентифікувати сигнал.

На практиці часто виникає необхідність розшукати кінець кабелю (або пари проводів) у з'єднанувальній муфті чи розподільчій коробці (наприклад, для підключення додаткових телефоних розеток). У цьому разі застосовують схему вимірювань, що представлена на рис.6.13.

Для трасування кабелю з робочим сигналом використовується неінтерферуючий метод трасування, відображений на рис.6.14, відповідно до якого використовується подача сигналу у пару

земля-кабель.

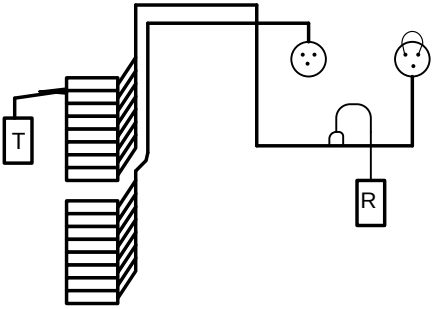


Рис.6.12. Шлейфова схема трасування кабелю за допомогою індуктивного задавальника

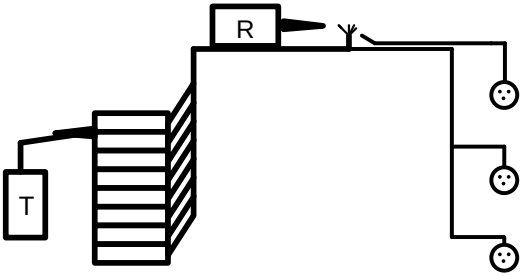


Рис.6.13. Схема пошуку кінця кабелю у розподільчій коробці з використанням активної антени

Вимірювання, що пов'язані з кросуванням кабелів. Для ефективного (тобто, найбільш оперативного та якісного) кросування кабелів між двома віддаленими кросовими шафами використовується спеціалізоване устаткування, яке включає в себе два двоканальні прилади, що працюють сумісно у парі. Точніше, у парі працюють два кросувальника, кожний із котрих користується приладом, що входить до складу цього спеціалізованого обладнання. Один із кросувальників працює з боку першої шафи, а інший – з боку другої шафи. Один із двох каналів обладнання

використовується для організації телефонного зв’язку між кросувальниками (тобто, організується зв'язок через так звану „холодну пару”), а другий канал використовується для кросування методом гальванічного тестування (тобто, «продзвонювання»). Перевагою такого методу у порівнянні з простим «продзвонюванням» є наявність зв’язку у процесі кросування.

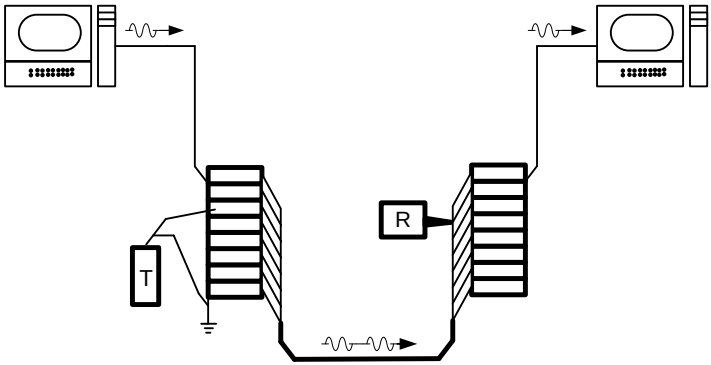


Рис.6.14. Трасування кабелю з використанням неінтерферуючого методу

На рис.6.15 відображені основні схеми вимірювань під час кросування кабелів між кросовими шафами. Навушники на рис.6.15 показують наявність аудіосигналу та мовного зв’язку через гарнітуру, а сам тестовий комплект використовується для аудіо та світлової сигналізації про виявлення кабелю. Існує декілька методів організації кросування. Перший метод (рис. 6.15а) полягає у шлейфовому попарному кросуванні. При цьому один кросувальник забезпечує шлейф (тобто, перемикає пари), а другий відшукує пошкоджені зашлейфовані пари у кросовій шафі. Другий метод (рис. 6.15б) припускає покроковий аналіз кожного із проводів. У цьому випадку один кросувальник (на рис.6.15 той, що з правого боку) заземлює досліджуваний провід, а другий кросувальник (той, що зліва) заземлює один із контактів вимірювача і використовує другий для пошуку заземленого

проводу. Недолік такого методу полягає у тому, що заземлений провід помилково може бути прийнятий за пошуковий. У процесі кросування може також здійснюватися заземлення кабелів (рис. 6.15в), а також аналіз опору лінії чи прикінцевих пристроїв (рис. 6.15г).

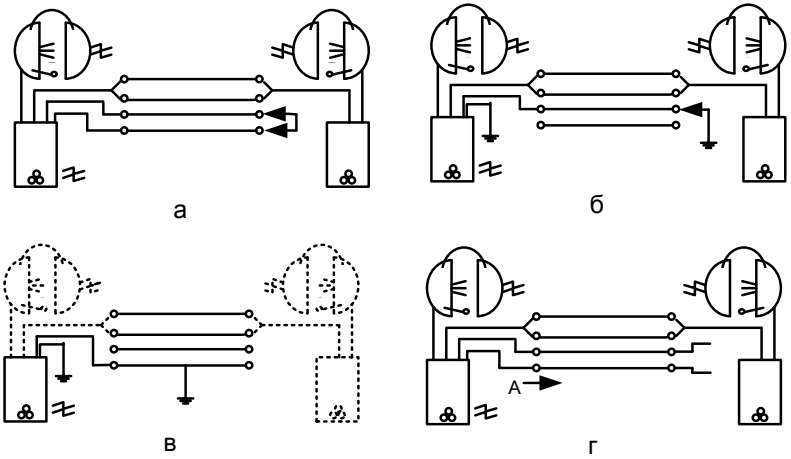


Рис.6.15. Основні схеми кросування кабелів між кросовими шафами

6.3.11. Кабельні імітатори

Імітатори кабелів застосовуються для проведення повномасштабних випробувань:

- вперше розробленого обладнання абонентських ліній;

- на етапі впровадження в експлуатацію нового обладнання абонентських ліній на існуючій структурованій кабельній системі (СКС) з конкретно визначеними характеристиками, якщо є сумніви, що це обладнання здатне нормально функціонувати на цій СКС. Імітатори надають можливість оцінити придатність обладнання до роботи у СКС із заданими параметрами, і, отже, визначити коло потенційних постачальників такого обладнання.

Параметри реальної або еталонної СКС являються параметрами імітації, що мають бути реалізовані імітатором.

Принцип імітації абонентської кабельної лінії зводиться до конструювання фізичної моделі цієї лінії із певного набору фізичних моделей стандартних відрізків (ділянок) абонентської лінії. Ці фізичні моделі (котрі ще називають тестовими шлейфами абонентського кабелю) будуються на основі пасивних компонентів електричних ланцюгів (зокрема, високоточних резісторів, конденсаторів, котушок індуктивності) та імітують ділянки дуплексних ліній із ізотропними (тобто, однорідними) характеристиками. Зрозуміло, що тестові шлейфи мають якомога точніше відображати параметри ділянок реальної абонентської лінії. Тому параметри цих шлейфів специфікуються стандартами, зокрема стандартом *ANSI T1.601/ETSI*.

На ринку інструментальних засобів існують прилади (точніше, комп'ютерізовані інструментальні комплекси), що забезпечують фізичну імітацію будь-яких ділянок абонентських ліній, у т.ч. еталонних тестових шлейфів згідно із стандартом *ANSI T1.601/ETSI*. Ці інструментальні засоби називаються імітаторами кабелів. З використанням імітаторів кабелів існує можливість протестувати роботу обладнання абонентських ліній, такого як обладнання *ISDN, HDSL, ADSL*, аналогових модемів і т.ін.

Конкретна інформація щодо технології користування імітаторами кабелів міститься у відповідних стандартах *ETSI* та *ANSI*. Щоб скласти більш/менш детальне уявлення про імітацію абонентських ліній, слід звернутися до книги І.Г. Бакланова „Методы измерений в системах связи" (М.: ЭКО-ТРЕНДЗ, 1999).

6.4 Вимірювання параметрів аналогових комутованих телефонних каналів

6.4.1. Норми на параметри комутованих телефонних каналів

В експлуатаційній практиці виникає необхідність у вимірюваннях параметрів комутованих телефонних ліній, зокрема з метою визначення їх відповідності певним нормованим значенням. Тому інтерес являють норми на параметри комутованих каналів зв'язку ТМЗК (телефонних мереж загального користування), основні з котрих (але не усі) представлені у табл.6.1. Ці норми слугують для оцінки якості телефонних каналів під час

періодичних експлуатаційних вимірювань. У разі виявлення невідповідності виміряних значень параметрів цим нормам експлуатаційний персонал повинен здійснити заходи щодо пошуку несправної ділянки каналу та усунути причини невідповідності.

Таблиця 6.1

Експлуатаційні норми на електричні параметри каналів комутованих ТМЗК

Найменування електричного параметру	**Норма**	**Примітка**
1. Граничне значення залишкового затухання між абонентами мережі на частоті 1000(1020)*Гц* повинно не перевищувати: - для каналів місцевих (тобто, міських та сільських) і зонових мереж; - для каналів міжміського зв'язку.	30,0 дБ 31,0 дБ	Затухання між кінцевими АТС мережі, куди підключені абоненти, нормуються значенням на 10дБ меншими, тобто відповідно 20,0дБ або 21,0дБ.
2. Імпедансо-частотна характеристика (ІЧХ) каналу нормується на частотах 1800*Гц* та 2400*Гц*. Граничне значення затухання на частотах 1800/2400*Гц* між абонентами повинно не перевищувати: - для каналів місцевих (тобто, міських та сільських) і зонових мереж; - для каналів міжміського зв'язку.	37,0/41,0дБ 38,0/42,0дБ	Затухання між кінцевими АТС мережі, куди підключені абоненти, нормуються значенням на 13,0/15,0 дБ менше.
3. Співвідношення сигнал/шум на виході комутованого каналу на стороні абонента або на АТС повинно не бути менше, ніж наступні значення (*дБ*): - для каналів місцевих (тобто, міських та сільських) і зонових мереж;	25,0 дБ	При вимірюваннях за схемою „абонент-абонент" рівень сигналу вимірювального генератора на частоті 1020*Гц* повинен бути мінус 5 *дБм*.

- для каналів міжміського зв'язку довжиною < 2500 км та довжиною > 2500 км.	25,0 дБ 20,0 дБ	При вимірюваннях за схемою „АТС- АТС" рівень сигналу вимірювального генератора на частоті 1020*Гц* повинен бути мінус 10 *дБм*.
4. Розмах тремтіння фази сигнала (джитер) на частоті 20-300 *Гц*, виміряний на стороні абонента або на АТС, повинен не перевищувати (у градусах).	15 градусів	Те ж саме, що і у попередньому пункті
5.Сумарний вплив короткочасних переривань сигналу (глибиною затухання сигнала більш, ніж 13,0 дБ, та тривалістю менше 300мс) та імпульсних завад (з амплітудою завади більше рівня сигналу) повинен не перевищувати (у відсотках кількості секундних інтервалів, що вражені цими перериваннями або імпульсними завадами, відносно загальної кількості секунд інтервала вимірювань).	30%	
6.Затухання луно-сигнала відносно основного повинно бути не менше нижчевказаних значень (у *дБ*):		
6.1.Відлуння від сигналу розмовляючого суб'єкта (в залежності від місця розташування дифсистеми на абонентській мережі цього суб'єкту): - на міжміській АТС; - на транзитному комутаційному вузлі; - на районній АТС.	 23,0 дБ 20,0 дБ 15,0 дБ	
6.2.Відлуння від сигналу		

слухаючого суб'єкта (в залежності від місця розташування дифсистеми на абонентській мережі цього суб'єкту):		
- на міжміській АТС;	23,0 дБ	
- на транзитному комутаційному вузлі;	20,0 дБ	
- на районній АТС .	15,0 дБ	

Ймовірність виконання вказаних норм повинна бути не гірше 0,9. Тобто, у середньому, на кожні десять актів вимірювань припустимо мати лише один акт, коли результат вимірювань не відповідає нормі. Якщо мова йде про контроль відповідності параметрів транка (тобто, певної множини каналів одного напрямку), то інтерес являє ймовірність відповідності параметрів каналів, що входять до транку, певним нормам. Ця ймовірність повинна бути не гірше 0,9. Тобто, ця норма має виконуватися, у середньому, для кожних дев'яти каналів із десяти.

6.4.2. Методика вимірювань параметрів каналів ТМЗК

Для вимірювань параметрів каналів комутованої ТМЗК можуть бути застосовані прилади будь-якого типу, що придатні для вимірювань параметрів двопроводової аналогової лінії зв'язку. Якщо є можливість, то краще за все використати спеціальний автоматизований програмно-апаратний вимірювальний комплекс (ПАВК), котрий згідно із заданою програмою автоматично встановлює з'єднання, здійснює вимірювання нормованих параметрів у необхідній кількості каналів, виконує статистичну обробку отриманих результатів та обчислює ймовірність відповідності нормам вимірюваного транка каналів. Проте вимірювання можуть здійснюватися за допомогою й інших вимірювальних приладів. Важливо лише, щоб характеристики цих приладів відповідали рекомендаціям МСЕ-Т серії „О". Зокрема, рекомендується застосовувати універсальні вимірювальні прилади, що розраховані на вимірювання параметрів двопроводових каналів комутованої телефонної мережі. Наприклад, прилади типу: *DLM-9*, *DLM-20* фірми *W.G.*, *K.3301* фірми *Siemens* або *ТДА-3* фірми

"*Аналітик-ТС*".

Процедура вимірювань передбачає, що з обох кінців вимірюваного каналу знаходяться спеціалісти-зв'язківці, котрі мають безпосередній телефонний зв'язок між собою. Набір номеру та перемови здійснюються за допомогою телефонних апаратів, потім канал переключається на один із вимірювальних приладів. Після вимірювань одного параметру ці спеціалісти домовляються щодо наступних вимірювань і т.д.

Вимірювання здійснюються, як це видно із табл.6.1, або між парами абонентів одного наскрізного (рос. – сквозного) телефонного каналу, або між парами АТС з підключенням до кінців з'єднувальної міжстанційної (тобто, не абонентської) лінії зв'язку. Після вимірювань параметрів у кожних п'ятнадцяти каналів досліджуваного транку має виконуватися статистична обробка отриманих результатів вимірювань з метою визначення ймовірності дотримання норм.

Вимірювання залишкового затухання здійснюється наступним чином. З одного кінця каналу підключається генератор синусоїдальних сигналів з вихідним опором 600 *Ом*, частотою 1020 *Гц* та рівнем передавання сигналів по потужності мінус 10 *дБм* (на АТС) або мінус 5 *дБм* (у абонента). Припускається використовувати для вимірювань також і частоту 1000 *Гц*, але за умов відсутності у вимірювальному тракті систем ІКМ. На іншому кінці вимірювального каналу має застосовуватися вимірювач рівнів потужності прийнятих сигналів із вхідним опором 600 *Ом*. Тривалість часу одного акту вимірювань – 10 *с*. Протягом цього часу реєструється усереднене значення рівня потужності прийнятого сигналу та обчислюється залишкове затухання сигналу в каналі.

Вимірювання АЧХ, як вже зазначалося (треба згадати, чим визначення АЧХ каналу відрізняється від визначення ІЧХ), здійснюється аналогічно вище вказаному.

Вимірювання відношення сигнал/завада щодо адитивних та мультиплікативних завад здійснюється наступним чином. З одного кінця вимірюваного каналу підключається генератор синусоїдальних сигналів з вихідним опором 600 *Ом*, частотою 1020 *Гц* та рівнем передавання сигналів по потужності мінус 10 *дБм* (на

АТС) або мінус 5 *дБм* (у абонента). Генератор повинен мати коефіцієнт нелінійності не більше 0,5% та рівень захищеності від продуктів паразітної модуляції по ланцюгам електроживлення не менше 60*дБ*. На виході каналу підключається вимірювач рівнів потужності прийнятих сигналів із вхідним опором 600 *Ом*, що має у своєму складі режекторний фільтр на частоті 1020 *Гц* та смуговий фільтр 300 – 3400 *Гц*. Вимірювання виконуються у смузі стандартного телефонного каналу протягом 20 – 30 с. Спочатку вимірюється рівень корисного сигналу на частоті 1020 *Гц* без включення у ланцюг вимірювань режекторного фільтру. Потім включається режекторний фільтр та реєструється усереднене значення сумарних завад у смузі каналу. Шукане відношення сигнал/завада, що характеризує рівень завадозахищеності каналу, обчислюється за формулою

$$P_{с/ш} = P_с - P_ш, \qquad (6.3)$$

де $P_с$ – рівень потужності корисного сигналу на частоті 1020 *Гц*, що віднесений до точки приймання на виході вимірюваного каналу, *дБм*;

$P_ш$ - сумарний рівень потужності адитивних та мультиплікативних завад у смузі каналу, *дБм*.

Примітка. Існують вимірювальні прилади, що одразу фіксують виміряне значення відношення сигнал/завада.

Вимірювання тремтіння фази (джитера). Вимірювання джитеру, як правило, здійснюється за допомогою прилада, що відповідає вимогам рекомендації МСЕ-Т О.91, наступним чином. На вхід каналу підключається генератор синусоїдальних сигналів з вихідним опором 600 *Ом*, частотою 1020 *Гц* та рівнем передавання сигналів по потужності мінус 10 *дБм* (на АТС) або мінус 5 *дБм* (у абонента). На вихід каналу підключається прилад, що здатний вимірювати джитер у смузі 20-300 *Гц*. Реєструється розмах тремтіння фази у кутових градусах. Тривалість акту вимірювань – 20 с.

Вимірювання імпульсних завад здійснюється за допомогою прилада, що відповідає вимогам рекомендації МСЄ-Т О.71, наступним чином. На вхід каналу підключається генератор синусоїдальних сигналів з вихідним опором 600 *Ом*, частотою 1020

Гц та рівнем передавання сигналів по потужності мінус 10 *дБм* (на АТС) або мінус 5 *дБм* (у абонента). На вихід каналу підключається прилад із вхідним опором 600 *Ом*, що здатний фіксувати імпульсні завади, котрі накладаються на прийнятий синусоїдальний сигнал. Поріг фіксації завад встановлюється на рівні приймання синусоїдального сигналу. Встановлюється інтервал вимірювань – 1 хвилина. Реєструється кількість секунд, протягом тривалості котрих прилад зафіксував імпульсні завади (при цьому не є важливим, скільки саме імпульсних завад було виявлено протягом тієї чи іншої секунди). Результатом вимірювань є доля (у відсотках) секунд відносно усіх секунд інтервалу вимірювань, що були вражені імпульсними завадами.

Вимірювання короткочасних переривань здійснюється за допомогою прилада, що відповідає вимогам рекомендації МСЕ-Т О.62, наступним чином. На вхід каналу підключається генератор синусоїдальних сигналів з вихідним опором 600 *Ом*, частотою 1020 *Гц* та рівнем передавання сигналів по потужності мінус 10 *дБм* (на АТС) або мінус 5 *дБм* (у абонента). На вихід каналу підключається прилад із вхідним опором 600 *Ом*, що здатний фіксувати рівні, що на 13 *дБ* нижче, ніж приймальний рівень синусоїдального сигналу. Тобто, поріг фіксації переривань встановлюється на 13 дБ нижче рівня приймання синусоїдального сигналу. Встановлюється інтервал вимірювань – 1 хвилина. Реєструється кількість секунд, протягом тривалості котрих прилад зафіксував короткочасні переривання сигналу (при цьому не є важливим, скільки саме переривань було виявлено протягом тієї чи іншої секунди). Результатом вимірювань є доля (у відсотках) секунд відносно усіх секунд інтервалу вимірювань, що були вражені короткочасними перериваннями сигналу.

Вимірювання луно-сигналів на ближньому кінці. На вхід канала подаються зондуючі радіоімпульси тривалістю 4 *мс* з періодичністю від 100 до 3000 *мс*. Частота заповнення радіоімпульсів – 2000 *Гц*, а рівень потужності – мінус 5 *дБм*. До виходу вимірюваного каналу підключається узгоджувальний опір величиною 600 *Ом*. Зрозуміло, що від дальнього кінця каналу внаслідок неповної узгодженості навантаження на канал відбивається частина енергії корисного сигналу, що

розповсюджується у зворотному напрямі через канал і може бути зафіксована на ближньому кінці каналу у вигляді так званих луно-сигналів. Тому вимірювач луно-сигналів розташовують на ближньому кінці поряд з генератором зондуючих імпульсів. Цей вимірювач спочатку приймає зондуючий радіоімпульс, що використовується, перш за все, для розгортки луно-діаграми у координатах: по вісі абсцис – затримка луно-сигналів у мс; по вісі ординат – затухання луно-сигналів відносно зондуючого імпульсу. Період розгортки вимірювача встановлюється на рівні періоду генерації зондуючих імпульсів. На луно-діаграмі відображається серія луно-сигналів (якщо вони мали місце під час вимірювань), що дозволяє визначити як затримки луно-сигналів, так і їхні рівні відносно зондуючого імпульсу. Вимірювач зазвичай автоматично усереднює отримані значення параметрів луно-сигналів протягом декількох періодів розгортки. Рекомендований інтервал усереднення – 20 – 25 с.

Вимірювання параметрів луно-сигналів у чотирьох проводовій частині каналу (тобто, між АТС) виконується згідно рекомендації *G 122* МСЕ-Т.

Вимірювання луно-сигналів на дальньому кінці. Вимірювання луно-сигналів на дальньому кінці каналу подібні вимірюванням на ближньому кінці. Одна відмінність: вимірювач луно-сигналів встановлюється на дальньому кінці. Оскільки луно-сигнали, що приходять на дальній кінець, багатократно відбиваються від двох дифсистем, то періодичність циклу вимірювань вибирається на рівні 9 с, а загальний інтервал усереднення – 30 с.

Загальна потужність луно-сигналів на дальньому кінці підраховується як сума потужностей окремих луно-сигналів. Луно-сигналами, потужність котрих на 10 *дБ* менше за потужність першого луно-сигналу, як правило, нехтують.

Контрольні питання до шостої лекції

1. Наведіть еквівалентну схему відрізка електричного кабелю.
2. Якими первинними параметрами визначається відрізок електричного кабелю?
3. Який вигляд мають частотні залежності первинних параметрів відрізка електричного кабелю?

4.Як визначити фізичну цілісність кабелю за допомогою звичайного тестера?

5. Чому на практиці вимірюють, головним чином, вторинні параметри кабелю?

6. Яким чином здійснюється вхідний контроль кабелю?

7. Надайте характеристику аналізаторам ланцюгів (*Network Analyzer*).

8. Яким чином здійснюється локалізація місця пошкодження кабелю?

9. Який принцип дії кабелепошукача?

10. Які експлуатаційні завдання доцільно вирішувати за допомогою кабелепошукача?

11. Який принцип дії та функціональні можливості металевого рефлектометра дальньої дії?

12. Які категорії робіт із оптоволоконним обладнанням розрізняють на практиці?

13. Яким чином здійснюється вимірювання оптичної потужност та затухання оптичного сигналу у кабелі?

14. Який принцип дії аналізатора втрат оптичної потужності (*Optical Loss Test Set, OLTS*)?

15. Яким чином оцінюється величина параметрів затухання в оптичній лінії?

16. Який принцип дії оптичного рефлектометра (*Optical Time Domain Reflectometer, OTDR*)?

17. Яким чином вимірюється перехідне затухання в оптоволоконних лініях?

18. Наведіть алгоритм пошуку пошкоджень в обладнанні ВОЛЗ.

19. Яким чином здійснюється стресове тестування апаратури ВОЛЗ?

20. Що таке власне та робоче затухання кабелю?

21. Як вимірюються параметри затухання сигналів в абонентській лінії?

22. Як вимірюються імпедансо-частотні характеристики абонентської лінії?

23. Які функціональні можливості аналізаторів абонентських ліній?

24. Як виміряти характеристики групового часу сповільнення

(ГЧС) абонентської лінії?

25. Як виміряти перехідне затухання на ближньому та на дальньому кінцях?

26. Як виміряти параметр *NEXT* за допомогою портативного рефлектометру металевих кабелів?

27. Як виміряти параметр захищеності лінії від перехідних завад?

28. Як визначити робочу смугу частот лінії через визначення параметру *ACR*?

29. Як виміряти параметр повернених втрат *SRL (Structural Return Loss)*?

30. Як виміряти швидкість розповсюдження сигналів?

31. Що таке тональне або імпульсне тестування параметрів абонентських ліній?

32. Як здійснюється трасування кабелю з використанням активної антени?

33. Як здійснюється пошук кінців кабелів у кросовому шкафу?

34. Які сфери застосування кабельних імітаторів?

35. Які параметри комутованих телефонних каналів нормуються?

36. У чому сутність методики вимірювань параметрів каналів ТМЗК?

Література до шостої лекції

1) И.Г. Бакланов. Технологии измерений в современных телекоммуникациях. –М.: ЭКО-ТРЕНДЗ, 1998. Розділи 4, 5 та 10.2.

2) И.Г. Бакланов. Методы измерений в системах связи. -М.: Эко-Трендз, 1999.

3) А.Б. Семёнов, С.Н. Стрижаков, И.Р. Сунчелей. Структурированные кабельные системы. –М.: ДМК Пресс, 2002. Розділ 2.

САМОСТІЙНЕ ЗАНЯТТЯ ЗА МАТЕРІАЛАМИ ЛЕКЦІЇ №6

6.5. Вимірювання параметрів обладнання цифрових систем передачі (ЦСП), що побудовані за технологіями *PDH/SDH*

Розглянемо особливості вимірювання параметрів бінарних цифрових потоків (зокрема, бінарного потоку типу *E1*), що циркулюють каналами систем передавання із часовим ущільненням стандартних цифрових каналів.

6.5.1. Загальні відомості щодо вимірювань параметрів ЦСП

На стадії експлуатації обладнання ЦСП вимірюються як власне параметри цифрових систем передавання (такі, наприклад, як параметри готовності та деградації цифрового каналу, параметри бітових та блокових помилок, параметри розсинхронізації тощо), так і характеристики циклової структури інформації, що передається первинними каналами (зокрема, здійснюється аналіз протоколів передавання блоків ЦСП).

У цифрових системах передачі, як відомо, застосовуються різноманітні типи модуляції та багаторівневого лінійного кодування сигналів, проте прикінцеве обладнання цих систем використовує бінарний цифровий канал (див. рис. 6.16).

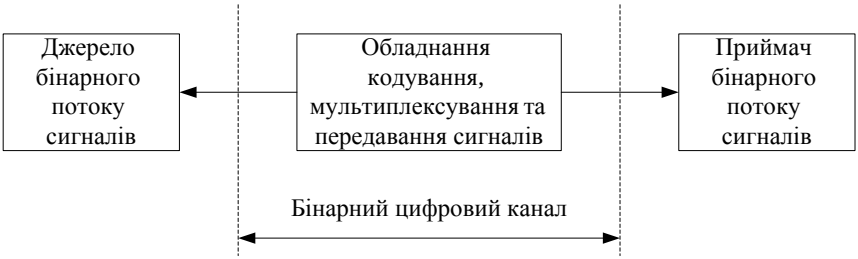


Рис.6.16. До визначення бінарного цифрового каналу

Основне призначення **бінарного цифрового каналу** – це передавання цифрової інформації у двійковій формі, тобто у вигляді потоку бітів. Тому визначальні параметри якості такого

каналу мають бути пов'язані із параметром помилки за бітами *BER* (*Bit Error Rate*) та його похідними. Параметр *BER* вважається одним із основних визначальних параметрів канального рівню у будь-якій системі передавання цифрових даних. Дійсно, із теорії електрозв'язку звісно, що вичерпною (тобто, найбільш повною) характеристикою якості будь-якого бінарного цифрового каналу є функція розподілу ймовірності виникнення помилок у часі *p(t)*, що є характерною для цього каналу. Проте функція *p(t)* – це теоретична абстракція, яку неможливо точно виміряти. Більш реально здійснити оцінку математичного очікування від цієї характеристики, тобто оцінку

$M(p(t)) = \int^{+\infty} p(t)dt$, яка асимптотично сходиться до

$$M(p(\bar{t})) = \int^{t} p(t)dt \quad . \tag{6.4}$$

Якщо задатися конкретним достатньо великим значенням часового інтервалу $[t_1, t_2]$, то стане можливим більш/менш точно визначити оцінку математичного чекання *M(p(t))* і, отже, від теоретичних абстракцій перейти до конкретних вимірювань параметрів якості бінарного цифрового каналу. Параметр *BER*, виміряний на інтервалі $[t_1, t_2]$, представляє середню кількість помилок, що виникли в каналі протягом цього інтервалу вимірювань. Отже, він і є оцінкою математичного чекання функції *p(t)*, тобто

$$BER = M(p(t)) = BITS_{err} / BITS_{\sum}, \tag{6.5}$$

де $BITS_{err}$ - кількість бітів, вражених помилками на інтервалі $[t_1, t_2]$;

$BITS_{\sum}$ - загальна кількість переданих бітів на цьому інтервалі.

Таким чином, найбільш суттєвою характеристикою якості бінарного цифрового каналу, яку реально можливо визначити під час його експлуатації, є параметр *BER*. Методики вимірювань цього параметру широко застосовуються на практиці, а сам параметр, окрім вищенаведеної, має й інші назви, зокрема такі як коефіцієнт помилок за бітами, частота (частість) бітових помилок, швидкість бітових помилок або іншу англійську назву *RATE*.

Параметр *BER* – це відношення кількості виниклих бітових помилок до загальної кількості бітів, що були передані через досліджуваний цифровий канал протягом наперед визначеного інтервалу часу і за умов, що цей канал був у стані готовності. Підкреслимо, що ті помилкові біти, що були виявлені у стані неготовності каналу, мають не враховуватися. Визначення прийнятної величини інтервалу часу вимірювань, а також умов, за яких цифровий канал можливо вважати, що він знаходиться у стані готовності, є відповідальним завданням, оскільки від цих визначень залежить точність і, навіть, сам сенс вимірювань.

Аналіз виразу (6.5) показує, що чим більший інтервал часу вимірювань, тим більше параметр *BER* наближається до істинного значення теоретичної величини метематичного чекання функції *p(t).* На результат оцінки середнього значення випадкової функції *p(t)* також впливають особливості тонкої структури потоку бітів, що просувається через цифровий канал, зокрема тривалість та розмах пульсацій бітового трафіку. При різних значеннях параметрів, що характеризують внутрішню структуру бітових потоків в каналі, за інших рівних умов можуть бути отримані неоднакові значення параметру *BER*. Тому значну увагу слід приділити коректному вибору тестових бітових послідовностей, що мають використовуватися під час вимірювань. Ці послідовності повинні більш/менш точно відображати характер реальних бітових потоків, що притаманні для досліджуваного цифрового каналу.

6.5.2. Вимірювання із відключенням та без відключення бінарного каналу від корисного навантаження

Розрізняють два основних методологічних підходи до вимірювань бінарного каналу – з відключенням та без відключення цього каналу від корисного навантаження.

Вимірювання з відключенням каналу передбачають, що на період вимірювань реальний клієнтський трафік від каналу відключається, а на його вхід подається певним чином сформована тестова послідовність бінарних сигналів. Передбачається, що в процесі проходження цієї тестової послідовності через досліджуваний канал вона піддається певній деформації через вплив всілякого роду негативних факторів. На приймальному боці

за допомогою спеціалізованих інструментальних засобів ці деформації виявляються, а параметри деформацій, зокрема параметри виниклих помилок, вимірюються. Саме за цією методологією вимірюється параметр *BER*. Зрозуміло, що коректність вимірювань може бути досягнена лише за умов синхронізації між собою переданих та прийнятих тестових послідовностей.

Вимірювання без відключення каналу не передбачають необхідність відключення реального трафіку від вимірюваного каналу. У цьому випадку параметри деформацій бітового потоку визначаються шляхом аналізу реального трафіку, що просувається через вимірюваний канал, за допомогою спеціальних алгоритмів аналізу. Вимірювання без відключення каналу часто називають пасивним моніторингом каналу, що здійснюється певним інструментальним засобом, наприклад аналізатором цифрового каналу, котрий приєднується до виходу бінарного каналу паралельно із приймальним засобом цифрової системи передачі у режимі так званого високоомного підключення. За схемою без відключення корисного навантаження на канал виміряти параметр *BER* не є можливим, оскільки на приймальній стороні точно невідомо, яка саме бітова послідовність була спрямована на вхід вимірюваного каналу. Тому у цьому випадку замість параметру помилки за бітами доцільно узяти параметр помилки за так званим кодом *CRC*, тобто узяти параметр *CRC ERR*, що може бути виміряний без відключення каналу та без передавання тестової послідовності бітів. Визначення цього параметру надано далі.

Якщо порівнювати між собою дві вищезазначені методології вимірювань (з відключенням або без відключення каналу), то на стадії експлуатації обладнання з економічної точки зору бажано його не відключувати від корисного навантаження, тобто здійснювати вимірювання без відключення бінарного цифрового каналу. Однак у цьому випадку не існує можливостей безпосереднього порівняння на приймальній стороні переданої послідовності бітів із прийнятою, тому що для реальних умов передавання інформації не існує способів точного визначення на приймальній стороні того, що саме було передано. За цих умов доводиться використовувати опосередковані способи вимірювань

якості бінарного каналу, зокрема параметрів помилок, яким, на жаль, притаманне широке поле невизначеності щодо гарантованості отриманих оцінок точності вимірювань. Інша справа із вимірюваннями, коли існує можливість відключити корисний трафік від робочого бінарного каналу. У цьому випадку можливе безпосереднє порівняння на приймальній стороні переданої тестової послідовності із прийнятою послідовністю, що дозволяє гарантовано визначити параметр *BER* з точністю до однієї бітової помилки.

6.5.3. Основні параметри бінарного цифрового каналу

Усю множину параметрів бінарного цифрового каналу умовно розподіляють на дев'ять груп, визначення котрих надано нижче:

1) чотири параметри готовності/неготовності каналу – ***AS, AS(%), UAS, UAS(%)***;

2) два параметри кількості бітових помилок - ***BIT ERR*** (або скорочено ***BIT***), ***BER*** (або інша назва цього параметру ***RATE***);

3) вісім параметрів тривалості бітових помилок – ***ES, EFS, ES(%), EFS(%), ESR, SES, SES(%), SESR***;

4) чотири параметри кількості блокових помилок – ***EB, BLER, BBE, BBER***;

5) два параметри помилок *CRC* - ***CRC ERR, CRC RATE***;

6) два параметри розсинхронізації - ***CLKSLIP*** (або скорочено ***SLIP***), ***CLKSLIPS*** (або скорочено ***SLIPS***);

7) два параметри деградації якості робочого каналу – ***DGRM, DGRM(%)***;

8) один параметр пов'язаності каналу - ***LOSS***;

9) два параметри якості передавання тестової послідовності – ***PATL, PATLS***.

Усі параметри визначаються згідно з рекомендаціями МСЕ-Т (*ITU-T*) *G.821, G.826, M.2100* та *M.2101*.

В експлуатаційній практиці прийнята англійська абревіатура назв цих параметрів.

Усі вищеназвані параметри бінарного каналу широко застосовуються на практиці. Тому детально пояснемо сенс кожного з них.

6.5.4. Параметри готовності/неготовності каналу

1) ***AS (availability seconds)* – секунди готовності каналу [*c*]**. Це проміжок часу, впродовж котрого спостерігаються зовнішні ознаки нормального функціонування цього каналу, зокрема коли існує кон'юнкція наступних трьох подій: по-перше, на приймальній стороні фіксується наявність несучої сигналу; по-друге, спостерігається нормальна робота системи циклової синхронізації; по-третє, кількість суміжних секунд, вражених помилками (тобто, послідовно розташованих у часі секунд, протягом кожної із котрих виявлялись помилки), не перевищує наперед визначеного порогового значення. Наприклад, згідно із рекомендацією *G.821* канал переходить у стан неготовності, якщо виявлено десять і більше суміжних секунд, протягом котрих спостерігались помилки у прийманні бітів. Зрозуміло, якщо із загального часу сеансу зв'язку (зокрема, із загального часу проходження тестової послідовності) відняти проміжки часу неготовності каналу, то отримаємо значення параметру *AS*.

2) ***AS(%) (availability seconds, percents)* – відсоток часу готовності каналу [%].** Це – кількість секунд готовності каналу, що виміряна відносно тривалості сеансу зв'язку (або тривалості проходження всієї тестової послідовності). Цей параметр у значній мірі характеризує рівень якості цифрового бінарного каналу, оскільки надає уявлення про тривалість проміжку часу, коли канал здатний нормально функціонувати, у порівнянні із загальною тривалістю сеансу зв'язку.

3) ***UAS (unavailability seconds)* – секунди неготовності каналу [*c*]**. Це - проміжок часу, впродовж котрого спостерігаються зовнішні ознаки ненормального функціонування цього каналу, зокрема спостерігається хоча б одна із наступних трьох подій: або на приймальній стороні фіксується втрата несучої сигналу; або спостерігається порушення нормальної роботи системи циклової синхронізації; або кількість суміжних секунд, вражених помилками (тобто, послідовно розташованих у часі секунд, протягом кожної із котрих виявлялись помилки), перевищує наперед визначене порогове значення. Наприклад, згідно із рекомендацією *G.821* канал переходить у стан неготовності, якщо виявлено десять і більше суміжних секунд, протягом котрих

спостерігались помилки у прийманні бітів, або з моменту втрати несучої, або з моменти втрати синхронізації. Зрозуміло, якщо із загального часу сеансу зв'язку (зокрема, із загального часу проходження тестової послідовності) відняти проміжки часу неготовності каналу *UAS*, то отримаємо значення параметру *AS*, тобто має місце наступне співвідношення:

$$T_{сеанс} = AS + UAS, \qquad (6.6)$$

де $T_{сеанс}$ – тривалість сеансу зв'язку (сеансу вимірювань).

4) ***UAS(%) (unavailability seconds, percents)*** **- відсоток часу неготовності каналу [%].** Це – кількість секунд неготовності каналу, що виміряна відносно тривалості сеансу зв'язку (або тривалості проходження всієї тестової послідовності). Цей параметр, як і параметр *AS(%)*, характеризує рівень якості цифрового бінарного каналу. Справедливе наступне співвідношення:

$$AS(\%) + UAS(\%) = 100\%.. \qquad (6.7)$$

6.5.5. Параметри кількості бітових помилок

1) ***BIT ERR (bit errors)*** або скорочено ***BIT*** **– кількість бітових помилок [безрозмірна величина]**. Це – кількість помилково прийнятих бітів, що були виявлені протягом сеансу зв'язку (протягом проходження тестової послідовності). Бітові помилки підраховуються тільки під час перебування цифрового каналу у стані готовності *AS*. *BIT* – це чисельник у виразі, що визначає величину параметра *BER*.

2) ***BER (bit error rate)*** або скорочено ***RATE*** **– коефіцієнт бітових помилок (частота бітових помилок, параметр помилок за бітами)** [безрозмірна величина]. Це – основний параметр якості цифрового бітового каналу. Визначається як відношення кількості бітових помилок до загальної кількості бітів, що були передані через канал протягом одного сеансу зв'язку (або протягом проходження однієї тестової послідовності). При цьому канал має бути у стані готовності. При виявленні десяти послідовних секунд з помилками, підрахунок параметра *BIT* припиняється, а аналізатор

переключається на підрахунок параметру *UAS* (тобто, на підрахунок проміжку часу неготовності каналу). Як тільки працездатність працездатність каналу буде відновлена (тобто, як тільки канал знову повернеться до стану готовності) підрахунок кількості помилково прийнятих бітів буде продовжений. І так – до кінця сеансу зв'язку.

6.5.6. Параметри тривалості бітових помилок

1) ***ES (errors seconds)* – секунди з помилками [*c*]**. Це - проміжок часу (виміряний у секундах), впродовж котрого спостерігаються помилки усіх видів у каналі, котрий знаходиться у стані готовності. Тобто, *ES* – це кількість секунд з помилками, що виявлені серед усіх секунд готовності каналу *AS*. Секунди з помилками, що виявлені у стані неготовності каналу *UAS*, не враховуються.

2) ***EFS (error free seconds)* – секунди роботи каналу без помилок [*c*]**. Це - проміжок часу (виміряний у секундах), впродовж котрого спостерігалась безпомилкова робота каналу, котрий знаходився у стані готовності. Тобто, *EFS* – це загальна кількість секунд перебування каналу у стані безпомилкової роботи. Секунди без помилок, що виявлені у стані неготовності каналу *UAS*, не враховуються. Справедливе наступне співвідношення:

$$AS = ES + EFS. \tag{6.8}$$

3) ***ES(%) (errors seconds, percents)* – відсоток секунд з помилками [*c*].** Це – кількість секунд з помилками *ES*, що виміряна відносно тривалості сеансу зв'язку (або тривалості проходження всієї тестової послідовності). Секунди неготовності каналу не враховуються.

4) ***EFS(%) (error free seconds, percents)* – відсоток секунд роботи каналу без помилок [*c*]**. Це - загальна кількість секунд перебування каналу у стані безпомилкової роботи, що виміряна відносно тривалості сеансу зв'язку (або тривалості проходження всієї тестової послідовності). Секунди неготовності каналу не враховуються. Справедливе наступне співвідношення:

$$AS[\%] = ES[\%] + EFS[\%]. \quad (6.9)$$

5) ***ESR (errors seconds rate)* – коефіцієнт помилок щодо секунд з помилками [безрозмірна величина].** Це – відносна кількість секунд з помилками *ES* щодо загальної кількості секунд у *AS*. Тобто, параметр *ESR* є ідентичним параметру *ES[%]*, але виміряний не у відсотках.

6) ***SES (severally errors seconds)* - секунди з багатократними помилками [*c*].** Це - це кількість секунд з багатократними помилками, що виявлені серед усіх секунд готовності каналу *AS*. Тобто, *SES* – це проміжок часу, виміряний у секундах, впродовж тривалості кожної із цих секунд спостерігалась не одна, а кілька помилок. Секунди з багатократними помилками, що виявлені у стані неготовності каналу *UAS*, не враховуються.

Згідно рекомендації *G.821* параметр *SES* вимірюється за умови, що $BER > 10^{-3}$.

Існує й інша інтерпретація правила підрахунку кількості секунд, що уражені багатократними помилками, а саме, враховуються тільки ті секунди, протягом тривалості котрих було виявлено більше 30% блоків із помилками.

7) ***SES(%) (severally errors seconds, percents)* – відсоток секунд з багатократними помилками [*c*].** Це – кількість секунд з багатократними помилками *SES*, що виміряна відносно тривалості сеансу зв'язку (або тривалості проходження всієї тестової послідовності). Секунди неготовності каналу не враховуються.

8) ***SESR (severally errors seconds rate)* - коефіцієнт помилок щодо секунд з багатократними помилками [безрозмірна величина].** Це – відносна кількість секунд з багатократними помилками *SES* щодо загальної кількості секунд у *AS*. Тобто, параметр *SESR* є ідентичним параметру *SES[%]*, але виміряний не у відсотках.

6.5.7. Параметри кількості блокових помилок

1) ***EB (error block)* – кількість помилкових блоків [безрозмірна величина]**. Це – кількість помилково прийнятих блоків з бітовими послідовностями, що були виявлені протягом сеансу зв'язку (або протягом проходження тестової послідовності

блоків, якщо вимірювання проводилися у режимі тестування із відключенням каналу від корисного навантаження). Помилковим вважається блок, що містить у собі хоча б один помилковий біт. Помилкові блоки підраховуються тільки під час перебування цифрового каналу у стані готовності *AS*. *EB* – це чисельник у виразі, що визначає величину *BLER*.

2) ***BLER (block error rate)* – коефіцієнт блокових помилок (частота або частість блокових помилок) [безрозмірна величина]**. Це – відношення кількості помилково прийнятих блоків до загальної кількості блоків, що були транспортовані через канал протягом одного сеансу зв'язку. Цей параметр доцільно вимірювати у мережах передачі даних за умов, коли передаються блоки фіксованої довжини.

3) ***BBE (background block error)* – блок із фоновою помилкою.** Це – блок з помилками, але такий, що не може бути віднесений до секунд із багатократними помилками (до *SES*)**.** Тобто, такий блок був виявлений, коли значення параметру *BER* було менше, ніж 10^{-3}, або був виявлений на односекундних інтервалах, що містять менше 30% блоків із помилками.

4) ***BBER (background block error rate)* – коефіцієнт фонових блокових помилок [безрозмірна величина]**. Це – відношення кількості прийнятих блоків із фоновими помилками до загальної кількості блоків, що були транспортовані через канал протягом одного сеансу зв'язку. При цьому канал має бути у стані готовності, а блоки із багатократними помилками, що включені до проміжків часу *SES*, не враховуються.

6.5.8. Параметри помилок CRC

1) ***CRC ERR (cyclic redundancy code error)* – кількість помилок *CRC*.** Це – кількість помилок, що були виявлені протягом одного сеансу зв'язку у реально працюючому каналі без його відключення завдяки використанню циклового надлишкового коду (*CRC*). Необхідна умова вимірювань параметру *CRC ERR* – наявність механізму формування коду *CRC* на передавальній стороні та механізму аналізу коду *CRC* на приймальній стороні.

Слід підкреслити, що параметр *CRC ERR* дає менш точне уявлення, ніж параметр *BER*, про рівень помилок у цифровому

бінарному каналі. Будь-яка виявлена помилка *CRC* не обов'язково пов'язана із однією бітовою помилкою, оскільки при передаванні одного блоку можуть виникнути декілька бітових помилок, однак *CRC*-механізм у цьому випадку зафіксує лише одну помилку *CRC*. Окрім цього, кілька бітових помилок можуть компенсувати одна одну і не увійти у сумарну оцінку *CRC ERR*. Усе це негативно впливає на точність оцінки рівня помилок в каналі. Проте застосування механізму *CRC* надає можливість контролювати рівень помилок в каналі без його відключення від корисного навантаження.

2) ***CRC RATE (CRC errors rate)* – частота помилок *CRC* в каналі [безрозмірна величина]**. Це - – відношення кількості помилок *CRC* до загальної кількості бітів, що були транспортовані через канал протягом одного сеансу зв'язку. Тобто, параметр *CRC RATE* характеризує середню частоту помилок *CRC* в каналі.

6.5.9. Параметри розсинхронізації

1) ***CLKSLIP (clock slips)*** або скорочено ***SLIP* – кількість тактових прослизань** (рос. – проскальзываний) **[безрозмірна величина]**. Параметр, що характеризує кількість синхронних керованих прослизань, що виявились з моменту початку тестування. Прослизання – це небажаний повтор або втрата групи суміжних бітів у синхронній або плезіохронній бітовій послідовності внаслідок виникнення неспівпадіння між швидкостями читання та запису у буферній пам'яті. Прослизання є однією із основних причин втрати циклової синхронізації. На практиці в обладнанні *SDH/PDH* знайшли застосування так звані еластичні керовані буфери, які здатні керувати прослизаннями. У цьому випадку мова йде про керовані прослизання. Інтерес до вимірювань параметру *SLIP* пов'язаний, перш за все, із спробами виявити причини переходу каналу у стан неготовності (якщо таке мало місце). Якщо, наприклад, спостерігається одночасне підвищення значень параметрів *SLIP* та *UAS*, то з великою ймовірністю можливо стверджувати, що причиною переходу каналу у стан неготовності є підвищений рівень кількості тактових прослизань.

2) ***CLKSLIPS (clock slips seconds)*** або скорочено ***SLIPS* –**

тривалість тактових прослизань[с]. Це – сумарний час у секундах спостерігання синхронних керованих тактових прослизань, що мали місце протягом усього періоду тестування.

6.5.10. Параметри деградації якості робочого каналу

1) ***DGRM (degraded minutes)* – кількість хвилин деградації якості [*хв*].** Це - кількість однохвилинних інтервалів протягом одного сеансу тестування, що були уражені кількома помилками кожний, однак при цьому канал був у стані готовності, а середня кількість бітових помилок (тобто, значення параметра *BER*) не перевищувала 10^{-6}. Іншими словами, йдеться про ситуацію, коли канал загалом знаходиться у працездатному стані (з невисоким рівнем бітових помилок, оскільки значення параметру *BER* є не гірше за 10^{-6}), однак іноді виникають більш/менш тривалі періоди виникнення помилок, що не порушують стан готовності каналу, але призводять до тимчасової деградації якості каналу. Сумарну тривалість часових проміжків такої деградації визначає параметр *DGRM*.

2) ***DGRM(%) (degraded minutes, percents)* - відсоток хвилин деградації якості [%].** Це – кількість хвилин деградації якості, що представлена у відсотках відносно загальної кількості хвилин, що зайняв процес тестування.

6.5.11. Параметри пов'язаності каналу

1) ***LOSS (loss of signal seconds)* – тривалість втрати сигналу [*с*].** Цей параметр характеризує тривалість часу, протягом котрого сигнал було втрачено. Якщо сигнал на приймальній стороні не виявляється, вважається, що у цьому разі порушується пов'язаність (рос. – связность) робочого каналу. Слід зауважити, що пов'язаність може втрачатися на різних рівнях взаємодії інформаційних систем. Якщо втрачається несуча сигналу або втрачаються бінарні сигнали, що утворюють бітовий потік у ЦСП, то мова йде про порушення пов'язаності каналу на фізичному рівні. Якщо ж не приходять повідомлення із підтвердженням факту приймання переданого блоку (або блоків) даних, то порушується пов'язаність каналу на більш вищих рівнях згідно із семирівневою моделлю взаємодії відкритих систем.

6.5.12. Параметри якості передавання тестової послідовності

1) ***PATL (pattern loss)* – кількість втрат тестової послідовності**. Визначається протягом одного сеансу тестування.

2) ***PATLS (pattern loss seconds)* – тривалість часу втрат тестової послідовності [с].** Цей параметр характеризує сумарну тривалість проміжків часу, протягом котрих було втрачено тестову послідовність.

6.5.13. Тестові послідовності для вимірювань параметрів бінарних цифрових каналів

Для визначення параметрів бінарного цифрового каналу за схемами, що передбачають можливість відключення від цього каналу корисного навантаження, широке застосування отримали різного роду тестові послідовності сигналів, представлених у двійковій формі. У цих випадках використовується кореспондована (тобто, пов'язана між собою) пара – генератор та аналізатор тестових послідовностей. Між генератором та аналізатором має існувати синхронізація щодо тестових послідовностей, інакше порівняння цих послідовностей на приймальній стороні буде неможливим.

Для різних експлуатаційних та інсталяційних задач потрібні різні види тестових послідовностей. Наприклад, якщо вирішується завдання із первісної інсталяції системи синхронізації, то доцільно використати фіксовану періодичну послідовність типу 1010.....10, оскільки із цієї послідовності на приймальній стороні достатньо просто виділити сигнали тактової синхронізації. Якщо ж необхідно визначити проміжок часу, на якому система синхронізації спроможна підтримувати синхронізм без її підстройки коригувальними сигналами, то використовують фіксовану бітову послідовність, що складається цілком тільки із нулів або тільки із одиниць. За таких тестових послідовностей на приймальній стороні коригувальні сигнали формуватися взагалі не будуть. Якщо мова йде про моделювання реального трафіка, то використовуються псевдовипадкові бінарні послідовності (ПВП, *PRBS – pseudorandom sequence*). Істинні (або майже істинні) випадкові послідовності на практиці майже не використовуються, оскільке їхнє формування являє складну технічну задачу.

6.5.14. Фіксовані тестові послідовності

Розглянемо наступні фіксовані тестові послідовності:

1) послідовність типу **1111 .... 1111** (тільки одиниці) – використовується, головним чином, для так званого стресового тестування, коли моделюються нештатні ситуації роботи каналу. Наприклад, у неструктурованому потоці типу *E1* ця послідовність сприймається як сигнал несправності (*AIS*);

2) послідовність типу **0000 .... 0000** (тільки нулі) – також використовується, головним чином, для стресового тестування. У багатьох випадках послідовне передавання нулів означає відсутність сигналу у каналі;

3) альтеративна послідовність типу **1010 .... 1010** – використовується для налагодження обладнання каналу, зокрема пристроїв синхронізації;

4) послідовності типу „**одна одиниця на три біти**”, „**одна одиниця на чотири біти**”, «**одна одиниця на вісім бітів**”, „**три одиниці на двадцять чотири біти**” – це промислові стандарти, що використовуються для дослідження проблем працездатності канального обладнання за різних умов його функціонування;

5) послідовність типу ***FOX*** ідентифікує речення „*Quick brown fox*”. Якщо це речення закодувати у двійковому коді *ASCII*, то отримаємо майже унікальну бітову послідовність, яку зручно використати для виявлення факту синхронізації обладнання. Якщо кожну бітову тетраду цієї послідовності закодувати 16-ти річним кодом, то отримаємо наступну послідовність:

2A, 12, A2, 04, 8A, AA, 92, C2, D2, 04, 42, 4A, F2, EA, 72, 04, 62, F2, 1A, 04, 52, AA, B2, 0A, CA, 04, F2, 6A, A2, 4A, 04, 2A, 12, A2, 04, 32, 82, 5A, 9A, 04, 22, F2, E2, 04, 8C, 4C, CC, 2C, AC, 6C, EC, 1C, 9C, 0C, B0, 50.

Можуть застосовуватися й інші нестандартизовані фіксовані послідовності в залежності від специфіки завдань, що вирішує експлуатаційний персонал.

Фіксовані тестові послідовності можуть передаватися із вказівкою на початок циклу, що задається спеціальним бітом (котрий, зазвичай, називають бітом ***f***) або спеціальною послідовністю бітів.

6.5.15. Псевдовипадкові тестові послідовності

Псевдовипадкові послідовності (ПВП) також широко використовують на практиці для вимірювань параметрів канального рівня. Слід підкреслити, що існує широкий спектр застосувань, де використовують генератори ПВП, що побудовані за різними принципами, функціонують у різних цілях і, тому, мають різні функціональні характеристики. Наприклад, генератор ПВП, що використовується для вирішення криптографічних задач, оцінюється за зовсім іншими критеріями, ніж генератор ПВП, що входить до складу вимірювального обладнання у телекомунікаціях, де фактор випадковості при формуванні бітових послідовностей не є вирішальним. Для вирішення телекомунікаційних завдань у більшості випадків застосовують стандартизовані типи ПВП, що генеруються на передавальній стороні та аналізуються на приймальній стороні за допомогою відносно простих та недорогих інструментальних засобів, побудованих на основі регістрів зсуву. До основних характеристик ПВП, що генеруються цими інструментальними засобами, слід віднести довжину ПВП у бітах (нагадаємо, що N-регістровий зсувний регістр виробляє ПВП довжиною L, де L визначається як $2^N - 1$) та вигляд поліному, що реалізується інструментальним засобом (наприклад, $D^{15} + D^{14} + 1 = 0$). Вибір конкретних значень цих характеристик здійснюється виходячи із міркувань, що наведені нижче.

У сучасній практиці для тестування обладнання цифрових каналів знайшли застосування наступні види стандартизованих МСЕ-Т псевдовипадкових послідовностей:

ПВП виду „63”. Формується 6-фазним регістром зсуву. Використовується для аналізу параметрів низькошвидкісних каналів передачі даних;

ПВП виду „127”. Формується 7-фазним регістром зсуву. Використовується також для аналізу параметрів низькошвидкісних каналів передачі даних;

ПВП виду „511”. Формується 9-фазним регістром зсуву. Використовується для аналізу параметрів вторинних мереж передачі даних, зокрема тих, що побудовані згідно стандарту *ITU-T V.52*;

ПВП виду „2047”. Формується 11-фазним регістром зсуву.

Використовується для аналізу параметрів вторинних мереж передачі даних, а також обладнання *ISDN*;

ПВП виду „2e15”. Формується 15-фазним регістром зсуву. Ця ПВП може містити до 14 нулів підряд, що дає можливість дослідити якість роботи системи синхронізації. Використовується для аналізу параметрів систем *PDH*, що працюють на невеликих швидкостях передавання даних;

ПВП виду „2e20”. Формується 20-фазним регістром зсуву. Використовуються при вимірюваннях за стандартом *ITU-T O.151*. Ця ПВП може містити до 14 нулів підряд.

ПВП виду „20ITU”. Також формується 20-фазним регістром зсуву. Ця ПВП відрізняється від ПВП „2e20” та може містити до 18 нулів підряд.

ПВП виду „2e23”. Формується 23-фазним регістром зсуву. Використовуються при вимірюваннях за стандартом *ITU-T O.151*. Ця ПВП знайшла широке застосування для аналізу параметрів систем *SDH*, що працюють на великих швидкостях передавання даних.

6.5.16. Типова схема вимірювань параметру BER

Типова схема вимірювань параметру *BER* (та похідних параметрів від нього) за умов відключення від цифрового бінарного каналу (ЦБК) корисного навантаження та підключення до нього (замість навантаження) генератора та аналізатора ПВП показана на рис. 6.17.

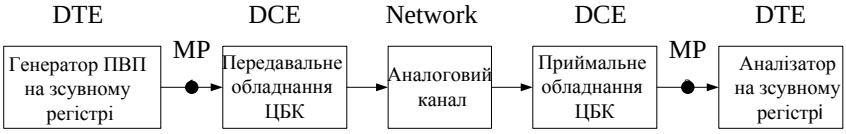


Рис.6.17. Типова схема вимірювань параметру BER, де MP_1 та MP_2 - точки вимірювань

Основна умова здійснення вимірювань за цією схемою полягає у необхідності досягнення синхронізму між переданими та прийнятими ПВП. Проте якщо аналізатор ПВП побудовано на

зсувних регістрах із замкненим ланцюгом зворотного зв'язку, то визначення факту втрати синхронізму не є проблемою: в момент втрати синхронізму на виході аналізатору з'являється інтенсивний потік бітових помилок, котрий за інтенсивністю приблизно лише у два рази менший за інтенсивність потоку сигналів тактової синхронізації, що відносно легко виявити на практиці. У момент відновлення синхронізму цей інтенсивний потік помилок зникає, а на виході аналізатора реєструються лише ті бітові помилки, що обумовлені недосконалістю цифрового каналу, тобто помилки, які враховуються під час вимірювань параметру *BER*. От же, процес вимірювань за схемою, що базується на використанні аналізатору ПВП на зсувних регістрах із зворотним зв'язком, нескладно і зручно здійснювати та контролювати. Тому саме ця схема рекомендована МСЕ-Т (див. рекомендації *ITU-T O.151* та *ITU-T O.153*) та широко застосовується в експлуатаційній практиці.

Специфіка вимірювань за цією схемою полягає у необхідності узгодженого вибору довжини *L* тестової ПВП в залежності від номільної швидкості передавання даних, на яку розраховано обладнання досліджуваного каналу. При невдалому виборі *L* може виникнути так званий джитер (тремтіння) регістрів зсуву, що входять до складу вимірювального засобу. Це, у свою чергу, призведе до суттєвого спотворення результату вимірювань. Слід відрізняти джитер регістрів зсуву від джитеру та вандеру параметрів цифрового сигналу в каналі (зокрема від джитеру та вандеру частоти або фази сигналу в каналі). Джитер сигналу в каналі є характеристикою якості каналу, оскільки величина цього джитеру впливає на якість передавання даних через канал. У той час як джитер регістрів зсуву не має відношення до каналу, а є наслідком некоректного вибору довжини тестової ПВП.

Для запобігання виникненню джитеру регістрів зсуву слід дотримуватися рекомендованих у *ITU-T O.151* довжин ПВП, що наведені у табл. 6.2. Як бачимо із табл.6.2, для вимірювань параметрів високошвидкісного обладнання (із номінальною швидкістю функціонування 34 Мбіт/с і вище) слід вибирати вимірювальний засіб, що здатний генерувати більш довгі ПВП. Тоді спектр сигналу ПВП уміститься у відносно вузьку смугу пропускання приймальної частини системи синхронізації ЦСП.

Таблиця 6.2

Рекомендації *ITU-T O.151* щодо вибору довжини ПВП

Номінальна швидкість передачі, *кбіт/с*	Довжина ПВП, *біт*	Поліном, що реалізується вимірювальним засобом	Спектральна відстань між субгармоніками сигналу ПВП Δf , *Гц*
64	$2^{15} - 1$	$D^{15} + D^{14} + 1 = 0$	1,95
2048	$2^{15} - 1$	$D^{15} + D^{14} + 1 = 0$	62,5
8448	$2^{15} - 1$	$D^{15} + D^{14} + 1 = 0$	257,8
34368	$2^{23} - 1$	$D^{23} + D^{18} + 1 = 0$	4,1
139264	$2^{23} - 1$	$D^{23} + D^{18} + 1 = 0$	16,6

А ширина спектру сигналу ПВП, у свою чергу, залежить від спектральної відстані Δf між субгармоніками цього сигналу. Із збільшенням швидкості передавання бітового потоку спектральна відстань Δf збільшується і, от же, може виникнути ситуація, коли спектр сигналу ПВП не уміститься у смугу пропускання системи синхронізації, що призведе до виникнення джитеру регістрів зсуву. Щоб запобігти цієї ситуації, у вимірювальному обладнанні слід використати поліном більш високого ступеню. Тоді довжина тестової ПВП збільшиться, а спектральна відстань між субгармоніками спектру сигналу ПВП зменшиться.

6.5.17. Способи розрахунку параметру BER за результатами вимірювань кількості бітових помилок у цифровому бінарному каналі

Існує два основних способи розрахунку параметру *BER*. Вибір одного із них залежить від того, що є більш важливим під час вирішення конкретного завдання – тривалість процесу вимірювань чи точність отриманого результату вимірювань.

Якщо є важливішою точність вимірювання, то безпосередньо перед початком вимірювань задаються бажаним значенням точності результату вимірювань. Наприклад, задамося значенням відносної похибки вимірювань η на рівні 1%. За умов нормального розподілу виникнення бітових помилок буде дійсним вираз: $\eta = 1/\sqrt{N}$, де N – кількість підрахованих бітових помилок. Якщо ми хочемо виміряти параметр *BER* з відносною похибкою, не більшою

за 1%, ми маємо вести в процесі вимірювань підрахунок бітових помилок до тих пір, поки не буде виявлено 10^4 помилок, оскільки $1/\sqrt{10^4} = 10^{-2}$, тобто 1%. Якщо ж нас задовольнить похибка у 10%, то маємо вести підрахунок бітових помилок набагато менш тривалий час, а саме до тих пір, поки не буде виявлено 10^2 помилок, оскільки $1/\sqrt{10^2} = 10^{-1}$, тобто 10%. Із вищенаведеного витікає основний недолік розглянутого способу вимірювання параметру *BER* – апріорна невизначеність часу вимірювань. Якщо помилки трапляються дуже рідко, то тривалість вимірювань із заданою точністю буде дуже великою. Тобто, необхідно буде здійснювати довготривале тестування, що, як правило, не є реальним на стадії експлуатації каналу.

Згідно іншого способу розрахунку параметру *BER* перед початком вимірювань задаються не точністю, а тривалістю одного сеансу вимірювань. Як варіант, можливо задатися не тривалістю вимірювань, а загальною кількістю бітів, котрі мають бути передані через канал протягом одного сеансу вимірювань. Наприклад, обумовлюється, що за один сеанс вимірювань має бути передано 10^6 бітів. У кінці сеансу вимірювань фіксується кількість виниклих бітових помилок та розраховується параметр *BER*. Проте похибка вимірювань за цим способом, на жаль, не є відомою. Можлива, наприклад, ситуація, коли під час передавання 10^6 бітів бітові помилки не виявились взагалі. От же, основним недоліком другого способу розрахунку параметру *BER* є невизначеність похибки вимірювань за умов, коли протягом сеансу вимірювань була виявлена недостатня кількість помилок. На практиці зазвичай припускають, що точність вимірювань за другим способом приблизно у десять разів гірша, ніж зворотна кількість переданих через канал бітів, тобто якщо передано 10^6 бітів, то точність вимірювань складає приблизно 10^{-5}. Проте повної довіри (із статистичної точки зору) до достовірності отриманого результату вимірювань немає. Якщо ж, виходячи із реальних умов функціонування бінарного каналу, можливо припустити, що процес утворення помилок в каналі є випадковим із нормальним законом розподілу, то існує можливість зробити оцінку виміряного значення параметру *BER* із бажаним ступенем статистичної достовірності такого вимірювання. Для цього слід скористатися

даними, що внесені до табл. 6.3.

Наприклад, вимірювання параметру *BER* виконувались на каналі *E1* (тобто, на швидкості бітового потоку, що дорівнював 2,048Мбіт/с) протягом 120 с. У результаті вимірювань було зафіксовано 200 бітових помилок. Тоді первісна (попередня) оцінка цього параметра буде визначена як

$$200/(2048000 \times 120) = 0{,}815 \times 10^{-6}.$$

Таблиця 6.3

Оцінка достовірності результатів вимірювань параметру *BER*

Кількість підрахованих бітових помилок за увесь період тестових вимірювань	Поправочний коефіцієнт на виміряне значення параметру *BER* для наведених нижче значень (у відсотках) коефіцієнту статистичної достовірності результату вимірювань:		
	70%	90%	95%
2	1,8	2,6	3,2
5	1,4	1,85	2,1
10	1,25	1,55	1,7
20	1,16	1,35	1,45
50	1,09	1,2	1,26
100	1,06	1,15	1,18
200	-	1,1	1,12
500	-	1,06	1,08

Однак ми бажаємо уточнити цю оцінку і отримати результат оцінки із статистичною достовірністю 95%. Тоді із табл.6.3 із рядка, що починається значенням кількості помилок „200”, та із стовпця „95%” беремо поправочний коефіцієнт „1,12” та множимо його на виміряну первісну оцінку параметру *BER*, що дорівнює $0{,}815 \times 10^{-6}$. Таким чином, отримаємо уточнену оцінку параметру $BER = 0{,}915 \times 10^{-6}$ з достовірністю 95%.

6.5.18. Способи розрахунку параметру ES за результатами вимірювань кількості секунд з помилками

Параметр *ES*, як вже було вказано, дозволяє оцінити долю часу від загального часу знаходження каналу у стані готовності, коли канал був вражений бітовими помилками. Характеристики каналу, коли він знаходився у стані неготовності, при цьому не враховуються. Знаючи долю часу від загального часу

функціонування каналу, коли канал перебував у стані готовності (параметр *AS*), та знаючи оцінку параметру *ES*, оператор електрозв'язку може оцінити реальний рівень якості каналу, зокрема визначити час роботи каналу без помилок (оцінити значення параметру *EFS*) за формулою *EFS = AS – ES*, що є важливим при плануванні навантаження на канал.

Існує два способи розрахунку параметру *ES* – синхронний та асинхронний - в залежності від того, яким чином визначені поняття „односекундний інтервал, вражений помилками" та „односекундний інтервал без помилок".

МСЕ-Т визначило поняття „односекундний інтервал без помилок" як односекундний інтервал в роботі каналу, протягом котрого не було виявлено будь-якої помилки. На верхньому рядку рис.6.18 відображено вісім односекундних інтервалів бітового потоку, що просувається через цифровий канал.

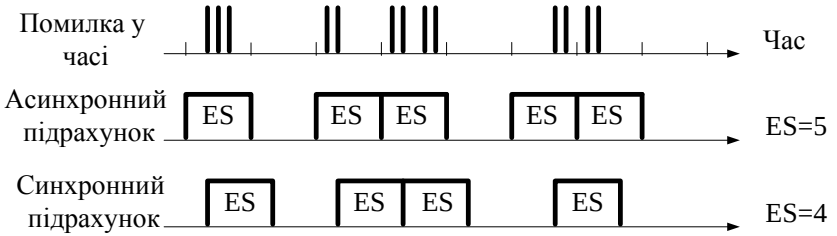


Рис.6.18. Способи визначення параметру ES

Видно, що другий, п'ятий та восьмий інтервали є вільними від помилок. Тому якщо безпосередньо дотримуватися вищенаведеного визначення „односекундного інтервала без помилок", то і підрахунок односекундних інтервалів має здійснюватися таким чином, щоб саме другий, п'ятий та восьмий інтервали визначались як інтервали без помилок. У цьому разі має бути використаний наступний так званий асинхронний спосіб розрахунку параметру *ES* (він пояснюється на середньому рядку рис.6.18).

Увесь інтервал вимірювання розбивається на однакові проміжки односекундних інтервалів та здійснюється підрахунок кількості інтервалів, протягом кожного із котрих виявлялась будь-яка

кількість помилок (зрозуміло, за умов непорушення стану готовності каналу). За асинхронним способом розрахунку (див. середній рядок рис.6.18) часові проміжки між односекундними інтервалами, на яких були виявлені помилки, є однаковими.

Зовсім інша картина спостерігається, якщо використати так званий синхронний спосіб підрахунку кількості односекундних інтервалів, що вражені помилками. Цей спосіб (що пояснюється на нижньому рядку рис.6.18) визначає „односекундний інтервал, вражений помилками" як односекундний інтервал, що безпосередньо йде услід за виявленою помилкою. Тобто, потік виміряних односекундих інтервалів, вражених помилками, синхронізується із часом появи помилок. Тому відповідно до синхронного способу розрахунку параметру *ES* часові проміжки між односекундними інтервалами, на яких були виявлені помилки, не є однаковими та зовсім по-іншому розташовані на часовій вісі.

Асинхронний спосіб знайшов застосування в Європі (саме цей спосіб рекомендований МСЕ-Т), в той час як синхронний спосіб розрахунку поширений у США.

У принципі, як це видно із рис.6.18, ці способи на однаковому потоку помилок дають різні результати. У діапазоні малих значень параметру ES (тобто, на високоякісних каналах) та за умов нормального розподілу ймовірності появи помилок різниця у результатах застосування цих способів підрахунку не є суттєвою. Однак коли канал вражений великою кількістю помилок та ще коли ці помилки мають схильність до групування, то різниця у результатах підрахунку параметру *ES* за різними способами може досягати 20%.

Кожен із способів має свої переваги та недоліки. Асинхронний спосіб – простий з точки зору технічної реалізації, в той час як синхронний метод є інваріантний щодо вибору часу початку вимірювань.

6.5.19. Схема вимірювань параметрів канального рівню без відключення цифрового каналу від корисного навантаження

Для здійснення вимірювань параметрів цифрового каналу без відключення від нього корисного навантаження використовується схема аналізу надлишкового циклового коду (*CRC*). Один із

варіантів такої схеми надано на рис.6.19.

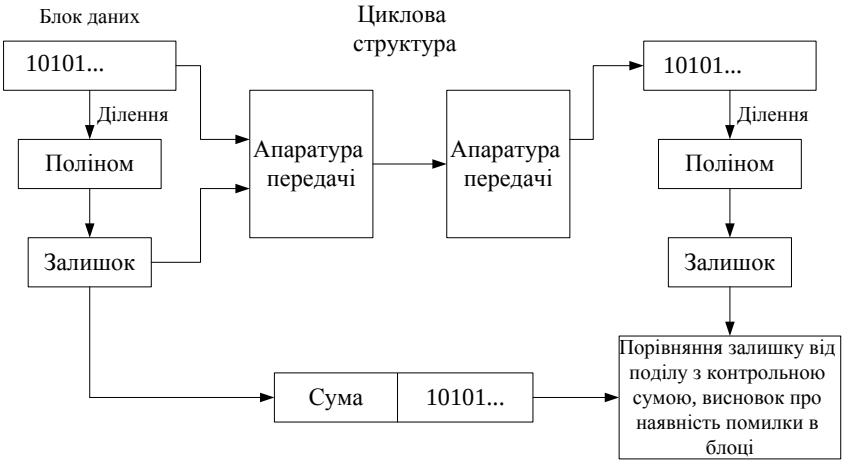


Рис.6.19. Схема вимірювань параметрів цифрового каналу без відключення від нього корисного навантаження

Перед тим, як корисний трафік подати на передавальне обладнання ЦСП, його кодують, так званим, завадостійким кодом, використання котрого забезпечує можливість на приймальній стороні цифрового каналу шляхом декодування виявляти (і, навіть, усувати) можливі помилки передавання цього трафіку. Існує широкий спектр різних завадостійких кодів, характеристики котрих вивчаються у рамках курсу „Теорія електрозв'язку". Усім цим кодам за різних умов притаманна різна ступень ефективності виявлення помилок. Однак більшість кодів, що реалізуються обладнанням ЦСП, відноситься до класу *CRC*-кодів. Алгоритм функціонування будь-якого коду *CRC* полягає у наступному. На передавальній стороні бітовий потік, що переносить корисний робочий трафік, розбивається на блоки бітів однакового наперед визначеного розміру, наприклад по 16 бітів кожний блок. І над кожним блоком послідовно по черзі здійснюється операція ділення вмісту цих блоків на певним чином обраний алгебраїчний поліном, наприклад на поліном виду $X^4 + X^1 + 1$ (що у двійковій формі представляється як 10011) або на поліном виду $X^{16} + X^{12} + X^5 + 1$

(що у двійковій формі представляється як 10001000000100001) і т. ін.. Ділення виконується у двійковій формі. Тому і залишки від ділення отримуються у двійковій формі. Розрядність двійкового числа, що представляє залишок, на одну одиницю менше розрядності двійкового числа, що представляє поліном. Ці залишки (що іноді називаються контрольними сумами або ідентитентами) упаковуються в окремі бітові блоки. Блоки із залишками разом із блоками бітів робочого трафіку передаються послідовно один за одним через цифровий канал. Таким чином, на приймальній стороні каналу маємо два пов'язаних між собою потоки бітових блоків, так що кожному блоку робочого трафіку відповідає кореспондований з ним блок із залишком. Над кожним блоком робочого трафіку на приймальній стороні здійснюється операція ділення на той же поліном і таким же чином, як і на передавальний стороні. Утворений залишок порівнюється із прийнятою інформацією про залишок, що був утворений на передавальній стороні. Якщо процес передавання блоку із робочим трафіком та відповідного йому блоку із залишком не супроводжувався виникненням помилок, то порівнювальні залишки мають співпадати. Інакше (тобто, коли порівнювальні залишки не співпадають) робиться висновок про наявність помилок у прийнятих блоках.

Розглянутий вище методологічний підхід до виявлення помилок часто називають методом *CRC*, з використанням котрого вимірюють параметри *CRC ERR* та *BLER*. Основна перевага цього методу – можливість вимірювань на реально працюючому каналі без відключення робочого трафіку. Однак, на жаль, цей метод не забезпечує тієї точності вимірювань, що притаманний методам тестування каналу із відключенням від нього корисного трафіку. Зокрема, тому, що він не забезпечує можливість локалізації та підрахунку виниклих помилок в межах прийнятого блоку із робочим трафіком. За його допомогою можливо лише визначити, чи є у складі прийнятого блоку помилкові біти. А скільки таких помилкових бітів, тим більш, де конкретно вони розташовані в межаж бітової послідовності – визначити не є можливим. Можлива ситуація, коли робочий блок був прийнятий без помилок, а у блоці із відповідним залишком були помилкові біти. У цьому випадку

порівнювальні залишки будуть не співпадати. Більше того, можливі ситуації, коли в каналі утворюються пари помилок, котрі на приймальній стороні під час операції ділення взаємно компенсуються. І, як результат, порівнювальні залишки у цих випадках будуть співпадати. Тобто, помилки в робочому блоці будуть не виявлені, хоч у дійсності вони мали місце. Отримаємо спотворення результатів вимірювань. Таким чином, метод *CRC* не дає повної гарантії щодо об'єктивності отриманих результатів вимірювань, а точність цих результатів суттєво нижча за точність результатів тестових вимірювань з відключенням навантаження. Якщо точність вимірювань параметру *BER* залежить від кількості переданих бітів, то точність вимірювань параметру *CRC ERR* (а також *BLER*) залежить від кількості переданих блоків.

Ефективність застосування методу *CRC* залежить від формату транспортованих блоків із робочим трафіком (зокрема, їх розміру та структури) та типу реалізованого в обладнанні поліному (зокрема, ступеню цього поліному). Напрямки використання вимірювального обладнання, що реалізує метод *CRC*, та відповідні характеристики цього обладнання надані у табл. 6.4.

Таблиця 6.4

Основні характеристики обладнання, що реалізує метод *CRC*

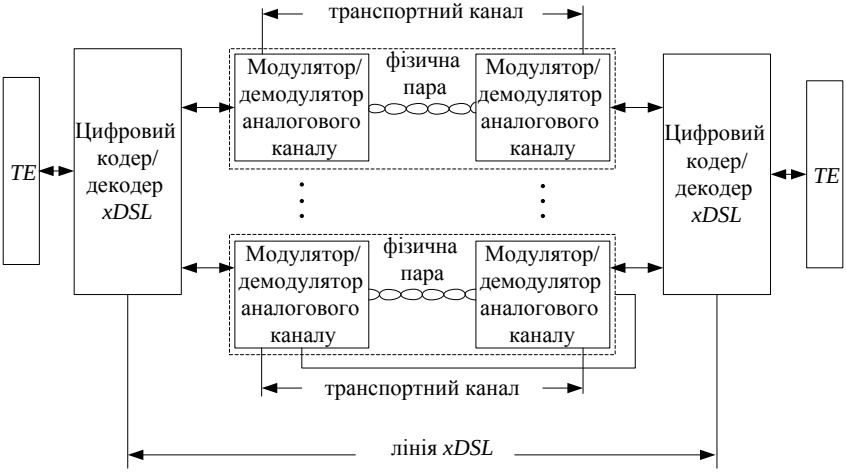
Тип коду	**Реалізований поліном**	**Розрядність ідентитенту**	**Основні сфери використання**
CRC-4	$X^4 + X + 1$	4	Канали типу *E1*
CRC-6	$X^6 + X + 1$	6	Канали типу *DS1*
CRC-16 FCS	$X^{16} + X^{12} + X^5 + 1$	16	Обладнання, що реалізує протоколи: *HDLC, V.41, ISDN, Frame Relay*
CRC-32	$X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^8 + X^7 + X^5 + X^4 + X^2 + X + 1$	32	Обладнання, що реалізує протоколи: *SMDS, LAN*

6.6. Особливості вимірювання параметрів цифрових каналів, що утворені на базі аналогових ліній телефонних мереж абонентського доступу (канали ISDN та xDSL)

6.6.1. Вимірювання параметрів обладнання xDSL

6.6.1.1. *Структурна схема включення обладнання xDSL*. Структурна схема включення обладнання xDSL, параметри котрого мають бути охоплені контролем під час транспортування даних у форматах PDU обладнання xDSL, відображена на рис.6.20.

Лінія xDSL створюється на базі фізичних абонентських пар телефонних проводів. Параметри таких електричних ланцюгів щодо передавання мовних сигналів та низькошвидкісних даних визначені у відповідних нормативних документах (зокрема, у ГСТУ 45.005-98, ГСТУ 45.008-98, КНД 45-033-96, КНД 45-055-97). У цих же документах надані норми на діапазони значень фізичних параметрів телефонних каналів абонентського доступу та відповідні методики їхнього визначення. Усі вищевказані норми мають виконуватися щодо телефонних пар, на базі котрих створюються лінії xDSL.



Позначки: *TE (Terminal Equipment)* - термінальний вузол

Рис.6.20. Структурна схема обладнання при транспортуванні даних у форматах *PDU xDSL*

Однак у фонових процедурах поточного контролю відповідності обладнання *xDSL* перевірки щодо цих норм, як правило, не виконуються, оскільки таке потребує довготривалих випробувань в режимі відключення корисного навантаження на лінію. Тому контроль параметрів фізичних каналів здійснюється лише під час планових процедур технічного обслуговування абонентських телефонних каналів та після виникнення невідповідностей в роботі *xDSL*-обладнання, що не були усунуті під час вирішення проблем у передаванні бітових потоків або проблем канального, мережного (і вище) рівнів.

Лінію *xDSL* розглядають як цифрову систему передачі, що у змозі за певних умов забезпечити швидкість у діапазоні 2 Мбіт/с і більше. Тому під час вимірювань параметрів фізичного рівня використовують рекомендацію МСЕ-Т G.703, яка регламентує вимірювання параметрів фізичного інтерфейсу канала *E1*, зокрема таких параметрів як швидкість та частота передавання бітів, припустима форма цифрового сигналу, тип та алгоритм лінійного кодування, припустимий рівень фазового тремтіння сигналу (джитер та вандер).

6.6.1.2. *Вимірювані параметри обладнання xDSL***.** Параметри обладнання *xDSL* оцінюються окремо щодо кожного із напрямків передачі, а також окремо щодо кожного абонентського транспортного каналу, які у сукупності можуть утворювати за допомогою засобів *xDSL* абонентську лінію *xDSL*. Якщо абонентська лінія утворена на основі використання однієї телефонної пари (тобто, одного транспортного каналу), то значення параметрів каналу та лінії *xDSL* співпадають.

1) ***Параметри функціональності щодо трафіка xDSL.***

Це бітова швидкість передавання даних:

- у дуплексній лінії *xDSL* - ***RL (Rate line)***;

- у дуплексному транспортному каналі, який утворений на основі однієї із фізичних пар телефонних проводів, що прокладена між споживачем мережних послуг і вузлом електрозв'язку – ***RC (Rate channel)***.

Примітка 6.3. Якщо для організації однієї xDSL-лінії передбачається використання двох або трьох фізичних пар проводів, то слід відрізняти параметри швидкості для лінії xDSL від параметрів швидкості для транспортного каналу,

утвореного на базі однієї із телефонних пар.

Примітка 6.4. Контроль інших показників швидкості передавання даних засобами xDSL, зокрема символьна швидкість, швидкість модуляції або ширина смуги пропускання, в експлуатаційній практиці не знайшов широкого застосування.

RL_{AD} - швидкість передавання даних у прямому напрямку передачі через абонентську лінію *xDSL* (тобто, від вузла зв'язку до покупця послуги), що вимірюється у біт/с (*bps – bits per second*).

RC_{AD} – швидкість передавання даних у прямому напрямку передачі через транспортний канал *xDSL*, що вимірюється у біт/с.

RL_{AR} - швидкість передавання даних у зворотному напрямку передачі через абонентську лінію *xDSL* (тобто, від покупця послуги до вузла зв'язку), що вимірюється у біт/с.

RC_{AR} – швидкість передавання даних у зворотному напрямку передачі через транспортний канал *xDSL*, що вимірюється у біт/с.

2) ***Параметри секунд, уражених помилками.***

ES-L (Errored second – line) – кількість виявлених на ближньому кінці лінії *xDSL* впродовж одного сеансу вимірювань односекундних інтервалів, протягом кожного з котрих були виявлені, але не виправлені по одній або більше помилок. Рахується, що вияв помилок здійснюється шляхом обчислення значення *CRC* (*Cyclic redundancy check*) під час циклічного декодування фреймів на приймальній стороні лінії *xDSL*. Помилка фіксується, якщо *CRC* не дорівнює *F0B816*. Виявлені помилки підсумовуються за усіма приймальними транспортними каналами, що складають лінію *xDSL*. Крім того, враховуються як *ES* секунди з дефектами типу *LOS* (*Loss of signal*, втрата сигналу) та (або) *SEF* (*Severely errored frame*, кілька помилкових фреймів) та (або) *LPR* (*Loss of power*, втрата потужності).

Примітка 6.5. Показники *LOS*, *SEF* та *LPR* визначені в *ITU-T Rec. G.997.1*.

ESR-L (Errored second ratio – line) – коефіцієнт помилок щодо секунд з помилками, виявлених на ближньому кінці лінії *xDSL* впродовж одного сеансу вимірювань.

FECS-L (Forward error correction second – line) – кількість виправлених на ближньому кінці лінії xDSL впродовж одного сеансу вимірювань одно секундних інтервалів, протягом кожного з котрих були виявлені та виправлені по одній або більше помилок.

Рахується, що кількість виправлених помилок дорівнює кількості виправлених кодових слів за результатами циклічного декодування прийнятих фреймів та аналізу FCS (Frame check sequence) і CRC. FCS формується на передавальній стороні лінії згідно з ISO/IEC 3309. Використовується поліном для перевірки виду $x^{16+}x^{12}+x^5+1$. Виправлені помилки підсумовуються за усіма приймальними транспортними каналами, що складають лінію xDSL.

Примітка 6.6. Показник *FECS* характеризує інтенсивність завад в лінії *xDSL*.

SES-L (Severely errored second – line) – кількість виявлених на ближньому кінці лінії *xDSL* впродовж одного сеансу вимірювань одно секундних інтервалів, протягом кожного з котрих були виявлені, але не виправлені не менш ніж вісімнадцять помилок. Механізм вияву помилок – аналогічний визначенню *ES*. Виявлені блоки по 18 або більше помилок підсумовуються за усіма приймальними транспортними каналами, що складають лінію *xDSL*. Крім того, враховуються як *SES* групи по 10 і більше секунд з дефектами типу *LOS* (*Loss of signal*, втрата сигналу) та (або) *SEF* (*Severely errored frame*, кілька помилкових фреймів) та (або) *LPR* (*Loss of power*, втрата потужності).

***SESR-L* (*Severely errored second ratio – line*)** - коефіцієнт помилок щодо секунд з 18 і більше помилками, виявлених на ближньому кінці лінії *xDSL* впродовж одного сеансу вимірювань.

***ES-LFE* (*Errored second – line far end*)** - кількість виявлених на віддаленому кінці лінії *xDSL* впродовж одного сеансу вимірювань одно секундних інтервалів, протягом кожного з котрих були виявлені, але не виправлені по одній або більше помилок. Механізм виявлення та правило підрахунку помилок – аналогічні визначенню *ES –L*.

ESR-LFE (Errored second ratio – line far end) - коефіцієнт помилок щодо секунд з помилками, виявлених на віддаленому кінці лінії *xDSL* впродовж одного сеансу вимірювань.

FECS-LFE (Forward error correction second – line far end)- кількість виправлених на віддаленому кінці лінії *xDSL* впродовж одного сеансу вимірювань односекундних інтервалів, протягом кожного з котрих були виявлені та виправлені по одній або більше

помилок. Механізм виявлення та правило підрахунку виправлених помилок – аналогічні визначенню *FECS –L*.

SES-LFE (Several error second – line far end) - кількість виявлених на віддаленому кінці лінії *xDSL* впродовж одного сеансу вимірювань одно секундних інтервалів, протягом кожного з котрих були виявлені, але не виправлені не менш ніж вісімнадцять помилок. Механізм виявлення та правило підрахунку помилок – аналогічні визначенню *SES –L*.

SES-LFE (Several error second ratio – line far end) - коефіцієнт помилок щодо секунд з 18 і більше помилками, виявлених на віддаленому кінці лінії *xDSL* впродовж одного сеансу вимірювань.

3) ***Параметри секунд неготовності каналу.***

LOSS-L (Loss of signal second - line) – кількість виявлених на ближньому кінці лінії *xDSL* впродовж одного сеансу вимірювань одно секундних інтервалів, протягом кожного з котрих було виявлено одна або більше подій, що ідентифікувались як втрата сигналу.

Примітка 6.7. Початок події втрати сигналу фіксується через 2,5 ± 0,5 с після виявлення ознак втрати сигналу. Закінчення події втрати сигналу фіксується через 10± 0,5с після зникнення ознак втрати сигналу.

UAS-L (Unavailable second – line) - кількість виявлених на ближньому кінці лінії *xDSL* впродовж одного сеансу вимірювань односекундних інтервалів, протягом кожного з котрих лінія *xDSL* рахувалась як непридатна для користування.

Примітка 6.8. Лінія *xDSL* рахується непридатною для користування з моменту, коли виявлено 10 суміжних секунд з помилками типу *ES* або *SES*. Ці 10 помилкових секунд враховуються при визначенні *UAS*. Лінія *xDSL* рахується знов придатною для користування з моменту, коли виявлено 10 суміжних секунд без помилок після помилкових секунд *ES* або *SES* . Ці 10 с виключаються із підрахунку *UAS*.

LOSS-LFE (Loss of signal second - line far end) - кількість виявлених на віддаленому кінці лінії *xDSL* впродовж одного сеансу вимірювань одно секундних інтервалів, протягом кожного з котрих було виявлено одна або більше подій, що ідентифікувались як втрата сигналу.

UAS-LFE (Unavailable second – line far end) – кількість виявлених на віддаленому кінці лінії *xDSL* впродовж одного сеансу

вимірювань одно секундних інтервалів, протягом кожного з котрих лінія *xDSL* була непридатною для користування.

4) ***Параметри блокових помилок.***

CV-C (Code violation– channel) – кількість виявлених на ближньому кінці транспортного каналу (одного з тих, що утворює лінію *xDSL*) протягом одного сеансу вимірювань помилкових результатів циклічного декодування прийнятих фреймів, тобто кількість виявлених помилкових значень *CRC*.

FEC-C (Forward error correction –channel) - кількість виправлених протягом одного сеансу вимірювань кодових слів (за результатами циклічного декодування прийнятих фреймів) на ближньому кінці транспортного каналу.

CV-CFE (Code violation – channel far end) - кількість виявлених протягом одного сеансу вимірювань помилкових *CRC* на віддаленому кінці транспортного каналу.

FEC-CFE (Forward error correction – channel far end) - кількість виправлених протягом одного сеансу вимірювань кодових слів (за результатами циклічного декодування прийнятих фреймів) на віддаленому кінці транспортного каналу.

5) ***Параметри деградації якості каналу.***

DGRM (Degradion minuts) - відсоток хвилин деградації якості. Визначається як відсоток хвилин, протягом котрих лінія *xDSL* була непридатною для користування, відносно загальної кількості хвилин в періоді функціонування обладнання, який визначається умовами *SLA*.

$\boldsymbol{MTTR_{max}}$ - верхня межа середнього часу відновлення працездатності обладнання *xDSL*. Вимірюється у хвилинах.

6.6.1.3. *Нормативи на параметри обладнання xDSL*

Слід розрізняти нормативи на параметри обладнання *xDSL* як цифрової системи передачі даних і нормативи якості на параметри фізичного середовища транспортування сигналів даних, тобто на параметри абонентських телефонних пар проводів, які, як правило, входять до складу багатопарних телефонних кабелів, на базі котрих побудовані канали мереж абонентського доступу до телефонної мережі загального користування (*PSTN*).

Використання абонентських телефонних пар в *xDSL*-лініях має

специфічні особливості, які потрібно враховувати під час досліджень проблем невідповідності на фізичному рівні.

Примітка 6.9. Специфіка пов'язана із високою швидкістю передавання сигналів через телефонну абонентську лінію, що потребує вирішення ряду проблем (зокрема, проблем електромагнітної сумісності через значний рівень міжканальних завад у багатоканальному телефонному кабелі, проблем забезпечення однорідності лінії – її симетрування, пошуку та нейтралізації незамкнених відводів від абонентської лінії, котушок Пупіна тощо), які у цьому розділі не розглядаються.

Вважається, що існуючі норми на фізичний інтерфейс канала *E1* припустимо використовувати під час аналізу фізичних інтерфейсів обладнання *xDSL*.

Суміщення ланцюгів дискретної та аналогової інформації, що має місце у разі використання обладнання *xDSL*, у кабельних лініях місцевого зв'язку є можливим лише за умов виконання вимог щодо електромагнітної сумісності. Перехідні завади у низькочастотних телефонних парах повинні бути нижчими, ніж нормовані значення, щоб гарантувати припустимий рівень достовірності транспортованої інформації. Тому мають бути виконаними вимоги ОСТ Р.45-81-97 «Совместимость электромагнитная цепей передачи дискретных и аналоговых сигналов местных сетей электросвязи», що регламентує електромагнітну сумісність обладнання *xDSL* з іншими засобами електрозв'язку, які використовуються в телефонних мережах абонентського доступу.

Дані щодо нормування параметрів електромагнітного впливу між ланцюгами *xDSL* на каналах мереж абонентського доступу з урахуванням видів модуляційних кодів (*HDB3*, *2B1Q* та *CAP*) наведено, наприклад у книзі Г.Ф. Конаховича та В.М. Чуприна „Мережі передавання пакетних даних". – К.: „МК-Прес", 2006.

Нормування параметрів обладнання *xDSL* здійснюється відносно параметрів *ESR* та *SESR*, оскільки визначення цих параметрів не потребує відключення корисного навантаження від лінії. За основу для визначення норм вибрані рекомендації МСЕ-Т *G.821* з урахуванням специфіки використання обладнання *xDSL*.

Розрізняють довгострокові та оперативні норми на параметри *ESR* та *SESR* для обладнання *xDSL*. Перевірка на відповідність оперативним нормам може здійснюватися протягом 15 хвилин, що

обумовило її використання в процесах поточного контролю відповідності. Перевірка на відповідність довгостроковим нормам потребує тривалих вимірювань. Зокрема, загальний час вимірювань в цьому випадку рекомендується вибирати на рівні 1 місяця.

Експлуатаційні норми на показники помилок для обладнання *xDSL* наведені у табл. 6.5.

Таблиця 6.5

Експлуатаційні норми на параметри обладнання *xDSL*

Довгострокові норми		Оперативні норми	
ESR	*SESR*	*ESR*	*SESR*
0,018	0,0003	0,009	0,00015

Щодо наведених норм слід зазначити наступне. Підрахунок *ES* та *SES* під час визначення параметрів *ESR* та *SESR* здійснюється тільки на інтервалах придатності лінії *xDSL* до користування, тобто секунди *UAS* не враховуються.

У рекомендації G.821 надані норми для *ESR* < 0,08, а для *SESR*< 0,002 щодо повного міжнародного *ISDN*-з'єднання. Надано також розподіл цих норм між трьома визначеними дільницями такого з'єднання. Для дільниці абонентського доступу визначені такі норми: *ESR* < 0,012, *SESR*< 0,0002. Для дільниці від місцевого вузлу до вузлу магістральної мережі: *ESR* < 0,006, *SESR*< 0,0001. Для лінії *xDSL* у якості нормованих значень *ESR* та *SESR* доцільно вибрати суми вищезазначених величин, тобто *ESR* < 0,018, *SESR*< 0,0003.

Значення нормованих показників *ESR* та *SESR* для оперативних норм відповідно до рекомендації G.821 удвічі менші значень цих показників для довгострокових норм.

6.6.1.4. *Схеми, умови, точки та порядок вимірювань параметрів обладнання xDSL*

В експлуатаційній практиці для вимірювання параметрів обладнання *xDSL*, норми на котрі зафіксовані у табл.6.5, використовують дві схеми організації вимірювань: "точка-точка" та вимірювання через шлейф. Поточний контроль стану обладнання *xDSL* здійснюється за схемою "точка – точка" у фоновому режимі без відключення корисного навантаження. Під

час планового контролю та пошуку шляхів вирішення проблем невідповідності застосовуються як тестові вимірювання за схемою “точка – точка”, так і шлейфова схема вимірювань, що потребує відключення корисного навантаження від досліджуваного обладнання.

Примітка 6.10. Для тестових вимірювань за схемою “точка-точка” потрібно два синхронізованих між собою аналізатори: один використовують в якості генератора тестуючої цифрової послідовності, що імітує роботу термінального обладнання, а інший виконує функції приймача цифрової послідовності. Шлейфова схема потребує лише одного інструмента вимірювань (але необхідності задіяння каналів обох напрямків передавання) і реалізується у двох варіантах: локального або віддаленого шлейфу.

У фоновому режимі поточного контролю вимірюються параметри *ESR* та *SESR*. У якості інструменту вимірювань використовуються штатні механізми обладнання *xDSL*. Під час цих вимірювань фіксуються також параметри *LOS, SEF* та *LPR,* оскільки поточні значення цих параметрів враховуються в процедурах обчислення *ESR* та *SESR*. Період одного сеансу оперативних вимірювань параметрів *ESR* та *SESR* під час поточного контролю – 15 хвилин. Отримані оцінки оперативних вимірювань усереднюються на місячній вибірці та порівнюються з довгостроковими нормами (див. табл. 6.5).

Примітка 6.11. Дозволяється для усереднення використовувати дані оперативних вимірювань, що отримані в години найбільшого добового завантаження обладнання *xDSL*, наприклад з 12 до 14 години у кожній добі.

Плановий контроль та аналіз проблем невідповідності передбачає необхідність вимірювання параметрів за умов, що наведені у табл. 6.6.

Таблиця 6.6

Параметр	Точка вимірювань (ближній/віддалений кінець каналу)	Необхідність контролю на вузлі зв’язку	Необхідність контролю на термінальному вузлі
FECS-L	*N*	M	M
FECS-LFE	*F*	M	O
ES-L	*N*	M	M

ES-LFE	*F*	M	O
SES-L	*N*	M	M
SES-LFE	*F*	M	O
LOSS-L	*N*	O	O
LOSS-LFE	*F*	O	O
UAS-L	*N*	M	M
UAS-LFE	*F*	M	O
CV-C	*N*	M	M
CV-CFE	*F*	M	O
EC-C	*N*	M	M
EC-CFE	*F*	M	O

Примітка 6.12. M – означає обов'язковість моніторингу параметра. O – означає бажаність (але не обов'язковість) моніторингу параметра. *N* - ближній кінець лінії *xDSL*. *F* – віддалений кінець лінії *xDSL*.

В процесі контролю відповідності вимірювання здійснюються на обох кінцях лінії *xDSL*.

Вимірювання вищенаведених параметрів можуть здійснюватися шляхом генерування на передавальній стороні та аналізу на приймальній стороні відповідних тестових цифрових послідовностей за схемою "точка – точка" . В цьому випадку необхідно застосовувати два синхронізованих між собою аналізатори протоколів. Дозволяється здійснювати вимірювання параметрів із табл. 6.6 за шлейфовою схемою. У будь-якому випадку періодичність тестування (тобто, тривалість одного сеансу вимірювань) під час контролю відповідності – 900с.

Схема організації вимірювань параметрів обладнання *xDSL* за шлейфовим методом, а також відповідні точки доступу до послуги та відповідні пари точок вимірювань, відображені на рис. 6.21. Якщо мати на увазі формат фреймів *xDSL*, що має структуру відповідно до рис.6.22 (тобто, з максимальною довжиною поля даних фрейму - 510 байтів для всіх різновидів технології *xDSL*, окрім технології згідно з рекомендацією МСЕ-Т *G.992.3*; для технології *G.992.3* максимальна довжина поля даних фрейму має дорівнювати 1024 байтів), то контроль обладнання при наданні послуги транспортування фреймів *xDSL* доцільно здійснювати на мережному рівні за шлейфовою схемою шляхом пінгування *ICMP*-

пакетами.

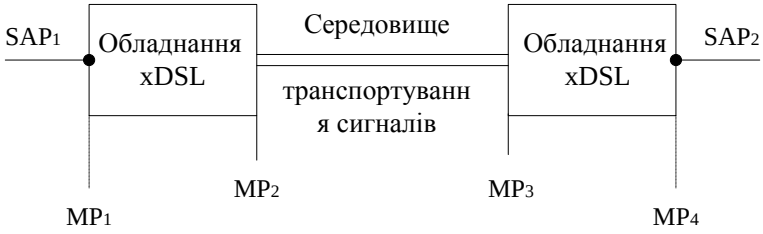


Рис. 6.21. Вимірювальна схема для визначення поточних параметрів обладнання *xDSL*, де SAP_j - j-та точка доступу до послуги; MP_i - і-та пара точок вимірювань

$7E_{16}$	Прапорець початку фрейма (*Opening Flag*)
FF_{16}	Адресне поле (*Address field*)
$O3_{16}$	Поле ідентифікатора (*Control field = UI frame*)
Інформаційне навантаження	Максимум 510 байтів
FCS	*Frame Check Sequence* (Перший октет)
FCS	*Frame Check Sequence* (Другий октет)
$7E_{16}$	Прапорець закінчення фрейма (*Closing Flag*)

Рис. 6.22. Формат фреймів *xDSL*

В цьому випадку до точок SAP_1 та SAP_2 (див. рис.6.21) приєднуються хости і за умов, що в кожен один тестовий фрейм упаковано лише один пакет, встановлюється режим періодичного тестування послідовностями ICMP-пакетів через фіксовані інтервали часу.

Тестові пакети генеруються за допомогою штатних програмних засобів хоста – ініціатора вимірювань, потім інкапсулюються у поле даних тестових фреймів (за допомогою штатних програмно-апаратних засобів обладнання *xDSL*) із розрахунку “в один фрейм – один пакет” і далі просуваються через контрольоване з’єднання до кінцевого віддаленого вузлу цього з’єднання. На віддаленому вузлі за допомогою штатних програмних засобів хоста у точці SAP_2 здійснюється шлейфування (тобто, логічне замикання пари вимірювальних точок) згідно рис.6.21 з подальшим передаванням

тестових пакетів (що упаковані у тестові фрейми) у зворотному напрямку та обробкою цих протокольних блоків даних (у т.ч., вилучення із фреймів тестових ICMP-пакетів) за допомогою штатних програмно-апаратних засобів хоста – ініціатора вимірювань.

Вищенаведений спосіб надає можливість виконати оцінювання параметрів обладнання *xDSL* шляхом вимірювань та розрахунків параметрів мережного рівня, котрі мають відповідати нормам якості обслуговування мережного рівня.

Розрахунок звітних значень безпосередньо параметрів обладнання *xDSL* здійснюється за результатами кожного сеансу вимірювань.

6.6.2. Вимірювання параметрів базового доступу BRI ISDN

6.6.2.1. *Структура базового доступу***.** Звісно, що існує можливість використати звичайну аналогову абонентську телефонну лінію для організації цифрового каналу доступу до вузлу комутації каналів (іноді і до вузлу комутації пакетів). Для цього найчастіше використовують так званий базовий доступ за технологією *ISDN* (*Basic Rate Interface, BRI*). Апаратна структура базового доступу *BRI ISDN* (див. рис.6.23) передбачає на ділянці між термінальним обладнанням кінцевого користувача (*Terminal Equipment, TE*) та модулем лінійного закінчення (*Line Termination, LT*), що функціонує у складі обладнання вузлу комутації, можливість створення трьох логічних каналів передавання бітових потоків – двох каналів типу B (кожний із них на швидкість 64 кбіт/с) та одного каналу типу D (на швидкість 16 кбіт/с). (Логічна структура лінії *BRI ISDN* на рис.6.23 не показана). У залежності від того, де конкретно розміщується модуль мережного закінчення (*Network Termination, NT*) – на боці користувача чи у складі обладнання вузлу комутації, маємо довгу лінію зв'язку на інтерфейсі ***U*** та коротку лінію на інтерфейсі ***S*** чи навпаки. Не заглиблюючись у подробиці побудови обладнання за технологією *ISDN* (ця технологія вивчається у рамках окремої навчальної дисципліни), зазначимо, що на стадії експлуатації обладнання *BRI ISDN* проблеми можуть виникнути як на ділянці цифрового каналу між *TE* та *NT* (тобто, на інтерфейсі ***S***), так і на ділянці цього каналу

між *NT* та *LT* (тобто на інтерфейсі ***U***).

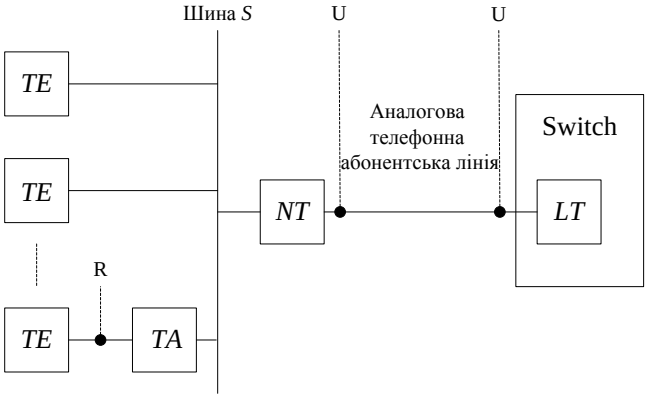


Рис.6.23. Апаратна структура цифрового базового доступу *BRI ISDN*

Інтерфейс S. Ділянку цифрової абонентської лінії між *TE* та *NT* називають шиною ***S***. Конструктивно шина ***S*** являє собою чотирьохпроводову кабельну лінію із розетками для підключення пристроїв *TE* (у т.ч., і через термінальний адаптер *TA*), що закінчується так званим термінатором (тобто, резістором із хвилевим опором, що має дорівнювати характеристичному імпедансу шини). До шини ***S*** може бути підключено від одного до восьми пристроїв *TE*. Чим більша кількість *TE* підключена до шини, тим коротша вона має бути. Максимальна довжина шини ***S*** (із одним підключеним *TE*) – 1000м. Сигнали на шині ***S*** утворюються шляхом амплітудно-імпульсної маніпуляції несучої бітового потоку (точніше, - відповідно до біполярного методу AMI, коли логічна одиниця кодується нульовим потенціалом, а логічний нуль - чередуванням потенціалів протилежної полярності). Структура цих сигналів – циклова (в деяких випадках – надциклова): як на етапі активації/деактивації лінії (на якому здійснюється обмін п’ятьма стандартними сигналами INFO 0 – INFO 4), так і на етапі передавання/приймання побітових даних у рамках встановленного з’єднання. Тривалість одного циклу передачі – 250 *мкс*. Розмір бітового блока даних, що відповідає одному циклу – 48 біт, із них два байти – канала B_1, ще два байти –

канала B_2, чотири біта – канала С, інші 12 бітів – службові, у т.ч. і для організації циклової синхронізації.

Інтерфейс U. Ділянку цифрової абонентської лінії між *LT* та *NT* називають лінією ***U***. Конструктивно лінія ***U*** являє собою двопроводову кабельну лінію, що створена на основі однієї із пар багатопарного кабелю, зокрема типу „звита пара", що пролягає від абонента телефонної мережі до АТС. Специфікації лінії ***U*** не є стандартизованими. Тому і довжина цієї лінії – не регламентована. Тим не менш, максимальна довжина лінії ***U*** навіть за сприятливих умов передачі бітового потоку не може перевищувати 3– 5,5 км, а у багатьох випадках не повинна перевищувати 1500м. Сигнали у лінії ***U*** утворюються шляхом лінійного кодування за методом *2B1Q* (іноді за методом *4B3T* або U_p0). Структура цих сигналів мало чим відрізняється від структури сигналів на шині ***S***, тобто вона має циклічний характер як на етапі активації/деактивації лінії, так і на етапі передавання/приймання побітових даних у рамках встановленного з'єднання.

Технологія *ISDN* передбачає необхідність використання абонентської сигналізації. Проблеми вимірювань параметрів сигналізації, у т.ч. абонентської сигналізації *ISDN,* висвітлені у матеріалах лекції №8.

6.6.2.2. *Вимірювання параметрів базового доступу***.**

Експлуатаційні процедури та порядок їхнього здійснення щодо обладнання базового доступу на фізичному рівні взаємодії є добре апробованими і полягають у наступному (див. рис.6.24).

Як бачимо на рис.6.24, послідовний аналіз проблем із невідповідністю параметрів обладнання базового доступу їх номінальним значенням на фізичному рівні взаємодії складається із чотирьох груп експлуатаційних завдань:

1) передінсталяційні вимірювання існуючих абонентських кабелів (у випадках, коли для побудови базового доступу намагаються використати вже прокладені абонентські телефонні кабелі та існує проблема вибору телефонних пар, котрі мають відповідати вимогам із передавання цифрових потоків згідно специфікаціям технології *ISDN*);

2) тестування обладнання базового доступу за допомогою автоматичних експлуатаційних тестів з метою отримання

упевненості, що усі активізовані послуги *ISDN* надаються у повному обсязі із визначеним рівнем якості;

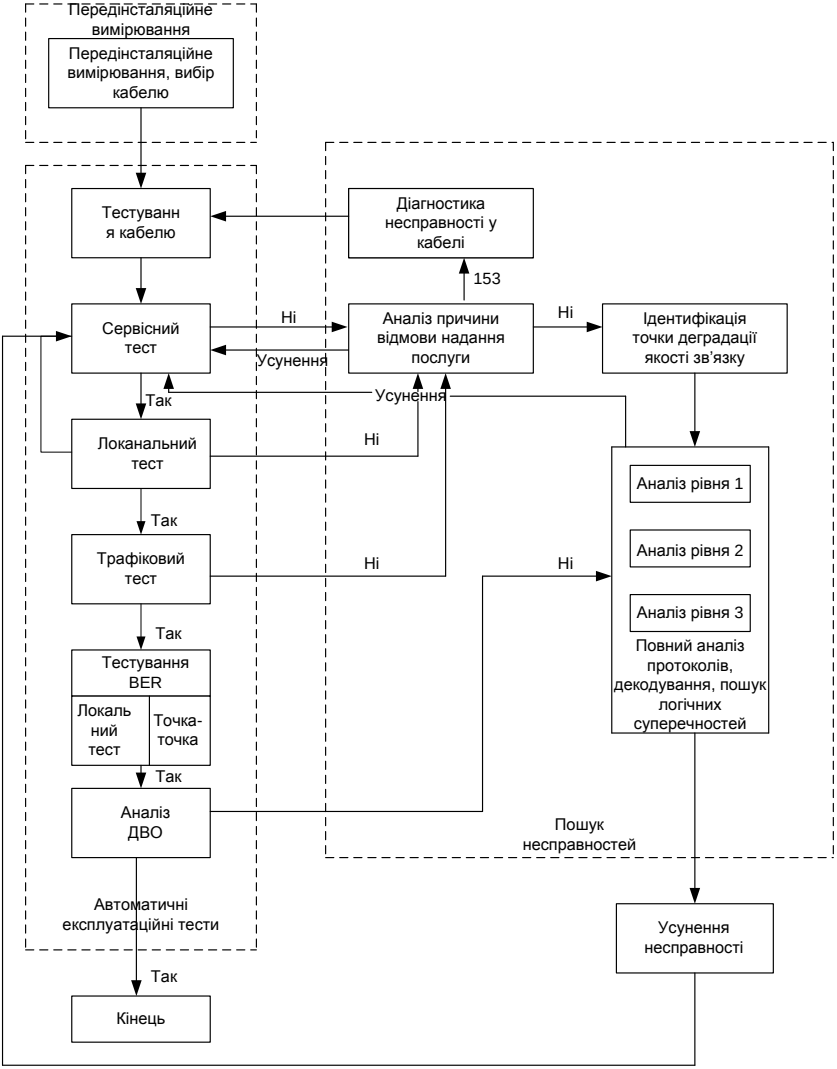


Рис.6.24. Порядок робіт з експлуатації обладнання *BRI ISDN*

3) пошук несправностей;

4) усунення несправностей.

Примітка 6.13. Пошук та усунення несправностей в роботі обладнання *BRI ISDN* пов'язаний, багато у чому, з аналізом протоколів абонентської сигналізації канального та мережного рівнів згідно семирівневої моделі OSI. Проблеми вимірювань параметрів. абонентської сигналізації для *ISDN*, висвітлені у матеріалах лекції №8.

У рамках передінсталяційних вимірювань здійснюють вимірювання наступних параметрів фізичного рівня взаємодії (як на інтерфейсі ***S*** , так і на інтерфейсі ***U***):

Відсутність напруги електроживлення на шині S. Вимірюється звичайним тестером або мультиметром.

Коректність розводки жил кабелю шини S. Вимірюється звичайним тестером або мультиметром. Визначаються також можливі розриви та короткі замикання у кабелі.

Величина опору ізоляції у жилах кабелю як на шині S, так і на лінії U. Вимірюється мегометром. Має відповідати паспортним даним на кабель.

Довжина кабелю шини S. Вимірюється візуально за позначками на кабелі. Припустима довжина шини залежить від кількості та місць розташування пристроїв *TE* і має не перевищувати рекомендованих норм.

Величина опору термінатора шини S. Вимірюється за допомогою спеціалізованого пристрою – індикатора стану шини *S*. Зазвичай цей опір має дорівнювати 100 Ом. Індикатор стану шини (наприклад, виробництва компанії *Aurora Profi*) складається із генератора, що імітує сигнали модулю *LT* і включається у блок *NT* з боку інтерфейса *U*, та аналізатора, що включається одразу до усіх абонентських розеток шини *S*. Індикатор стану шини *S* здатний вимірювати усі зазначені вище фізичні параметри кабелю.

Величина затухання у кабелі на інтерфейсі U. Для вимірювань параметрів затухання A або A_p абонентської лінії на інтерфейсі ***U*** є можливим застосувати звісні методи тонального або імпульсного тестування. Методи та засоби вимірювання параметра затухання розглядались нами у підрозділах 6.3.1 та 6.3.8 цієї лекції.

Величина перехідного затухання на ближньому та на дальньому кінцях лінії на інтерфейсі U. Для вимірювань

параметрів *NEXT* та *FEXT* також можливо використати метод тонального тестування із застосуванням аналізаторів абонентських ліній (із діапазоном розгортки ІЧХ – 2мГц) або метод імпульсної рефлектометрії. Обидва названі методи висвітлені у підрозділі 6.3.4 цієї лекції.

Виявлення неоднорідностей в лінії на інтерфейсі U. Зокрема виявлення котушок Пупіна та (або) пасивних відводів від лінії. Для цього будують графік ІЧХ абонентської лінії будь-яким звісним способом, наприклад із застосуванням аналізаторів абонентських ліній або шляхом безпосереднього аналізу рефлектограм, що отримуються завдяки застосуванню рефлектометра. Відповідний матеріал міститься у підрозділах 6.3.2 та 6.3.8 цієї лекції.

Автоматичні експлуатаційні тести, що запускаються у рамках тестування обладнання базового доступу, складаються із (див. рис.6.18):

- **сервісного тесту**, що має визначити перелік послуг, що можуть надаватися абоненту через один із логічних каналів В у складі перевіряємого інтерфейсу базового доступу (цей тест у локальному варіанті фактично перевіряє коректність програмування параметрів модулю *LT*, а у варіанті віддаленого доступу – параметрів усього ланцюга обладнання на трасі „локальний *NT* – віддалений *TE*");

- **поканального тесту**, що забезпечує перевірку окремо кожного із двох існуючих логічних каналів типу В у складі перевіряємого інтерфейсу *BRI;*

- **трафікового тесту**, що забезпечує перевірку здатності обладнання витримувати максимальне завантаження одночасно двох існуючих логічних каналів типу В у складі перевіряємого інтерфейсу *BRI*;

- ***BER*-тесту**, тобто тесту, за допомогою якого визначається параметр бітових помилок *BER*. Методи та засоби визначення цього параметру розглянуто у підрозділі 6.4.1 цієї лекції).

6.6.3. Вимірювання параметрів первинного доступу ISDN

6.6.3.1. *Структура первинного доступу***.** Базовий доступ забезпечує можливість передавання цифрових інформаційних

потоків із сумарною швидкістю 144 кбіт/с, не більше. Однак у багатьох практично важливих випадках цього явно недостатньо. Наприклад, якщо ставиться завдання підключити до телефонної мережі загального користування (*PSTN*) яку-небудь корпоративну АТС (*PBX*) з ємністю 500 номерів і більше, то у цьому випадку пропускна здатність з'єднувальної лінії зв'язку має вимірятися одиницями, а то і десятками мегабіт у секунду. Такий діапазон швидкостей якраз і забезпечує обладнання первинного доступу ISDN (Primary Rate Interface, PRI).

Логічна структура PRI ISDN - тридцять каналів типу B, кожний із котрих розрахований на швидкість 64 кбіт/с, та один канал типу D на швидкість 64 кбіт/с, тобто маємо логічну структуру первинного доступу у вигляді 30B + D.

Канали типу B можуть об'єднуватися в один логічний високошвидкісний канал передачі користувацьких даних на швидкість 1920 кбіт/с, у той час як канал типу D використовується для забезпечення системи сигналізації.

Апаратна структура цифрового первинного доступу *PRI ISDN* показана на рис.6.25.

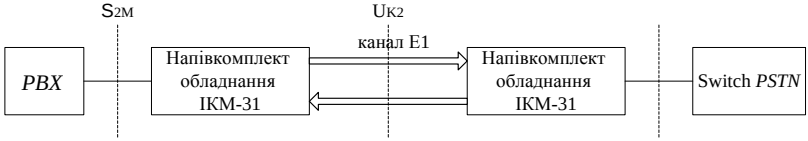


Рис.6.25. Апаратна структура цифрового первинного доступу *PRI ISDN*

Така апаратна структура *PRI* органічно вписується у структуру канала типу *E1* із цикловою синхронізацією, якщо цей канал утворюється засобами обладнання ІКМ-31. Тобто, у цьому випадку канал первинного доступу має циклову структуру та являє собою канал *E1*, в якому шляхом часового мультиплексування (*TDM*) у тайм-слоти *TS1 – TS30* упаковано 30 каналів типу B, у тайм-слот *TS31* упаковано канал типу D, а тайм-слот *TS0* відведено для передавання сигналу циклової синхронізації *FAS* (*Frame Alignment Signal*). Якщо порівнювати рис.6.17 з рис.6.25, то неважко побачити, що функції *NT* та *LT* у схемі первинного доступу виконують прикінцеві напівкомплекти обладнання ІКМ-31, між котрими на інтерфейсі U_{K2} утворюється дуплексний канал типу *E1*

(на швидкість 2048 кбіт/с) із фізичним розділенням напрямків передавання даних, тобто в якості середовища розповсюдження сигналів потоку *E1* використовується чотирьохпроводова металева лінія зв'язку (або два волокна оптоволоконної лінії). Максимально припустима довжина такої лінії – 1800м. Вид лінійного кодування (у більшості випадків) – *HDB3*. Функції *TE* на рис.6.25 виконує, зокрема, корпоративна АТС (*PBX*).

Інтерфейс S_{2M} згідно специфікації *PRI* може бути тільки „точка – точка", а само обладнання ІКМ-31 розміщається, як правило, біля обладнання *PBX*. Тому вимірювання параметрів інтерфейсу S_{2M} не мають суттєвого експлуатаційного значення.

Обладнання каналу *PRI* відповідно до специфікацій *ISDN* має бути завжди в активному стані, тому відпадає необхідність вимірювань параметрів процесів активації/деактивації лінії (як це необхідно робити під час аналізу *BRI*).

Технологія *PRI ISDN* передбачає необхідність використання певним чином обраних систем сигналізації. Проблеми вимірювань параметрів обладнання сигналізації, у т.ч. сигналізації для *ISDN*, висвітлені у матеріалах лекції №8.

Пошук несправностей в обладнанні первинного доступу виконується, головним чином, шляхом аналізу задіяних у ньому сигналізаційних протоколів. Засоби та процедури здійснення такого аналізу також висвітлені у матеріалах лекції №8.

6.6.3.2. *Вимірювання параметрів первинного доступу*

Обладнання первинного доступу фактично складається із відрізків кабелів (металевих або оптичних), що слугують середовищем розповсюдження сигналів, та каналоутворюючого обладнання на обох кінцях лінії зв'язку. Вимірювання параметрів задіяних кабелів являють інтерес, головним чином, на передексплуатаційних стадіях життєвого циклу обладнання. Методи та засоби таких вимірювань детально розглянуто нами у підрозділах 6.1 та 6.2 цієї лекції. Щодо каналоутворюючого обладнання, то у даному випадку розгляду мають підлягати параметри обладнання ІКМ-31. Засобами цього обладнання утворюються потоки бітових даних типу *E1*. Методи та засоби вимірювання параметрів такого потоку розглянуто нами у

підрозділі 6.4. Більш детально проблематика вимірювань параметрів каналу *E1* висвітлена у [5].

6.7. Особливості вимірювання параметрів кабельних систем із частотним ущільненням аналогових телефонних каналів

Вимірювання параметрів первинних аналогових мереж із частотним ущільненням абонентських телефонних каналів (системи типу К-60, К-120, К-1920 і т.ін.) розглядати не будемо через їхню моральну та фізичну застарілість. Проте не усе це обладнання знято із експлуатації. Тому у разі необхідності інформацію щодо вимірювань параметрів обладнання із частотним ущільненням аналогових каналів слід шукати у багато чисельних публікаціях початку 80-х років, що присвячені системам багатоканального зв'язку, зокрема у [6].

Контрольні питання до самостійного заняття шостої лекції

1.Надайте визначення параметру *BER*.

2. Чим розрізняються два основних методологічних підходи до вимірювань бінарного каналу – з відключенням та без відключення цього каналу від корисного навантаження?

3. Дайте визначення параметрам готовності/неготовності каналу.

4. Дайте визначення параметрам тривалості бітових помилок.

5. Дайте визначення параметрам кількості блокових помилок.

6. Дайте визначення параметрам помилок CRC.

7. Дайте визначення параметрам розсинхронізації.

8. Дайте визначення параметрам деградації якості робочого каналу.

9. Дайте визначення параметру пов"язаності каналу.

10. Дайте визначення параметрам якості передавання тестової послідовності.

11. Надайте характеристику різним видам тестових послідовностей для вимірювань параметрів бінарних цифрових каналів.

12. Надайте типову схему вимірювань параметру *BER* (та похідних параметрів від нього).

13. Як запобігти виникненню джитеру регістрів зсуву під час

формування псевдовипадкових тестових послідовностей.

14. Надайте характеристику основним способам розрахунку параметра *BER*.

15. Як оцінити достовірність результатів вимірювань параметра *BER*.

16. Надайте характеристику основним способам розрахунку параметра *ES*.

17. Надайте типову схему вимірювань параметрів канального рівню без відключення цифрового каналу від корисного навантаження.

18. Надайте основні характеристики обладнання, що реалізує метод *CRC*.

19. Надайте структурну схему включення обладнання *xDSL*.

20. Назвіть параметри обладнання *xDSL*, що підлягають оцінці.

21. Які нормативи на параметри обладнання *xDSL* як цифрової системи передачі даних?

22. Надайте схеми, назвіть умови, укажіть точки та порядок вимірювань параметрів обладнання *xDSL*.

23. Надайте апаратну структуру цифрового базового доступу *BRI ISDN*.

24. Укажіть порядок робіт з експлуатації обладнання *BRI ISDN*.

25. Які параметри обладнання *BRI ISDN* підлягають вимірюванням?

26. Надайте апаратну структуру цифрового первинного доступу *PRI ISDN*.

Література до самостійного заняття шостої лекції

1) И.Г. Бакланов. Технологии измерений в современных телекоммуникациях. –М.: ЭКО- ТРЕНДЗ, 1998. Розділи 4, 5 та 10.2.

2) А.Б. Семёнов, С.Н. Стрижаков, И.Р. Сунчелей. Структурированные кабельные системы. –М.: ДМК Пресс, 2002. Розділ 2.

3) Ю.А. Парфёнов, Д.Г. Мирошников. «Последняя миля» на медных кабелях. –М.:Эко-Трендз, 2001. Глава 3.

4) Г.Ф. Конахович, В.М. Чуприна. Мережі передавання пакетних даних. – К.: „МК-Прес”, 2006.

5) И.Г. Бакланов. Технологии измерений первичной сети. Часть 1. Системы Е1, PDH, SDH.–М.:ЭКО-ТРЕНДЗ, 2000. Разделы 2, 3, 4.

6) А.М. Зингеренко, Н.Н. Баева, М.С. Тверецкий. Системы многоканальной связи. –М.:Связь, 1980.

ЛЕКЦІЯ №7 ВИМІРЮВАННЯ ПАРАМЕТРІВ ОБЛАДНАННЯ НА КАНАЛЬНОМУ РІВНІ ВЗАЄМОДІЇ ІНФОРМАЦІЙНИХ СИСТЕМ

Розглядаються наступні питання:

Лекційне заняття

7.1. Основні схеми вимірювань параметрів канального рівню

7.2. Параметри канального рівню, що підлягають вимірюванням

7.3. Вимірювання параметрів канального рівню обладнання пакетних мереж

7.4. Вимірювання параметрів функціональності послуг

7.5. Вимірювання параметрів якості передавання протокольних блоків даних

Самостійне заняття. Вимірювання параметрів обладнання *Frame Relay* та *xDSL*

7.6. Вимірювання параметрів обладнання систем передавання фреймів на транспортній мережі *Frame Relay*

7.7. Вимірювання параметрів абонентського доступу до транспортної мережі з використанням обладнання *Frame Relay* та *xDSL*

7.1. Основні схеми вимірювань параметрів канального рівню

Узагальнена схема вимірювань параметрів канального рівню, незалежно від того, яке саме телекомунікаційне обладнання мереж передавання даних (МПД) є об'єктом вимірювань, показана на рис.7.1.

На практиці для позначення складових елементів цієї схеми прийнято використовувати англійську абревіатуру скорочень:

DTE (*Digital Terminal Equipment*) – цифрове термінальне обладнання;

DCE (*Digital Canal Equipment*) – цифрове канальне обладнання;

MP (*measurement point*) – точка вимірювань.

DTE, як правило, розташоване у точці присутності користувача мережних ресурсів, належить цьому користувачеві і включено до складу його інформаційної системи, на якій він вирішує свої прикладні задачі. Наприклад, під *DTE* розуміють мережний адаптер у складі комп'ютеру користувача із відповідним програмним драйвером.

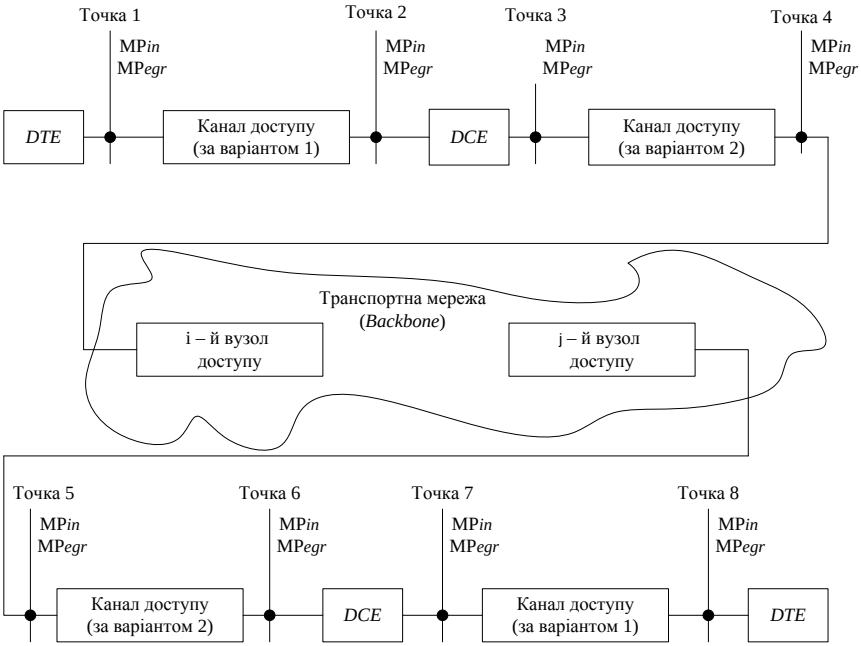


Рис.7.1. Узагальнена схема вимірювань параметрів канального рівню, де MP_{in} – точка вимірювань увідного потоку інформації; MP_{egr} – точка вимірювань вивідного потоку інформації

DCE – це обладнання канального закінчення, яке призначено, головним чином, для узгодження (рос., – сопряжения) характеристик термінального обладнання користувача із характеристиками каналу передавання даних. Наприклад, під *DCE* розуміють всілякого роду модемне обладнання або блок *NT* в обладнанні *ISDN* або пристрій доступу *FRAD* (*Frame Relay Eccess Device*) до ресурсів мережі *Frame Relay* тощо. *DCE* в залежності від конкретних умов користування може бути розташоване як на мережному вузлі оператора електрозв'язку (тобто, в зоні його контролю), так і знаходитись у безпосередній близькості від *DTE* на площах користувача мережних ресурсів. Зрозуміло, що вибір місця розташування канального закінчення (*DCE*) залежить від того, що більш доцільно організувати – абонентський цифровий

канал доступу між термінальним обладнанням користувача (*DTE)* та обладнанням канального закінчення *DCE* (варіант 1) або канал абонентського доступу між *DCE* та вузловим обладнанням мережі, що використовуються для транспортування цифрових даних (варіант 2). На практиці у більшості випадків знайшов застосування варіант 2, оскільки в цьому випадку характеристики елементів ТЛК-обладнання, що утворюють канал, будуть узгодженими з характеристиками середовища транспортування інформації, що забезпечує можливість передавання інформації на великі відстані. Варіант 1 такого узгодження не забезпечує, тому канал у цьому випадку не може бути довшим, ніж кілька десятків метрів (в особливих випадках, не більше кілька сотень метрів).

Зустрічаються дві основні схеми організації вимірювань параметрів канального рівня – **вимірювання типу „точка – точка”** (без утворення зворотного каналу) та **вимірювання „за шлейфом”** (з утворенням зворотного каналу). В телекомунікаціях існує таке поняття як **точка вимірювань** (*measurement point, MP*). Визначити точку вимірювань – це, по-перше, визначити її місце розташування на схемі організації вимірювань (наприклад, на інтерфейсі між *DTE* та *DCE* або на інтерфейсі між закінченням каналу доступу та комутатором мережі тощо), а по-друге, визначитися з напрямом передавання потоку інформації, характеристики котрого мають бути виміряні. Зокрема, позначимо як MP_{in} точку, де організується спостереження за параметрами увідного потоку протокольних блоків даних (*PDU, Protocol Data Unit*), і як MP_{egr} точку, де вимірюються параметри вивідного потоку.

У випадку застосування схеми організації вимірювань типу „точка – точка” треба мати два напівкомплекти вимірювального обладнання, що розташовані у віддалених одна від одної точках MP_{in} та MP_{egr}, що не завжди зручно, оскільки виникає необхідність вирішення відносно непростої задачі синхронізації роботи цих напівкомплектів. Задача синхронізації вимірювального обладнання, що підключено до віддалених одна від одної точок вимірювань, суттєво спрощується, якщо обидва його напівкомплекти розташувати поруч в одному місці, тобто організувати вимірювання за шлейфом, коли вимірювальні засоби зосереджені в

одному місці.

У залежності від того, параметри якого саме елементу обладнання каналу підлягають вимірюванням, можуть бути організовані різноманітні види шлейфів. Зокрема, наприклад, якщо існує необхідність аналізу параметрів мережного адаптеру (або його драйверу), що входить до складу комп'ютеру користувача (тобто, до *DTE*), то вивідний порт адаптеру замикають на його увідний порт та утворюють локальний шлейф на *DTE*, коли логічні точки вимірювань забезпечуються інструментальним програмним засобом, інстальованим на *DTE*. Схема організації такого шлейфу показана на рис.7.2.

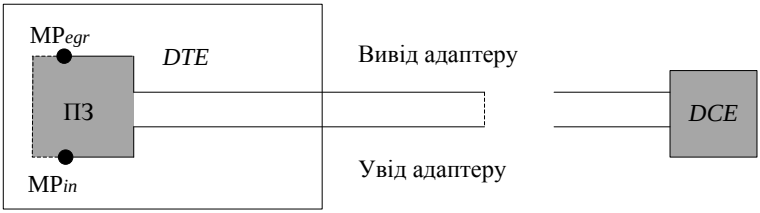


Рис.7.2. Схема організації локального шлейфу на *DTE*

Якщо існує необхідність аналізу параметрів не тільки *DTE*, а і каналу передавання між *DTE* та *DCE* (але не самого *DCE*), то на стороні *DCE* вивідний порт цього каналу з боку свого *DTE* (логічний або фізичний - в залежності від конкретної схеми зв'язку) замикають на його увідний порт та утворюють локальний шлейф на *DCE* згідно рис. 7.3.

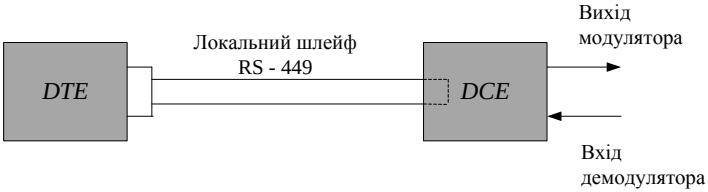


Рис.7.3. Схема утворення локального шлейфу на *DCE* (з боку свого *DTE*)

Якщо існує необхідність аналізу параметрів усього комплекту

обладнання доступу до мережних ресурсів (тобто, *DTE* + *DCE* + канал між ними) за умов, що це обладнання розташовано локально (тобто, в одному місці або майже в одному місці, коли відстань між *DTE* та *DCE* не перевищує кілька сотень метрів), то локальне *DCE* відключається від каналу, що йде у напрямку транспортної мережі (тобто, у напрямку вузлу доступу до мережі), а відповідні порти локального *DCE* замикаються один на одний, як це показано на рис. 7.4.

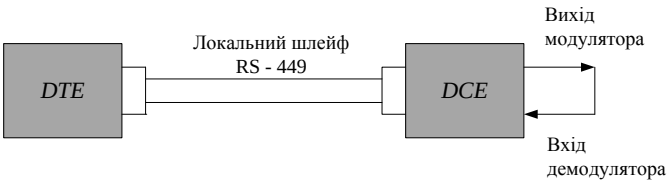


Рис.7.4. Схема утворення локального шлейфу на *DCE* (з боку мережі доступу)

Якщо потрібно дослідити параметри не тільки прикінцевого обладнання, що розташоване локально на термінальному вузлі користувача мережних ресурсів, але ще і обладнання каналу доступу до вузлу мережі, але без включення вузлового обладнання мережі, то замикають кінці каналу доступу на інтерфейсі з вузловим обладнанням так, як це показано на рис.7.5.

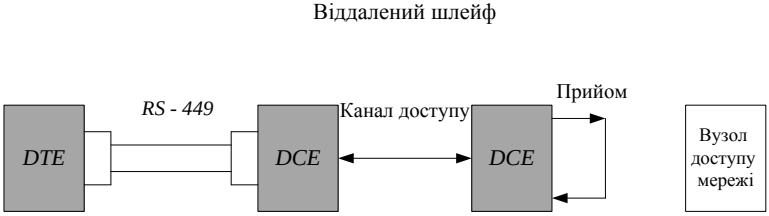


Рис.7.5. Схема утворення віддаленого шлейфу

Як результат, утворюється, так званий, віддалений шлейф. Накінець, якщо існує необхідність визначити параметри усього обладнання, що утворює цифровий канал або канал передачі даних, що проходить через певним чином визначені вузли транспортної мережі, то замикають шлейф на дальньому кінці віддаленого *DCE*

так, як це показано на рис. 7.6.

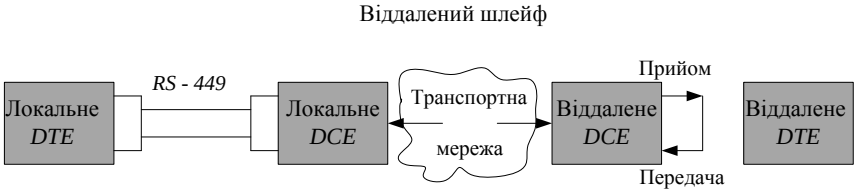


Рис.7.6. Схема утворення віддаленого шлейфу для вимірювань параметрів обладнання усього цифрового каналу

Однак у цьому випадку обов'язковою умовою є використання двонаправленого (дуплексного) каналу передавання між *DTE* та *DCE*. Це не завжди є можливим. Окрім того, щодо шлейфової схеми, то завжди існує невизначеність вимірювань, оскільки неможливо точно розділити вклад у загальний результат вимірювань, що вноситься прямим та зворотним каналами передавання.

7.2. Параметри канального рівню, що підлягають вимірюванням

Вимірювання параметрів канального рівню здійснюють, головним чином, з метою визначення рівня якості передавання протокольних блоків даних (*PDU*). Позначення та визначення цих параметрів доцільно обрати таким чином, щоб вони були інваріантні від специфіки конкретних технологій та обладнання, щодо котрих здійснюються вимірювання. Тому у складі позначення будь-якого параметру канального рівню (якщо мова йде не про конкретну технологію транспортування протокольних блоків даних, а про параметр, що є характерним для будь-якої технології канального рівня) присутня абревіатура *PDU*. Заміна сполучення літер „*PDU*" у позначеннях параметрів на сполучення літер, що ідентифікують конкретну технологію (наприклад, на „*FR*"), означає, що мова йде про параметр конкретної технології транспортування *PDU* (у даному прикладі про технологію *Frame Relay*).

Нижче розглянуто параметри (показники) канального рівня, що

використовуються у практиці експлуатаційних вимірювань параметрів будь-якого обладнання, що побудовано на основі використання тієї чи іншої технології канального рівня.

7.2.1. Показники швидкості передавання PDU (PDUTS)

***PDUTS* (*PDU transfer speed*)** – параметр, що характеризує швидкість передавання *PDU* через вимірювальну точку. Визначається як кількість подій проходження *PDU* через вибрану точку вимірювань (*measurement point, MP*), що зафіксовані протягом вибраного проміжку часу. Враховуються усі *PDU*, що пройшли через *MP*: як коректно транспортовані, так і з помилками. В залежності від вибору величини інтервалу вимірювань розрізняють миттєву та середню швидкість передавання *PDU*. В залежності від рівня зобов'язань, що бере на себе сервіс-провайдер щодо надання транспортної послуги, розрізняють гарантовану (узгоджену) швидкість та швидкість, яка забезпечується при сервісі "з максимальними зусиллями".

PDUTS` – миттєва швидкість передавання *PDU* через вимірювальну точку. Визначається як кількість подій проходження *PDU* через вибрану *MP*, що зафіксовані протягом мінімально припустимого для даної транспортної технології інтервалу вимірювань T_{min}. В багатьох випадках T_{min} вибирають на рівні 1с.

***PDUTS`*** $_{max}$ - верхня припустима межа (тобто, припустиме максимальне значення) *PDUTS`*. Цей показник для окремих транспортних технологій нормується.

PDUTS ^{0} - усереднене на інтервалі сеансу вимірювань значення *PDUTS`*. Тривалість сеансу вимірювань T_0 обумовлюється окремо у сервісних угодах (*service level agreement, SLA*) або вибирається, як правило, на рівні 1 години.

PDUTS $^{0}_{max}$ - верхня припустима межа (тобто, припустиме максимальне значення) $PDUTS^0$. Цей показник у більшості випадків нормується.

Примітка 7.4. Швидкість транспортування вимірюється також у байтах або у бітах за 1с.

7.2.2. Показники обсягу транспортованого трафіка на визначеному проміжку часу

***B_c* (*Committed Burst Size*)** – узгоджений обсяг пульсації, тобто максимальна кількість бітів або байтів, яка буде гарантовано транспортуватися впродовж визначеного проміжку часу *T*.

***B_e* (*Excess Burst Size*)** – додатковий обсяг пульсації, тобто максимальна кількість бітів або байтів, яка буде "з максимальними зусиллями" (але без конкретних гарантій) транспортуватися впродовж визначеного проміжку часу *T*.

7.2.3. Показники затримки передачі PDU (PDUTD)

***PDUTD* (*PDU transfer delay*)** – параметр, що характеризує затримку *PDU* під час його передавання через вимірювальну секцію між увідною та вивідною точками вимірювань.

Примітка 7.5. При організації вимірювань за шлейфовим методом увідна та вивідна *MP* розташовані на одному термінальному вузлі.

$PDUTD_0$ - усереднене на інтервалі сеансу вимірювань значення *PDUTD*. Визначається як середнє арифметичне усіх виміряних значень *PDUTD* за виключенням 10% мінімальних та 10% максимальних значень цього показника в інтервалі даного сеансу вимірювань. Затримка визначається для всіх *PDU*, що пройшли через вимірювальну секцію: як коректно транспортованих, так і з помилками.

$PDUTD_{max}$ - верхня припустима межа (тобто, припустиме максимальне значення) $PDUTD_0$. Цей показник у більшості випадків нормується.

***P* (*$PDUTD_{max}$*)** – ймовірність (частість) перевищення $PDUTD_{max}$. Визначається як відношення кількості подій перевищення значення $PDUTD_{max}$ до загальної кількості сеансів вимірювань величини $PDUTD_0$ протягом однієї години.

***P_{max}* (*$PDUTD_{max}$*)** - припустиме максимальне значення ймовірності перевищення $PDUTD_{max}$. Цей показник в багатьох випадках нормується.

7.2.4. Показники варіації затримки PDU (PDUDV)

***PDUDV* (*PDU delay variation*)** – параметр, що характеризує

відхилення у затримці *PDU* відносно $PDUTD_0$ під час його передавання через вимірювальну секцію між увідною та вивідною точками вимірювань. Так, якщо затримку *k*-го *PDU* в потоці позначити як $PDUTD_k$, то

$$PDUDV_k = |PDUTD_k - PDUTD_0|. \quad (7.1)$$

***PDUDV*$_0$** - усереднене на інтервалі сеансу вимірювань значення *PDUDV* (варіація затримки або джитер). Визначається як середнє арифметичне усіх виміряних значень $PDUDV_k$ за виключенням 10% мінімальних та 10% максимальних значень цього показника в інтервалі даного сеансу вимірювань. Варіація затримки визначається для всіх *PDU*, що пройшли через вимірювальну секцію: як коректно транспортованих, так і з помилками.

***PDUDV*$_{max}$** - верхня припустима межа $PDUDV_0$ (тобто, припустимий максимальний діапазон відхилення *PDUTD* від $PDUTD_0$). Цей показник у більшості випадків нормується.

P (PDUDV*$_{max}$*) – ймовірність (частість) неперевищення $PDUDV_{max}$. Визначається як відсоток *PDU* від загальної кількості *PDU*, що пройшли через вимірювальну секцію у даному сеансі вимірювань, затримки котрих не перевищили $PDUDV_{max}$.

P*$_{min}$ *(PDUDV*$_{max}$*) - припустиме мінімальне значення *P (*$PDUDV_{max}$*)*. Цей показник в багатьох випадках нормується.

7.2.5. Показники втрат PDU під час їхнього транспортування (PDULR)

***PDULR* (*PDU loss ratio*)** – коефіцієнт втрат *PDU*. Параметр, що характеризує втрати *PDU* під час їхнього передавання через вимірювальну секцію між увідною та вивідною точками вимірювань. Визначається як відношення загальної кількості втрачених (у т.ч., відкинутих) *PDU* до загальної кількості переданих *PDU* протягом одного сеансу вимірювань.

***PDULR*$_0$** - усереднене на сумарному інтервалі визначеної серії сеансів вимірювань значення *PDULR* .

Примітка 7.6. Кількість сеансів вимірювань, що складає визначену серію, має бути обгрунтована.

PDULR$_{max}$ **-** верхня припустима межа усередненого на сумарному інтервалі визначеної серії сеансів вимірювань значення *PDULR$_0$* (тобто, припустиме максимальне значення *PDULR$_0$* на сумарному інтервалі визначеної серії сеансів вимірювань). Цей показник в багатьох випадках нормується.

7.2.6. Показники втрат блоків PDU під час їхнього транспортування (PDUSLBR)

***PDUSLBR* (*PDU severe loss block ratio*) -** коефіцієнт втрат блоків *PDU*. Параметр, що характеризує втрати блоків *PDU* під час їхнього передавання через вимірювальну секцію між увідною та вивідною точками вимірювань. Визначається як відношення загальної кількості втрачених (у т.ч., відкинутих) блоків *PDU* до загальної кількості переданих блоків *PDU* протягом однієї серії сеансів вимірювань.

Примітка 7.7. Серія сеансів вимірювань складається із сеансів тривалістю T_s. І якщо кількість втрачених *PDU* на проміжку T_s перевищить поріг s1, то всі *PDU* на цьому проміжку відкидаються, а цей блок *PDU* вважається втраченим.

PDUSLBR$_{max}$ - верхня припустима межа (максимально припустиме значення) *PDUSLBR* (для визначених T_s та s1). Цей показник іноді нормується.

7.2.7.Показники некоректного транспортування PDU (PDU ER)

***PDUER* (*PDU error ratio*) -** коефіцієнт некоректно транспортованих *PDU*. Параметр, що характеризує кількість *PDU,* що були ушкоджені під час їхнього передавання через вимірювальну секцію між увідною та вивідною точками вимірювань. Під ушкодженням розуміється будь-яка невідповідність вмісту інформаційних полів *PDU* або результату підрахунку контрольних сум (який, як правило, фіксується у заголовках *PDU*). Визначається як відношення загальної кількості некоректно транспортованих *PDU* до загальної кількості переданих *PDU* протягом одного сеансу вимірювань.

PDUER$_0$ - усереднене на сумарному інтервалі визначеної серії сеансів вимірювань значення *PDUER* .

PDUER$_{max}$ - верхня припустима межа *PDUER$_0$* (тобто, максимально припустиме значення *PDUER$_0$* на сумарному

інтервалі визначеної серії сеансів вимірювань). Цей показник в багатьох випадках нормується.

7.2.8. Показники швидкості утворення зайвих PDU (PDUSR)

***PDUSR* (*PDU spurious rate*) –** швидкість утворення зайвих *PDU*. Параметр, що характеризує інтенсивність утворення зайвих (фальшивих) *PDU*. Визначається як відношення кількості зайвих *PDU*, що утворились протягом одного сеансу вимірювань, до його тривалості.

***PDUSR*$_0$** - усереднене на сумарному інтервалі визначеної серії сеансів вимірювань значення *PDUSR* .

***PDUSR*$_{max}$** - верхня межа (максимально припустиме значення) *PDUSR*$_0$.

7.2.9. Показники завантаження обладнання

K*$_{зав}$ – *коефіцієнт завантаження обладнання (зокрема, каналу транспортування даних, комутатора, порту або будь-якого іншого мережного обладнання). Характеризує ступінь завантаження обладнання трафіком, який циркулює через це обладнання. Визначається як відношення швидкості передавання *PDU* , що реально просуваються через обладнання, завантаження котрого розглядається, до його пропускної здатності. В залежності від вибору величини інтервалу вимірювань *PDUTS* розрізняють миттєвий та середній коефіцієнт завантаження. Завантажене обладнання може функціонувати одночасно на кількох рівнях телекомунікаційних протоколів, тобто одночасно оброблювати *PDU* різних форматів. Тому коефіцієнт завантаження може визначатися на рівні фізичних сигналів, кадрів канального рівня або мережних пакетів.

Примітка 7.8. Під час обчислювань $K_{зав}$ необхідно слідкувати за однаковістю визначення даних щодо швидкості та пропускної здатності (у бітах або у байтах або у кількості *PDU* за секунду, з урахуванням або тільки даних споживачів або усіх полів визначеного формату *PDU*).

***K'*$_{зав}$** – миттєвий коефіцієнт завантаження обладнання. Визначається як відношення миттєвої швидкості передавання *PDU* (тобто, *PDUTS'*) через вимірювальну точку (логічну або фізичну, яка вибирається, як правило, на уводі або на виводі досліджуваного

обладнання) до пропускної здатності цього обладнання.

К'завтах – верхня припустима межа (тобто, припустиме максимальне значення) *К'зав*. Цей показник для окремих транспортних технологій нормується.

К'зав0 – усереднене на інтервалі сеансу вимірювань значення *К'зав*. Тривалість сеансу вимірювань T_0 обумовлюється окремо у *SLA* або вибирається окремо для кожної телекомунікаційної технології відповідно до нижче наданих нормованих значень.

К'зав0max – верхня припустима межа (тобто, припустиме максимальне значення) $K'_{зав0}$. Цей показник у більшості випадків нормується.

7.2.10. Показники експлуатаційної надійності обладнання

Будуть розглянуті у подальшому на лекції №12.

7.3. Вимірювання параметрів канального рівню обладнання пакетних мереж

Обладнання пакетних мереж передавання даних (МПД) використовується, як правило, на магістральних транспортних мережах і реалізується за специфікаціями технологій канального рівню – таких як *Frame Relay, ATM, Optical Ethernet, X.25* тощо. Проте транспортні мережі можуть також бути реалізованими на мережному рівні засобами стеку протоколів *TCP/IP*.

Примітка 7.8. Обладнання *X.25* наразі знімається із експлуатації внаслідок його моральної застарілості.

Вимірювання параметрів канального рівня здійснюють як для визначення стану працездатності обладнання, так і для оцінки якості його функціонування.

7.3.1. Структура середовища транспортування даних

На рис.7.7 відображена в узагальненому виді структура середовища транспортування протокольних блоків даних (*PDU)* каналами МПД через сукупність мережних доменів $МД_i$.

Домени відправників та отримувачів *PDU*, тобто ДВ та ДО, являють собою кінцеві (термінальні) вузли транспортної мережі, у складі обладнання котрих зазвичай містяться локальні комп'ютерні

мережі, сервери, шлюзи, окремі хости, а також термінальне обладнання (*TE*) абонентського доступу до крайових вузлів (ER) транспортної мережі.

Примітка 7.9. Під словом „домен” у цьому випадку розуміється область території, у межах котрої підтримується однакова технічна політика щодо забезпечення експлуатації ТЛК-обладнання.

Примітка 7.10. Під словом „хост” розуміється комп’ютер (робоча станція), що має *IP*-адресу.

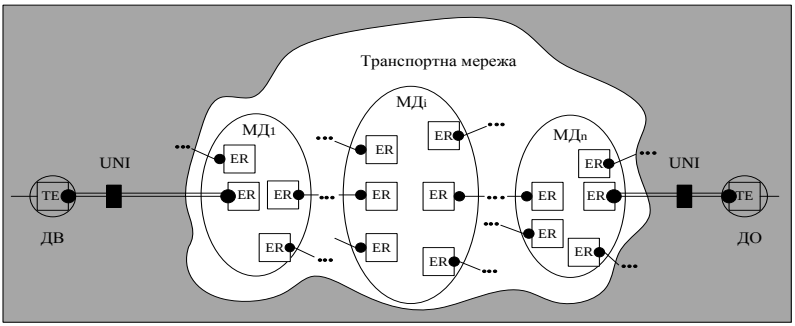


Рис.7.7. Структура середовища транспортування протокольних блоків даних (*PDU)* каналами МПД

Для споживачів мережних ресурсів поряд з послугами абонентського доступу інтерес представляють послуги наскрізного міжвузлового з’єднання типу “споживач – споживач” *("user-to-user" connection*) та типу “точка – точка” (“*end-to–end" network connection*).

У разі надання послуги типу “споживач – споживач” оператор електрозв’язку бере на себе зобов’язання щодо забезпечення узгодженого із споживачем рівня якості обслуговування впродовж усієї ділянки транспортної мережі між термінальними вузлами споживача (тобто, зона відповідальності оператора охоплює також канали абонентського доступу, включаючи термінальне обладнання на обох кінцях з’єднання).

У разі надання послуги типу “точка - точка” сервіс-провайдер має забезпечувати узгоджену якість обслуговування тільки на ділянці, що розташована між крайовими вузлами транспортної мережі, а обладнання доступу до цих крайових вузлів знаходиться у зоні відповідальності споживача.

7.3.2. Базові схеми та точки вимірювань

Точка вимірювання (*MP, measurement point*) – це фізична та (або) логічна точка на структурній схемі організації вимірювань (зокрема, на структурній схемі з’єднань між елементами відповідного ТЛК-обладнання), стосовно котрої діють норми на показники параметрів, що визначають якість мережних ресурсів.

На канальному рівні взаємодії (згідно семирівневої моделі *OSI*) *MP* в залежності от конкретних умов функціонування обладнання може розглядатися або як фізична точка, доступ до котрої забезпечується за допомогою апаратних засобів, або як логічна точка, доступ до котрої забезпечується за допомогою програмних засобів хоста (*TE*), обладнання мережного закінчення (*DCE, NT* тощо) та (або) модулів лінійного закінчення (*LT*), що містяться у складі обладнання крайових вузлів транспортної мережі - крайових комутаторів або маршрутизаторів цієї мережі.

Базова схема вимірювань, що придатна для оцінювання параметрів канального рівня між будь-якими двома кінцевими вузлами транспортної мережі, відображена на рис.7.8, де уся можлива сукупність проміжних мережних доменів та міждоменних каналів передачі (*network section ensemble, NSE*) на шляху просування протокольних блоків даних (*protocol data unit, PDU*) між цими вузлами моделюється однією вимірювальною мережною секцією (NS_0).

Примітка 7.11. У загальному випадку *PDU* між кожною парою кінцевих вузлів можуть транспортуватися в режимі без встановлення фізичних або логічних з’єднань. Шляхи проходження *PDU* в цьому випадку можуть бути різними.

Примітка 7.12. Нагадаємо, що під мережним доменом розуміють будь-який фрагмент мережі, у межах котрого здійснюється єдина політика експлуатації обладнання.

На рис. 7.8 відображено чотири пари точок вимірювань (*measurement point, MP*): $MP_1 - MP_4$. Кожна пара MP_i (у даному випадку індекс *i* ідентифікує місце розташування точок на вимірювальній схемі) відображає *i*-ту точку вимірювань параметрів увідного трафіку ($MP_{in\ i}$) та *i*-ту точку вимірювань параметрів вивідного трафіку ($MP_{egr\ i}$), тобто MP_i – це пара точок $MP_{in\ i}$ та $MP_{egr\ i}$.

Точки MP_{in} зазвичай називають увідними вимірювальними точками (*ingress measurement point, ingress MP*), а точки MP_{egr} – вивідними вимірювальними точками (*egress measurement point, egress MP*).

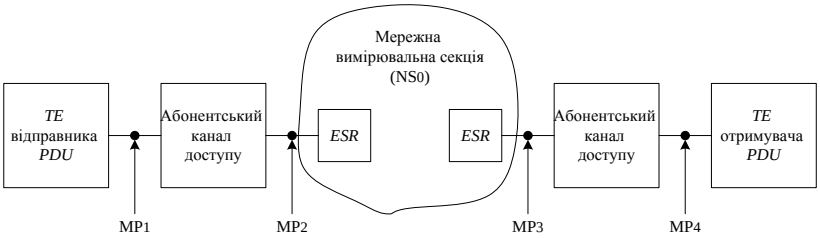


Рис.7.8. Базова вимірювальна схема для оцінювання параметрів наскрізного з'єднання між двома кінцевими вузлами транспортної, де MP_i - і-та пара точок вимірювань; *ESR* - крайовий комутатор/маршрутизатор (або маршрутизатор доступу); *TE* - термінальне обладнання.

Під час здійснення вимірювань на фізичному (та іноді на канальному) рівні (згідно моделі *OSI*) вимірювальні точки являють собою фізичні точки, що утворюються за допомогою апаратних інструментальних засобів. Під час здійснення вимірювань на канальному, мережному або більш високому рівні інформаційної взаємодії вимірювальні точки являють собою логічні точки, що утворюються за допомогою програмних інструментальних засобів.В процесі вимірювань канальних параметрів розглядається потік *PDU*, що проходить через визначену пару вимірювальних точок – увідну та вивідну, які вибираються на границях *NS* та каналів передавання даних.

В експлуатаційній практиці з метою спрощення процедур вимірювань використовують шлейфовий метод, згідно з яким шлях

проходження потоку *PDU* утворюється таким, щоб увідна та вивідна точки вимірювань були сумісними та могли оброблятися одним інструментальним засобом. Це дозволяє позбавитись проблеми синхронізації точок вимірювань. Зокрема, на практиці часто використовується шлейфова схема вимірювань, згідно якої здійснюється замикання точок $MP_{in\ i}$ та $MP_{egr\ i}$ на віддаленому кінці вимірювальної схеми. Як правило, таке замикання під час вимірювань на канальному, мережному та (або) сеансовому рівнях моделі *OSI* виконується штатними програмними засобами відповідного телекомунікаційного обладнання. Пояснення щодо шлейфового методу вимірювань раніш вже розглядались у матеріалі лекції №6 (див., зокрема, рис.6.15а).

У точках вимірювань (*measurement point, MP*) здійснюються спостереження за подіями і вимірюються певні характеристики цих подій, що пов'язані із проходженням *PDU* через ці точки. Згідно з рис.7.8 знайшли використання чотири пари точок вимірювань. Оцінювання параметрів наскрізного з'єднання типу "споживач – споживач" здійснюється шляхом синхронного зіставлення певних характеристик подій, що спостережуються у точках MP_1, за умов здійснення замикання пари точок MP_4 . Оцінювання параметрів наскрізного з'єднання типу "точка - точка" здійснюється шляхом синхронного зіставлення певних характеристик подій, що спостережуються у точках MP_2, за умов здійснення замикання пари точок MP_3 . Оцінювання якості транспортування *PDU* через канал абонентського доступу здійснюється аналогічним методом. Наприклад, під час оцінювання параметрів абонентського каналу доступу відправника *PDU* вимірюються характеристики подій у парі точок вимірювань MP_1 за умов замикання точок MP_2. Або вимірюються характеристики подій у парі точок MP_2 за умов замикання точок MP_1.

Базова схема вимірювань для оцінювання параметрів окремої проміжної *NS* (або *NSE*) транспортної мережі показана на рисунку 7.9.

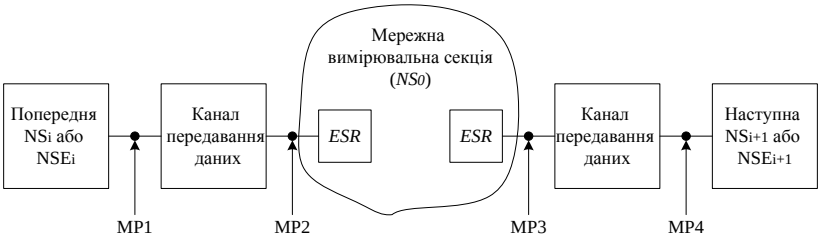


Рис.7.9. Базова вимірювальна схема для оцінювання параметрів проміжної мережної вимірювальної секції, де MP_i - і-та пара точок вимірювань; NS_i, NSE_i - і-та мережна секція (мережний домен або ансамбль мережних доменів); *ESR* - крайовий комутатор/маршрутизатор

Із рис. 7.9 видно, що базова схема вимірювань параметрів проміжної секції між будь-якими двома парами точок вимірювань принципово не відрізняється від схеми вимірювань параметрів наскрізних з'єднань.

Примітка 7.13. Такі вимірювання здійснюють з метою локалізації місць виникнення невідповідностей в роботі мережного обладнання, зокрема місць перенавантажень трафіком або місць виникнення завад в каналах зв'язку.

Базова схема вимірювань для оцінювання параметрів послуги абонентського доступу показана на рис.7.10.

Із рис. 7.10 видно, що базова схема вимірювань параметрів цієї послуги передбачає здійснення замикання між собою точок MP_2 та MP_3, розташованих на вузлі доступу до ресурсів транспортної мережі, та організації вимірювань характеристик подій, що спостерігаються у синхронізованих між собою точках MP_1 та MP_4 на термінальному вузлі споживача.

Існує також можливість організації вимірювань на стороні оператора електрозв'язку (або сервіс-провайдера): в цьому випадку замикаються точки MP_1 та MP_4, а події спостерігаються у точках MP_2 та MP_3.

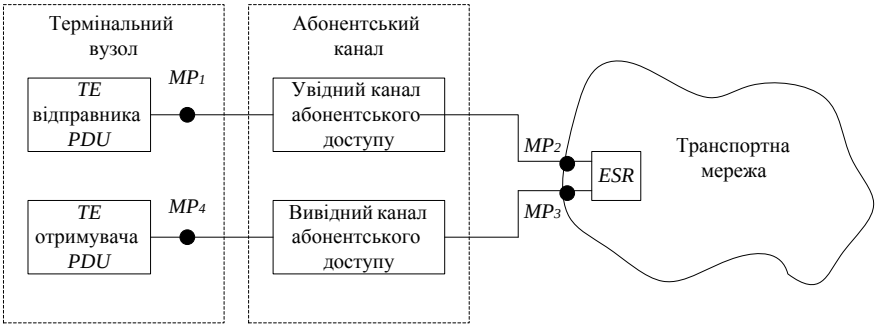


Рис.7.10. Базова схема вимірювань параметрів абонентського доступу, де *ESR* - крайовий комутатор/маршрутизатор (або маршрутизатор доступу); *MPi* - і-та точка вимірювань

7.3.3. Кореспондовані події та їх характерні наслідки

Під час оцінювання характеристик процесу транспортування *PDU* за базовими вимірювальними схемами, що надані вище, використовується поняття **"визначальна подія щодо транспортування *PDU*"** (надалі - визначальна подія). Така подія має місце, якщо виникає конкатенація (тобто, одночасна поява) наступних подій:

1) *PDU* перетинає *MP*, щодо якої організовано спостереження;

2) стандартна процедура верифікації контрольної суми у заголовку *PDU* (якщо це передбачено протоколом) функціонує коректно;

3) поля адрес відправника і отримувача у заголовку *PDU* є дійсними.

Зазвичай розрізняють чотири види визначальних подій:

1) подія виводу певним чином згенерованого тестового *PDU* із місцевого *i*-го вузлу (за ініціативою котрого здійснюються вимірювання), коли цей *PDU*, рухаючись в напрямку віддаленого *i+1*-го вузла – отримувача тестової послідовності даних, вибраного у даному сеансі вимірювань, перетинає точку $MP_{egr\ i}$, що асоціюється із місцем з'єднання цього місцевого ініціюючого вузла із середовищем транспортування даних;

2) подія уводу тестового *PDU* у вибраний віддалений *i+1*-й

вузол транспортної мережі, коли цей *PDU*, рухаючись від місцевого *i*-го вузла через середовище транспортування даних, перетинає точку $MP_{in\ i+1}$, що асоціюється із місцем з'єднання віддаленого $i+1$-го вузла із середовищем транспортування даних;

3) подія виводу ретрансльованого тестового *PDU* із віддаленого $i+1$-го вузла, коли цей *PDU*, рухаючись в напрямку місцевого *i*-го вузла – відправника тестових даних, перетинає точку $MP_{egr\ i+1}$, що розташована у місці з'єднання цього віддаленого $i+1$-го вузла із середовищем транспортування даних;

4) подія уводу тестового *PDU* у місцевий *i*-й вузол транспортної мережі, коли цей *PDU*, рухаючись від $i+1$-го віддаленого вузла через середовище транспортування даних, перетинає точку $MP_{in\ i}$, що асоціюється із місцем з'єднання місцевого ініціюючого вузлу із середовищем транспортування даних.

Аналогічних чотири види визначальних подій слід розглядати і під час оцінювання параметрів будь-яких проміжних мережних секцій або ансамблів мережних секцій, параметрів наскрізних з'єднань та параметрів послуг некомутованого доступу.

В процесі оцінювання якості надання транспортної послуги, як правило, розглядають так звані **кореспондовані (пов'язані) визначальні події (*corresponding events*).**

Будь-яку подію виводу *PDU*, що спостерігається у певним чином вибраній одній вимірювальній точці, називають кореспондованою з подією уводу *PDU* , що спостерігається в іншій вимірювальній точці, якщо обидві ці події "створив" один і той же протокольний блок даних під час проходження через визначену вимірювальну секцію. Цей *PDU* також називається кореспондованим.

Кореспондовані визначальні події (надалі - кореспондовані події) є наслідком синхронного розгляду процесу проходження *PDU* через дві різні вимірювальні точки. При цьому є важливим визначення проміжку часу T_{max}, впродовж котрого процес проходження *PDU* повинен розглядатися в рамках кожної спроби визначення факту кореспондованості очікуваних подій. За звичайних умов T_{max} – це максимально припустима затримка *PDU* на визначеній ділянці мережі. Якщо реальний час затримки *PDU* τ перевищує T_{max}, то такий *PDU* вважається втраченим (загубленим).

Інтервал вимірювань в процесі поточного контролю відповідності $T_{вим}$ має бути більшим за інтервал визначення кореспондованості між парою визначальних подій T_{max}, оскільки потрібен певний час на аналіз наслідків такого визначення.

7.3.4. Характерні наслідки вияву визначальних подій

У процесі оцінювання канальних параметрів важливо не тільки виявити усі визначальні події, що відображають процес транспортування *PDU* через визначені вимірювальні точки на певних проміжках часу, і не тільки факти їхньої можливої кореспондованості. Необхідно також в кінці кожного елементарного тесту на виявлення кореспондованих подій, який запускається на виконання кожний раз в момент, коли черговий *PDU* перетинає увідну *MP*, на вивідній *MP* після виявлення кореспондованої події (якщо такий факт мав місце) виміряти певні характеристики (або виявити певні ознаки) прояву цієї події. І, потім, на основі отриманих значень виміряних характеристик (або виявлених ознак) визначити один із нижченаведених можливих наслідків просування *PDU* на шляху між двома вимірювальними точками. *PDU*, який перетинає контрольовану вивідну *MP*, може бути або успішно транспортований, або спотворений помилками, або втрачений (загублений), або фальшивий (зайвий).

З урахуванням вищезазначеного та пояснювальних схем, які відображені на рис.7.11, характерні наслідки проходження кожного *PDU* через вимірювальну схему фіксуються наступним чином.

1) *PDU* вважається успішно переданим у разі вияву конкатенації наступних умов:

а) усі вивідні *MP*, на котрих виявлені кореспондовані визначальні події протягом заданого проміжку часу $t \le T_{max}$, є дозволеними;

б) усі поля формату *PDU*, який перетнув дозволену увідну *MP*, включені у відповідні поля кореспондованого *PDU* (або кореспондованих фрагментів *PDU*), що перетнув (перетнули) вивідну *MP*;

в) вміст поля даних отриманого *PDU* (або сукупності отриманих фрагментів) співпадає із вмістом цього поля, що входить до складу кореспондованого переданого *PDU*;

2) *PDU* вважається спотворений помилками (тобто, прийнятим з помилками) у разі вияву конкатенації наступних умов:

а) усі вивідні *MP*, на котрих виявлені кореспондовані визначальні події протягом заданого проміжку часу $t \le T_{max}$, є дозволеними;

б) усі поля формату *PDU*, який перетнув дозволену увідну *MP*, включені у відповідні поля кореспондованого *PDU* (або кореспондованих фрагментів *PDU*), що перетнув (перетнули) вивідну *MP*;

в) вміст поля даних отриманого *PDU* (або сукупності отриманих фрагментів *PDU*) не співпадає із вмістом цього поля, що входить до складу кореспондованого з ним переданого *PDU* та (або) дані у заголовку отриманого *PDU* пакета (або заголовках отриманих фрагментів *PDU*) не є коректними.

3) *PDU* вважається втраченим у разі вияву диз'юнкції наступних умов:

а) усі поля формату *PDU*, який перетнув дозволену увідну *MP*, включені у відповідні поля кореспондованого з ним *PDU* (або кореспондованих фрагментів *PDU*), що перетнув (перетнули) вивідну *MP*, але мали місце кореспондовані події у недозволених вивідних *MP*, тобто відбулася некоректна маршрутизація *PDU*;

б) одне або кілька полів формату *PDU*, який перетнув дозволену увідну *MP*, відсутні у кореспондованого з ним *PDU* (або кореспондованих фрагментів *PDU*), що перетнув (перетнули) вивідну *MP*, тобто відбулося знищення *PDU* або його частини на шляху між двома *MP*.

4) *PDU* вважається фальшивим, якщо виявлена подія виводу цього *PDU*, для котрої протягом заданого проміжку часу $t \le T_{max}$ не знайшлося кореспондованої з нею події уводу *PDU*.

У зв'язку з наданими вище визначеннями характерних наслідків проходження *PDU* через вимірювальну секцію слід підкреслити, що ці визначення базуються на спостереженнях визначальних подій у певним чином вибраних вимірювальних точках. Шляхом відповідного вибору цих точок досягається можливість оцінювання параметрів якості обслуговування щодо будь-якого каналу абонентського доступу, наскрізного з'єднання або ділянки такого з'єднання, зокрема каналу передачі даних, *NS* або *NSE*.

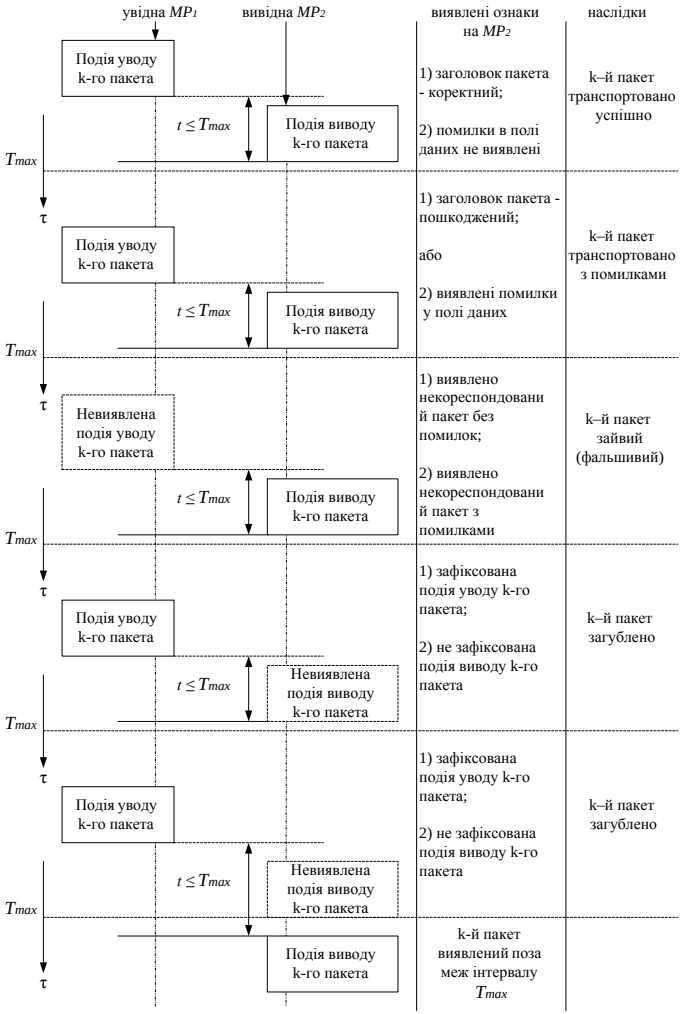


Рис.7.11. Характерні наслідки вияву визначальної події під час передавання даних

Примітка 7.14. Певна частина *PDU* з помилками у заголовках, що не виявлені механізмом підрахунку контрольної суми, далі в процесі обробки будуть знищені або переспрямовані за допомогою інших процедур. В таких ситуаціях події уводу *PDU* у вимірювальну секцію з помилковими заголовками не будуть створювати кореспондовані з ними події виводу *PDU* із цієї секції, тобто такі *PDU* будуть вважатися втраченими. Інша частина *PDU* з помилками у заголовках, що не була

знищена або переспрямована, буде вважатися прийнятою з помилками.

У наданих визначеннях враховується можливість фрагментації *PDU*, коли наслідком події уводу *PDU* у вимірювальну секцію є не одна, а кілька подій виводу фрагментів цього *PDU*. При цьому, якщо будь-який фрагмент виявиться втраченим, то вважається втраченим весь *PDU*. Якщо втрат фрагментів не виявлено, але виявлені помилки хоча б в одному фрагменті, то весь *PDU* вважається помилковим. Тільки тоді *PDU* вважається успішно переданим, коли усі фрагменти цього *PDU* були успішно просунуті через дозволені точки виводу.

Примітка 7.15. Характерним наслідком вияву певної сукупності визначальних подій є втрата блоку *PDU* (*PDU severe loss block outcome*). Фіксується втрата блоку *PDU* у тому випадку, коли протягом інтервалу спостереження T_S відношення кількості подій виводу кореспондованих *PDU* у дозволених точках виводу до загальної кількості подій уводу *PDU* через дозволену точку уводу перевищує порогове значення s1.

7.4. Вимірювання параметрів функціональності послуг

Оскільки множину параметрів функціональності транспортних послуг складають параметри швидкості передавання *PDU* та параметри обсягу трафіка, що транспортується впродовж визначеного проміжку часу, то основний метод оцінювання цих параметрів базується на підрахунку кількості *PDU*, що перетинають вибрану *MP* протягом визначеного проміжку часу. Точка та інтервал вимірювання, а також ознаки сукупності *PDU,* що мають бути враховані, вибираються виходячи із цілей вимірювань і визначаються далі стосовно кожної транспортної технології, яка використовується оператором електрозв'язку.

7.5. Вимірювання параметрів якості передавання протокольних блоків даних

Загальним способом оцінювання поточних значень параметрів якості передавання блоків даних є проведення їх періодичних вимірювань через фіксовані інтервали часу. Як правило, здійснюються прямі вимірювання характеристик тестового трафіку. Елементарний акт вимірювання виконується відносно *PDU*, що перетинає увідну вимірювальну точку (*ingress*

measurement point, ingress MP), і полягає у виявленні можливої кореспондованої події у вивідній вимірювальній точці (*egress measurement point, egress MP*) та фіксації наслідків цієї події (наприклад, втрата *PDU*, затримка та величина затримки, помилка в полі даних і т. ін.). Процес вимірювань полягає у здійсненні серії послідовних елементарних актів вимірювання. В результаті отримують дані, що використовуються як похідні в процедурах оцінювання значень вимірювальних параметрів.

У більшості випадків використовується шлейфова схема організації вимірювань (як через локальний, так і через віддалений шлейф), тобто вивідні порти вимірювальної секції одного напрямку передавання *PDU* фізично або логічно замикаються на увідні порти цієї секції із зворотного напрямку передавання так, щоби забезпечувалась можливість обробки подій, що виникають на увідній та вивідній вимірювальних точках, єдиним локально розташованим інструментальним засобом вимірювань.

Вимірювання виконуються в режимі тестування. Структура тестового потоку PDU відображена на рис.7.12. Процес вимірювань полягає у надсиланні на вивідну *MP* певним чином визначеної сукупності (групи) тестових *PDU*, котрі, проходячи через вимірювальну секцію в одному напрямку, через вибрані точки перемикання напрямків на віддаленому кінці вимірювальної секції і далі через вимірювальну секцію у зворотному напрямку, мають спостерігатися на увідній *MP*, що має бути розташована на тому ж вузлі мережі, де розташована вивідна *MP*.

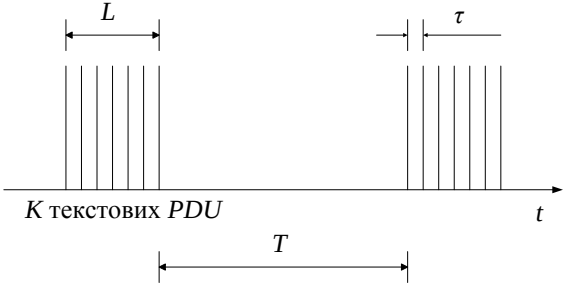


Рис.7.12. Ілюстрація структури тестового потоку PDU при організації вимірювань параметрів канального рівня

Увідні та вивідні *PDU* генеруються і оброблюються єдиним

вимірювальним засобом. Одна група складається із N тестових *PDU*, котрі передаються із інтервалом τ. Генерація однієї групи тестових *PDU* триває L одиниць часу, де $L = N \times \tau$. Групи *PDU* генеруються з періодом T. Більшість показників параметрів транспортних послуг вимірюється на інтервалі T. Тому цей інтервал називають сеансом вимірювань. Деякі показники не можуть бути оцінені протягом одного сеансу вимірювань. Для оцінювання таких показників здійснюється серія сеансів вимірювань. Тривалість однієї серії сеансів вимірювань позначається як T_0. Розмір (довжина) будь-якого тестового *PDU* в процесі одного сеансу вимірювань не змінюється і дорівнює ν байт. У цьому разі кількість груп *PDU*, що враховується протягом однієї серії сеансів вимірювань N_0, обчислюється за формулою: $N_0 = T_0 \setminus T$.

Значення ν, τ, N, T та T_0 нормуються у розрізі кожної телекомунікаційної технології, що мають застосування на практиці. Для більшості телекомунікаційних технологій дані, що є необхідними для обчислення цих параметрів, накопичуються у базах *MIB* контрольованого обладнання за допомогою механізмів протоколу *SNMP*.

У процесі вимірювань необхідно дотримуватись наступних вимог:

1) Вимірювання повинні за ідентичних умов проведення вимірювань давати однакові результати, тобто забезпечувати відтворюваність результатів вимірювань.

2) Для незначних змін умов проведення вимірювань повинні спостерігатись незначні відхилення результатів вимірювань.

3) Необхідно на кількісному рівні оцінювати можливі похибки вимірювань. На основі аналізу похибок мають бути сформульовані вимоги до інструментальних засобів та умов проведення вимірювань, дотримання яких дозволить знизити похибки або тримати їх у припустимих межах.

4) Якщо розмір ν тестових *PDU* не регламентується, то з метою зменшення часу їхньої обробки величина ν має бути якнайменшою.

5) Інтервал $L = N \cdot \tau$, що визначає час передавання будь-якої однієї групи тестових *PDU* через вимірювальну секцію, повинен бути таким, щоб імовірність зміни маршруту їхнього проходження

між вимірювальними точками була достатньо малою.

6) Якщо інтервал τ між тестовими *PDU* у групі вибрано занадто малим, то *PDU* будуть надсилатись у мережу занадто швидко, що може викликати їхню буферизацію у вихідних чергах портів мережного обладнання. Для уникнення буферизації тестових *PDU* під час вимірювань необхідно визначити мінімально припустиме значення часу τ, при якому тестові *PDU* не впливають один на одного.

7) Для найбільш повного визначення характеру змін значень вимірюваних параметрів у реальному часі інтервал $\boldsymbol{T}$ між сусідніми групами тестових *PDU*, що просуваються через вивідну *MP*, повинен бути достатньо малим. З іншого боку, з метою зменшення похибок вимірювання через вплив тестового трафіку на поточну завантаженість мережних ресурсів значення інтервалу $\boldsymbol{T}$ доцільно збільшувати. Тому оптимальне значення $\boldsymbol{T}$ на практиці визначається емпіричним шляхом з урахуванням конкретних цілей та умов проведення вимірювань.

8) Часто оцінки значень вимірюваних параметрів залежать не тільки від розмірів, але і від типу *PDU*, які були використані в процесі вимірювань. Тому, визначаючи певний параметр або вказуючи його конкретне значення, завжди слід зазначати, *PDU* якого типу використовувались у процесі вимірювань.

9) Характеристики апаратних засобів та програмного забезпечення (ПЗ) вузлів мережі, які задіяні у процесі вимірювань, можуть впливати на результати вимірювань. Особливо це стосується випадків, коли реєстрація часу настання мережних подій здійснюється засобами прикладного ПЗ вузла мережі, а не засобами операційної системи. Тому у випадку, коли необхідно вимірювати параметри затримок *PDU* у каналах зв'язку між вузлами мережі, доцільно розглянути можливість використання замість штатних засобів вузла мережі в якості вимірювального обладнання спеціалізованих інструментальних засобів, наприклад, аналізатора протоколів.

Метод, умови, точки та порядок вимірювань коефіцієнтів завантаження обладнання $K'_{зав}$ та $K'_{зав0}$ мають відповідати визначеним для випадку вимірювань показників швидкості передавання *PDU*.

Умови та порядок контролю показників надійності будуть розглянуті у подальшому на лекції №12.

Контрольні питання до сьомої лекції

1. Наведіть та поясніть узагальнену схему вимірювань параметрів канального рівню.
2. У чому полягають переваги шлейфового методу організації вимірювань?
3. Наведіть та поясніть схему організації локального шлейфу на *DTE*.
4. Наведіть та поясніть схему утворення локального шлейфу на *DCE* (з боку свого *DTE*).
5. Наведіть та поясніть схему утворення локального шлейфу на *DCE* (з боку транспортної мережі).
6. Наведіть та поясніть схему утворення віддаленого шлейфу для аналізу параметрів каналу передавання між локальним та віддаленим *DCE*.
7. Наведіть та поясніть схему утворення віддаленого шлейфу для вимірювань параметрів обладнання усього цифрового каналу.
8. Назвіть та надайте визначення показникам швидкості передавання *PDU*.
9. Назвіть та надайте визначення показникам обсягу транспортованого трафіка на визначеному проміжку часу.
10. Назвіть та надайте визначення показникам затримки передачі *PDU*.
11. Назвіть та надайте визначення показникам варіації затримки *PDU*.
12. Назвіть та надайте визначення показникам втрат *PDU* під час їхнього транспортування.
13. Назвіть та надайте визначення показникам некоректного транспортування *PDU*.
14. Назвіть та надайте визначення показникам швидкості утворення зайвих *PDU*.
15. Надайте визначення коефіцієнту завантаження обладнання.
16. Назвіть та надайте визначення показникам експлуатаційної надійності обладнання.
17. Відобразіть в узагальненому виді структуру середовища

транспортування протокольних блоків даних (*PDU*) каналами МПД.

18. Що таке точка вимірювання (MP, measurement point)?

19. Відобразіть та поясніть базову схему вимірювань, що придатна для оцінювання параметрів канального рівня між будь-якими двома кінцевими вузлами транспортної мережі.

20. Відобразіть та поясніть базову схему вимірювань для оцінювання параметрів окремої проміжної *NS* (або *NSE*) транспортної мережі.

21. Відобразіть та поясніть базову схему вимірювань для оцінювання параметрів послуги абонентського доступу.

22. Надайте визначення кореспондованим подіям та їх характерним наслідкам.

23. У чому сутність методів вимірювань параметрів функціональності послуг?

24. Яким чином реалізовуються методи вимірювань параметрів якості передавання протокольних блоків даних?

25. Яких вимог необхідно дотримуватись у процесі вимірювань?

Література до сьомої лекції

1) В.Г. Оліфер, Н. А.Оліфер. Комп'ютерні мережі. Принципи, технології, протоколи: Посібник для вузів. Друге видання – СПб.: Питер, 2003. Розділ 21, стор. 816 – 828.

2) І.Г. Бакланов. Технології вимірювань у сучасних телекомунікаціях. –М.: ЕКО-ТРЕНДЗ, 1998. Розділ 10.3.

3) І.Г. Бакланов. Технології вимірювань первинної мережі. Частина друга. –М.: ЕКО-ТРЕНДЗ, 2000. Розділ 4.

4) І.Г. Бакланов. Методи вимірювань у системах зв"язку.. –М.: ЕКО-ТРЕНДЗ, 1999. Розділи 4 та 6.

САМОСТІЙНЕ ЗАНЯТТЯ ЗА МАТЕРІАЛАМИ ЛЕКЦІЇ №7 ВИМІРЮВАННЯ ПАРАМЕТРІВ ОБЛАДНАННЯ FRAME RELAY та xDSL

Норми на параметри канального рівню не можуть бути визначені безвідносно до конкретних характеристик застосованих телекомунікаційних технологій та умов їхнього використання. Тому нижче, як приклад, розглядаються технології вимірювання параметрів та норми на ці параметри у розрізі популярних технологій канального рівня - технології *Frame Relay* та технології *xDSL* .

7.6. Вимірювання параметрів обладнання систем передавання фреймів на транспортній мережі *Frame Relay*

Обладнання систем передавання фреймів за технологією *Frame Relay* (надалі скорочено - *FR*) використовується як для транспортування фреймів *FR* каналами глобальної транспортної мережі, так і для організації абонентського доступу до транспортної мережі. У цьому підрозділі мова йде лише про транспортну мережу *FR*. Технологія вимірювань параметрів абонентського доступу, що здійснюється з використанням обладнання *FR*, розглядається у наступному підрозділі.

7.6.1. Схеми організації вимірювань

Послуга із транспортування фреймів *FR*-каналами транспортної мережі надається оператором *FR*-мережі у двох модифікаціях: для наскрізних з'єднань типу "точка – точка" (коли обладнання абонентського *FR*-доступу знаходиться у зоні відповідальності оператора електрозв'язку або сервіс-провайдера) та для наскрізних з'єднань типу "споживач – споживач" (коли обладнання абонентського *FR*-доступу знаходиться у зоні відповідальності споживачів).

Для організації вимірювань зазвичай використовується шлейфова схема як при з'єднаннях типу "точка – точка" (така схема показана на рис.7.13), так і при з'єднаннях типу "споживач – споживач".

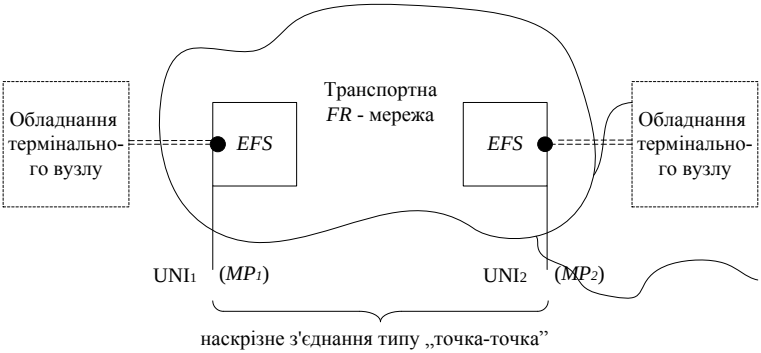


Рис. 7.13. Схема організації вимірювань параметрів обладнання *FR* при наскрізному з’єднанні типу “точка – точка”

На рис.7.14 показана схема організації вимірювань параметрів обладнання *FR* при наскрізному з’єднанні типу „користувач – користувач”. Як бачимо, за цією схемою у ланцюг вимірювань включені також канали абонентського доступу користувачів через пристрій *FRAD* (*Frame Relay Access Device*) до найближчого крайового комутатору *EFS* (*Edge FR-Switch*) транспортної *FR*-мережі.

7.6.2. Вимірювані параметри

1) **Параметри функціональності послуг із транспортування фреймів - *AR, CIR, EIR, Bc, Be*** та ***T***.

***AR* (*Access Rate*) -** швидкість доступу до транспортної мережі. *AR* – це максимальна швидкість передавання даних, яку забезпечує фізичний канал абонентського доступу до транспортної мережі (тобто, *AR* – це пропускна спроможність каналу доступу). Вимірюється, як правило, у кількості транспортованих через канал байтів протягом 1 секунди.

Гарантовану верхню межу швидкості передавання протокольних блоків даних (у даному випадку, фреймів) ***PDUTS***` при наданні послуг на основі використання обладнання *FR* називають *CIR.*

***CIR* (*Committed Information Rate*)** – це узгоджена (інші назви - середня, обов’язкова) швидкість передавання даних споживача, що вимірюється у кількості переданих байтів протягом обумовленого

інтервалу визначення *CIR*, яку мережний оператор зобов'язався гарантовано підтримувати. Тривалість сеансу вимірювань *T* (тобто, інтервал визначення *CIR*) обумовлюється окремо у сервісній угоді *SLA* між користувачем та оператором або вибирається так, щоб протягом одного сеансу вимірювань була передана одна група із *N* фреймів (див. рис.7.12).

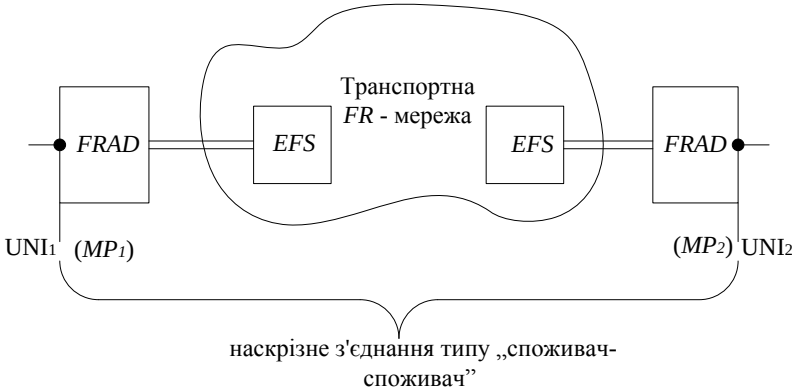


Рис. 7.14. Схема організації вимірювань параметрів обладнання *FR* при наскрізному з'єднанні типу "споживач - споживач"

Припустиму верхню межу швидкості ***PDUTS*`** при наданні послуг "з максимальними зусиллями" на основі використання обладнання *FR* називають *EIR*.

***EIR* (*Excess Information Rate*)** – додаткова (до *CIR*) швидкість передавання даних споживача, що вимірюється у кількості переданих байтів протягом обумовленого інтервалу визначення *CIR*, яку мережний оператор зобов'язався підтримувати "з максимальними зусиллями". Тривалість сеансу вимірювань *T* (тобто, інтервал визначення *EIR*) вибирається такою ж, як і при визначенні *CIR*.

2) Параметри якості транспортування фреймів *QoS* та *NP*

Із всієї множини параметрів канального рівня, що розглядались на лекції №7, зробимо уточнені визначення декількох із них. Саме тіх, що визначають специфіку використання *FR*-обладнання на вітчизняних МПД. Це не означає, що тільки ці параметри

вимірюються та нормуються в експлуатаційній практиці, коли мова йде про *FR*-обладнання. Деякі інші параметри, як це буде нижче показано, теж вимірюються і нормуються. Однак технологія їхнього вимірювання не має особливостей щодо того, що було розглянуто на лекції №7.

Звернемо увагу, що мнемонічні позначення нижченаведених параметрів отримано шляхом заміни у позначеннях канальних параметрів, що розглядались на лекції №6, буквосполучення "*PDU*" на "*FR*", оскільки у даному випадку в якості *PDU* використовуються фрейми *FR*.

Крім того, підкреслимо, що множина параметрів якості транспортування фреймів для з'єднань типу "споживач – споживач" та "точка – точка" вибрана однаковою.

Таким чином, щодо трафіка *FR* прийняті нижченаведені уточнені визначення параметрів.

Характеристики втрат фреймів

$\boldsymbol{FRLR_{max(CIR)}}$ – максимально припустиме значення коефіцієнту втрат фреймів, що відправлені із додержанням заданих значень *CIR* (тобто, за умов, коли у полі формату фрейма ознака *DE=0*). Визначається як відношення загальної кількості втрачених фреймів потоку *CIR* протягом однієї серії сеансів вимірювань до загальної кількості переданих фреймів цього потоку.

$\boldsymbol{FRLR_{max(EIR)}}$ - максимально припустиме значення коефіцієнту втрат фреймів, що відправлені із ознакою *DE=1*. Визначається як відношення загальної кількості втрачених фреймів додаткового потоку *EIR* протягом однієї серії сеансів вимірювань до загальної кількості переданих фреймів цього потоку.

Характеристики навантаження FR- обладнання

$\boldsymbol{K'_{зав0max}(IP)}$ – верхня межа середнього коефіцієнту навантаження обладнання *IP* (для випадків, коли *FR*-мережа виконує функції транспортування пакетів *IP*).

$\boldsymbol{K'_{зав0max}(FR)}$ - верхня межа середнього коефіцієнту навантаження обладнання *FR*.

Характеристики затримки фреймів

$\boldsymbol{FRTD_{max(CIR)}}$ - максимально припустиме значення затримки фреймів $FRTD_0$, усередненої на інтервалі сеансу вимірювань значення *FRTD* щодо потоку *CIR*, тобто потоку фреймів, що

відправлені із додержанням заданих значень *CIR* (за умов, коли ознака *DE=0*). Визначається як середнє арифметичне усіх виміряних значень *FRTD* за виключенням 10% мінімальних та 10% максимальних значень цього показника в інтервалі даного сеансу вимірювань.

***FRTD*$_{max(EIR)}$** - максимально припустиме значення затримки фреймів *FRTD*$_0$, усередненої на інтервалі сеансу вимірювань значення *FRTD* щодо потоку *EIR*, тобто потоку фреймів, що відправлені із додержанням заданих значень *EIR* (за умов, коли ознака *DE=1*). Визначається як середнє арифметичне усіх виміряних значень *FRTD* за виключенням 10% мінімальних та 10% максимальних значень цього показника в інтервалі даного сеансу вимірювань.

Характеристики некоректного транспортування фреймів (FRER)

***FRER*$_{max}$ –** максимально припустиме значення кількості прийнятих фреймів із виявленими помилками на сумарному інтервалі визначеної серії сеансів вимірювань. Цей показник фактично являє собою параметр *BLER* або *CRC ERR* (в залежності від того, яким чином виявляються помилки), якщо під блоком бітів розуміти фрейм.

7.6.3. Нормативи на параметри наскрізних FR-з'єднань

Рекомендовані нормативні значення параметрів якості транспортування потоків фреймів каналами транспортної *FR*-мережі для наскрізних з'єднань типу "точка - точка" надано у табл. 7.1.

Таблиця 7.1

Норми на параметри якості транспортування потоків фреймів каналами транспортної мережі для наскрізних з'єднань типу "точка – точка"

Вимірювані параметри	Характеристика параметра	Нормативне значення
***FRTD*$_{max\ (CIR)}$**	Верхня межа щодо затримки фреймів з ознакою *DE*=0 (тобто, для потоку *CIR*), мс	80

P_{max} $(FRTD_{max})$	Поріг ймовірності перевищення $FRTD_{max}$ для потоку *CIR*, безрозмірний	1×10^{-2}
$FR\ LR_{max\ (CIR)}$	Верхня межа втрат фреймів потоку *CIR*, безрозмірна	1×10^{-3}
$FRER_{max}$	Верхня межа помилкових фреймів, безрозмірна	1×10^{-4}
$Кг_{min}$	Нижня межа коефіцієнту готовності обладнання *FR*	0,996
$MTTR_{max}$	Верхня межа середнього часу відновлення працездатності обладнання *FR*, хвилин	300

Аналізуючи наведені у табл. 7.1 нормативні значення параметрів, слід зазначити, що вони стосуються лише PVC-з'єднань і визначені, виходячи з умови необхідності забезпечення якості транспортування пакетів магістральною транспортною *IP*-мережею, що накладена на мережу *FR*. У свою чергу, якість передавання пакетів *IP* визначається нормами, які будуть розглянуті далі на лекції №8.

Щодо норми на параметр $FRER_{max}$ слід мати на увазі наступне. Як правило, на практиці вимірювання усередненого значення блокової помилки $FRER_0$ в процесі поточного контролю відповідності не здійснюється. Однак в процесі пошуку вирішення проблем невідповідності необхідно упевнитися, що поточні значення цього параметру не перевищують норми (тобто, нормативного значення $FRER_{max}$) на усіх вузлах (проміжних та крайових) впродовж PVC- з'єднання. Дані, що є необхідними для обчислення поточних значень цього параметра, фіксуються на основі спостереження за параметром *FCS* та накопичуються у базах *MIB* за допомогою механізмів протоколу *SNMP*.

Рекомендовані нормативні значення параметрів якості транспортування потоків фреймів каналами транспортної *FR*-мережі для наскрізних з'єднань типу "споживач – споживач" надано у табл. 7.2.

Таблиця 7.2

Норми на параметри якості транспортування потоків фреймів для наскрізних з'єднань типу "споживач – споживач"

Вимірювані параметри	Характеристика параметра	Клас 0	Клас 1
$\boldsymbol{FRTD_{max\ (CIR)}}$	Верхня межа щодо затримки фреймів з ознакою *DE=0* (тобто, для потоку *CIR*), мс	100	400
$\boldsymbol{P_{max}\ (FRTD_{max})}$	Поріг ймовірності перевищення $FRTD_{max}$ для потоку *CIR*, безрозмірний	1×10^{-2}	1×10^{-2}
$\boldsymbol{FR\ LR_{max\ (CIR)}}$	Верхня межа втрат фреймів потоку *CIR*, безрозмірна	1×10^{-3}	1×10^{-3}
$\boldsymbol{FRER_{max}}$	Верхня межа помилкових фреймів, безрозмірна	1×10^{-4}	1×10^{-4}
$\boldsymbol{K_{г min}}$	Нижня межа коефіцієнту готовності обладнання *FR* , безрозмірна	0,996	0,996
$\boldsymbol{MTTR_{max}}$	Верхня межа середнього часу відновлення працездатності обладнання *FR*, хвилин	300	300

У табл.7.2 норми надані у розрізі двох класів обслуговування. Визначення цих класів обслуговування прийнято із міркувань, що сервіси канального рівня мають забезпечувати узгоджену роботу із сервісами мережного рівня з тим, щоб задана якість обслуговування у транспортній мережі підтримувалась "із кінця в кінець".

Нормативні значення параметрів *FR*-обладнання, що надані у табл. 7.2, визначені, виходячи з умови необхідності забезпечення якості транспортування пакетів магістральною транспортною *IP*-мережею, що побудована на базі мережі *FR*, відповідно до норм на обладнання *IP*. Для обладнання *IP*, як це буде розглянуто далі на лекції №8, існує п'ять класів обслуговування. Однак норми на *FR*-обладнання надані лише для перших двох класів обслуговування (тобто, для класу 0 та класу 1), оскільки гарантії надаються лише для потоків *CIR*.

Наведені у табл.7.2 нормативні значення параметрів якості

транспортування фреймів стосуються лише PVC- з'єднань.

7.6.4. Умови, точки та порядок вимірювань параметрів наскрізних FR-з'єднань

В процесі оцінювання параметрів якості транспортування фреймів необхідно дотримуватись загальних вимог щодо організації вимірювань, що були викладені на лекції №5. Крім того, під час вимірювань поточні значення параметру помилок $FRER_0$ будь-якого із пакетних комутаторів транспортної мережі, що утворюють оцінюване PVC-з'єднання, мають бути не більшими за $FRER_{max}$.

Якщо на *FR*-мережу накладена *IP*-мережа, то порядок вимірювань зазвичай полягає у наступному. Спочатку контролюється якість транспортування пакетів *IP* (а не фреймів, котрі переносять ці пакети), тобто з обох кінців контрольованого з'єднання підключаються хости і встановлюється режим періодичного тестування послідовностями *ICMP*-пакетів через фіксовані інтервали часу. Здійснюються активні вимірювання шляхом "пінгування" тестовими *IP*-пакетами через контрольоване *PVC*-з'єднання у прямому і зворотному напрямках передавання тестових даних.

Параметри процесу тестування (тобто, структура тестового потоку *ICMP*-пакетів) розглядається далі на лекції №8 (підрозділ 8.1.4).

В процесі вимірювань мають виконуватися такі дві умови:

1) в кожен один тестовий фрейм необхідно упаковувати лише один *IP*-пакет;

2) уся тестова послідовність *ICMP*-пакетів має упаковуватися у тестовий потік фреймів з ознакою *DE=0*, тобто у потік *CIR*.

За цих умов поточні оцінки вимірювальних параметрів та норми на параметри якості обслуговування щодо потоків *FR* та *IP* співпадають. Це надає можливість виконати оцінювання параметрів якості транспортування потоків фреймів на відповідність нормам табл. 7.1 та 7.2 шляхом вимірювань та відповідних розрахунків параметрів мережного рівня (як це робиться – розглядається на лекції №8).

Використовується шлейфова схема організації вимірювань за

схемами, що відображені на рис. 7.13 та рис. 7.14.

Тестові *IP*-пакети генеруються за допомогою штатних програмних засобів вузлу – ініціатора вимірювань, потім інкапсулюються у поле даних тестових фреймів (за допомогою штатних програмно-апаратних засобів канального рівня, тобто пристроя *FRAD* або *FR*-комутатора) із розрахунку "в один фрейм – один пакет" і далі просуваються через контрольоване *PVC*-з'єднання до кінцевого віддаленого вузлу цього з'єднання. На віддаленому вузлі за допомогою штатних програмних засобів мережного рівня здійснюється шлейфування (тобто, логічне замикання пари вимірювальних точок) згідно рис. 7.13 або рис.7.14 з подальшим передаванням тестових пакетів (що упаковані у тестові фрейми) у зворотному напрямку та обробкою цих протокольних блоків даних (у т.ч., вилучення із фреймів тестових *ICMP*-пакетів) за допомогою штатних програмно-апаратних засобів вузлу – ініціатора вимірювань.

Зокрема, підчас вимірювань при наскрізному з'єднанні типу "точка – точка" хости з вимірювальним програмним забезпеченням (що забезпечує пінгування та шлейфування на мережному рівні) безпосередньо підключаються до портів крайових *FR*-комутаторів, що утворюють контрольоване *PVC*-з'єднання. Далі необхідно замкнути між собою (на логічному рівні) пару вимірювальних точок MP_2 дальнього кінця з'єднання (див. рис.7.13) та здійснювати "пінгування" тестовими *ICMP*-пакетами через точку $MP_{egr\ 1}$, що розташована на ближньому кінці утвореного шлейфу. При цьому спостереження за кореспондованими тестовими *ICMP*-пакетами, що просуваються каналами транспортної мережі у зворотному напрямку, здійснюється у точці $MP_{in\ 1}$.

Пінгування, вимірювання та обробка результатів вимірювань здійснюється програмними засобами мережного рівня вузлу, де розташований крайовий комутатор EFS_1, а логічне замикання точок MP_2 – штатними програмними засобами вузлу, де розташований крайовий комутатор EFS_2.

Вимірювання при наскрізному з'єднанні типу "споживач – споживач" виконуються аналогічним чином, але при цьому відповідні вимірювальні точки знаходяться на термінальних вузлах споживачів. Зазвичай у цьому випадку для вимірювань

використовуються штатні програмні засоби хостів споживачів.

На вимогу споживача або після виявлення ознак невідповідності параметрів *PVC*-з'єднання на рівнях за стеком протоколів, що є вищими за канальний рівень, та котрі не були усунуті засобами мережного рівня, здійснюється аналіз параметрів канального рівня.

При цьому береться до уваги, що структура тестового потоку фреймів *FR* ідентична структурі тестового потоку *ICMP*-пакетів, оскільки в кожний фрейм тестового потоку інкапсульовано лише один *ICMP*-пакет. У цьому випадку кількість загублених фреймів буде дорівнювати кількості загублених *ICMP*-пакетів, а оцінювані значення параметрів затримки для потоків пакетів та фреймів будуть співпадати.

Кількість помилково отриманих фреймів визначається шляхом аналізу параметра *FCS* (*Frame Check Sequence*). Якщо контрольна послідовність у полі *FCS* вказує на існування помилок у прийнятому фреймі, то такий фрейм знищується. Тому аналіз параметра *FCS* слід здійснювати на кожному із вузлів транспортної мережі на шляху *PVC*-з'єднання як у прямому, так і у зворотному напрямках.

Оскільки вимірювання на відповідність нормам здійснюються лише у *PVC*-з'єднаннях щодо потоків *CIR*, то оцінювання параметрів девіації затримок у потоках фреймів втрачає сенс.

Розрахунок звітних значень параметра $FRTD_{(CIR)}$ здійснюється за результатами кожного сеансу вимірювань, параметрів $\boldsymbol{FR\ LR_{0(CIR)}}$, $\boldsymbol{FRER_0}$, $\boldsymbol{P(FRTD_{max})}$ - за результатами кожної серії сеансів вимірювань. Параметри ***Кг*** та ***MTTR*** розраховуються після кожної події відновлення обладнання.

7.7. Вимірювання параметрів абонентського доступу до транспортної мережі з використанням обладнання *Frame Relay* та *xDSL*

7.7.1. Структурна схема включення обладнання FR та xDSL

Структурна схема з'єднань обладнання *FR* та *xDSL*, за допомогою котрого здійснюється доступ до транспортної *FR*-

мережі, відображена на рис.7.15. На цій схемі показані точка доступу до послуги та відповідні пари точок вимірювань параметрів цієї послуги.

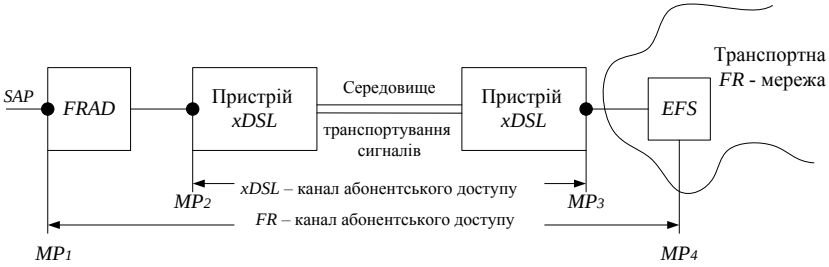


Рис.7.15. Структурна схема з'єднань обладнання *FR* та *xDSL* у каналі абонентського доступу до транспортної *FR*-мережі

Саме така схема організації доступу до ресурсів транспортної мережі може бути задіяна, якщо користувач цих ресурсів розташований віддалено від найближчого крайового вузлу транспортної мережі і в його розпорядження можуть бути передані лише телефонні абонентські лінії. Обладнання *xDSL* у цьому випадку утворює швидкісний цифровий потік (до 2 Мбіт/с), що переносить фрейми між пристроєм *FR*-доступу (*FRAD*) та крайовим комутатором транспортної *FR*-мережі.

7.7.2. Вимірювані параметри

Класифікатор параметрів якості обслуговування при наданні послуги абонентського доступу до транспортної *FR*-мережі з використанням обладнання *FR* та *xDSL*, містить дві підмножини вимірюваних параметрів. Перша підмножина характеризує якість доступу на рівні використання обладнання *FR*. Визначення параметрів цієї підмножини розглянуті у підрозділі 7.6.2. Визначення параметрів другої підмножини, які характеризують якість доступу на рівні використання обладнання *xDSL*, розглянуті раніше на лекції №6 (у підрозділі 6.6).

7.7.3. Нормативи на параметри абонентського доступу

Орієнтовні норми на вимірювані параметри обладнання *FR*

надано у табл.7.1 та 7.2.

Орієнтовні експлуатаційні норми на показники помилок для обладнання *xDSL*, яке застосовується при наданні послуги абонентського доступу до транспортної мережі, наведені у табл.6.5.

Контрольні питання до самостійного заняття сьомої лекції

1. У яких двох модифікаціях надається послуга із транспортування фреймів *FR*-каналами транспортної мережі?
2. Надайте та поясніть схеми організації вимірювань при наданні послуг із транспортування фреймів.
3. Надайте визначення параметрам функціональності послуг із транспортування фреймів - *AR, CIR, EIR, Bc, Be* та *T*.
4. Надайте визначення параметрам якості транспортування фреймів *QoS* та *NP*.
5. Укажіть норми на параметри якості транспортування потоків фреймів каналами транспортної мережі для наскрізних з'єднань типу "точка – точка".
6. Укажіть норми на параметри якості транспортування потоків фреймів для наскрізних з'єднань типу "споживач – споживач".
7. Визначіть умови, точки та порядок вимірювань параметрів наскрізних *FR*-з'єднань.
8. Наведіть структурну схему з'єднань обладнання *FR* та *xDSL*, за допомогою котрого здійснюється доступ до транспортної *FR*-мережі. На цій схемі покажіть точки доступу до послуги та відповідні пари точок вимірювань параметрів цієї послуги.

Література до самостійного заняття сьомої лекції

1) Г.Ф. Конахович, В.М. Чуприна „Мережі передавання пакетних даних". – К.: „МК-Прес", 2006.

ЛЕКЦІЯ №8. ВИМІРЮВАННЯ ПАРАМЕТРІВ ОБЛАДНАННЯ НА МЕРЕЖНОМУ РІВНІ ВЗАЄМОДІЇ ІНФОРМАЦІЙНИХ СИСТЕМ

Розглядаються наступні питання:

Лекційне заняття

8.1. Вимірювання параметрів обладнання транспортних мереж *IP*

8.2. Вимірювання параметрів абонентського доступу до транспортної мережі *IP* з використанням обладнання *IP*

8.3. Вимірювання параметрів абонентського доступу до транспортної мережі *IP* з використанням обладнання *Frame Relay*

8.4. Вимірювання параметрів абонентського доступу до транспортної мережі *IP* з використанням обладнання *xDSL*

8.1. Вимірювання параметрів обладнання транспортних мереж *IP*

Більшість сучасних пакетних мереж для надання послуг із транспортування інформації основана на використанні обладнання, що реалізують телекомунікаційний протокол *IP*. У цьому підрозділі мова йде лише про глобальну транспортну мережу *IP*. Технологія вимірювань параметрів обладнання мереж доступу до глобальної транспортної мережі *IP*, що здійснюється з використанням обладнання *IP*, *FR* та *xDSL* розглядається у наступних підрозділах цього лекційного матеріалу.

8.1.1. Схеми організації вимірювань

Послуга із транспортування пакетів *IP*-каналами транспортної мережі надається оператором *IP*-мережі у двох модифікаціях: для наскрізних з'єднань типу "точка – точка" (коли обладнання абонентського *IP*-доступу знаходиться у зоні відповідальності оператора електрозв'язку) та для наскрізних з'єднань типу "споживач – споживач" (коли обладнання абонентського IP-доступу знаходиться у зоні відповідальності споживачів).

Для організації вимірювань зазвичай використовується шлейфова схема як при з'єднаннях типу "точка – точка" (така схема показана на рис.8.1), так і при з'єднаннях типу "споживач – споживач" (див. рис.8.2). *SAP* (*Service Access Point*) – точка доступу

до транспортної послуги. Це - фізична та (або) логічна точка на структурній схемі організації інформаційної взаємодії елементів транспортної мережі (зокрема, на структурній схемі з'єднань відповідного телекомунікаційного обладнання), стосовно котрої діють норми на показники параметрів транспортного обслуговування. На мережному рівні взаємодії *SAP* розглядається як логічна точка, доступ до котрої забезпечується за допомогою програмних засобів хоста та (або) крайового комутатора/маршрутизатора. На рис.8.2 показана схема організації вимірювань параметрів обладнання *IP* при наскрізному з'єднанні типу „користувач – користувач".

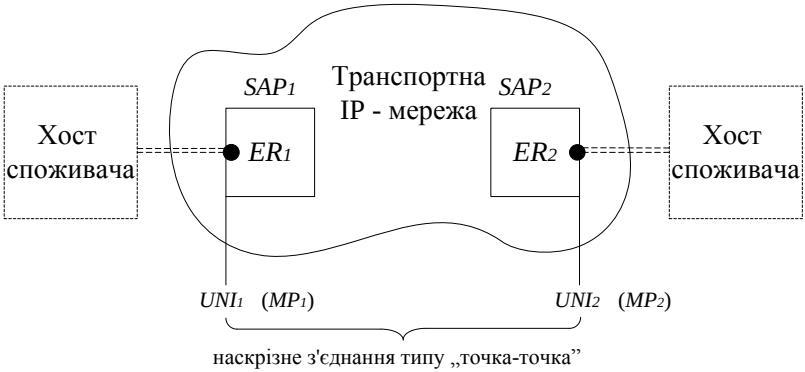


Рис. 8.1. Схема організації вимірювань параметрів обладнання транспортної IP-мережі при наскрізному з'єднанні типу "точка –точка"

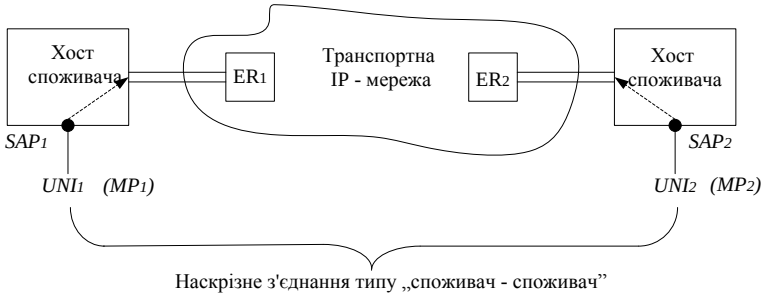


Рис.8.2. Схема організації вимірювань параметрів обладнання IP-мережі при наскрізному з'єднанні типу "споживач-споживач"

Як бачимо, за цією схемою у ланцюг вимірювань включені також канали абонентського доступу користувачів до найближчих крайових маршрутизаторів *ER* (*Edge Router*) транспортної *IP*-мережі.

8.1.2. Вимірювані параметри

1) **Параметри функціональності послуг із транспортування пакетів - *IPTS`*, *IPTS`*$_{max}$, *IPTS*$^0_{max}$, B_c, B_e.**

Характеристики швидкості передавання пакетів

IPTS` - миттєва швидкість передавання пакетів *IP* через вимірювальну точку. Вимірюється, як правило, у кількості транспортованих через канал *IP*-пакетів протягом 1 секунди.

***IPTS`*$_{max}$** - припустиме максимальне значення миттєвої швидкості передавання пакетів *IP* через вимірювальну точку.

***IPTS*$^0_{max}$** - припустиме максимальне значення усередненого на інтервалі сеансу вимірювань значення *IPTS`*. Інтервал сеансу вимірювання прийнято (але не завжди) обирати на рівні 1година.

Характеристики обсягу транспортованого трафіку

B_c - максимальна кількість байтів, яка гарантовано транспортується впродовж визначеного проміжку часу *T* (параметр B_c прийнято називати узгодженим або обов'язковим обсягом пульсацій трафіку).

B_e – максимальна кількість байтів, яка транспортується "з максимальними зусиллями" впродовж визначеного проміжку часу *T* (додатковий обсяг пульсації).

Примітка 8.1. Значення *T* визначається умовами сервісної угоди оператора з клієнтом (*Service Level Agreement, SLA*).

2) Параметри якості транспортування пакетів

У табл.8.1 надано класифікатор параметрів якості транспортування *IP*-пакетів з використанням мереж пакетної комутації, технічна та організаційна підтримка котрих забезпечується більшістю операторів глобальних *IP*-мереж. Конкретні визначення цих параметрів надано нижче. Звернемо лише увагу, що мнемонічні позначення нижченаведених параметрів отримано шляхом заміни у позначеннях параметрів, що розглядались на лекції №6, літеросполучення "*PDU*" на "*IP*", оскільки у даному випадку в якості протокольних блоків даних

(*Protocol Data Unite, PDU*) використовуються пакети *IP*.

Таблиця 8.1

Класифікатор параметрів якості обслуговування при наданні послуг із транспортування пакетів каналами транспортної *IP*-мережі

Параметри якості обслуговування		
мережно-орієнтовані (параметри *NP*)	сервіс-орієнтовані (параметри *QoS*)	мережно/сервіс незалежні
1. $IPLR_{max}$; 2. $IPSLBR_{max}$; 3. $IPER_{max}$; 4. $K'_{зав0max}(IP)$; 5. $Kг_{min}$	1. $IPTD_{max}$; 2. $IPDV_{max}$; 3. P_{max} $(IPTD_{max})$; 4. $P_{IP}SA_{min}$ (PIA); 5. $T_{IP}U_{max}$ (TIU)	1. RP_{max} ; 2. $MTTR_{max}$

Примітка 8.2. Набір параметрів послуги із транспортування пакетів *IP* вибрано однаковим: для з'єднань типу "точка – точка"; для з'єднань типу "споживач – споживач"; для абонентського доступу до магістральної *IP*-мережі.

Примітка 8.3. Параметр $P_{IP}SA$ в літературі часто позначають як *PIA*, а параметр $T_{IP}U$ – як *TIU*. Пояснення щодо цих параметрів надано далі за текстом.

Характеристики втрат пакетів

IPLR (IP loss ratio) – коефіцієнт втрат пакетів. Параметр, що характеризує втрати пакетів під час їхнього передавання через вимірювальну секцію між увідною та вивідною точками вимірювань. Визначається як відношення загальної кількості втрачених (у т.ч., відкинутих) пакетів до загальної кількості переданих пакетів протягом одного сеансу вимірювань.

$IPLR_0$ - усереднене на сумарному інтервалі визначеної серії сеансів вимірювань значення *IPLR* .

$IPLR_{max}$ – максимально припустиме значення коефіцієнту втрат пакетів.

IPSLBR (IP severe loss block ratio) - коефіцієнт втрат блоків пакетів. Параметр, що характеризує втрати блоків пакетів під час їхнього передавання через вимірювальну секцію між увідною та вивідною точками вимірювань. Визначається як відношення загальної кількості втрачених (у т.ч., відкинутих) блоків пакетів до загальної кількості переданих блоків пакетів протягом однієї серії сеансів вимірювань.

Примітка 8.4. Серія сеансів вимірювань складається із сеансів тривалістю T_s. І якщо кількість втрачених пакетів на проміжку T_s перевищить поріг s1, то всі пакети на цьому проміжку відкидаються, а цей блок пакетів вважається втраченим.

IPSLBR$_{max}$ - верхня припустима межа (максимально припустиме значення) *IPSLBR* (для визначених T_s та s1). Цей показник іноді нормується.

Характеристики затримки пакетів

IPTD (IP time delay) – час затримки пакетів. Параметр, що характеризує проміжок часу, протягом котрого пакети просуваються через вимірювальну секцію між увідною та вивідною точками вимірювань.

IPTD$_{max}$ - максимально припустиме усереднене значення затримки пакетів. Затримки пакетів усереднюються на певним чином обраному інтервалі сеансу вимірювань. $IPTD_{max}$ визначається як середнє арифметичне усіх виміряних значень *IPTD* за виключенням 10% мінімальних та 10% максимальних значень цього показника в інтервалі даного сеансу вимірювань.

P (IPTD$_{max}$) – ймовірність (частість) перевищення $IPTD_{max}$. Визначається як відношення кількості подій перевищення значення $IPTD_{max}$ до загальної кількості усіх виміряних значень величини *IPTD* протягом однієї години.

P$_{max}$ (IPTD$_{max}$) - припустиме максимальне значення ймовірності перевищення величини $IPTD_{max}$. Цей показник в багатьох випадках нормується.

Характеристики варіації затримки пакетів

IPDV (IP delay variation) – параметр, що характеризує відхилення у затримці пакетів відносно $IPTD_0$ під час його передавання через вимірювальну секцію між увідною та вивідною точками вимірювань. Так, якщо затримку *k*-го пакета у потоці пакетів позначити як $IPTD_k$, то

$$IPDV_k = |IPTD_k - IPTD_0|. \qquad (8.1)$$

IPDV$_0$ - усереднене на інтервалі сеансу вимірювань значення

IPDV (варіація затримки або джитер затримки пакетів). Визначається як середнє арифметичне усіх виміряних значень $IPDV_k$ за виключенням 10% мінімальних та 10% максимальних значень цього показника в інтервалі даного сеансу вимірювань. Варіація затримки визначається для всіх пакетів, що пройшли через вимірювальну секцію: як коректно транспортованих, так і з помилками.

***IPDV*$_{max}$** - верхня припустима межа $IPDV_0$ (тобто, припустимий максимальний діапазон відхилення *IPTD* від $IPTD_0$). Цей показник у більшості випадків нормується.

Характеристика некоректного транспортування пакетів (IPER)

IPER (IP error ratio) - коефіцієнт некоректно транспортованих пакетів. Параметр, що характеризує кількість пакетів, що були ушкоджені під час їхнього передавання через вимірювальну секцію між увідною та вивідною точками вимірювань. Під ушкодженням розуміється будь-яка невідповідність вмісту інформаційних полів пакетів. Визначається як відношення загальної кількості некоректно транспортованих пакетів до загальної кількості переданих пакетів протягом одного сеансу вимірювань.

***IPER*$_0$** - усереднене на сумарному інтервалі визначеної серії сеансів вимірювань значення *IPER* .

***IPER*$_{max}$** – максимально припустиме значення $IPER_0$.

Показники доступності транспортної послуги

IPAF (IP availability function) – функція доступності послуги із транспортування пакетів. Характеризує співвідношення між проміжками часу, коли послуга є доступною для споживачів, і проміжками часу, коли ця послуга є недоступною. Визначається наступним чином. Узгоджений між постачальником та споживачем графік надання транспортної послуги (за звичайних умов, такий графік охоплює проміжок часу в одну добу і передбачає режим цілодобового безперервного обслуговування) розбивається на часові проміжки T_{av}.

Примітка 8.5. Кількість таких часових проміжків в рамках графіка надання послуги має бути обґрунтована.

Визначається критерій доступності послуги на проміжку T_{av}. В якості такого критерію вибирається показник $IPLR_0$ або $IPER_0$ (або обидва разом). Визначається поріг доступності послуги у метриці вибраного показника – c_1 або c_2. Якщо на проміжку T_{av} $IPLR_0 > c_1$ або (та) $IPER_0 > c_2$, то послуга на цьому проміжку вважається недоступною. В протилежному випадку (тобто, коли $IPLR_0 \le c_1$ або (та) $IPER_0 \le c_2$) послуга на проміжку T_{av} вважається доступною.

Примітка 8.6. Вибір набору критеріїв доступності послуги та значення порогів *c1* або (та) *c2* мають бути обгрунтовані.

Таким чином, в процесі обслуговування може бути *k1* часових інтервалів тривалістю T_{av}, коли послуга є доступною, та *k2* часових інтервалів, коли послуга – недоступна (при загальній кількості можливих інтервалів у графіку обслуговування $k = k1 + k2$).

$P_{IP}SA$ (percent IP service availability) – відсоток (коефіцієнт) доступності послуги із транспортування пакетів. Характеризує відсоток часу відносно загального часу обслуговування (який, як правило, узгоджується у сервісній угоді *SLA*), коли існує можливість користуватися послугою. Визначається як відсоток часових інтервалів тривалістю T_{av}, коли послуга є доступною, до загальної кількості часових інтервалів, що визначені у графіку обслуговування. Параметр $P_{IP}SA$ в літературі часто позначають як *PIA*.

Примітка 8.7. Відсоток недоступності послуги ***$P_{IP}SU$* (*percent IP service unavailability*)** визначається як $P_{IP}SU = 100 - P_{IP}SA$.

$P_{IP}SA_{min}$ - припустиме мінімальне значення коефіцієнта доступності $P_{IP}SA$.

$T_{IP}U$ (Time IP service unavailability) – сумарна кількість годин протягом року, коли відсутня можливість користуватися послугою із транспортування пакетів. Параметр $T_{IP}U$ в літературі часто позначають як *TIU*.

$T_{IP}U_{max}$ – припустиме максимальне значення $T_{IP}U$.

<u>Показники доступності мережного обладнання</u>

Доступність ресурсів мережного обладнання напряму пов’язана із двома факторами (якщо не рахувати проблем з інформаційною безпекою): рівнем завантаження цього обладнання користувацьким

трафіком та рівнем експлуатаційної надійності мережного обладнання. При перевищенні певного рівня завантаженості мережні ресурси внаслідок неприпустимого погіршення їхньої якості можуть стати недоступними для користувачів. Зрозуміло також, що у випадку відмови обладнання його ресурси становляться недоступними для користувачів. Отже, показники доступності мережного обладнання мають визначатися як характеристиками навантаження на *IP*-обладнання, так і характеристиками його експлуатаційної надійності.

Характеристика навантаження на IP- обладнання

$K_{зав}$ – коефіцієнт завантаження обладнання. Характеризує ступінь завантаження мережного обладнання пакетним трафіком, який циркулює через це обладнання. Визначається як відношення швидкості передавання пакетів через обладнання, завантаження котрого розглядається, до його пропускної здатності. Підкреслимо, що коефіцієнт завантаження обладнання пакетним трафіком (або, як кажуть, коефіцієнт навантаження на обладнання пакетним трафіком) визначається відношенням реально досягнутої швидкості передавання пакетів *IP* на певним чином обраному проміжку часу до пропускної здатності обладнання. Оскільки зазвичай існують пульсації трафіку, то для підвищення об'єктивності вимірювань ступеню завантаженості обладнання бажано здійснювати усереднення виміряних значень коефіцієнтів завантаження на різних проміжках часу. Вибір часу усереднення – окреме питання, що вирішується з огляду на конкретні умови використання обладнання. В залежності від вибору величини інтервалу вимірювань розрізняють миттєвий та середній коефіцієнт завантаження.

$K'_{зав}$ – миттєвий коефіцієнт завантаження обладнання. Визначається як відношення миттєвої швидкості передавання пакетів (тобто, параметр *IPTS'*, що вимірюється на інтервалі в одну секунду) через вимірювальну точку (як правило, логічну точку, яка вибирається на уводі або на виводі досліджуваного обладнання) до пропускної здатності цього обладнання.

$K'_{завтах}$ – верхня припустима межа миттєвого коефіцієнту завантаження обладнання, тобто припустиме максимальне

значення К'зав. Цей показник іноді для окремих транспортних технологій нормується.

К'зав0 – усереднений на інтервалі сеансу вимірювань коефіцієнт завантаження обладнання, тобто усереднене на інтервалі сеансу вимірювань значення *К'зав*. Тривалість сеансу вимірювань T_0 обумовлюється окремо у сервісних угодах *SLA*.

К'зав0max – верхня припустима межа усередненого коефіцієнту завантаження обладнання, тобто припустиме максимальне значення $K'_{зав0}$. Таким чином, $K'_{зав0max}(IP)$ – верхня припустима межа середнього коефіцієнту навантаження обладнання *IP*. Цей показник у більшості випадків нормується.

<u>Показники експлуатаційної надійності мережного обладнання</u>

P(T_N) **- ймовірність безвідмовної роботи** мережного обладнання на проміжку часу T_N. Визначається згідно з ДСТУ 2860-94 як ймовірність того, що в межах заданого наробітку T_N відмови мережного обладнання не настануть. Цей показник щодо телекомунікаційного обладнання не нормується, але може обчислюватись з метою отримання даних щодо надійності виробів окремих постачальників обладнання.

MTBF (Mean Time Between Failures) **– середній час між відмовами.** Характеризує рівень надійності обладнання без урахування впливу на надійність цього обладнання процесів технічного обслуговування та ремонту. Визначається згідно з ДСТУ 2860-94. Цей показник щодо телекомунікаційного обладнання не нормується. Використовується для визначення коефіцієнту готовності (див. далі).

MTTR (Mean Time To Repair) **– середній час відновлення (ремонту) після відмови обладнання.** Характеризує рівень досконалості служб технічного обслуговування та ремонту. Визначається згідно з ДСТУ 2860-94. Використовується для визначення коефіцієнту готовності.

MTTR_max – максимально припустиме значення *MTTR*. Цей показник, як правило, нормується.

Кг **- коефіцієнт готовності обладнання.** Комплексний показник експлуатаційної надійності мережного обладнання, який

характеризує співвідношення між *MTTR* та *MTBF* згідно з формулою:

$$Кг = MTBF/ (MTBF + MTTR). \quad (8.2)$$

Визначається згідно з ДСТУ 2860-94.

Кг$_{min}$ **- мінімально припустиме значення коефіцієнту готовності.** Цей показник, як правило, нормується.

<u>Показники зручності використання транспортної послуги</u>

RP (Reporting Period) - інтервал звітування, тобто періодичність представлення покупцю транспортної послуги звітів про поточний стан обслуговування. (Бажано, з точки зору покупців послуги, щоб цей інтервал був якомога меншим).

RP$_{max}$ - максимально припустиме значення *RP*, що наведене у *SLA.*

8.1.3 Нормативи на параметри якості у розрізі класів обслуговування

З метою забезпечення можливості якісного транспортування потоків пакетів *IP*, що наразі генеруються основною масою прикладних застосувань реальних і потенційних споживачів, усі найбільш популярні види потоків, що транспортуються каналами мереж *IP*, згруповані на основі визначених для них загальних ознак за шістьома класами трафіка *IP*. З урахуванням характеристик цих класів визначено шість стандартизованих рівнів надання транспортної послуги, тобто шість класів обслуговування (див. табл.8.2).

Таблиця 8.2

Норми на параметри обладнання *IP* при наскрізних з'єднань типу "споживач – споживач"

Параметри обладнання *IP* / Сервіс-орієнтовані	Характеристика параметра	Клас 0	Клас 1	Клас 2	Клас 3	Клас 4	Клас 5

параметри							
$IPTD_{max}$	Верхня межа щодо затримки пакетів, мс	100	400	480	480	1000	н/в
$IPDV_{max}$	Верхня межа щодо варіації затримки, мс	50	50	150	н/в	н/в	н/в
P_{max} $(IPTD_{max})$	Поріг ймовірності перевищення $IPTD_{max}$, безрозмірний	1×10^{-2}	1×10^{-2}	1×10^{-2}	5×10^{-2}	н/в	н/в
$P_{min}(IPDV_{max})$	Поріг відсотка неперевищення $IPDV_{max}$, % (у відсотках)	1,0	1,0	н/в	н/в	н/в	н/в
$P_{IP}SA_{min}$ *(PIA)*	Нижня межа щодо відсотка часу доступності послуги, % (у відсотках)	99	99	99	99	н/в	н/в
$T_{IP}U_{max}$ *(TIU)*	Верхня межа щодо годин недоступності послуги, годин на рік	88	88	88	88	н/в	н/в
Мережно-орієнтовані параметри							
$IPLR_{max}$	Верхня межа втрат пакетів,	1×10^{-3}	1×10^{-3}	1×10^{-3}	1×10^{-3}	1×10^{-3}	н/в

	безрозмірна						
$IPER_{max}$	Верхня межа помилкових пакетів, безрозмірна	1×10^{-4}	1×10^{-4}	1×10^{-4}	1×10^{-4}	1×10^{-3}	н/в
$Кг_{min}$	Нижня межа коефіцієнту готовності	0,996	0,996	0,996	0,996	0,996	н/в
Сервіс/мережно-незалежні параметри							
$MTTR_{max}$	Верхня межа середнього часу відновлення працездатності, хвилин	300	300	300	300	500	н/в

Кожний клас обслуговування характеризується певним набором нормованих значень (або діапазонів значень) показників якості послуги (тобто, сервіс-орієнтованих параметрів), мережної досконалості (тобто, мережно-орієнтованих параметрів) та сервіс/мережно-незалежних параметрів обслуговування.

Примітка 8.8. Рівень якості транспортної послуги не може асоціюватися із суб'єктивними уявленнями типу "більш якісна або менш якісна послуга", а задається конкретними значеннями параметрів цієї послуги.

Примітка 8.9. Позначка "н/в" означає "не визначено".

Примітка 8.10. Нормативні визначення параметрів $IPTD_{max}$, $IPDV_{max}$, $IPLR_{max}$ та $IPER_{max}$ відповідають *ITU-T Recommendation Y.1541* для наскрізного з'єднання типу "споживач – споживач".

Примітка 8.11. Оцінювання параметрів $K'_{зав0}$ та $IPER_0$ в процесі поточного контролю відповідності не здійснюється. Однак в процесі пошуку вирішення проблем невідповідності необхідно упевнитися, що поточні значення цих параметрів не перевищують норми (відповідно $K'_{завmax}$ та $IPER_{max}$) на усіх вузлах

(проміжних та крайових) впродовж можливих шляхів просування *IP*-пакетів. Дані, що є необхідними для обчислення поточних значень цих параметрів, накопичуються на вузлах у базах *MIB* контрольованого обладнання за допомогою механізмів протоколу *SNMP*.

Примітка 8.12. Значення параметру $P_{IP}SA_{min}$ (тобто, значення параметру *PIA*) визначається відповідно до *ITU-T Recommendation Y.1541* за таких умов: інтервал вимірювань параметра – 1 доба; доступність оцінюється за параметром $IPLR_0$; поріг визначення доступності c1 береться на рівені 0,01 для класів 0 та 2 і на рівні 0,005 для класів 1 та 3; проміжок часу T_{av}, що відведений для визначення $IPLR_0$ та порівняння з порогом c1, дорівнює тривалості однієї серії сеансів вимірювань параметра $IPLR_0$. Пояснення щодо обчислення цього параметру надано вище.

Примітка 8.13. Пояснення щодо обчислення параметру T_{IP} *U* (тобто, *TIU*) надано вище.

Примітка 8.14. Значення параметру RP_{max} визначається умовами *SLA*.

Для наскрізних з'єднань типу "споживач – споживач" нормовані значення показників якості транспортування *IP*-пакетів, що класифіковані за визначеними шістьома класами обслуговування, надані у табл.8.2.

Для наскрізних з'єднань типу "точка – точка" норми на показники за класами обслуговування не класифікуються, оскільки рівень якості транспортування пакетів між будь-якими двома вузлами магістральної транспортної мережі має бути однаковим.

Рекомендовані норми на показники якості обслуговування магістральною транспортною *IP*-мережею надані у табл.8.3 .

Таблиця 8.3

Норми на параметри обладнання *IP* при наскрізних з'єднань типу "точка – точка"

Параметри обладнання *IP*	Характеристика параметра	Нормативне значення параметра
	Сервіс-орієнтовані параметри	
$IPTD_{max}$	Верхня межа щодо затримки пакетів, мс	80
$IPDV_{max}$	Верхня межа щодо варіації затримки, мс	30

P_{max} *(IPTD$_{max}$)*	Поріг ймовірності перевищення *IPTD$_{max}$*, безрозмірний	1×10^{-2}
P_{min} *(IPDV$_{max}$)*	Поріг відсотка неперевищення *IPDV$_{max}$*, % (у відсотках)	1,0
$P_{IP}SA_{min}$ *(PIA)*	Нижня межа щодо відсотка часу доступності послуги, % (у відсотках)	99
$T_{IP}U_{max}$ *(TIU)*	Верхня межа щодо годин недоступності послуги, годин на рік	12
	Мережно-орієнтовані параметри	
IPLR$_{max}$	Верхня межа втрат пакетів, безрозмірна	1×10^{-3}
IPER$_{max}$	Верхня межа помилкових пакетів, безрозмірна	1×10^{-4}
Кг$_{min}$	Нижня межа коефіцієнту готовності	0,996
	Сервіс/мережно-незалежні параметри	
MTTR$_{max}$	Верхня межа середнього часу відновлення працездатності, хвилин	300

8.1.4 Умови, точки та порядок вимірювань параметрів наскрізних IP-з'єднань

В процесі оцінювання параметрів якості транспортування пакетів необхідно дотримуватись загальних вимог щодо організації вимірювань, що були викладені на лекції №5. Крім того, під час вимірювань пікове навантаження будь-якого із міжвузлових комутаторів та маршрутизаторів мережі повинно не перевищувати 90%. При піковому навантаженні будь-якого з міжвузлових каналів зв'язку та маршрутизаторів, що перевищує 90%, транспортна мережа вважається перенавантаженою і такою, що не задовольняє вимогам до якості послуг передавання інформації.

Поточні значення параметру *IPER$_0$* на всіх вузлах уздовж можливих шляхів просування *IP*-пакетів повинно не перевищувати норму *IPER$_{max}$*.

Вимірювання здійснюються активним способом в режимі періодичного тестування через фіксовані інтервали часу методом

“пінгування” тестових *ICMP*-пакетів. Використовується шлейфова схема організації вимірювань за схемами, що відображена на рис.8.1 (при з’єднаннях типу “точка – точка”) або на рис.8.2 (при з’єднаннях типу “споживач – споживач”). На цих рисунках відображені відповідні точки доступу до послуги та відповідні пари вимірювальних точок.

Зокрема, підчас вимірювань при наскрізному з’єднанні типу “точка – точка” необхідно замкнути між собою (на логічному рівні) пару вимірювальних точок MP_2 (див. рис.8.1) та здійснювати “пінгування” тестовими *ICMP*-пакетами через точку $MP_{egr\ 1}$, що розташована на SAP_1. При цьому спостереження за кореспондованими тестовими *ICMP*-пакетами, що просуваються каналами транспортної мережі у зворотному напрямку від SAP_2 до SAP_1, здійснюється у точці MP_{in1}, що розташована на SAP_1. Пінгування, вимірювання та обробка результатів вимірювань здійснюється штатними програмними засоби крайового маршрутизатора ER_1, а логічне замикання точок MP_2 – штатними програмними засобами крайового маршрутизатора ER_2.

Примітка 8.15. Конкретні назви штатних інструментальних програмних засобів, що застосовуються під час вимірювань, та методика їхнього використання вказуються у регламентах експлуатації телекомунікаційного обладнання, що інстальовано у вузлах транспортної мережі.

Вимірювання при наскрізному з’єднанні типу “споживач – споживач” виконуються аналогічним чином, але при цьому SAP_1 та SAP_2 (і відповідні вимірювальні точки) знаходяться на термінальних вузлах споживачів.

Зазвичай у цьому випадку для вимірювань використовуються штатні програмні засоби хостів користувачів.

Структура тестового потоку пакетів IP повинна відповідати структурі, що надана на рисунку 5.2 (див. лекцію №5), і мати наступні характеристики:

1) довжина поля даних тестових пакетів $\boldsymbol{\nu}$ - не більша за 64 байта;

2) кількість пакетів в одній групі $\boldsymbol{N}$ (тобто, в одному сеансі вимірювань) – 100;

3) періодичність генерації груп тестових пакетів $\boldsymbol{T}$ – один раз кожні 6 хвилин;

4) мінімальний міжпакетний інтервал τ в рамках однієї групи пакетів – 100 мс;

5) тривалість одного сеансу вимірювань $\boldsymbol{T}$ - 6 хвилин;

6) тривалість однієї серії сеансів вимірювань $\boldsymbol{T_0}$ - 1 година.

Розрахунок звітних значень параметрів $IPTD_0$, $IPDV_0$, $P(IPDV_{max})$, $K'_{зав0}$ здійснюється за результатами кожного сеансу вимірювань, тобто звітний проміжок часу щодо цих параметрів дорівнює 6 хвилинам. Розрахунок звітних значень параметрів $IPLR_0$ та $P(IPTD_{max})$ - за результатами кожної серії сеансів вимірювань, тобто звітний проміжок часу для цих параметрів дорівнює 1 години. Для параметра $P_{IP}SA$ звітний проміжок – 1 доба. Параметр $T_{IP}U$ розраховується на звітному проміжку, що дорівнює одному року. Параметри $Кг$ та $MTTR$ розраховуються після кожної події відновлення обладнання.

8.1.5 Дії у разі виявлення невідповідності

Поточний контроль якості наскрізного з'єднання виконується шляхом відслідковування поточних оцінок параметра втрат пакетів $IPLR_0$. У процесі поточного контролю цього параметру може виявитись перевищення його нормованого значення $IPLR_{max}$. У цьому випадку необхідно переконатися в коректності роботи обладнання мережного (і, можливо, більш високого) рівня у кінцевих вузлах контрольованого наскрізного з'єднання, наприклад шляхом відключення від нього обладнання сусідніх вузлів і "пінгування" тестовими пакетами по локальному шлейфу, що створюється як на ближньому, так і на віддаленому кінцях контрольованого з'єднання. Якщо проблем на рівні протоколу *IP* (і вище) на локальних шлейфах не виявлено, необхідно розпочати пошук проблем в роботі транспортної мережі.

Плановий періодичний контроль якості наскрізного з'єднання виконується шляхом відслідковування поточних оцінок усіх параметрів мережного рівня (не тільки $IPLR_0$), нормовані значення котрих надано у табл. 8.2. У процесі планового контролю можуть виявитися невідповідності щодо нормованих значень будь-якого із параметрів. У цьому випадку необхідно розпочати пошук проблем в роботі транспортної мережі.

У разі виявлення невідповідності щодо нормованих значень

сервіс-орієнтованих параметрів необхідно розпочати пошук проблем, пов'язаних із можливими перенавантаженнями *IP*-трафіком каналів транспортної *IP*-мережі.

Пошук шляхів вирішення проблеми невідповідності на мережному рівні здійснюють шляхом порівняльного аналізу виміряних поточних значень параметрів мережного рівня з відповідними нормативними значеннями цих параметрів. При цьому використовується шлейфова схема організації вимірювань.

Під час пошуку проблемної ділянки на шляху просування пакетів утворюють наскрізне *TCP/IP*-з'єднання. В цьому випадку значення параметрів аналізуються щодо всіх *IP*-маршрутизаторів, розташованих на шляху просування пакетів. Локалізація проблеми полягає у виявленні міжвузлової ділянки, де зафіксоване суттєве відхилення від норм щодо будь-якого параметра.

У разі виявлення невідповідності щодо нормативних значень мережно-орієнтованих параметрів необхідно розпочати пошук проблем, пов'язаних із відмовами в роботі мережного обладнання згідно з положеннями регламентуючої експлуатаційної документації на мережне обладнання, що використовується.

Якщо проблем на рівні протоколів *TCP* та *IP* не виявлено, необхідно розпочати пошук проблем в роботі обладнання канального, а потім фізичного рівнів, що забезпечує транспортування пакетів *IP*.

8.2 Вимірювання параметрів абонентського доступу до транспортної мережі *IP* з використанням обладнання *IP*

Параметри функціональності обладнання абонентського доступу щодо трафіка IP аналогічні параметрам, що надані у підрозділі 8.1.1 цієї лекції.

Номенклатура параметрів якості транспортування пакетів (тобто, параметрів *QoS* та *NP* обладнання абонентського доступу) також співпадають із даними, що надані у табл.8.1.

8.2.1. Нормативи на параметри якості

Нормативи якості транспортування пакетів при наданні послуги абонентського доступу до транспортної мережі *IP* з використанням обладнання *IP*, за аналогією з п. 8.1.3, надаються у розрізі шести

класів обслуговування. З урахуванням характеристик цих класів у табл. 8.4 для вищезазначеної послуги надані рекомендовані нормативні визначення відповідних показників.

Таблиця 8.4

Норми на параметри обладнання при наданні послуг абонентського доступу до транспортної мережі *IP* з використанням обладнання *IP*

Параметри обладнання / Сервіс-орієнтовані параметри	Характеристика параметра	Клас 0	Клас 1	Клас 2	Клас 3	Клас 4	Клас 5
$IPTD_{max}$	Верхня межа щодо затримки пакетів, мс	10	160	200	200	400	н/в
$IPDV_{max}$	Верхня межа щодо варіації затримки, мс	10	10	60	н/в	н/в	н/в
P_{max} $(IPTD_{max})$	Поріг ймовірності перевищення $IPTD_{max}$, безрозмірний	1×10^{-2}	1×10^{-2}	1×10^{-2}	5×10^{-2}	н/в	н/в
P_{min} $(IPDV_{max})$	Поріг відсотка неперевищення $IPDV_{max}$, % (у відсотках)	1,0	1,0	н/в	н/в	н/в	н/в
$P_{IP}SA_{min}$ (PIA)	Нижня межа щодо відсотка часу	99	99	99	99	н/в	н/в

	доступності послуги, % (у відсотках)						
$T_{IP}U_{max}$ *(TIU)*	Верхня межа щодо годин недоступності послуги, годин на рік	38	38	38	38	н/в	н/в
Мережно-орієнтовані параметри							
$IPLR_{max}$	Верхня межа втрат пакетів, безрозмірна	1×10^{-3}	1×10^{-3}	1×10^{-3}	1×10^{-3}	1×10^{-3}	н/в
$IPER_{max}$	Верхня межа помилкових пакетів, безрозмірна	1×10^{-4}	1×10^{-4}	1×10^{-4}	1×10^{-4}	1×10^{-4}	н/в
$Кг_{min}$	Нижня межа коефіцієнту готовності	0,996	0,996	0,996	0,996	0,996	н/в
Сервіс/мережно-незалежні параметри							
$MTTR_{max}$	Верхня межа середнього часу відновлення працездатно	150	150	150	150	300	н/в

	сті, хвилин						

8.2.2. Умови, точки та порядок вимірювань

Вимірювання параметрів послуги абонентського *IP*-доступу виконуються за шлейфовою схемою, що відображена на рис. 8.3.

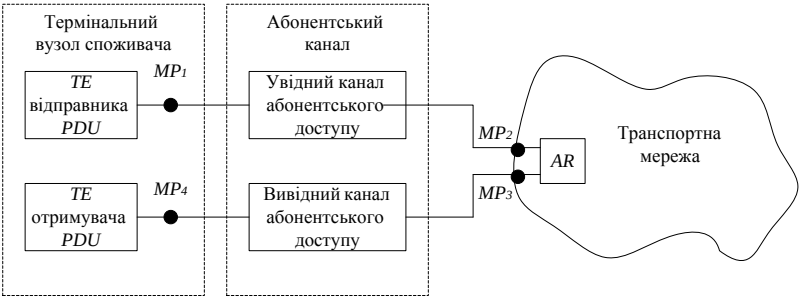


Рис.8.3. Базова схема вимірювань для оцінювання параметрів абонентського IP-доступу до глобальної транспортної мережі

В процесі оцінювання параметрів якості транспортування пакетів необхідно дотримуватись загальних вимог щодо організації вимірювань, що були викладені на лекції №5. Крім того, під час вимірювань пікове навантаження на крайовий маршрутизатор (маршрутизатор доступу, *Access Router, AR*), до якого під'єднано контрольований абонентський IP-канал, повинно не перевищувати 90%. При піковому навантаженні цього маршрутизатору, що перевищує 90%, транспортна мережа вважається перенавантаженою і такою, що не задовольняє вимогам до якості послуг передавання інформації. Поточні значення параметру $IPER_0$ на крайовому маршрутизаторі повинно не перевищувати норму $IPER_{max}$, тобто 1×10^{-4}.

Зокрема, підчас вимірювань необхідно замкнути між собою (на логічному рівні) пару вимірювальних точок MP_2 та MP_3 (див. рис. 8.3) та здійснювати "пінгування" тестовими *ICMP*-пакетами через точку $MP_{egr\ 1}$, що розташована на SAP_1. При цьому спостереження за кореспондованими тестовими *ICMP*-пакетами, що просуваються каналом абонентського доступу у зворотному напрямку від SAP_2 до

SAP_1, здійснюється у точці $MP_{in\ 1}$, що розташована на SAP_1. Пінгування, вимірювання та обробка результатів вимірювань здійснюється штатними програмними засоби хоста, а логічне замикання точок MP_2 та MP_3 – штатними програмними засобами сервера доступу вузлу транспортної мережі.

Примітка 8.16. Конкретні назви штатних інструментальних програмних засобів, що застосовуються під час вимірювань, та методика їхнього використання вказуються у регламентах експлуатації телекомунікаційного обладнання, що інстальовано у вузлах транспортної мережі.

Структура тестового потоку пакетів *IP* повинна відповідати структурі, що надана на рисунку 5.2 (див. лекцію №5), і мати наступні характеристики:

1) довжина поля даних тестових пакетів $\boldsymbol{\nu}$ - не більша за 64 байта;

2) кількість пакетів в одній групі $\boldsymbol{N}$ (тобто, в одному сеансі вимірювань) – 100;

3) періодичність генерації груп тестових пакетів $\boldsymbol{T}$ – один раз кожні 6 хвилин;

4) мінімальний міжпакетний інтервал $\boldsymbol{\tau}$ в рамках однієї групи пакетів – 100 мс;

5) тривалість одного сеансу вимірювань $\boldsymbol{T}$ - 6 хвилин;

6) тривалість однієї серії сеансів вимірювань $\boldsymbol{T_0}$ - 1 година.

Розрахунок звітних значень параметрів $IPTD_0$, $IPDV_0$, $P(IPDV_{max})$, $K'_{зав0}$ здійснюється за результатами кожного сеансу вимірювань, тобто звітний проміжок часу щодо цих параметрів дорівнює 6 хвилинам. Розрахунок звітних значень параметрів $IPLR_0$ та $P(IPTD_{max})$ - за результатами кожної серії сеансів вимірювань, тобто звітний проміжок часу для цих параметрів дорівнює 1 годині. Для параметра $P_{IP}SA$ звітний проміжок – 1 доба. Параметр $T_{IP}U$ розраховується на звітному проміжку, що дорівнює одному року. Параметри $Kг$ та $MTTR$ розраховуються після кожної події відновлення обладнання.

8.2.3 Дії у разі виявлення невідповідності – аналогічно тим, що розглянуті у підрозділі 8.1.5 цієї лекції.

8.3. Вимірювання параметрів абонентського доступу до транспортної мережі *IP* з використанням обладнання *Frame Relay*

8.3.1 Параметри функціональності

Параметри функціональності щодо трафіка *IP* розглянуто у підрозділі 8.1.1 цієї лекції. Параметри функціональності щодо трафіка *FR* (це – параметри *AR, CIR, EIR, Bc* та *Be*) визначені у підрозділі 7.6.2 лекції №7.

8.3.2 Параметри якості транспортування фреймів (тобто, на параметри QoS та NP обладнання абонентського FR-доступу)

У табл.8.5 надано класифікатор параметрів якості обслуговування при наданні послуги абонентського доступу до транспортної *IP*-мережі з використанням обладнання *FR*.

Визначення параметрів цієї послуги щодо трафіка *IP* надано у розділі 8.1, якщо у якості *PDU* розглядати пакети *IP*. Визначення цих параметрів щодо трафіка *FR* надано у підрозділі 7.6.2 лекції №7.

Таблиця 8.5

Класифікатор параметрів якості обслуговування при наданні послуги абонентського доступу до транспортної мережі IP з використанням обладнання FR

Параметри якості обслуговування		
мережно-орієнтовані (параметри *NP*)	сервіс-орієнтовані (параметри *QoS*)	мережно/сервіс незалежні
1. $IPLR_{max}$; *2. $IPER_{max}$;* *3. $K'_{зав0max}(IP)$;* *4. $Kг_{min}$;* *5. $K'_{зав0max}(FR)$;* *6. FR LR_{max} (CIR);* *7. FR LR_{max} (EIR);* *8. $FRER_{max}$*	*1. $IPTD_{max}$;* *2. $IPDV_{max}$;* *3. P_{max} ($IPTD_{max}$);* *4. P_{min} ($IPDV_{max}$);* *5. $P_{IP}SA_{min}$;* *6. $T_{IP}U_{max}$;* *7. $FRTD_{max(CIR)}$;* *8. $FRTD_{max(EIR)}$*	*1. RP_{max} ;* *2. $MTTR_{max}$*

Примітка 8.17. Мнемонічні позначення параметрів, що наведені у табл.8.5, отримані шляхом заміни у позначеннях параметрів, що наведені у підрозділі 7.2 лекції №7, буквосполучення "*PDU*" на "*IP*" та "*FR* ", оскільки у даному випадку в якості *PDU* використовуються пакети *IP* та фрейми *FR*.

Примітка 8.18. При експлуатації обладнання *FR* активно використовується механізм визначення пов'язаності каналу. Однак параметр пов'язаності є інструментальним засобом спостереження за працездатністю каналу і не характеризує якість обслуговування.

8.3.3 Нормативи на параметри якості у розрізі класів обслуговування

Рекомендовані нормативні значення показників якості обслуговування при наданні послуги абонентського доступу до транспортної мережі *IP* з використанням обладнання *FR* надано у табл.8.6.

Таблиця 8.6

Нормативи якості обслуговування при наданні послуги абонентського доступу до транспортної мережі *IP* з використанням обладнання *FR*

Параметр и обслуг.	Характеристика параметра	Клас 0	Клас 1	Клас 2	Клас 3	Клас 4	Клас 5
Сервіс-орієнто-вані пара-метри							
$IPTD_{max}$	Верхня межа щодо затримки пакетів, мс	10	160	200	200	400	н/в
$IPDV_{max}$	Верхня межа щодо варіації затримки, мс	10	10	60	н/в	н/в	н/в
P_{max} $(IPTD_{max})$	Поріг ймовірності перевищення $IPTD_{max}$, безрозмірний	1×10^{-2}	1×10^{-2}	1×10^{-2}	5×10^{-2}	н/в	н/в

P_{min} *(IPDV$_{max}$)*	Поріг відсотка неперевищення *IPDV$_{max}$*, % (у відсотках)	1,0	1,0	н/в	н/в	н/в	н/в
$P_{IP}SA_{min}$ *(PIA)*	Нижня межа щодо відсотка часу доступності послуги, % (у відсотках)	99	99	99	99	н/в	н/в
$T_{IP}U_{max}$ *(TIU)*	Верхня межа щодо годин недоступності послуги, годин на рік	38	38	38	38	н/в	н/в
FRTD$_{max}$ (CIR)	Верхня межа щодо затримки фреймів з ознакою *DE*=0, мс	10	160	160	160	160	н/в
FRTD$_{max}$ (EIR)	Верхня межа щодо затримки фреймів з ознакою *D*E=1, мс	н/в	н/в	н/в	н/в	н/в	н/в
Мережно-орієнтовані параметри							
IPLR$_{max}$	Верхня межа втрат пакетів, безрозмірна	1×10^{-3}	1×10^{-3}	1×10^{-3}	1×10^{-3}	1×10^{-3}	н/в
IPER$_{max}$	Верхня межа помилкових пакетів,	1×10^{-4}	1×10^{-4}	1×10^{-4}	1×10^{-4}	1×10^{-4}	н/в

	безрозмірна						
$Кг_{min}$	Нижня межа коефіцієнту готовності	0,996	0,996	0,996	0,996	0,996	н/в
$FR\ LR_{max}$ (CIR)	Верхня межа втрат фреймів з ознакою DE=0, безрозмірна	1×10^{-3}	1×10^{-3}	1×10^{-3}	1×10^{-3}	1×10^{-3}	н/в
$FRER_{max}$	Верхня межа помилкових фреймів, безрозмірна	1×10^{-4}	1×10^{-4}	1×10^{-4}	1×10^{-4}	1×10^{-4}	н/в
Сервіс/мережно-незалежні параметри							
$MTTR_{max}$	Верхня межа середнього часу відновлення працездатності, хвилин	300	300	300	300	500	н/в

Примітка 8.19. Позначка “н/в” означає “не визначено”.

Примітка 8.20. Нормативні визначення параметрів $IPTD_{max}$, $IPDV_{max}$, $IPLR_{max}$ та $IPER_{max}$ узгоджені з рекомендаціями *ITU-T Recommendation Y.1541*.

Примітка 8.21. Значення параметру $P_{IP}SA_{min}$ визначається за тими ж умовами, що і при наданні транспортної *IP* послуги.

Примітка 8.22. Значення параметру RP_{max} визначається умовами *SLA*.

Примітка 8.23. Значення параметру *MTTR* враховується, починаючи з моменту фіксації стану непрацездатності обладнання.

Примітка 8.24. Параметри *Кг* та *MTTR* визначаються для усього обладнання,

що використовується для надання послуги.

8.3.4 Умови, точки та порядок вимірювань

В процесі оцінювання параметрів якості транспортування пакетів необхідно дотримуватись загальних вимог щодо організації вимірювань, що були викладені на лекції №5. Крім того, під час вимірювань пікове навантаження крайового *IP*-маршрутизатора (маршрутизатора доступу *AR*), через котрий забезпечується доступ до *IP*-мережі, повинно не перевищувати 90%, а поточні значення параметру помилок $IPER_0$ цього маршрутизатору мають бути не більшими за $IPER_{max}$. Поточні значення параметру помилок $FRER_0$ крайового *FR*-комутатору мають бути не більшими за $FRER_{max}$.

Примітка 8.25. Дані, що є необхідними для обчислення поточних значень цих параметрів, накопичуються у базах *MIB* контрольованого обладнання за допомогою механізмів протоколу *SNMP*. Параметр $FRER_0$ обчислюється на основі спостереження за ознакою *FCS* у форматі фрейму.

Методи та порядок вимірювань параметрів якості обслуговування, що використовуються під час надання послуги абонентського *FR*-доступу до транспортної мережі *IP*, є аналогічними тим, що раніш було розглянуто у лекції №7. А саме, контроль якості обслуговування виконується за шлейфовою схемою на мережному рівні, тобто встановлюється режим періодичного тестування послідовностями *ICMP*-пакетів через фіксовані інтервали часу. За допомогою штатних механізмів *FR*-обладнання в каналі абонентського доступу утворюється *PVC*-з'єднання між пристроєм *FRAD* та крайовим *FR*-комутатором із гарантованою швидкістю передавання даних, що дорівнює *CIR*. Здійснюються активні вимірювання шляхом "пінгування" тестовими *IP*-пакетами через утворене *PVC*-з'єднання у прямому і зворотному напрямках передавання тестових даних. Однак в залежності від того, параметри якого рівня вимірюються – мережного чи канального - використовуються різні пари точок вимірювань.

Використовується шлейфова схема організації вимірювань за схемою включення, що відображена на рис.8.4.

Рис.8.4. Схема організації вимірювань параметрів послуги абонентського доступу до транспортної IP-мережі з використанням обладнання Frame Relay

На рис.8.4 показана точка доступу до послуги SAP та відповідні пари вимірювальних точок. Зокрема, підчас вимірювань на *IP*-рівні необхідно замкнути між собою пару вимірювальних точок MP_4 (за допомогою програмних засобів крайового *IP*-маршрутизатора або хоста, що до нього приєднаний) та здійснювати "пінгування" тестовими *ICMP*-пакетами через точку MP_{egr1}, що розташована на SAP термінального хоста. При цьому спостереження за кореспондованими тестовими *ICMP*-пакетами, що просуваються *IP*-каналом абонентського доступу у зворотному напрямку від крайового *IP*-маршрутизатора до SAP, здійснюється у точці MP_{in1}, що розташована на SAP термінального хоста. Таким чином, пінгування, вимірювання та обробка результатів вимірювань параметрів *IP* рівня здійснюється штатними програмними засобами термінального обладнання споживача, а логічне замикання точок MP_4 – штатними програмними засобами крайового *IP*-маршрутизатора (маршрутизатора доступу) або хоста, що до нього приєднаний.

Під час вимірювань параметрів канального рівня необхідно замкнути між собою пару вимірювальних точок MP_3, але на мережному рівні (тобто, за допомогою програмних засобів спеціально виділеного хоста, що напряму без використання крайового *IP*-маршрутизатора приєднується до комутатора) та здійснювати "пінгування" тестовими *ICMP*-пакетами через точку MP_{egr1}, що розташована на SAP термінального хоста або через точку MP_{egr2} за допомогою спеціально виділеного хоста (у випадку виникнення проблем з хостом споживача). При цьому

спостереження за кореспондованими тестовими пакетами, що просуваються абонентським *FR*-каналом у зворотному напрямку від крайового *FR*-комутатора до *FRAD*, здійснюється у точці MP_{in2}, що створюється програмними засобами спеціально виділеного хоста.

Примітка 8.26. На практиці існує можливість здійснювати вимірювання з боку крайового вузлу *IP*-мережі. В цьому випадку замикання шлейфу робиться парою точок MP_1, а "пінгування" та обробка результатів вимірювань виконується за допомогою програмних засобів крайового вузлу.

Параметри процесу тестування (тобто, структура тестового потоку *ICMP*-пакетів, періодичність звітування тощо) – згідно п. 8.1.4.

В процесі вимірювань мають виконуватися такі дві умови:

1) в кожен один тестовий фрейм необхідно упаковувати лише один пакет;

2) уся тестова послідовність *ICMP*-пакетів має упаковуватися у тестовий потік фреймів з ознакою *DE*=0, тобто у потік *CIR*.

За цих умов поточні оцінки вимірювальних параметрів та норми на параметри якості обслуговування щодо потоків *FR* та *IP* співпадають. Це надає можливість виконати оцінювання параметрів послуги із транспортування потоків фреймів на відповідність нормам шляхом вимірювань та відповідних розрахунків параметрів мережного рівня.

На вимогу споживача або після виявлення ознак невідповідності параметрів *PVC*- з'єднання на рівнях за стеком протоколів, що є вищими за канальний рівень, та котрі не були усунуті засобами мережного рівня, здійснюється аналіз параметрів канального рівня.

Розрахунок звітних значень параметра $FRTD_0$ здійснюється за результатами кожного сеансу вимірювань, параметрів $FRLR_{0(CIR)}$, $FRLR_{0(EIR)}$ - за результатами кожної серії сеансів вимірювань. Параметр $FRER_0$ розраховується на звітному проміжку, що дорівнює 1 добі.

8.3.5. Дії у разі виявлення невідповідності

В процесі надання послуги абонентського доступу до транспортної мережі *IP* з використанням обладнання *Frame Relay*

здійснюється постійний контроль поточного стану обслуговування на рівні *IP*. Такий контроль виконується шляхом відслідковування поточних оцінок параметра втрат пакетів $IPLR_0$. У процесі поточного контролю цього параметру може виявитись перевищення його нормативного значення $IPLR_{max}$. У цьому випадку необхідно переконатися в коректності роботи обладнання мережного рівня (кінцевого хоста та крайового IP-маршрутизатора), наприклад шляхом відключення від нього канального *FR*-обладнання і "пінгування" тестовими пакетами по локальним шлейфам кінцевого хоста та крайового *IP*-маршрутизатора, що створюються як на ближньому, так і на віддаленому кінцях контрольованого *PVC*-з'єднання. Якщо проблем на рівні протоколу *IP* (і вище) на локальних шлейфах не виявлено, необхідно розпочати пошук проблем в роботі *FR*-обладнання.

Плановий періодичний контроль параметрів якості надання послуги абонентського доступу до транспортної мережі *IP* з використанням обладнання *Frame Relay* виконується шляхом відслідковування поточних оцінок усіх параметрів мережного рівня (не тільки $IPLR_0$), які мають співпадати з оцінками параметрів канального рівня. У процесі планового контролю може виявитись перевищення будь-якого із нормованих значень параметрів. У цьому випадку необхідно переконатися в коректності роботи обладнання мережного рівня.

Примітка 8.27. Пошук шляхів вирішення проблем невідповідності на канальному рівні щодо контрольованого *PVC*-з'єднання має сенс лише для потоку тестових фреймів с ознакою *DE*=0, швидкість котрого встановлюється на рівні *CIR*.

Примітка 8.28. Пінгування *ICMP*-пакетами в потоці фреймів з ознакою *DE*=1 (тобто, організація тестових *EIR*-потоків) здійснюється з метою оцінки ненормованого параметра $FRLR_{0\ (EIR)}$ в процесі визначення рівня завантаженості крайового *FR*-комутатора, через який здійснюється абонентський доступ.

У випадку виникнення невідповідностей під час транспортування пакетів *IP* через канал абонентського доступу, що створений на основі використання обладнання *FR*, необхідно перейти до повномасштабних системних вимірювань параметрів, що надані в табл.8.6, та пошуку шляхів вирішення виявленої

проблеми спочатку на мережному, а потім на канальному рівнях. Якщо на цих рівнях проблему не вирішено, необхідно дослідити працездатність обладнання фізичного рівня, що, можливо, призведе до необхідності відключення корисного навантаження від проблемного абонентського каналу.

У разі виявлення перевищень нормованих значень мережно-орієнтованих параметрів розпочинають пошук проблем, пов'язаних із відмовами в роботі мережного обладнання згідно з положеннями регламентуючої експлуатаційної документації на мережне обладнання, що використовується.

8.4. Вимірювання параметрів абонентського доступу до транспортної мережі *IP* з використанням обладнання *xDSL*

Структурна схема обладнання *xDSL*, параметри котрого мають бути охоплені контролем під час надання послуги абонентського доступу до транспортної мережі *IP* з використанням обладнання *xDSL*, відображена на рис.8.5. Як бачимо, одна лінія зв'язку *xDSL* може включати у себе від одного до трьох аналогових транспортних каналів, тобто від одної до трьох пар фізичних проводів абонентських ліній телефонного зв'язку. На вузлі доступу до *IP*-мережі лінія *xDSL* приєднується до мультиплексору абонентського доступу *xDSL*, тобто до *DSLAM* (*Digital Subscribe Access Multiplexor*). Цей мультиплексор може бути конструктивно виконаний у вигляді окремого пристрою або входити до складу серверу абонентського доступу *AS* або до складу маршрутизатору абонентського доступу *AR*.

8.4.1 Параметри функціональності

Параметри функціональності щодо трафіка *IP* розглянуто у підрозділі 8.1.1 цієї лекції. Параметри функціональності щодо трафіка *xDSL* (це – параметри RL_{AD}, RC_{AD}, RL_{AR}, RC_{AR}) визначені у підрозділі 6.6 лекції №6. Зокрема, це бітова швидкість передавання даних:

- у дуплексній лінії *xDSL* - ***RL (Rate line)***;

- у дуплексному аналоговому транспортному каналі, який утворений на основі однієї із фізичних пар телефонних проводів, що прокладена між споживачем мережних послуг і вузлом

електрозв'язку – ***RC (Rate channel)***.

Зрозуміло, що слід відрізняти параметри швидкості для лінії *xDSL* від параметрів швидкості для транспортного каналу, утвореного на базі однієї із телефонних пар.

RL_{AD} - швидкість передавання даних у прямому напрямку передачі через абонентську лінію *xDSL* (тобто, від вузла зв'язку до покупця послуги), що вимірюється у біт/с (*bps – bits per second*).

RC_{AD} – швидкість передавання даних у прямому напрямку передачі через транспортний канал *xDSL*, що вимірюється у біт/с.

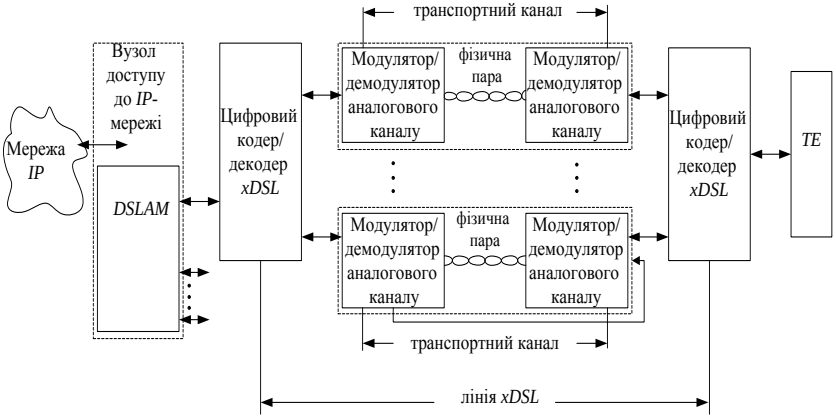


Рис.8.5. Структурна схема абонентського доступу з використанням обладнання

8.4.2. Параметри якості транспортування фреймів xDSL (тобто, на параметри QoS та NP обладнання абонентського xDSL-доступу)

Класифікатор параметрів якості обслуговування при наданні послуги абонентського доступу до транспортної *IP*-мережі з використанням обладнання *xDSL*, технічна та організаційна підтримка котрих має забезпечуватися операторами електрозв'язку, містить дві підмножини параметрів. Перша підмножина характеризує якість обслуговування на рівні використання обладнання *IP*. Визначення параметрів цієї підмножини надано у розділі 8.1 Параметри другої підмножини, які характеризують якість обслуговування на рівні використання обладнання *xDSL*,

надані у підрозділі 6.5.1.2 лекції №6.

8.4.3. Нормативи на параметри якості у розрізі класів обслуговування

Рекомендовані норми на показники якості обслуговування, що стосуються мережного рівня (тобто, рівня *IP*) надання послуги абонентського доступу до транспортної *IP*-мережі з використанням обладнання xDSL, наведені у табл.8.7.

Експлуатаційні норми на параметри якості обслуговування канального рівня при наданні послуги абонентського доступу до транспортної мережі *IP* з використанням обладнання *xDSL* наведені у табл.8.8.

Пояснення щодо нормування параметрів обладнання xDSL було надано у підрозділі 6.5.1.3 лекції №6.

Таблиця 8.7

Нормативні значення показників якості обслуговування мережного рівня при наданні послуги абонентського доступу до транспортної мережі *IP* з використанням обладнання *xDSL*

Параметри *IP*-обладнання	Характеристика параметра	Клас 0	Клас 1	Клас 2	Клас 3	Клас 4	Клас 5
Сервіс-орієнто-вані параметри							
$IPTD_{max}$	Верхня межа щодо затримки пакетів, мс	10	160	200	200	400	н/в
$IPDV_{max}$	Верхня межа щодо варіації затримки, мс	10	10	60	н/в	н/в	н/в
P_{max} $(IPTD_{max})$	Поріг ймовірності перевищення $IPTD_{max}$, безрозмірний	1×10^{-2}	1×10^{-2}	1×10^{-2}	5×10^{-2}	н/в	н/в
P_{min}	Поріг	1,0	1,0	н/в	н/в	н/в	н/в

(IPDV$_{max}$)	відсотка неперевищення *IPDV$_{max}$*, % (у відсотках)						
P$_{IP}$SA$_{min}$ (PIA)	Нижня межа щодо відсотка часу доступності послуги, % (у відсотках)	99	99	99	99	н/в	н/в
T$_{IP}$U$_{max}$ (TIU)	Верхня межа щодо годин недоступності послуги, годин на рік	38	38	38	38	н/в	н/в
Мережно-орієнто-вані параметри							
IPLR$_{max}$	Верхня межа втрат пакетів, безрозмірна	1×10^{-3}	1×10^{-3}	1×10^{-3}	1×10^{-3}	1×10^{-3}	н/в
IPER$_{max}$	Верхня межа помилкових пакетів, безрозмірна	1×10^{-4}	1×10^{-4}	1×10^{-4}	1×10^{-4}	1×10^{-4}	н/в
Кг$_{min}$	Нижня межа коефіцієнту готовності	0,996	0,996	0,996	0,996	0,996	н/в
Сервіс/мережно-незалежні параметри							
MTTR$_{max}$	Верхня межа середнього часу відновлення працездатнос	300	300	300	300	500	н/в

	ті, хвилин						

Примітка 8.29. Позначка “н/в” означає “не визначено”.

Примітка 8.30. Нормативні визначення параметрів $IPTD_{max}$, $IPDV_{max}$, $IPLR_{max}$ та $IPER_{max}$ узгоджені з рекомендаціями *ITU-T Recommendation Y.1541*.

Примітка 8.31. Значення параметру $P_{IP}SA_{min}$ визначається за тими ж умовами, що і при наданні транспортної *IP* -послуги.

Примітка 8.32. Значення параметру RP_{max} визначається умовами *SLA*.

Примітка 8.33. Значення параметру $MTTR_{max}$ враховується, починаючи з моменту фіксації стану непрацездатності обладнання.

Таблиця 8.8

Експлуатаційні норми на параметри канального рівня при наданні послуги абонентського доступу до транспортної мережі *IP* з використанням обладнання *xDSL*

Довгострокові норми		Оперативні норми	
ESR	*SESR*	*ESR*	*SESR*
0,012	0,0002	0,006	0,0001

Примітка 8.34. Із всієї множини параметрів *xDSL* канального рівня, що розглянуті у підрозділі 6.5.1.2 лекції №6, нормуються лише параметри *ESR* та *SESR*. Нагадаємо, що *ES* (*errors seconds*) – це проміжок часу (виміряний у секундах), впродовж котрого спостерігаються помилки усіх видів у каналі, котрий знаходиться у стані готовності. Тобто, *ES* – це кількість секунд з помилками, що виявлені серед усіх секунд готовності каналу *AS*. Секунди з помилками, що виявлені у стані неготовності каналу *UAS*, не враховуються. *ESR* (*errors seconds rate*) – коефіцієнт помилок щодо секунд з помилками [безрозмірна величина] – це відносна кількість секунд з помилками *ES* щодо загальної кількості секунд у *AS*.

Примітка 8.35. Підрахунок *ES* та *SES* під час визначення *ESR* та *SESR* здійснюється тільки на інтервалах придатності лінії *xDSL* до користування, тобто секунди *UAS* не враховуються.

Примітка 8.36. У рекомендації *G.821* надані норми щодо повного міжнародного *ISDN*-з’єднання: для $ESR < 0{,}08$ і для $SESR < 0{,}002$. У цій рекомендації надано також розподіл цих норм між трьома визначеними дільницями такого з’єднання. Для дільниці абонентського доступу визначені наступні норми: $ESR < 0{,}012$, $SESR < 0{,}0002$. Саме ці значення вибрані у якості норм для лінії *xDSL*, що використовується для абонентського доступу.

Примітка 8.37. Значення нормованих показників *ESR* та *SESR* для оперативних норм відповідно до рекомендації *G.821* удвічі менші значень цих показників для довгострокових норм.

8.4.4 Умови, точки та порядок вимірювань

Структурна схема організації вимірювань параметрів якості обслуговування при наданні послуги абонентського доступу до транспортної *IP*-мережі з використанням обладнання *xDSL*, відповідні точки доступу до послуги та пари вимірювальних точок відображені на рис.8.6.

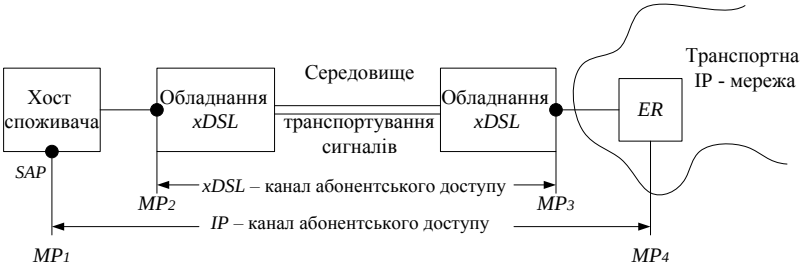


Рис.8.6. Схема вимірювань параметрів послуги абонентського доступу до транспортної IP-мережі з використанням обладнання xDSL

Умови, методи, точки та порядок вимірювань параметрів канального рівня обладнання *xDSL* аналогічні тим, що наведені у підрозділі 6.6.1.4 лекції №6.

Обладнання *xDSL* передбачає вимірювання лише параметрів *ESR* та *SESR*. Ці вимірювання здійснюються у реальному часі у фоновому режимі за схемою «точка – точка» без відключення корисного навантаження на лінію *xDSL*. Період одного сеансу вимірювань під час контролю – 15 хвилин.

8.4.5 Дії у разі виявлення невідповідності

В процесі надання послуги абонентського доступу до транспортної мережі *IP* з використанням обладнання *xDSL* здійснюється постійний контроль поточного стану обслуговування на рівні *IP*. Такий контроль виконується шляхом відслідковування поточних оцінок параметра втрат пакетів $IPLR_0$. У процесі

поточного контролю цього параметру може виявитись перевищення його нормативної межі $IPLR_{max}$. У цьому випадку необхідно переконатися в коректності роботи обладнання мережного рівня, наприклад шляхом відключення від нього канального *xDSL*-обладнання і "пінгування" тестовими пакетами по локальному шлейфу, що створюється як на ближньому, так і на віддаленому кінцях абонентського каналу. Якщо проблем на рівні протоколу *IP* (і вище) на локальних шлейфах не виявлено, необхідно розпочати пошук проблем в роботі *xDSL*-обладнання.

Плановий періодичний контроль параметрів якості надання послуги абонентського доступу до транспортної мережі *IP* з використанням обладнання *xDSL* виконується шляхом відслідковування поточних оцінок усіх параметрів мережного рівня (тобто, усіх параметрів із табл.8.7, не тільки $IPLR_0$) за умов, коли в кожен один тестовий фрейм *xDSL* упаковується лише один пакет *IP*. У процесі планового контролю може виявитись перевищення будь-якого із нормативних значень параметрів. У цьому випадку необхідно переконатися в коректності роботи обладнання мережного рівня, зокрема виконуючи дії згідно п.8.1.5.

У разі виявлення перевищень нормативних значень мережно-орієнтованих параметрів на шлейфі, побудованому згідно рис.8.6 між парами вимірювальних точок MP_1 та MP_4, розпочинають пошук проблем, пов'язаних із відмовами в роботі мережного обладнання згідно з положеннями регламентуючої експлуатаційної документації на мережне обладнання, що використовується. Від оперативного експлуатаційного контролю відповідності параметрів, що надані в табл.8.7, переходять до системних вимірювань канального рівня (починаючи із вимірювань параметрів, що зазначені у табл.8.8).

Примітка 8.38. У ряді випадків такі вимірювання потребують відключення корисного навантаження від проблемної лінії *xDSL* або проблемного транспортного каналу *xDSL*.

Якщо дослідження проблем канального рівня не дало позитивного результату, необхідно здійснити комплекс повномасштабних вимірювань фізичного рівня з урахуванням положень, що викладені у лекції №6.

Контрольні питання до восьмої лекції

1. Що таке наскрізне з'єднання типу "точка – точка"?

2. Наведіть та поясніть схему організації вимірювань параметрів обладнання транспортної *IP*-мережі при наскрізному з'єднанні типу "точка –точка".

3. Що таке *SAP* (*Service Access Point*)?

4. Наведіть та поясніть схему організації вимірювань параметрів обладнання транспортної *IP*-мережі при наскрізному з'єднанні типу "споживач-споживач".

5. Надайте характеристики параметрам функціональності послуг із транспортування пакетів.

6. Надайте характеристики параметрам якості транспортування пакетів.

7. Які показники доступності транспортної послуги Ви знаєте?

8. Які показники доступності мережного обладнання Ви знаєте?

9. Які показники експлуатаційної надійності Ви знаєте?

10. Що таке клас обслуговування?

11. Який існує порядок вимірювань параметрів наскрізних IP-з'єднань?

12. Яка має бути структура тестового потоку пакетів IP при вимірюваннях параметрів наскрізного IP-з'єднання?

13. Які дії має виконувати експлуатаційний персонал у разі виявлення невідповідності під час поточного контролю якості наскрізного з'єднання?

14. Наведіть та поясніть базову схему вимірювань для оцінювання параметрів абонентського *IP*-доступу до глобальної транспортної мережі.

15. Наведіть та поясніть схему організації вимірювань параметрів послуги абонентського доступу до транспортної *IP*-мережі з використанням обладнання *Frame Relay*.

16. Надайте характеристики параметрам послуги абонентського доступу до транспортної *IP*-мережі з використанням обладнання *Frame Relay*.

17. Які мають бути параметри процесу тестування під час вимірювань параметрів послуги абонентського доступу до транспортної *IP*-мережі з використанням обладнання *Frame Relay*?

18. Які дії має виконувати експлуатаційний персонал у разі

виявлення невідповідності під час поточного контролю параметрів послуги абонентського доступу до транспортної *IP*-мережі з використанням обладнання *Frame Relay*?

19. Наведіть та поясніть схему організації вимірювань параметрів послуги абонентського доступу до транспортної *IP*-мережі з використанням обладнання *xDSL*.

20. Надайте характеристики параметрам послуги абонентського доступу до транспортної *IP*-мережі з використанням обладнання *xDSL*.

21. Які мають бути параметри процесу тестування під час вимірювань параметрів послуги абонентського доступу до транспортної *IP*-мережі з використанням обладнання *xDSL*?

22. Які дії має виконувати експлуатаційний персонал у разі виявлення невідповідності під час поточного контролю параметрів послуги абонентського доступу до транспортної *IP*-мережі з використанням обладнання *xDSL*?

Література до восьмої лекції

1) Г.Ф. Конахович, В.М. Чуприн. Сети передачи пакетной коммутации.–К.: МК-Пресс, 2006. Розділи 9, 10 та 14.

МОДУЛЬ №3. ТЕХНОЛОГІЇ ПІДТРИМКИ ПРАЦЕЗДАТНОГО СТАНУОБЛАДНАННЯ

ЛЕКЦІЯ №9. ХАРАКТЕРИСТИКА ЗАДАЧ ТА ПРОЦЕДУР ПІДТРИМКИ ПРАЦЕЗДАТНОСТІ

Розглядаються наступні питання:
Лекційне заняття
9.1. Узагальнена модель дослідження працездатності обладнання
9.2. Основні методи контролю
9.3. Основні засоби контролю
Самостійне заняття. Тестування взаємодії відкритих систем.

9.1. Узагальнена модель дослідження працездатності обладнання

Нагадаємо базові поняття, котрими користуються в процесі технічної експлуатації ТЛК-обладнання: функціональна група задач експлуатації, задача експлуатації, метод вирішення задачі експлуатації, процедура експлуатації, окрема процедурна операція, методика здійснення процедури експлуатації (що розглядається як опис умов та порядку виконання процедурних операцій), норми на припустимі значення показників (параметрів) обладнання – об'єкту експлуатації, інструментальний засіб здійснення експлуатаційної процедури.

Нагадаємо також, що підтримка працездатного стану ТЛК-обладнання (тобто, *Fault Maintenance*) – одна з основних груп задач технічної експлуатації (ТЕ). Як вже раніш зазначалось (див. лекцію №1), до *Fault Maintenance* відносяться три типових види задач ТЕ: контроль стану обладнання (тобто, контроль відповідності його параметрів припустимим нормам), діагностування стану обладнання та відновлення працездатного стану обладнання після його відмови. Іноді на основі результатів довготривалого контролю та діагностування ставлять та вирішують задачі прогнозування стану обладнання на майбутні проміжки часу та (або) задачі розвитку (тобто, удосконалення) ТЛК-обладнання, що є об'єктом експлуатації. Таким чином, до функціональної групи задач підтримки працездатності ТЛК-обладнання відносяться п'ять

видів задач: контроль стану в поточний момент часу (К), діагностування стану (Д), відновлення нормального стану (В), прогнозування стану (П) та удосконалення стану (У) обладнання в період експлуатації цього обладнання.

Під час вирішення усіх цих задач експлуатаційний персонал, як правило, здійснює, у той чи інший спосіб, процедури вимірювань параметрів обладнання, процедури тестування та моніторингу обладнання і процедури аналізу результатів вимірювань (зокрема, процедури аналізу телекомунікаційних протоколів).

Процедури вимірювання. Щодо процедур вимірювання параметрів, то вони були детально розглянуті на попередніх лекціях у рамках модулю №2 і додаткових пояснень не потребують. Зокрема, процедура вимірювання, що здійснюється з метою знаходження значення величини параметру за допомогою спеціальних інструментальних засобів, розглядається як однократний акт порівняння величини параметра, що вимірюється, із величиною певного еталону – мірила величини цього параметру. Будь-який інструментальний засіб безпосередньо або опосередковано відтворює еталон вимірюваного параметру (або похідні від нього) та порівнює величину цього еталону з величиною параметру. Формальні визначення характеристик процесів вимірювання вивчаються у рамках дисципліни „Метрологія, стандартизація, сертифікація та акредитація". У контексті цієї лекції лише нагадаємо, що результат вимірювання розглядається як приблизна оцінка (з тою чи іншою похибкою) істинного значення величини вимірюваного параметру. Приблизну оцінку істинного значення величини, що отримана шляхом вимірювавння, називають також дійсним значенням величини вимірюваного параметру. Так що істинне значення величини – це абстракція, а її дійсне значення – це результат вимірювання. Різниця між дійсним та істинним значенням величини – це похибка вимірювань, що залежить від багатьох чинників, у т.ч. і від інструментальних похибок вимірювального засобу.

Примітка 9.1. Окремим різновидом вимірювань є процедура рахування, що використовується для визначення числового значення дискретної величини, дискретного параметра фізичного процесу або кількості предметів у даній множині. Результатом рахування є безрозмірне число.

На практиці інтерес являє не тільки проблема зменшенння похибки вимірювання, але і проблема гарантування того, що ця похибка навіть у найгірших умовах вимірювань не перевищить наперед визначену межу. Тобто, необхідно отримати гарантії, що величина похибки вимірювань буде у припустимих межах.

Процедури аналізу. Якщо ж маємо справу із багатократними певним чином упорядкованими актами вимірювань, результати котрих оброблюються за наперед визначеними правилами у наперед визначених умовах вимірювань з наперед визначеною метою, то така процедура називається **аналізом**. Іншими словами, аналіз якогось об'єкта (наприклад, стану елемента обладнання, змін значень параметра обладнання, форми канального сигналу, коректності реалізації телекомунікаційного процесу або протоколу) являє собою метод дослідження цього об'єкту за допомогою спеціальних інструментальних засобів, що здійснюють багатократні вимірювання параметрів цього об'єкту із подальшою обробкою отриманих результатів вимірювань відповідно до визначених правил цієї обробки. Наприклад, аналіз форми сигналів здійснюють з використанням таких інструментальних пристроїв як аналізатори спектрів, аналіз результатів рахування – аналізаторів статистичних даних, а аналіз коректності виконання ТЛК-протоколів – аналізаторів протоколів.

Процедури аналізу протоколів. Звернемо увагу, що під протоколом (у будь-якій сфері, не тільки у телекомунікаціях) розуміється певний набір правил або стандартів, що регламентують виконання наперед визначених процедур. Телекомунікаційні протоколи (ТЛК-протоколи) регламентують: формати представлення сигналів та інформаційних повідомлень, що ці сигнали переносять; порядок утворення каналів транспортування сигналів та повідомлень (з'єднання/розривання фізичних та логічних каналів, утворення/розривання сеансів зв'язку тощо); порядок обміну сигналами та повідомленнями в межах утворених каналів або сеансів зв'язку. Тому ТЛК-протоколи відображаються у вигляді логічно структурованих наборів сигналів та (або) повідомлень, елементи котрих є функціями часу. Здійснення операцій над цими наборами під час вирішення експлуатаційних завдань є ні чим іншим, як процедури аналізу ТЛК-протоколів.

До процедур аналізу протоколів відноситься також процедура пошуку відповідності реалізації протоколу заданій нормі, що також представлена у вигляді логічно структурованого набору сигналів та (або) повідомлень. Такий унормований набір називається специфікацією протоколу. Вищезазначена процедура пошуку передбачає виконання операції порівняння, у результаті котрої встановлюється відповідність або невідповідність реалізації аналізованого протоколу його специфікації.

Процедури тестування. На практиці значний відсоток проблем виникає через несприятливі збіги різноманітних обставин (на кшалт всіляких збоїв, помилок, логічних конфліктів, виходу значень параметрів за межі припустимих норм тощо), що призводять до виникнення невідповідностей, а, в найгірших випадках, і до відмов в роботі обладнання.

Примітка 9.2. Ще раз нагадаємо, що збій (а також помилка, логічний конфлікт, вихід параметра за межі норм і т.ін.) та відмова – це принципово різні речі. Зазвичай збій (помилка, конфлікт і т.ін) в роботі обладнання не завжди призводить до призупинки надання послуг клієнтам, що користуються ресурсами цього обладнання. Тобто, внаслідок збою рівень якості надання послуг може погіршитися, але процес надання послуг не призупиняється. Відмова обладнання – набагато більш негативне явище, ніж його збій. Внаслідок відмови процес надання послуг з використанням ресурсів цього обладнання призупиняється, що призводить до прямих бізнесових збитків для операторів ТЛК-систем.

Зазвичай невідповідності в роботі обладнання виникають відносно рідко. Однак ситуація ускладнюється тим, що проблеми невідповідності можуть непрогнозовано виникати, потім зникати, потім знов виникати і т.д. При цьому часто трапляється, що проміжки часу, коли обладнання перебуває у невідповідному стані, є незрівняно меншими, ніж проміжки нормальної роботи обладнання. Тому за таких умов, якщо не здійснювати спеціальних цілеспрямованих заходів, існує проблема із своєчасним виявленням моментів виникнення невідповідностей в роботі обладнання.

Одним із розповсюджених прийомів, особливо коли нема упевненості у нормальному функціонуванні обладнання, являється моделювання умов роботи обладнання, що сприяють виявленню можливих невідповідностей в його роботі. Процедура тестування за своєю сутністю якраз і є моделюванням таких умов. Перед тим, як розпочати процедуру тестування, тестувальник повинен

заздалегідь знати реакцію контрольованої системи на той чи інший тестовий вплив на увідні порти цієї системи (наприклад, вплив у вигляді визначеного набору еталонних сигналів та реакцію у вигляді визначених повідомлень від об'єкту тестування). І якщо увідні тестуючі впливи адекватно відображають вірогідні умови виникнення невідповідностей в роботі обладнання, то за цих умов, слід сподіватися, на більшу ймовірність своєчасного виявлення моментів виникнення шуканих невідповідностей в роботі обладнання.

Процедуру тестування іноді розглядають як різновид процедури аналізу, що пов'язаний із активним цілеспрямованим втручанням у хід роботи обладнання. Звичайна процедура аналізу передбачає необхідність здійснення багатократних вимірювань параметрів обладнання у штатних умовах його функціонування, тобто коли воно зайнято обробкою корисного навантаження. Тестування же передбачає створення штучних умов функціонування обладнання і саме таких умов, коли очікується із найбільшим ступенем ймовірності прояв невідповідності в роботі обладнання, якщо таки він мав місце у реальності. Сутність будь-якого тестування полягає у поданні на вхід обладнання, що проходить тестування, точно визначеного набору тестових сигналів або повідомлень і порівнянні отриманої реакції – вихідних сигналів або повідомлень – із звісними еталонними сигналами або повідомленнями. Якщо реакція обладнання на тестові сигнали або повідомлення співпала (у заданих межах) із еталоном, то робиться висновок, що обладнання знаходиться у працездатному стані. Якщо ж такий збіг не спостерігався, то робиться висновок, що в роботі обладнання виникла проблема невідповідності.

Таким чином, процедуру тестування можливо визначити як встановлення експериментальним шляхом за допомогою спеціальних тестуючих засобів факта відповідності (або невідповідності) між станом контрольованого обладнання, що знаходиться під штучно створеним впливом строго визначеної послідовності тестових сигналів (або тестових повідомлень), та заданою нормою. Норма задається у вигляді наперед визначеного набору еталонних сигналів (або еталонних повідомлень) і зберігається у явному або неявному вигляді у складі тестуючого

засобу. Цей тестуючий засіб також зберігає (або відтворює в процесі тестування), окрім норми, набір тестових сигналів (або тестових повідомлень), що подаються на вхід обладнання. Зрозуміло, що результат тестування може відповідать або не відповідать заданій нормі із певною достовірністю та погрішністю (похибкою) тестування. Достовірність тестування визначається як ймовірність знаходження параметрів контрольованого об'єкту у нормі або поза нормою. Поняття погрішності тестування відноситься лише до параметрів обладнання, що мають кількісний вимір. Тобто, до параметрів фізичних сигналів та елементів обладнання, а не до параметрів логічних об'єктів типу ТЛК-протокол. Погрішність тестування – це різниця між отриманими значеннями параметрів сигналів на виході обладнання (як реакції на вплив вхідних тестових послідовностей сигналів) та значеннями еталонних сигналів на границях заданої норми. Зрозуміло також, що процедури тестування в залежності від експлуатаційних завдань можуть включати до свого складу як процедури вимірювань, так і процедури аналізу виміряних даних.

На практиці знайшли застосування різноманітні процедури тестування, що здійснюються з метою вирішення широкого спектру експлуатаційних завдань. Із найбільш поширених застосувань цієї процедури слід вказати на наступні.

Тестування робочих режимів функціонування обладнання. На вхід контрольованого обладнання подають тестові послідовності, що є характерними для штатних режимів роботи обладнання. Якщо реакція обладнання на ці тестові впливи є штатною, тобто знаходиться у межах заданих норм, то робиться висновок, що обладнання знаходиться у нормальному працездатному стані. У протилежному випадку, робиться висновок про існування проблем із відповідністю параметрів обладнання заданим нормам.

Стресове тестування обладнання. На практиці іноді необхідно визначити граничні можливості роботи обладнання у тих чи інших умовах його функціонування: граничну пропускну спроможність елементів обладнання, максимально можливе навантаження на обладнання, можливість штатного функціонування обладнання в умовах інтенсивного впливу негативних факторів і т.ін. У цьому випадку на вхід обладнання

подають стресові впливи і спостерігають за його реакцією. Якщо ця реакція знаходиться у нормі, то збільшують інтенсивність стресових впливів. І так до тих пір, поки не знайдуть границю між нормальним станом обладнання і станом, коли виникають невідповідності у його роботі.

Локалізація проблем невідповідності в роботі обладнання шляхом моделювання ймовірних умов виникнення цих невідповідностей. Зрозуміло, що у цьому випадку на вхід обладнання подають тестові послідовності, що моделюють умови, за яких найбільш ймовірно, як на думку тестувальників, проявляться ознаки виникнення прогнозованої ними невідповідності в роботі обладнання. На практиці у супроводжувальній експлуатаційній документації, як правило, надається перелік характерних невідповідностей, що можуть виникнути в процесі експлуатації обладнання. Тому для кожної такої невідповідності бажано мати наперед визначені набори тестових послідовностей, щоб у випадках, коли існує підозра щодо виникнення цієї невідповідності на практиці, мати можливість запуску цих тестових послідовностей в роботу.

Процедури моніторингу. Однозначного розуміння (не говорячи вже про визначення) поняття „моніторинг", наскільки нам відомо, не існує. В одних випадках під моніторингом розуміється розподілена у часі та (або) у просторі процедура вимірювання та аналізу одночасно багатьох параметрів багатьох об'єктів на відповідність встановленим нормам на припустимі значення цих параметрів. Отже згідно із цим визначенням під час моніторингу процедури тестування не здійснюються. Проте існує й інше розуміння моніторингу, відповідно до якого під час моніторингу на вхід контрольованої системи мають подаватися точно визначені послідовності сигналів, які за певних умов розглядають як тестові сигнали. У цьому разі моніторинг визначається як різновид процедури тестування.

Узагальнена модель дослідження працездатності обладнання, що ілюструє взаємозв'язок процедур та задач підтримки працездатності ТЛК-обладнання, відображена на рис.9.1 у вигляді графа. У центральній частині рисунку бачимо певну площину, що складається із трьох видів процедур: вимірювання

(В), аналіз (А) та тестування (Т). (Процедури моніторингу на рис.9.1 не позначені, оскільки вони розглядаються як різновиди процедур В, А або Т). Експлуатаційні задачі із підтримки працездатності, а саме контроль відповідності (К) та діагностування (Д) відображаються на рисунку у вигляді вершин графа, що спираються на площину видів процедур.

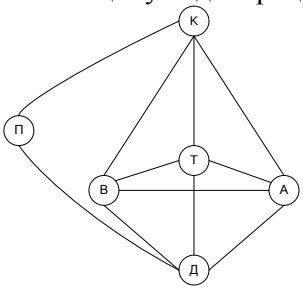


Рис.9.1. Взаємозв'язок процедур та задач підтримки працездатності

Окрім цього, на рис.9.1 буквою П позначена задача прогнозування стану обладнання, для вирішення котрої необхідно знати результати контролю або діагностування цього обладнання.

9.2. Основні методи контролю працездатності

Оскільки контроль працездатності обладнання передбачає виконання процедур вимірювання, аналізу та тестування, то доцільно розглянути основні методи реалізації цих процедур.

Методи вимірювання. Існують три основні групи методів вимірювання фізичних величин:

1) **методи зіставлення**, згідно котрих процедура вимірювання складається із лише одної операції порівняння вимірюваної величини із еталонною величиною заданого розміру (зрозуміло, що перш ніж здійснити порівняння, необхідно якимось чином заздалегідь відтворити еталонну величину заданого розміру);

2) **методи урівноваження**, згідно котрих процедури вимірювання здійснюються поступово за декілька кроків наближення вимірюваної величини до еталонної величини заданого розміру;

3) **диференціальні методи**, згідно котрих процедури вимірювання також здійснюються поступово за декілька кроків,

але для вимірювань використовуються дві різні міри та процедура порівняння, що визначає спочатку різність у першому наближенні, потім у другому більш точному наближенні і т.д.

Вимірювальні засоби, що призначені для вимірювань фізичних величин, як правило включають до свого складу міру (тобто, об'єкт, що відтворює еталонну величину, яка має бути однорідною із вимірюваною величиною), механізм реалізації процедури порівняння міри із вимірюваною величиною та вимірювальний перетворювач, що призначений для узгодження характеристик вимірювального пристрою із характеристиками користувацького (вивідного) інтерфейсу цього пристрою. Окрім цього, до вищеназваного складу додають ще і масштабний перетворювач, що призначений для узгодження за розміром міри та вимірюваної величини.

Методи зіставлення та урівноваження реалізують на основі використання схем із багатоканальною нерегульованою мірою та операцією порівняння, що виконується одночасно кількома пристроями порівняння, або із одноканальною нерегульованою мірою і кількома багатоканальними масштабними перетворювачами. Засоби, що побудовані на методі урівноваження, при цьому, можуть здійснювати одночасне або різночасне урівноваження. Одночасне урівноваження передбачає одноетапну зміну вихідної величини (або коефіцієнту перетворення регульованого масштабного перетворювача) до тих пір, пока вона зрівняється із вхідною вимірюваною величиною. Різночасне урівноваження (яке називається також методом заміщення) здійснюється у два етапи і базується на виконанні вимірювань із використанням регульованого масштабного перетворювача та схеми порівняння. На першому етапі значення вихідної величини масштабного перетворювача запам'ятовується, а на другому етапі на вхід схеми порівняння подається змінний вихідний сигнал регульованої міри до тих пір, поки він зрівняється із величиною, що була зафіксована у пам'яті.

Диференціальні методи також реалізуються на основі використання двохетапних процедур. Вимірювана величина X_0 спочатку вимірюється за допомогою міри, що має великий крок квантування. У результаті отримується перше наближення до цієї

величини X_1. Далі береться різниця $\Delta x_1 = X_0 - X_1$. На другому етапі процедури ця різниця вимірюється за допомогою міри, що має менший крок квантування. У результаті отримується наближена оцінка величини різниці, тобто Δx_2. Накінець, за результатами обох етапів маємо оцінку шуканої величини: $X_0 = X_1 + \Delta x_2$.

В експлуатаційній практиці, як правило, цікавляться середніми значеннями вимірюваних параметрів обладнання, де інтервал усереднення обирається в залежності від характеру задач, що потребують вирішення. Для вимірювань усереднених значень параметрів до складу вимірювальних засобів додаються інтегратори – аналогові або цифрові.

Методи аналізу. Метод аналізу – це певна сукупність правил, згідно котрих встановлюють залежність відношення порядку між повідомленнями у ТЛК-протоколі або співвідношення між розмірами однорідних величин (зокрема, значеннями вимірюваного параметра або спектральними складовими у спектрі сигналу) від часової координати або частотного параметра у відповідності із реалізованим принципом аналіза ТЛК-протоколу або фізичного процесу за допомогою того чи іншого засобу аналіза. Наприклад, спектральний аналіз форми сигналів передбачає перехід від часового представлення сигналів до частотного представлення цих сигналів за допомогою прямого перетворення Фур'є, а відтворення сигналу, спектр якого є відомим, – за допомогою зворотного перетворення Фур'є. На відміну від аналіза спектрів, під час аналізу логічно структурованих даних використовуються тільки логічні операції. Тому методи аналізу логічно структурованих даних розділяють за методами кодування/декодування цих даних або за методами організації взаємодії елементів контрольованої системи (зокрема, за методами аналізу ТЛК-протоколів). Наприклад, для реалізації процедур виявлення та корекції помилок під час передавання даних використовуються різноманітні методи аналізу кодів: аналіз *CRC*, аналіз кода Ріда-Соломона, кода Боуза-Чоудхурі-Хоквінгема і т.ін. Проте особливе місце в задачах підтримки працездатності ТЛК-обладнання займає аналіз ТЛК-протоколів, котрому присвячено матеріал наступної лекції.

Методи тестування. На практиці існує широкий спектр видів та методів тестування ТЛК-обладнання, обгрунтований вибір

котрих та їхнє коректне використання при вирішенні багатьох експлуатаційних завдань являє непросту інженерну задачу, що потребує спеціальних навичок та знань. У типових випадках під час експлуатації ТЛК-обладнання використовують так звані експлуатаційні тести, умови та сфери застосування котрих у вигляді процедур тестування робочих режимів функціонування обладнання або процедур стресового тестування і т.ін. було розглянуто вище. Узагальнена схема проведення такого тестування має наступний вигляд. До обладнання, що підлягає тестуванню, підключається апаратний тестувальний пристрій або у склад цього обладнання уводяться тестувальні програмні засоби, що здатні відтворювати норму у вигляді наперед визначеного набору еталонних сигналів (або еталонних повідомлень, якщо мова йде про тестування ТЛК-протоколів). Окрім цього, тестувальні засоби (програмні або апаратні) мають бути здатними генерувати набори тестових послідовностей сигналів (або повідомлень), які під час тестування подаються на вхід досліджуваного обладнання. Якщо реакція обладнання на тестові сигнали або повідомлення співпала (у заданих межах) із нормою, то робиться висновок, що обладнання знаходиться у працездатному стані. Якщо ж таке співпадіння не спостерігається, то робиться висновок, що в роботі обладнання виникла проблема невідповідності.

Набагато більш складні методи та процедури тестування використовуються для тестування відповідності ТЛК-протоколів заданим специфікаціям. У цьому випадку, зокрема, застосовуються методи так званого абстрактного тестування. Теорія побудови та практика використання абстрактних тестів детально висвітлена у книзі О.Б. Іванова „Контроль соответствия в телекоммуникациях и связи» (М.: Компания Сайрус Системс, 2001). Основні положення теорії абстрактного тестування викладено у матеріалі самостійного заняття до цієї лекції. Конкретні процедури тестування, що базуються на використанні теорії абстрактного тестування, розглянуті у наступній лекції №10.

9.3. Основні засоби контролю

Спеціалізоване програмне забезпечення (ПЗ) або апаратні пристрої, що використовуються для вирішення задач контролю

(наприклад, вимірювальний прилад для визначення поточних значень фізичної величини або аналізатор перевірки коректності виконання протоколу тощо), відносяться до інструментальних засобів контролю. Інструментальний засіб контролю, як правило, являє собою перетворювач певних параметрів фізичних досліджуваних процесів, що характеризують об'єкт контролю, в інформаційні сигнали, зручні для сприймання контролюючою особою (із числа експлуатаційного персоналу) або автоматизованим контролюючим процесом. Отже, у складі засобу контролю маємо два основних інтерфейси: вхідний (інструментальний) інтерфейс, через котрий цей засіб приєднується до об'єкту контролю, та вихідний (користувацький) інтерфейс, через котрий результати контролю надаються особі або процесу - користувачеві цього засобу. Ефективність інструмента зазвичай характеризується функцією перетворення вхідної фізичної величини у вихідну фізичну величину, яка може бути відградуйована та представлена у зручній для сприймання формі. Наприклад, функція перетворення ометра може мати в якості вихідної величини кут повороту стрілки засобу контролю або цифрову індикацію виміряних значень величини електричного опору.

На рис.9.2 схематично відображена послідовність перетворень певної фізичної вимірюваної величини у типовому вимірювальному приладі, котра не залежить від природи цієї величини.

Як бачимо на рис.9.2, сучасні вимірювальні прилади реалізують цифрову обробку даних навіть у випадках, коли за їхньої допомоги здійснюють вимірювання аналогових величин. У безпосередньому контакті із об'єктом контролю знаходиться вимірювальний перетворювач (у випадках, коли вимірювана фізична величина має електричну природу – напруга, індуктивність, електрична ємність, опір і т. ін.) або електричний давальник, що перетворює у певній точно визначеній пропорції вимірювану величину фізичного параметра у відповідний цій величині електричний сигнал. Таким чином, вихід давальника – це зазвичай напруга, електричний опір або струм, що є пропорційними характеристиці вимірюваної величини. Для забезпечення такої пропорційності давальник має

задовольняти наступні дві вимоги:

1) повинен майже не впливати на контрольований об'єкт, тобто енергія, що відбирається давальником від об'єкта, має бути мінімально можливою, інакше контроль може виявитися некоректним;

2) повинен бути чутливим, по можливості, лише до вимірюваного параметру і не сприймати інші впливи, зокрема бути термостабільним.

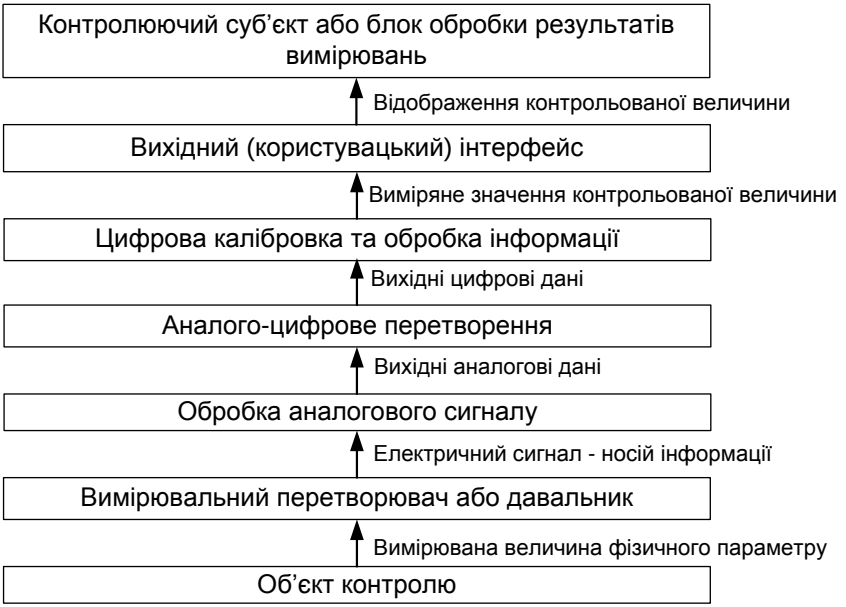


Рис.9.2. Послідовність перетворень вимірюваної величини у вимірювальному приладі (знизу уверх)

Функцію цифрової обробки вимірюваного сигналу, що надходить від аналого-цифрового перетворювача (АЦП), виконують за допомогою одного або кількох мікропроцесорів з метою:

1) виділення необхідної інформації із оброблюваного сигналу;

2) перетворення даних у необхідну форму, наприклад конвертування даних із часової форми представлення у частотну

шляхом перетворення Фур'є;

3) співставлення оброблюваної інформації з певною еталонною інформацією;

4) форматування даних, що надаються через вихідний інтерфейс.

Суттєвою проблемою при користуванні засобами контролю є визначення їхньої точності. Якщо параметри міри еталону та вимірювального засібу не співпадають або у ланцюгу обробки вимірюваного сигналу спостерігаються нелінійні явища, то можуть виникнути так звані **систематичні помилки** (погрішності) приладу. Такого роду помилки можуть бути нейтралізовані шляхом використання так званого **методу калібровки**. Зокрема, калібровка може полягати у тому, що від отриманого результату вимірювання віднімають попередньо обраховане зміщення, яке враховує систематичну погрішність вимірювального приладу. Зрозуміло, що у цьому випадку необхідно знати природу виникнення систематичних помилок і вміти здійснювати обчислення їхньої величини. На жаль, окрім систематичних, під час вимірювань можуть виникнути і **випадкові помилки**, які внаслідок їхньої стохастичної природи з теоретичної точки зору повністю усунути не є можливим. Для мінімізації випадкових помилок застосовують статистичну обробку результатів багатократних вимірювань. Зрозуміло, що у цьому випадку необхідно знати природу виникнення випадкових помилок і вміти будувати функції їхнього розподілу. Коли усі механізми систематичних та випадкових помилок виявлені та нейтралізовані, помилки, що залишилися, якраз і визначають **остаточну погрішність** вимірювального приладу.

На рис.9.3 надано типову структурну схему сучасного вимірювального засобу, де основні компоненти цього засобу являють певні апаратні блоки, що здійснюють перетворення сигналів та даних згідно з рис.9.2.

Сучасна практика свідчить, що для вирішення багатьох задач контролю необхідно комплексувати вимірювальні пристрої у комп'ютеризовані вимірювальні комплекси, що здатні виконувати великі обсяги обчислень під час обробки сигналів в комп'ютері та забезпечувати режим контролю віддалених об'єктів. Використання

великої кількості інструментальних приладів, що приєднані до одного комп'ютера, дозволяє мінімізувати витрати на проведення вимірювань та створити механізм централізованого контролю та обробки даних. Для обробки особливо великих обсягів даних створюють локальні вимірювальні мережі, що складаються із декількох комп'ютерів. Ці комп'ютери можуть функціонувати у паралельному режимі, вирішуючи одну задачу, або вирішувати функціонально різні завдання.

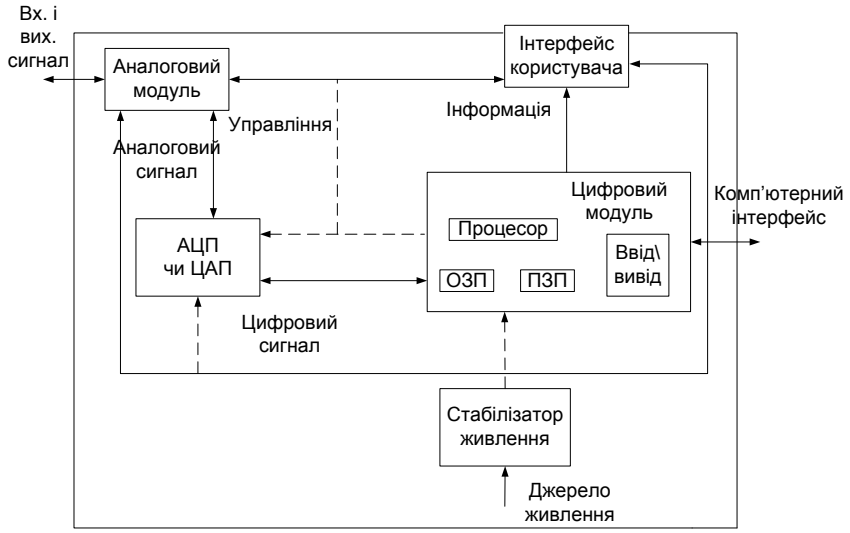


Рис.9.3. Типова структурна схема вимірювального засобу

Під час здійснення контролю розрізняють:

- режим не реального часу, коли вимірювання параметрів контрольованих об'єктів триває стільки, скільки є необхідним для вирішення експлуатаційного завдання;

- режим „м'якого" реального часу, коли для отримання корисного результату експлуатаційне завдання має бути виконано за допомогою засобів контролю до наперед визначеного часу;

- режим „жорсткого" реального часу, коли результат роботи системи контролю вважається неправильним, якщо воно не виконано протягом наперед заданого проміжку часу.

На рис.9.4 показана типова структура системи контролю, що функціонує у режимі реального часу.

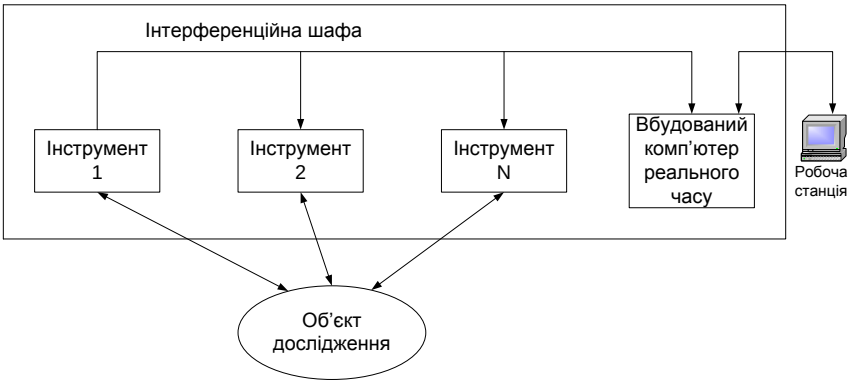


Рис.9.4. Типова структура системи контролю реального часу

Вбудований у систему контроля комп'ютер здійснює у реальному часі функції управління окремими пристроями, що входять до складу цієї системи, та обробки результатів вимірювань. Цей комп'ютер взаємодіє із пристроями через внутрішню інтерфейсну шину, у той час як інший інтерфейс використовується для взаємодії із зовнішним комп'ютером адміністратора системи контролю.

Контрольні питання до дев'ятої лекції

1. Чим процедури вимірювань відрізняються від процедур аналізу?
2. Назвіть п'ять видів задач, що складають функціональну групу задач підтримки працездатності ТЛК- обладнання.
3. Надайте характеристику помилкам вимірювань.
4. Надайте характеристику процедурам аналізу.
5. Надайте характеристику процедурам аналізу телекомунікаційних протоколів.
6. У яких випадках використовують процедури тестування?
7. Чим відрізняється поняття «збій» від поняття «відмова»?
8. Надайте визначення процедурі тестування.
9. Що таке погрішність тестування?

10. Які види процедур тестування Ви знаєте?

11. Надайте характеристику процедурам моніторингу.

12. Поясніть граф, що відображає взаємозв'язок процедур та задач підтримки працездатності ТЛК- обладнання.

13. Надайте характеристику трьом основним групам методів вимірювання фізичних величин.

14. Що таке метод аналізу?

15. Поясніть узагальнену схему проведення тестування.

16. Надайте характеристику інструментальним засобам контролю.

17. Назвіть послідовність перетворень вимірюваної величини у вимірювальному приладі.

18. Які характеристики точності вимірювальних приладів Ви знаєте?

19. Поясніть типову структурну схему сучасного вимірювального засобу.

20. Чим відрізняється режим „м'якого" реального часу від режиму «жорсткого» реального часу?

Література до дев'ятої лекції

1) А.Б.Иванов. Контроль соответствия в телекоммуникациях и связи. –М.: Компания Сайрус Системс, 2001.

САМОСТІЙНЕ ЗАНЯТТЯ ЗА МАТЕРІАЛАМИ ЛЕКЦІЇ №9 . ТЕСТУВАННЯ ВЗАЄМОДІЇ ВІДКРИТИХ СИСТЕМ

Теорія тестування інформаційної взаємодії відкритих систем, у т. ч. і через канали зв'язку, висвітлена у книзі О.Б. Іванова „Контроль соответствия в телекоммуникациях и связи» (М.: Компания Сайрус Системс, 2001). Згідно цієї теорії для тестування інформаційної взаємодії відкритих систем пропонується застосовувати методи так званого абстрактного тестування. Щоб реалізувати ці методи на практиці, необхідно уміти аналізувати характеристики телекомунікаційних протоколів з використанням так званих бланків *PICS*. Наступний матеріал присвячено побудові бланків *PICS* та способу їх використання при розробці специфікацій ТЛК - протоколів. Конкретні процедури тестування,

що реалізують специфікації, при створенні яких були використані бланки *PICS*, розглянуті у лекції №10.

PICS – це формальне відображення повної специфікації телекомунікаційного протоколу. На стадії експлуатації ТЛК - обладнання *PICS* використовуються для аналізу:

- можливостей наборів стандартизованих тестів, які входять до штатних компонентів ТЛК-обладнання МПД, з метою використання цих можливостей в процесі ТЕ обладнання;
- особливостей взаємодії обладнання різних постачальників обладнання;
- особливостей використання обладнання, яке реалізує не стандартизовані на рівні міжнародних стандартів та (або) рекомендацій телекомунікаційні протоколи (наприклад, так звані "фірмові" протоколи).

Бланк PICS являє собою набір питань, структурований таким чином, щоб надати можливість розробникові протоколу шляхом надання відповідей на ці питання однозначно визначити і зафіксувати повні специфікації протоколу з метою його стандартизації. Інформація, яка міститься у бланку PICS, має однозначно визначати на формальному рівні усі характеристики та параметри розроблюваного протоколу.

Бланк *PICS* використовується також, коли виникає необхідність задокументувати процес виконання протоколу з метою отримання гарантій, що структура тестової послідовності відповідає дозволеній.

Якщо аналізований протокол є стандартизованим на рівні МСЕ-Т (*ITU-T*), то вже заповнений бланк *PICS* обов'язково міститься в окремому розділі відповідної Рекомендації *ITU-T* або Міжнародного стандарту щодо цього протоколу.

Якщо аналізований протокол не є стандартизований на рівні *ITU-T*, то заповнений бланк *PICS* має надаватися постачальником обладнання, що реалізує цей протокол.

Якщо персонал оператора електрозв'язку має намір використати протокол власної розробки (зокрема, адаптувати певний стандартизований протокол до умов діяльності цього оператора), то для цього протоколу необхідно розробити відповідний бланк *PICS* (зокрема, відкоригувати існуючий бланк *PICS*

стандартизованого протоколу).

Коло питань, які відображаються у бланку *PICS*, за змістом охоплюють усі функції, елементи процедур, параметри, опції, *PDU*, часові відліки (тайм-аути), багаторівневі залежності, обмеження та інші характеристики, що визначені у специфікації протоколу. Зокрема, визначаються усі конкретні послідовності *PDU*, які мають просуватися між вузлами мережі, специфікується реакція протоколу на усі правильно і неправильно отримані *PDU*-послідовності, характеризуються опції підтримки приймання/ передавання *PDU* для протоколів без встановлення з'єднання або початку/кінця сеансів зв'язку для протоколів із встановленням з'єднання і т. ін.

Бланк *PICS* має складатися таким чином, щоб специфікація протоколу, яка відображається у *PICS*, містила у собі вимоги відповідності за статикою (у т.ч., і для багаторівневих залежностей) та динамікою.

Бланк *PICS* має однозначно визначати дозволений специфікацією спосіб виконання протоколу і детально відображати у табличній формі:

- затверджений діапазон варіацій глобальних параметрів в процесі виконання визначених функцій протоколу;
- опції протоколу, що доповнюють ті опції, які є обов'язковими для виконання.

У вхідній частині бланку *PICS* визначається статус кожної функції протоколу. Статус функції може бути:

- обов'язковим, коли ця можливість запитується для виконання у відповідності із специфікацією протоколу;
- вибірковим, коли функціональна можливість за певних умов може бути виконувана, і якщо вона виконується, то повинна відповідати специфікації протоколу;
- забороненим, коли існує вимога не застосовувати дану можливість у запропонованому контексті;
- не застосовуваним, коли ні одна із вимог не може бути відображена у запропонованому контексті;
- умовним, коли вимога залежить від вибору інших вибіркових або умовних одиниць.

Бланк *PICS* не може встановити раніш визначений статус для

певної можливості протоколу, він тільки може показати, що цей статус (обов'язковий, за вибором, заборонений або не застосовуваний) залежить від оцінки твердження або від умовного виразу.

Уведення у бланк PICS має поле для запису настанов постачальника елементу обладнання (*IUT*) відносно забезпечення можливостей виконання протоколів у вигляді:

- можливості виконання;
- неможливості виконання;
- інших категорій підтримки, що відносяться до протоколу.

Якщо вимоги відповідності за динамікою не забезпечують вичерпне визначення правил виконання, то в основну частину специфікації протоколу вносяться додаткові правила. У випадку, коли та чи інша можливість протоколу не підтримується, то це відображається у бланку.

В уведенні встановлюються процедури, які слід провести під час визначення відповідності за статикою, в той час як у самому бланку *PICS* визначаються додаткові спеціальні процедури, які необхідно провести під час визначення відповідності за статикою.

Бланки *PICS* представляються у наступній формі:

Перший розділ PICS (***Ідентифікація виконання***) установлює:

- процес виконання і систему, до якої він належить;
- постачальника системи;
- контактну особу на випадок виникнення якихось питань щодо змісту *PICS*.

Другий розділ (Ідентифікація протоколу) визначає Рекомендацію *CCITT* або Міжнародний стандарт, до яких може бути застосований бланк *PICS*.

Інші розділи (Характеристики) містять опис можливостей протоколу та його інформаційних параметрів. Зокрема, можуть бути відображені такі питання:

Характеристика виклик / відповідь. *У*ведення у бланк *PICS* може бути використане для визначення імовірності початку зв'язку певним процесом виконання та (або) форм реагування на зв'язок, ініційований іншою системою. Може бути показаний спосіб організації бланків *PICS* для відображення вищезазначеного (наприклад, у вигляді двох сукупностей стовпчиків у таблиці чи

двох сукупностей таблиць).

Основні можливості. Бланк *PICS* має вступну частину для кожної основної можливості. При цьому усі функціональні можливості протоколу розподіляються на великі «блоки» процесів виконання (тобто функціональні набори, сервісні класи, сервісні елементи, класи протоколів тощо). Для кожного такого «блоку» надається статус відповідності можливості і забезпечується місце для надання розпоряджень щодо підтримки виконавця. Ці визначення включаються в окремі розділи бланка *PICS*, за винятком випадку, коли протокол містить тільки один подібний «блок».

У бланку *PICS* не відтворюються вимоги відповідності за динамікою для кожної основної характеристики, припускаючи, що основна можливість буде реалізована у всій своїй повноті. Виключення з цього правила повинні мати технічне обґрунтування.

Часові відліки (Таймери) і параметри протоколу. Уведення у бланк *PICS* використовується для перерахування всіх часових характеристик і параметрів протоколу, визначених у специфікації протоколу зокрема дозволені чи обов'язкові тривалості. Типи даних і значення (чи області значень) специфікуються для кожного параметра протоколу. Надається місце для специфікації елементів чи значень, що підтримуються.

Протокольні блоки даних (PDU). Для ідентифікації підтримки *PDU* в уведення включено перелік усіх визначених для протоколу *PDU*, які групуються відповідно до їхніх основних можливостей. При цьому пункт відповідності може надавати чи не надавати інформацію з вибіркового статусу елементів окремого протоколу. У деяких протоколах статус певних елементів протоколу знаходиться в основній частині специфікації (вимоги відповідності за динамікою), а в інших протоколах вони включені у пункт відповідності.

Параметри PDU. Уведення у бланк *PICS* може бути використане для перерахування (для кожного типу *PDU*) параметрів, для яких існують різні можливості процесу виконання. При цьому бланк *PICS* повинен представляти кожний задокументований параметр, який визначається:

- статусом, заснованим на встановленні кожного напрямку у

вигляді відсилання/одержання;

- простором, для визначення того, підтримується чи ні даний параметр по кожному з напрямків;

- областями значень та (або) типами інформації, дозволеними в кожному з напрямків відповідним протоколом чи специфікацією передачі синтаксису.

Характеристики погоджень. Уведення у бланк може бути використано і для опису опцій узгодження, що містяться в протоколі, а також для вказівки на ті опції, що були виконані.

Обробка помилок протоколу. Якщо специфікація протоколу дозволяє реалізацію більше одного методу обробки помилок, то уведення у бланк *PICS* може бути використане для перерахування суті даних методів і для вказівки на методи, що підтримуються.

Багаторівневі залежності. У разі необхідності уведення у бланк *PICS* використовується для встановлення підтримки виконання спеціальних вимог до базових рівнів, що не визначені як обов'язкові специфікаціями протоколу базового рівня.

Інші умови. Якщо існує складна взаємодія між опціями, яку необхідно перевірити при визначенні відповідності за статикою, і опціями, що не можуть бути зв'язані з окремим уведенням у бланк *PICS*, така взаємодія відображається в окремому розділі у формі булевих позначень чи таблиць.

Контрольні питання до самостійного заняття дев’ятої лекції

1. Що таке *PICS*?
2. Що таке бланк *PICS*?
3. Для чого використовують бланк *PICS*?
4. Яке коло питань відображають у бланку *PICS*?
5. Що відображають в уведенні у бланк *PICS*?
6. Які характеристики протоколу установлюються у розділах бланку *PICS*?

Література до самостійного заняття дев’ятої лекції

1) А.Б.Иванов. Контроль соответствия в телекоммуникациях и связи. –М.: Компания Сайрус Системс, 2001.

ЛЕКЦІЯ №10. ОЦІНЮВАННЯ СТАНУ ОБЛАДНАННЯ. ВИРІШЕННЯ ПРОБЛЕМ НЕВІДПОВІДНОСТІ

Розглядаються наступні питання:

Лекційне заняття

10.1. Контроль відповідності параметрів обладнання
10.2. Поточний профілактичний контроль
10.3. Тестування відповідності
10.4. Аналіз телекомунікаційних протоколів

Самостійне заняття. **Аналіз протоколів систем сигналізації**

10.5. Загальна характеристика систем сигналізації
10.6. Аналіз протоколів систем абонентської сигналізації
10.7. Аналіз протоколів систем міжстанційної сигналізації

10.1. Контроль відповідності параметрів обладнання

Визначення поняття «Контроль відповідності». Експлуатаційний персонал має здійснювати взаємо узгоджений комплекс організаційно-технічних заходів, що називається "контроль відповідності".

Контроль відповідності будемо розглядати як одну із основних груп потоків процесів експлуатації ТЛК-обладнання, змістом якого є визначення (оцінювання) ступеню узгодженості параметрів та характеристик стану елементів обладнання або технологічних процесів, які ними здійснюються, із унормованими значеннями цих параметрів та унормованими специфікаціями цих характеристик, що вказані:

- у ДСТУ або НД профільного міністерства (або державного комітету) у галузі електрозв'язку;
- у штатній або супроводжувальній технічній документації, яка містить вимоги до параметрів та характеристик стану елементів і фрагментів обладнання або технологічних процесів, що підлягають контролю, за умов, коли відповідних вимог щодо потрібних значень контрольованих параметрів або унормованих специфікацій характеристик об'єктів контролю у чинних НД України не існує;
- у міжнародних базових та функціональних стандартах і профілях впливових міжнародних організацій в галузі телекомунікацій, таких як МСЕ-Т (*ITU-T*), *ISO*, *FR*-форум, *ATM*-

форум тощо за умов, коли відповідних вказівок ні в НД України, ні в супроводжувальний та (або) штатній технічній документації щодо контрольованих елементів чи технологічних процесів не існує.

З метою підвищення точності відображення правил експлуатації обладнання уточнимо поняття “параметр” та “характеристика”. Поняття “параметр” будемо відносити до вимірюваних величин. Параметр може мати певний діапазон значень величин, що визначаються на кількісному рівні. Поняття “характеристика” будемо пов’язувати з певним елементом логічної структури об’єкту, що характеризується – технологічного процесу або телекомунікаційного протоколу. Характеристики об’єктів будемо відображати за допомогою специфікацій.

Мета організації процесів контролю відповідності - отримати відповіді на питання, чи знаходиться обладнання або певна частина цього обладнання у працездатному стані, чи у повній мірі ресурси обладнання використовуються для надання послуг клієнтам, чи функціонує воно відповідно до вимог документів, які регламентують потоки процесів технічної експлуатації (ТЕ), і чи здатне це обладнання до коректної взаємодії з іншими частинами телекомунікаційної системи.

Документи, які регламентують контроль відповідності:

1) технічні паспорти, формуляри та технічні умови на обладнання, що експлуатується;

2) дані паспортизації фізичних ліній, каналів зв’язку та трактів, що знаходяться у користуванні;

3) регламенти та інструкції з експлуатації обладнання;

4) комплекти штатної експлуатаційно-технічної документації;

5) документи на поставку іноземного обладнання, у т.ч. контрактні умови;

6) внутрішньо корпоративні організаційно-технічні документи оператора електрозв’язку з питань експлуатації ТЛК-обладнання;

7) вітчизняні, міждержавні та міжнародні нормативні документи (НД) – ДСТУ, КНДУ, НД галузевого міністерства, міждержавні стандарти (головним чином, України та Російської Федерації), міжнародні стандарти та рекомендації *ISO*, МСЕ-Т,

ANSI, ETSI та ін., що стосується напрямку телекомунікацій та захисту інформації;

8) проектна документація на ТЛК-систему та її фрагменти.

Вимоги (норми) до специфікацій характеристик або значень параметрів, на відповідність котрим здійснюють контроль стану обладнання, будемо поділяти на:

- **обов'язкові**, що мають виконуватися без будь-яких виключень;
- **умовні,** що мають виконуватися при певних умовах, які визначені у відповідних специфікаціях контрольованих характеристик стану обладнання та режимів його функціонування;
- **додаткові**, що, можливо, і не нормуються у визначених документах, але контролюються експлуатаційним персоналом оператора електрозв'язку у рамках прийнятої ним політики ТЕ.

За функціональною ознакою вимоги (норми) підрозділяють на дві групи (згідно з рекомендаціями МСЕ-Т X.290 – X.296):

- **вимоги відповідності за статикою** (за цими вимогами здійснюється функціональний контроль обладнання);
- **вимоги відповідності за динамікою** (за цими вимогами здійснюється контроль взаємодії елементів обладнання).

Вимоги відповідності за статикою визначають сукупність припустимих функціональних характеристик елемента обладнання, який підлягає контролю. Цей контрольований елемент обладнання позначають як *IUT – Implementation Under Test*, в той час як усе контрольоване обладнання позначають як *SUT – System Under Test*. Вимоги відповідності за статикою являють собою мінімально припустимий набір контрольованих параметрів та специфікацій, який у змозі забезпечити процес функціонування обладнання. Наприклад, вимоги за статикою визначають мінімальний набір функцій певного протоколу, які мають бути перевірені шляхом його тестування в процесі аналізу коректності реалізації контрольованого протоколу на *N*-му та (*N-1*)-му рівнях семирівневої моделі *OSI*.

Вимоги відповідності за динамікою визначають сукупність припустимих режимів та процесів взаємодії елементів реальної системи, які підлягають контролю, і являють собою найбільш повний набір параметрів та характеристик контрольованих

елементів, що повністю визначають процес їхнього коректного функціонування. Наприклад, вимоги за динамікою можуть задавати вичерпні специфікації телекомунікаційного протоколу – умови його використання, формат протокольного блоку даних (*PDU*), перехідні стани, правила встановлення з'єднань тощо.

Виходячи із вищезазначеного, можливо стверджувати, що відповідне обладнання *SUT* – це таке обладнання, яке задовольняє вимогам відповідності і за статикою і за динамікою для всієї визначеної сукупності *IUT* і протоколів їхньої взаємодії.

Показники відповідності для ТЛК-обладнання стосовно канального та мережного рівнів моделі *OSI* у НД України наразі не унормовані. Тому деякі оператори електрозв'язку ці показники визначають окремо для кожної телекомунікаційної технології, що ними використовується, шляхом конкретизації узагальнених мережних характеристик, які наведені у табл.10.1 у розрізі фаз встановлення/розривання з'єднань. Множина цих узагальнених характеристик структурована згідно із рекомендацією МСЕ-Т *X.140*, а також із урахуванням положень, що визначені у рекомендаціях МСЕ-Т *E.430* та *E.800.*

Таблиця 10.1

Узагальнені мережні характеристики, що використовуються операторами електрозв'язку для визначення показників контролю відповідності

Фази з'єднань:	Узагальнені мережні характеристики:		
	характеристики швидкості	характеристики точності	характеристики гарантованості
фаза встанов-лення з'єднання	затримка в установленні з'єднання	імовірність організації помилкового з'єднання	імовірність відмови в установленні з'єднання
фаза передачі даних	1) швидкість передачі даних; 2) затримка у доставці даних	3) імовірність виникнення помилок в даних; 4) імовірність отримання зайвих даних; 5) імовірність не точного з'єднання	імовірність втрати даних

фаза розриву з'єднання	затримка у звільненні мережного з'єднання	імовірність відмови у роз'єднанні

Шляхи реалізації контролю відповідності. Контроль відповідності здійснюється шляхом реалізації наперед визначених комбінацій процедур вимірювань, аналізу, тестування та моніторингу об'єктів контролю (див. рис.9.1). Конкретне визначення цих процедур у процесах контролю стану ТЛК-обладнання має міститися у відповідних документах - інструкціях, методиках та (або) регламентах ТО елементів та фрагментів обладнання. Ці документи у сукупності становлять внутрішньо корпоративну базу нормативно-технічної документації (НТД), що регламентує процеси ТЕ оператора електрозв'язку.

Методи та умови проведення контролю відповідності обладнання мають враховувати:

- можливий гетерогенний (неоднорідний) характер мереж, де використовується ТЛК-обладнання, тобто той факт, що мережне обладнання може функціонувати із використанням не одного, а кількох стеків телекомунікаційних протоколів, які, в свою чергу, реалізують багаторівневі моделі взаємодії мережних елементів, як правило, за ідеологією відкритих інформаційних систем;
- можливий нерегулярний характер топологічної схеми розташування вузлів ТЛК-мережі та характеристик потоків інформації як від абонентів, так і за напрямками встановлених з'єднань;
- можливий мультисервісний характер надання послуг з використанням ресурсів ТЛК-обладнання;
- можливість використання обладнання різних постачальників, котрі, зокрема, не у повній мірі додержуються стандартів та рекомендацій впливових міжнародних організацій у сфері телекомунікацій, тим більш національних стандартів України.

Кадрове забезпечення контролю відповідності. Контроль відповідності здійснюється з урахуванням існуючої ієрархічної структури кадрового забезпечення експлуатаційних робіт, а також функціональної структури вузлів мереж та каналів передачі даних. Якщо реалізована схема централізованого керування ТЛК-

мережею, то контроль відповідності здійснюється адміністраторами вузлу централізованого керування. У випадку децентралізованого керування контроль відповідності виконується силами персоналу вузлів ТЛК-мережі.

За ступенем автоматизації розрізняють наступні можливі режими виконання контролю:

- ручний, що здійснюється тільки безпосередньо технічним персоналом;
- автоматизований за умов часткової участі персоналу;
- автоматичний, повністю без участі персоналу.

В залежності від режимів роботи обладнання контроль виконується:

- без зупинки в наданні послуг користувачам (у так званому фоновому режимі контролю);
- з частковими обмеженнями в обслуговуванні користувачів;
- з перервами у наданні послуг.

За часовою координатою розрізняють і використовують на практиці наступні види контролю:

- поточний безперервний (у фоновому режимі);
- планово-періодичний;
- позачерговий.

Поточний профілактичний контроль здійснюється персоналом регулярно без зупинок в наданні послуг користувачам шляхом відтворення постійно активізованих процедур контролю на фоні роботи обладнання за основним призначенням і за умов, коли контрольоване обладнання виконує свої функції нормально і відсутні будь-які ознаки змін у його стані

Планово-періодичний контроль виконується персоналом згідно із затвердженими графіками проведення експлуатаційних робіт відповідно до вимог документів, що регламентують процеси ТО контрольованого обладнання.

Позачерговий контроль проводиться персоналом у разі виникнення проблем у процесі експлуатації контрольованого обладнання (у т.ч., і під час переконфігурування цього обладнання), проведення позачергових перевірок стану обладнання з ініціативи керівництва оператора електрозв'язку або уповноважених органів, отримання обгрунтованих заявок-прохань

з боку користувачів на виконання позачергового контролю.

При цьому слід зауважити, що ми не розглядаємо процедури здійснення інсталяційного контролю, який проводиться під час первісного налагоджування обладнання мереж або в період приймально-здавальних випробувань. Правила виконання інсталяційного контролю не регламентується експлуатаційними документами. А стресовий контроль на стадії експлуатації ТЛК-обладнання, зазвичай, не проводиться.

Вибір співвідношення вищезазначених видів контролю в конкретних умовах експлуатації ТЛК-обладнання залежить від багатьох чинників (зокрема, від характеристик обладнання, топології мережі, набору надаваних послуг, рівнів попиту на ці послуги тощо). Зазвичай це співвідношення визначається виходячи із прагнень мінімізувати вартість ТЕ, забезпечивши при цьому необхідні номенклатуру та рівень якості надаваних користувачам телекомунікаційних послуг. У будь-яких випадках персонал повинен забезпечити можливість контролю стану обладнання вузлів та міжвузлових з'єднань усіх рівнів ієрархічної структури ТЛК-мереж, усіх типів абонентського доступу до магістральних мереж та Інтернет, а також контролю наскрізних характеристик обладнання мереж.

Вимоги до організації контролю відповідності. Контроль відповідності має бути організованим таким чином, щоб забезпечувати:

- повторюваність результатів контролю, тобто результат будь-якої процедури контролю в однакових умовах його проведення має бути незмінним незалежно від часу виконання цієї процедури;
- зіставимість (порівнювальність) результатів контролю незалежно від того, хто саме його здійснює – персонал оператора електрозв'язку, постачальника обладнання або незалежної організації, що здійснює сертифікацію (для забезпечення зіставимості необхідно, щоб існували однозначно визначені специфікації процедур контролю);
- доступність процедур та результатів контролю, тобто достатня ступінь деталізації задокументованої інформації щодо характеристик використання процедур контролю і результатів

контролю (у т. ч., інформації про всі вхідні/вихідні дані контролю, виниклі тестові події і т. ін.).

Умови здійснення процедур контролю (кліматичні, метрологічні, енергозабезпечення, безпеки тощо) мають відповідати наведеним у діючій експлуатаційно-технічній документації на штатне ТЛК-обладнання. Під діючою експлуатаційно-технічною документацією розуміють таку, що відповідним чином кодифікована, ідентифікована, зареєстрована і включена до множини об'єктів конфігураційного контролю середовища експлуатації ТЛК-системи.

Аналіз результатів контролю відповідності, як правило, здійснюється в наступних випадках:

- в період експлуатації ТЛК-обладнання за призначенням згідно із затвердженими графіками виконання експлуатаційних робіт відповідно до вимог документів, які регламентують експлуатаційні процеси у розрізі видів вузлів мереж та типів обладнання, яке на цих вузлах використовується;
- після проведення ремонту обладнання або профілактичних заходів ТО;
- під час планових або позачергових перевірок стану обладнання;
- при введенні (запуску) нового або модернізованого елемента або фрагмента ТЛК-системи в експлуатацію;
- за заявами користувачів.

За ступенем глибини (ретельності) здійснення контролю процеси контролю відповідності підрозділяють на:

1) поточний профілактичний контроль (визначення котрого надано вище);

2) тестування відповідності, яке виконується персоналом шляхом активізації на контрольованому обладнанні спеціалізованих програмних тестових засобів, що входять до комплекту поставок цього контрольованого обладнання;

3) аналіз протоколів, яке виконується персоналом за допомогою програмно-апаратних інструментальних засобів, що не входять до комплектів поставок контрольованого обладнання (головним чином, із використанням спеціальних пристроїв, що називають аналізаторами протоколів).

10.2. Поточний профілактичний контроль

Процес функціонування ТЛК-обладнання має знаходитися під постійним контролем експлуатаційного персоналу. Якщо контрольоване обладнання виконує свої функції нормально і відсутні зовнішні ознаки негативних змін у його стані, то під час поточного контролю достатньо обмежитися пасивним спостереженням у реальному часі за ходою функціонування обладнання шляхом аналізу інтегральних показників такого функціонування, які, як правило, відображаються на системних консолях центрів керування вузлами та (або) фрагментів мереж.

Сучасні системи управління та контролю у ТЛК-системах побудовані на основі схеми “агент/менеджер” з використанням для агрегації отриманих даних механізмів експертних систем і дозволяють забезпечити досить високу ступінь глибини контролю в автоматичному режимі роботи обладнання. Вбудовані засоби контролю на фоні роботи обладнання за основним призначенням здійснюють збір та первинну обробку необхідних даних для оцінки працездатності контрольованого обладнання, транспортування цієї інформації до центрів її структуризації та агрегації, інтелектуальну її обробку з метою виявлення невідповідностей в роботі задіяних телекомунікаційних протоколів та генерації тривожних сигналів. Зрозуміло, що правила прийняття рішень, які реалізуються автоматичними засобами контролю, є формалізованими. Вони не враховують тонку структуру умов виникнення невідповідностей в роботі обладнання і тому поступаються за глибиною аналізу тестуванню відповідності або аналізу за допомогою аналізаторів протоколів. Тому в процесі поточного контролю існує необхідність в постійному експрес-аналізі поточного стану обладнання з боку експлуатаційного персоналу. Такий експрес-аналіз виконується на основі інтегральних характеристик функціонування обладнання, які надаються персоналу засобами вбудованого контролю.

Поточний профілактичний контроль – це, як правило, пасивний контроль, який виконується у фоновому режимі шляхом спостерігання за ходою функціонування обладнання без здійснення будь-яких змін в його структурі (тобто, без проведення переключень, перекомутацій, переконфігурацій, змін у режимах роботи, генерації додаткових сигналів тощо).

Поточний контроль здійснюється штатними засобами контролю, які, як правило, інстальовані у складі штатних підсистем керування контрольованим обладнанням та (або) у складі централізованих систем керування мережами. Поточний контроль забезпечує базовий (тобто, найменший) рівень глибини контролю і потребує найменшу кількість ресурсів для його здійснення. В процесі поточного контролю проводиться спостереження за відносно невеликою кількістю контрольованих параметрів та характеристик обладнання, які, як правило, мають інтегрований (узагальнюючий) характер.

10.3. Тестування відповідності

Більш високу ступінь глибини контролю (у порівнянні із поточним контролем) забезпечує так зване тестування відповідності. В процесі тестування відповідності використовується тільки штатне обладнання і штатні (головним чином, стандартизовані) тестові засоби, які відповідним чином зафіксовані у документах, що відображають комплекти поставок контрольованого обладнання. Тестування відповідності засновано на використанні активних методів контролю і забезпечує достатню для цілей експлуатації глибину контролю, але за умов, коли програмно-апаратні засоби здійснення тестування правильно інстальовані і знаходяться у працездатному стані, а самі тести є коректними і вичерпними.

Тестування відповідності розглядається як один із методів контролю стану обладнання і, головним чином, полягає в тестуванні відповідних протоколів канального рівня і вище. Реалізуються процедури активного контролю, коли в процесі тестування протоколів використовуються зовнішні впливи із наперед визначеними характеристиками.

В залежності від ступеню (глибини) контролю передбачають використання процедур тестування наступних чотирьох типів:

1) тестування характеристик (тобто, функціональне тестування) контрольованого елемента обладнання (*IUT*), коли перевіряється ствердження, що функціональні характеристики *IUT* задовольняють вимогам відповідності за статикою, які заявлені у спеціальному документі із нормуючими специфікаціями, що має

назву “звіт відповідності виконання протоколу” (*PICS*);

Примітка 10.1. Технологія тестування із використанням бланку *PICS* визначена рекомендаціями МСЕ-Т *CCITT X.290-X.296*. Аналіз характеристик телекомунікаційних протоколів за бланками *PICS* наведений у матеріалах самостійного заняття до лекції №9.

2) базове тестування взаємодії контрольованого елемента обладнання (*IUT*), котре забезпечує доказ відповідності (*IUT*) у разі відсутності доказів протилежних стверджень;

3) тестування поведінки (тобто, більш глибоке тестування взаємодії), котре забезпечує вичерпне тестування в межах характеристик *IUT* у розрізі вимог тестування за динамікою;

4) оцінка порогу визначеності, котра дозволяє визначити стан контрольованого елемента обладнання відносно певних вимог відповідності, що є специфічними для конкретних, як правило, не стандартизованих реалізацій протоколів.

Політика ТЕ оператора електрозв’язку має передбачати постійне у часі циклічне базове тестування взаємодії всіх основних елементів обладнання ТЛК-системи на фоні його роботи за основним призначенням з метою підтвердження достатньої відповідності за умов, коли обладнання працює нормально і відсутні будь-які ознаки можливості змін у стані.

Базове тестування здійснюється за допомогою так званих базових тестів взаємодії (*BIT*). *BIT* не використовуються для знаходження причин ушкоджень в обладнанні в процесі його діагностики або ремонту.

У випадках, коли в рамках аналізу коректності реалізації певного телекомунікаційного протоколу необхідно виконати повну перевірку узгодженості між реальними функціональними характеристиками *IUT* і тими нормованими характеристиками, що внесені в бланк *PICS*, експлуатаційний персонал має здійснювати тестування на відповідність вимогам за статикою усіх функціональних характеристик *IUT*, які відображені у *PICS*. Процедури тестування функціональних характеристик основних елементів сучасного ТЛК-обладнання, здебільшого, є стандартизованими. Для них визначені стандартизовані абстрактні тестові послідовності (*ATS*).

У випадках, коли необхідно виконати перевірку узгодженості у

всьому діапазоні вимог відповідності за динамікою, здійснюють тестування так званої поведінки *IUT*, специфікації котрої відображені у *PICS*. Процедури тестування поведінки основних елементів сучасного ТЛК-обладнання також, здебільшого, є стандартизованими. Для них визначені стандартизовані *ATS*, а також так звані тести дійсної поведінки *IUT*, тобто стандартні реакції *IUT* у відповідь на дійсну і недійсну поведінку засобу тестування.

Функціональне тестування та тестування поведінки можуть виконуватись сумісно або у вигляді окремих груп тестів, але вони не можуть застосовуватися для вирішення виникаючих проблем, коли інші тести вказують на можливу невідповідність, навіть якщо результати тестування характеристик або поведінки виявились задовільними.

Експлуатаційний персонал має здійснювати функціональне тестування та тестування поведінки у випадках, що передбачені у попередньому підрозділі.

У випадках, коли стандартизовані процедури абстрактного тестування не у повній мірі охоплюють усі аспекти функціонування якогось *IUT*, експлуатаційний персонал має здійснювати оцінку порога визначеності цього *IUT*, тобто запускати на виконання залежні від структури *SUT* нестандартизовані тести, які мають доповнювати стандартизовані тести, що використовуються в процесі оцінки відповідності. При цьому методи тестування вибираються таким чином, щоб забезпечувалась можливість тестування тих аспектів оцінюваного *IUT* (зокрема, протоколу), які неможливо перевірити за допомогою стандартизованих *ATS*.

Оцінка порогу визначеності здійснюється для:

1) реалізації стандартизованих цілей тестування, коли через неможливість перевірки вимоги відповідності або обмеженість вибраного методу тестування задіяні процедури тестування не можуть бути включені в стандартизовану *ATS*;

2) отримання відповіді типу “так/ні” в чітко визначеній ситуації (наприклад, для з’ясування певних характеристик контрольованого процесу під час пошуку причин виниклих проблем і т. ін.);

3) дослідження проблем, що виникають в процесі виконання

стандартизованої *ATS*.

Але в будь-яких випадках отримана оцінка порогу визначеності не може бути використана в якості висновку про повну відповідність результатів тестування.

Процедура тестування *IUT* на відповідність вимогам нормуючих специфікацій здійснюється за схемою, що відображена на рис.10.1. Ця процедура реалізується головним чином під час планово-періодичного або позачергового контролю і полягає у послідовному виконанні наступних трьох етапів її здійснення:

1) підготовка до тестування;

2) проведення тестування;

3) підготовка звітів із результатами тестування.

В процесі підготовки до тестування необхідно:

- вибрати із множини можливих *IUT*, які моделюють *SUT*, для визначеного телекомунікаційного протоколу той елемент контрольованого обладнання, що має бути охоплений тестуванням у даному акті тестування;

- вибрати із множини штатних *PICS* або створити новий *PICS* шляхом формулювання відповідей на перелік питань, що відображені у стандартизованому бланку *PICS* (бланк *PICS* являє собою набір питань у формі запитувача або таблиці, пов'язаних із можливостями протоколу, які сформульовані у вигляді вимог відповідності за статикою та динамікою – див. матеріали самостійного заняття до лекції №9);

- виходячи із специфікацій вибраного *PICS* вибрати конкретний тест з метою подальшого його запуску в даному акті тестування (що фактично означає вибір методу абстрактного тестування та стандартизованої *ATS*);

- підготувати обладнання (тобто, *SUT*) та інструментальні засоби (як програмні, так і, можливо, апаратні) для тестування.

Щоб протестувати процес виконання телекомунікаційного протоколу з урахуванням специфічних особливостей функціонування ТЛК-системи в умовах діяльності оператора електрозв'язку, потрібна інформація щодо *IUT* та середовища тестування як додаток до інформації, яка відображена у *PICS*.

Рис.10.1 Процедура тестування *IUT* на відповідність вимогам нормуючих специфікацій

Ця додаткова інформація вноситься у бланк *PIXIT*, який після заповнення має містити інструкцію:

- котра уточнює дані , що відображені у *PICS* (наприклад, *PIXIT* може вказувати на конкретні значення певного параметра, діапазон значень якого заданий у *PICS*);
- котрі із характеристик, що заявлені у *PICS*, мають бути перевірені, а котрі – ні;
- про обладнання, що має бути охоплене тестуванням (наприклад, адресна інформація, інформація про засоби тестування верхнього рівня і т. ін.);
- необхідну для ідентифікації *IUT*, посилання на інші суміжні *PICS* тощо.

PIXIT повинна не суперечити *PICS*. Для кожної *ATS* має існувати лише один *PIXIT*.

Процес підготовки обладнання до тестування полягає, головним чином, у перевірці конфігурації обладнання, яке має дозволяти обмін протоколами між *SUT* і системою тестування.

В процесі проведення тестування послідовно виконуються наступні роботи:

1) параметризація вибраного тесту на основі вибраних або створених *PICS* та *PIXIT*, тобто отримання послідовності тестування з конкретно визначеними параметрами, яка називається *PETS*;

2) здійснення базового тестування взаємодії (в разі потреби);

3) здійснення функціонального тестування з метою визначення відповідності за статикою;

4) здійснення тестування поведінки з метою визначення відповідності за динамікою;

5) оцінка порогу визначеності (в разі потреби);

6) аналіз результатів тестування.

Процес тестування являє собою процес виконання *PETS* із фіксацією результатів проходження процедури тестування в документі, що має назву “паспорт відповідності”. Процес тестування може мати циклічний характер, тобто повторюватися (де)кілька разів.

Результат тестування являє собою відображення послідовності

подій, які мали місце в період виконання процедури тестування, і містить у собі всі вхідні і вихідні дані в точках управління та спостереження за *IUT*. Результат тестування може співпадати або відрізнятися від очікуваного, тобто події, що мали місце під час здійснення процедури тестування, можуть співпадати або не співпадати із подіями, визначеними у процедурі абстрактного тестування для реалізованої тестової послідовності.

Висновок щодо результату тестування може бути такий – "пройшов", "не пройшов" або "непереконливо".

"Пройшов" означає, що отриманий результат у даному циклі тестування *IUT* співпадає з очікуваним і, отже, відповідає вимогам відповідності.

"Не пройшов" означає, що отриманий результат у даному циклі тестування *IUT* або не відповідає вимогам відповідності (хоча б стосовно однієї вимоги), або містить хоча б одну недійсну подію відносно подій, які визначено в *ATS*, тобто містить неочікуваний результат тестування.

"Непереконливо" означає, що отриманий результат у даному циклі тестування *IUT* не дає можливість зробити ні один із двох вищезазначених висновків. В такій ситуації прийнято робити висновок, що отриманий результат відповідає вимогам відповідності.

Неочікуваний результат тестування, здебільшого, у вигляді помилки контрольного завдання фіксується у паспорті відповідності. Помилки можуть бути виявлені як у самій процедурі абстрактного тестування, так і в процедурі її параметризованої реалізації (тобто, після її прив'язки до конкретних умов застосування). У паспорті відповідності фіксується також можливе аномальне закінчення контрольного завдання, коли виконання процедури тестування передчасно зупинено внаслідок подій, які неможливо ідентифікувати як помилки контрольного завдання.

Звіт із результатами тестування має назву "звіт про тестування відповідності протоколу" (*PCTR*) або "звіт про тестування відповідності *IUT*".

У *PCTR* документуються усі результати задіяних процедур тестування *IUT*, дається посилання на паспорт відповідності, що містить отримані результати тестування, а також на всі інші

документи, які були пов'язані з процесом тестування – *PICS, PIXIT,* нормативну та експлуатаційну документацію.

PCTR підготовлюється для кожного протестованого *IUT*, які у сукупності відображають *SUT*. Ці *PCTR* є основою для підготовки узагальнюючого звіту про тестування *SUT*, який має мнемонічну назву *SCTR.*

Процедура тестування всього контрольованого обладнання (тобто, *SUT*) – це є послідовне виконання процедур тестування тих *IUT*, які у сукупності моделюють цю *SUT.*

Після здійснення процедури тестування *SUT* оформлюється *SCTR* , який являє собою документ із стислим оглядом результатів контролю відповідності *SUT*, в якому мають бути перераховані всі *PICS* та *PIXIT*, що були задіяні у даній процедурі.

10.4. Аналіз телекомунікаційних протоколів

Аналіз протоколів з використанням аналізаторів протоколів в принципі забезпечує таку ж ступінь глибини контролю відповідності, як і тестування відповідності, і здійснюється у тих випадках, коли є сумніви щодо коректності або вичерпності тестового забезпечення або працездатності штатних програмно-апаратних засобів здійснення тестування. Якщо аналіз певного протоколу за допомогою аналізатора протоколу засвідчує коректність його відтворення засобами контрольованого обладнання, а результати тестування відповідності цього протоколу дають протилежний результат, то це вказує на некоректність тестового забезпечення або програмно-апаратних засобів здійснення тестування. Аналізатори протоколів використовуються також для пасивного спостереження за трафіком та сигнальним обміном у точках їхнього підключення до елементів ТЛК-обладнання. Однак найбільш доцільною сферою використання процедур аналізу телекомунікаційних протоколів вважається пошук та локалізація проблем в експлуатації ТЛК-обладнання, особливо в задачах виявлення та усунення логічних конфліктів в роботі його програмного забезпечення (ПЗ).

ТЛК-протоколи бувають різні. Серед найбільш розповсюджених слід відзначити так звані транспортні протоколи, що призначені для передавання користувацької інформації на різних рівнях моделі

взаємодії інформаційних систем (маються на увазі транспортні протоколи фізичного, канального, мережного, сеансового і більш вищих рівнів - відповідно до семирівневої моделі *OSI ISO*), а також протоколи сигналізації, що, головним чином, забезпечують процедури встановлення/розривання сеансів зв'язку між користувачами ТЛК-систем або підтримують надання замовлених абонентами послуг під час встановлених сеансів зв'язку. В мережах *IP* знайшли широке використання протоколи маршрутизації, в мережах та окремих каналах керування – протоколи керування, у підсистемах захисту інформації – протоколи шифрування і т.ін. Проте усі ТЛК-протоколи з точки зору вибору методології їхнього аналізу мають багато спільних рис. Саме ці спільні риси у підходах до аналізу протоколів і є предметом викладу у подальшому матеріалі лекції.

Об'єктом вивчення під час аналізу протоколу є його траса. Як правило, до певним чином обраної точки аналізу на одному із інтерфейсів ТЛК-обладнання підключається аналізатор протоколу, що здатний із усієї суміші сигналів та (або) повідомлень, що проходять через обрану точку аналізу, відфільтрувати та зареєструвати саме ті сигнали та повідомлення, котрі складають трасу досліджуваного протоколу. Тобто, траса являє собою послідовний запис сигналів та (або) повідомлень протоколу, що проходять через певним чином обрану точку аналізу.

Примітка 10.2. Зрозуміло, що у багатьох випадках через ту ж саму точку аналізу можуть проходити повідомлення, які відносяться до різних телекомунікаційних протоколів. Щоб зафіксувати повідомлення якогось одного протоколу, необхідно до обраної точки аналізу підключити аналізатор, який має бути налагоджений на аналіз саме того протоколу, що являє у даний момент експлуатаційний інтерес. Існують універсальні багатопротокольні аналізатори, котрі можуть бути налаштовані на аналіз будь-якого протоколу із тієї множини протоколів, яку вони здатні проаналізувати.

Не завжди усі сигнали та повідомлення досліджуваного протоколу під час вирішення конкретного завдання на конкретному проміжку часу являють експлуатаційний інтерес. Як правило, перед початком аналізу протоколу експлуатаційний персонал вже має певні передбачення щодо характеру виниклої проблеми. Тому із всієї множини сигналів та повідомлень протоколу, що з'являються у точці аналізу, за допомогою засобів фільтрації та

декодування відбираються, декодуються та фіксуються на аналізаторі саме ті інформаційні елементи протоколу, що являють у даний момент експлуатаційний інтерес.

За ступенем деталізації інформації, що надається для аналізу протоколу, **розрізняють прості та деталізовані траси.**

Проста траса – це запис послідовності основних повідомлень досліджуваного протоколу із вказівкою часових моментів їх фіксації в аналізаторі. Проста траса не містить супутньої (допоміжної) інформації, яка б деталізувала опис процесу обміну даними, що здійснюється у рамках цього протоколу.

Деталізована траса – це послідовний запис не тільки основних повідомлень протоколу, але і більш/менш детальний опис усіх інформаційних полів та інформаційних елементів цих повідомлень.

На практиці широко використовуються як прості, так і деталізовані траси сигналізаційних протоколів, зокрема їхні комбінації. Наприклад, спочатку будують просту трасу, для того щоб визначити, чи взагалі був логічний конфлікт під час обміну сигналами досліджуваного протоколу. Для цього спочатку задаються певним проміжком часу, у рамках якого передбачається можливість виникнення логічного конфлікту. І саме на цьому часовому проміжку будують просту трасу, аналізуючи яку, намагаються: або виявити логічний конфлікт в структурі протокольного обміну даними, або виявити характер виниклої проблеми, або знайти у потоці повідомлень, що проходять через досліджувану точку аналізу, саме те повідомлення, яке являє експлуатаційний інтерес. Потім за результатами аналізу простої траси будують ту або іншу деталізовану трасу, за допомогою якої намагаються не тільки виявити характер проблеми, але і знайти місце та причини її виникнення.

Таким чином, локалізація точки логічного конфлікту пов’язана із визначенням зони траси, де ймовірно перебувають дані, що надають можливість визначити причину конфлікту. Для пошуку цієї зони використовується проста траса. Далі, після того, як більш/менш вузька ділянка простої траси, що представляє інтерес, визначена, доцільно саме для цієї вузької часової ділянки побудувати трасу проміжної або, навіть, повної деталізації. Дані більш деталізованих трас, що отримані на відносно вузькому

проміжку часу, можуть надати більш повне уявлення про причину виникнення логічного конфлікту, ніж дані простої траси. Проте навіть на обраній вузькій зоні проміжної або деталізованої траси може міститися достатньо великий обсяг надлишкових даних, що заважає усуненню проблемної ситуації. Тому для відокремлення корисної інформації від надлишкової під час аналізу деталізованої траси реалізують процедуру фільтрації – відсіювання повідомлень тих протоколів, інформаційних полів та інформаційних елементів, котрі не мають відношення до виниклої проблеми. Фільтрація може здійснюватися за різними ознаками – за рівнями протоколів (канальний рівень протоколів, мережний і т.д.), за конкретними видами протоколів у рамках обраного рівню протоколів (наприклад, у рамках мережних протоколів *TCP/IP* відфільтровуються повідомлення конкретного протоколу із множини *IP, TCP, ARP, ICMP, UDP, RARP*), за видами повідомлень або інформаційних елементів у рамках досліджуваного протоколу, за окремими параметрами цих елементів тощо. У будь-якому разі застосування фільтрів до деталізованих трас дозволяє зменшити обсяги наданої для аналізу інформації та отримати так звані траси проміжної деталізації, які за умови коректного їхнього використання є найбільш зручними для вирішення експлуатаційних завдань.

Існують так звані **бінарні деталізовані траси**, що забезпечують максимальну (побітову) деталізацію відображення процесу реалізації протоколу, та **інтерпретаційні траси**, що відображають лише частину інформації щодо протокольного процесу, але найбільш важливу в конкретних умовах його функціонування.

Типова схема пошуку точки та причини виникнення логічного конфлікту у класичній мережі передачі даних (МПД) показана на рис.10.2. Як бачимо на рис.10.2, спочатку на простій трасі, що побудована на достатньо широкому часовому інтервалі, шукають точку виникнення логічного конфлікту. Зрозуміло, що для цього потрібен певний рівень базових знань щодо структури протоколів, що входять до складу реалізованого в МПД стеку ТЛК-протоколів, та певні практичні навички користування задіяним аналізатором протоколів.

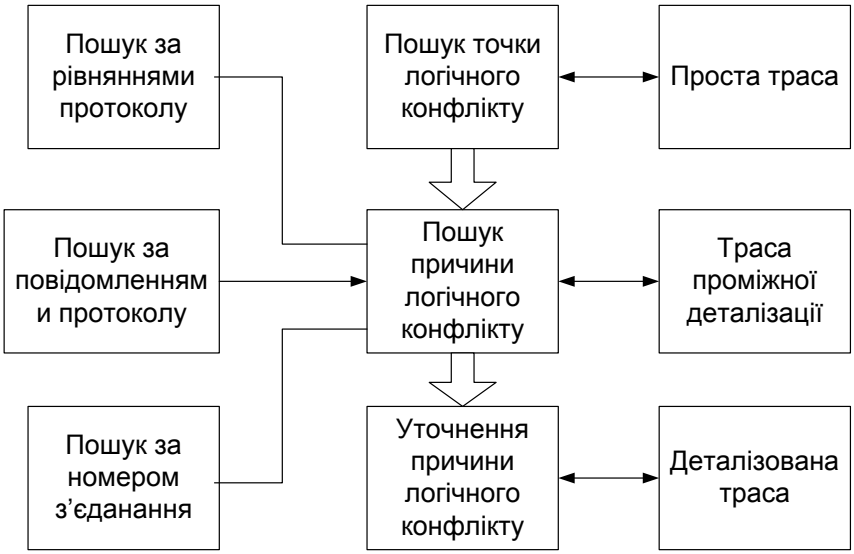


Рис.10.2. Порядок вирішення проблеми, що пов'язана із можливим виникненням логічного конфлікту в роботі ТЛК-обладнання

Після того, як така точка на простій трасі буде знайдена, будують інтерпретаційну трасу проміжної деталізації, що охоплює вузький часовий інтервал роботи мережі в зоні точки виникнення конфлікту. Шляхом поетапного фільтрування даних траси проміжної деталізації відбирають найбільш інформативні дані, на основі аналізу котрих висувають гіпотезу (припущення) щодо можливої причини виникнення логічного конфлікту. Зрозуміло, що для цього потрібні глибокі знання протоколів, щодо яких висувається гіпотеза. Накінець, для підтвердження (або спростування) висунутої гіпотези у точці логічного конфлікту будується деталізована траса, у рамках якої декодується уся необхідна для цього інформація.

Розрізняють пасивні та активні методи аналізу протоколів.

Пасивний метод аналізу протокола зазвичай зводиться до пасивного моніторингу повідомлень досліджуваного протоколу у заздалегідь обраній точці спостереження на одному із інтерфейсів ТЛК-обладнання без будь-якого активного втручання в роботу

цього обладнання. Для цього використовується так званий пасивний аналізатор протоколу, у складі котрого відсутні будь-які імітатори сигналів протоколу (пасивний аналізатор здатний лише перехоплювати сигнали та повідомлення досліджуваного протоколу з наступним їхнім декодуванням). Зазвичай пасивний аналізатор включають послідовно у розрив ланцюгів інтерфейсу (у точці спостереження), наприклад у розрив між пристроями *DTE* та *DCE* так, щоб усі потоки інформації цього інтерфейсу безпосередньо проходили через пасивний аналізатор. Інший спосіб включення пасивного аналізатора передбачає застосування так званого *Y*-кабелю, що забезпечує високоомне паралельне підключення аналізатора до точки спостереження без порушень прямих з'єднань ланцюгів інтерфейсу. У цьому випадку впливом пасивного аналізатора на процес обміну сигналами через досліджуваний інтерфейс можливо знехтувати. Зрозуміло, що пасивні методи аналізу протоколів лише фіксують реальну картину обміну повідомленнями досліджуваного протоколу в обраній точці спостереження. Вони не дають змоги змоделювати ситуацію в точці аналізу, яка б дозволила створити умови (наприклад, шляхом імітації роботи тих чи інших елементів обладнання) для більш чіткого прояву наслідків ймовірної проблеми і, отже, для більш швидкої локалізації цієї проблеми або виявлення причин її виникнення. Більш ефективними у цьому плані слід вважати активні методи аналізу протоколів.

Активний метод аналізу протокола передбачає активне втручання аналізатора в роботу ТЛК-обладнання, зокрема шляхом заміщення сумнівного елемента або одразу кількох елементів на імітатор їхньої роботи в рамках досліджуваного протоколу. Для цього використовується так званий активний аналізатор протоколу, котрий має у своєму складі засоби імітації сигналів протоколу і, отже, здатний не тільки фіксувати та декодувати повідомлення протоколу, але і також моделювати роботу тих чи інших елементів ТЛК-обладнання, що впливають на роботу цього протоколу. Зазвичай активний аналізатор під'єднують до ланцюгів інтерфейсу (у точці спостереження) так, щоб мати можливість в процесі аналізу відключати від інтерфейсу (фізично або логічно) активні елементи ТЛК-обладнання, а замість них підключати імітатори цих

елементів. Зазвичай у цьому випадку моделюється ситуація, що є найбільш сприятливою для підтвердження або спростування гіпотези щодо виниклої проблеми в роботі досліджуваного протоколу.

Слід мати на увазі, що пасивні методи аналізу найбільш широко використовуються для розв'язання складних проблемних ситуацій, що виникають у складних багатопротокольних мережах, зокрема у глобальних мережах передачі даних, коли дані одних протоколів інкапсульовані у формати інших протоколів, коли здійснюється фрагментація протокольних блоків даних та (або) трансляція протоколів у шлюзах. У цих випадках застосування методів заміщення або імітації активних елементів обладнання для аналізу протоколів являє складну технічну задачу. З іншого боку, для дослідження роботи протоколів систем абонентського доступу зручно використовувати активні аналізатори протоколів, котрі мають у своєму складі імітатори термінального обладнання користувачів (*TE, DTE*), обладнання мережного закінчення (*NT, DCE*) та (або) лінійного закінчення вузлового комутаційного обладнання (*LT*).

В якості інструментальної бази аналізу ТЛК-протоколів використовуються різного роду пристрої (або в окремих випадках – програмні продукти) під узагальненою назвою „аналізатори протоколів". На ринку інструментальних засобів пропонуються, як правило, багатопротокольні аналізатори, функціональність котрих забезпечує можливість аналізу великої групи, як правило, однотипних протоколів. Зокрема, існують аналізатори, що призначені для аналізу широкого спектру транспортних протоколів МПД, інші аналізатори призначені для аналізу протоколів *ISDN*, існують аналізатори сигналізаційних протоколів, зокрема системи *SS7*, і т.ін. Зрозуміло, що аналізатор повинен настроюватися відповідним чином на аналіз кожного окремого типу протоколу. Більшість аналізаторів протоколів є багатофункціональними приладами, які поряд з основною функцією – аналізом протоколів, здатні виконувати багато інших функцій (зокрема, вимірювати визначальні параметри ТЛК-обладнання), що сприяють вирішенню експлуатаційних проблем. Деякі із аналізаторів протоколів, що представлені на ринку вимірювальної техніки, оснащені

унікальними експертними системами, що дозволяють автоматизувати процес аналізу протоколів.

До основних сфер застосування аналізаторів протоколів слід віднести:

- аналіз структури протоколів (що робиться, головним чином, на передексплуатаційних стадіях життєвого циклу ТЛК-обладнання);
- аналіз коректності реалізації протоколів (застосовується, в основном, під час приймально/здавальних випробувань обладнання);
- пошук шляхів усунення проблем в роботі ТЛК-обладнання під час його експлуатації (виявлення логічних конфліктів в роботі ПЗ, помилкових встановлень параметрів, збоїв в роботі ПЗ, перенавантажень елементів обладнання тощо);
- аналіз коректності процесів фрагментації, інкапсуляції та конвертації протоколів;
- аналіз коректності роботи розподілених прикладних застосувань, зокрема коректності узгодження форматів даних прикладного рівня із форматами задіяних ТЛК-протоколів транспортної мережі.

Контрольні питання до десятої лекції

1. Надайте визначення поняттю «Контроль відповідності».
2. Яка мета організації процесів контролю відповідності?
3. Назвіть документи, які регламентують контроль відповідності?
4. На які групи за функціональною ознакою поділяють вимоги (норми) до специфікацій характеристик або значень параметрів?
5. Які шляхи реалізації контролю відповідності Ви знаєте?
6. Надайте класифікацію видів контролю за часовою координатою.
7. Назвіть вимоги до організації контролю відповідності.
8. В яких випадках здійснюється аналіз результатів контролю відповідності?
9. На які групи за ступенем глибини (ретельності) здійснення контролю підрозділяють процеси контролю відповідності?
10. Надайте характеристику процесам поточного профілактичного контролю.

11. Надайте характеристику процесам тестування відповідності.

12. Поясніть процедуру тестування *IUT* на відповідність вимогам нормуючих специфікацій.

13. Надайте характеристику процедурам аналізу телекомунікаційних протоколів.

14. Що таке траса протоколу?

15. Чим відрізняється проста траса від проміжної та деталізованої?

16. Що таке бінарна траса?

17. Що таке інтерпретаційна траса?

18. Який порядок вирішення проблеми, що пов'язана із можливим виникненням логічного конфлікту в роботі ТЛК-обладнання?

19. Чим відрізняються пасивні методи аналізу протоколів від активних?

20. Які основні сфери застосування аналізаторів протоколів?

Література до десятої лекції

1. І.Г. Бакланов. Технології вимірювань у сучасних телекомунікація. –М.: ЕКО-ТРЕНДЗ, 1998.

САМОСТІЙНЕ ЗАНЯТТЯ ЗА МАТЕРІАЛАМИ ЛЕКЦІЇ №10. ВИМІРЮВАННЯ ПАРАМЕТРІВ СИСТЕМ СИГНАЛІЗАЦІЇ

10.5. Загальна характеристика систем сигналізації

Система сигналізації – це один із різновидів системи керування телекомунікаційними мережами, основним призначенням котрої є встановлення/розривання сеансів зв'язку між клієнтами цих мереж, а в межах вже утворених з'єднань - встановлення певних режимів функціонування обладнання або ініціювання та підтримка роботи механізмів надання послуг відповідно до наданих команд з боку адміністраторів або клієнтів ТЛК-системи.

Обладнання систем сигналізації може входити до складу будь-якої телекомунікаційної мережі – як з пакетною комутацією, так і з комутацією каналів. Проте в пакетних мережах система сигналізації може використовуватися не завжди. Зокрема,

дейтаграмний спосіб просування пакетів *IP* через пакетну мережу не передбачає необхідність використання будь-якої системи сигналізації, в той час як протокол *TCP*, основна функція котрого полягає у встановленні/розриванні сеансів зв'язку на інфраструктурі мереж *IP*, фактично виконує роль сигналізаційного протоколу. У мережах з комутацією каналів, перш за все у телефонних мережах, системи сигналізації є необхідним елементом ТЛК-інфраструктури. Можливо саме тому термін „сигналізація" походить своїми коренями із проблематики телефонних мереж.

Примітка 10.3. Термін „телефонна сигналізація" отримав широке застосування ще за часів впровадження в експлуатацію аналогових телефонних систем з комутацією каналів. Обладнання систем телефонної сигналізації в залежності від дій клієнтів (або персоналу) телефонної системи зв'язку генерує певний набір технологічних сигналів (інакше, - команд або повідомлень), організує процедури обміну цими сигналами між вузлами телефонної мережі та, використовуючи ці сигнали, утворює або розриває телефонне з'єднання між термінальними вузлами телефонної мережі. Обладнання систем сигналізації – важливий компонент будь-якої телефонної мережі. Тому організація вимірювань параметрів цього обладнання являє актуальну експлуатаційну задачу.

Існує кілька десятків різновидів систем телефонної сигналізації та кілька різних класифікаторів їхніх характеристик. Однак у методологічних підходах до здійснення вимірювань параметрів цих систем є багато спільного. Певна специфіка проявляється лише у тому, про яку сигналізацію йдеться – міжстанційну чи абонентську. У разі вимірювань параметрів абонентської сигналізації або під час аналізу сигналізаційного протоколу необхідно розрізняти аналогову абонентську лінію від цифрової абонентської лінії, оскільки підходи до вимірювань параметрів та аналізу протоколів сигналізації на цих лініях суттєво відрізняються.

10.6. Аналіз протоколів систем абонентської сигналізації

Абонентська сигналізація в аналогових лініях зв'язку. Обмін сигналізаційною інформацією в аналогових абонентських лініях здійснюється на фізичному рівні взаємодії. Тому і параметри систем аналогової абонентської сигналізації відносяться до параметрів фізичного рівня, методи вимірювань котрих було розглянуто на лекції №6.

Існують аналізатори сигналізаційних протоколів для стандартних телефонних каналів тональної частоти, що призначені для перевірки коректності функціонування обладнання телефонної абонентської сигналізації та розв'язання логічних конфліктів, що можуть мати місце під час функціонування таких систем. Системи аналогової абонентської сигналізації (що функціонують як у смузі стандартного каналу ТЧ, так і поза цієї смуги) вважаються морально застарілими і у рамках цієї навчальної дисципліни не розглядаються.

Абонентська сигналізація в цифрових лініях зв'язку. Цифрова абонентська лінія, як правило, будується за специфікаціями одного із варіантів технології *ISDN*. У разі реалізації базового доступу *ISDN BRI* сигналізаційні дані передаються через логічний *D*-канал у формі сигналізаційних повідомлень із швидкістю 16 кбіт/с, а обмін сигналізаційними даними здійснюється згідно специфікацій одної із існуючих систем абонентської сигналізації.

Загальна характеристика абонентської сигналізації в каналі ISDN BRI. В Україні найбільш поширеною в абонентських лініях *ISDN* є сигналізація типу *DSS1* (точніше, її європейській варіант - *EDSS1*). Вона специфікується двома протоколами обміну сигнальними повідомленнями:

- на канальному рівні семирівневої моделі – протоколом *LAPD* відповідно до рекомендації МСЕ-Т *Q.921* (цей протокол визначає циклову структуру бітового потоку, що передається через логічний канал *D*);

- на мережному рівні семирівневої моделі – протоколом сигналізаційних повідомлень, що визначає інформаційне поле циклу *LAPD* відповідно до рекомендації МСЕ-Т *Q.931*.

Детально структура цифрової абонентської лінії *ISDN BRI*, а також структура та формати відповідних протоколів базового доступу розглядаються у рамках навчальної дисципліни „Інтегральна цифрова система зв'язку". Тому відразу перейдемо до розгляду методів аналізу цих протоколів.

Методи аналізу протоколів абонентської сигналізації в каналі ISDN BRI. Аналіз протоколів – поширений вид експлуатаційних робіт на мережах *ISDN*, оскільки на практиці знайшли реальне використання багато різних видів та версій

протоколів *ISDN BRI*, сумісна робота котрих, на жаль, часто призводить до виникнення логічних конфліктів в каналах абонентської сигналізації. Система сигналізації *DSS1* також має багато різновидів і тому не позбавлена зазначеного вище недоліку.

На практиці використовується кілька підходів до аналізу протоколів *BRI* – як активне тестування обладнання канала доступу *ISDN BRI* за допомогою імітаторів елементів цього обладнання, які включаються в канал замість реально працюючих елементів, так і пасивний моніторинг роботи протоколу без порушень номінальних умов його функціонування. Активне тестування сприяє зменшенню кількості помилкових кроків у поетапній процедурі локалізації проблеми і, отже, більш швидкому розв'язанню логічних конфліктів в роботі обладнання. У той час як пасивний моніторинг дозволяє у багатьох випадках, хоч і з меншою швидкістю, але все ж успішно локалізувати виниклу проблему без відключення каналу від корисного навантаження. Окрім того, у режимі пасивного моніторингу здійснюють збір статистичних даних щодо поточних параметрів завантаження каналу сигналізації, що вкрай важливо для вирішення багатьох експлуатаційних задач.

Для пояснення методів аналізу протоколів *BRI*, що застосовуються на практиці, наведемо структурну схему базового доступу за технологією *ISDN* (див. рис.10.3).

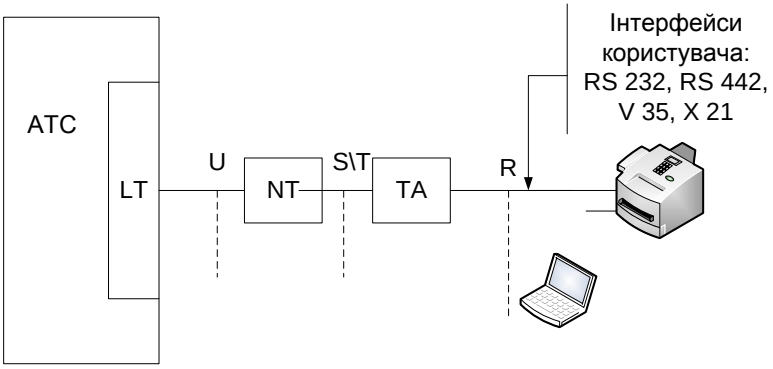


Рис.10.3. Структурна схема абонентського доступу згідно технології *ISDN BRI*

Метод поетапного активного тестування абонентської лінії з послідовним відключенням її елементів. Для тестування використовуються аналізатори протоколів базового доступу, що поряд з іншими функціональними можливостями здатні імітувати роботу основних елементів цифрової абонентської лінії *ISDN BRI*. До складу таких аналізаторів включають: імітатор модулю станційного лінійного закінчення *LT*, імітатор блоку мережного закінчення *NT*, імітатор термінального *ISDN*–обладнання абонента *TE*, а також, у разі необхідності, імітатори того виду абонентського обладнання, що підключається до лінії через термінальний адаптер *TA* (мається на увазі обладнання з інтерфейсом *RS232*, *RS442*, *V.35* і т. ін.).

Якщо керуватися схемою рис.10.3, то зазвичай пропонується наступна послідовність реалізації методу. Спочатку від досліджуваної абонентської лінії відключається станційне обладнання на інтерфейсі *U*, тобто від лінії відключається модуль *LT*, що функціонує у складі АТС, а замість нього до досліджуваної лінії підключається його замінник - імітатор *LT*, що є складовою частиною аналізатора (тестера) протоколу. Це надає змогу протестувати увесь тракт абонентської лінії, окрім станційного обладнання АТС. І якщо таке тестування дасть позитивний результат, то джерело логічного конфлікту (якщо такий має місце) слід шукати в роботі модулю *LT* або взагалі в роботі АТС. За цією ж схемою зручно вимірювати параметр бітової помилки в каналі доступу (параметр *BER*). Якщо блок *NT* перебуває на клієнтському боці, то часто виникає потреба у тестуванні абонентської лінії на інтерфейсі *U*, але вже з боку клієнта. Тоді блок *NT* від лінії на інтерфейсі *U* відключають, а замість нього до лінії підключають аналізатор, що функціонує в режимі імітації сигналів цього блоку у бік станційної частини обладнання. Це надає змогу визначитися із коректністю роботи як станційної частини обладнання, так і безпосередньо самої абонентської лінії на інтерфейсі *U*.

Можуть виникнути сумнівми щодо працездатності блоку *NT*. Тоді його доцільно відключити від шини на інтерфейсі *S/T*, а до порта цього інтерфейса на блоці *NT* підключити аналізатор, що функціонує в режимі імітації сигналів *TE*. Якщо ж є сумніви щодо коректності функціонування протоколу на шині *S/T* внаслідок

можливих логічних конфліктів через некоректну роботу обладнання *TE*, то слід відключити це обладнання від шини *S/T*, а замість нього підключити аналізатор в режимі імітації роботи *TE*. Тоді буде змога протестувати роботу обладнання усієї цифрової абонентської лінії, окрім термінального обладнання абонента *TE*.

Накінець, якщо існує проблема з підключенням до лінії обладнання абонента, що не відповідає стандартам *ISDN BRI*, тоді замість цього обладнання через адаптер *TA* підключають імітатор сигналів відповідного інтерфейсу (*RS232, RS442* тощо). Це надає змогу перевірити коректність функціонування усіх елементів обладнання *ISDN BRI* у комплексі.

Метод пасивного моніторингу абонентської лінії без відключення її елементів. При пасивному аналізі протокола у будь-якій точці цифрової абонентської лінії відпадає необхідність імітації елементів цієї лінії та, саме головне, виключається будь-який вплив аналізатора на сигнальний обмін. У цьому випадку пасивний аналізатор підключається до лінії або паралельно у режимі високоомного включення (за допомогою так званого *T*-подібного моніторингового кабелю, див. рис.10.4), або у розрив лінії так, щоб сигнальний потік проходив безпосередньо через аналізатор (див. рис.10.5 та рис.10.6).

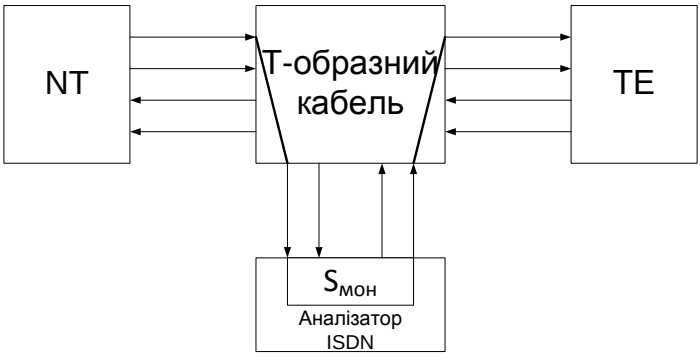


Рис.10.4. Паралельне підключення пасивного аналізатора *ISDN* у шину *S/T* через *T*-подібний моніторинговий кабель

Метод пасивного моніторингу зручно використовувати для

виявлення логічних протиріч у роботі обладнання *ISDN BRI*, оскільки при цьому аналізатор майже не впливає на реальний обмін сигналами в лінії, але і не забезпечує повний аналіз процесу виконання протоколу.

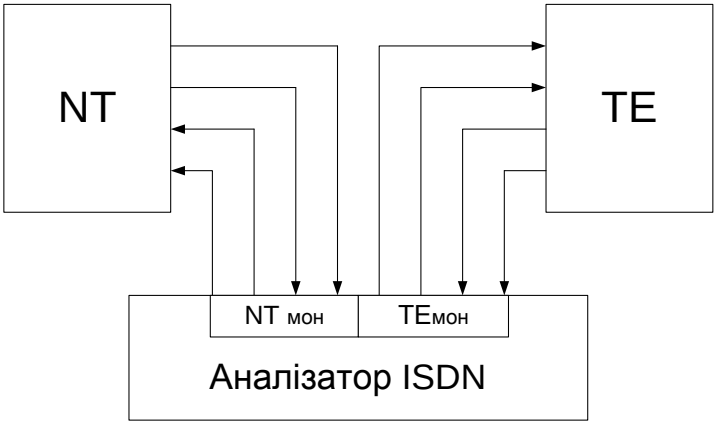


Рис.10.5. Включення пасивного аналізатора *ISDN* у розрив шини *S/T*

Слід підкреслити, що на інтерфейсі *S/T* аналізатор підключають до лінії як через *T*-подібний кабель згідно рис.10.4, так і у розрив лінії згідно рис.10.5.

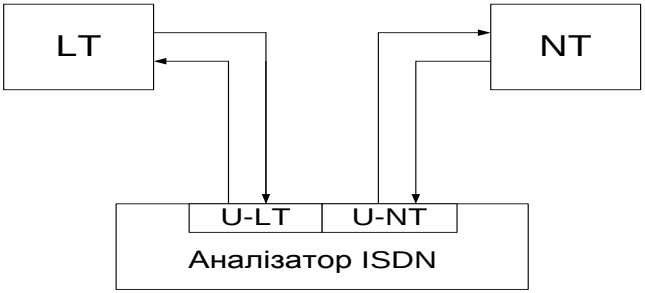


Рис.10.6. Включення пасивного аналізатора *ISDN* у розрив шини *U*

У той час як на інтерфейсі *U* єдино можливий варіант

підключення – у розрив лінії згідно рис.10.6 (на цьому інтерфейсі вельми жорсткі вимоги до параметрів електроживлення лінії, які можуть бути порушені навіть при високоомному підключенні аналізатора).

Вже було сказано, що основним результатом роботи аналізатора є побудована ним траса протоколу. В якості прикладу (див. рис.10.7) нижче наведено уривок простої траси протоколу базового доступу, що побудована за допомогою аналізатора *Aurora Duet* (Приклад траси узято із книги И.Г. Бакланов. *ISDN* и *FRAME RELAY*: технология и практика измерений. –М.: ЭКО-ТРЕНДЗ, 2000).

```
N < T   11: 56 : 27. 650
L1 :
09 : 30 : 12.  658
< - - - - - - - - - - - - L1 –  Info 2
                    09 : 30 : 12. 663
L1 –  Info 3  - - - - - -  - - - - -  - >
09 : 30 : 12.  663
 < - - - - - - - - - - - - L1     Info 4
                    09 : 30 : 12. 666
UI - - - - - - - - - - - - - - - - - - - - >
09 : 30 : 12.  677
< - - - - - - - - - - - - - - - - - - UI
                    09 : 30 : 12.  694
< - - - - - - - - - - - - - - - - - - UI
                    09 : 30 : 12.  717
SABME - - - - - - - - - - - - - - - - >
09 : 30 : 12.  724
< - - - - - - - - - - - - - - - - - - UA
                    09 : 30 : 12.  745
SETUP  ( CR 3) - - - - - - - - - - >
09 : 30 : 12.  755
< - - -  - - - - CALL PROC (CR 3)
                    09 : 30 : 12. 855
RR - - - - - - - - - - - - - - - - - - >
09 : 30 : 12. 951
< - - - - - - - - ALERTING (CR  3)
                    09 : 30 : 13.  017
RR - - - - - - - - - - - - - - - - >
< - - - - - - - - - - - - - - - - - - UA
                    09 : 30 : 19. 561
L1  –  Info 0 - - - - - -  - - - - -  - >
09 : 30 : 19.  754
L1  –  Info 1 - - - - - -  - - - - -  - >
09 : 30 : 31.  103
< - - - - - - - - - - - - L1 –  Info 2
                    09 : 30 : 31. 108
L1  –  Info 3  - - - - - -  - - - - -  - >
09 : 30 :  31.  109
 < - - - - - - - - - - - - L1 –  Info 4
                    09 : 30 : 31. 111
UI - - - - - - - - - - - - - - - - - - - - >
09 : 30 : 31.  122
< - - - - - - - - - - - - - - - - - - UI
                    09 : 30 : 31.  138
< - - - - - - - - - - - - - - - - - - UI
                    09 : 30 : 31.  163
SABME - - - - - - - - - - - - - - - - >
09 : 30 : 31.  169
< - - - - - - - - - - - - - - - - - - UA
                    09 : 30 : 31.  191
SETUP  ( CR 4) - - - - - - - - - - >
09 : 30 : 31.  201
< - - -  - - - - CALL  PROC (CR 4)
                    09 : 30 : 31. 298
RR - - - - - - - - - - - - - - - - - - >
09 : 30 : 31. 391
```

```
09 : 30 : 13.  111
< - - - - - - - - - - - - - - - - - - -  UI
                                  09 : 30 : 13.  649
UI - - - - - - - - - -  - - - - - - - - - >
09 : 30 : 13.  654
< - - - - - - - -  CONNECT (CR 3)
                                  09 : 30 : 15.  471
CONNECT   ACK (CR 3) - - - - >
09 : 30 : 15.  479
 < - - - - - - - - - - - - - - - - - - -  RR
                                  09 : 30 : 15.  592
< - -  - - -DICCONNECT  (CR 3)
                                  09 : 30 : 19.  307
RELEASE (CR 3)  - - - - - - - - >
09 : 30 : 19.  323
< - - - - - - -  REL. COMP (CR 3)
                                  09 : 30 : 19.  370

RR  - - - - - - - - - -  - - - - - - - - - >
09 : 30 : 19.  471
DISC - - - - - - - - -  - - - - - - - - >
09 : 30 : 19.  531
```

```
< - - - - - - - - CONNECT (CR  4)
                                  09 : 30 : 31. 554
CONNECT  ACK (CR  4)- - - - ->
09 : 30 : 31. 561
< - - - - - - - - - - - - - - - - - - -  RR
                                  09 : 30 : 31.  643
 < - - - - - - - - - - - - - - - - - - -  UI
                                  09 : 30 : 32.  100
UI - - - - - - - - - - - - - - - - - - - - - >
09 : 30 : 32.  105
DISCONNECT  (CR  4)- - - - - ->
09 : 30 : 34.  079
< - -  - - - RELEASE (CR 4)
                                  09 : 30 : 34.  155
REL.  COMP  (CR 4) - - - - - - - - -
>
09 : 30 : 34.  165
DISC - - - - - - - - - - - - - - - - - - -
>
09 : 30 : 34.  322
< - - - - - - - - - - - - - - - - - - -  UA
                                  09 : 30 : 34.  346
L1  –  Info 0- - - - - - - - - - - - - >
09 : 30 : 34. 501
```

Рис.10.7. Уривок простої траси протоколу базового доступу *ISDN*

Розглянемо, яким чином декодувати цей уривок траси. Перш за все, звернемо увагу на часові мітки (тобто, часові позначки) виду 09:30:xx.xxx (дев'ять годин, тридцять хвилин, xx.xxx секунд, де значення секунд задано з точністю до тисячної частки секунди, тобто з точністю до трьох десяткових розрядів після точки, що відділяє цілу частину числа секунд від її дробної частини). Ці часові мітки надані безпосередньо під кожним штриховим вектором, що вказує напрямок передавання сигнального повідомлення, або під кожним позначенням сигнального повідомлення, яке відображається праворуч або ліворуч від штрихового вектора. Тобто, на зображеній трасі будь-яке зафіксоване аналізатором сигнальне повідомлення є початком

(ініціатором) напрямку обміну. Виключення являє лише заголовок траси - перші три рядки початку траси, тобто три верхні рядки лівої колонки у записі траси, які безпосередньо не відносяться до траси. Ці три рядки відображають дії користувача аналізатора протоколу (інженера-зв'язківця), що вирішує експлуатаційне завдання, що пов'язане із аналізом протокола. Зокрема, перший рядок *N<T* 11:56:27.650 означає, що рівно об 11годині 56 хвилин 27,650 секунд користувач задав команду аналізатору роздрукувати просту трасу вже виконаного протоколу у напрямі від *TE* до *NT*. Він також задав рівень протоколу, з якого слід почати трасування (це другий рядок – L1:), а також початок часового інтервалу (це третій рядок траси, тобто 09:30:12.658) починаючи з якого мають фіксуватися сигнальні повідомлення. Далі, починаючи із четвертого рядка першого стовпця і закінчуючи останнім рядком третього стовпця, відображається безпосередньо проста траса протоколу *ISDN BRI*.

Таким чином, проста траса відображена у вигляді двох колонок запису, читати яку треба послідовно зліва направо, спочатку записи першої колонки (зверху униз), потім продовження траси - у другій колонці. При цьому перше сигнальне повідомлення траси (тобто, L1 – info 2) було згенеровано у момент 09:30:12.663 і пішло у напрямі від *NT* до *TE* (на це вказує напрямок штрихового вектору, а саме ← - - - -), а останнє сигнальне повідомлення траси (тобто, L1 – info 0) було згенеровано у момент 09:30:34.501 і пішло у напрямі від TE до NT (на це вказує напрямок штрихового вектору, а саме - -- -→). Тобто, проста траса протоколу у даному випадку побудована тривалістю трохи меншою, ніж 22 сек.

Щоб розібратися із змістом цієї траси, необхідно мати певні знання щодо побудови досліджуваного протоколу. У даному випадку, необхідно уявляти порядок обміну сигнальними повідомленнями першого рівня протоколу (тобто, сигналами типу info 0 - info 4) у момент активації/деактивації шини S як з боку *NT*, так і з боку *TE*. Перші три штрихових вектори у зображені траси (info 2, info 3 та info 4) якраз і відображають цей обмін у процедурі активації шини *S* за умов, коли ініціатором активації цієї шини являється *NT*.

Необхідно також уявляти, яким чином здійснюється процедура

встановлення з'єднання на другому (канальному) рівні протоколу (тобто, обмін сигнальними повідомленнями типу UI, SABME і т. ін.). І, накінець, треба знати зміст та порядок обміну сигнальними повідомленнями третього рівню (типу SETUP, CONNECT, DISCONNECT, RELEASE і т. ін.) як під час встановлення з'єднання, так і під час його розривання. Якщо такі знання у користувача аналізатора є, то він без особливих зусиль декодує наведену вище просту трасу протоколу.

Зокрема, він побачить, що спочатку йде процедура активації шини *S* з боку *NT*. Останнє повідомлення першого рівня L1 у рамках цієї процедури - info 4 – мало місце у момент 09:30:12.666. Далі починається процедура встановлення каналу на другому рівні протоколу, починаючи з повідомлення UI, що пройшло в момент 09:30:12.677, і закінчуючи повідомленням UA, що пройшло в момент 09:30:12.745. Після встановлення канала шляхом передачі повідомлення SETUP з боку TE (у момент 09:30:12.755) починається процес встановлення з'єднання третього рівня. У моменти подачі сигналу CONNECT (09:30:15.471) та сигналу підтвердження CONNECT ACK (09:30:15.479) процес встановлення з'єднання було закінчено. Однак вже приблизно через чотири секунди (у момент 09:30:19.307) сигнальне повідомлення DISCONNECT повідомило про початок процесу розриву з'єднання за ініціативою *NT*. Процес розриву супроводжується обміном повідомленнями як другого так і третього рівнів. Друга частина траси починається з моменту 09:30:31.103, коли за ініціативою *TE* (сигнальним повідомленням info 1) починається процес активації шини *S*. Цей процес закінчується у момент 09:30:34.079, коли у бік *NT* надсилається повідомлення DISCONNECT. Після чого починається процес розриву з'єднання, який закінчується у момент 09:30:34.501.

Висновок, який слід зробити після розгляду цієї траси: обмін сигнальними повідомленнями здійснювався коректно, логічних конфліктів не виявлено. Проте, якщо була б виявлена якась некоректність в обміні, то для більш точного аналізу виявленого конфлікту, скоріш за все, необхідно було б побудувати більш деталізовані траси протоколу, які, у свою чергу, мають набагато більш складну логічну побудову. Треба мати більш глибокі знання

щодо структури протоколу та певний практичний досвід користування аналізатором протоколу, щоб розраховувати на успіх під час аналізу деталізованих трас.

10.7. Аналіз протоколів міжстанційної сигналізації

Із множини протоколів міжстанційної сигналізації, що наразі мають застосування у сучасних ТЛК-системах, розглянемо найбільш поширений – протокол загальноканальної сигналізації *SS7*.

Загальна характеристика протоколу SS7. Система сигналізації №7 (*Signaling System 7, SS7*) наразі – основний стандарт міжстанційної (точніше, - міжвузлової) сигналізації не тільки на телефонних мережах загального користування (ТМЗК), але і на базатьох інших різновидах ТЛК-мереж, зокрема на мережах стільникового зв'язку, мережах *ISDN*, мультисервісних мережах і т.ін. Більше того, на сучасному етапі розвитку телекомунікацій система *SS7* виконує функцію об'єднання різнорідних ТЛК-систем (зокрема, телефонних стаціонарних та мобільних, *IP*-мереж, включаючи Інтернет, мереж передавання даних і т.ін.) в єдині глобальні ТЛК-інфраструктури, що здатні задовольнити попит користувачів мережних ресурсів у широкому спектрі різноманітних ТЛК-послуг. Оскільки у цій системі використовується принцип відокремлення потоків сигнальної інформації від потоків інформації користувачів, а сама сигнальна інформація (що стосується кожного із утворених абонентських з'єднань) має передаватися у смузі загального (спільного) для цих з'єднань каналу сигналізації, то нерідко систему *SS7* називають також системою загальноканальної сигналізації №7 (ЗКС-7).

Слід окремо зазначити, що система *SS7* відіграє вирішальну роль в організації взаємодії обладнання національних ТЛК-мереж різних країн між собою, тобто *SS7* – це міждержавна система сигналізації, на її основі побудовано міжнародні телефонні мережі, міжнародні мережі стільникового мобільного зв'язку, глобальні корпоративні ТЛК-мережі, мережа Інтернет тощо.

Система *SS7* – одна із найбільш складних у технічному плані систем, що вивчається у рамках навчальної дисципліни „Телекомунікаційні та інформаційні мережі". Тому обмежемося

коротким розглядом структури мережі сигналізації *SS7* (див. рис.10.8) з точки зору можливостей здійснення аналізу сигналізаційного протоколу, що реалізується засобами цієї мережі.

На рис.10.8 прийнято наступні позначення: *STP* – пункт передавання сигнальних повідомлень; *SSP* – абонентський пункт сигналізації; *SCP* – пункт надання додаткових послуг. Слід зазначити, що на рис.10.8 використано найбільш широко застосовані назви та позначення елементів структури мережі *SS7* , які узято із проблематики так званих інтелектуальних мереж (*INET*) (напевне тому, що розробка архітектурної концепції *SS7* співпала у часі із розробками концепції *INET*). !!!

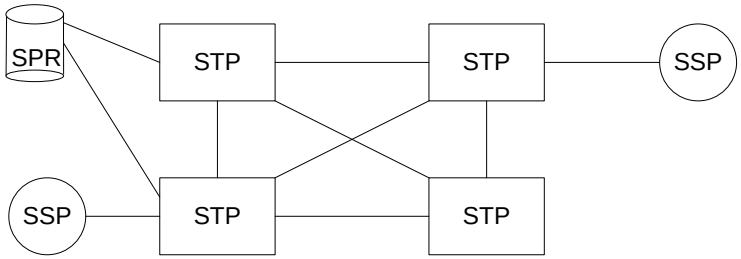


Рис.10.8. Узагальнена структура мережі сигналізації *SS7*

При вирішенні задач аналізу сигналізаційного протоколу більш зручно сприймати структуру мережі *SS7* як класичну мережу передачі даних (МПД), де *STP* виконує функції маршрутизації пакетів (у які упаковано сигнальні повідомлення), *SSP* – функції термінального обладнання мережі *SS7* (але не термінального обладнання транспортної мережі, яку мережа *SS7* обслуговує. Функції *SSP* на телефонній мережі зазвичай виконує АТС, оскільки саме АТС у телефонній мережі є джерелом та отримувачем повідомлень міжстанційної сигналізації), а *SCP* – функції серверу, що містить загальнодоступні дані, що є необхідними для підтримки послуг, які можуть бути надані системою сигналізації тим ТЛК-процесам, що цією системою користуються. Слід наголосити, що система сигналізації *SS7* (і це її основна структурна особливість) створюється або як окрема підсистема у рамках транспортної мережі, сигналізаційна інформація якої у вигляді повідомлень

сигналізаційного протоколу циркулює по логічно (а не фізично) виділеним каналам зв'язку (наприклад, в часових проміжках *TS16* систем ІКМ-31 у рамках каналу *E1*), або взагалі як окрема фізично виділена мережа сигналізації із своїм власним вузловим обладнанням та своїми власними каналами зв'язку.

Сигналізаційний протокол *SS7* має специфічну чотирьохрівневу структуру і являє собою певний набір програмних підсистем, що поступово по мірі розвитку протоколу доповнюється новими підсистемами, що здатні обслуговувати нові різновиди ТЛК-систем. Зокрема, склад одної із ранішніх версій цього протоколу, що призначений для обслуговування ТЛК-інфраструктур, створених на основі класичних телефонних мереж, мереж *ISDN*, стільникових мереж *GSM* та *NMT*, відображено на рис.10.9.

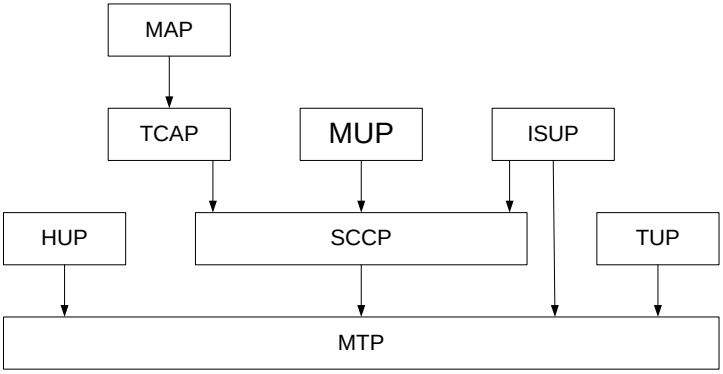


Рис.10.9. Структура протоколу сигналізації *SS7*

ПЗ, що реалізує представлену на рис.10.9 версію протоколу *SS7*, складається із наступних програмних підсистем:

- *MTP* – підсистема передавання сигнальних повідомлень;
- *SCCP* – підсистема управління наскрізними з'єднаннями;
- *HUP* - підсистема передавання сигналів керування, що підтримує голосовий зв'язок у мережах стандарту *NMT*;
- *TUP* - підсистема передавання сигналів керування, що підтримує голосовий зв'язок у класичних телефонних мережах;
- *ISUP* - підсистема передавання сигналів керування, що

підтримує користувачів мережі *ISDN*;

- *TCAP* - підсистема підтримки транзакцій;

- MUP - підсистема підтримки користувачів мережі стандарту *NMT*;

- *MAP* - підсистема підтримки користувачів мережі стандарту *GSM*.

Більш пізні версії протоколу *SS7* мають більш розширений склад підсистем. На практиці інсталюють версію цього протоколу, що забезпечує підтримку саме тих ТЛК-технологій, що реалізовані в конкретному проекті створюваної ТЛК-інфраструктури.

Оскільки мережу *SS7* з позицій технічної експлуатації (ТЕ) доцільно розглядати як МПД, то і, відповідно, для здійснення ТЕ слід використовувати раніш розглянуті підходи, що є характерними для експлуатації МПД. Сказане стосується і проблем аналізу сигналізаційного протоколу *SS7*.

Аналіз протоколу *SS7* здійснюється практично на усіх стадіях життєвого циклу обладнання цієї системи сигналізації:

- на стадії проектування нової ТЛК-інфраструктури аналізують коректність функціонування нової версії цього протоколу, що має забезпечити підтримку роботи усіх ТЛК-систем, що входять до складу створюваної інфраструктури;

- на стадії запуску в експлуатацію нових ТЛК-систем також необхідно детально протестувати вперше інстальоване обладнання *SS7* на відповідність його характеристик технічним умовам;

- на стадії експлуатації обладнання ТЛК-інфраструктури іноді необхідно протестувати обладнання нового каналу сигналізації або протестувати реалізацію цього протоколу після переінсталяції його параметрів;

- на стадії експлуатації обладнання ТЛК-інфраструктури слід використовувати різні методи експлуатаційного аналізу протоколу *SS7* для виявлення та усунення можливих логічних конфліктів в роботі ТЛК-обладнання.

Основні методи експлуатаційного аналізу протоколу SS7. В експлуатаційній практиці протокольний аналіз *SS7* здійснюють шляхом заміщення одного із елементів обладнання цієї системи на імітатор цього елементу із наступним аналізом реакції залишившейся частини обладнання на тестуючі впливи імітатора.

Для цього використовують активний аналізатор *SS7*, до складу котрого входять імітатори обладнання *SSP, STP* та *SCP*. Включення аналізатора *SS7* в якості імітатора *SSP* показано на рис.10.10.

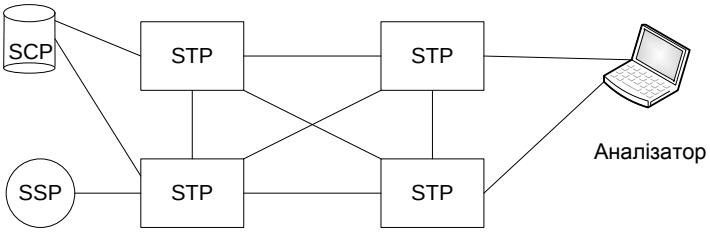


Рис.10.10. Включення аналізатора *SS7* в якості імітатора *SSP*

Таке включення імітатора найчастіше здійснюють перед тим, як підключити нову АТС до телефонної мережі (зокрема, до *PSTN*). У цьому випадку необхідно упевнитись, що з боку пунктів *STP* мережі *SS7* на вперше встановлене обладнання АТС (точніше, на обладнання *SSP*, що входить до складу цієї АТС) здійснюється коректне надходження потоків сигналізаційних повідомлень. Аналізатор на схемі.10.10 імітує роботу прикінцевого пункту сигналізації *SSP*, що підключений до двох пунктів *STP*, що реально працюють у складі існуючої мережі *SS7*. При цьому траси досліджуваного протоколу будуються засобами АТС або аналізатора *SS7*. Включення за схемою 10.10 дозволяє виконати повний аналіз усіх рівнів протоколу, а також, у необхідних випадках, здійснити так зване стресове тестування сигналізаційної системи, коли імітуються всілякого роду порушення в алгоритмі сигнального обміну з тим, щоб визначити реакцію системи на ці порушення.

На рис.10.11 показане включення аналізатора *SS7* в якості імітатора *STP*. Таке включення імітатора є актуальним перед тим, як увести в експлуатацію новий вузловий пункт сигналізації *STP*, наприклад на міжміській АТС Обладнання *STP* здійснює лише маршрутизацію та передавання сигналізаційних повідомлень. Тому імітатор, що включений на схемі рис.10.11 замість *STP*, здійснює імітацію лише на перших трьох рівнях протоколу *SS7*.

Аналізатор у цьому випадку забезпечує повний аналіз цих рівнів протоколу, а також стресове тестування за різних умов імітації нештатних ситуацій в роботі обладнання – імітація перенавантаження сигналізаційного каналу, імітація регулярного зникання повідомлень сигнального трафіку, дублювання повідомлень і т.ін.

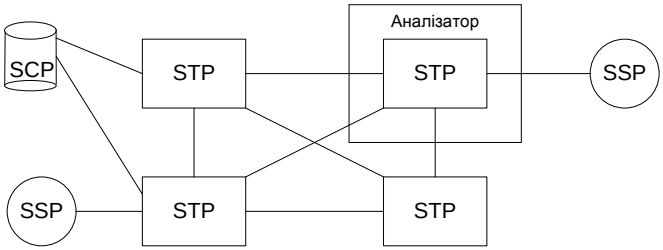


Рис.10.11. Включення аналізатора *SS7* в якості імітатора *STP*

Часто до обладнання *STP* підключають пасивний аналізатор *SS7*, що надає змогу збирати статистичну інформацію щодо „поведінки" сигнального трафіку у цій точці. Це вкрай важливо для аналіза потенціалу експлуатованої системи *SS7* та визначення показників ефективності її функціонування.

Дослідити роботу механізмів гнучкого керування сигнальним трафіком можливо лише шляхом стресового тестування і бажано не в одній, а одночасно в кількох точках розміщення *STP*. Схема підключення двох аналізаторів *SS7* одночасно до двох точок STP_1 та STP_2 показана на рис.10.12. Включення аналізаторів за схемою рис.10.12 дозволяє здійснювати комплексний аналіз реакції мережі *SS7* у точці розміщення STP_2 за умов, коли потік тестуючих повідомлень надсилається засобами імітатора STP_1, і навпаки. Зокрема, можливо імітувати перенавантаження сигнального каналу між STP_1 та *SSP* і в цей час спостерігати, як сигнальний трафік поступово переміщається від STP_1 до STP_2. Можливо також імітувати порушення готовності каналу між STP_1 та *SSP* і дивитися, чи перенесеться за цих умов сигнальний трафік від STP_1 до STP_2.

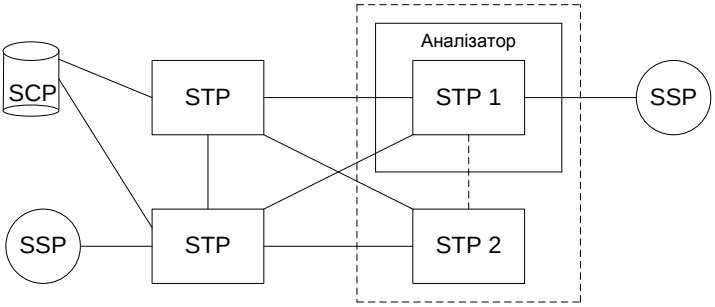


Рис.10.12. Підключення аналізаторів *SS7* замість двох *STP*

Імітація роботи обладнання *SCP* здійснюється вкрай рідко (тільки коли необхідно увести в експлуатацію новий пункт надання послуг) і у рамках цієї навчальної дисципліни не розглядається.

Більш часто на практиці виконується стресове тестування вже функціонуючих елементів обладнання *SS7*. Зокрема, на рис.10.13 показана схема включення аналізатора у канал між *STP* та *SSP*. Аналізатор, що включений за такою схемою, забезпечує внесення бажаних стресових впливів на досліджуваний сигналізаційний канал (зокрема, внесення додаткових затримок у передавання повідомлень, дублювання сигналізаційних повідомлень, їхня втрата тощо) і, тим самим, дозволяє побачити наслідки таких впливів експлуатаційному персоналу.

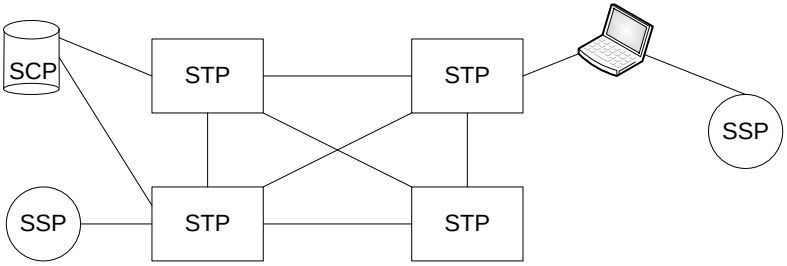


Рис.10.13. Схема включення аналізатора SS7 у канал між STP та SSP

Нарешті, кілька слів щодо класифікації аналізаторів *SS7*. Існує чотири основних класи таких аналізаторів:

- унікальні дуже досконалі (і, отже, високовартісні) аналізатори

SS7, що використовуються для національного та транснаціонального моніторингу мереж *SS7*;

- аналізатори *SS7*, що використовують розробники нових систем сигналізації;

- аналізатори *SS7*, що використовують для комплексних вимірювань в процесі експлуатації обладнання *SS7*;

- прості тестери із функціями *SS7*.

Зрозуміло, що на стадії експлуатації користуються пристроями, що віднесені до останніх двох класів.

Контрольні питання до самостійного заняття десятої лекції

1. Надайте загальну характеристику системам сигналізації.
2. Надайте характеристику абонентській сигналізації в аналогових лініях зв'язку.
3. Надайте характеристику абонентській сигналізації у цифрових лініях зв'язку.
4. Які методи аналізу протоколів абонентської сигналізації в каналі *ISDN BRI* Ви знаєте?
5. Яким чином Ви декодуєте уривок траси протоколу?
6. Надайте загальну характеристику протоколу *SS7*?
7. Поясніть узагальнену структуру мережі сигналізації *SS7*.
8. Яка структура протоколу сигналізації *SS7*?
9. Поясніть основні методи експлуатаційного аналізу протоколу *SS7*.
10. Яким чином включається аналізатор в мережу *SS7*?

Література до самостійного заняття десятої лекції

1) І.Г. Бакланов. Технології вимірювань у сучасних телекомунікація. –М.: ЕКО-ТРЕНДЗ, 1998.

2) І.Г. Бакланов. ISDN та FRAME RELAY: технологія та практика вимірювань. –М.: ЕКО-ТРЕНДЗ, 2000.

ЛЕКЦІЯ №11. АДМІНІСТРУВАННЯ РЕСУРСАМИ ТЕЛЕКОМУНІКАЦІЙНОГО ОБЛАДНАННЯ

Розглядаються наступні питання:

Лекційне заняття

11.1. Загальна характеристика задач адміністрування
11.2. Порядок здійснення процедур адміністрування
11.3. Адміністрування вузлу мережі
11.4. Конфігурування характеристик обладнання
11.5. Адміністрування систем сигналізації
11.6. Адміністрування білінгової системи

11.1. Загальна характеристика задач адміністрування

В інструкціях з експлуатації будь-якого сучасного ТЛК-обладнання зазвичай один із підрозділів присвячено опису функцій керування та адміністрування цього обладнання (тобто, опису функцій *Operation and Maintenance, O&M*). Функціями *O&M* користується персонал оператора зв'язку, щоб забезпечити належне надання мережних послуг та оптимальні умови функціонування як окремих елементів обладнання, так і всієї ТЛК-системи у цілому. Зокрема шляхом використання певних груп цих функцій (головним чином, груп функцій виду *Fault Management* та *Security Management*) мережний адміністратор здійснює аудит ресурсів, відновлює роботу обладнання після реалізації загроз інформації, реалізовує прийняту політику забезпечення захисту від несанкціонованого доступу (НСД) до ресурсів мережі. В апаратних засобах активних макро-елементів ТЛК-системи, як правило, реалізовані зручні інтерфейси управління цими елементами, а менеджери цих елементів (*Element Manager, EM*) є доступними як через локальні термінали, так і через систему централізованого керування мережею (*Network Management System, NMS*). Іншими словами, кожний активний макро-елемент ТЛК-системи (зокрема, комутатор, маршрутизатор, сервер або шлюз) має, щонайменше, два порти керування: один - для підключення локального засобу управління (тобто, комп'ютера із відповідним управлінським ПЗ), другий – для підключення до мережі централізованого керування.

Щоб мати уявлення про функціональні можливості сучасних

ТЛК-систем щодо адміністрування цими системами, розглянемо, для прикладу, базову функціональність *O&M* типової ТЛК-системи. Засоби *O&M* сучасної ТЛК-системи забезпечують:

- налаштування графічного інтерфейсу адміністраторів обладнання на бажану архітектуру відтворення процесів, що мають місце у ТЛК-системі під час її функціонування (тобто, налаштування під особисті «смаки» адміністраторів системи);
- керування парольною інформацією при організації доступу до ресурсів системи та при організації захищених з'єднань (надання паролів, зміна паролів тощо);
- автентифікацію та авторизацію користувачів ресурсами та можливостями ТЛК-системи;
- конфігурування параметрів обладнання та автоматичну реєстрацію змін цих параметрів;
- попереднє встановлення конфігураційних профілів для елементів обладнання, у т. ч. і бажаних профілів захищеності інформації;
- встановлення порогів для виявлення подій, що впливають на працездатність обладнання, на рівень якості надання послуг і на рівень захисту інформації;
- відображення тривожних сигналів, що надходять при виявленні подій від елементів ТЛК-системи;
- модифікацію параметрів елементів та всієї ТЛК-системи у цілому;
- адміністрування обладнанням;
- локалізацію проблем невідповідності, у т.ч. можливість постійного контролю параметрів обладнання за допомогою спеціалізованих засобів спостереження з метою вияву невідповідностей в роботі цього обладнання і у разі виявлення такої невідповідності активізація засобів спеціально створеної системи тривожної сигналізації (*alarm system*) про виниклу подію (будь-яка система тривожної сигналізації зазвичай зберігає інформацію щодо виниклих тривожних подій у журналі реєстрації подій невідповідностей - *alarm history*);
- можливість ідентифікації невідповідності за допомогою засобів системи тривожної сигналізації та інформування спеціалізованих експертних та виконавчих систем (*recovery system*),

що забезпечують пошук та вирішення проблем невідповідності в роботі обладнання;

- можливість обмеження негативних наслідків виникнення невідповідності шляхом ізоляції невідповідного елемента від інших елементів обладнання та включення справного резервного елементу (якщо він існує) в роботу замість ізольованого;
- можливість детального аналізу характеристик виявленої невідповідності за допомогою діагностичної системи та надання результатів такого аналізу адміністраторам мережі, а також експертним та виконавчим системам;
- можливість тестування обладнання з метою підтвердження його справності;
- можливість реконфігурування елементів та всієї системи у цілому;
- можливість внесення змін (апгрейт) із віддаленого вузлу централізованого управління у ПЗ кожного із елементів ТЛК-системи.

Визначення терміну "адміністрування". Адміністрування – це одна із функцій *O&M*, яку виконують адміністратори - суб'єкти, діяльність котрих безпосередньо пов'язана з управлінням ресурсами системи. Зазвичай в телекомунікаціях під адмініструванням розуміють конкретні управлінські дії адміністраторів ТЛК-обладнання з настроювання програмно-апаратних елементів обладнання та (або) ТЛК-системи у цілому відповідно до конкретних умов використання. Маються на увазі, наприклад, такі дії адміністраторів як генерація команд управління, встановлення конкретних значень параметрів обладнання, змінювання режимів роботи, форматування даних, формування списків подій, встановлення логічних обмежень в роботі обладнання та користувачів, управління базами даних, встановлення найменувань об'єктів, ідентифікаторів суб'єктів, правил розмежування доступу тощо.

Розрізняють: первісне (початкове) адміністрування ТЛК-системи, що робиться на стадії уводу її в експлуатацію, коли її вперше настроюють на конкретні умови використання; оперативне (поточне) адміністрування на стадії експлуатації цієї системи.

Якщо б умови використання ТЛК-системи з плином часу не змінювалися, то не було б потреби в оперативному адмініструванні її ресурсів. Однак в процесі експлуатації умови функціонування ТЛК-системи, як правило, змінюються: міняються користувачі ТЛК-послуг, змінюються їхні потреби щодо номенклатури та рівнів якості послуг, змінюється вартість послуг та умови їхнього надання і т. ін. – все це обумовлює необхідність здійснення поточного адміністрування ресурсами ТЛК-системи.

Адміністратори із числа експлуатаційного персоналу здійснюють за пультом системного монітора у реальному часі певні послідовності управлінських дій, що називаються процедурами адміністрування. Процедурами адміністрування охоплено практично усі апаратні засоби ТЛК-системи та спеціалізовані програмні застосування, які інстальовані і виконуються в системі, підтримуючи надання телекомунікаційних послуг в процесі функціонування ТЛК-обладнання за основним призначенням.

Локальне та централізоване адміністрування. Адміністрування будь-якого елементу ТЛК-обладнання можливо здійснювати як за допомогою вбудованих в його склад локальних засобів управління цим елементом, так і через віддалений пункт централізованого керування.

Локальне адміністрування будь-якого окремого макро-елементу ТЛК-обладнання, що функціонує у складі будь-якого вузлу ТЛК-мережі (наприклад, маршрутизатора, комутатора або сервера) здійснюється через його термінал управління. Іншими словами, будь-який активний елемент вузлового обладнання сучасної ТЛК-мережі, будь то комутатор, шлюз чи сервер, має свої власні засоби управління, зокрема порт до якого завжди існує можливість під'єднати комп'ютер з інстальованими на ньому програмами локального управління цим активним елементом. Однак адміністрування цього ж макро-елементу можливо здійснювати, у разі потреби, і дистанційно за допомогою засобів централізованого керування, розташованих на зазвичай віддаленому вузлі керування (*Management Node*). Оскільки функції управління та технічного обслуговування усіх телекомунікаційних вузлів сучасної мережі здійснюються, як правило, із вузлу керування, то і адміністрування

усієї ТЛК-мережі здійснюється засобами вузлу керування. Функції вузлу керування іноді виконує термінал управління (*Management Terminal*) телекомунікаційної системи.

Технологія адміністрування ресурсами ТЛК-обладнання. Підтримку функцій адміністрування ресурсами ТЛК-обладнання виконує відповідне спеціалізоване програмне забезпечення (ПЗ), що функціонує у реальному часі і зазвичай у фоновому режимі без призупинки роботи ТЛК-системи згідно основного призначення. Адміністратор ТЛК-системи, сидячи за клавіатурою монітора, в процесі адміністрування взаємодіє з цим ПЗ через відповідний, як правило, графічний інтерфейс управління системою (*GUI - Graphical User Interface* - графічний інтерфейс користувача).

Деякі адміністративні дії можуть бути виконані у так званому режимі термінального доступу (або, інакше, в режимі віддаленого управління), коли адміністратор перетворює свій комп'ютер у віртуальний термінал активного елементу ТЛК-системи, до якого він отримує доступ. Між комп'ютером адміністратора та портом управління активного елементу встановлюється так званий інтерфейс командної лінії *CLI* (*Command Line Interface*), через який адміністратор має можливість послідовно символ за символом надавати команди у підсистему управління активним елементом (як іноді кажуть, у режимі командного рядка) та отримувати відповіді - реакції на надані команди (також послідовно символ за символом), що виводяться у вигляді символьного тексту на дисплей адміністратора. Наприклад, через CLI можуть бути надані команди:

- на запуск або припинення роботи шлюзу;
- на виконання головних прикладних задач;
- контролю кількості записів у вивідному файлі та характеристик поточного вивідного файлу, що надається у систему післяпроцесорної обробки цих записів;
- на перевстановлення статистичних лічильників;
- запитів до різних модулів шлюзу тарифікації.

Існує велика кількість протоколів віддаленого управління (що працюють на прикладному рівні семирівневої моделі *OSI*), але найбільш популярним вважається протокол *telnet*, який найчастіше використовується в середовищі ОС *Unix*. Протокол *telnet* працює в

архітектурі «клієнт - сервер». Клієнтська частина ПЗ знаходиться на комп'ютері адміністратора, а серверна - на активному елементі ТЛК-системи. При натисканні клавіші дисплею відповідний код перехоплюється клієнтом *telnet*, інкапсулюється у *TCP*-повідомлення та відправляється через командну лінію (або мережу, якщо адміністратор знаходиться у віддаленому вузлі мережі) до активного елементу ТЛК-системи, що підлягає адмініструванню. Серверне ПЗ активного елементу вибирає із *TCP*-повідомлення прийнятий код клавіші та передає його до ОС цього елементу. ОС розглядає сеанс *telnet* як один із сеансів локального користувача. Якщо реакція активного елементу на прийняту команду являє собою певну сукупність символьних рядків, що мають бути виведені на екран дисплею, серверне ПЗ протоколу *telnet* кожен символ цієї сукупності окремо упаковує в *TCP*-повідомлення та відправляє його до комп'ютера адміністратора. Клієнтське ПЗ протоколу *telnet* витягує ці символи із *TCP*-повідомлень та відображає їх у вікні терміналу адміністратора, емулюючи термінал віддаленого вузлу.

Віддалене управління вельми економно використовує пропускну здатність командної лінії (оскільки у цьому випадку передаються лише коди клавіш та екранні символи), але є практично незахищеним від несанкціонованого перехоплення та підмін.

З метою пояснення технології адміністрування розглянемо ***типову структуру ПЗ сучасної ТЛК-системи***. Характеристики топологічної структури ТЛК-системи у даному розгляді не враховуються: це може бути локальна система з одним вузлом і з одним активним елементом (наприклад, комутатором) у вузлі або, у загальному випадку, глобальна мережа з багатьма вузлами і з багатьма активними елементами (наприклад, сукупністю маршрутизаторів, комутаторів, шлюзів з лінійкою серверів тощо) у кожному вузлі та ще і з відокремленим вузлом керування мережею. Як правило, у складі кожного активного елементу такої системи функціонує операційна система (ОС) – спеціалізована або загального призначення, в операційне середовище котрої поміщені комплекси прикладних програм різноманітного призначення. В кожен комплекс входять, доповняючи одна одну, комп'ютерні

програми, що сумісно функціонують заради підтримки функціонування якогось конкретно визначеного процесу (наприклад, маршрутизації пакетів) або заради вирішення якогось конкретно визначеного завдання (наприклад, вимірювання інтенсивності трафіка). Ці комплекси мають ієрархічну структуру, тобто у складі комплексів вищого рівня інстальовані комплекси більш низького рівня ієрархії і т. д. Ці комплекси прикладних програм називають прикладними застосуваннями або просто застосуваннями.

Відносно ОС, що знайшли застосування в активних елементах сучасних ТЛК-систем, слід вказати на наступне. Зазвичай у реальних системах використовуються або широко розповсюджені ОС загального призначення (*WINDOWS, UNIX, Linux* і т. ін.), або вузько спеціалізовані ОС (наприклад, *CISCO IOS, Nokia IPSO*™), що спеціально розроблені для використання у виробах компаній – розробників ТЛК-обладнання. У спеціалізованих ОС усі функції та можливості операційних систем, що не використовуються ТЛК-обладнанням, усунено, проте додаткові можливості, що підвищують ефективність роботи обладнання, реалізовано. Тому спеціалізовані ОС, що входять до складу активних елементів ТЛК-систем, характеризуються більш високою швидкодією, компактністю та захищеністю від несанкціонованого доступу (НСД). Проте вони мають вузьку сферу застосування і проблеми із взаємодією з ОС інших видів.

Щодо прикладних застосувань, які функціонують у складі ТЛК-систем, необхідно відмітити наступне. Прикладні застосування вищого рівня ієрархії, як правило, розділяють на групи згідно функціонального призначення (див. рис.11.1).

Як бачимо, до основних груп застосувань відносять комплекси програм, які безпосередньо забезпечують функціонування ТЛК-систем за основним призначенням. Основне призначення ТЛК-системи – надання ТЛК-послуг із транспортування інформації (наприклад, передача даних), з організації інформаційної взаємодії віддалених один від одного суб’єктів або процесів (наприклад, телефонний зв'язок або інтерактивна взаємодія віддалених комп’ютерних систем), із забезпечення доступу до різноманітних інформаційних сервісів (перш за все, до сервісів Інтернет).

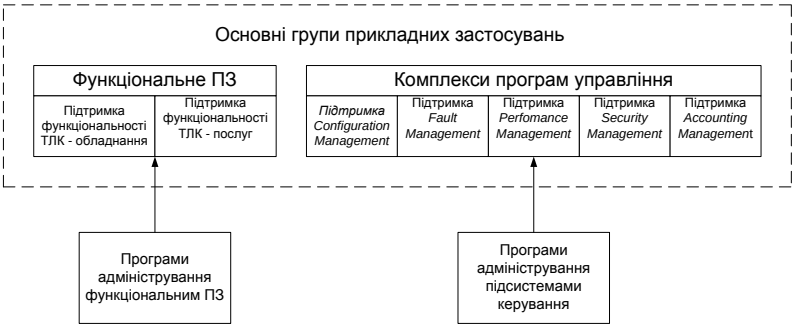


Рис.11.1. Загальна структура прикладного ПЗ ТЛК-систем

Наприклад, основні групи прикладних застосувань типової телефонної комутаційної системи, яка є основним елементом будь-якої АТС або телефонного серверу, підтримують процеси:

- обробки викликів (рос. – вызовов), зокрема фіксації та маршрутизації викликів, активізації процесів надання додаткових послуг, підтримки взаємодії між процесами надання послуг, а також збір даних про виклики (які потім використовуються як вихідні дані при вимірюваннях навантаження та тарифікації);

- обробки з`єднань**,** тобто встановлення та розривання з'єднань на фізичному рівні роботи обладнання (за запитами програми управління викликами);

- обробки сигналізаційної інформації;

- підтримки механізмів надання додаткових послуг;

- реєстрації та тарифікації (*registration and charging*), зокрема запис детальних даних про виклики *CDR* (*Call Detailed Record*);

- вимірювання навантаження (*traffic measurements*), зокрема вимірювання інтенсивності трафіка та запис даних з результатами вимірювань.

А також здійснюють функції серверів:

- системи попередньої оплати, що забезпечує можливість надання та тарифікацію послуг для користувачів, що зробили попередню оплату;

- інтегрованої системи повідомлень**,** що забезпечує безпосередній запис спеціально підготовлених повідомлень для інформування клієнтів, відтворення цих повідомлень за запитами

клієнтів або в широкомовному режимі, підтримку інтерактивного голосового меню.

Розглянуті вище групи прикладних застосувань іноді об'єднують загальною назвою "Функціональне ПЗ", оскільки воно безпосередньо задіяне в забезпеченні функціонування ТЛК-системи за основним призначенням. Функціональне ПЗ забезпечує підтримку функціональності як самого ТЛК-обладнання, так і підтримку заданих характеристик ТЛК-послуг. Це ПЗ на стадії експлуатації ТЛК-системи, як правило, завжди перебуває в активному стані. Проте функціональне ПЗ не завжди є доступним експлуатаційному персоналу. У випадках його невідповідної роботи доводиться звертатися до постачальників обладнання або їх представників.

Окрім функціонального, в структурі прикладного ПЗ маємо іншу групу прикладних застосувань вищого рівня ієрархії, що реалізують функції керування функціональними підсистемами ТЛК-системи – керування наданням послуг, трафіком, процедурами технічного обслуговування, підсистемою захисту від несанкціонованого доступу (НСД), білінговими процедурами тощо (див. *TMN*-модель керування, що регламентується, зокрема, стандартом *ISO 7498-4* та рекомендацією *ITU-T X.700*). Ці групи прикладних застосувань, як правило, входять до складу локального комплексу програм управління будь-яким активним елементом будь-якої сучасної ТЛК-системи. Однак в локальному варіанті вони забезпечують підтримку процесів управління лише в межах свого активного елементу. У більш розширених варіантах ці групи прикладних застосувань входять до складу ПЗ вузлу керування ТЛК-системою, якщо ця ТЛК-система являє собою багатовузлову мережу з централізованою системою керування. ПЗ централізованих систем керування не тільки здатне координувати сумісну роботу вузлів, але і виконувати функції віддаленого керування кожним окремим вузлом мережі (як в режимі віддаленого вузлу, так і в режимі термінального доступу). Так що відпадає необхідність в утриманні кваліфікованого персоналу на окремих вузлах.

Однак у даній лекції мова йде про спеціалізовані застосування, що забезпечують підтримку процедур адміністрування ресурсами

ТЛК-обладнання, зміст яких полягає у безпосередньому настроюванні параметрів прикладних систем на конкретні умови використання. Ці застосування являють собою теж комплекси прикладних програм, які, у принципі, мають адмініструвати як функціональне ПЗ, так і ПЗ системи керування ТЛК-системою. Однак програми настроювання функціонального ПЗ, як правило, в комплект поставок обладнання ТЛК-систем не входять, оскільки вважається, що функціональне ПЗ на проміжках часу між черговими актами модернізації систем (зокрема, в періоди між встановленням чергових версій ПЗ) не змінюється. Інша справа з адмініструванням ПЗ систем керування. Комплекси програм з адміністрування, що входять до складу прикладних застосувань, які підтримують функції керування елементами ТЛК-системи (або всією ТЛК-системою у цілому), знайшли широке застосування в експлуатаційній практиці. Як правило, комплекси програм з адміністрування – це прикладні застосування нижчого рівня ієрархії (див. рис.11.1). Якщо вони входять до складу груп застосувань вузлу керування ТЛК-системою, то завдяки їх використанню можливо здійснити адміністрування будь-якого елементу на будь-якому вузлі ТЛК-мережі. Комплекси програм з адміністрування, що входять до складу локальних комплексів програм управління окремими активними елементами мережі можливо використати для настроювання лише окремих елементів цієї мережі. Фактично з***міст процедур адміністрування*** програм керування полягає у безпосередньому настроюванні параметрів прикладних систем керування на реалізацію функцій керування ресурсами ТЛК-обладнання, які згідно *TMN*-моделі керування розділено на п’ять функціональних груп (див. лекцію №4):

1) керування конфігурацією параметрів ТЛК-обладнання та найменуванням (*Configuration Management*);

2) вияв та знешкодження збоїв та помилок у роботі ТЛК-обладнання (*Fault Management*);

3) забезпечення продуктивності та надійності роботи ТЛК-обладнання (*Performance Management*);

4) підтримка прийнятої політики забезпечення захисту інформаційних ресурсів ТЛК-системи (*Security Management*);

5) облік використаних ресурсів ТЛК-системи на визначених

інтервалах часу (*Accounting Management*).

Так, наприклад, програми адміністрування прикладних застосувань, що виконують функції управління конфігуруванням, входять до складу групи застосувань *Configuration Management*. Програми адміністрування застосувань, що здійснюють підтримку технічного обслуговування та ремонту обладнання, входять до складу групи застосувань *Fault Management*. Програми адміністрування застосувань, що здійснюють підтримку надання телекомунікаційних послуг та управління трафіком, входять до складу групи застосувань *Performance Management*. Програми адміністрування застосувань, що здійснюють підтримку механізмів захисту інформації, входять до складу групи застосувань *Security Management*. На кінець, програми адміністрування застосувань, що здійснюють облік використаних ресурсів ТЛК-системи та білінгових систем, входять до складу групи застосувань *Accounting Management*.

На жаль, проблематика управління (у т.ч., адміністрування) ресурсами ТЛК-обладнання не охоплена в достатній мірі стандартизацією. Тому структура прикладного ПЗ систем управління у складі обладнання різних ТЛК-систем суттєво різниться. Існує суттєва відмінність ПЗ різних ТЛК-систем і за іншими параметрами. Зокрема програми адміністрування різняться і за переліком реалізованих застосувань, і за змістом виконуваних функцій, і за ступенем автоматизації процедур адміністрування, і за зовнішнім виглядом інтерфейсів управління. Тому набуття практичних навичок роботи з ПЗ конкретної ТЛК-системи вимагає певних зусиль і потребує певного часу.

Інтерфейс між адміністратором та системою управління ТЛК-обладнанням має певні особливості, що полягають у наступному.

Для здійснення функцій *O&M* у невеликих за розмірами ТЛК-систем, як правило, використовують однотипний інтерфейс управління. У найпростіших випадках - це інтерфейс командної лінії *CLI* із застосуванням протоколу *telnet*, який найчастіше використовується в середовищі *Unix*-подібних ОС. Проте цей інтерфейс є найбільш вразливим з точки зору інформаційної безпеки. В пакетних мережах найбільш популярним вважається

GUI - графічний інтерфейс управління системою, зокрема Web-інтерфейс.

У великих за розмірами ТЛК-системах (особливо глобальних, гетерогенних та (або) мультисервісних) застосовують складну схему взаємодії адміністратора із підсистемою *O&M*, що базується на кількох типах інтерфейсів управління. Зазвичай у великих ТЛК-системах з підсистемою *O&M* одночасно працюють кілька груп адміністраторів із різними посадовими обов'язками та різними правами доступу до ресурсів цих систем. Одні адміністратори займаються підтримкою задач *Configuration Maintenance*, інші *QoS Maintenance*, а ще інші *Security Maintenance* тощо. Бажано, щоб потоки управлінської інформації, які генеруються цими групами адміністраторів, логічно не перетинались (щоб адміністратори не заважали один одному, щоб умисно або ненавмисно не втручались у сферу відповідальності інших адміністраторів і т. ін.). Тому для кожної групи адміністраторів застосовують окремий інтерфейс управління. Окрім того, з метою підвищення надійності управління бажано, щоб для здійснення відповідальних функцій *O&M* було можливим використати кілька різних інтерфейсів управління. Якщо вийде з ладу один тип інтерфейсу, то існувала б можливість задіяти інший тип інтерфейсу управління.

Приклад одного із варіантів розподілу функцій *O&M* між типами стандартних інтерфейсів управління наведено у табл.11.1.

Таблиця 11.1

Розподіл функцій *O&M* між стандартними інтерфейсами управління

Тип інтерфейсу управління	CLI	IPSEC	SNMP	WEB	FTP	NTP
Локальний доступ до керування парольною інформацією		x	x			
Віддалене керування парольною інформацією		x				
Доступ до індикаторів стану обслуговування			x	x		
Доступ до індикаторів стану обладнання			x	x		

Конфігурування параметрів послуг			x	x		
Конфігурування параметрів обладнання	x		x	x		
Синхронізація внутрішнього таймера			x	x		x
Віддалене керування парольною інформацією						
Встановлення статусу тривожних повідомлень			x			
Доступ до списку тривожних подій			x			
Фільтрування внутрішніх подій			x			
Обмін конфігураційними даними, апгрейт версій програмного забезпечення					x	
Керування скиданням та зберіганням даних					x	
Завантаження програмного забезпечення					x	

Як бачимо із табл.11.1, локальний доступ адміністраторів до керування парольною інформацією здійснюється або через незахищений інтерфейс за допомогою протоколу управління *SNMP* або через захищений інтерфейс, що створюється з використанням тунелювання , VPN та стеку протоколів IPSEC. Віддалений доступ до керування парольною інформацією здійснюється, як правило, в режимі віддаленого вузлу з використанням засобів захисту інформації.

Моніторинг якості функціонування обладнання та якості обслуговування (*Performance monitoring*) засновано на використанні індикаторів стану *KPI*, за допомогою котрих надається інформація про характеристики трафіка, поточні значення параметрів обладнання та обслуговування. Цей моніторинг є необхідним також для збору статистичної інформації в задачах прогнозування пульсацій трафіку. Доступ до індикаторів стану обладнання та обслуговування здійснюється згідно даних табл..11.1 через інтерфейси управління, що створені на базі

використання *SNMP* та (або) *WEB.*

Процедури конфігурування параметрів обладнання та послуг також виконуються за допомогою *SNMP* та (або) *WEB*. Наразі встановлення операційних параметрів активних елементів сучасних ТЛК-систем найбільш зручно здійснювати через *Web*-інтерфейс. Наприклад, обладнання сучасного крайового шлюзу розпізнає два типи користувачів: *admin* та *monitor*. Користувачі типу *monitor* мають можливість тільки переглядати дані у шлюзі, в той час як користувачі типу *admin* користуються широкими правами доступу до ресурсів шлюзу (конфігурування, адміністрування тощо). Зокрема, *Web*-інтерфейс, що реалізується ПЗ під назвою Voyager, забезпечує доступ до всієї он-лайнової інформації щодо кожної прикладної задачі, що виконується на шлюзі, включаючи он-лайнову підказку. Бажано, щоб адміністрування шлюзу (зокрема, первісна його інсталяція) здійснювалось також за допомогою текстових команд через послідовний інтерфейс *CLI.*

Користувач типу *monitor* за допомогою браузера має можливість отримати доступ до наступної статистичної інформації:

- статистика роботи протоколу маршрутизації;
- статистика роботи шлюзу (загальні відомості, дані щодо точки доступу, тривожні повідомлення);
- статистика системних ресурсів (період працездатного стану, помилки, файлова система);
- таблиця просування пакетів;
- статистика інтерфейсів;
- моніторинг апаратних засобів.

Користувач типу *admin* через *Web*-інтерфейс має можливість виконувати наступні конфігураційні задачі:

- конфігурування інтерфейсів;
- конфігурування процедур маршрутизації (за протоколами *BGP, OSPF, RIP, IGRP, DVMRP,* а також процедур *static routes, route aggregation, route distribution, routing options*);
- управління трафіком (списками доступу, формуванням трафіку тощо);
- конфігурування крайового шлюзу, включаючи призначення *IP*-адрес, встановлення сигналів тривоги, конфігурування статистичної інформації.

Згідно даних табл.11.1 тривожні повідомлення зазвичай транспортуються засобами протоколу *SNMP*. Обмін конфігураційними даними, у т.ч. апгрейти версій ПЗ, забезпечується засобами інтернет-протоколу *FTP*.

ТЛК-системи у своєму складі, як правило, мають годинники реального часу (таймери), що дозволяє синхронізувати процеси, що на них виконуються. Синхронізація цих годинників із зовнішнім годинником *NMS* здійснюється засобами протоколу *NTP*. Годинники реального часу можуть також конфігуруватися за допомогою протоколу *SNMP*.

11.2. Порядок здійснення процедур адміністрування

Порядок здійснення адміністрування ресурсами ТЛК-обладнання у найбільш узагальненому вигляді полягає в наступному. Як правило, ПЗ будь-якої ТЛК-системи має ієрархічну структуру. У головному вікні програмного комплексу інстальованої системи керування, найбільш ймовірно, буде відображатися меню з найменуваннями функціональних груп інстальованих прикладних застосувань. Бажано, щоб це меню було складено згідно *TMN*-моделі керування, тобто у ньому відображалися найменування п'яти функціональних груп задач керування. Але на практиці таке буває не завжди. Виробники ТЛК-обладнання у міру свого розуміння умов застосування своїх виробів реалізують власні концепції побудови інтерфейсу управління. Так що головне вікно може бути побудовано на основі класифікації прикладних систем, відмінної від *TMN*-моделі керування. У будь-якому разі основне (кореневе) меню графічного інтерфейсу управління ТЛК-системи, яка підлягає адмініструванню, буде містити перелік інстальованих груп прикладних застосувань. В залежності від змісту експлуатаційних робіт адміністратор завжди має можливість за допомогою "мишки" обрати для користування ту або іншу групу застосувань. Наприклад, він може обрати групу *Configuration Management* або *Fault Management* і т. ін.. Зробивши вибір тої чи іншої групи застосувань, адміністратор побачить на екрані системного монітору головне вікно обраної групи, а в ньому меню, що містить перелік найменувань конкретних застосувань, які інстальовані в межах цієї

групи, у т.ч. застосувань, що використовуються для адміністрування ТЛК-системи. Наприклад, обравши групу *Configuration Management*, у меню цієї групи адміністратор може побачити серед інших такі застосування як “Конфігурування вузлу керування”, “Конфігурування мережі”, “Конфігурування вузлового обладнання”, “Конфігурування елементів вузлу”, “Конфігурування інтерфейсів та користувачів” і т. ін.. Із назв застосувань можливо скласти уявлення про об’єкти адміністрування. Зробивши вибір конкретного застосування із обраної групи, наприклад “Конфігурування вузлового обладнання”, адміністратор побачить на екрані системного монітору головне вікно цього застосування, а в ньому меню, що містить перелік найменувань більш вузько функціональних (але більш конкретних) застосувань, що використовуються для адміністрування окремих вузлів ТЛК-системи. У меню застосування “Конфігурування вузлового обладнання” адміністратор може побачити серед інших такі конкретно-орієнтовані застосування як “Адміністрування загальних даних вузлу”, “Адміністрування доступу до вузлу”, “Адміністрування користувачів вузлу”, “Адміністрування послуг вузлу”, “Адміністрування вузлової сигналізації” тощо. На кінець, обравши конкретне застосування, яке у даний момент потрібне для роботи, наприклад “Адміністрування загальних даних вузлу”, адміністратор побачить на екрані монітору вікно цього застосування, що забезпечує взаємодію адміністратора з інструментарієм цього застосування. У вікні знайде відображення послідовність дій адміністратора (ініційовані ним команди, задані параметри і т. ін.) та реакція системи на ці дії. Зрозуміло, що адміністратор повинен знати користувацький інтерфейс даного застосування (відповідні команди, реакцію на ці команди тощо) та мати практичні навички роботи з адміністрування системи.

Наведена вище схема взаємодії адміністратора з прикладним ПЗ ТЛК-системи не є єдино можливою. Зокрема, головне вікно програмного комплексу керування ТЛК-системою може мати меню, що побудовано за топологічною ознакою, тобто в цьому меню будуть відображатися найменування вузлів та каналів зв’язку мережі. Вибравши із меню конкретний топологічний елемент мережі, адміністратор отримує можливість перейти до меню, в

якому відображаються функціональні групи застосувань, область дії котрих обмежена вибраним топологічним елементом мережі.

11.3. Адміністрування вузлу мережі

Адміністрування вузлу ТЛК-мережі полягає у послідовному виконанні відповідних процедур, які підтримуються відповідними прикладними застосуваннями нижнього рівня ієрархії, що інстальовані у складі програмного комплексу керування мережею (або у складі ПЗ окремого активного елементу, якщо мова йде про локальне управління цим елементом). Іншими словами, щоб виконати певну процедуру адміністрування, необхідно вибрати із меню прикладного застосування відповідної функціональності більш конкретні застосування (прикладні програми) необхідного призначення.

Наприклад, для адміністрування вузлу телефонної мережі необхідно у меню вибрати бажаний вузол та застосування, що призначені:

- для адміністрування програм управління конфігурацією вузлу (із групи *Configuration Management*);
- для управління процедурами діагностики обладнання (із групи *Fault Management*);
- для управління трафіком (із групи *Performance Management*);
- для перегляду довідника з експлуатації (із групи *Performance Management*);
- для управління дозволами на роботу з окремими застосуваннями (із групи *Security Management*);
- для адміністрування даних в системі обліку використаних ресурсів (із групи *Accounting Management*);
- для управління ТЛК-системою.

Можуть знайти використання й інші застосування, наприклад для адміністрування графіків передавання і узгодження топологічних даних.

Для адміністрування вузлу керування телефонною мережею необхідно у меню вибрати найменування вузлу керування та наступні застосування:

- «Конфігурування вузлу керування», яке дозволяє встановлювати сервер бази даних вузлу керування, адмініструвати

елементи мережі, управляти параметрами системи збору даних про використані мережні ресурси, задавати параметри синхронізації станційних процесів тощо;

- «Управління розкладом передачі», яке дозволяє управляти розкладом передачі різних видів даних (тарифні дані, дані щодо виконання додаткових послуг, дані щодо аварійних сигналів тощо) із телекомунікаційного вузлу у вузол керування;

- «Конфігурування інтерфейсів відкритого типу», яке дозволяє конфігурувати систему інтерфейсів відкритого типу та адмініструвати користувачів, котрим забезпечується доступ до системи через ці інтерфейси;

- «Управління конфігурацією системи», яке дозволяє виконувати із вузлу керування адміністрування інших вузлів мережі – апаратних засобів, загальних даних, доступів, даних абонентів, додаткових послуг, маршрутизацію викликів, систем сигналізації;

- «Управління діагностикою», яке дозволяє виконувати адміністрування поточних випробувань, випробувань за запитами та результатів вимірювань;

- «Контроль за аварійними сигналами» (*Alarm Monitoring*), яке дозволяє виконувати перегляд аварійних сигналів у телекомунікаційних вузлах, системах електроживлення, вузлах керування, а також архівних даних за цими сигналами;

- «Адміністративне управління тарифікацією та реєстрацією даних обліку вартості телефонних розмов», яке дозволяє адмініструвати тарифні дані, передавати та оброблювати записи детальних даних щодо зроблених викликів (*Call Detailed Record - CDR*) і тарифних лічильників, накопичувати *CDR* на носіях даних, а також передавати дані у білінгову систему та забезпечувати їхній захист;

- «Управління робочими характеристиками», яке дозволяє адмініструвати вимірювання та накопичення статистичних даних, а також показувати результати, що отримані після вимірювань на абонентських комплектах, групах визначених послуг, з'єднувальних лініях тощо;

- «Управління безпекою», яке дозволяє або забороняє доступ до прикладних застосувань;

- «Управління системою», яке дозволяє адмініструвати основні дані вузлів, адмініструвати мережу керування, виконувати інсталяцію ПЗ вузлів, створювати копії баз даних та даних про конфігурацію мережі, виконувати процедури узгодження баз даних, підготовлювати план нумерації, змінювати нумерацію та управляти програмою відстеження викликів. (Нагадаємо, що план нумерації – це набір правил, що визначає, яким чином треба створювати телефонні номери).

11.4. Конфігурування характеристик обладнання

Мається на увазі встановлення певним чином обраної конфігурації параметрів обладнання, режимів його роботи, функціональних можливостей, найменувань об'єктів, ідентифікаторів суб'єктів тощо. От же, конфігурування параметрів ТЛК-обладнання (*Configuration Maintenance*) будемо розглядати як одну з функціональних груп задач експлуатації.

Розробники сучасного ТЛК-обладнання намагаються зробити його багатофункціональним, багаторежимним, побудованим за модульним принципом. Це забезпечує можливість його використання у широкому колі прикладних застосувань, які в багатьох випадках суттєво відрізняються умовами функціонування. Тому ще до введення обладнання в експлуатацію необхідно його характеристики (параметри, режими, функції) настроїти на конкретні умови використання. Процес настроювання характеристик обладнання з метою отримання бажаної структури його функціональних можливостей називається конфігуруванням.

Конфігуруванню зазвичай підлягають: як апаратні, так і програмні засоби, що входять до складу експлуатованого ТЛК-обладнання; як окремі елементи обладнання різного ступеню агрегації (модулі, блоки, вузли, тобто типові елементи заміни в обладнанні), окремі макро-елементи вузлового обладнання (комутатори, маршрутизатори, сервери і т. ін.), так і уся багатовузлова ТЛК-система (мережа) у цілому. Конфігуруванню можуть підлягати і окремі функції, послуги і функціональні підсистеми, засоби реалізації котрих розосереджені по різним елементам обладнання.

Розрізняють процедури первісної інсталяції конфігурації

обладнання, процедури поточного (оперативного) конфігурування та процедури переінсталяції конфігурації обладнання під час його модернізації.

Цілі та зміст процедур поточного конфігурування, що виконуються на стадії експлуатації ТЛК-обладнання, суттєво відрізняються від цілей та змісту первісного конфігурування параметрів, що виконується на стадії уведення обладнання в експлуатацію, а також від процесів переінсталяції конфігурації обладнання під час його модернізації.

На стадії уведення обладнання в експлуатацію здійснюється **первісна інсталяція** програмних та апаратних засобів ТЛК-системи та конфігурування параметрів таким чином, щоб її характеристики повністю відповідали положенням та умовам проектної документації на цю систему і враховували конкретні умови її використання на існуючій або створюваній ТЛК-мережі.

На стадії експлуатації будь-якої ТЛК-системи існує необхідність в оперативних змінах **поточної конфігурації** штатних програмно-апаратних засобів ТЛК-системи з тим, щоб ця конфігурація адекватно відображала поточні вимоги користувачів і персоналу до кількості та якості послуг, що надаються системою. А ці вимоги постійно змінюються у реальному часі. Процес поточного (оперативного) керування конфігурацією, як правило, не зачіпає системних компонентів обладнання і, тому, може здійснюватися у фоновому режимі роботи цього обладнання, тобто без призупинки його функціонування за основним призначенням.

На стадії експлуатації ТЛК-обладнання час від часу може підлягати модернізації. Під час модернізації зазвичай виконується **переінсталяція обладнання** і, отже, виникає потреба у його реконфігуруванні. У випадках, коли реконфігуруванню підлягають і системні компоненти ТЛК-системи, то доводиться призупиняти її роботу за основним призначенням.

Як приклад розглянемо процедуру конфігурування вузлу, в якому розміщено обладнання цифрової системи комутації телефонних каналів. Для здійснення цієї процедури використаємо застосування “Адміністрування конфігурації вузлу“, що входить до складу групи застосувань *Configuration Management*. Головне вікно цього застосування містить меню з найменуваннями застосувань

конкретного призначення більш низького рівня ієрархії, а саме (див. рис.11.2):

- застосування *Global* для адміністрування загальних даних вузлу;
- застосування *Access* для адміністрування доступів;
- застосування *Subscriber* для адміністрування бази даних абонентів (включаючи дані про додаткові послуги, що вони отримують);
- застосування *Routing* для маршрутизації викликів;
- застосування *Signalling* для адміністрування систем сигналізації.

Розглянемо можливості кожного із вищевказаних застосувань.

Меню *Global*. Команди у цьому меню призначені для адміністрування даних, що відносяться до цього вузлу у цілому, а саме:

- загальні дані про вузол;
- дані про апаратні засоби вузлу;
- дані про джерела синхронізації;
- дані про послуги, що є загальними для усіх користувачів.

Рис.11.2. Склад застосування “Адміністрування конфігурації вузлу“

Меню *Access*. Команди у цьому меню призначені для адміністрування параметрів фізичних абонентських портів, а також створення або розривання взаємоз`єднань між абонентськими портами та абонентськими номерами. Кожному цифровому або аналоговому порту (зокрема, підключеному до мережі

телефонному апарату) можливо надати кілька абонентських номерів.

Меню *Subscriber*. З використанням цього меню можливо записувати, змінювати та видаляти дані про абонентів (оскільки нові абоненти підключаються до мережі, а деякі старі з різних причин відключаються від неї).

Кожний абонентський запис може містити наступні дані:

- ідентифікатор вузлу, в зоні обслуговування котрого знаходиться абонент;
- абонентський номер абонента;
- тип основної послуги, яку отримує абонент (наприклад, доступ до міської телефонної мережі загального користування);
- модуль обладнання, в якому знаходиться порт, що зв'язаний з абонентським номером (щоб при необхідності його було легко знайти персоналу);
- фізичний порт, з яким з'єднується даний абонентський номер;
- набір додаткових послуг абоненту (наприклад, переспрямування виклику, конференцзв'язок, зворотний довиклик тощо – додаткових послуг може бути кілька десятків);
- вимірювальна група, до якої підключено абонента;
- дані абонента щодо використаних ним ресурсів.

Меню *Routing*, що застосовується для адміністрування механізмів маршрутизації з'єднань. Щоб здійснювати таке адміністрування, необхідно мати уяву про топологію телефонної мережі та реалізований на комутаційному вузлі (тобто, на АТС) алгоритм маршрутизації.

Припустимо, що маємо фрагмент мережі, що показаний на рис.11.3.

На рис.11.3 показані мережні з'єднання комутаційного вузлу. Від нього до інших вузлів реалізовано чотири напрямки. У складі першого напрямку (до вузлу №1) маємо дві лінії зв'язку. Кожен із інших напрямків має лише одну лінію. Лінії позначені шестизначними номерами виду xxxxxx. Лінії перших двох напрямків ідентифікуються однією закріпленою за лінією цифрою. Лінія третього напрямку ідентифікується трьома закріпленими цифрами (322xxx), а четвертого – двома цифрами (32xxxx).

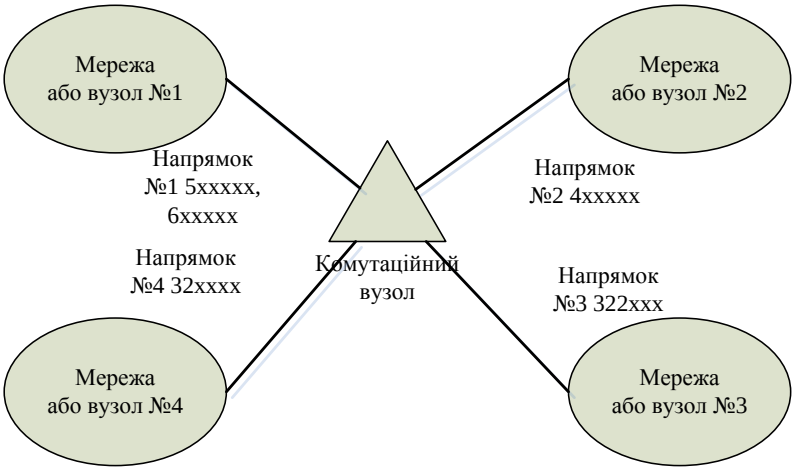


Рис.11.3. Приклад фрагменту телефонної мережі для пояснення маршрутизації

Маршрутизація виконується на основі аналізу перших прийнятих цифр, що закріплені за відповідними лініями зв'язку, тобто на основі префіксів. (Префікс це одна із частин послідовності цифр, що набирає абонент в процесі встановлення з'єднання. Префікс використовується для маршрутизації викликів). Префікси зв'язуються з даними про кінцеві точки з'єднань (тобто, з пунктами призначення викликів). Визначаються категорії пунктів призначення (зокрема, такі категорії як порти місцевих абонентів, або порти за межами даного вузлу, або коди процедур, що знаходяться під управлінням абонента під час надання якоїсь абонентської послуги, або спеціальні можливості вузлу і т. ін.).

В процесі адміністрування механізмів маршрутизації адміністратор задає параметри кінцевих точок з'єднань (пунктів призначення), що ідентифікуються відповідними кодовими словами – префіксами. С префіксом зв'язані наступні параметри:

1) Зона тарифікації — це кодове слово, що визначає рівень тарифу для початкової (рос., - исходящей) точки з'єднання. Рівень тарифу встановлюється у відносних одиницях, оскільки конкретні платежі, які здійснюють абоненти, залежать від ціни одиниці, яка, у свою чергу, залежить від багатьох факторів, що враховуються

засобами білінгової системи. При визначенні префіксу також визначаються можливі реакції кінцевої АТС на запити щодо з'єднань, які можуть вплинути на роботу вихідної (рос., - исходящей) станції, що ініціює з'єднання, і тому мають бути враховані під час адміністрування. А саме, необхідно вказати, яка буде реакція вихідної станції на наступні запити кінцевої станції:

- номер абонента, який ініціював виклик;
- зворотне передавання номеру переадресування;
- повторне передавання префіксу;
- добір номера абонента (частотним способом).

Для кожної кінцевої точки вказуються відповідні часові обмеження (тайм-аути), у рамках котрих мають здійснюватися відповідні дії. Якщо ці дії в рамках тайм-аутів не встигли завершитися, то процес обробки виклика припиняється. Розрізняють наступні тайм-аути:

-проміжок часу на встановлення з'єднання;

-проміжок часу на чекання відповіді абонента;

-тривалість розмови;

-тривалість сигналу зайнято при невдалій спробі з'єднання.

Завершення процесу встановлення з'єднання також може програмуватися. Ознакою закінчення встановлення з'єднання може бути:

-відповідний сигнал управління;

-тайм-аут після передавання сигналу;

-певна логічна комбінація етапу з'єднання та останнього сигналу.

Вищеназвані дії адміністратора можуть розповсюджуватися на комбінації пунктів призначення та обраних маршрутів.

2) Маршрут — набір можливих шляхів встановлення з'єднання з кінцевою точкою (з пунктом призначення). У процесі адміністрування механізмів створення маршруту необхідно визначити:

- яка кількість знаків префіксу має бути задіяна для визначення маршруту;
- після якої цифри набраного номеру можливо починати встановлення з'єднання;
- яку кількість знаків від початку набраного номеру слід

пропустити для встановлення з'єднання;

- з якого знака слід почати починати передавання інформації;
- у випадку термінової заміни номеру на ділянці маршруту вказати, який саме знак слід замінити для продовження з'єднання.

3) Напрямок або група каналів (ліній). Характеристики групи каналів або ліній, які безпосередньо з'єднують сусідні АТС, задаються адміністратором. Напрямок характеризується:

- фізичним середовищем передавання (аналогові лінії, цифрові канали);
- типом сигналізації (регістрова, лінійна тощо) ;
- режимом роботи напрямку (вихідні, вхідні, двосторонні) та пріоритетом роботи двосторонніх ліній.

Якщо існує можливість перенавантаження напрямку, то адміністратор тимчасово на певний період часу може встановити обмеження на використання певного виду зв'язку (тобто, встановити обмеження на використання місцевого, міжміського або міжнародного зв'язку). Можливо встановлення обмежень на використання комбінацій видів зв'язку або встановлення, навпаки, дозволів на використання певних видів зв'язку, тобто відкриття напрямку для певного виду зв'язку. У загальному випадку напрямок може складатися із окремих каналів, кожен з котрих може адмініструватися окремо.

Адміністратор може задати також метод пошуку незанятих каналів при встановленні з'єднань:

- в порядку зростання номеру каналу у напрямі;
- в порядку убування номеру каналу у напрямі;
- поточний номер каналу плюс одиниця після кожного вибору каналу;
- метод випадкового пошуку.

Перші два методи називають пошуком з постійним пріоритетом.

4) Канал (лінія) — це пристрої та лінії, які забезпечують створення фізичного середовища передавання інформації між АТС. Вони мають ті ж самі характеристики, що і напрямки. Для кожного каналу (або лінії) можуть призначатися відповідні тайм-аути. Ці тайм-аути обмежують або інтервал встановлення з'єднання, або загальний інтервал часу зайняття лінії у випадках неотримання сигналу відповіді.

Меню ***Routing*** об'єднує команди, за допомогою яких здійснюється адміністрування наступних об'єктів:

-префікси;

-пункти призначення;

-пріоритети та значення критеріїв, що впливають на вибір маршрутів;

-дані маршрутів;

-дані про групи з'єднувальних ліній;

-дані про з'єднувальні лінії;

-дані оператора зв'язку.

Щоб мати уявлення про послідовність дій адміністратора під час конфігурування ТЛК-обладнання, наведемо в якості прикладу порядок конфігурування АТС для типових умов її використання.

1. Увід коду станції та коду місцевої телефонної мережі.

2. Створення імені станції та його прив'язка до коду місцевої мережі.

3. Визначення діапазону телефонних номерів підмережі абонентського доступу (тобто, визначення плану нумерації).

4. Створення користувача (адміністратора) з правом доступу до підсистеми управління станцією.

5. Увід паролю адміністратора.

6. Конфігурування характеристик блоків станції.

7. Конфігурування характеристик модулів станції.

8. Активізація модулів.

9. Створення абонентських номерів (тобто, здійснення відповідних записів з даними про абонентські номери).

10. Призначення додаткових класів послуг.

11. Присвоєння абонентським портам абонентських номерів.

12. Прописування внутрішньої маршрутизації.

13. Прописування зовнішньої маршрутизації.

14. Увід інформації щодо прийнятих обмежень, заборон та умов функціонування обладнання.

У базових станціях систем мобільного зв'язку, як правило, реалізуються функції управління конфігурацією. Якщо будь-який елемент добавляється або виключається із поточної конфігурації апаратних засобів станції, то інформація щодо цієї події вноситься у відповідну базу даних. Якщо у поточній конфігурації виявляється

несанкціонований елемент, то виробляється відповідне повідомлення для системи сповіщення.

11.5. Адміністрування систем сигналізації

Для адміністрування характеристик систем сигналізації, що робиться зазвичай під час інсталяції обладнання ТЛК-системи, може бути використано окреме застосування, спеціально створене для виконання цього виду робіт, або використано застосування "Адміністрування конфігурації вузлу", що входить до складу групи застосувань *Configuration Management*. Через меню *Signalling* цього застосування можливо задіяти команди, що слугують для записів, змінювань та видалення параметрів систем сигналізації та відповідних інтерфейсів, які планується використати в телефонній мережі. Технологія адміністрування систем сигналізації подібна технології конфігурування параметрів вузлу комутації, що була розглянута у попередньому прикладі.

11.6. Адміністрування білінгової системи

Білінгова система – це програмний комплекс, що призначений для здійснення обліку використаних клієнтами ресурсів ТЛК-системи, кількості та якості послуг, які отримані клієнтами, а також для розрахунку та списання коштів із рахунків клієнтів у відповідності з прийнятими тарифами телекомунікаційної компанії.

Завдання, які вирішує білінгова система, полягають в наступному:

-накопичення інформації про кількість та якість отриманих клієнтами послуг (так званий акаутінг);

- розрахунки обсягу оплат, що мають зробити клієнти, у відповідності із прийнятими тарифними планами;

-забезпечення процедур поповнення рахунків клієнтів;

-автентифікація та авторизація абонентів, що здійснюють оплату використаних ресурсів ТЛК-системи;

-контроль кількості коштів на рахунках абонентів та списання коштів у відповідності із прийнятими тарифами;

-інформування клієнтів про поточний стан їхніх рахунків;

-внесення змін у тарифи;

-представлення статистичних даних у розрізі білінгових операцій;

-оформлення вихідних даних для бухгалтерського обліку.

На практиці знайшла застосування велика кількість різних білінгових систем. Вибір конкретної системи в конкретних умовах використання залежить від багатьох факторів, насамперед від масштабів ТЛК-системи, кількості її вузлів, кількості клієнтів, характеру та різноманітності послуг, що надаються системою, ступеню автоматизації та інтелектуалізації білінгових процесів, різноманіття та принципів побудови тарифних планів тощо.

У великих ТЛК-мережах ПЗ білінгової системи, зазвичай, розміщають у Центрах обробки білінгової інформації (*Billing Centre, CCBS*), які зв'язують відповідними транспортними каналами із серверами вузлового обладнання, де накопичується інформація у вигляді так званих білінгових записів *CDR* (читається як *Charging Data Record*, а не *Call Detailed Record* як це прийнято у телефонії). Файли із білінговими записами *CDR* з даними щодо кількості та якості отриманих клієнтами послуг (*Charging files*) передаються із цих серверів до центрів *CCBS* з використанням або незахищеного *FTP*-сервісу із стеку протоколів *TCP/IP* (якщо транспортування даних здійснюється через спеціально виділені канали зв'язку), або створюється захищений транспортний тунель з використанням технології *VPN* (*Virtual Private Networks*) і захищеного протоколу *GTP´* (*Gateway Transport Protocol*) над стеком *TCP/IP* (якщо транспортування даних здійснюється через незахищене середовище).

Для адміністрування параметрів білінгової системи, як правило, використовують окреме застосування, спеціально створене для виконання цього виду робіт. Технологія адміністрування білінгової системи подібна технології конфігурування параметрів вузлу комутації, що була розглянута у попередньому прикладі. Зокрема, встановлення операційних параметрів білінгової системи найбільш зручно здійснюється через Web-інтерфейс. Система розпізнає два типи користувачів: *admin* та *monitor*. Користувачі типу *monitor* мають можливість тільки переглядати дані у *CCBS*, в той час як користувачі типу *admin* користуються широкими правами доступу до ресурсів білінгової системи (конфігурування, адміністрування

тощо). Web-інтерфейс, що реалізується ПЗ, забезпечує доступ до всієї он-лайнової інформації щодо кожної прикладної задачі, що виконується у білінгової системі, включаючи он-лайнову підказку. Адміністрування білінгової системи за допомогою текстових команд (зокрема, первісна його інсталяція) можливо також здійснювати через послідовний інтерфейс *CLI*.

Контрольні питання до одинадцятої лекції

1. Які групи функцій *O&M* Ви знаєте ?
2. Яким чином побудовано інтерфейс управління окремим елементами ТЛК-систем ?
3. Надайте визначення терміну “адміністрування“.
4. Надайте характеристику системі централізованого керування ТЛК-системою.
5. Які переваги та недоліки має система централізованого керування у порівнянні із локальною системою керування ?
6. Надайте характеристику режиму віддаленого управління.
7. Надайте характеристику протоколу *telnet*.
8. Яка типова структура ПЗ сучасної ТЛК-системи ?
9. Що таке функціональне ПЗ ?
10. Які основні групи прикладних застосувань типової телефонної комутаційної системи Ви знаєте ?
11. У чому полягає зміст процедур адміністрування програм керування ?
12. Які особливості інтерфейсу між адміністратором та системою управління ТЛК-обладнанням ?
13. Наведіть порядок здійснення процедур адміністрування.
14. Яким чином здійснюється адміністрування вузлу мережі ?
15. Яким чином здійснюється конфігурування характеристик обладнання ?

ЛЕКЦІЯ №12. ПІДТРИМКА НАДІЙНОСТІ ФУНКЦІОНУВАННЯ ОБЛАДНАННЯ

Розглядаються наступні питання:

Лекційне заняття

12.1. Загальна характеристика задач підтримки надійності функціонування обладнання

12.2. Показники експлуатаційної надійності обладнання

12.3. Умови та порядок контролю показників надійності

12.4. Методи та засоби резервування програмно-апаратних елементів обладнання

12.5. Архівація програмного забезпечення та баз даних

12.6. Антивірусне програмне забезпечення

Самостійне заняття. Вимірювання параметрів радіочастотних каналів передавання інформації

12.1. Загальна характеристика задач підтримки надійності функціонування обладнання

Актуальність вирішення задач підтримки надійності функціонування ТЛК-обладнання. Сучасне ТЛК-обладнання функціонує цілодобово у реальному часі та призначене, в багатьох випадках, для технічної підтримки надання телекомунікаційних послуг величезній кількості клієнтів. Затримки в обслуговуванні цих клієнтів або навіть незначне погіршення якості їхнього обслуговування можуть призвести до значних економічних збитків для телекомунікаційних операторів та провайдерів інформаційних послуг. Не говорячи вже про ТЛК-обладнання спеціального призначення: відмови в роботі цього обладнання можуть призвести до катастрофічних наслідків. Тому забезпеченню високої надійності функціонування обладнання (*Reliability*) у сфері телекомунікацій приділяється особлива увага.

Методи та механізми забезпечення надійності роботи ТЛК-обладнання базуються на моделях та методичних підходах, що розглядалися у рамках навчальної дисципліни «Теорія надійності». Знання основних результатів цієї теорії є необхідною передумовою успішного вирішення експлуатаційних завдань, що пов’язані із забезпеченням надійності функціонування ТЛК-обладнання. Зокрема, необхідно знати основні поняття та визначення, що

використовуються в теорії надійності (такі як безвідмовність, відновлюваність, живучість, довговічність, збій, відмова, види відмов тощо), основні показники надійності (такі як наробіток на відмову, ймовірність безвідмовної роботи, інтенсивність відмов, коефіцієнт готовності і т. ін.) та основні аналітичні вирази, що зв'язують ці показники (експоненціальний закон надійності, формули для розрахунків показників надійності тощо). Однак на цьому матеріалі зупинятися не будемо, але зазначимо наступне.

Особливості вирішення проблем підтримки надійності ТЛК-обладнання під час його експлуатації.

1) ТЛК-обладнання, як правило, відноситься до класу **відновлювальних систем**, тобто його експлуатація у часі являє почергову зміну інтервалів працездатності та простоїв обладнання. У періоди простоїв здійснюється відновлення працездатності (тобто, ремонт), обладнання знов працює до чергової відмови і т.д. Тому під час вирішення проблем надійності ТЛК-обладнання слід користуватися методологічними підходами та показниками надійності, що розроблені в теорії надійності для відновлювальних об'єктів. Зокрема, доцільно вважати, що ТЛК-обладнання під час свого функціонування формує потік відмов, який характеризується параметром потоку відмов $\lambda(t)$, і цей потік відповідає умовам:

- ординарності (коли ймовірність появи двох і більше відмов в один і той же момент є нехтовно малою);
- стаціонарності (коли ймовірність появи k відмов не залежить від часу, а є функцією довжини інтервалу спостереження Δt і числа відмов k);
- відсутності післядії (коли для будь-яких двох інтервалів спостереження кількість відмов в одному з них не залежить від кількості відмов в іншому).

Окрім того, доцільно вважати, що щільність розподілу наробітку між відмовами підкоряється експоненціальному закону і, от же, можливо рахувати, що $\lambda(t) = \lambda = 1/T_0$, де T_0 - наробіток для сталого процесу експлуатації (після періоду приробітку нового обладнання). За таких умов ймовірність безвідмовної роботи $P(t)$, щільність розподілу відмов $f(t)$ та час наробітку на відмову T_0 відповідно дорівнюють:

$$P(t) = exp(-\lambda t);$$

$$f(t) = \lambda \exp(-\lambda t);$$
$$T_0 = 1/\lambda. \quad (12.1)$$

Вище наведено імовірнісне визначення наробітку на відмову та інших показників надійності, що при вирішенні експлуатаційних завдань має теоретичне значення. На практиці більш придатною є статистична оцінка цих показників, зокрема

$$T_0 = (1/n)\sum_{i}^{n} t_{pi} \quad (12.1)$$

де n – кількість відмов за відповідний період спостереження, а t_{pi} - час наробітку на i-ту відмову. Статистичне оцінювання показників надійності завжди можливо організувати під час експлуатації ТЛК-системи.

2. На етапі експлуатації ТЛК-системи навряд чи виникне необхідність у розрахунках надійності елементів ТЛК-обладнання або усієї системи у цілому. (Такі розрахунки робляться, як правило на етапах конструювання та виготовлення обладнання системи). На стадії експлуатації більш важливо, щоб експлуатаційний персонал досконально знав методи забезпечення надійності в процесі експлуатації обладнання і володів практичними навичками настроювання та підтримки працездатності механізмів реалізації цих методів.

Зокрема, персонал має добре орієнтуватися у різноманітних методах цілеспрямованого уведення у склад обладнання **ресурсної надлишковості** (апаратної, програмної або інформаційної). Ресурсна надлишковість хоч і збільшує капітальні та експлуатаційні витрати телекомунікаційних операторів, проте надає змогу підтримувати безвідмовність та відновлюваність обладнання на прийнятних рівнях і, отже, забезпечувати прийнятний рівень доступності ТЛК-послуг для користувачів.

3. Одним із найбільш розповсюджених методів забезпечення надійності, що базується на уведенні у склад обладнання апаратної та (або) програмної надлишковості, є **резервування обладнання**.

Структура високонадійного безвідмовного ТЛК-обладнання, як правило, передбачає можливість резервування (зокрема, дублювання) роботи типових елементів заміни - ТЕЗів (апаратних

модулів - плат, слотів, блоків, касет, кошиків і т. ін. та (або) програмних модулів, програм у цілому і, навіть, цілих комплексів програм). У відповідальних випадках резервуванню підлягають усі макро-елементи ТЛК-системи – мультиплексори, канали зв'язку, вузлові комутатори, маршрутизатори, шлюзи, системні сервери, контролери тощо, у т.ч. макро-елементи програмного забезпечення – операційні системи, технологічні бази даних, спеціалізовані програмні комплекси тощо. Ступінь охоплення елементів ТЛК-системи резервуванням в залежності від умов використання обладнання може бути різною – від пасивного (холодного) резервування ТЕЗів (коли вони зберігаються у зручному місці у відключеному стані) до організації режиму гарячого резервування з автоматичним відключенням проблемного ТЕЗу від працюючого обладнання та включенням замість нього дублюючого справного елементу. Зрозуміло, що гаряче резервування передбачає необхідність організації паралельної роботи основного (активного) та резервного (гарячого) елементів обладнання таким чином, щоб не втрачати час на уведення в дію резервного елементу в момент, коли визначилась подія, що пов'язана із втратою працездатності активного елемента. У критично важливих випадках коефіцієнт резервування може перевищувати 2, тобто у склад обладнання може включатися більше, ніж два аналогічних ТЕЗа – їх може бути три і, навіть, чотири. Таке багатократне резервування елементів обладнання має широке застосування в сучасних мережах мобільного зв'язку. Дублюються не тільки ТЕЗи, але і порти обладнання, що надає змогу заміщати несправні канали зв'язку, перенаправляти потоки інформації в обхід несправних ділянок мережі або утворювати кільцеподібні мережні структури, котрі у ряді випадків можуть забезпечувати потрібні характеристики надійності найбільш економним шляхом.

4. Окрім резервування, використовують й інші методи забезпечення високої надійності роботи ТЛК-обладнання. Якщо, наприклад, у склад ТЛК-системи входять кілька однотипних елементів, що виконують однакові функції, то нерідко на їхній основі створюють розподілену структуру таким чином, щоб вони утворили певний **ресурсний пул**. У цьому випадку, коли виходить із ладу будь-який із цих елементів, то виконання його функцій

беруть на себе інші працездатні елементи, що входить до складу утвореного пулу. Зрозуміло, що у цьому випадку коефіцієнти завантаження цих елементів мають бути меншими, ніж одиниця, інакше створення ресурсного пулу втрачає сенс.

5. До особливостей сучасних ТЛК-систем слід віднести їхню **гнучкість щодо відмов як програмних, так і апаратних елементів**. Вимоги до показників їхньої надійності є настільки високими, що у разі відмови одного якогось або, навіть, цілої групи елементів обладнання робота цих систем не повинна призупинятися. Обладнання має бути не тільки безвідмовним (тобто, з великими інтервалами наробітку на відмову), але і самовідновлювальним (з автоматичним і швидким відновленням роботи після відмови). У сучасні зразки ТЛК-обладнання вмонтовані механізми самовідновлення після збоїв та відмов, у т.ч. і після відмов в роботі програмного забезпечення.

6. У процесі експлуатації ТЛК-обладнання особливу увагу приділяють забезпеченню **надійності функціонування програмного забезпечення (ПЗ)**. Небезпека відмов ПЗ полягає у тому, що на відміну від відмов апаратних елементів відмови ПЗ часто неможливо виявити відразу. Ці відмови виявляються пізніше, коли ПЗ під час вирішення якоїсь прикладної задачі стикається з певними труднощами. Наприклад, у випадку виникнення помилки під час виконання якої-небудь програми, що здійснює управління розподілом пам'яті буферних пристроїв, може відбутися зациклення пакетів, некоректна обробка черг тощо. Щоб цього уникнути, для виявлення помилок у ПЗ на практиці широко використовуються різноманітні методи уведення інформаційної надлишковості, зокрема коди з виявленням та корекцією помилок. Однак основним методом підвищення надійності ПЗ слід вважати резервування його елементів.

7. Для забезпечення високої надійності роботи обладнання застосовують цілу низку **заходів організаційно-технічного характеру**, що підтримують стабільність характеристик середовища, в якому функціонує обладнання: температуру, вологість повітря, високоякісне заземлення, стабільне електропостачання, а також параметри систем забезпечення фізичної безпеки роботи обладнання (від пожеж, ударів блискавок,

несанкціонованого доступу в приміщення, де розташоване обладнання, не уповноважених осіб тощо).

12.2. Показники експлуатаційної надійності обладнання

***P(T_N)* - ймовірність безвідмовної роботи** ТЛК-обладнання на проміжку часу T_N. Визначається згідно з ДСТУ 2860-94 як ймовірність того, що в межах заданого наробітку T_N відмови мережного обладнання не настануть. Цей показник щодо телекомунікаційного обладнання не нормується, але може обчислюватись (точніше, оцінюватись у статистичному сенсі) з метою отримання даних щодо надійності виробів окремих постачальників обладнання. На стадії експлуатації ТЛК-обладнання цей показник майже не використовується.

***MTBF (Mean Time Between Failures)* – середній час між відмовами.** Більш точна назва: середній час наробітку між відмовами $T_{0сер}$. Характеризує рівень надійності обладнання як такого без урахування впливу на надійність цього обладнання процесів технічного обслуговування та ремонту. Визначається згідно з ДСТУ 2860-94. Цей показник широко використовується в експлуатаційній практиці, але щодо телекомунікаційного обладнання не нормується. Використовується для визначення коефіцієнту готовності, який дає більш інтегральну оцінку рівню надійності обладнання.

***MTTR (Mean Time To Repair)* – середній час відновлення (ремонту) після відмови обладнання.** Характеризує функціональність обладнання з точки зору забезпечення відновлення обладнання після відмов та рівень досконалості служб технічного обслуговування та ремонту (рівень організації робіт з технічного обслуговування та ремонту обладнання, кваліфікація персоналу, ступінь досконалості інструментальних засобів для ремонту тощо). Визначається згідно з ДСТУ 2860-94. Використовується для визначення коефіцієнту готовності.

***MTTR*$_{max}$ –** максимально припустиме значення *MTTR*. Цей показник, як правило, нормується.

***K*$_г$ - коефіцієнт готовності обладнання.** Комплексний показник експлуатаційної надійності мережного обладнання, який

характеризує співвідношення між *MTTR* та *MTBF* згідно з формулою:

$$K_г = MTBF / (MTBF + MTTR). \qquad (12.3)$$

Визначається згідно з ДСТУ 2860-94. Цей показник називають комплексним, оскільки він характеризує як рівень надійності самого обладнання (з урахуванням усіх механізмів забезпечення надійності, які у ньому реалізовані, а також заходів з підтримки цієї надійності), так і рівень засобів і заходів, що відновлюють роботу цього обладнання після відмов. Дійсно, із (12.3) витікає: якщо $MTTR \to 0$ (якщо маємо ідеальну службу відновлення обладнання), то $K_г \to 1$. У той же час, якщо $MTBF \to \infty$ (якщо маємо ідеальну надійність обладнання), то незалежно від рівню відновлюваності обладнання також $K_г \to 1$. За малих значень *MTBF* та за великих значень *MTTR* коефіцієнт готовності обладнання $K_г \to 0$.

$K_г^{min}$ **- мінімально припустиме значення коефіцієнту готовності.** Цей показник, як правило, нормується. Для сучасного інфраструктурного обладнання глобальних пакетних мереж та систем мобільного зв'язку значення цього коефіцієнту досягає, як кажуть, «чотирьох дев'яток», тобто $K_г \to 0{,}9999$. Деякі постачальники обладнання стверджують, що рівень надійності їхніх виробів забезпечує досягнення $K_г \to 0{,}99999$.

$K_П$ **- коефіцієнт простою обладнання.** Визначається за формулою:

$$K_П = 1 - K_г. \qquad (12.4)$$

12.3. Умови та порядок контролю показників надійності

Контроль надійності ТЛК-обладнання проводять шляхом організації експлуатаційних спостережень – збиранням та обробленням статистичних даних про надійність обладнання в умовах його експлуатації за основним призначенням. Щодо ТЛК-обладнання застосовується послідовний план контролю показників надійності: в процесі експлуатації контрольованого обладнання послідовно у часі реєструються моменти вияву відмов та моменти закінчення відновлювальних робіт (див. рис.12.1). І далі після кожного акту усунення відмов здійснюється поточна точкова (рос. - точечная) оцінка вибраних показників надійності і порівняння їх з

нормованими значеннями цих показників. Для визначення моментів вияву відмов організується безперервний у часі контроль відповідності параметрів, які характеризують працездатність цього обладнання. Контроль здійснюється у фоновому режимі, коли до потоків *PDU* споживачів додається потік тестових *PDU,* вимірювання параметрів та (або) аналіз вмісту полів формату котрих дозволяє зробити висновок щодо працездатності контрольованого обладнання.

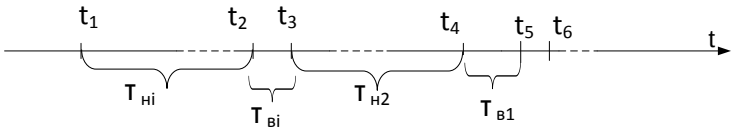


Рис. 12.1. Послідовний план контролю показників надійності, де $\mathbf{T_{ні}}$ - і-тий інтервал напрацювання між відмовами; $\mathbf{T_{ві}}$ – і-тий інтервал відновлення працездатності

Статистичні дані щодо відмов мережного обладнання збирають з використанням так званих карток обліку відмов, у яких вказують, поміж інших даних, серійний номер мережного обладнання, напрацювання з початку його експлуатації, дату виявлення відмови, назву (адресу) елементу, в якому виявлено відмову (плата, блок, програмний модуль і т. ін.), причину відмови, тривалість відновлення працездатного стану мережного обладнання. До карток обліку відмов вносять інформацію лише щодо тих відмов мережного обладнання, для усунення яких виконувалась заміна апаратних засобів (плат, блоків і т. ін.) або переінсталяція програмного забезпечення контрольованого мережного обладнання.

Математичну обробку отриманих даних про поточні значення інтервалів $\mathbf{T_{ні}}$ та $\mathbf{T_{ві}}$ під час оцінювання проводять згідно з ГОСТ 27.410.

Пов'язаність каналу транспортування даних. Однією із основних процедур визначення стану обладнання під час контролю

працездатності є процедура контролю пов'язаності (рос. – связаності) каналу транспортування даних. Якщо канал є зв'язаним, то тестове сигнальне повідомлення має безперешкодно пройти через цей канал від його початку до його кінця і в зворотному напрямі. Цим забезпечується гарантія, що канал, щонайменше, є фізично справним. Згідно з цією процедурою періодично з наперед визначеним інтервалом часу на увід одного із напрямків передачі через контрольований канал надсилається *PDU* із запитом щодо підтвердження певних характеристик утвореного каналу (наприклад, надсилається сигнальне повідомлення "*STATUS ENQUIRY*"). Обладнання, що знаходиться на кінцевому (вивідному) кінці каналу цього напрямку, у відповідь на отриманий запит має надіслати у зворотному напрямку *PDU* із підтвердженням факту отримання запиту та запитаними характеристиками (наприклад, відправити сигнальне повідомлення "STATUS"). І якщо підтвердження у визначений проміжок часу не надійшло або воно надійшло, але запитані характеристики вказують на певну невідповідність в роботі обладнання, то в цей момент фіксується факт порушення пов'язаності каналу, що рахується як вияв відмови (тобто, переходу обладнання у непрацездатний стан). Після закінчення відновлювальних робіт перевіряється коректність функціонування процедури контролю пов'язаності. І якщо порушення пов'язаності не спостерігаються, робиться висновок про відновлення стану працездатності контрольованого обладнання.

Контроль ймовірності безвідмовної роботи. Вихідними даними для оцінювання $P(T_N)$ є задане напрацювання T_N та припустиме значення $P^0(T_N)$. Вибір параметрів плану контролю здійснюють за таблицями 36-38 додатку 7 ГОСТ 27.410.

Контроль коефіцієнта готовності. Вихідними даними для оцінювання $K_г$ є мінімально припустиме значення цього коефіцієнта $K_г^{min}$ та ризик споживача β (точніше, рівень ризику споживача отримати помилкову оцінку коефіцієнта готовності). Рівень ризику β задається в діапазоні значень від 0 до 1. Якщо $\beta = 0{,}00$, то ризик є відсутнім. Якщо $\beta = 1{,}00$, то маємо стовідсотковий ризик. Якщо $\beta = 0{,}15$, то маємо п'ятнадцятивідсотковий ризик.

Оцінку $K_г$ проводять після кожного r-того відновлення. А саме,

на кожному r-тому кроці експлуатаційних спостережень обчислюють локальну (рос. – точечную) оцінку коефіцієнта готовності $\hat{E}_{\hat{a}r}$ за наступними формулами: ?? ?

$$\hat{E}_{\hat{a}r} = \frac{\hat{T}}{\hat{T}_{\hat{a}} + \hat{T}}, \qquad (12.5)$$

де $\hat{T} = \frac{1}{r}\sum_{i=1}^{r} \tau_{\acute{i}i}$; $\hat{T}_{\hat{a}} = \frac{1}{r}\sum_{i=1}^{r} \tau_{\hat{a}i}$;

$\tau_{ні}$; $\tau_{ві}$ – i-ті інтервали безвідмовної роботи та відновлення відповідно.

Необхідно визначити обсяг вибірки (тобто, мінімально необхідне значення r), за якої оцінка коефіцієнта готовності $\hat{E}_{\hat{a}r}$ буде представницькою. Порядок такого визначення наведено у додатку 7 ГОСТ 27.410. Із цього ГОСТу витікає, що обсяг вибірки залежить від ризику β. Зокрема, лінія прийняття рішення щодо коректності визначення коефіцієнту готовності для $\beta = 0{,}05$ (згідно з рисунком 4-11 додатку 7 ГОСТ 27.410) відображена на рис.12.2.

Як бачимо із рис. 12.2, щоб із ризиком споживача на рівні $\beta =$ 0,05 (тобто, при п'ятивідсотковій ймовірності виникнення помилки у прийнятті рішення щодо визначення реального значення $K_г$) отримати упевненість, що реально виміряне значення коефіцієнту готовності відповідає $K_г^{min} = 0{,}998$, обсяг отриманих даних про поточні значення інтервалів $\tau_{ні}$ та $\tau_{ві}$ має бути не менш, ніж $r = 25$. Тобто, на основі спостережень за потоком відмов якогось одного зразка обладнання сказати щось більш/менш об'єктивне про реальне значення його коефіцієнту готовності можливо тільки після надто тривалого терміну спостережень, і то не завжди. Може статися, що зразок обладнання буде демонтовано внаслідок його моральної застарілості задовго до того, коли у картці обліку відмов буде зафіксовано двадцять п'ять подій, що пов'язані із відновлювальними роботами на цьому зразку. Інша справа, коли існує можливість проаналізувати кілька облікових карток, в яких зафіксовані відмови різних зразків однотипного обладнання. Наприклад, в компанії працює десять зразків однотипних комутаторів і налагоджена централізована служба аналізу даних

усіх облікових карток. Тоді буде достатнім зафіксувати на кожному із комутаторів усього лише по три події відмов, щоб із п'ятивідсотковим ризиком зробити оцінку реального значення $K_г$ оцінюваних комутаторів.

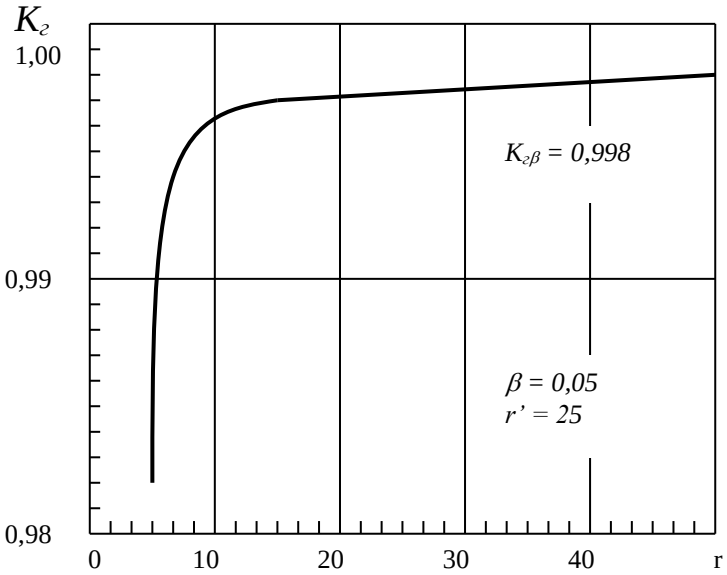


Рис.12.2. Лінія прийняття рішення щодо коректності оцінки коефіцієнту *Кг*

12.4. Методи та засоби резервування програмно-апаратних елементів обладнання

Важливою особливістю роботи ТЛК-обладнання є необхідність забезпечення цілодобового режиму його функціонування. Це передбачає необхідність реалізації заходів щодо надійного резервування елементів обладнання (як апаратних засобів, так і ПЗ), забезпечення безперервного електроживлення від кількох джерел енергії та запобігання порушень доступності ресурсів обладнання для законних (легальних) користувачів.

Розрізняють: **системну надійність**, **апаратну надійність** та **надійність програмного забезпечення**.

Системна надійність. Структурні елементи обладнання та механізми їхнього функціонування, що реалізують основні принципи функціонування ТЛК-системи як єдиного цілого, забезпечують так звану системну надійність обладнання.

В якості прикладу розглянемо варіант забезпечення системної надійності основного системного блоку (*BBU*) базової станції (*BTS*) стільникового зв'язку за схемою 1+1+2, що показаний на рис.12.3.

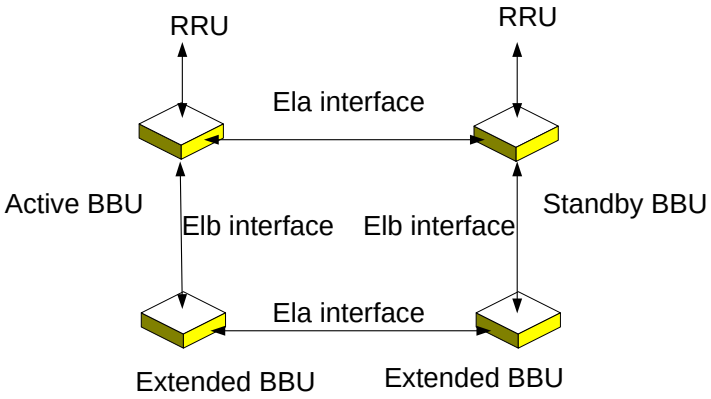


Рис.12.3. Варіант забезпечення системної надійності блоку BBU шляхом одночасного гарячого та пасивного резервування за схемою 1+1+2

Тобто, маємо: один активний системний блок *Active BBU*, що на даному інтервалі часу бере на себе робоче навантаження базової станції; один системний блок *Standby BBU*, що здійснює функції гарячого резервування активного блоку; два додаткових пасивних системних блоки *extended BBU*, що здійснюють функції холодного резервування активного (або «гарячого») системного блоку. До основного системного блоку базової станції можуть бути підключені віддалені блоки *RRU*, що розміщуються у можливих місцях концентрації абонентського навантаження на певних відстанях від місця розміщення основного обладнання *BTS*. Так що вкрай бажано також забезпечити надійність каналу

транспортування інформації між основним та віддаленим блоками базової станції.

Як бачимо із рис.12.3, до активного робочого блоку *Active BBU* через спеціалізований EIa-інтерфейс підключено в якості гарячого резерву блок *Standby BBU*, що знаходиться у режимі *Standby*, тобто у режимі очікування моменту переключення у робочий активний стан. Блок *Standby BBU* працює паралельно із активним системним блоком, виконуючи ті ж самі операції у режимі реального часу, що і блок *Active BBU*. Бажано, щоб у будь-який момент часу поточні стани цих блоків були однаковими. У цьому випадку у разі виходу з ладу активного блоку буде забезпечена можливість майже миттєвого переключення обладнання базової станції на роботу із блоком *Standby BBU*. Організація паралельної роботи активного та «гарячого» системних блоків базової станції залежить від того, в якому режимі (активному чи пасивному) використовується додатковий (резервний) канал транспортування інформації між *Standby BBU* та *RRU*. Якщо резервний канал є активним, тобто повністю дублює роботу основного каналу між *Active BBU* та *RRU,* то у цьому випадку забезпечується можливість незалежної роботи блоку *Standby BBU* від роботи блоку *Active BBU*. Фактично у цьому випадку обидва названі блоки (якщо вони є справними) у будь-який момент часу знаходяться в однаковому стані, внаслідок чого проміжок часу переключення активного блоку на резервний може бути зведений до мінімуму. Якщо ж резервний канал між *Standby BBU* та *RRU* є пасивним, то синхронізація станів обох блоків здійснюється через EIa-інтерфейс. Тому в момент виникнення проблем із активним блоком необхідно виділити певний проміжок часу на передавання на резервний блок останніх даних щодо поточного стану активного блоку та на переведення резервного каналу між *BBU* та *RRU* в активний стан.

Окрім того, у конфігурації рис.12.3 системну надійність блоку BBU забезпечує холодний резерв - два додаткових *extended BBU,* які у штатних умовах знаходяться у пасивному стані і не підтримують режим *Standby*. Холодний резерв використовується у тих випадках, коли вийдуть з ладу одночасно як активний системний блок *Active BBU*, так і «гарячий» резервний блок *Standby BBU*. В залежності від побудови EIb-інтерфейсу проміжок часу,

необхідний для синхронізації станів холодних та гарячих блоків *BBU*, може бути різним. Якщо, наприклад, холодний блок *extended BBU* лише включено у контур електропостачання, а у процесі штатного функціонування *BTS* обмін даними через EIb-інтерфейс не здійснюється, то у цьому разі стан холодного блоку ніяким чином не корелюється із поточним станом гарячих блоків і, отже, перехід холодного блоку в активний стан (у разі потреби) буде здійснюватися протягом досить тривалого часу, що може призвести до втрати значної кількості інформації і, навіть, до відмови в обслуговуванні абонентів стільникової мережі. Щоб цього уникнути, EIb-інтерфейс може бути побудовано таким чином, щоб забезпечувати підтримку певного проміжного рівню синхронізації станів холодних та гарячих блоків. Таке компромісне рішення, з одного боку, спрощує і, отже, здешевлює EIb-інтерфейс, а, з іншого боку, забезпечує прийнятну величину тривалості переходу холодного блоку в активний стан.

Інший варіант забезпечення системної надійності обладнання *BTS* показано на рис.12.4.

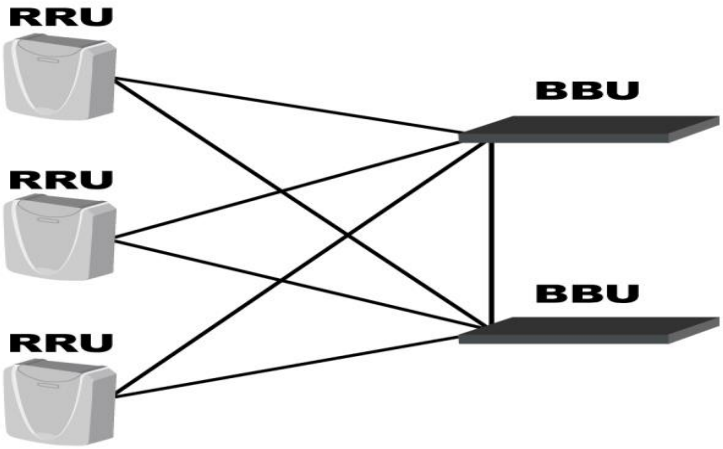


Рис.12.4. Варіант забезпечення системної надійності блоку *RRU* шляхом його одночасного гарячого та пасивного резервування за схемою 1+1+1

Як бачимо, використовується схема гарячого резервування системного блоку *BBU* (маємо два *BBU*: один з котрих - *Active BBU*, а інший - *Standby BBU*, що зв'язані через EIa-інтерфейс). Проте кожен із *BBU* з'єднаний відповідними каналами із трьома *RRU*. Тобто, маємо потрійне резервування віддаленого блоку базової станції. Режими резервування *RRU* та відповідних каналів транспортування інформації можуть бути обрані різними. Зокрема, за схемою 1+1+1, тобто обрано один активний *RRU*, один гарячий *RRU* та один холодний *RRU*.

На практиці широкого застосування набула кільцева схема резервування обладнання, наприклад така, що показана на рис.12.5. Вихід з ладу будь-якого одного або суміжних елементів цієї схеми не позначиться на працездатності інших елементів кільця, а здійснення функцій непрацездатних елементів можуть узяти на себе елементи, що функціонують справно.

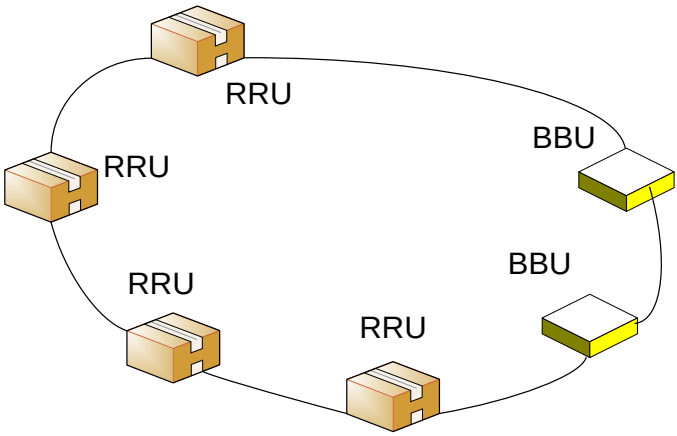


Рис.12.5. Кільцевий варіант забезпечення системної надійності обладнання *BTS*

Апаратна надійність забезпечується на усіх стадіях життєвого циклу ТЛК-обладнання. На стадії проектування вона забезпечується низкою конструктивних апаратних рішень, спеціально спрямованих на підвищення надійності функціонування

апаратних елементів обладнання, зокрема шляхом застосування надійної елементної бази під час конструювання апаратних елементів ТЛК-обладнання, використанням спеціальних технічних рішень, що припускають можливість нормальної роботи обладнання у широкому діапазоні змін параметрів обладнання та середовища його експлуатації (наприклад, температурних перепадів, змін вологості повітря, параметрів енергозабезпечення тощо), застосуванням елементів автоматики, що змінюють режими роботи обладнання в залежності від змін в умовах його експлуатації, застосуванням вбудованих електровентиляторів (фенів), що забезпечують охолодження апаратних елементів обладнання в процесі їхнього функціонування та ін.. На стадії виготовлення підвищення апаратної надійності досягається шляхом організації вхідного контролю працездатності комплектуючих виробів та їхнього стресового випробування безпосередньо перед їхнім монтажем. На стадії експлуатації використовуються різноманітні заходи організаційно-технічного характеру, що сприяють стабільній роботі ТЛК-обладнання: створення якісного контуру заземлення, екранування обладнання від зовнішніх електромагнітних впливів, захист від блискавок, використання сучасних систем виявлення проблемних ситуацій в роботі обладнання та їх усунення, застосування системи контролю та керування параметрами середовища експлуатації тощо. Особлива увага на цій стадії приділяється особливостям застосування джерел безперебійного енергозабезпечення та систем захисту від нештатних коливань параметрів електромережі.

Програмна надійність. Внаслідок багатьох несприятливих факторів під час функціонування програмних засобів, що інстальовані у складі ТЛК-обладнання, можуть виникнути збої, помилки і, навіть, відмови роботі ПЗ. Тому у сучасних ТЛК-системах забезпеченню надійності функціонування програмного забезпечення (ПЗ) приділяється не менша увага, ніж забезпеченню апаратної надійності.

Примітка 12.1. Нагадаємо, що **під збоєм** розуміється нетривала подія некоректної роботи ПЗ, яка випадковим чином з'являється і через деякий час самоусувається. Найбільш ймовірною причиною появи збою є небажана дія на ходу обчислювального процесу зовнішнього впливу, що має випадковий характер.

Зокрема, це - імпульсні або флуктуаційні завади, електромагнітні наводи, лінійні спотворення форми фізичних сигналів, луно-сигнали тощо. На відміну від збою **помилки** в роботі ПЗ мають регулярний характер, тобто якщо виникли умови, за яких утворюється помилка, то повторне відтворення цих умов стабільно призводить до повторного утворення цієї помилки. Найбільш ймовірними причинами появи помилок є небажаний вплив кінцевої розмірності розрядної сітки процесору (помилки округлення), помилки апроксимації функцій, синтез некоректних алгоритмів та розрахункових схем тощо. Найбільш негативні наслідки мають **відмови** в роботі ПЗ, оскільки в цьому випадку виникають порушення доступності легальних користувачів до ресурсів ТЛК-системи, що, у свою чергу, знижує конкурентоспроможність провайдера послуг, призводить до економічних збитків.

Для забезпечення надійності ПЗ застосовують ті ж самі методи, що і для підтримки надійності апаратних засобів ТЛК-обладнання. Резервування ПЗ – основний серед них. У відповідальних випадках ТЛК-системи комплектується засобами відновлення ПЗ. Ці засоби, у разі необхідності, дозволяють перезавантажити ПЗ системи. Зокрема, дозволяють завантажити резервну копію ПЗ. Резервна копія ПЗ будь-якого макро-елементу системи зберігається на самому макро-елементі та (або) на віддаленому вузлі мережі глобального керування. За звичайних умов здійснюється централізоване перезавантаження ПЗ макро-елементів ТЛК-системи із віддаленого вузлу у фоновому режимі без переривань в роботі макро-елементу. Зазвичай будь-який макро-елемент системи зберігає у флеш-пам’яті як поточну, так і попередню конфігурацію ПЗ. Якщо, наприклад, відбудеться випадкове переривання в електропостачанні, то протягом кількох секунд поточна конфігурація ПЗ буде перезавантажена із флеш-пам’яті в оперативну пам’ять макро-елемента.

На прикладі технічних рішень виробників сучасного ТЛК-обладнання розглянемо основні методи та засоби резервування елементів цього обладнання та його програмного забезпечення.

Обладнання сучасних ТЛК-систем сконструйовано як відмовостійке обладнання з високим рівнем надійності функціонування. Елементи програмного та апаратного забезпечення під час його роботи знаходяться під постійним контролем відповідних прикладних застосувань. У випадку відмови будь-якого функціонального елементу автоматично здійснюється його майже миттєва заміна на ідентичний резервний

елемент.

Надійність функціонування будь-якого макро-елемента (комутатора, маршрутизатора, шлюзу, сервера, контролера і т. ін.) сучасної глобальної ТЛК-системи характеризується наступними показниками:

- коефіцієнт готовності $K_г$ - не менше 0,9999;
- середній час відновлення після відмови *MTTR* (*Mean Time To Repair*) – не більше 30 хвилин;
- точність локалізації проблеми невідповідності до одного елемента заміни – у 70% зафіксованих випадків виявлення проблем;
- точність локалізації проблеми невідповідності до чотирьох елементів заміни – у 95% зафіксованих випадків виявлення проблем.

Засоби ТЛК-системи, як правило, забезпечують наступний набір сервісів щодо виконання процедур резервування обладнання:

1) дублювання (2N), коли кожний активний елемент обладнання має ідентичний запасний елемент, що знаходиться в стані «гарячого» резерву (тобто, якщо кількість активних елементів дорівнює N, то має існувати така ж кількість елементів гарячого резерву);

2) заміщення (N+1), коли на групу із N ідентичних активних елементів існує лише один додатковий елемент, що знаходиться у стані холодного резерву;

3) надлишкове ресурсне забезпечення (SN+), коли група елементів обладнання функціонує як пул певного функціонального ресурсу, кількість котрого дещо перевищує в його номінальній потребі (в цьому випадку, якщо один із елементів обладнання вийде з ладу, то потребу у використанні його ресурсу задовольнять інші елементи цього пулу ресурсу).

Зрозуміло, що критично важливі елементи, відмови котрих призводять до відмови в роботі усього обладнання у цілому, а також елементи, показники надійності котрих є гіршими за припустимі в конкретних умовах функціонування обладнання, мають резервуватися за методом дублювання (2N). Якщо ж відмови в роботі певного елементу, що входить до складу групи ідентичних елементів, не призводять до відмови усього обладнання у цілому, а

призводять лише до зниження рівня якості надання послуг, то такий елемент доцільно резервувати за методом заміщення (N+1). Якщо ж маємо групу елементів, які у змозі підтримувати, поряд з іншим, якусь однакову функціональність, і ці елементи працюють з неповним навантаженням, то із цих елементів доцільно утворити ресурсний пул за методом надлишкового ресурсного забезпечення (SN+).

12.5. Архівація програмного забезпечення та баз даних

Резервне копіювання ПЗ та даних, що обробляються у ТЛК-системах, є важливим елементом підтримки надійності функціонування обладнання. Резервне копіювання здійснюється за допомогою відповідних програмно-апаратних засобів згідно з прийнятими в компанії правилами адміністративно-організаційного характеру.

Зокрема, використовуються наступні адміністративно-організаційні заходи:

- розроблюються спеціальні процедури резервного копіювання інформації, у яких враховується специфіка видів інформаційних об'єктів, що копіюються, типів структурних елементів та режимів функціонування системи, а також визначається для кожного з інформаційних компонентів періодичність створення резервних копій;
- організовується облік, зберігання та відновлення скопійованої інформації у відповідності з їхніми грифами конфіденційності;
- розроблюються процедури переміщення скопійованої інформації для кожного інформаційного компонента ТЛК-системи;
- визначається відповідальність за порушення процедур резервного копіювання, архівації, переміщення, обліку, зберігання та оновлення скопійованої та архівованої інформації;
- розробляється схема ротації магнітних носіїв.

До програмно-апаратних засобів резервного копіювання інформації слід віднести:

- жорсткі диски та магнітні стрічки для копіювання інформації;
- штатні засоби резервного копіювання операційних середовищ та систем керування базами даних.

12.6. Антивірусне програмне забезпечення

Операційне середовище глобальних ТЛК-систем загального призначення, як правило, фізично ізолюється від інших телекомунікаційних систем. В цих випадках організація антивірусного захисту не є першочерговою справою. Однак в ТЛК-системах спеціального призначення, навіть у фізично ізольованих від зовнішніх впливів, для запобігання несанкціонованих дій персоналу існує необхідність в інсталяції, поряд з іншим, антивірусного ПЗ. Локальні ТЛК-системи зазвичай мають з'єднання з іншими телекомунікаційними системами. Тому встановлення на них антивірусного ПЗ є обов'язковим. У відповідальних випадках підсистема антивірусного захисту повинна базуватися на антивірусних продуктах різних фірм-розробників (при створенні мають бути використані продукти не менш, ніж двох різних фірм) для забезпечення можливості контролю проникнення вірусів у максимально стислі строки після їх появи та взаємного контролю різних продуктів.

Підсистема антивірусного захисту повинна мати у своєму складі робоче місце адміністратора антивірусного захисту, з якого забезпечується централізоване управління цією підсистемою.

Підсистема антивірусного захисту має охоплювати усі засоби обчислювальної техніки (АРМ, робочі станції, сервери), що встановлені у доменах безпеки телекомунікаційних мереж.

Повинен забезпечуватися захист від комп'ютерних вірусів:

- комп'ютерних систем шляхом перевірки всього http-, ftp- та smtp- трафіку, що проходить через ці комп'ютерні системи;
- файлових серверів та серверів баз даних шляхом перевірки файлів та процесів на цих серверах за допомогою антивірусного монітору або сканеру, що встановлюється на цих серверах.

Процедури використання антивірусного програмного забезпечення

ПЗ ІТКС, у т.ч. ПЗ комплексних систем захисту інформації (КСЗІ), може бути уражене комп'ютерними вірусами. Вірус у даному випадку розглядається як програма, що несанкціоновано впроваджується в обчислювальне середовище ІТКС з метою заподіяння шкоди її користувачам та власникам. Під словом «вірус» розуміють програму, яка не тільки здійснює деструктивну

функцію, але і має здатність розмножуватися. Існує велика кількість різноманітних видів вірусних програм, для протидії котрим використовують так звані антивіруси - ПЗ, що здатне виявляти та знешкоджувати віруси. Антивірусне ПЗ також характеризується великою різноманітністю, що не є предметом розгляду у даній роботі. Важливо лише підкреслити, що будь-який сучасний антивірусний продукт, як правило, реалізує майже усі звісні методи пошуку та знешкодження можливих вірусних атак, тому отримати докази на формальному рівні щодо переваг одного продукту над іншим не уявляється можливим. Кожен конкретний антивірусний продукт є унікальним, його конкретні недоліки або переваги можливо виявити лише шляхом постійного спостереження за ефективністю його функціонування в конкретних умовах застосування. У відповідальних випадках бажано встановлення в ІТКС кількох різних антивірусних програм, що працюють на різних рівнях сканування системи. Але одночасну роботу деяких антивірусів неможливо узгодити між собою, на що треба звернути особливу увагу.

Основною особливістю технології боротьби з вірусами є необхідність постійного оновлення антивірусного ПЗ. Кожен день в мережному середовищі з'являються все нові види вірусів, що потребує швидкого реагування - розробки відповідних засобів та механізмів для їхнього знешкодження. Тому розробники антивірусного ПЗ постійно слідкують за появою нових вірусів і намагаються якнайшвидше розробити адекватні засоби їхньої нейтралізації. Розроблені засоби у вигляді так званих оновлень антивірусного ПЗ розповсюджуються, як правило, через мережу Інтернет. Персонал ІТКС має постійно оновлювати встановлене антивірусне ПЗ: чим частіше, тим краще.

Для кожного активного елементу ІТКС слід використовувати відповідний антивірусний засіб. Антивірус для серверного обладнання відрізняється від антивірусу для робочої станції або для шлюзу. Бажано антивіруси використовувати у комплексі з іншими засобами захисту інформації, зокрема міжмережними екранами або додатковими програмами типу «Антиспам», «Антируткіт» і т.ін., які доповнюють функціональність основної антивірусної програми. Технологія застосування антивірусів

широко висвітлена в літературі. Ми лише розглянемо особливості боротьби із вірусами в КСЗІ.

Операційне середовище КСЗІ в ІТКС загального призначення, як правило, фізично ізолюється від інших телекомунікаційних систем. В цих випадках організація антивірусного захисту не є першочерговою справою, проте для запобігання несанкціонованих дій персоналу за цих умов бажано здійснювати інсталяцію, поряд з іншим, антивірусного ПЗ. В ІТКС спеціального призначення, навіть у фізично ізольованих від зовнішніх впливів, встановлення антивірусного ПЗ для запобігання несанкціонованих дій персоналу вважається необхідною справою. Локальні ІТКС зазвичай мають з'єднання з іншими телекомунікаційними системами. Тому встановлення на них антивірусного ПЗ є вкрай бажаним.

В якості прикладу розглянемо порядок оновлення антивірусного ПЗ, що має позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації (ТЗІ) і регламентується Наказом № 45 від 26.03.07р. Адміністрації Державної Служби спеціального зв'язку та захисту інформації (Держспецзв'язку) України. Не все обладнання ІТКС, що знайшло використання в Україні, має позитивний експертний висновок за критеріями ТЗІ, однак дотримання основних положень цього документу буде корисним при забезпеченні антивірусного захисту будь-якої інформаційної системи, у т.ч. і КСЗІ.

Ці положення полягають у наступному:

1) оновлення антивірусного ПЗ конкретної ІТКС здійснюється шляхом періодичного отримання та інсталяції відповідних комп'ютерних програм - антивірусних оновлень;

2) оновлення антивірусного ПЗ, що має позитивний експертний висновок за критеріями ТЗІ, здійснюється з використанням антивірусних оновлень, які розміщуються на веб-сайті Центру антивірусного захисту інформації (ЦАЗІ) Держспецзв'язку України (www.cazi.dsszzi.gov.ua). (На цьому веб-сайті розміщуються тільки антивірусні оновлення, які пройшли експрес-експертизу у ЦАЗІ, і тільки для тих продуктів антивірусного ПЗ, які мають позитивний експертний висновок Держспецзв'язку України. Список цих продуктів надано на сайті ЦАЗІ);

3) Слід не менше ніж раз на день отримувати вищезазначені

антивірусні оновлення та інсталювати ці оновлення відповідно до технічної документації на впроваджене в ІТКС антивірусне ПЗ.

У відповідальних випадках підсистема антивірусного захисту повинна базуватися на антивірусних продуктах різних фірм-розробників (при створенні мають бути використані продукти не менш, ніж двох різних фірм, але ці продукти мають не заважати в роботі один одному) для забезпечення можливості контролю проникнення вірусів у максимально стислі строки після їх появи та взаємного контролю різних продуктів.

Підсистема антивірусного захисту повинна мати у своєму складі робоче місце адміністратора антивірусного захисту, з якого забезпечується централізоване управління цією підсистемою.

Підсистема антивірусного захисту має охоплювати усі засоби обчислювальної техніки (АРМ, робочі станції, сервери), що встановлені у доменах безпеки телекомунікаційних мереж.

Повинен забезпечуватися захист від комп'ютерних вірусів:

- комп'ютерних систем шляхом перевірки всього http-, ftp- та smtp-трафіку, що проходить через ці комп’ютерні системи;
- файлових серверів та серверів баз даних шляхом перевірки файлів та процесів на цих серверах за допомогою антивірусного монітору або сканеру, що встановлюється на цих серверах.

Контрольні питання до дванадцятої лекції:

1. Чим обумовлена актуальність задач підтримки надійності функціонування обладнання ?
2. Які особливості задач підтримки надійності функціонування ТЛК-обладнання під час його експлуатації?
3. Які показники експлуатаційної надійності обладнання Ви знаєте?
4. Визначить умови та порядок контролю показників надійності.
5. Надайте характеристики методам та засобам резервування програмно-апаратних елементів обладнання.
6. Яким чином здійснюється архівація програмного забезпечення та баз даних?
7. Які вимоги до використання антивірусного програмного забезпечення?

Використана література:

1) Г.Ф. Конахович, В.М. Чуприн. Сети передачи пакетной коммутации.–К..: МК-Пресс, 2006.

САМОСТІЙНЕ ЗАНЯТТЯ ЗА МАТЕРІАЛАМИ ЛЕКЦІЇ №12. ВИМІРЮВАННЯ ПАРАМЕТРІВ РАДІОЧАСТОТНИХ КАНАЛІВ ПЕРЕДАВАННЯ ІНФОРМАЦІЇ

Загальні положення

До радіочастотних систем відносяться засоби, що використовують в якості середовища транспортування інформації електромагнітне поле, яке розповсюджується у навколоземному просторі. До складу будь-якої радіочастотної системи, як правило, входять радіо-передавальний (ПРД) та радіоприймальний (ПРМ) пристрої, що взаємодіють між собою через антенні системи та навколоземний простір (так званий, „радіоефір"). У радіорелейних та супутникових системах зв'язку, а також у системах зв'язку з рухомими об'єктами широкого застосування набули також всілякого роду радіо-ретранслятори різного призначення.

Якщо розглядати радіочастотне обладнання з точки зору організації вимірювань його параметрів, то слід мати на увазі наступне:

1) умови розповсюдження радіосигналів у різних діапазонах радіохвиль істотно різняться, що суттєво впливає на вибір засобів та способів вимірювань параметрів радіообладнання;

2) для систем зв'язку з рухомими об'єктами і для радіорелейних систем передачі визначальною є оцінка параметрів згасання енергії сигналу при багатопроменевому розповсюдженні радіохвиль;

3) для систем супутникового зв'язку найбільш важливими вважаються вимірювання параметрів затримки сигналів, а також оцінка впливу доплерівського зсуву по частоті на якість передавання інформації.

Основними об'єктами щодо яких здійснюються радіочастотні вимірювання слід визначити безпосередньо приймально/передавальне та канало-утворювальне радіообладнання, а також обладнання ретрансляторів, що функціонують у складі мереж радіозв'язку. Окрема увага приділяється вимірюванням електромагнітних характеристик

радіоефіру, що пов’язано із необхідністю забезпечення контролю за дотриманням національного законодавства у сфері розподілу та використання радіочастот.

Основні параметри радіочастотного тракту, що підлягають вимірюванням

Як відомо, до складу типового радіочастотного тракту входять наступні компоненти: джерела і одержувачі інформації, в якості котрих, здебільшого, використовують пристрої, що призначені для передачі та (або) прийому інформації; кодеки (кодери/декодери) — пристрої, що перетворюють цифрові сигнали в кодові слова і навпаки; модеми (модулятори/демодулятори); фільтри ПЧ (проміжної частоти); конвертори; фільтри РЧ (радіочастоти); антенні пристрої, а також безпосередньо середовище розповсюдження (тобто, радіоефір).

До основних параметрів радіочастотного тракту, що підлягають вимірюванням, відносять:

1) співвідношення *C/N* (сигнал/шум) або *C/I* (сигнал/завада);

2) параметр бітової помилки — *BER*, який залежить від співвідношення *C/N*;

3) рівні потужності радіосигналів в межах зони обслуговування;

4) параметр згасання радіосигналів при багатопроменевому розповсюдженні.

Основні групи експлуатаційних вимірювань

Експлуатаційний інтерес являють наступні групи вимірювань:

- визначення залежності параметра бітової помилки *BER* від співвідношення сигнал/шум (*C/N*);

- вимірювання рівнів потужності радіосигналів у довільних точках в межах зони радіо-покриття з урахуванням багатопроменевого характеру розповсюдження радіохвиль;

- оцінка деградації якості зв'язку в радіочастотних системах передачі, що викликана фазовими шумами передавального тракту або тепловим шумом приймача;

- оцінювання рівня міжсимвольної інтерференції, який, головним чином, залежить від якості виготовлення фільтрів ПЧ і РЧ;

- вимірювання параметрів модуляції, що необхідні для виявлення можливих порушень в роботі модемної частини радіообладнання;

- визначення ступеню нелінійності підсилювальних елементів

радіообладнання.

Вимірювання співвідношення C/N (сигнал/шум)

В залежності від характеру експлуатаційних завдань розрізняють наступні визначення співвідношення *C/N*:

- відношення *C/N*, що визначається як відношення середньої потужності сигналу несучої до середньої потужності шумів у певним чином вибраній точці вимірювань;
- відношення *C/No*, що визначається як відношення середньої потужності сигналу несучої до потужності шумів, що вимірюються в межах смуги шириною 1Гц (величина *No* в таких випадках трактується як спектральна щільність шуму); таким чином, параметр *C/No* не залежить від ширини діапазону частот, у той час як параметр *C/N* пов'язаний із вимірюванням середніх потужностей шумів у межах робочого діапазону частот;
- відношення E_B/No, що визначається як відношення енергії сигналу, необхідної для передачі одного біту, E_B до спектральної щільності шуму *No*, що нормується до смуги 1 Гц.

Розглянемо співвідношення, що існують між вищеназваними параметрами.

Енергія сигналу на біт E_B пов'язана з параметром *C* (середньою потужністю сигналу несучої) простим співвідношенням:

$$E_B = CT_B = C/f_B ,$$

де *Тв* — час передачі одного біта, f_B — швидкість передачі інформації в бітах через радіоканал.

З урахуванням вищезазначеного, параметри *C/No* і *Eb/No* можна представити у наступному вигляді:

$\frac{E_B}{N_0} = \frac{C}{N_0}\frac{1}{f_B}$ або в децибелах $\frac{E_B}{N_0} = \frac{C}{N_0} - 10lgf_B$.

Нормована до смуги 1 Гц потужність шумів *No* (Вт/Гц) дорівнює відношенню потужності шумів *N* до ширини смуги шумів приймача B_N. Тому

$$\frac{E_b}{N_0} = \frac{C}{N} \cdot \frac{B_N}{f_b} \qquad (12.6)$$

або в децибелах $$\frac{E_b}{N_0} = \frac{C}{N} - 10\lg\frac{f_b}{B_N} \qquad (12.7)$$

Якщо ширина смуги приймача кількісно дорівнює швидкості інформації, що приймається, тоді

$$E_B/N_0 = C/N ,$$

тобто відношення енергії сигналу на біт інформації до нормованої потужності шумів в смузі 1Гц дорівнює відношенню *C/N* (відношенню середніх потужностей сигналу до шуму).

Вимірювання залежності параметра BER від співвідношення C/N

Визначення параметру бітових помилок *BER* було надано вище у лекції №7. Цей параметр вважається основним під час розгляду будь-якої системи зв'язку. Проте для отримання повної уяви щодо ефективності роботи цифрової радіочастотної системи передавання інформації необхідне знання залежності параметра *BER* від співвідношення *C/N — BER=f(C/N).* При проведенні вимірювань параметрів радіочастотних систем передачі і цифрових радіоканалів мереж радіозв'язку знання залежності *BER=f(C/N)* дозволяє достатньо повно охарактеризувати інстальовану систему у реальних умовах її використання. Зокрема, знаючи залежність *BER* від співвідношення сигнал/шум і вимірюючи параметри сигналу на різних ділянках радіочастотного тракту, можна оцінити шумовий внесок тих або інших ділянок і ланцюгів в загальне погіршення якості в системі передачі інформації.

Вимірювання параметрів модулятора/демодулятора

Для вимірювання параметрів модему використовують аналізатори, що забезпечують можливість оцінювання характеристик реальних сигналів у радіосистемі за допомогою діаграм станів або окових діаграм. Ці діаграми, як свідчать матеріали для самостійного вивчення до лекції №5, дають детальну інформацію про структуру, зміни та відхилення параметрів цифрової модуляції. Іншими словами, можливі

відхилення від номінальних значень характеристик роботи модемного обладнання радіосистеми можливо виявити та оцінити за допомогою окових діаграм або діаграм станів.

На рис.12.6 наведено діаграма станів сигналу (зліва) та окова діаграма сигналу (справа), що характеризує штатний режим роботи модему із цифровою модуляцією16QAM (квадратурна амплітудна модуляція із 16-ма станами сигналу), яка часто використовується у цифрових радіорелейних системах передачі.

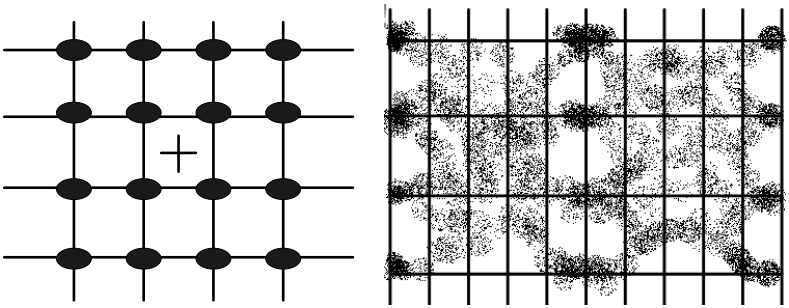


Рис.12.6. Діаграма станів (ліворуч) і окова діаграма (праворуч) сигналів, що характеризують штатний режим роботи реальної радіосистеми з модуляцією 16 QAM

За допомогою цих діаграм представляється можливим виявити характер можливих порушень в роботі модему.

На діаграмі станів (див. діаграму ліворуч на рис.12.6) наочно видно вплив шумів, який призводить до „розмивання" точок, що відображають стани досліджуваного сигналу. А на оковій діаграмі (див. діаграму праворуч на рис.12.6) ясно помітні три пари пари "очей", оскільки модуляція 16QAM є трьохрівневою за параметром амплітуди.

Серед можливих порушень роботи радіочастотного тракту несправність елементів модулятора/демодулятора, як свідчить експлуатаційна практика, найважче локалізувати. Тому розглянемо деякі характерні варіанти порушень роботи модулятора/демодулятора і відповідні цим порушенням діаграми.

Втрата синхронізації в каналі. Відмова в роботі

демодулятора, його відключення або порушення фазової синхронізації між модулятором і демодулятором може призвести до втрати сигналу у радіосистемі. У цьому випадку (тобто, коли сигнал пропав) діаграма станів являє випадковий розподіл сигналів за трьома рівнями модуляції (перші два рівні – це кола, третій зовнішній рівень на лівому рис.12.7 буде відображатися окремими точками поза кол), а "око" окової діаграми закривається повністю (правий рис. 12.7).

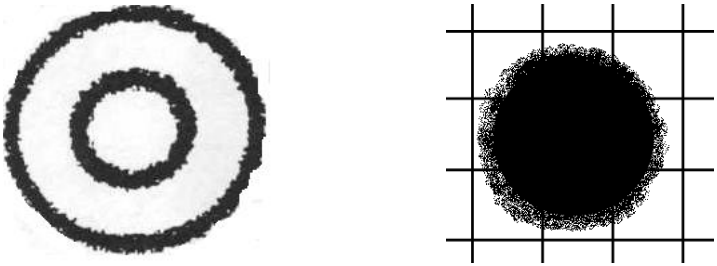


Рис.12.7. Відображення втрати синхронізації в каналі на діаграмі станів (ліворуч) та на оковій діаграмі (праворуч)

Порушення ортогональності I і Q векторів демодулятора. Одне з поширених порушень в роботі демодулятора - коли вектори I і Q полярних координат демодулятора виявляються не ортогональними. Це призводить до розмитості станів ортогональної сітки координат на діаграмі станів (див. лівий рис.12.8) та малому розкриву очей на оковій діаграмі (див. правий рис.12.8).

Порушення ортогональності може супроводжуватися (але не завжди) помилкою фазової синхронізації у ланцюгу відновлення несучої. У разі відсутності помилки результат дії цієї несправності на окову діаграму зводиться до закривання "ока" на діаграмі по сигналу *I* і відсутності якої-небудь зміни по сигналу *Q*. За наявності помилки фазової синхронізації "ока" по цим двом сигналам будуть закриті.

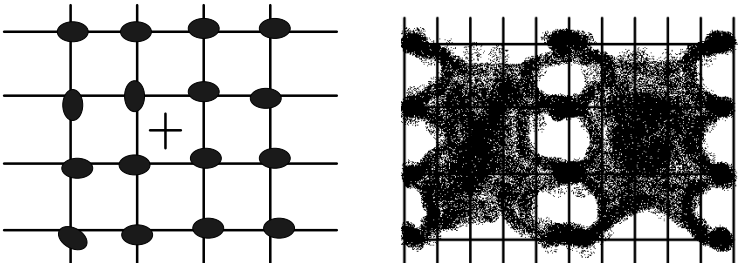


Рис. 12.8. Ілюстрація ефекту порушення ортогональності сигналів *I* і *Q* у демодуляторі на діаграмі станів (ліворуч) і на оковій діаграмі (праворуч)

Необхідно відзначити, що аналіз однієї тільки окової діаграми не дозволяє встановити причину несправності модему, оскільки за наявності високого рівня адитивних шумів в каналі на оковій діаграмі неможливо відрізнити ефект порушення ортогональності сигналів від впливу високого рівню шумів. Тому достовірне виявлення причини несправності в цьому випадку може дати тільки діаграма станів.

Неправильне встановлення рівнів модуляції/демодуляції. На рис.12.9 показана типова діаграма станів для випадку, коли існує помилка у встановленні рівнів модуляції/демодуляції. Це може бути пов'язано з надмірною нелінійністю амплітудної характеристики модулятора або з порушенням роботи цифро-аналогового перетворювача. Як бачимо, відстань між другим і третім рядом розмитих точок є суттєво більшою, ніж відстань між іншими рядами точок на діаграмі станів, що є аномалією.

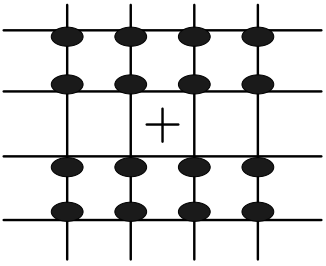


Рис. 12.9. Відображення встановлення не збалансованого рівняамплітуди сигналу на діаграмі станів

Аналіз роботи підсилювачів

Детальний аналіз роботи підсилювачів виконується під час проектування, виготовлення та заводських випробувань систем радіозв'язку. Для цієї мети зазвичай використовуються раніш розглянуті скалярні і векторні аналізатори ланцюгів (*Network Analyzers*). Проте в експлуатаційній практиці радіосистем аналізатори ланцюгів не знайшли широкого використання, тому що більшість проблем в роботі підсилювачів на стадії експлуатації можливо вирішити за допомогою більш розповсюджених в експлуатаційних організаціях спеціальних аналізаторів радіосигналів і параметрів модуляції. За допомогою цих аналізаторів можливо здійснювати аналіз діаграм станів та окових діаграм. Основні експлуатаційні проблеми здебільшого пов’язані із необхідністю вимірювати шуми підсилювачів, що функціонують у складі радіочастотного тракту, та з вимірюваннями параметрів нелінійності підсилювальних ділянок (оскільки перенавантаження підсилювача по амплітуді сигналу може призвести до його переходу у нелінійний режим і, як наслідок, до різкого збільшення параметра помилок у цифровій системі передачі).

Спочатку розглянемо, яким чином можна здійснювати локалізацію причин деградації якості щодо характеристик нелінійності підсилювального тракту за допомогою окових діаграм і діаграм станів .

На рис. 12.10 представлені діаграма станів і окова діаграма сигналів для випадку перенавантаження підсилювача, що побудований на лампі біжучої хвилі (ЛБХ), на 3*Дб* зверх норми. Поява у цьому випадку інтермодуляційного ефекту внаслідок небажаних АМ/ФМ-перетворень сигналу та підвищення кількості помилок призводять до закриття "ока" окової діаграми та до розмивання „картинок” на обох діаграмах. Як бачимо на рис.12.10, ці картинки далекі від ідеалу.

Звісно, що перенавантаження підсилювача виникає внаслідок неправильної установки параметрів роботи радіообладнання. Тому найбільш доцільний шлях усунення перенавантаження - це зниження рівня сигналу на вході відповідного підсилювача для

забезпечення його роботи в лінійному режимі. Упевнитися, що підсилювач працює саме у лінійному режимі, можливо за допомогою вищерозглянутих діаграм. Для цього треба поступово знижувати рівень сигналу на вході підсилювача і в цей час спостерігати за діаграмами. Як тільки картинки на них прийдуть до норми, то це свідчитиме, що перенавантаження підсилювача усунуто. Таким чином, для виявлення причин зниження якості радіозв'язку достатньо локалізувати ділянку деградації, щоб потім налаштувати систему за допомогою вищерозглянутих діаграм.

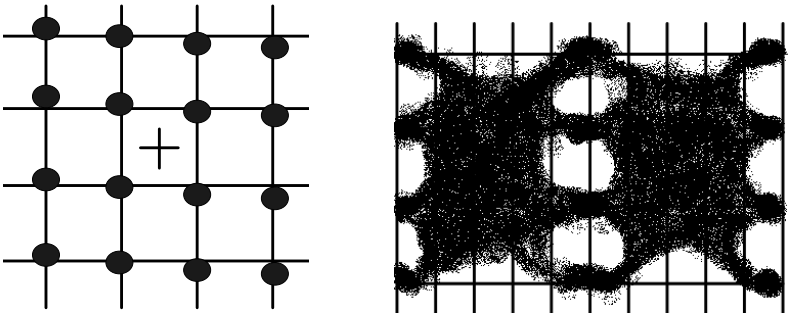


Рис. 12.10. Ілюстрація нелінійних спотворень сигналу на діаграмі станів (зліва) та на оковій діаграмі (праворуч)

Аналіз роботи фільтрів

Погана фільтрація сигналів може призводити до порушень форми сигналів, до підвищення рівня міжсимвольної інтерференції в каналі та, як наслідок, до збільшення параметра помилок у цифровій системі передавання.

На жаль, на діаграмі станів ефекти, що пов'язані з порушенням роботи фільтрів, практично не відображаються. Проте прийнятну оцінку ефектів, що спричинені порушеннями в роботі фільтрів, дає окова діаграма. Зокрема, погана фільтрація сигналу призводить до того, що "око" окової діаграми втрачає форму і розмивається.

Вимірювання рівня власних теплових і фазових шумів елементів радіочастотного тракту

Високий рівень шумів призводить до збільшення значень

параметра помилок. Діаграми, що представляють сигнали при співвідношенні сигнал/шум у 15*дБ*, представлені на рис.12.11.

Як бачимо, підвищений рівень шуму на діаграмах стану і оковій діаграмі не призводить до геометричної трансформації діаграм, але виявляється через збільшення розміру точок відображення станів сигналу і появу ефекту "закривання очей".

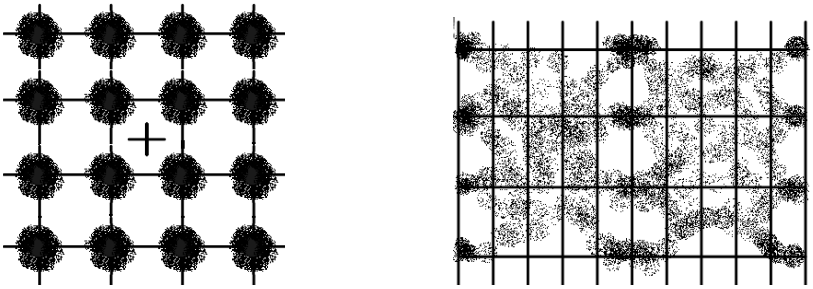


Рис.12.11. Ілюстрація високого рівню шумів на діаграмі і на оковій діаграмі

Вимірювання шумів виконується з метою локалізації точок, де рівень шумів є неприпустимо великий. Враховуючи, що власні шуми різних пристроїв радіочастотного тракту у порівнянні із корисними сигналами характеризуються вельми малими величинами, для вимірювань зазвичай використовують диференціальні методи. Сутність диференціального методу вимірювання шуму (у випадках, коли мають справу із шумами малої потужності) полягає у наступному.

Досліджуваний сигнал змішують із додатковим спеціально сформованим одно-частотним сигналом таким чином, щоб утворився сигнал інтерференції достатньо малої величини. Утворений інтерференційний сигнал за величиною легше порівнюється із реальними шумами у радіоканалі. Тому вимірювання шумів здійснюють по різниці між величиною інтерференційного сигналу та величиною шуму. Відповідна діаграма станів та окова діаграма для модуляції 16*QAM* з відношенням сигнал/інтерференція *C/I*=15*дБ* представлені на рис. 12.12.

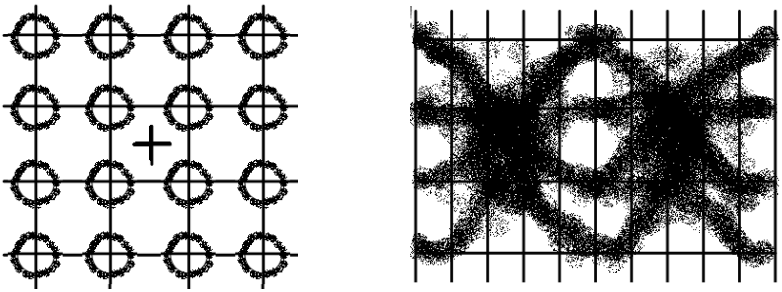


Рис. 12.12. Вимірювання шумів за диференційним методом

Слід зазначити, що здійснювати оцінку характеристик фазових шумів через їхній низький рівень за допомогою окових діаграм або діаграми станів не представляється можливим. Проте необхідність точного вимірювання фазових характеристик компонентів радіочастотного тракту в експлуатаційній практиці існує. Тому вимірювання фазових шумів виділено в окремий клас вимірювальних технологій, що будуть розглянуті далі.

Вимірювання параметрів генераторів приймально-передавального обладнання

Важливим параметром вимірювань радіочастотних систем передачі із цифровою модуляцією є фазовий джитер - фазове тремтіння сигналу задавального генератору приймача або передавача. Фазове тремтіння сигналу генератора за певних умов може значно збільшити величину параметру помилок.

Для аналізу джитеру використовують діаграму станів. Окова діаграма до джитеру є нечутливою.

Діаграма станів в каналі з фазовим джитером представлена на рис.12.13.

Для усунення проблем, пов'язаних з наявністю джитеру, зазвичай проводять додаткові вимірювання параметрів роботи задавальних генераторів і усувають несправність.

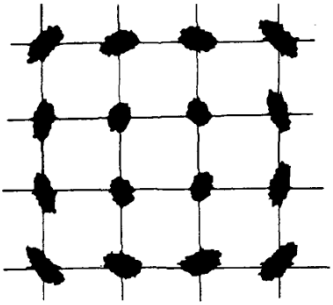


Рис. 12.13. Ілюстрація прояву фазового джитеру на діаграмі станів

Комплексні вимірювання радіочастотних трактів

У більшості випадків вимірювання параметрів радіочастотного тракту проводяться для того, щоб мінімізувати параметр помилок у системі передачі *BER*.. Остаточні параметри радіочастотної системи передачі, як правило, визначаються у вигляді функціональних залежностей параметра *BER*. Так, наприклад, залежність *BER* від відношення сигнал/шум у радіочастотній системі передачі вважається в багатьох випадках найбільш важливим параметром, оскільки дозволяє врахувати внесок у погіршення якості передачі практично всіх елементів, що утворюють радіочастотний тракт.

Зазвичай кожен із пристроїв, що функціонує у складі радіочастотного тракту, вносить певний внесок у сумарну величину параметра помилок. Тому комплексні вимірювання радіочастотних трактів доцільно проводити після вимірювань параметрів кожного із пристроїв, що входять до складу радіочастотного тракту, або з урахуванням звісних параметрів цих пристроїв (наприклад, на основі даних про характеристики пристроїв, що надаються у технічній документації).

Комплексні вимірювання радіочастотних трактів у значній мірі пов'язані із особливостями розповсюдження сигналу уздовж тракту, оскільки включають не лише вимірювання характеристик тракту, на які встановлені гранично припустимі обмеження, але і параметрів стійкості його роботи залежно від зовнішніх умов поширення сигналу через радіотракт.

Вимірювальна техніка для відображення діаграм сигналів радіочастотного тракту

Діаграми станів та окові діаграми, як було показано вище, можуть бути корисними для аналізу якості роботи різних пристроїв, що функціонують у складі радіочастотного тракту. Аналіз сигналів у вигляді окових діаграм або діаграм станів проводиться за допомогою спеціальних аналізаторів радіосигналів і параметрів модуляції. Характеристики таких аналізаторів представлені у табл. 12.1.

Таблиця 12.1

Характеристики аналізаторів радіо сигналів і параметрів модуляції

Модель	***MS8604 A***	***R3465***	***89441A***	***89440A***	***FSEA20/30***
Виробник	*Anritsu*	*Advantest*	*HP*	*HP*	*R&S*
Типи модуляції	*DQPSK, π/4 DQPSK, GMSK*	*BPSK, QPSK, QPSK із зсувом, DQPSK, π/4 DQPSK, 8PSK, GMSK*	*BPSK, QPSK, QPSK із зсувом, DQPSK, π/4 DQPSK, 8PSK, 16-256 QAM, VSB, MSK, FSK 2- і 4-рівнева, GMSK*	*BPSK, QPSK, QPSK із зсувом, DQPSK, π/4 DQPSK, 8PSK, 16-256 QAM, VSB, MSK, FSK 2- і 4-рівнева*	*BPSK, QPSK, QPSK із зсувом, DQPSK, π/4 DQPSK, 8PSK, MSK, GMSK*
IQ-діаграми	+	+	+	+	+
Діаграми станів	+	+	+	+	+

Робочий діапазон	*100 Гц - 8,5Гц*	*9 кГц - 210,5 Гц*	*0-2,65 Гц*	*0- 1,8 Гц*	*20 Гц - 3,5 Гц*

Спектральний аналіз сигналів радіочастотних систем передачі

Звісно, що законодавство України регламентує використання національного радіочастотного ресурсу. Зокрема, законодавством передбачено, що кожен конкретний вид радіосистем повинен функціонувати лише у спеціально відведеній смузі радіочастот. Існують спеціально відведені смуги радіочастот, що призначені для роботи, наприклад, радіосистем військового призначення (при цьому кожному типу радіосистем відведено свою окрему смугу частот), смуги частот для підтримки роботи авіаційного транспорту, для стільникових систем мобільного зв'язку, для морського транспорту і т.д. Органи контролю зобов'язані протистояти незаконному використанню радіочастотного ресурсу, а також забезпечувати електромагнітну сумісність одночасно працюючих радіосистем. Контроль використання радіочастотного ресурсу та аналіз електромагнітної сумісності працюючих радіосистем обумовлює необхідність здійснення спектрального аналізу радіосигналів. Окрім того, аналіз спектру сигналів, що випромінює працююча радіочастотна система, має значну експлуатаційну цінність, оскільки виникнення відмов або інших порушень в роботі будь-яких радіопристроїв зазвичай відбивається на результатах спектрального аналізу сигналів радіочастотного тракту. Зокрема, у цих випадках з'являються додаткові субгармоніки, паразитні сигнали, змінюється спектральний склад сигналу і т.ін.. Усе це можливо виявити за допомогою спектрального аналізу сигналів, результати котрого, у свою чергу, дозволяють зробити висновок щодо працездатності досліджуваної радіосистеми і, у разі порушень її роботи, визначити причину цих порушень. Іншим корисним застосуванням спектрального аналізу є пошук і усунення причин

інтерференції між сусідніми радіоканалами. Для того, щоб величина інтерференції була у припустимих межах, спектр робочих сигналів радіосистеми повинен знаходитись у межах так званої спектральної маски.

Як приклад, на рис.12.14 представлена форма спектральної маски для робочого сигналу у каналі радіорелейної системи передачі (РРЛ) із смугою пропускання 30*Мгц*.

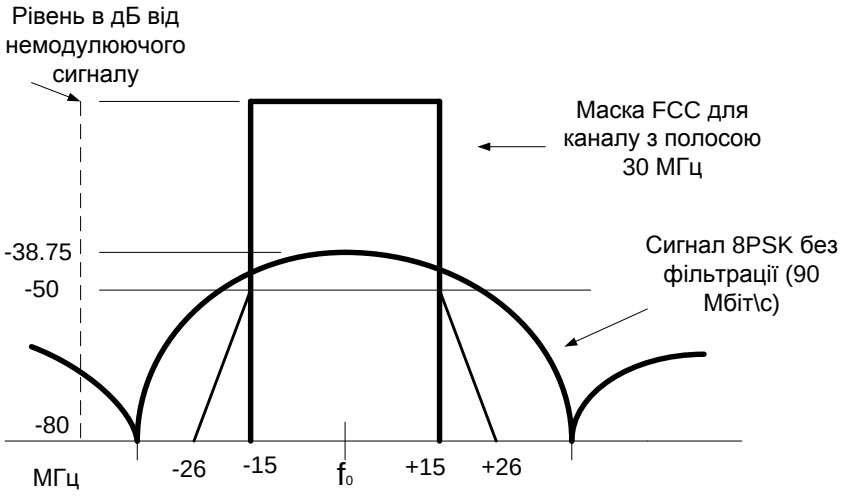


Рис.12.14. Спектральна маска робочого сигналу в каналі РРЛ

Як видно із рис.12.14, спектри реальних радіосигналів (зокрема, сигнал з модуляцією *8PSK*) безпосередньо не поміщаються у маску. Тому для забезпечення нормальної роботи РРЛ потрібне використання фільтрів у робочій смузі каналу.

Сучасні аналізатори спектрів радіосигналів здатні встановлювати необхідні спектральні маски робочих сигналів: стандартні або такі, що задаються користувачами аналізатора. Ілюстрація випадку, коли робочий сигнал повністю розмістився у межах спектральної маски, наведена на рис.12.15.

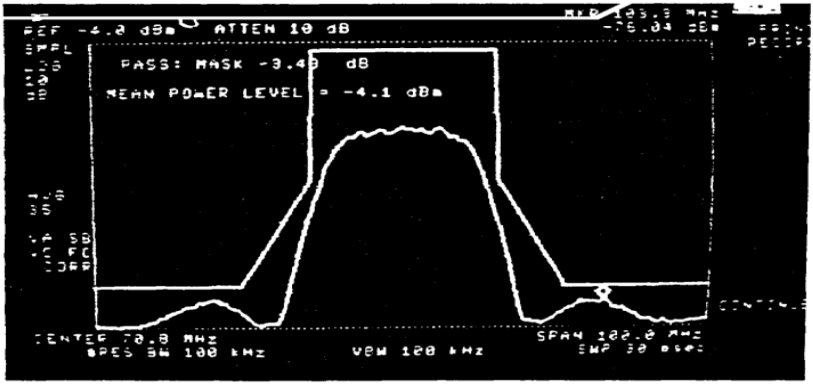


Рис. 12.15. Вимірювання спектру радіосигналу за допомогою аналізатора *HP 11758V*

Вимірювання частоти і потужності радіосигналів

Зазвичай частоту радіосигналів вимірюють за допомогою частотомірів, а їхню потужність – за допомогою вимірювачів потужності. Проте нерідко існує необхідність здійснювати одночасні вимірювання частоти та потужності радіосигналів. У цих випадках використовують спеціалізовані прилади, які одночасно виконують функції частотоміра та вимірювача потужності радіосигналів.

Існує можливість для одночасних вимірювань частоти і потужності радіосигналів використати аналізатор спектру, що здатний здійснювати так звані маркерні вимірювання. Такий аналізатор забезпечує можливість переміщення маркера уздовж спектральної характеристики досліджуваного сигналу з одночасним відображенням на екрані виміряних значень параметрів частоти і потужності радіосигналу. Більше того, такий аналізатор також здатний виконувати функції згладжування спектральної характеристики, фільтрації шумів і т.ін., що розширює можливості обробки досліджуваних сигналів.

Як приклад, на рис.12.16 представлена спектральна характеристика робочого сигналу у радіоканалі і результат маркерного вимірювання потужності у *дБм* і частоти у *МГц*.

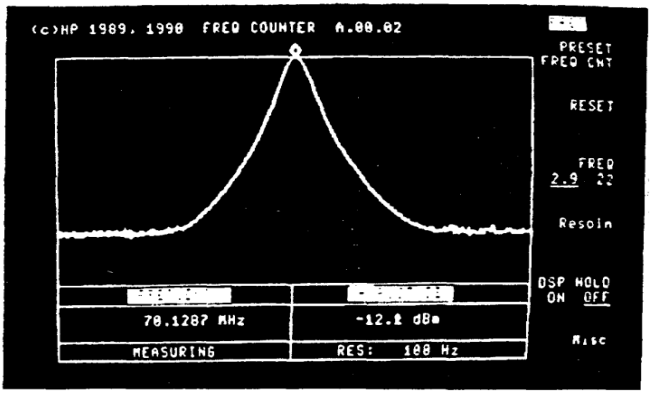


Рис. 12.16. Результати маркерних вимірювань частоти і потужності робочого сигналу

Недоліком маркерних вимірювань зазвичай визнається їх недостатня точність, проте для вирішення більшості експлуатаційних завдань точність вимірювань не є суттєвим параметром. Це і зумовило широке застосування аналізаторів спектру у вищерозглянутих цілях.

Вимірювання залежності параметра помилок від співвідношення сигнал/шум

Як було вказано вище, залежність *BER = f(C/N)* є основною характеристикою тракту радіочастотної системи передачі. На основі цієї залежності визначають величину співвідношення „сигнал/шум”, що гарантує задану величину параметра помилок у досліджуваній системі.

Якщо порівнювати теоретично розраховану залежність параметра помилок від співвідношення *C/N* з експериментально отриманою залежністю, то можна переконатися, що на практиці слід брати дещо більше значення *C/N* для заданого значення *BER*, ніж те, що отримано як результат теоретичного розрахунку. Зрозуміло, що таке пов’язане із неідеальністю параметрів реальних пристроїв (зокрема, трактів ПЧ та РЧ), що входять до складу досліджуваних радіосистем.

У сучасній практиці існує декілька методів визначення

залежності BER = f(C/N), з яких слід виділити два основні методи: більш традиційний, пов'язаний з внесенням додаткового загасання до тракту РЧ, і сучасніший, пов'язаний з точним внесенням шумів до тракту прийому.

Схема традиційного методу вимірювань параметра *BER=f(C/N)* представлена на рис.12.17. Вона заснована на використанні у приймачі РЧ тракту певного пристрою - атенюатора, за допомогою якого вноситься додаткове загасання. Рівень сигналу прийому вважається постійним на проміжку часу вимірювання. Параметр помилки вимірюється аналізатором цифрових каналів, а рівень сигналу і шуму вимірюють вимірювачем потужності.

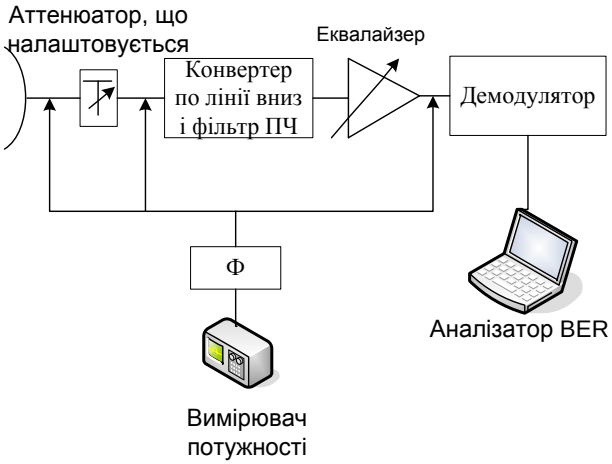


Рис.12.17. Використання атенюатора (із можливістю його переналагодження) для вимірювань характеристики *BER=f(C/N)*

На практиці результат вимірювання шумів в тракті ПЧ без фільтрації дає значення, що є більше за значення реальної потужності шумів в робочій смузі тракту. Тому при вимірюваннях потужності використовують додаткові фільтри Ф, що налаштовані на робочу смугу частот.

Основний недолік традиційного методу – це припущення щодо незмінності рівню потужності робочого сигналу на інтервалі

вимірювань, оскільки у реальних умовах досягти цього практично неможливо. Завжди існує нестабільність приймального сигналу, що може бути пов'язана із загасанням, обумовленим природними явищами (дощ, нагрівання атмосфери і т.д). Такі природні явища приводять до значних варіацій параметрів середовища розповсюдження радіосигналів - радіоефіру. Як наслідок, потужність робочого сигналу може змінюватися на 1-2 *дБ* навіть протягом дня із стабільною погодою. Аналіз залежності *BER* від рівня сигналу, що приймається, в сучасних цифрових системах передачі показує, що дана характеристика має високу крутизну: зменшення рівня сигналу навіть на 1*дБ* може привести до збільшення рівня *BER*, що вноситься системою передачі, у десять разів. Таким чином, традиційний метод вимірювань *BER=f(C/N)* з використанням атенюатора не забезпечує необхідну точність результатів вимірювань, особливо при малих значеннях параметра *BER*.

Для виконання вимірювань залежності *BER=f(C/N)* при малих значеннях параметра *BER* використовується інтерференційний метод, схема котрого представлена на рис.12.18.

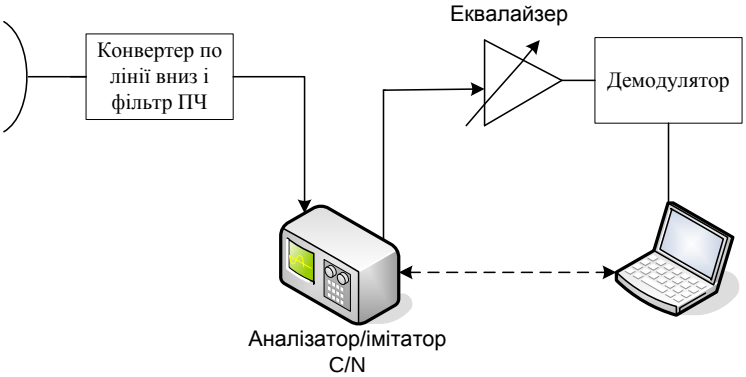


Рис 12.18. Інтерференційний метод вимірювань характеристики *BER = f(C/N)*

Цей метод можна застосовувати, якщо у розпорядженні дослідників є спеціальний прилад – аналізатор та імітатор співвідношення сигнал/шум (зокрема, пристрій *HP3708A*). Цей

прилад здатний автоматично регулювати рівень шумів в залежності від рівня сигналу, що приймається. Тобто, цей прилад здатний підтримувати на заданому рівні співвідношення *C/N*, незважаючи на те, що рівень потужності приймального сигналу в процесі вимірювань весь час змінюється. Якщо, наприклад, рівень сигналу починає збільшуватися, то і рівень шуму також збільшується. Це забезпечує підчас вимірювань параметра *BER* постійне значення *C/N* на бажаному рівні. Тому даний метод забезпечує високу точність вимірювань характеристики *BER = f(C/N)* в діапазоні можливих значень параметра *BER* аж до $1x10^{-12}$.

Контрольні питання до самостійного заняття дванадцятої лекції

1. Що таке *PICS*?
2. Що таке бланк *PICS*?
3. Для чого використовують бланк *PICS*?
4. Яке коло питань відображають у бланку *PICS*?
5. Що відображають в уведенні у бланк *PICS*?
6. Які характеристики протоколу установлюються у розділах бланку *PICS*?

Література до самостійного заняття дванадцятої лекції

1) И.Г.Бакланов. Методы измерений в системах связи. –М.: ЭКО-ТРЕНДЗ, 1999. раздел 10.

МОДУЛЬ №4. ТЕХНОЛОГІЇ УПРАВЛІННЯ ТРАФІКОМ ТА НАДАННЯМ ТЕЛЕКОМУНІКАЦІЙНИХ ПОСЛУГ

ЛЕКЦІЯ №13. НАВАНТАЖЕННЯ НА ТЛК-ОБЛАДНАННЯ: ПОКАЗНИКИ, МЕТОДИ ВИМІРЮВАННЯ ТА РОЗРАХУНКИ

Розглядаються наступні питання:

Лекційне заняття

13.1. Визначення терміну «навантаження»

13.2. Визначення терміну «інтенсивність навантаження»

13.3. Визначення показників нерівномірності навантаження

13.4. Визначення характеристик нерівномірності пакетного трафіка

13.5. Методи вимірювання навантаження

13.6. Оцінка характеристик обладнання з урахуванням інтенсивності навантаження

Самостійне заняття. *Управління телефонним трафіком*

13.7. Основні поняття та визначення

13.8. Параметри телефонного трафіка

13.9. Потоки телефонних викликів: властивості та характеристики

13.10. Розрахунок телефонного трафіка

13.11. Особливості вимірювання телефонного трафіка

13.1. Визначення терміну „навантаження”

Будь-яке обладнання може експлуатуватися із різним ступенем інтенсивності. Якщо воно функціонує за даних умов із максимально можливою інтенсивністю, то забезпечується максимально можлива продуктивність його використання, тобто забезпечується максимальний корисний ефект від його експлуатації. У цьому випадку говорять, що обладнання працює в умовах повного навантаження. Якщо ж це обладнання функціонує, як кажуть, не на повну потужність, тобто із невисокими рівнями інтенсивності, або взагалі часто простоює, то мова йде про низький рівень навантаження на обладнання і, зрозуміло, такий стан речей не може задовольнити власників цього обладнання, оскільки на його закупівлю та організацію експлуатації було витрачено певні кошти. Бажано, щоб ці кошти „працювали” із максимальним економічним ефектом.

Примітка 13.1. Наприклад, на закупівлю, увід та організацію експлуатації певного ТЛК-обладнання було витрачено півтора мільйони гривень, а за умов його повного навантаження отримано річний прибуток у розмірі 0,5 млн. грн., то термін окупності цього обладнання (без урахування всіляких тонкощів) становитиме три роки, що в галузі телекомунікацій вважається прийнятною величиною. Якщо ж на стадії експлуатації інтенсивність використання цього обладнання складає 20% від максимально можливої інтенсивності, то річний прибуток складатиме лише 0,1 млн. грн., а термін окупності в цьому разі становитиме 15 років, що робить капіталовкладення в таке обладнання явно неефективними.

Примітка 13.2. Слід звернути увагу на те, що обладнання більшості механічних систем (наприклад, автомобільні або авіаційні двигуни, компресори, насоси тощо) у режимі повного навантаження функціонує із підвищеними рівнями фізичного зносу, що негативно впливає на рівень надійності та зменшує термін його експлуатації. Проте ТЛК-обладнання у загальному випадку не відноситься до механічних систем. Надійність та термін експлуатації ТЛК-обладнання майже не залежить від ступеню інтенсивності його експлуатації. Виключення можуть складати елементи деяких ланцюгів електроживлення, що працюють за умов високих значень величини струму.

Вищевказане у повній мірі відноситься і до ТЛК-обладнання. Зокрема, у більшості випадків (зокрема, для обладнання пакетних мереж) в якості параметра продуктивності вибирається показник реально досягнутої швидкості обробки інформації на цьому обладнанні. Щодо канального обладнання то під швидкістю обробки інформації розуміється швидкість її передавання через канал зв'язку. Найвищий рівень можливої продуктивності ТЛК-обладнання визначається як його пропускна здатність. Проте мається на увазі, зокрема, не теоретично можлива пропускна здатність каналу, яка визначається для ідеальних умов його функціонування за звісною формулою Шеннона (тобто, $C=\Delta F\log_2(1+P_c/P_ш)$, де ΔF - ширина смуги пропускання каналу, а P_c та $P_ш$ - потужності відповідно сигналів та завад), а експлуатаційна пропускна здатність, що визначається з урахуванням конкретних умов функціонування обладнання.

Якщо мова йде про вузлове обладнання пакетних мереж (комутатори, маршрутизатори, шлюзи, сервери і таке інше), то під пропускною здатністю (або продуктивністю) розуміється максимально можлива за даних умов кількість одиниць інформації (бітів, кадрів, фреймів, пакетів, повідомлень, протокольних блоків

даних тощо), що може бути нормально оброблена цим обладнанням протягом певним чином вибраного проміжку часу. Зазвичай обирається проміжок часу, що дорівнює 1 секунді. Під словом «нормально» мається на увазі, що у принципі швидкість обробки інформації в обладнанні може бути і більше, ніж його пропускна здатність, але в цих випадках якість обробки буде «не нормальною», тобто показники якості (такі як коефіцієнт втрат пакетів, коефіцієнт бітових помилок, показники спотворень сигналів тощо) будуть гіршими, ніж для нормальних умов обробки інформації.

Примітка 13.3. Підкреслимо, що за різних умов експлуатації одне і те ж обладнання може функціонувати із різними значеннями експлуатаційної пропускної здатності. Тому необхідно конкретизувати умови, за яких визначається пропускна здатність ТЛК-обладнання. З іншого боку, під час вимірювань пропускної здатності враховуються лише ті одиниці інформації, що оброблюються за нормальних умов експлуатації, тобто без порушень цих умов. Зокрема, пропускна здатність обладнання пакетних мереж визначається за умов забезпечення визначених показників якості транспортування пакетів – коефіцієнту втрат протокольних блоків (PDU) та (або) коефіцієнту помилково прийнятих PDU. Пропускна здатність обладнання бітового каналу визначається за умов забезпечення визначених показників якості передавання бітів - параметру бітових помилок BER, параметрів електромагнітного впливу на суміжні електричні ланцюги NEXT, FEXT тощо.

Визначення навантаження на обладнання мереж з комутацією пакетів суттєво відрізняється від визначення навантаження на обладнання мереж з комутацією каналів. Навантаження на обладнання пакетних мереж вимірюється в одиницях кількості інформації (у бітах, байтах, блоках і т. ін.), що оброблюється цим обладнанням за певним чином обраний період часу. Зазвичай у цій сфері використовують поняття «інтенсивність навантаження», що розуміється як кількість обробленої інформації протягом однієї секунди. Зрозуміло: якщо протягом певної поточної однієї секунди вузлове обладнання пакетної мережі нормально (тобто, без порушень умов експлуатації) обробило v_0 одиниць інформації, а пропускна спроможність цього обладнання за даних умов дорівнює c_0 [одиниць інформації за секунду], то миттєвий коефіцієнт навантаження k_0 на це обладнання визначиться як безрозмірна величина (в межах від 0 до 1)

$$k_0 = v_0 / c_0. \quad (13.1)$$

Якщо ж мова йде про канали передавання даних, то під пропускною здатністю такого каналу розуміється максимально можлива за даних умов швидкість передавання цих даних, що також вимірюється у бітах, байтах, кадрах, фреймах, пакетах і таке інше, що пройшли через канал протягом однієї секунди. В якості умов визначення пропускної здатності такого каналу можуть висуватися вимоги забезпечення заданого рівня коефіцієнту помилок, коефіцієнту втрат пакетів тощо.

Зрозуміло: якщо протягом певної поточної однієї секунди канальне обладнання нормально транспортувало через цей канал $v_к$ одиниць інформації, а пропускна здатність каналу за даних умов дорівнює $c_к$ [одиниць інформації/с], то миттєвий коефіцієнт навантаження $k_к$ на цей канал визначиться як безрозмірна величина (в межах від 0 до 1)

$$k_к = v_к / c_к . \quad (13.2)$$

Пакетний трафік, зазвичай, має стрімко пульсуючий характер, а засобам, що його обробляють, притаманна певна інерційність дії. Тому для більш адекватного відображення процесів обробки інформації в пакетних мережах миттєві коефіцієнти навантаження під час вирішення різноманітних експлуатаційних завдань, як правило, усереднюють на певних проміжках часу: на однохвилинних інтервалах, на двохвилинних інтервалах, на п’ятихвилинних інтервалах тощо. У свою чергу, отримані усереднені значення коефіцієнту навантаження усереднюють на годинних інтервалах, потім на добових проміжках часу, потім на місячних і т.д..

Наданими вище визначеннями коефіцієнту навантаження зручно користуватися, оскільки за таких визначень ступінь реальної продуктивності функціонуючого обладнання безпосередньо залежить від рівня інтенсивності потоків інформації, що просуваються через канали передавання або через вузлове обладнання, тобто від інтенсивності оброблюваного трафіка. Чим більш значні за інтенсивністю потоки інформації реально

оброблює ТЛК-обладнання (точніше сказати, чим більше інтенсивність реально оброблюваних потоків наближається до величини пропускної здатності цього обладнання), тим вище рівень навантаження на це обладнання і тим більший корисний ефект від його використання. Вищезазначене характерне для будь-яких пакетних мереж.

Інша справа, мережі з комутацією каналів, зокрема із телефонними мережами. Засобами цих мереж, як правило, здійснюється фізичне або логічне «проключення» (тобто, утворення) каналів між окремими парами абонентів, при цьому величиною інтенсивності потоків інформації, що циркулюють у рамках утворених телефонних каналів, власник ТЛК-обладнання (зокрема, оператор електрозв'язку) не цікавиться, оскільки абонентська плата залежить не від інтенсивності розмов клієнтів, а від проміжку часу використання «проключених» каналів. Тому ступінь навантаження на обладнання мереж з комутацією каналів, у т.ч. телефонних мереж, зручно визначати у часовому вимірі.

За одиницю вимірювання навантаження у мережах з комутацією каналів прийнято одне годино-зайняття (1 год.-зайн.), тобто таке навантаження, яке обслуговується однією двохполюсною мережею протягом однієї години, якщо ця мережа буде безперервно зайнята обслуговуванням.

Примітка 13.4. Одна гілка будь-якої мережі, що являє собою сукупність обладнання двох вузлів, які з'єднані між собою одним каналом зв'язку, називається двохполюсною мережею. Прикладом двохполюсної мережі може слугувати звичайний абонентський канал телефонної мережі загального користування (ТМЗК, PSTN або ЦМІО, ISDN), що з одного кінця закінчується телефонним апаратом, а з іншого – апаратним модулем обладнання лінійного закінчення (аналогового або цифрового) АТС. Якщо ми будемо безперервно розмовляти через цей телефонний канал протягом двох годин, то ми утворимо навантаження на цей канал величиною 2 год.-зайн.. (Як бачимо, у цьому випадку користуються зовсім іншим визначенням поняття «завантаження», ніж у випадку пакетних мереж). Якщо ми протягом однієї години будемо мати п'ять телефонних розмов тривалістю шість хвилин кожна, то утворимо навантаження величиною 0,1 год.-зайн. Х 5 розмов = 0,5 год.-зайн..

Примітка 13.5. Ще інше визначення параметрів навантаження маємо для групових та лінійних трактів багатоканальних аналогових систем передавання (АСП) із частотним розділенням каналів (тобто, ЧРК-систем типу К-60П, К-120, К-300, К-1020 тощо). Для цих систем навантаження визначається граничними

енергетичними параметрами групового сигналу, які у даному контексті не розглядаються, зокрема тому, що ці системи вважаються застарілими і практично зняті з експлуатації.

Якщо певний елемент телефонної мережі може використовуватися лише у монопольному режимі, тобто на будь-якому проміжку часу обслуговувати лише одну пару користувачів, то у цьому разі навантаження на цей елемент протягом однієї години не може бути більшим, ніж 1 год.-зайн.. Проте якщо цей елемент (наприклад, ущільнений міжстанційний канал, телефонний комутатор або фрагмент телефонної мережі) може використовуватися у мультиплексному режимі (тобто, одразу кількома парами користувачів), то навантаження на цей елемент протягом однієї години може суттєво перевищувати значення 1 год.-зайн.. Наприклад, навантаження протягом однієї години на АТС великої ємності, яка здатна одночасно підтримувати десятки тисяч телефонних з'єднань, може досягати десятки тисяч годино-зайнять. Навантаження протягом однієї години на ущільнені міжстанційні канали телефонного зв'язку також може досягати великих значень, що вимірюються тисячами годино-зайнять.

Підкреслимо, що навантаження має сенс розглядати тільки з прив'язкою до певного наперед визначеного проміжку часу, наприклад до однієї години функціонування обладнання.

Пропускна здатність одного окремого телефонного вузлу визначається максимально можливою кількістю телефонних з'єднань, яку здатне одночасно підтримувати обладнання цього вузлу на наперед визначеному інтервалі часу. Навантаження на такий вузол визначається як сумарний час обслуговування усіх утворених телефонних з'єднань на цьому інтервалі часу. А коефіцієнт навантаження на телефонний вузол визначається як відношення навантаження до пропускної здатності цього вузлу (зрозуміло, на наперед визначеному проміжку часу). Якщо, наприклад, якась АТС у будь-який момент здатна одночасно підтримувати рівно десять тисяч телефонних з'єднань, то максимально можливе навантаження на цю АТС протягом однієї години буде дорівнювати 10000 год.-зайн.. Зрозуміло, що у реальному житті навряд чи будуть часто виникати ситуації повного завантаження цієї АТС, оскільки потік заявок на телефонні

з’єднання з боку абонентів являє випадковий процес, ймовірне значення математичного чекання котрого зазвичай є суттєво меншим, ніж пропускна здатність АТС. (Якщо це не так, то телефонна мережа буде неприпустимо перевантаженою, внаслідок чого оператор зв’язку вимушений буде замінити цю АТС на більш потужну). У більшості випадків на значних проміжках часу АТС буде, скоріш за все, недозавантажена, проте можливі ситуації її короткотривалого перенавантаження, зокрема, коли у певні моменти кількість заявок на телефонні з’єднання буде перевищувати поріг величиною 10000. У цьому випадку рівень якості надання телефонних послуг погіршиться (підвищиться ймовірність отримання сигналу „зайнято”, а в деяких випадках можливе навіть блокування роботи усіх клієнтів АТС).

Навантаження на фрагмент телефонної мережі, що складається із кількох вузлів, також визначається сумарним часом обслуговування усіх утворених телефонних з’єднань. Проте величина цього навантаження не є арифметичною сумою навантажень усіх вузлів, що утворюють мережний фрагмент, а обчислюється за спеціальними формулами, які враховують співвідношення кількості локальних з’єднань, утворених у рамках кожного окремого вузлу, до кількості транзитних з’єднань, що проходять через кілька вузлів мережного фрагменту. Методи визначення завантаження фрагментів телефонних мереж вивчаються у рамках навчальних дисциплін з телефонії.

13.2. Визначення терміну «інтенсивність навантаження»

Рівень навантаження на будь-яке ТЛК-обладнання в реальних умовах експлуатації, як правило, не є постійною величиною у часі. Цей рівень, як показують результати спостережень за реальним трафіком (як телефонним, так і пакетним), весь час змінюється. В одних випадках закон цих змін має майже непередбачуваний характер (що притаманно пакетним мережам), в інших - закон змін має випадковий характер із звісною функцією розподілу ймовірностей (що притаманно телефонним мережам). На фоні випадкових або непередбачуваних змін рівня навантаження на ТЛК-обладнання часто спостерігаються періодичні, відносно регулярні коливання цього рівню (зокрема, по годинам доби, дням

тижня та місяцям року), які піддаються розрахунку.

Під час вирішення багатьох експлуатаційних завдань зручно користуватися поняттям «інтенсивність навантаження», під яким розуміється рівень навантаження, що віднесений до короткотривалій одиниці часу.

Для пакетних мереж інтенсивність навантаження на вузлове обладнання визначається, як було вже вказано, як кількість одиниць інформації (бітів, кадрів, фреймів, пакетів, повідомлень, протокольних блоків даних тощо), що оброблюється цим обладнанням протягом одиниці часу. Якщо інтенсивність навантаження вимірюється протягом 1 секунди, то у цьому випадку виміряне значення інтенсивності прийнято вважати миттєвою швидкістю обробки трафіка (формально кажучи, поняття «мить» є теоретичною абстракцією). І, взагалі, для вузлового обладнання пакетних мереж розмірність параметру інтенсивності навантаження має розмірність швидкості обробки протокольних блоків даних (PDU). Тобто, інтенсивність навантаження та середня швидкість обробки PDU, що визначені на однаковому проміжку часу, є ідентичними величинами.

Інша річ, обладнання телефонних мереж (точніше, мереж з комутацією каналів – ТМЗК, ЦМІО і т.ін.). У цьому випадку під інтенсивністю навантаження розуміється навантаження (що вимірюється у годино-зайнятті), яке утворюється протягом однієї години. За одиницю інтенсивності навантаження обладнання з комутацією каналів прийнято ерланг (Ерл). Один ерланг - це навантаження в 1 год.-зайн, що утворене протягом однієї години. Розмірність параметра інтенсивності навантаження - [год.-зайн./год].

Для двохполюсних мереж з комутацією каналів використовують наступні терміни: «інтенсивність вихідного навантаження» (рос. - «интенсивность исходящей нагрузки»), що відноситься до навантаження вихідним трафіком (котре йде від обладнання); «інтенсивність увідного навантаження» (рос. - «интенсивность поступающей нагрузки»), що відноситься до навантаження увідним трафіком (котре йде до обладнання). Зрозуміло, що загальна інтенсивність навантаження визначається як сума інтенсивностей вихідного та увідного навантажень.

13.3. Визначення показників нерівномірності навантаження

Інтенсивність навантаження на ТЛК-обладнання у загальному випадку є змінною величиною, яку доцільно розділити на три складові.

Одна складова – це, як правило, непередбачуваний процес швидких змін у часі (як кажуть, - пульсацій) миттєвих значень інтенсивності навантаження на ТЛК-обладнання. Миттєві зміни навантаження – непередбачуваний результат одночасної діяльності багатьох користувачів ТЛК-обладнання. «Поведінку» активних користувачів на короткострокових проміжках часу майже неможливо прогнозувати. Ці користувачі непередбачуваним чином створюють або розривають сеанси зв'язку, зокрема непередбачуваним чином включають/виключають на своїх комп'ютерах різноманітні прикладні застосування з невизначеними характеристиками. Тому у більшості випадків функція розподілу (тобто, щільність ймовірності) пульсацій навантаження не може бути визначена, а характеристики пульсацій (розмах, тривалість і т. ін.) не піддаються прогнозуванню.

Друга складова інтенсивності навантаження – це повільно змінюваний майже випадковий процес порівняно нешвидких змін у часі поточних величин інтенсивності навантаження, усереднених на більш/менш коротких проміжках часу. Усереднення навантаження на коротко тривалих проміжках часу називають згладжуванням навантаження. Усереднена складова інтенсивності навантаження краще піддається прогнозуванню, ніж пульсації.

Третя складова - це періодичні, відносно регулярні повільні коливання рівня навантаження, зокрема по годинам доби, дням тижня та місяцям року.

Для кількісного оцінювання регулярної складової нерівномірності навантаження використовують коефіцієнти місячної, добової або погодинної нерівномірності (в залежності від проміжку часу, протягом якого здійснюється оцінка нерівномірності навантаження).

Коефіцієнт місячної нерівномірності $k_м$ для певного місяця (наприклад, для липня) визначається співвідношенням середньодобового навантаження для цього місяця $H^{д}_{міс}$ до середньодобового навантаження за рік $H^{д}_{рік}$, тобто

$$k_м = H^д_{міс} / H^д_{рік}. \quad (13.3)$$

У мережах з комутацією каналів середньодобове навантаження вимірюється у годино-зайнятті. Береться сума навантажень щодо кожної доби місяця (року), яка ділиться на кількість діб у місяці (році).

Коефіцієнт добової нерівномірності $k_д$ для певної доби місяця (наприклад, для понеділків в липні місяці) визначається співвідношенням середньодобового навантаження для цієї доби $H^д_{доб}$ до середньодобового навантаження за місяць $H^д_{тиж}$, тобто

$$k_д = H^д_{доб} / H^д_{міс} . \quad (13.4)$$

Наприклад, необхідно визначити $k_д$ для понеділків липня місяця. Тоді середньодобове навантаження за цю добу $H^д_{доб}$ є середньоарифметичне навантаження усіх понеділків, що усереднене за липень, тобто в якості складових суми узято чотири (або п'ять) значень навантаження для усіх понеділків липня, які після сумування розділено на чотири (або п'ять). У той час як середньодобове навантаження за липень $H^д_{міс}$ визначається шляхом усереднення навантаження усіх діб липня.

Коефіцієнт погодинної нерівномірності $k_{год}$ для певної години доби (наприклад, для проміжку між 12.00 та 13.00 годинами), що оцінюється шляхом спостережень за навантаженнями протягом одного тижню, визначається співвідношенням середньогодинного навантаження для цієї години $H^{год}_{год}$ до середньогодинного навантаження за тиждень $H^{год}_{тиж}$, тобто

$$k_{год} = H^{год}_{год} / H^{год}_{тиж}. \quad (13.5)$$

Наприклад, необхідно визначити $k_{год}$ для часового інтервалу між 12.00 та 13.00 годинами. Тоді середньогодинне навантаження для цієї години $H^{год}_{год}$ є середньоарифметичне навантаження цієї години, що усереднене за тиждень, тобто в якості складових суми узято сім значень навантаження для часового інтервалу між 12.00 та 13.00 годинами щодо кожного дня тижня, які після сумування розділено на сім. У той час як середньогодинне навантаження за

тиждень $H^{год}_{тиж}$ визначається шляхом усереднення навантаження усіх годинних проміжків тижня.

Коефіцієнт концентрації для години найбільшого навантаження $k_{ГНН}$ – це співвідношення між інтенсивністю навантаження в годину найбільшого навантаження (ГНН) $I_{ГНН}$ та середньодобовою інтенсивністю навантаження $I_{доб}$, тобто

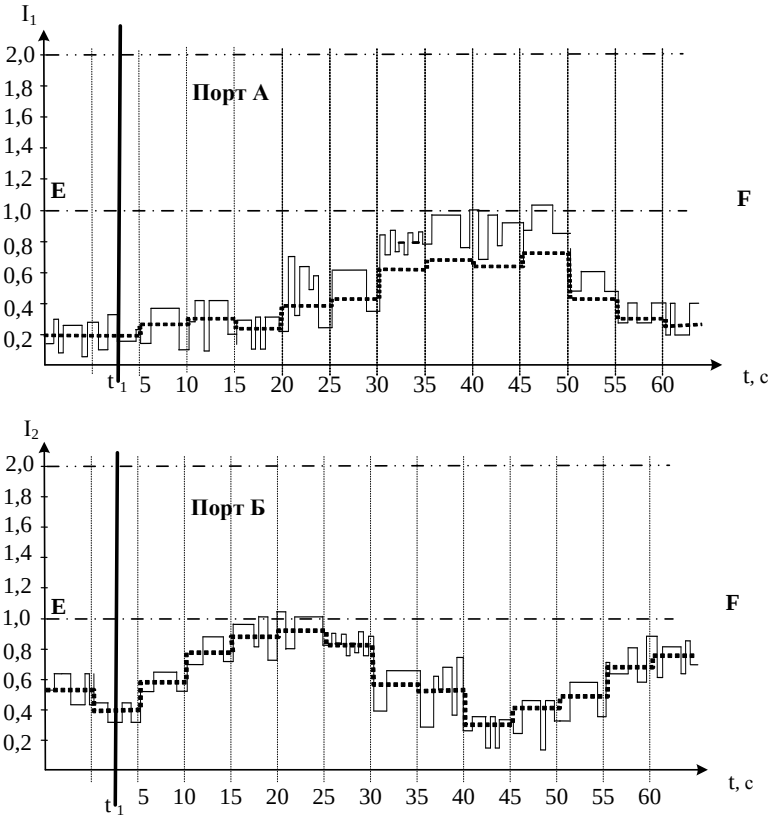
$$k_{ГНН} = I_{ГНН} / I_{доб}. \qquad (13.6)$$

Година найбільшого навантаження (ГНН) – це неперервний інтервал часу тривалістю 60 хвилин, протягом котрого середня інтенсивність навантаження є найбільшою за добу.

13.4. Визначення характеристик нерівномірності пакетного трафіку

13.4.1. Візьмемо найпростіший випадок 2-портового (на уводі) пакетного комутатора із пропускною здатністю 2,0 тис. оброблюваних пакетів за секунду. В початковий момент шляхом відповідного конфігурування програмного забезпечення (ПЗ) цього комутатора розподілимо його пропускну здатність порівну між його двома портами. В цьому разі продуктивність (або, як не зовсім точно кажуть, ширина смуги пропускання) кожного із портів комутатора буде дорівнювати 1,0 тис. пакетів за секунду. Включимо цей комутатор у фрагмент пакетної мережі і навантажимо кожний із портів певним потоком увідних пакетів. (Потоки вивідних пакетів не розглядаємо, щоб не ускладнювати ситуацію).

Будь-який потік пакетів у мережах з пакетною комутацією, зокрема в Інтернет, має складний пульсуючий характер (див. рис.13.1). На жаль, надійних апробованих математичних моделей пульсуючих потоків пакетів поки що не розроблено. На відміну від потоків телефонних викликів (рос. – вызовов), для котрих розроблено добре апробовані математичні моделі, що вивчаються у рамках навчальної дисципліни «Теорія телетрафіка». Щодо пакетного трафіка то слід вказати на більш/менш вдалі спроби його математичного моделювання, зокрема шляхом його представлення у вигляді фрактального або самоподібного процесу.



I_i – швидкість потоку на і-му порту, де і=1,2

Рис.13.1. Типовий приклад однохвилинної реалізації потоків пакетів низької інтенсивності на портах пакетного комутатора

Тим не менш, на рівні якісного аналізу можливо стверджувати, що інтенсивність реального пульсуючого потоку пакетів зручно розділити на дві складові. Одна складова – це повільно змінюваний у часі майже передбачуваний процес (в залежності від годин доби, розкладу роботи користувачів, випадкових зовнішніх подій тощо), що являє собою процес порівняно нешвидких змін у часі поточних величин інтенсивності потоку пакетів (тобто, змін

середньої швидкості надходження пакетів до порту комутатора), виміряних на великих проміжках часу. Друга складова – це, як правило, непередбачуваний процес швидкісних змін у часі (як кажуть, - пульсацій) миттєвих значень інтенсивності потоку пакетів (тобто, швидких змін миттєвої швидкості надходження пакетів до порту комутатора).

Миттєві зміни швидкості потоку – непередбачуваний результат одночасної діяльності багатьох користувачів, які непередбачуваним чином включають/виключають на комп'ютерах свої прикладні застосування.

Примітка 13.6. Нагадаємо, що непередбачуваний процес має принципову відмінність від випадкового процесу. Випадковий процес характеризується звісною функцією розподілу ймовірностей або хоча б звісними характеристиками цієї функції розподілу, такими як математичне чекання, дисперсія, функція кореляції і т. ін.. В той час як для непередбачуваного процесу його функція розподілу вважається невідомою. Поведінку випадкового процесу з певною ймовірністю можливо передбачити, а непередбачуваний процес тому і зветься непередбачуваним, що хід його змін неможливо оцінити та вгадати.

Повільні зміни середньої швидкості потоку пакетів називають трендом потоку, а швидкі зміни миттєвих значень швидкості потоку називають пульсаціями потоку.

На верхньому рисунку 13.1 надано характерний приклад однохвилинного часового відрізку реалізації потоку пакетів низької інтенсивності, де пунктирною лінією показані повільні зміни тренду потоку, що надходить на увід порту А, а суцільною лінією, котра флуктуює впродовж цього тренду, показані пульсації потоку пакетів. I_1 - інтенсивність (або швидкість) потоку пакетів на уводі порту А. Горизонтальна пунктирна лінія EF, що проведена паралельно часовій вісі на рівні 1,0 тис. пакетів відображає пропускну здатність (щодо швидкості обробки пакетів) увідного порту А пакетного комутатора, що є предметом даного розгляду.

На нижньому рисунку 13.1 відображений цей же часовий відрізок, але стосовно реалізації потоку пакетів, що надходить до другого порту комутатора (до порту Б). Експлуатаційна практика показує, що у більшості випадків швидкість зростання та убування миттєвої швидкості потоку пакетів на портах комутатора, величини пульсацій та терміни їхнього існування мають майже не прогнозований характер. Як бачимо із рис.13.1, характер змін

інтенсивності в обох потоках для даного прикладу майже однаковий, але якщо перший потік має значно менші величини середньої інтенсивності на першій половині відображеного часового проміжку у порівнянні із величинами середньої інтенсивності цього потоку, відображеними на другій половині часового проміжку, то щодо другого потоку – картина майже протилежна. Якщо мати на увазі, що $К_{зі}$ - коефіцієнт навантаження і-го порту комутатора вимірюється відношенням середньої інтенсивності потоку, що надходить до порту, до пропускної здатності цього порту, то для нашого прикладу в точці t_1 миттєві значення цього коефіцієнту для порту А складають $К_{з1}$=0,2, а для порту Б складають $К_{з2}$=0,5. В майже всіх інших часових точках існування потоків значення коефіцієнту навантаження портів для наведеного прикладу набагато менші за одиницю, при цьому потоки не є синхронними. Винятки складають невеличкі проміжки часу (часовий відрізок між 45 та 50 секундою на верхньому рисунку та відрізок в районі 20 секунди на нижньому рисунку), коли миттєві значення навантаження портів перевищують їхні пропускні спроможності. Пряма горизонтальна лінія EF на кожному із рисунків 13.1 відображає пропускну здатність відповідного порту комутатора (щодо наведеного прикладу - на рівні 1,0 тис. пакетів за секунду). Коефіцієнт навантаження порту дорівнює 1 у випадку, коли швидкість просування пакетів через цей порт дорівнює його пропускній здатності. Як бачимо із рис.13.1, існує значний запас щодо підвищення завантаженості обох портів комутатора, оскільки усереднені на однохвилинному інтервалі коефіцієнти завантаження кожного із портів виявились значно меншими за одиницю (десь на рівні 0,45). Пульсації потоків на обох портах хоч і мають значні коливання, але вони, здебільшого, не перевищують лінії пропускних здатностей портів, що означає відсутність перенавантажень портів комутатора і можливість надання високоякісних послуг (оскільки за цих умов механізми знищення пакетів у комутаторі через перенавантаження його портів не включаються в роботу, а черги у буферній пам’яті портів не переповнюються – як результат, незапланованих затримок пакетів в мережі не відбувається).

Примітка 13.7. Аналізуючи «поведінку» потоків пакетів на рис.13.1, слід

звернути увагу на моменти перевищення інтенсивності цих потоків лінії EF, що відображає величину пропускної здатності порту пакетного комутатора. У даному прикладі пропускна здатність кожного із двох портів зафіксована на рівні 1,0 тис. пакетів в секунду. От же, якщо миттєва швидкість потоку пакетів, що просуваються на увід порту (яка визначається як інтенсивність навантаження на цей порт) перевищить пропускну здатність порту, то в цей момент, якщо не передбачити відповідних заходів, комутатор буде не в змозі нормально обробити усі пакети даного потоку. Тобто, або виникнуть небажані затримки пакетів в чергах, що утворюються у буферній пам'яті порту комутатора, або, взагалі, надлишкові пакети будуть незворотно втрачені. Тому для запобігання таким небажаним подіям в пакетних комутаторах передбачено використання спеціалізованих програмно-апаратних механізмів (зокрема, утворення черг пакетів у буферній пам'яті портів, приорітезація потоків, їхнє згладжування і т. ін..), які активізуються в моменти, коли пульсації пакетного трафіку перевищують пропускну здатність обладнання, що цей трафік оброблює. Технологія запобігання небажаним наслідкам пульсацій потоків пакетів реалізується у рамках так званої інженерії трафіка, яка буде далі розглядатися.

Хотілося б підвищити коефіцієнт завантаження портів розглянутого комутатора, але при цьому не втратити можливість надання послуг із необхідним рівнем якості. На рис.13.1 маємо п'ятисекундні інтервали усереднення пакетного трафіку. Якщо оцінювати можливий діапазон значень коефіцієнту навантаження кожного із портів розглянутого комутатору саме на цих п'ятисекундних інтервалах, то неважко упевнитися, що він лежить у межах 0,2 - 1,0. Тобто, в якісь п'ятисекундні інтервали маємо значне недовантаження обладнання портів комутатора (коли $0,2 \le K_{зі} \le 0,4$), а в якісь інтервали маємо високе навантаження, яке б задовольнило будь-якого оператора ТЛК-мережі (коли $0,65 \le K_{зі} \le 1,0$).

Рішення задачі підвищення коефіцієнтів завантаження портів здійснимо на шляху запровадження принципу адаптивного керування пропускною спроможністю портів пакетного комутатору за критерієм максимізації коефіцієнту використання обладнання цього комутатору за умов неперевищення нормативів якості обробки пакетів. (Зазвичай у ролі показників якості, що нормуються, вибирають рівень затримок пакетів та коефіцієнт втрат пакетів).

13.4.2. Розглянемо найпростішу процедуру адаптивного керування шириною смуг портів комутатора, що не в повній мірі, але здатний враховувати "поведінку" пакетного трафіку на його

портах. Припустимо, що у складі обладнання комутатора функціонує функціонально простий аналізатор, який здатний лише вимірювати поточні значення відсотку знищених пакетів на уводах портів комутатора у порівнянні із загальною кількістю пакетів потоку, що надходять до цих портів. Такі вимірювання аналізатор кількості знищених пакетів здійснює через апріорі визначені достатньо короткі проміжки часу (наприклад, через кожні 10с). Припустимо також, що у складі комутатору функціонує система автоматичного регулювання (САР) з відповідними регуляторами, яка дозволяє у реальному часі перерозподіляти пропускну здатність комутатора між його портами в залежності від виміряних аналізатором даних. Роботу вищеназваної системи можна пояснити наступним чином. Поки виміряні значення відсотку знищених пакетів на портах комутатора будуть меншими за припустимий відповідними нормами рівень втрат пакетів (наприклад, меншими за 1%), САР не змінює пропускні здатності (ширини смуг) портів комутатора, оскільки в цьому стані перенавантаження портів – відсутні, а потоки пакетів отримують якісну і своєчасну обробку в комутаторі. Але як тільки аналізатор виявить факт перевищення відсотку знищених пакетів одновідсоткового порогу на одному із портів, то це означає виникнення перенавантаження на цьому порту і доцільність включення адаптаційного механізму перерозподілу пропускної здатності комутатора на користь перенавантаженого порту за рахунок недовантаженого порту. (Зрозуміло, якщо обидва порти одночасно увійшли в стан перенавантаження, то без втрат в якості обслуговування вийти із цього стану неможливо, і в цій ситуації будь-які механізми адаптації не допоможуть. Але таке, як свідчать результати експлуатаційних вимірювань, трапляється дуже рідко). Іншими словами, в момент часу, коли аналізатор кількості знищених пакетів виявить перенавантаження лише в одному із двох портів комутатора, то в цей момент включається механізм перерозподілу пропускної здатності комутатора таким чином, що смуга пропускання перенавантаженого порту розширюється за рахунок звуження смуги пропускання недовантаженого порту. Ця ситуація відображена на рис. 13.2.

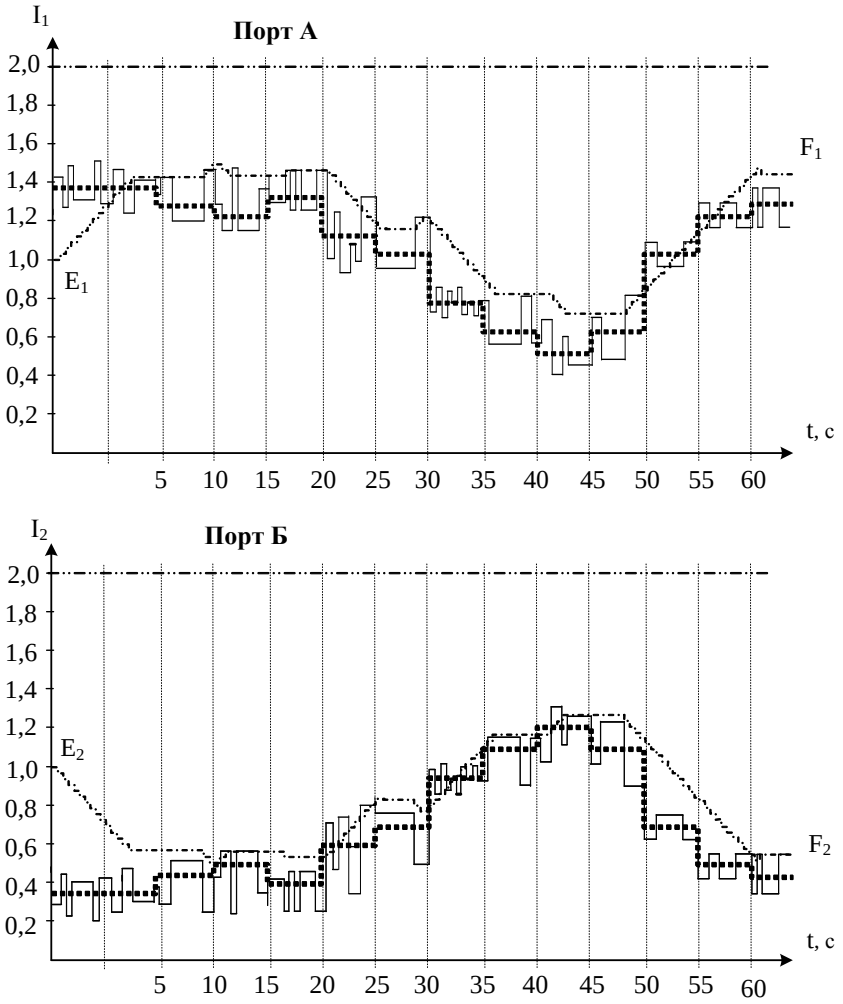


Рис.13.2. Ілюстрація прикладу адаптивного регулювання смуг пропускання портів пакетного комутатору

Як бачимо, на різних проміжках часу виділяються різні за величиною смуги пропускання портів комутатора таким чином, що на проміжках часу, коли, наприклад, на першому порту

інтенсивність потоку пакетів збільшується (загрожуючи перенавантажити цей порт пакетним трафіком), ширина смуги пропускання цього порту розширюється (пряма пропускної здатності першого порту E_1F_1 піднімається уверх) . Одночасно з цим ширина смуги іншого порту зменшується (пряма пропускної здатності другого порту E_2F_2 пересувається униз), але не настільки, щоб на цьому порту утворились перенавантаження.

Припустимо, що на певному проміжку часу на першому порту аналізатор виявив перенавантаження – тому саме цьому порту додається певна частка пропускної здатності комутатора так, щоб уникнути перенавантаження (тобто, щоб верхні піки пульсацій потоку на цьому порту стали нижче за лінію E_1F_1). На другому порту на цьому проміжку часу було недовантаження – тому ширина смуги цього порту дещо звужується, але не настільки, щоб на ньому виникло перенавантаження (лінія пропускної здатності E_2F_2 цього порту також не перетинається верхівками пульсацій потоку, що надходить до цього порту). Якщо розрахувати коефіцієнти використання портів для умов, що відображені на рис.13.2, то можливо констатувати, що усереднені значення цього коефіцієнту на обох портах суттєво підвищилися до рівнів, що перевищують 0,7 – 0,75. При цьому, якщо не спостерігаються часті та (або) значні піки пульсацій трафіка, шляхом коректного вибору закону авторегулювання за цих умов є можливим запобігти суттєвим перевищенням поточним трафіком смуг пропускання портів комутатору, що свідчитиме про можливість якісної обробки пакетів портами комутатора. На жаль, реальний пакетний трафік характеризується досить частими великими та “гострими” піками пульсацій, які, зрозуміло, негативно впливають на можливість підвищення коефіцієнта використання комутаторного обладнання. Тому в експлуатаційній практиці отримали широке застосування різноманітні механізми так званого “згладжування” пульсацій потоку пакетів.

13.4.3. На рис.13.3 відображені вже згладжені потоки пакетів на обох портах комутатора, що розглянуті на попередньому рис.13.2.

Як бачимо, після згладжування піки потоків “розмазались” і створились умови для суттєвого підвищення завантаження комутатора.

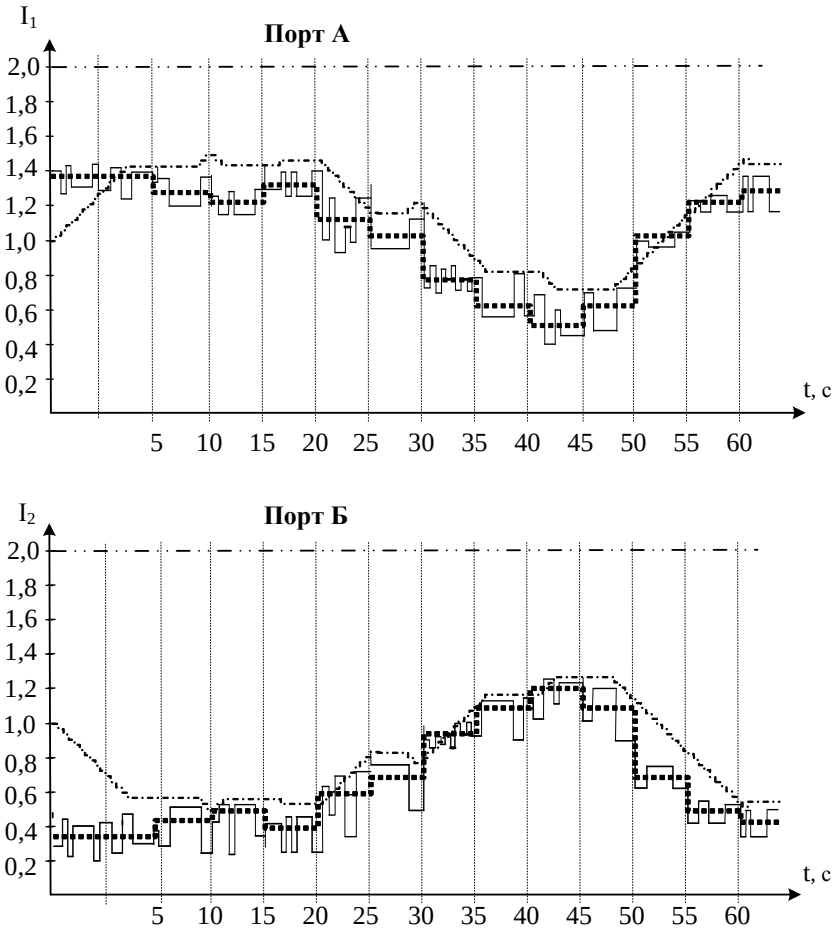


Рис.13.3. Ілюстрація прикладу адаптивного регулювання смуг пропускання портів комутатора з урахуванням механізмів "згладжування" пульсацій пакетного трафіку

Тим не менш, в багатьох випадках за умов, коли пакетний трафік характеризується значною кількістю великих за величиною та тривалістю піків, параметри котрих непрогнозовано змінюються

у часі з великою швидкістю, динамічні характеристики системи авторегулювання перерозподілом пропускної здатності комутатора мають вирішальне значення. Дійсно, розглянута вище система авторегулювання не має у своєму складі елементів, котрі дозволяють своєчасно реагувати на швидкі зміни у пульсаціях трафіку.

Тому сигнали авторегулювання часто не встигають за темпом змін у трафіку. Як результат, спостерігається ситуація, коли або поточний трафік досить часто перевищує пропускну спроможність портів (в цьому випадку через втрати пакетів якість обслуговування різко погіршується), або з метою запобігання втрат пакетів здійснюється резервування пропускної здатності комутатора (за рахунок певного зниження коефіцієнтів навантаження елементів мережного обладнання).

Від вищенаведених недоліків буде позбавлено комутаційне обладнання, у складі котрого застосовується САР, що здатна своєчасно відслідковувати характер змін у пульсаціях пакетного трафіка. На жаль, реальний трафік в мережах пакетної комутації характеризується надзвичайно високою швидкістю змін. Тому до технічних засобів САР щодо параметрів швидкодії висуваються надзвичайно жорсткі вимоги. Навіть за умов застосування сучасної наносекундної елементної бази не завжди вдається побудувати САР, що встигали б відслідковувати реальні зміни характеристик потоків пакетів на портах комутаторів. Тому з урахуванням вищезазначеного особливо привабливими виглядають системи, що містять у своєму складі механізми прогнозування майбутнього стану потоків пакетів на портах комутатора. Однак ці системи виходять за межі даного розгляду.

13.5. Методи вимірювання навантаження

Вимірювання показників навантаження широко використовуються під час вирішення багатьох експлуатаційних завдань. Володіння методами та практичними навичками вимірювання цих показників конче необхідне експлуатаційному персоналу, особливо адміністраторам, в зоні відповідальності котрих знаходиться група задач *Performance Maintenance*. Розглянемо кілька характерних експлуатаційних задач, вирішення

котрих напряму пов'язано із вимірюванням показників навантаження.

1) Персонал, який займається задачами *Performance Maintenance*, повинен раціональним чином розподіляти потоки інформації, що просуваються каналами зв'язку між вузлами мережі, з тим, щоб забезпечити необхідний рівень якості обслуговування цих потоків. Адміністратори, зазвичай, намагаються більш/менш рівномірно завантажити усі елементи мережного обладнання, оскільки у цьому разі усі користувальницькі потоки з точки зору запобігання негативному впливу пульсацій трафіку знаходяться у приблизно однакових умовах. (На більш завантажених ділянках мережі ймовірність перенавантаження внаслідок пульсацій трафіка суттєво збільшується). Крім того, на рівномірно завантаженій мережі значно простіше визначити різницю між її пропускною спроможністю та обсягом вже задіяних мережних ресурсів і, отже, більш точно оцінити можливості щодо збільшення її завантаженості (з метою подальшого підключення нових користувачів, уведення додаткових послуг, підвищення якості обслуговування тощо).

2) Персонал повинен постійно слідкувати в оперативному режимі за «поведінкою» трафіка, намагаючись вчасно виявити нештатні події, що виникли внаслідок непрогнозованого збільшення розмаху та (або) тривалості пульсацій трафіку. Такі нештатні події можуть призвести до суттєво негативних, а в окремих випадках і до форс-мажорних наслідків.

Якщо внаслідок неочікуваних обсягів пульсацій пакетного трафіку пакети в чергах буферних пристроїв портів активних мережних елементів (комутаторів, маршрутизаторів тощо) затримуються довше розрахованого часу, то порушуються умови сервісних угод (*SLA*) з клієнтами щодо обумовлених параметрів затримок і девіації затримок пакетів. Це призводить до неякісного обслуговування чутливого до затримок трафіку (мультимедіа, IP-телефонія тощо). Однак можливі і більш негативні наслідки.

В мережах з комутацією пакетів через тривалі або, можливо, нетривалі, але великі за розмахом пульсації трафіку виникають переповнення черг у буферних пристроях портів. Черги мають,

іноді хоч і доволі великі, але кінцеві розміри. Тому «зайві» пакети (тобто, ті, що не помістилися у чергах), як правило, знищуються, що призводить до підвищення коефіцієнту втрат пакетів за межі унормованих значень. Як результат, користувальницькі потоки не отримують обумовлені у *SLA* рівні якості обслуговування. В окремих випадках через різке і тривале збільшення коефіцієнту втрат пакетів у мережі нормальне функціонування прикладних задач користувачів взагалі виявляється неможливим, що призводить до відмови в обслуговуванні.

В мережах з комутацією каналів через стрімке збільшення інтенсивності навантаження (наприклад, внаслідок незвичайної активності телефонних абонентів) також можливі відмови в обслуговуванні клієнтів. Тому оператори телефонних мереж намагаються відслідковувати незвичайні (особливо, форс-мажорні) події у суспільному житті громадян, які користуються їхніми послугами, з тим, щоб своєчасно прийняти необхідні заходи з розподілу потоків інформації, що просуваються каналами зв'язку між вузлами телефонної мережі.

3) Персонал повинен мати можливість виявлення та локалізації проблем, що пов'язані із перенавантаженням елементів обладнання. Для цього, необхідно, перш за все, організувати вимірювання поточних значень інтенсивності потоків інформації на кожному із елементів мережі.

4) Персонал має забезпечити оперативну фіксацію інформації щодо інтенсивності оброблюваного трафіка. Ця інформація використовується як вихідна в задачах оптимізації роботи мережі, прогнозування навантаження на мережу, інженерії трафіка (див. далі), планування та подальшого розвитку мережі. На основі результатів прогнозування навантаження здійснюють розрахунки необхідної кількості додаткового обладнання (каналів транспортування інформації, комутуючого та іншого вузлового обладнання), яке має бути уведено в дію для забезпечення якісного обслуговування клієнтів мережі. Після усереднення та статистичної обробки зафіксованої інформації щодо інтенсивності трафіка та порівняння цієї інформації із можливостями обладнання мережі, зазвичай, виявляються шляхи подальшого удосконалення характеристик мережі: підвищення коефіцієнту навантаження на

мережу без втрати рівня якості обслуговування; підвищення рівня якості обслуговування шляхом більш раціонального вибору параметрів служби *QoS* (див. далі); переінсталяція параметрів механізмів згладжування та формування трафіку (зокрема, зміна виділених для черг обсягів буферної пам'яті) і т. ін.

Як бачимо, вимірювання навантаження елементів мережі широко застосовується в експлуатаційній практиці.

В залежності від змісту вирішуваних завдань обираються відповідні показники навантаження, методи та інструментальні засоби його вимірювання.

Розглянемо методи вимірювання навантаження в мережах з комутацією каналів. В системах комутації каналів, як було вже вказано, навантаження вимірюють у кількості годино-зайнять на визначеному інтервалі часу, а інтенсивність навантаження – у ерлангах [год.-зайн./год.]. Необхідно підкреслити, що вимірюється тільки дійсне навантаження, яке реально було обслужене. Так зване втрачене навантаження (наприклад телефонні виклики), що з різних причин не було обслужене, безпосередньо виміряти неможливо (оскільки не є відомою тривалість викликів, що обслужені не були). Проте втрачене навантаження можливо розрахувати (якщо в цьому виникає потреба) через виміряні значення інтенсивності дійсного навантаження згідно формул, відомих із теорії телетрафіка, котрі у даній лекції не розглядаються.

Якщо існує потреба виміряти навантаження на якомусь одному двохполюсному елементі мережі з комутацією каналів (зокрема, на абонентській телефонній лінії) за певний період часу (наприклад, від *0* до *T*), то слід використати будь-який вимірювальний засіб (програмний або апаратний), який здатний фіксувати проміжки часу, коли цей елемент зайнятий обслуговуванням. Тоді навантаження на цей елемент *H* (за визначений період часу) визначиться згідно формулі

$$H = \sum_{i=1}^{n} H_i , \qquad (13.7)$$

де H_i - тривалість *i*-го зайняття елементу мережі, *n* - кількість зайнять елемента мережі протягом інтервалу *0,T*.

Якщо отримане таким чином навантаження H розділити на загальний час вимірювань у годинах, тобто віднести його до одиниці часу, то отримана величина буде представляти інтенсивність навантаження $У$ цього двохполюсного елементу:

$$У = H / T = \sum_{i=1}^{n} H_i / \sum_{i=1}^{n} t_i. \qquad (13.8)$$

Якщо існує потреба виміряти навантаження на багатополюсному елементі мережі з комутацією каналів (зокрема, на комутаторі каналів) за певний період часу (наприклад, від 0 до T), то слід використати будь-який вимірювальний засіб (програмний або апаратний), який здатний фіксувати кількість зайнятих обслуговуванням двохполюсних елементів (наприклад, зайнятих телефонних ліній) в окремі моменти часу. Оскільки середнє значення навантаження багатополюсного елементу за період вимірювань дорівнює середній кількості одночасно зайнятих двохполюсних елементів, то навантаження H на багатополюсний елемент (за визначений період часу) визначиться згідно формулі

$$H = \sum_{i=1}^{N} k_i, \qquad (13.9)$$

де k_i - кількість одночасно зайнятих двохполюсних елементів під час i-го сканування багатополюсного елементу; N - загальна кількість сканувань.

Вищенаведений метод вимірювання навантаження багатополюсного елементу іноді називають методом сканування, якому, на жаль, притаманна певна методологічна похибка, оскільки відповідно до нього навантаження вимірюється лише у певні окремі моменти, а не безперервно у часі. Середня похибка методу сканування визначається за формулою Пальма:

$$dH = H \cdot \mathrm{SQRT}\left(\frac{1}{n} \cdot \left(\frac{1 + e^{+\alpha}}{1 - e^{-\alpha}} - 2\right)\right), \qquad (13.10)$$

де n - сумарна кількість зайнятих двохполюсних елементів за весь період вимірювань T; α - відношення інтервалу Δt між двома суміжними моментами сканування (інтервалами сканування) до середнього часу одного зайняття θ.

Зрозуміло, що для визначення інтенсивності навантаження на багатополюсний елемент необхідно отримане значення навантаження H розділити на загальний період сканування T.

Розглянемо методи вимірювання навантаження в мережах з комутацією пакетів. В системах комутації пакетів, як було вже вказано, навантаження вимірюють у кількості інформації (тобто, бітів, байтів, фреймів, пакетів і т. ін.), що була оброблена обладнанням системи протягом певним чином обраного періоду часу. Якщо цей період виявиться тривалим, то оперувати значними обсягами інформації, що представляють навантаження, при вирішенні експлуатаційних завдань буде незручно. Тому при експлуатації пакетних мереж, головним чином, користуються поняттям «інтенсивність навантаження», що розуміється як кількість оброблених пакетів (точніше – протокольних блоків даних, *PDU*) протягом однієї секунди. Так що параметр інтенсивності навантаження має розмірність швидкості обробки пакетів вузловим обладнанням (або швидкості транспортування пакетів, якщо мова йде про канали передачі даних).

Для вимірювання інтенсивності навантаження в пакетних мережах, як правило, використовують методи прямого підрахунку *PDU*, що просуваються через певним чином обрану точку вимірювання. Кожна подія перетину пакетом точки вимірювання фіксується та накопичується у відповідному лічильнику. Зрозуміло, що для обробки гігабітових потоків необхідно резервувати великі обсяги пам’яті, якщо ми бажаємо накопичити дані про поточну інтенсивність завантаження на великих проміжках часу. Тому з метою економії пам’яті дані про поточну інтенсивність завантаження, як правило, усереднюють на інтервалах різної тривалості. Величина інтервалу усереднення залежить від змісту

експлуатаційних задач.

З метою зменшення ресурсів пам'яті, що мають бути витрачені на проведення вимірювань, вимірювання інтенсивності навантаження в деяких випадках проводять вибірково з певним періодом вимірювань. За цих умов отримують не всю можливу сукупність даних про інтенсивність навантаження (так звану генеральну сукупність), а лише певну її частину (тобто, вибіркову сукупність). Як результат, виникає помилка вибірки Δ, яка визначається як величина відхилення певних параметрів вибіркової сукупності даних від аналогічних параметрів генеральної сукупності. Вибіркова сукупність повинна з контрольованою точністю відображати генеральну сукупність даних, що робить актуальним завдання оцінки мінімально необхідного обсягу вибіркових даних n, які забезпечують задану точність вимірювань (тобто, не перевищення припустимого значення помилки вибірки Δ). Така оцінка робиться з використанням методів математичної статистики. Зокрема, один із найпростіших методів визначення необхідного обсягу вибіркових даних полягає в наступному.

Помилку вибірки Δ розуміють як відхилення середнього значення вибіркової сукупності з обсягом n від середнього значення генеральної сукупності з обсягом N, де $N >> n$. Тоді відповідно до теореми Чебишева – Ляпунова

$$\Delta \approx \gamma \sigma / \sqrt{n}, \qquad (13.11)$$

де γ – коефіцієнт, що визначає ймовірність того, що фактична помилка виявиться не більше Δ (існує у табульованому вигляді; якщо, наприклад, γ =2,6, то формула є вірною з ймовірністю 1%); σ – середньо квадратичне відхилення вибіркової сукупності.

Вирішуючи (13.11) відносно n, отримаємо значення мінімально необхідного обсягу вибіркової сукупності:

$$n_{min} = \gamma^2 \sigma^2 / \Delta^2. \qquad (13.12)$$

13.6. Оцінка характеристик обладнання з урахуванням інтенсивності навантаження

Поняття «інтенсивність навантаження» широко використовується в експлуатаційній практиці при вирішенні різноманітних експлуатаційних завдань. Розглянемо приклад, що є типовим для задач експлуатації телефонних мереж, коли використовують звісні співвідношення між продуктивністю обладнання комутаційної системи, ємністю абонентської бази телефонного вузлу та необхідною пропускною здатністю міжстанційних ліній зв'язку.

Припустимо, що необхідно організувати так званий виніс (тобто, віддалений концентратор абонентських телефонних каналів), що має бути розташованим у сільському населеному пункті, віддаленому від однієї із районних АТС м.Києва. Функціональні можливості виносу у порівнянні із повноцінною АТС суттєво звужені. Зокрема, абоненти, що приєднані до одного виносу, вимушені створювати телефонні з'єднання при спілкуванні між собою тільки через віддалену АТС. Проте в якості виносу можливо використати, як варіант, і міні АТС. У даному випадку суттєвою перевагою застосування виносу (а не повно функціонального сільського телефонного вузлу) для селян є забезпечення можливості користування номерним ресурсом київської міської телефонної мережі.

Припустимо також, що лінія зв'язку між київською АТС та сільським виносом вже прокладена, а на базі цієї лінії побудована цифрова система передачі (ЦСП) з використанням обладнання типу ІКМ-30. Пропускна спроможність побудованої ЦСП – 2хЕ1, тобто забезпечена можливість одночасного передавання 2х30=60 телефонних розмов.

За таких умов для організації виносу необхідно визначити:

1) мінімально необхідну продуктивність обладнання виносу;

2) максимально можливу кількість абонентів, що можуть бути підключені до виносу;

3) необхідну кількість абонентських портів станційного обладнання київської АТС для підключення виносу до цієї АТС.

Визначення вищезазначених трьох параметрів обладнання фрагменту телефонної мережі отримаємо із застосуванням поняття

«інтенсивність навантаження».

Інтенсивність навантаження елементів обладнання фрагменту телефонної мережі, що розглядається у даному прикладі, доцільно визначати в ерлангах (Ерл). Для двохполюсної мережі 1Ерл = 1 год.-зайн./год. Проте на ділянці між АТС та її виносом маємо 60 еквівалентних двохполюсних мереж. Тому максимально можлива у даних умовах інтенсивність навантаження обладнання ЦСП – 60Ерл.

Якщо в якості показника продуктивності виносу обрати максимально припустиме значення інтенсивності його навантаження, за яким під час функціонування виносу не порушуються припустимі норми за усіма іншими показниками якості його роботи (зокрема, за показниками завадостійкості, затримок у встановленні/роз'єднанні телефонних з'єднань тощо), то у нашому прикладі мінімально необхідна продуктивність виносу має бути визначена на рівні 60Ерл, не менше.

Для визначення максимально можливої кількості абонентів, що можуть бути підключені до виносу, необхідно задатися розрахунковим значенням можливого питомого навантаження на одну абонентську лінію, що підключена до виносу. Раніше, коли ще не було Інтернету, цей показник регламентувався національними та міжнародними нормами на рівні 0,07Ерл на одного абонента, тобто вважалося, що у середньому протягом однієї години одна абонентська лінія може бути зайнятою телефонними перемовинами не більше 4,2 хвилин. Сучасні абоненти, як свідчить практика, більш активно користуються послугами телефонного зв'язку. Тому в якості сучасної норми показника питомого навантаження на одну абонентську лінію беруть значення 0,1 – 0,2 Ерл/аб (для звичайних користувачів) або 0,2- 0,4 Ерл/аб (для бізнес-клієнтів). У нашому прикладі задамося розрахунковим значенням показника питомого навантаження на одну абонентську лінію, що підключена до виносу, на рівні 0,15Ерл/аб, тобто будемо вважати, що у середньому протягом однієї години кожна окрема абонентська лінія може бути зайнятою телефонними перемовинами не більше 9,0 хвилин. За цих умов мережа абонентського доступу до обладнання виносу має складатися із 60Ерл / 0,15Ерл = 400 абонентських ліній, не більше.

Інакше, неприпустимо зростає ймовірність виникнення перенавантаження елементів обладнання даного фрагменту телефонної мережі. Так що, для нашого прикладу максимально можлива кількість абонентів, що можуть бути підключені до виносу, складає 400 осіб.

Щодо третього показника, тобто необхідної кількості абонентських портів станційного обладнання київської АТС, через котрі віддалений виніс буде підключено до цієї станції, то він має дорівнювати сумарній кількості телефонних розмов, що одночасно передаються засобами побудованої ЦСП. У нашому прикладі для підключення виносу до АТС має бути зарезервовано 60 портів. Маються на увазі логічні, а не фізичні порти.

Контрольні питання до тринадцятої лекції

1. Надайте визначення терміну «навантаження».
2. Надайте визначення терміну «інтенсивність навантаження».
3. Що таке експлуатаційна пропускна здатність обладнання?
4. Чим відрізняється визначення навантаження на обладнання мереж з комутацією пакетів від визначення навантаження на обладнання мереж з комутацією каналів?
5. Що таке миттєвий коефіцієнт навантаження?
6. Що узято за одиницю вимірювання навантаження у мережах з комутацією каналів?
7. Що таке двохполюсна мережа? Яке максимальне навантаження витримує двохполюсна мережа протягом однієї години?
8. Надайте визначення коефіцієнту навантаження на телефонний вузол?
9. Надайте характеристику змінам інтенсивності трафіку?
10. Що таке один ерланг?
11. Назвіть показники нерівномірності навантаження.
12. Які три складові у змінах інтенсивності пакетного трафіку Ви здатні назвати?
13. Які показники використовуються для кількісного оцінювання регулярної складової нерівномірності навантаження?
14. Надайте визначення коефіцієнту концентрації для години найбільшого навантаження.

15. Що таке ГНН?

16. Поясніть принцип адаптивного керування пропускною спроможністю портів пакетного комутатору.

17. Які методи вимірювання навантаження Ви знаєте?

18. Назвіть кілька характерних експлуатаційних задач, вирішення котрих напряму пов'язано із вимірюванням показників навантаження.

19. Як вимірюють навантаження на багатополюсному елементі мережі з комутацією каналів?

20. Поясніть метод сканування при вимірюванні навантаження багатополюсного елементу.

Література до тринадцятої лекції

1) М.Н.Арипов, Г.П.Захаров, С.Т.Малиновский, Г.Г.Яновский. Проектирование и техническая эксплуатация сетей передачи дискретных сообщений. –М.: Радио и связь, 1988. -360с.

САМОСТІЙНЕ ЗАНЯТТЯ ЗА МАТЕРІАЛАМИ ЛЕКЦІЇ №13 УПРАВЛІННЯ ТЕЛЕФОННИМ ТРАФІКОМ

13.7. Основні поняття та визначення

Телефонний виклик - це вимога джерела виклику на встановлення з'єднання з іншим абонентом, яке надійшло в мережу телефонного зв'язку. Виклики характеризуються моментом надходження. В якості джерела виклику може служити телефонний аппарат.

Основними термінами теорії телетрафіка (ТТ) є такі вихідні поняття як:

- повідомлення;
- виклик;
- заняття;
- час заняття;
- пучок ліній;
- трафік;
- година найбільшого навантаження;

- концентрація;
- втрати і т.д.

Предметом вивчення теорії телетрафіка стали процеси обслуговування системою телефонного зв'язку потоків повідомлень та їх кількісні характеристики на станціях, комутаційних вузлах, мережах зв'язку, а також їх окремих частинах.

Математичний апарат, досліджуваний теорією телетрафіка, включає чотири основні елементи:

- потік вхідних повідомлень;
- систему розподілу інформації, тобто систему обслуговування;
- характеристики якості системи;
- дисципліна обслуговування.

Потік повідомлень включає поняття про модель потоку викликів (вимог на з'єднання), закони розподілу тривалості обслуговування повідомлень, а також тип займаного для передачі повідомлень канала і спосіб передачі - аналоговий або дискретний.

Система обслуговування характеризується структурою побудови та набором структурних параметрів.

Під дисципліною обслуговування розуміють:

- спосіб обслуговування (з явними втратами, з очікуванням, з повторенням або комбінований);
- порядок обслуговування (в порядку черговості, у випадковому порядку і з пріоритетом);
- режим шукання виходів комутаційної системи (вільний, груповий і індивідуальний).

До характеристик якості обслуговування вхідних повідомлень належать:

- ймовірність явної втрати повідомлень;
- ймовірність умовної втрати повідомлень;
- середній час затримки повідомлень;
- ймовірність втрати виклику, що надходить;
- інтенсивність обслуговуваного навантаження і т.п.

До основних понять теорії телетрафіка відносять поняття повідомлення - як сукупності інформації, що має початок і кінець, і призначеної для передачі через мережу зв'язку або комутаційну систему. Повідомлення характеризується обсягом, категорією,

адресою джерела і приймача повідомлень, а також формою представлення інформації.

Повідомлення підрозділяється на:

- обслужене (передане через мережу зв'язку);
- втрачене (не передане внаслідок зайнятості, пошкодження, зайнятості і не відповіді приймача);
- затримане (надійшло в мережу зв'язку і очікує початку передачі);
- умовно втрачене (надійшло в мережу зв'язку і затримане понад допустимого (контрольного) строку, навіть якщо воно потім і було передане).

Виклик – це, як було вже відмічено, вимога джерела на встановлення з'єднання, яка надійшла в мережу зв'язку, комутаційну систему, на вхід ступені шукання, в керуючий пристрій (КП) з метою передачі повідомлень. Виклики характеризуються моментом надходження. Джерело виклику - телефонний або телеграфний апарат, прилад або лінія зв'язку, керуючий пристрій. Приймачами викликів також є апарати, прилади та лінії.

Виклики поділяються на:

- обслужені (коли джерела цих викликів отримали з'єднання з потрібними приймачами);
- загублені (які отримали відмову у встановленні з'єднань);
- затримані (ті, що очікують початку встановлення з'єднання через відсутність в даний момент вільних і доступних ліній);
- надходжені (незалежно від того, чи були ці виклики обслужені, втрачені або затримані).

Заняття - будь-яке використання приладів, ліній і пристроїв з метою встановлення з'єднань незалежно від того, закінчилося воно передачею повідомлень, чи ні. Заняття характеризується моментом і його тривалістю.

Час заняття (тривалість) - це проміжок часу, протягом якого лінія зайнята. Як правило, у розрахунках комутаційних пристроїв і в цілому при проектуванні систем електрозв'язку використовується середній час заняття.

Пучок ліній - це група ліній (приладів), на якій одночасно можна здійснювати передачу певної кількості повідомлень, наприклад,

певну кількість телефонних розмов.

Трафік (навантаження) – визначається як сума часу заняття у годинах

$$A = \frac{C \cdot \bar{t}}{60} \quad \textit{Ерланг} \tag{13.13}$$

де С - число викликів; $\bar{t}$ - середній час заняття у хвилинах; А – трафік.

Трафік, як правило, вимірюють у годинах найбільшого навантаження (ГНН).

Година найбільшого навантаження – це безперервний проміжок часу доби, протягом якого інтенсивність трафіку є найбільшою.

Розрахунок пропускної здатності мереж телекомунікації базується на вихідних даних на годину найбільшого навантаження (ГНН). Вважається: якщо вже в ГНН забезпечується необхідна якість обслуговування, то в інші години, тим більш, мережа має забезпечити необхідну якість. Слід також врахувати, що ГНН для різних видів телекомунікації не збігаються. Так, телефонний зв'язок використовує реальні масштаби часу, що вимагає безумовного забезпечення необхідних ресурсів мережі для задоволення запитів користувачів. У той час, як при передачі даних, доставка повідомлень може бути відкладена на інші години, зокрема на момент спаду ГНН.

ГНН істотно впливають на трафік мережі, який оцінюється концентрацією k.

Під *концентрацією* розуміється зіставлення трафіку в ГНН із середньодобовим трафіком (середнє за 24 години) або середньомісячним трафіком (середнє за 30 діб х 24 години). Отримані таким чином величини, висловлюють добові чи місячні концентрації трафіку.

Значення трафіку для телефонних мереж істотно залежить від ємностей телефонних станцій та мережі у цілому.Концентрація на телефонних мережах коливається в залежності від ємності міських телефонних мереж (МТС) у межах k=*0,07÷0,17*.Проте якість обслуговування абонентів оцінюється не концентрацією, а втратами. *Втрати* - це міра якості обслуговування абонентів, якапозначається через – *Р*. Втрати визначаються як відношення

числа втрачених викликів до загальної кількості дзвінків, що надійшли на входи системи зв'язку (наприклад, на АТС):

$$P = \frac{C_{çàã}}{C_{ïîñò}} = \frac{C_{ïîñò} - C_{îáñ}}{C_{ïîñò}}, \qquad (13.14)$$

$C_{заг}$ – кількість втрачені викликів;

$C_{пост}$ – загальна кількість викликів;

$C_{обс}$ – кількість обслужених викликів.

Для телефонних мереж при втратах 0,02 ÷ 0,03 якість обслуговування мережі вважається задовільною.

Втрати обчислюються в тисячних частках. Якщо втрати P = 0,001, то це означає, що в середньому при великій кількості спостережень на кожну тисячу викликів буде втрачено один виклик.

13.8. Параметри телефонного трафіка

Основні параметри трафіку

Параметром, що істотно впливає на загальний трафік телефонних станцій і споруд зв'язку, є кількість джерел трафіку (,категорій абонентів) N.

На телефонних мережах розрізняють наступні категорії абонентів:

$N_{кі}$ - абоненти квартирного індивідуального сектору;

$N_{нг}$ - абоненти народно-господарського сектору;

$N_{бс}$ - абоненти бізнес сектору;

$N_{та}$ - абоненти телефонів-автоматів (таксофонів);

$N_{зл}$ - число з'єднувальних ліній (ЗЛ) до відомчих АТС (ВАТС).

Отже, загальне число абонентів складається як

$$N = Nкі + Nнг + Nбс + Nта + Nзл \qquad (13.15)$$

Іншим параметром трафіку, що враховується, є число викликів C, що надходять від кожного джерела. Тоді, відповідно до категорій абонентів необхідно розрізняти:

$C_{кі}$ - число викликів, що надходять від абонентів квартирного

індивідуального сектора телефонної мережі;

Снг - число викликів, що надходять від абонентів народно-господарського сектора;

Ста - число викликів, що надходять від таксофонів;

Сзл - число викликів, що надходять від ЗЛ до АТС.

Отже, середня кількість викликів визначається як

$$\overline{C} = \frac{\sum N_i C_i}{N} = \frac{N_{кі} C_{кі} + N_{нг} Снг + N_{бс} C_{бс} + N_{та} C_{та} + N_{зл} C_{зл}}{N} \quad (13.16)$$

Третім параметром трафіку є *середня тривалість заняття*, яка також залежить від категорії джерел викликів, а також видів з'єднань.

Розрізняють заняття, що характеризуються фактом здійснення розмов, зайнятістю абонента, невідповідю абонента, а також заняття, що пов'язані з помилками при наборі з боку абонента.

Статистика показує наступні дані про частки різного роду викликів і занять:

1) заняття, що закінчилося розмовою $К_р = 0,40 \div 0,60$;

2) заняття, що закінчилося зайнятістю абонента $К_{зн} = 0,20 \div 0,30$;

3) помилка при наборі номера $К_{пом} = 0,01 \div 0,03$;

4) невідповідь абонента $К_{на} = 0,12 \div 0,20$;

5) недобір або технічна несправність $К_{тех} = 0,03 \div 0,07$.

Прийнято, що сума всіх вищевказаних коефіцієнтів дорівнює одиниці:

$$K_р + K_{зн} + K_{пом} + K_{но} + K_{тех} = 1. \quad (13.17)$$

Перший коефіцієнт у виразі (13.17) визначає заняття, що закінчилися розмовою $К_р$. Для визначення цього коефіцієнта зазвичай використовують метод контрольних викликів. Метод зводиться до набору не менш 200 викликів від кожної станції в усіх напрямках з фіксацією і урахуванням кожного дзвінка. Дослідження показали, що середня тривалість заняття $t_р$ для телефонних мереж визначається як

$$t_р = t_{св} + t_{на} + t_{вс} + t_{пв} + Т + t_з, \quad (13.18)$$

де $t_{св}$ - час слухання сигналу "Відповідь станції" (3 с);

$t_{на}$ - 1,5с х n - час набору номера абонента;

n - число цифр у нумерації ГТС ;

$t_{вс}$ - час встановлення з'єднань (1,5 ÷ 2 с);

$t_{пв}$ - час посилки виклику (7 ÷ 8 с);

Т - середня тривалість чистої розмови;

tз - час звільнення приладів станцій після закінчення розмови (1 ÷ 1,5 с).

З урахуванням формули 13.18 виникає навантаження (трафік), яке для всіх категорій абонентів на станції можна визначити формулою:

$$A = \sum_{i=1}^{m} N_i C_i \bar{t}_i \qquad (13.19)$$

де i – категорія абонентів від 1 до m.

Якщо є дані про питому абонентського навантаження, тобто про трафік на одного індивідуального абонента y_i для різних категорій абонентів, то справедливо наступне:

$$y_i = C_i \cdot t_i. \qquad (13.20)$$

Тоді загальний для всієї станції трафік визначається формулою:

$$A = \sum_{i=1}^{m} N_i y_i \quad . \qquad (13.21)$$

Параметр y_i називають питомою абонентського трафіка категорії i і за рекомендацією Е.514 ITU-T в залежності від категорії може мати наступні значення:

$y_{кх}$ = 0,03 ерл.;

$y_{нх}$ = 0,06 ерл. ;

$y_{та}$ = 0,10 ерл.;

$y_{сл}$ = 0,17 ерл.

Раніше для проектування МТС в якості контрольних цифр приймалися наступні дані:

$y_{кв}$ = 0,03 ÷ 0,06 ерл;

$y_{нх}$ = 0,06 ÷ 0,12 ерл.

$y_{та}$ = 0,20 ÷ 0,40 ерл;

$y_{сл}$ = 0,60 ÷ 0,80 ерл;

$y_{атс} = 0,1 \div 0,60$ ерл;
$y_{бм} = 0,08 \div 0,20$ ерл.

13.9. Потоки телефонних викликів: властивості та характеристики

Випадкові потоки телефонних викликів класифікуються в залежності від наявності або відсутності трьох наступних їхніх властивостей:

- стаціонарності;
- післядії (точніше, - відсутності післядії);
- ординарності.

Стаціонарність потоку означає незмінність у часі статистичних параметрів процесу утворення викликів, тобто з часом ймовірнісні характеристики потоку не змінюються.

На міжміських та міжнародних телефонних станціях потік викликів має, як правило, явно виражений нестаціонарний характер, тому що інтенсивність потоку - число викликів в одиницю часу істотно залежить від годин доби, дня тижня, місяця року і навіть сезону року. Проте всередині доби майже завжди можна знайти одногодинні (наприклад, ГНН) або двогодинні проміжки часу (так звані.пікові періоди), протягом яких вступний потік викликів близький до стаціонарного.

Післядія - означає залежність ймовірнісних характеристик потоку від попередніх подій.

Потік викликів, що надходять від досить великої групи джерел, близький за своїми властивостями до потоку без післядії, якщо при цьому не враховувати повторних викликів. Потік від малої групи, навпаки, помітний післядією. Потік повторних викликів також є прикладом потоку з післядією, тобто повторний виклик виникає як результат втрати попереднього виклику.

Потік з післядією підрозділяється на два види - з простою і обмеженою післядією.

Ординарність означає практичну неможливість одночасного надходження дзвінків. Тобто, ймовірність надходження двох або більше викликів за будь-який нескінченно малий проміжок часу зводиться до нуля. У мережах електрозв'язку потік викликів, як

правило, ординарний.

До основних характеристик випадкового потоку відносяться: провідна функція, параметр потоку та інтенсивність.

Провідна функція випадкового потоку – це математичне сподівання числа викликів у проміжку [0, t). Ця функція - невід'ємна, безперервна і приймає тільки кінцеві значення.

Параметр потоку в момент t визначає щільність ймовірності надходження виклику:

$$\lambda(t) = \lim_{\Delta t \to 0} \frac{P_{i \geq 1}(t, t + \Delta t)}{\Delta t} \ . \qquad (13.10)$$

Інтенсивність стаціонарного потоку – математичне сподівання числа викликів в одиницю часу.

Для нестаціонарних потоків використовується поняття середньої і миттєвої інтенсивності.

Середня інтенсивність потоку в проміжку [t1, t2) – математичне сподівання числа викликів в цьому проміжку, що приведене до одиниці часу, і позначається як μ (t1, t2).

Миттєва інтенсивність потоку μ(t) в момент t – похідна провідної функції потоку по t.

Характеристики потоків викликів істотно впливають на схему розподілу реального трафіку на телефонних станціях. Рекомендується дослідження розподілу трафіку на станціях здійснювати за схемою, представленою на рис. 13.4.

Вимірювання трафіку, по суті, може бути зведене до вимірювання часу, а вимір миттєвого значення трафіку може бути зведене до вимірювання похідного трафіку за часом. Для комутаційної системи слід розрізняти трафік входів і виходів, Трафік входів, як правило, більше трафіку виходів. При вимірах на конкретному пучку визначають середню інтенсивність навантаження як середнє число зайнятих ліній за певний проміжок часу. Нагадаємо, що інтенсивність трафіку 1Ерл створюється безупинно зайнятою лінією протягом години. Відповідно інтенсивність трафіку 2Ерл створюється двома зайнятими лініями протягом години. Трафік розглядають як сукупність викликів, що проходять через групу ліній або каналів.Трафік характеризується трьома своїми параметрами:

- числом абонентів і їхніх категорій;
- числом дзвінків, що припадають на одного абонента;
- тривалістю заняття ліній.

Існує жорсткий взаємозв'язок між ємністю обладнання, трафіком і якістю обслуговування, тобто втратами.

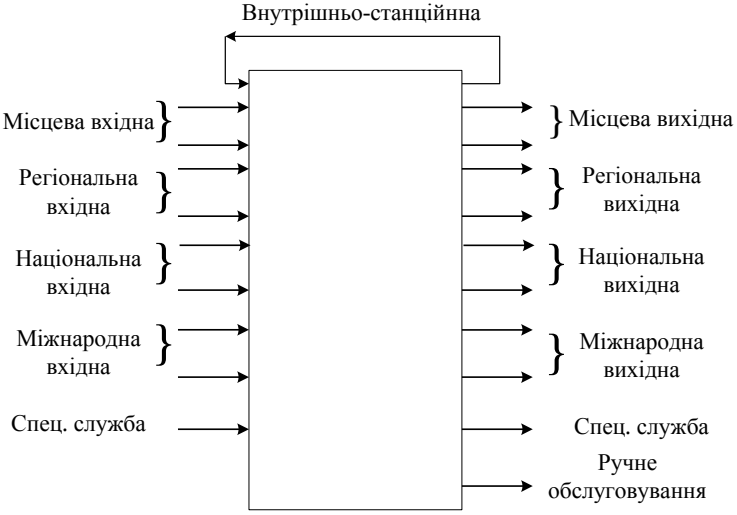


Рис. 13.4. Розподіл трафіку на мережах телекомунікацій

13.10. Розрахунок телефонного трафіка

Виникаючий трафік - це виклики, що надходять від абонентів телефонної мережі і займають на деякий час різні сполучні лінії та пристрої станції і мережі. Це вимагає цілодобового дослідження розподілу виникаючого трафіку за напрямками як внутрішньостанційних, так і до інших станцій мережі з метою визначення максимальної величини трафіку, що приходить в безперервний проміжок часу довжиною в одну годину. Згідно з рекомендаціями МСТ необхідно всі виміри проводити в статистичну годину найбільшої навантаженості (ГНН), коли середня інтенсивність трафіку максимальна. Вимірювання і визначення самої ГНН проводиться в робочі дні двічі на рік в місяці найбільшї навантаженості. Визначена таким чином

статистична ГНН називається фіксованою.

На криву розподілу трафіку впливає безліч чинників, зокрема, структурний склад абонентів досліджуваних станцій, тобто співвідношення часток бізнесових абонентів та адміністративного сектору, ритм міського життя (початок і кінець робочого дня, перерва і т.д.), програми телебачення, свята і т.д. Для більшості телефонних мереж характерна наявність трьох періодів максимального трафіку:

- ранкового (з 9.00-12.00);
- післяобіднього (з 14.00-16.00);
- вечірнього (з 20.00-22.00).

Як було вказано, потік виникаючих викликів у межах фіксованих ГНН і в ГНН окремих днів є нестаціонарним. Це призводить до значних коливань навантаження у часі і, як наслідок, до зростання середніх втрат. Нестаціонарність потоку на реальних мережах в існуючих методах розрахунку не враховують. Зазвичай вважають, що з ймовірністю 0,75 реальні втрати в межах фіксованого ЧНН не перевищать розрахункових, а в інших випадках перевищення буде, як правило, незначним.

Якщо припустити, що коливання інтенсивності трафіку на МТС щодо середнього значення навантаження $A_{ГНН}$ відбуваються за нормальним законом, то отримуємо наступну оцінку навантаження на МТС:

$$A_{МТС} = A_{ГНН} + 0{,}6742\sqrt{A_{ГНН}} \ . \qquad (13.11)$$

Найбільш достовірним шляхом визначення виникаючого навантаження в ГНН є використання реально виміряних даних на АТС. Проте найбільш простим і поширеним методом визначення виникаючого трафіку є метод, що базується на знанні питомої абонентського навантаження (трафіку), що приходить в середньому на одного абонента - y_i, тобто

$$A = \sum_{i=1}^{m} N_i y_i \ . \qquad (13.12)$$

Як правило, проектувальник системи зв'язку задається значенням y_i, виходячи із конкретних умов використання цієї системи.

13.11. Особливості вимірювання телефонного трафіка

Вимірювання трафіку проводяться з метою вирішення низки практичних і теоретичних завдань:

- проектування мереж електрозв'язку;
- управління мережами електрозв'язку;
- прогнозування навантаження;
- укладання угод SLA;
- перевірки гіпотез про кількісні і якісні властивості навантаження.

Об'єктами вимірювань можуть бути:

- загальна кількість викликів, що поступають;
- чисельність викликів від конкретних джерел трафіку;
- частка розмов, що відбулися;
- тривалість обслуговування викликів;
- затримки і втрати викликів.

У математичній статистиці всю досліджувану сукупність однорідних елементів прийнято називати *генеральною сукупністю*. Частину генеральної сукупності, вибраної для вимірювань, називають *вибірковою сукупністю.* Зазвичай досліджується поведінка вибіркової сукупності. Розрізняють три способи виміру:

- безперервне спостереження;
- сканування досліджуваного процесу;
- аналіз випадкових подій.

Для повнодоступного пучка обслуговуючих приладів будемо вважати, що час заняття дорівнює одиниці, а час вимірювань більш ніж у 20 разів перевищує середній час заняття У цьому випадку для розподілу статистичних оцінок можна використовувати нормальний закон.

Деякі важливі постулати:

Точність вимірювання зростає пропорційно

$$\frac{1}{\sqrt{T}}.$$

Абсолютна середньоквадратична похибка вимірювань для обслуженого навантаження (Y) при малій ймовірності втрат (менше 0,01) визначається за формулою:

$$\frac{1}{\sqrt{T}}\sqrt{2Y}\,.$$

Відносна середньоквадратична похибка вимірювань для обслуженого навантаження (Y) визначається за формулою:

$$\frac{1}{\sqrt{T}}\sqrt{\frac{2}{Y}}\,.$$

Абсолютна середньоквадратична похибка вимірювань при малій ймовірності втрат (менше 0,01) визначається за формулою:

$$\frac{1}{\sqrt{N}}\sqrt{2\pi(1-\pi)}\,.$$

Відносна середньоквадратична похибка вимірювань при малій ймовірності втрат визначається за формулою:

$$\frac{1}{\sqrt{N}}\sqrt{\frac{2(1-\pi)}{\pi}}\,.$$

Припустимо, що ми провели 5000 контрольних викликів і визначили оцінку ймовірності втрат викликів на рівні 0,01. Тоді відносна середньоквадратична похибка вимірювань складе приблизно 14%, що не завжди задовільняє вимогам експериментатора.

У таблиці наведено дані щодо необхідної кількості контрольних викликів для забезпечення вибраної точності оцінки.

Значення показника ймовірності втрат викликів	Необхідна кількість контрольних викликів для забезпечення нижченаведеної точності оцінок:		
	5%	10%	20%
0,01	39600	9900	2500
0,02	19600	4900	1200
0,03	12900	3200	800
0,04	9600	2400	600
0.05	7500	1900	500

Вказівки для проектування телефонних мереж містяться у рекомендаціях МСЕ (ITU) і національних стандартах Адміністрації

зв'язку. Зокрема, МСЕ рекомендує, щоб при міжнародному телефонному зв'язку для 30 максимальних ГНН втрати не перевищували 0,01. У той же час для 5 таких ГНН дозволяється встановлювати норму втрат у 0,07.

Зразкові норми для втрат викликів "від абонента до абонента" (end-to-end) для ТМЗК наведені у нижченаведеній таблиці.

Вид установлюючого з'єднання	Допустимі втрати
В межах МТС	0,03 – 0,05
Внітрішньо-зоновий зв'язок	0,07
Міжміський зв'язок (через МТС)	0,07
Міжміський зв'язок	0,13

ЛЕКЦІЯ №14

ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ НАДАННЯ ПОСЛУГ

Розглядаються наступні питання:

Лекційне заняття

14.1. Характеристика систем надання послуг, що використовуються на практиці

14.2. Узагальнена бізнес-модель надання послуг

14.3. Сервісна угода про надання послуг (*SLA*)

14.4. Структура життєвого циклу сервісної угоди

14.5. Порядок укладання та розривання сервісної угоди

14.6. Порядок та засоби інформаційної взаємодії при наданні послуг

Як було вже сказано, до основних завдань експлуатації телекомунікаційних систем відноситься забезпечення надання телекомунікаційних послуг. Тому технології надання послуг з використанням ресурсів ТЛК-систем є об'єктами ретельного вивчення у рамках цієї навчальної дисципліни. Почнемо з розгляду питань організаційного забезпечення надання ТЛК-послуг. Інформаційне та технічне забезпечення систем надання послуг буде розглянуто в наступних лекціях цього модулю.

14.1 Характеристика систем надання послуг, що використовуються на практиці

Система надання фіксованого набору телекомунікаційних послуг із стандартизованими параметрами, яка не передбачає можливостей їхньої адаптації та (або) оптимізації під конкретні особливості застосувань користувачів, має ряд суттєвих вад. Це обумовило доцільність впровадження в експлуатаційну практику провідних операторів електрозв'язку та сервіс-провайдерів принципово інших систем надання послуг, що базуються на чітко визначеній диференціації послуг за рівнями якості.

Диференціація рівнів якості надання послуг дозволяє організувати диференційоване обслуговування клієнтів за сервісними угодами (*Service Level Agreement, SLA),* в яких фіксуються саме ті набори параметрів якості послуг, що влаштовують покупців. У сервісних угодах фіксуються також цілком конкретні зобов'язання сервіс-провайдера щодо

гарантованого надання послуг із заявленими рівнями якості, а також механізми перевірки з боку користувачів реально досягнутих рівнів якості в процесі надання послуг.

Впровадження диференційованої системи гарантованого надання послуг потребує від сервіс-провайдера суттєво вищого ступеню забезпечення усіх аспектів організації і ведення бізнесу на ресурсах приналежних йому ТЛК-мережах, ніж для випадків, коли ставиться за мету надання стандартизованих послуг з незмінними рівнями якості. Проте, переваги такого впровадження цілком виправдовують необхідність пов'язаних з цим витрат і полягають у наступному:

1) з'являється можливість за рахунок чіткої структуризації та диференціації потоків інформації і раціональної інженерії цих потоків, в середньому, майже втричі підвищити коефіцієнт навантаження (*Utilization*) обладнання ТЛК-систем (у порівнянні із ситуацією, коли оптимізація потоків в процесі надання послуг не здійснюється);

2) з'являється можливість транспортування каналами ТЛК-мереж практично усіх видів інформації, у тому числі і такої, що є чутливою до затримок у транспортуванні (зокрема, голосу, відео даних, рухомих зображень тощо), і, отже, суттєво розширити клієнтську базу;

3) створюються умови для підвищення конкурентоспроможності бізнесу у сфері надання телекомунікаційних послуг, оскільки диференційоване обслуговування з урахуванням тонкої структури вимог покупців до умов функціонування їхніх прикладних застосувань, гарантування бажаного рівня якості надання послуг сприяє більш повному задоволенню попиту на ці послуги;

4) створюються умови для підвищення динамізму в реагуванні на зміни потреб та очікувань споживачів телекомунікаційних послуг, що сприяє активності клієнтів і, через це, збільшенню кількості наданих послуг;

5) створюються передумови для зменшення часу переговорного процесу під час укладання сервісних угод завдяки кращій структуризації та повноти комерційних пропозицій щодо характеристик послуг та умов їхнього надання;

6) створюються умови для зменшення кількості можливих непорозумінь із користувачами послуг завдяки більш повній і точній формалізації умов надання послуг;

7) забезпечується можливість пріоритетного надання більш вигідних послуг (зокрема, з точки зору умов їхньої оплати), що сприяє підвищенню економічних показників ведення бізнесу;

8) створюються умови для формалізації взаємовідносин між підрозділами сервіс-провайдера та з іншими операторами та провайдерами під час надання наскрізних послуг, що сприяє підвищенню прозорості ведення бізнесу.

14.2. Узагальнена бізнес-модель надання послуг

Бізнесові взаємовідносини між суб'єктами, що визначають основні характеристики процесу надання послуг, у загальному вигляді відображені на рис.14.1. Ці взаємовідносини мають бути формалізовані на інтерфейсах між суб'єктами, які названі на рис.14.1.

Згідно наданої бізнес-моделі в ролі **сервіс-провайдера (*Service Provider, SP*)** виступає підприємство, що забезпечує надання послуг на комерційній основі із використанням належних йому ТЛК-ресурсів. Сервіс-провайдер силами своїх спеціалізованих підрозділів забезпечує виконання функцій **провайдерів телекомунікаційних послуг (*Telecom Service Provider, TSP*)** за різними видами технологій передавання даних, **провайдера послуг мережі Інтернет (*Internet Service Provider, ISP*)**, а також **провайдера послуг мережних застосувань (*Application Service Provider, ASP*),** включаючи надання інформаційних послуг (виконуючи при цьому функції так званого "контент-провайдера").

Сервіс-провайдер здійснює свою діяльність безпосередньо на належній йому мережі, а також інтегрує (зокрема, комбінує) послуги інших провайдерів, пропонуючи створені таким чином інтегровані послуги кінцевим покупцям. В загальному випадку, з метою забезпечення кінцевого покупця певною необхідною для нього послугою, може бути створений "ланцюг" із сервіс-провайдерів, в котрому кожний попередній провайдер надає певну

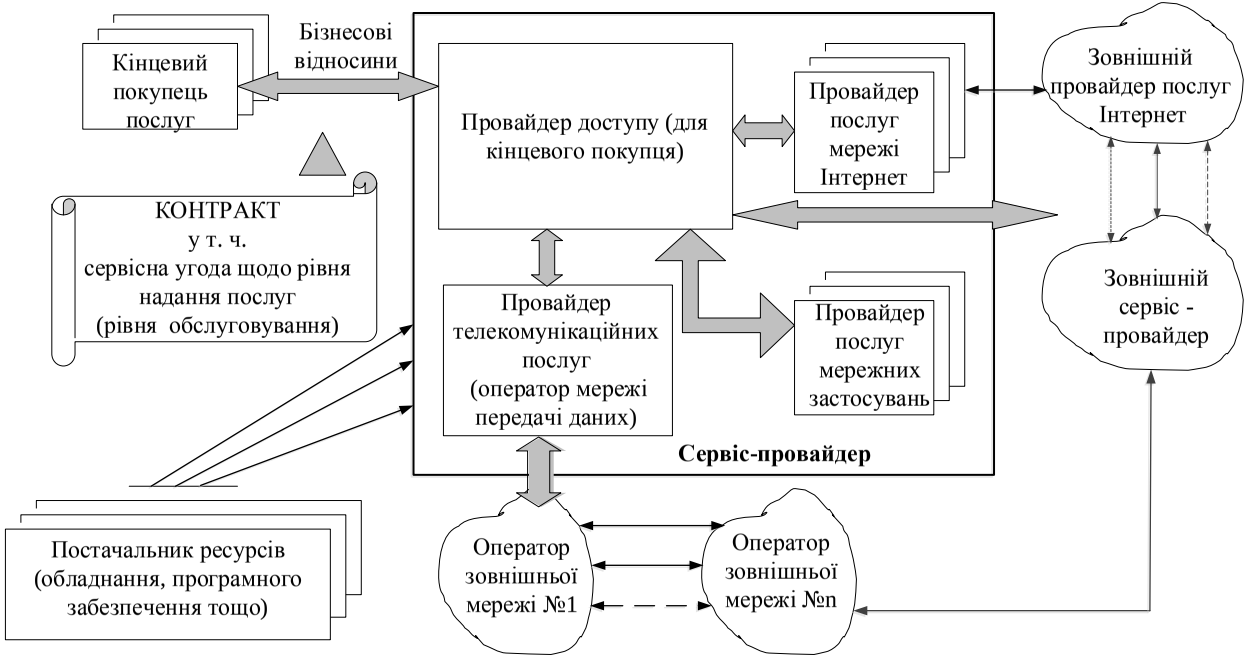


Рис.14.1. Узагальнена бізнес-модель надання послуг

проміжну послугу кожному наступному провайдеру, аж поки кінцевий провайдер отримає можливість забезпечити надання послуги кінцевому покупцю.

Одним із основних інтерфейсів у бізнес-моделі надання послуг, який у вирішальній мірі впливає на всю структуру взаємовідносин між суб'єктами цієї моделі, є інтерфейс "сервіс-провайдер – кінцевий покупець послуг". Специфікації цього інтерфейсу визначаються в процесі укладання відповідного контракту на обслуговування та (або) сервісної угоди *SLA* щодо рівня надання послуг (або рівня обслуговування), яка може бути складовою частиною контракту.

Зважаючи на широку номенклатуру послуг, що надаються сервіс-провайдером на базі використання ТЛК-ресурсів, різноманітність задіяних телекомунікаційних технологій та умов їхнього застосування, виникла необхідність у певній спеціалізації підрозділів сервіс-провайдера, що здійснюють контакт із кінцевими покупцями послуг (а також із безпосередніми користувачами кінцевих послуг, які авторизовані, тобто уповноважені, цими покупцями).

Підрозділ, який організовує і підтримує безпосередні контакти з кінцевим покупцем і користувачами кінцевих послуг, виступаючи при цьому в ролі головного організатора процесу надання кінцевих послуг, називають **провайдером доступу (*Access Provider*)**.

Організація процесу надання кінцевих послуг передбачає необхідність організації і формалізації бізнесових взаємовідносин провайдера доступу з іншими провайдерами послуг – як у рамках структури самого сервіс-провайдера, так і із зовнішніми сервіс-провайдерами. Ці взаємовідносини в багатьох випадках доцільно формалізувати на основі відповідних сервісних угод.

14.3. Сервісна угода про надання послуг (SLA)

14.3.1. Формальною основою надання сервіс-провайдером ТЛК-послуг з урахуванням їхньої якості є сервісна угода (*Service Level Agreement, SLA*).

SLA - це документ, що являє собою невід'ємну частину контракту (тобто, формальної комерційної угоди, яка укладається між адміністрацією сервіс-провайдера та покупцем цих послуг) і

містить у собі усі аспекти угоди щодо якості надання послуг або якості обслуговування.

У загальному випадку *SLA* укладається з метою визначення спільного розуміння щодо характеристик якості надаваних послуг, пріоритетів та умов щодо їхнього надання, ступеню досконалості виділених мережних ресурсів, умов та методів перевірки якості, гарантійних зобов'язань та умов відповідальності у разі недотримання вимог *SLA* і т. ін.

У *SLA* відображаються узгоджені позиції обох сторін: покупця телекомунікаційних послуг, що фіксує конкретні бажані для нього характеристики якості та умови надання послуг з метою забезпечення нормальної роботи його застосувань, і адміністрації сервіс-провайдера, що визначає фактичні обсяги своїх ресурсів, які необхідно виділити для виконання умов угоди.

Схематичне відображення основних питань, які мають бути вирішені під час укладання сервісної угоди згідно з рекомендацією МСЕ-Т *E.801* (у редакції *COM 2-R 58-E* 1996 р.), надане на рис.14.2.

Рис.14.2. Логічна структура вирішення основних питань, що пов'язані з укладанням сервісної угоди

14.3.2. В процесі роботи над сервісною угодою, якщо за згодою сторін передбачається застосування системи диференційованого обслуговування з гарантованим сервісом, визначаються позиції, які наведено нижче.

1) Ступінь конфіденційності змісту сервісної угоди та інших документів (зокрема, звітів про поточний стан обслуговування), що супроводжуватимуть процес надання послуг (а також, можливо, інші умови щодо конфіденційності взаємовідносин між суб'єктами угоди).

2) Види послуг, що мають надаватися згідно із сервісною угодою.

3) Функціональні характеристики (функціональні профілі) надаваних послуг (не обов'язково).

4) Точки (або групи точок) доступу до послуг.

5) Види та характеристики очікуваного трафіку покупця послуг, а також обмеження, яким цей трафік має відповідати.

6) Параметри сервісної угоди, що визначають гарантовані рівні якості надання послуг (для тих мережних послуг, які мають надаватися за системою диференційованого обслуговування з гарантованим сервісом).

7) Параметри сервісної угоди, що визначають показники кількості та якості виділених мережних ресурсів, що забезпечують надання тих мережних послуг, які мають надаватися за системою диференційованого обслуговування з гарантованим сервісом.

8) Параметри сервісної угоди, що визначають умови надання мережних послуг і, можливо, мережних ресурсів, які мають надаватися за системою обслуговування з перевагами (пріоритетне обслуговування).

9) Параметри сервісної угоди, що визначають умови надання мережних послуг і, можливо, мережних ресурсів, які мають надаватися за системою обслуговування з максимальними зусиллями (best effort).

10) Перелік параметрів, які мають контролюватися постачальником послуг.

11) Перелік параметрів, інформація щодо поточних оцінок котрих має надаватися покупцю послуг.

12) Методи, умови, засоби та процедури визначення параметрів,

що зафіксовані у SLA.

13) Порядок та засоби інформування покупця послуг, зокрема повнота та періодичність інформування щодо поточного стану та рівнів обслуговування.

14) Порядок та засоби інформування сервіс-провайдера щодо виниклих проблем в обслуговуванні.

15) Система та умови щодо плати за надані послуги (які можуть бути досить складними, якщо передбачається кілька рівнів якості обслуговування щодо різних видів трафіка покупця, за різними тарифами тощо). (Ця опція може бути визначена в інших документах контракту).

16) Санкції за порушення умов SLA (як постачальником послуг, так і покупцем, наприклад за відхилення параметрів його трафіку від узгоджених значень). Ці санкції можуть накладатися у вигляді грошових штрафів або у будь-якій іншій формі, наприклад у формі надання безкоштовного сервісу або надання послуг за більш низькими тарифами.

17) Умови переходу з однієї системи обслуговування на іншу або до обслуговування з різним рівнем якості в залежності від дня тижню або годин доби. Іншими словами, узгоджена динаміка змін у якості обслуговування.

18) Умови та порядок обробки трафіку, параметри котрого виходять за межі, що обумовлені у SLA. Зокрема, це можуть бути формалізовані правила розпізнавання різних видів потоків пакетів покупця послуг і кондиціювання цього трафіку (наприклад, умови знищення або маркування надлишкових пакетів) або згладжування пульсацій трафіку з метою покращення умов для роботи деяких застосувань (наприклад, тих, що працюють із мовною інформацією) або з метою зменшення затримок у транзитних вузлах мережі, оскільки більш рівномірне надходження пакетів сприяє зменшенню перенавантажень мережного обладнання.

19) Строк дії умов сервісної угоди.

20) Інші додаткові умови і положення, що спрямовані на покращення умов функціонування застосувань покупця послуг або полегшення умов та підвищення надійності надання послуг.

14.3.3. Для покупців, яких влаштовує обслуговування без надання гарантованого сервісу, сервіс-провайдер пропонує

обслуговування за типовою сервісною угодою, у якій фіксується перелік підтримуваних параметрів якості надаваних послуг та їхні конкретно визначені числові значення (надалі, типова *SLA*). Зокрема, пропонуються **трафарети сервісної угоди щодо рівня надаваних послуг (темплети *SLA, Service Level Agreement Templates*)** – визначення стандартних ступенів якості послуги, які можуть бути запропоновані покупцям послуги у рамках *SLA*. Наприклад, пропонуються трафарети, що визначають характеристики так званої "золотої послуги" або "срібної послуги" і т. ін.

У типовій *SLA* гарантії щодо підтримки параметрів якості послуг на кількісному рівні не надаються. Типова *SLA* містить ті значення параметрів якості послуг, підтримка котрих можлива без використання механізмів гарантування якості обслуговування протягом строку дії сервісної угоди за умов неперевищення прийнятого рівня запасу пропускної здатності задіяних каналів мережі.

14.3.4. Якщо передбачається обслуговування за системою диференційованого обслуговування з гарантованим сервісом (у тому числу, у складі комбінованої системи обслуговування), необхідно визначити підмножину параметрів у розрізі кожної послуги, підтримка котрих гарантується умовами сервісної угоди. З технічної точки зору така підтримка забезпечується засобами відповідної мережної служби, що має функціонувати у складі організаційної структури експлуатаційного персоналу ТЛК-системи. Ця служба називається службою підтримки якості надання послуг (службою *QoS*).

Підмножина параметрів сервісної угоди, що визначає гарантовану якість надання мережної послуги, тобто гарантовану *QoS* (елементи цієї підмножини ще називаються параметрами *Grade of Service*, параметрами *GoS*), фіксується у сервісній угоді.

У якості параметрів гарантованої *QoS* використовують:

- взаємо-узгоджений набір значень показників якості послуги, підтримка котрих має бути забезпечена під час надання послуги;

- взаємо-узгоджені значення функцій та (або) функціоналів від вибраних показників якості послуги, що з достатнім для

застосування рівнем ймовірності гарантують підтримку вибраного набору значень показників якості послуги (не обов'язково);

- взаємо-узгоджені проміжки часу, протягом котрих має здійснюватися вимірювання та, можливо, первісне (початкове) усереднення поточних значень параметрів якості послуги (**інтервали вимірювання**);

– взаємо-узгоджені проміжки часу, протягом котрих має здійснюватися усереднення виміряних поточних значень параметрів якості послуги (**інтервали поточного збору даних**). Ці усереднені значення параметрів якості послуги використовуються для визначення поточних оцінок досягнутих рівнів надання послуги та їх поточного порівняння із встановленими пороговими значеннями параметрів якості в процесі контролю відповідності;

- взаємо-узгоджені проміжки часу, протягом котрих має здійснюватися подальше усереднення та інтеграція (тобто, агрегація) тих поточних даних про параметри якості послуги, що отримані шляхом усереднення на інтервалі поточного збору даних, у тому числі і усереднення поточних оцінок досягнутих рівнів надання послуги (**інтервали агрегації даних**). Дані, що формуються на інтервалі агрегації, накопичуються в адміністративних файлах для подальшого їхнього використання в задачах мережного керування, планування та розвитку бізнесу. Ці дані у випадках, коли вони використовуються у якості інструмента контролю з боку покупця послуги, можуть накопичуватися у файлах, що є безпосередньо доступними для покупців;

- **інтервали звітування** (*Reporting Period*), тобто періодичність представлення покупцю послуг звітів про поточний стан обслуговування;

- **інтервали внутрішньо корпоративного звітування (***Reporting for Administration Period*), тобто періодичність представлення адміністрації сервіс-провайдера звітів про поточний стан обслуговування та використання ресурсів.

14.3.5. Не обов'язково усі позиції підрозділу 14.3.2 мають бути висвітлені під час укладання сервісних угод. В залежності від конкретних умов діяльності покупця послуг і ресурсних можливостей сервіс-провайдера узгоджуються лише ті із них, що є суттєвими з точки зору кожної із сторін угоди.

14.3.6. Зміст сервісної угоди має відповідати певним вимогам, які доцільно класифікувати за такими групами:

1) загальні вимоги (*Fulfillment*);

2) гарантії (*Assurance*);

3) інтерфейс із покупцем (*Customer Interface Management*).

14.3.7. Загальні вимоги:

1) вимірювальна метрика та визначення параметрів, які гарантуються умовами сервісної угоди, повинні мати однозначне тлумачення і бути зрозумілими покупцю;

2) методи вимірювання якості послуг, період вимірювань та період звітування мають бути визначені з урахуванням характеристик прикладних застосувань покупця послуг;

3) сервіс-провайдер повинен бути у змозі визначати параметри якості послуг та діапазони їхніх припустимих значень, які він здатний підтримувати за системою диференційованого обслуговування з гарантованим сервісом;

4) сервіс-провайдер повинен тримати в активному стані процедури виявлення порушень умов сервісної угоди, зокрема задіяти механізми тривожної сигналізації, наприклад, шляхом встановлення порогових значень контрольованих параметрів, перетинання котрих має сповіщати про досягнення зон із підвищеною ймовірністю виникнення порушень умов сервісної угоди;

5) сервіс-провайдер повинен у рамках вибраної метрики забезпечувати об’єктивність оцінок рівнів якості послуг, зокрема повторюваність результатів вимірювань;

6) мають бути визначені чіткі границі умов і обмежень, в зоні дії котрих гарантується обслуговування із визначеними рівнями, зокрема визначена динаміка змін рівнів обслуговування за годинами доби, днями тижня і т. ін.;

7) покупець послуг повинен мати можливість самостійно здійснювати оцінку якості отриманих послуг;

8) вибір форми та змісту звітних документів має бути узгоджений із умовами обслуговування;

9) мають бути обумовлені процедури вирішення конфліктних питань;

10) має бути визначена відповідальність сторін за недотримання

вимог *SLA*.

14.3.8. Гарантії:

1) сервіс-провайдер повинен бути у змозі контролювати та вимірювати якість гарантованих послуг та обслуговування, порівнювати досягнуті рівні якості із гарантованими у *SLA*, використовуючи для цього методи та процедури, що є прийнятними для покупця послуг та регуляторних органів;

2) точність та періодичність надання інформації щодо виконання умов *SLA* має бути узгодженою із покупцем послуг;

3) задіяні механізми автентифікації та захисту інформації від несанкціонованого доступу повинні бути достатніми, щоб виключити можливість несанкціонованого ознайомлення із персоніфікованими даними, призначеними для покупця послуг;

4) сервіс-провайдер має забезпечувати можливість виявлення деградації обслуговування та механізми сповіщення покупця про такі події;

5) сервіс-провайдер має забезпечувати механізми виявлення порушень умов *SLA* та механізми вирішення виникаючих проблем в рамках проміжку часу, обумовленого умовами *SLA*;

6) покупець послуг повинен контролювати процес надання послуг і зберігати інформацію щодо характеристик якості отриманих послуг протягом проміжків часу, обумовлених умовами *SLA*.

14.3.9. Інтерфейс із покупцем:

1) покупцю послуг має бути надана можливість інтерактивного зв’язку із сервіс-провайдером для сповіщення про виниклі проблеми із використанням усіх доступних видів зв’язку – телефон, факс, електронна пошта, віддалений запит до сервера тощо;

2) сервіс-провайдер повинен забезпечити швидкий і вичерпний відгук на запит покупця;

3) в контактних точках сервіс-провайдера із покупцями його послуг має накопичуватися та зберігатися достатньо повна і актуальна інформація, щоб у повній мірі задовольняти запити покупців.

14.4. Структура життєвого циклу сервісної угоди

14.4.1. Будь-яка сервісна угода, починаючи від моменту здійснення певних дій підготовчого характеру щодо її створення і до моменту її розривання, проходить кілька стадій свого розвитку, які у сукупності складають життєвий цикл цієї сервісної угоди. Більшість сервіс-провайдерів, маючи на увазі так звану *TOM*-модель управління телекомунікаційними системами, що підтримується МСЕ-Т, відповідно до процесного підходу управління якістю (згідно з вимогами ДСТУ *ISO 9000*) життєвий цикл сервісних угод розбивають на такі стадії:

1) створення або модернізація чи розвиток послуги (*Product/Service Development*);

2) узгодження та укладання сервісної угоди щодо рівня надання послуги (*Negotiation and Sales*);

3) імпліментація послуги (тобто, конфігурування, інсталяція параметрів та активізація послуги) (*Implementation*);

4) надання послуги відповідно до умов сервісної угоди (*Execution*);

5) аналіз та оцінювання результатів надання послуги (*Assessment*).

14.4.2. Необхідність модернізації та розвитку вже існуючих послуг, а також створення нових послуг обумовлюється конкуренцією на ринку надання телекомунікаційних послуг, змінами в потребах покупців послуг та здобутим сервіс-провайдером практичним досвідом в процесі надання послуг.

На цій підготовчій стадії життєвого циклу *SLA* здійснюються наступні види робіт:

- ідентифікація потреб та динаміки змін у потребах користувачів;
- визначення характеристик послуг, що мають відповідати новим потребам користувачів (зокрема, визначення бажаного набору параметрів послуги, їхніх припустимих значень, бажаних рівнів послуги тощо);
- визначення та оцінка мережних ресурсів, що є необхідними для впровадження нової або модернізованої послуги;
- розробка нових темплетів *SLA* (кінцевий результат робіт на цій стадії життєвого циклу сервісної угоди).

14.4.3. Стадія узгодження та укладання сервісної угоди передбачає виконання наступних робіт:

- відбір величин параметрів *SLA*, що забезпечують нормальне функціонування прикладних застосувань покупця послуги і, в той же час, не погіршують якість обслуговування вже існуючих користувачів послуг і не завдають неприпустимих перенавантажень мережного обладнання;
- узгодження цінових пропозицій;
- узгодження штрафних санкцій щодо невиконання умов *SLA*;
- узгодження методів, засобів та періодичності звітування щодо поточного стану обслуговування;
- узгодження методів та засобів зворотного зв'язку покупця послуги із сервіс-провайдером.

Кінцевим результатом на цій стадії життєвого циклу *SLA* є узгоджений та підписаний обома сторонами контракт із відповідною сервісною угодою.

14.4.4. На стадії імпліментації послуги здійснюються наступні види робіт:

- формуються заявки на усі види додаткових ресурсів, що необхідні для забезпечення надання послуги відповідно до умов *SLA*;
- активізуються заявлені ресурси;
- конфігуруються, інсталюються, активізуються та тестуються ресурси мережі, на основі якої буде здійснюватися надання послуги за новою сервісною угодою;
- конфігуруються, інсталюються, активізуються та тестуються механізми служби підтримки якості послуги відповідно до умов нової *SLA*;
- активізується та тестується послуга у цілому в умовах, що максимально наближені до реальних умов її надання.

Кінцевий результат цієї стадії життєвого циклу *SLA* – повністю придатна для користування послуга відповідно до умов нової *SLA.*

14.4.5. Процес надання послуги (в частині управління якістю обслуговування) складається із:

- контролю відповідності поточних параметрів обслуговування, що визначені у *SLA*;
- звітування про реальний стан обслуговування за сервісною

угодою;

- обробки запитів та реакції на запити покупця послуги відповідно до умов *SLA*;

- виявлення подій, що пов'язані із деградацією послуги або відмов у її наданні, та сповіщення спеціалізовані служби про виниклі події.

14.4.6. Аналіз та оцінювання результатів надання послуги виконується з метою забезпечення вирішення наступних двох задач:

1) аналіз якості надання послуги у розрізі окремої сервісної угоди;

2) інтегральна оцінка та аналіз ефективності функціонування служби *QoS*.

Аналіз якості надання послуги у розрізі окремої сервісної угоди передбачає оцінювання:

- якості наданої послуги;

- ступеню задоволеності покупця наданою послугою;

- потенційних можливостей щодо удосконалення послуги;

- можливих змін у вимогах покупця до змісту послуги та процесу її надання.

Інтегральна оцінка та аналіз ефективності функціонування служби QoS передбачає визначення:

- інтегральних показників якості надання послуг у розрізі груп користувачів і в цілому по всій клієнтській базі;

- проблем у системі надання послуг;

- нових цілей в обслуговуванні;

- нових шляхів щодо удосконалення системи надання послуг.

14.5. Порядок укладання та розривання сервісної угоди

14.5.1. Порядок укладання сервісної угоди

Будь-яка фізична або юридична особа, резидент або нерезидент України, (надалі, особа) має право на отримання телекомунікаційних послуг на основі використання ТЛК-систем загального користування (надалі, коротко кажучи, послуг).

Відмова особі в укладанні контракту на обслуговування, у тому числі в укладанні сервісної угоди щодо рівня надання послуг, може

обумовлюватися лише однією підставою – відсутністю ресурсних можливостей, потрібних для забезпечення надання послуг у заявлених обсягах та (або) із заявленим рівнем якості.

Надання пріоритетів в укладанні контрактів на обслуговування і сервісних угод щодо рівня надання послуг (або обслуговування), а також інших преференцій, визначається чинними нормативними документами.

Особа, яка має намір отримувати послуги, повинна надати відповідну заявку - замовлення встановленої форми і у встановленому порядку (*Order Handling*), в котрій вказати бажаний для неї перелік отримуваних послуг, бажані показники щодо кількості та якості цих послуг, а також бажані характеристики щодо динаміки надання заявлених послуг у реальному часі.

Адміністрація сервіс-провайдера повинна розглянути надану заявку (зазвичай, у тижневий термін, не довше) і надіслати відправнику заявки обгрунтовану відповідь щодо можливості або неможливості розпочати процес укладання контракту та відповідної сервісної угоди щодо рівня надання послуг.

Під час початкового опрацювання заявки, якщо мова йде про надання пріоритетного та (або) диференційованого обслуговування із гарантованим сервісом, необхідно оцінити вплив можливого додаткового навантаження на ресурси мережі, яке обумовлюється заявленими параметрами послуг, з оглядом на необхідність збереження якості обслуговування вже існуючих клієнтів. Для цього здійснюють перепланування завантажень елементів мережі та реінженерію потоків даних.

Якщо на етапі початкового опрацювання заявки виявилась суттєва невідповідність ресурсних можливостей ТЛК-системи заявленим вимогам, то, зрозуміло, заявка не задовольняється.

Якщо ж результати перепланування та реінженерії потоків виявились позитивними (тобто, виявлено достатньо незадіяних мережних ресурсів, які є можливим використати на забезпечення обслуговування відповідно до умов заявки), то заявник інформується про можливість укладання сервісної угоди на його умовах.

Якщо виявилось неможливим задовольнити умови заявки, але існують компромісні варіанти пропозицій, які за певних умов

можуть бути корисними покупцю послуг, то за згодою сторін розпочинається процес сумісного опрацювання заявки, протягом котрого здійснюється спроба узгодити номенклатуру і відповідні параметри кількісних та якісних показників послуг, умови та динаміку надання послуг, диференціацію послуг за системами надання послуг, гарантії надання послуг (у разі необхідності), множину контрольованих з боку клієнта параметрів якості обслуговування, порядок і механізми організації зворотного зв'язку між клієнтом та постачальником послуг тощо. Перелік усіх можливих позицій сервісної угоди, з якого вибираються позиції, що є суттєвими в умовах діяльності суб'єктів угоди і які підлягають узгодженню в процесі укладання угоди, визначений у підрозділі 14.3.2. За результатами опрацювання, якщо компроміс знайдений, то підписується контракт та укладається сервісна угода. У протилежному випадку, заявка не може бути задоволеною.

14.5.2. Порядок розривання (тобто, припинення дії) контракту на обслуговування та сервісної угоди щодо рівня надання послуг (або рівня обслуговування)

Усі умови припинення дії контракту та відповідної сервісної угоди, як правило, визначаються за взаємною згодою сторін і відображаються у текстах названих документів.

14.6. Порядок та засоби інформаційної взаємодії при наданні послуг

14.6.1. Порядок інформування покупця послуг про поточний стан обслуговування

Система диференційованого обслуговування із гарантованим сервісом передбачає необхідність організації та підтримки механізмів інформування покупців послуг щодо поточного стану та рівнів наданого обслуговування. Ці механізми використовуються покупцями послуг у якості інструмента контролю (перевірки) на відповідність поточного стану обслуговування тим умовам та вимогам, що зафіксовані у *SLA*.

Сервіс-провайдер з певною періодичністю має надсилати на адресу кожного із покупців послуг, які отримують обслуговування із гарантованим сервісом, повідомлення, що мають назву "**Звіт про**

поточний стан обслуговування” (“*Performance Report*”). Ці звіти надсилаються покупцям послуг у зручний для них спосіб з використанням в даних конкретних умовах доступних видів поштового або електрозв’язку, а також будь-яких інших систем транспортування даних. Наприклад, такі звіти можуть представлятися у вигляді роздруківок або надсилатися у електронній формі на регулярній основі або на вимогу покупця. Вони також можуть зберігатися у вигляді записів у базах даних, які, в цьому разі, мають бути доступними для покупців послуг.

Розрізняють три основних види звітів про стан обслуговування, які у сукупності дозволяють покупцям послуг отримати детальне уявлення щодо рівня якості наданого обслуговування: звіт про виконання вимог сервісної угоди щодо рівнів наданих послуг; звіт про якість наданої послуги; звіт про отримані мережні ресурси.

Звіт про виконання вимог сервісної угоди щодо рівнів наданих послуг (*Service Level Agreement Report*) – це стислий експрес-звіт сервіс-провайдера з поточними оцінками виконання вимог *SLA* щодо рівнів наданих послуг без деталізації характеристик стану обслуговування. Надсилається покупцю послуг в процесі обслуговування оперативно у реальному часі з обумовленою відносно короткою періодичністю. Аналіз даних, що містяться у звітах цього виду, здійснюється покупцями послуг, здебільшого, як елемент експрес-контролю якості функціонування їхніх прикладних застосувань, оскільки завдяки оперативності надання цих звітів забезпечується можливість оперативного реагування на можливі порушення вимог сервісних угод.

Як інтервал оцінювання рівнів наданих послуг для експрес-звіту, так і період звітування вибирають виходячи із конкретних умов функціонування прикладних застосувань покупця послуг. Для застосувань із високими динамічними характеристиками інтервал оцінювання може дорівнювати **інтервалу вимірювань** (*Measurement Interval*), а період звітування вибиратися таким, щоб мати достатній часовий ресурс для адекватного реагування на порушення вимог сервісної угоди.

Звіт про якість наданої послуги (*Quality of Service Report*) – звіт, що містить оцінку досягнутих рівнів якості наданої послуги, зокрема поточні оцінки параметрів *QoS*. Цей звіт надсилається на

адресу покупця послуги з метою надання йому можливості порівняти реально досягнутий рівень якості отриманої послуги з гарантованими параметрами *GoS*, що зафіксовані у *SLA*. Оцінювання параметрів здійснюється на **інтервалах поточного збору даних** (*Data Collection Interval*). Як правило, цей звіт генерується службою підтримки якості надання послуг (тобто, службою *QoS*) з обумовленою у сервісній угоді періодичністю. **Інтервал звітування** (*Reporting Period*) вибирається виходячи із конкретних умов функціонування прикладних застосувань покупця послуги і не обов'язково дорівнює інтервалу поточного збору даних.

Звіт про використані мережні ресурси (*Resource Report*) – звіт про характеристики реального трафіка застосувань покупця, що утворюється цими застосуваннями на визначених проміжках часу, а також про кількість і якість використаних покупцем мережних ресурсів за обумовлені проміжки часу.

Оцінки параметрів реального трафіка та використаних ресурсів здійснюються на інтервалах поточного збору даних, а інтервал звітування вибирають виходячи із конкретних умов функціонування прикладних застосувань покупця послуг.

Усі вищезазначені звіти представляються окремо щодо кожної точки доступу до послуги (або кожної групи точок доступу до послуги).

14.6.2. Засоби інформування покупця послуг щодо поточного стану та рівнів обслуговування

Сучасні інформаційні технології дозволяють задіяти зручні для користувачів засоби інформування щодо поточного стану та рівнів обслуговування.

Сервіс-провайдер використовує наступні способи та засоби інформування своїх клієнтів:

1) довідкова служба на основі використання центру телефонних викликів (так званих "Call-центрів");

2) довідкова служба на основі використання мультимедіацентрів (так званих "Контакт-центрів");

3) послуги електронної пошти в Інтернеті;

4) послуги спеціалізованого Веб-сервера в Інтернеті.

Задіяні технології інформування клієнтів мають бути оснащені сертифікованими засобами технічного захисту інформації, які із нормованими рівнями ефективності та гарантованості захисту унеможливлюють порушення конфіденційності і цілісності інформації, що надається клієнтам із використанням вищезазначених засобів. У відповідальних випадках на вимогу клієнта має бути забезпечена можливість використання механізмів електронного підпису і інших механізмів забезпечення юридичної значущості інформації, що надається у звітах про стан обслуговування.

В залежності від конкретних умов діяльності клієнта у нього існує можливість використання будь-якого із вищезазначених способів отримання інформації щодо поточного стану та рівнів наданого обслуговування.

14.6.3. Порядок та засоби внутрішньо корпоративної інформаційної взаємодії в процесі надання послуг

Комерційне використання ресурсів ТЛК-систем передбачає необхідність організації та підтримки механізмів внутрішньо корпоративного інформування щодо поточного стану обслуговування та використаних мережних ресурсів. Застосування цих механізмів здійснюється в цілях:

1) інформаційного забезпечення процесу надання послуг та експлуатації обладнання;

2) прогнозування стану і планування розвитку мережі;

3) розширення номенклатури та підвищення якості послуг і обслуговування;

4) контролю (перевірки) з боку адміністрації стану обладнання і обслуговування на відповідність вимогам стандартів та інших розпорядчих документів підприємства, які регламентують роботу персоналу.

Служба підтримки якості надання послуг (служба QoS) з певною періодичністю має надсилати на адресу адміністрації свого регіонального вузлу повідомлення, що мають назву "**Агрегований звіт про якість наданих послуг"** ("*Agregative Quality of Service Report*") – узагальнений звіт з оцінками виконання вимог *SLA* щодо рівнів наданих послуг у розрізі видів задіяних телекомунікаційних

технологій, видів потоків (класів трафіка), видів та (або) класів послуг. У звіті мають бути відображені усі випадки порушень вимог *SLA*, причини та наслідки їхнього виникнення, а також заходи, що були проведені з метою ліквідації негативних наслідків та запобігання порушень у майбутньому.

Узагальнення оцінок виконання вимог *SLA* щодо рівнів наданих послуг виконується на **інтервалах агрегації** (*Aggregate Interval*). Інтервал звітування - один раз на тиждень.

Експлуатаційні підрозділи з певною періодичністю мають надсилати на адресу адміністрації свого регіонального вузлу повідомлення, що мають назву **"Агрегований звіт про використані мережні ресурси"** ("*Agregative Resource Report*") – узагальнений звіт про характеристики реального трафіка, який утворюється застосуваннями покупців послуг на визначених проміжках часу, а також про кількість і якість використаних покупцями послуг мережних ресурсів за обумовлені проміжки часу. У звіті мають бути відображені усі випадки перенавантажень обладнання мережі та порушень вимог *SLA* з боку користувачів, причини та наслідки їхнього виникнення, а також заходи, що були проведені з метою ліквідації негативних наслідків та запобігання перевантажень та порушень у майбутньому.

Узагальнення оцінок параметрів реального трафіка та використаних ресурсів здійснюється на інтервалах агрегації. Інтервал звітування – один раз на тиждень.

Персонал ТЛК-систем повинен періодично надавати на адресу керівництва повідомлення, що мають назву "**Агрегований звіт про поточний стан обслуговування"** ("*Agregative Performance Report*") **–** узагальнений звіт про виконання вимог сервісних угод щодо якості обслуговування та використані мережні ресурси. У звіті мають бути відображені усі суттєві події, які були пов'язані із виникненням невідповідностей у наданні послуг та у використанні мережних ресурсів.

Узагальнення оцінок параметрів *QoS* наданих послуг та мережних ресурсів, оцінок параметрів реального трафіка та використаних ресурсів здійснюється на інтервалах агрегації. Інтервал звітування – один раз на місяць.

Контрольні питання до чотирнадцятої лекції

1. Які види систем обслуговування Ви знаєте?

2. З якою метою укладаються сервісні угоди?

3. Що таке *SLA*?

4. Що фіксується у сервісній угоді?

5. Які переваги і недоліки характерні для диференційованого обслуговування?

6. Які функції виконує сервіс-провайдер?

7. Поясніть структуру узагальненої моделі надання послуг.

8. Які функції виконує провайдер доступу?

9. Яка структура сервісної угоди за умов диференційованого обслуговування?

10. Що таке темплети *SLA*?

11. Яким чином забезпечується гарантована якість надання мережної послуги?

12. Що таке інтервал поточного збору даних?

13. Що таке інтервал агрегації даних?

14. Яким чином має здійснюватися інтерфейс із покупцем?

15. Який має бути порядок укладання та розривання сервісної угоди?

16. Яка структура життєвого циклу сервісної угоди?

Використана література:

1) Г.Ф. Конахович, В.М. Чуприн. Сети передачи пакетной коммутации.–К..: МК-Пресс, 2006. Розділ 4.

ЛЕКЦІЯ №15. ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ НАДАННЯ ПОСЛУГ

Розглядаються наступні питання:

Лекційне заняття

15.1. Характеристика інформаційного забезпечення технологій надання послуг

15.2. Структура взаємозв'язків між службами та процесами обслуговування

15.3. Мова відображення процесів обслуговування

15.4. Процедура підтримки створення та розвитку послуг

15.5. Процедура підтримки продажу послуг

15.6. Процедура обробки замовлень

15.7. Процедура опрацювання проблемних ситуацій

15.8. Процедура підтримки узагальнених аналізів та оцінки якості обслуговування

15.1. Характеристика інформаційного забезпечення технологій надання послуг

Технології гарантованого надання телекомунікаційних сервісів у відповідності із диференційованими вимогами клієнтів, тобто системи диференційованого обслуговування з гарантованим сервісом (ДОГС), наразі знайшли широке застосування в експлуатаційній практиці вітчизняних сервіс-провайдерів та операторів електрозв'язку. Проте кілька років тому ці технології у значній мірі не були здатними підтримувати нові функціональні можливості, що закладені у сучасне телекомунікаційне обладнання (ТКО), оскільки було відсутнім відповідне інформаційне забезпечення систем обслуговування. Характерний приклад – стандартизовані на міжнародному рівні технології інтеграції та диференціації мережних послуг *DiffServ, RSVP* та *MPLS* із стеку протоколів *TCP/IP*. Програмно-апаратні механізми цих протоколів, як правило, вмонтовані в сучасне ТКО. Їхня інсталяція мала забезпечити отримання суттєвих переваг для користувачів інформаційних сервісів. Тим не менш, внаслідок недосконалості прийнятих на той час методів експлуатації ТКО переваги цих технологій у достатній мірі були не задіяними.

Впровадження технології ДОГС пов'язано не тільки із необхідністю інсталяції нових програмно-апаратних механізмів керування потоками даних користувачів. Потрібна перебудова усієї системи обслуговування в напрямку реалізації можливостей щодо диференціації обслуговування у розрізі кожного окремого клієнта та забезпечення гарантій надання йому інформаційних послуг узгодженої з ним якості. Зокрема, щоб ефективно використовувати корисні властивості *DiffServ*, *RSVP* та *MPLS*, необхідно забезпечити диференційовану обробку у реальному часі потоків мережних пакетів (точніше – протокольних блоків даних, *PDU*) з урахуванням тонкої структури потреб задач користувачів. При цьому необхідно гарантувати підтримку у реальному часі узгодженого рівня якості обробки у розрізі кожної окремої задачі, налагодити моніторинг використаних ресурсів, забезпечити контроль якості надаваних сервісів диференційовано щодо кожної задачі, надати у розпорядження клієнтів мережі зручні у користуванні засоби контролю якості та кількості споживаних мережних ресурсів. А також багато чого іншого, що наразі пов'язується із поняттям *Quality of service*, *QoS* (якість послуги).

До інформаційного забезпечення технології ДОГС відносять дані щодо:

1) структури взаємозв'язків між службами та підрозділами, що займаються наданням інформаційних сервісів, розподілу функціональних обов'язків між ними;

2) класифікаторів параметрів якості обслуговування та параметрів ТКО, що впливають на якість обслуговування (Визначення цих параметрів є необхідним для підтримки заданих рівнів якості наданих послуг, оцінювання кількості використаних мережних ресурсів та їх адаптивного перерозподілу між клієнтськими застосуваннями в процесі обслуговування);

3) норм на параметри якості обслуговування та параметри ТКО;

4) класифікації інформаційних потоків, що підтримують процеси забезпечення *QoS*;

5) інтерфейсів між користувачами послуг та обслуговуючими службами.

Однак основним елементом інформаційного забезпечення цієї технології надання послуг слід вважати відповідні специфікації

процесів обслуговування.

Процеси обслуговування представляються у вигляді так званої процедурної (або процесної) моделі обслуговування (використана термінологія - згідно *ITU-T Recommendation E.800(08/94), E.801 (06/96), I.350 (03/93)*). Цю модель беруть за основу для розробки інформаційного забезпечення технологій надання ТЛК-послуг. Для відображення процедур використовують процесний (процедурний) підхід відповідно до вимог ДСТУ *ISO 9001*, який найбільш повно і точно відображає суть сучасних підходів до надання послуг на основі використання механізмів управління якістю обслуговування *QoS*. Ключовим моментом цього підходу, що привнесений в концепцію рекомендацій *E.800* та *E.801 MCE-T*, є вимога структуризації усіх процесів обслуговування у розрізі стадій життєвого циклу укладених сервісних угод (*Service Level Agreement*, *SLA*), потік котрих має оброблюватися оператором мережі у реальному часі диференційовано, тобто з урахуванням індивідуальних особливостей кожної із укладених *SLA*. Моделі процедур обслуговування мають у рамках кожної стадії життєвого циклу *SLA* показувати взаємозв'язок як між процесами обслуговування, так і між службами, які ці процеси підтримують. Процеси та їхні взаємозв'язки відображаються у вигляді відповідних графів, котрі і представляють створені процесні (процедурні) моделі обслуговування.

15.2. Структура взаємозв'язків між службами та процесами обслуговування

Технологічні процеси надання послуг на основі використання ресурсів ТЛК-систем мають бути узгоджені між собою і оптимізовані за критерієм мінімуму експлуатаційних витрат. З урахуванням вищезазначеного, а також прийнятого розподілу життєвого циклу підтримуваних сервісних угод за стадіями, що визначені у попередній лекції (підрозділ 14.4), структура процедур обслуговування має відтворювати взаємозв'язок служб та процесів обслуговування, що відображений на рис.15.1.

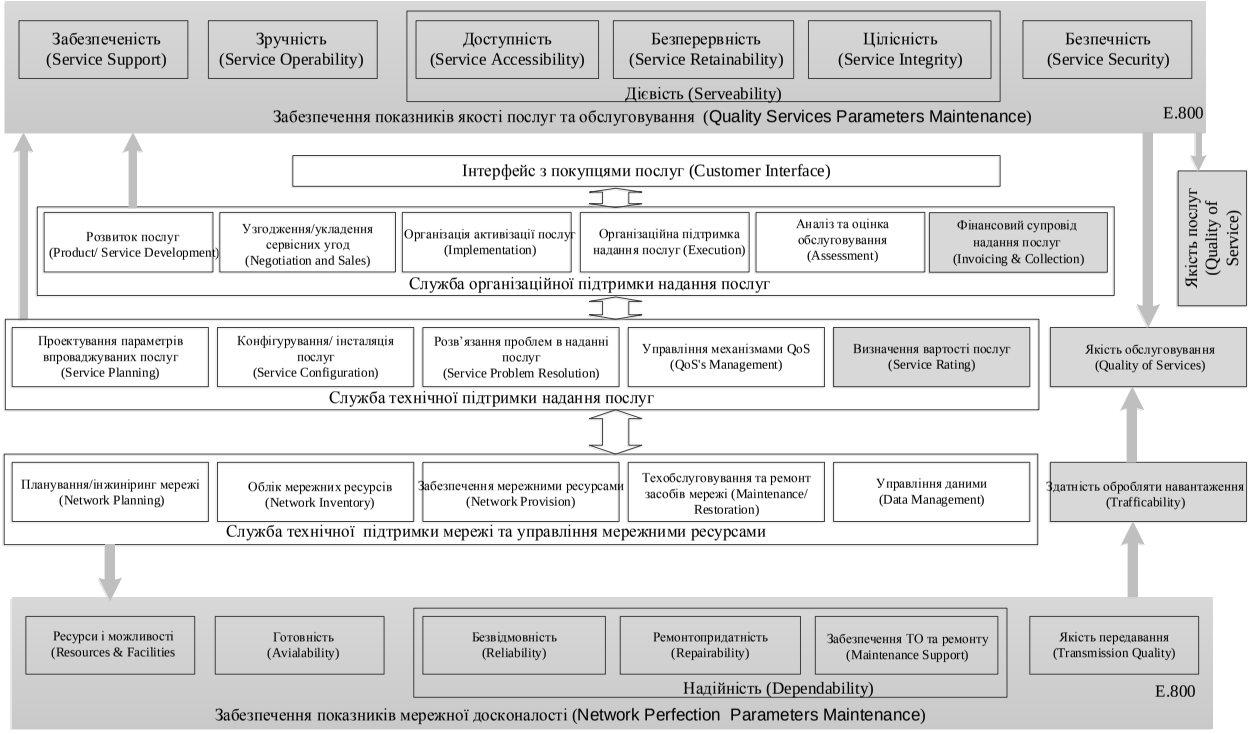


Рис.15.1. Взаємозв'язок служб та процесів обслуговування у ТЛК-система

Як видно із рис.15.1, уся множина технологічних процесів, які у сукупності визначають технологію надання послуг на базі ресурсів ТКО, за функціональною ознакою розподілена на три підмножини груп процесів:

1) підмножина груп процесів, що пов'язані із організаційною підтримкою надання послуг;

2) підмножина груп процесів, що пов'язані із технічною підтримкою надання послуг;

3) підмножина груп процесів, що пов'язані із технічною підтримкою мережі та управлінням ресурсами мережі.

У свою чергу, упорядкованість окремих процесів в рамках кожної із груп процесів відповідає структурі так званої *TOM*-моделі (*Telecommunication Operation & Management Model*), яка відображена на рис.15.1 у вигляді сукупності білих та темних прямокутників на білому фоні. (Два темних прямокутника на білому фоні відображають білінгові процеси - фінансовий супровід обслуговування та визначення вартості послуги, котрі хоч і входять до складу *TOM*-моделі, але у даному контексті не розглядаються). На кінець, структура розподілу процесів організаційної підтримки надання послуг повністю відображає стадії життєвого циклу сервісних угод, відповідно до умов котрих здійснюється обслуговування.

Кожна група процесів підтримується відповідною спеціалізованою службою оператора електрозв'язку. Зокрема, підтримку надання послуг, у т.ч. взаємодію із користувачами та покупцями послуг, здійснюють шість служб: функціональні обов'язки між п'ятьома із них розподілені відповідно до стадій життєвого циклу сервісних угод, а шоста служба забезпечує фінансовий супровід надання послуг і має враховуватися у процедурах обслуговування згідно із архітектурою *TOM*-моделі. Розподіл груп процесів технічної підтримки надання послуг, мережі та мережних ресурсів між спеціалізованими службами, які повинні реалізовувати ці процеси на практиці, здійснений відповідно до *TOM*-моделі, тобто п'ять служб на рівні управління наданням послуг і п'ять служб на рівні управління мережними ресурсами. Така структуризація груп процесів є гармонізованою із функціональною структурою характеристик властивостей якості

послуг та мережної досконалості (властивостей *QoS/NP*), що надана у рекомендації *E.800 MCE-T*. Ці властивості послуг та ресурсів мережі, а також їхній зв'язок із групами процесів та службами, які ці властивості забезпечують відображені на рис.15.1 у вигляді прямокутників на темному фоні.

Відображену структуру взаємозв'язків між службами підтримки обслуговування покупців послуг та групами процесів, які ці служби реалізують, використовують для побудови процедур обслуговування.

15.3. Мова відображення процесів обслуговування

Процедури обслуговування відобразимо у вигляді функціонально самодостатніх технологічних ланцюгів, що реалізують прийняту технологію обслуговування. Уся множина процесів обслуговування охоплюється наступними видами процедур:

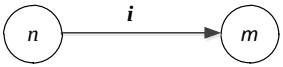
1) процедура підтримки створення та розвитку послуг;
2) процедура підтримки продажу послуг;
3) процедура опрацювання замовлень;
4) процедура опрацювання проблем;
5) процедура підтримки розрахунків за обслуговування;
6) процедура підтримки аналізу та оцінки якості обслуговування.

У якості основного складового елементу процедури обслуговування прийнято відображення одиничного вектору інформаційного потоку, який генерується певною однією службою і використовується іншою службою підтримки обслуговування. Іншими словами, кожен одиничний вектор має початок і кінець. Початок вектору пов'язується з групою процесів, що підтримуються якоюсь одною службою, а кінець – з групою процесів, що підтримуються будь-якою іншою службою.

Упорядковану послідовність одиничних векторів у вигляді ланцюго-подібного графа, яка відображає один із процесів обслуговування, назвемо процесною моделлю обслуговування.

Якщо за цих умов здійснити нумерацію служб, які входять до складу *TOM*-моделі, що відображена на рис.15.1, і нумерацію можливих інформаційних потоків за їхніми видами, то позначка

одиничного вектору буде мати наступний вигляд:



,

де n - порядковий номер служби – джерела даних інформаційного потоку;

m – порядковий номер служби – отримувача даних інформаційного потоку;

і - номер виду інформаційного потоку.

Нумерація служб згідно із їхніми порядковими номерами надана у табл. 15.1.

Таблиця 15.1

Прийнята нумерація функціональних служб оператора електрозв'язку

Назва функцій служби	Порядковий номер служби	Назва функцій служби (подовження)	Порядковий номер служби
Розвиток послуг	1	Розв'язання проблем в наданні послуг	9
Узгодження/укладення сервісних угод	2	Управління механізмами *QoS*	10
Організація активізації послуг	3	Визначення вартості послуг	11
Організація підтримки надання послуг	4	Планування / інженерія мережі	12
Аналіз та оцінка обслуговування	5	Облік мережних ресурсів	13
Фінансовий супровід надання послуг	6	Забезпечення мережними ресурсами	14

Проектування параметрів впроваджуваних послуг	7	Техобслуговування та ремонт засобів мережі	15
Конфігурування та інсталяція послуг за сервісними угодами	8	Управління даними	16

Нумерація видів інформаційних потоків буде надана надалі під час опису процедур обслуговування. При цьому прийняті наступні позначення:

ІП*x*, де *x* – порядковий номер виду інформаційного потоку (ІП);

$С_y$ – служба підтримки надання послуг (С) із порядковим номером, що позначається як *y*.

15.4. Процедура підтримки створення та розвитку послуг

Необхідність модернізації та розвитку вже існуючих послуг, а також створення нових послуг обумовлюється змінами в потребах клієнтів та здобутим практичним досвідом в процесі надання послуг.

На цій підготовчій стадії життєвого циклу *SLA* здійснюються наступні види робіт: ідентифікація потреб та динаміки змін у потребах користувачів; визначення характеристик послуг, що мають відповідати новим потребам користувачів (зокрема, визначення бажаного набору параметрів послуги, їхніх припустимих значень, бажаних рівнів послуги тощо); визначення та оцінка мережних ресурсів, що є необхідними для впровадження нової або модернізованої послуги; розробка нових темплетів *SLA* (кінцевий результат робіт на цій стадії життєвого циклу сервісної угоди).

Організаційно-технологічна схема відображення процесів, що мають виконуватися технологічними підрозділами оператора електрозв'язку на стадії створення нової або розвитку вже існуючої послуги (тобто, технологічний ланцюг потоків і процесів створення/модернізації послуги), показана у вигляді графа на рис.

15.2.

1. Джерело ІП 1 - **інтерфейс споживачів послуг (ІПК)**.

2. **ІП 1 –** це інформаційний потік із побажаннями та вимогами споживачів щодо характеристик вже існуючих послуг та розробки нових послуг: функціональні характеристики послуг, параметри продуктивності, параметри *QoS*, точки доступу до послуг (*SAP*), технології доступу тощо.

3. Отримувач даних ІП 1 – **служба узгодження /укладання сервісних угод (С2)**. Ця служба збирає та здійснює попередню агрегацію даних ІП 1.

4. **ІП 2** – інформаційний потік із агрегованими даними щодо характеристик вже існуючих або нових послуг, що є бажаними для потенційних користувачів.

5. Отримувач даних ІП2 – **служба розвитку послуг (С1).** Ця служба виконує оцінку даних ІП2 під кутом зору економічної доцільності модернізації існуючих або розробки нових послуг: бізнес-потенціал нової послуги, можливі додаткові прибутки від модернізації послуги і т. ін.

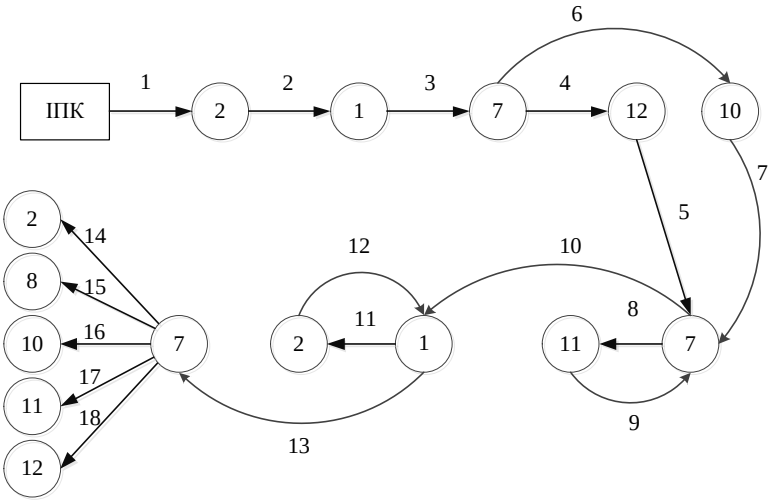


Рис. 15.2 . Процедура створення та розвитку послуги

6. **ІП3** – інформаційний потік із результатами оцінки бізнес-

потенціалу нових послуг та додатковими зисками від модернізації вже існуючих послуг, часу життя послуг та інших характеристик бізнес-плану впровадження послуг.

7. Отримувач даних ІП3 – **служба проектування параметрів впроваджуваних послуг (С7).** Ця служба на основі даних ІП3 здійснює проектування параметрів послуг: нових або тих, що мають бути модернізованими. В процесі проектування, як правило, досліджується кілька варіантів архітектури послуги, їхній вплив на рівень якості послуги. При цьому намагаються узгодити (оптимізувати) між собою вимоги до сервіс- та мережно-орієнтованих параметрів, а також до сервіс/мережно-незалежних параметрів, тобто найти компромісне рішення щодо вибору параметрів послуги. Компроміс полягає в тому, щоб, з одного боку, забезпечити високий рівень якості надання нової/модернізованої послуги, а з другого боку, при цьому суттєво не знизити коефіцієнт використання мережних ресурсів та (або) не підвищити ймовірність виникнення перенавантажень трафіку.

В процесі проектування параметрів послуги служба С7, як правило, взаємодіє із службою С10 і С12, надсилаючи відповідні запити (ІП4 і ІП5) на адресу цих служб. Служба С12 отримує запити щодо можливостей мережної інфраструктури підтримати запроектовані параметри нової/модернізованої послуги, а служба С10 - щодо можливостей механізмів QoS забезпечити необхідну якість надання нової/модернізованої послуги. Опрацювавши такі запити, служби С10 та С12 надсилають необхідні відповіді на адресу служби С7 (ІП5 та ІП7). Процес інформаційного взаємного обміну між службами С7 – С10 та С7 – С12 триває в ітеративному режимі доти, поки служба С7 отримає кінцеві результати проектування параметрів нової/модернізованої послуги.

8. **ІП 4** – потік запитів служби С7 на адресу служби С12 із попередніми (проміжними) оцінками параметрів впроваджуваної послуги щодо можливості мережної інфраструктури підтримати ці варіанти параметрів. Цей потік містить дані щодо усіх технічних параметрів послуги (як сервіс-орієнтованих, так і мережно-орієнтованих), необхідних для її надання, включаючи *QoS*-параметри, географічні та часові обмеження тощо. В запитах може міститися інформація про можливі варіанти рішень під час

проектування послуги із визначеними пріоритетами або преференціями в альтеративних рішеннях.

9. Отримувач даних ІП 4 – **служба планування/інженерії мережі (С12).**

Ця служба, взявши до уваги дані ІП 4, намагається розробити детальні вимоги щодо кількості та якості мережних ресурсів, які є необхідними для впровадження послуги із визначеними в ІП 4 характеристиками. Аналізуються вимоги, які пред'являються новою послугою до параметрів мережної досконалості, у порівнянні із існуючою структурою мережних ресурсів та навантажень мережних елементів. Проводиться інженерія додаткових потоків. Оцінюється вартість необхідних додаткових мережних ресурсів, вартість їхньої інсталяції, проміжок часу, потрібний для впровадження нової або модернізованої послуги на МПД і т.ін. Визначається також порядок дій персоналу під час впровадження послуги. Якщо в процесі дослідження можливостей мережі щодо впровадження/модернізації послуги виявиться, що існуючі технології не дозволяють із достатньою ефективністю здійснити таке впровадження, то служба С12 має надати рекомендації щодо доцільності і шляхів здійснення модернізації мережної інфраструктури з відповідними оцінками вартості модернізації та її терміну.

10. **ІП5** – потік відповідей служби С12 на запити служби С7 із результатами планування та інженерії мережі, що здійснювались у зв'язку із впровадженням нової послуги або модернізацією вже існуючої послуги за наданими у запитах специфікаціями послуги. Цей інформаційний потік містить дані з оцінками ресурсних та часових витрат на модифікацію мережної інфраструктури, які доведеться нести, якщо буде прийнято рішення про впровадження або модернізацію досліджуваної послуги за наданими специфікаціями.

11. **ІП 6** – потік запитів служби С7 на адресу служби С10 із попередніми (проміжними) оцінками параметрів впроваджуваної послуги щодо можливості підтримки наданих варіантів параметрів послуги механізмами QoS. Цей потік містить дані щодо усіх технічних параметрів послуги (як сервіс-орієнтованих, так і мережно-орієнтованих), необхідних для її надання, включаючи

параметри мережної досконалості, географічні та часові обмеження тощо. В запитах може міститися інформація про можливі варіанти рішень під час проектування послуги із визначеними пріоритетами або преференціями в альтеративних рішеннях.

12. Отримувач даних ІП6 – **служба управління механізмами QoS (С10).**

Ця служба, взявши до уваги дані ІП6, намагається розробити процедури управління якістю надання нової/модернізованої послуги, які є необхідними для впровадження послуги із визначеними в ІП6 характеристиками. Аналізуються вимоги, які пред'являються новою послугою до служби QoS, у порівнянні із існуючою архітектурою механізмів цієї служби. Оцінюються можливості щодо рівнів надання досліджуваної послуги, проміжок часу, потрібний для інсталяції нових процедур керування механізмами QoS і т.ін.

13. **ІП 7** – потік відповідей служби С10 на запити служби С7 із результатами розробки процедур управління механізмами QoS та оцінки можливих рівнів надання нової/модернізованої послуги за наданими у запитах специфікаціями цієї послуги.

14. Отримувач даних ІП5 та ІП 7 - **служба проектування параметрів впроваджуваних послуг (С7).** Ця служба, взявши до уваги дані потоків ІП5 та ІП7, оцінює здійснюваність (рос. – реализуемость) нової/модернізованої послуги за досліджуваними варіантами специфікацій цієї послуги. Якщо результат оцінки – позитивний, то ця служба здійснює техно-робоче проектування послуги, включаючи створення її трафаретів. Розроблюється також бізнес-план впровадження нової/модернізованої послуги в експлуатаційну практику сервіс-провайдера, включаючи розробку моделі ризиків, пов'язаних із цим впровадженням. В процесі проектування служба С7 взаємодіє в ітеративному режимі із службою С11 щодо визначення вартості послуги та розробки тарифної політики (потоки ІП8 та ІП9), а також через службу С2 взаємодіє із службою С3 щодо визначення потоків матеріальних ресурсів, які необхідно акумулювати для забезпечення впровадження нової/модернізованої послуги (потоки ІП10, ІП11, ІП12 та ІП13).

15. **ІП8** – потік запитів служби С7 на адресу служби С11 із

характеристиками нової/модернізованої послуги, що є необхідними для визначення вартості послуги та тарифної політики, пов'язаної із її продажем.

16. Отримувач даних ІП8 – **служба визначення вартості послуг (С11).** Ця служба на основі даних ІП8 надає рекомендації проектувальникам послуги з проблем ціноутворення та розробки тарифної політики.

17. **ІП 9** – потік відповідей служби С11 на запити служби С7 із рекомендаціями щодо визначення ціни нової/модернізованої послуги та відповідної тарифної політики.

18. **ІП 10** - потік запитів служби С7 на адресу служби С1 щодо обсягів та динаміки забезпечення матеріальними ресурсами процесу надання нової/модернізованої послуги.

19. Отримувач даних ІП 10 – **служба розвитку послуг (С1).** Ця служба, консультуючись із **службою узгодження/укладання сервісних угод (С2)** шляхом організації потоків **ІП 11 та ІП 12**, і на основі даних потоку ІП 10 розроблює варіанти постачання матеріальними ресурсами, необхідними для впровадження нової/модернізованої послуги.

20. **ІП 13** – потік відповідей служби С1 на адресу служби С7 із розробленими варіантами забезпечення впровадження нової/модернізованої послуги матеріальними ресурсами.

21. Отримувач даних ІП9 та ІП13 – **служба проектування параметрів впроваджуваних послуг (С7).** В результаті проектування на основі даних ІП5, ІП7, ІП9 та ІП13 служба С7 визначає усі параметри (точніше, - області припустимих значень усіх параметрів) нової/модернізованої послуги, які дозволяється використовувати у якості параметрів SLA під час укладання сервісних угод. Дані щодо функціональності нової/модернізованої послуги, областей припустимих значень параметрів SLA, цін та тарифної політики, усієї множини умов та обмежень, які мають супроводжувати процес її надання (зокрема, зони географічного покриття обслуговуванням, часові обмеження і т.ін.), за допомогою потоків ІП14, ІП15, ІП16, ІП17 та ІП18 надсилаються на адресу служб С2, С8, С10, С11,С12 з метою, щоб перелічені служби мали змогу підготуватися до надання нової/модернізованої послуги.

22. **ІП 14, ІП 15, ІП 16, ІП 17, ІП 18** – потоки із кінцевими

результатами проектування нової/модернізованої послуги, що надсилаються службою С7 на адресу служб, які мають безпосереднє відношення до процесу впровадження послуг. Це – служби С2, С8, С10, С11,С12.

15.5. Процедура підтримки продажу послуг

Стадія узгодження та укладання сервісної угоди передбачає виконання наступних робіт:

- відбір величин параметрів *SLA*, що забезпечують нормальне функціонування прикладних застосувань клієнтів і, в той же час, не погіршують якість обслуговування вже існуючих користувачів послуг і не завдають неприпустимих перенавантажень мережного обладнання;

- узгодження цінових пропозицій, штрафних санкцій щодо невиконання умов *SLA*, методів, засобів та періодичності звітування щодо поточного стану обслуговування, методів та засобів зворотного зв'язку клієнтів із сервіс-провайдером.

Кінцевим результатом на цій стадії життєвого циклу SLA є узгоджена та підписана обома сторонами сервісна угода.

Організаційно-технологічна схема відображення процесів, що мають виконуватися технологічними підрозділами оператора електрозв'язку на стадії підтримки продажу послуги (тобто, технологічний ланцюг потоків і процесів підтримки продажу послуги), показана у вигляді графа на рис.15.3. Кінцевим результатом робіт за цією стадією життєвого циклу SLA являється узгоджена за усіма параметрами та підписана з обох сторін сервісна угода, яка точно визначає обов'язки сторін, характеристики послуги, ціну, термін та умови її надання.

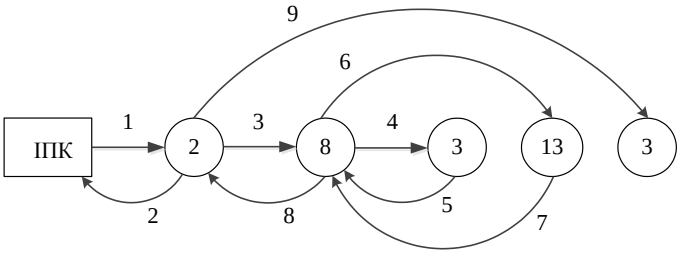


Рис.15.3. Процедура підтримки продажу послуги

Джерело ІП 1 - **інтерфейс покупців послуг (ІПК)**.

ІП 1 – потік запитів щодо можливостей та умов отримання послуги із попередньо визначеними характеристиками.

Отримувач даних ІП1 – **служба узгодження/укладання сервісних угод (С2).** Ця служба здійснює процедуру узгодження потреб покупця послуги із ресурсними можливостями оператора щодо надання послуг на базі приналежній йому ТЛК-системі. Уявнивши суть потреб покупця, зокрема потреб його прикладних застосувань в отриманні телекомунікаційних послуг, і знаючи ресурсні можливості ТЛК-системи, служба С2 в ітеративній взаємодії із покупцем намагається знайти компромісні пропозиції, які б задовольняли покупця за усіма аспектами обслуговування – функціональність послуги, *QoS*-параметри, ціна послуги, географічне покриття обслуговуванням, режими змін в умовах обслуговування, методи та точки доступу до послуги, механізми та періоди звітування, взаємні зобов'язання, штрафні санкції, інші умови *SLA*.

ІП 2 – потік відповідей служби С2 на запити потенційного покупця послуги в процесі узгодження умов сервісної угоди.

ІП 3 – потік із даними параметрів *SLA*, які служба С2 узгодила із покупцем послуги.

Отримувач даних ІП3 – **служба конфігурування/інсталяції послуг (С8).** Взявши до уваги дані ІП3, служба С8 здійснює В процесі такої оцінки служба С8 організує інформаційну взаємодію із службами С3 та С13, надсилаючи відповідні запити на їхню адресу.

ІП 4 – потік із запитами служби С8 на адресу служби С3 щодо можливих термінів акумуляції матеріальних ресурсів, необхідних для активізації послуги згідно із заданими параметрами SLA.

Отримувач даних ІП4 – **служба організації активізації послуг (С3)**. Взявши у якості вихідних дані ІП4, служба С3 здійснює оцінку терміну, необхідного для акумуляції матеріальних ресурсів згідно із заданими параметрами SLA.

ІП5 – потік із відповідями служби С3 на запити служби С8 щодо термінів акумуляції матеріальних ресурсів, необхідних для активізації послуг.

10. **ІП6 –** потік із запитами служби С8 на адресу служби С13 щодо можливих термінів підготовки мережних ресурсів до опрацювання замовлень, які відповідають наданим параметрам *SLA*.

11. Отримувач даних ІП6 – **служба обліку мережних ресурсів (С13).** Ця служба у відповідь на запити ІП6 визначає терміни підготовки мережних ресурсів до опрацювання замовлення згідно із наданими параметрами *SLA*.

12. **ІП 7** – потік із відповідями служби С13 на запити служби С8 щодо термінів підготовки мережних ресурсів.

13. Отримувач даних ІП5 та ІП7 – **служба конфігурування/інсталяції послуг (С8).** На основі аналізу власних ресурсів, а також даних потоків ІП5 та ІП7, ця служба визначає необхідний проміжок часу між моментом підписання контракту (та відповідної сервісної угоди) та моментом закінчення робіт із активізації послуги, що має надаватися відповідно до умов SLA.

14. **ІП8** – потік із відповідями служби С8 на запити служби С2, що містять визначення часових проміжків, які потрібні для конфігурування та інсталяції параметрів послуг відповідно до наданих умов *SLA* з урахуванням часу, необхідного для акумуляції усіх матеріальних ресурсів, що забезпечують активізацію цих послуг.

15. Отримувач даних ІП8 – **служба узгодження/укладання сервісних угод (С2).** Маючи дані параметрів *SLA*, які служба С2 узгодила із покупцем послуги, а також дані потоку ІП8, служба С2 здійснює процедуру підписання контракту та відповідної *SLA*. Після підписання контракту та сервісної угоди з боку обох сторін інформація щодо усіх параметрів *SLA*, які містяться в тексті підписаної сервісної угоди, передається службі С3 на опрацювання.

16. **ІП9 –** потік із параметрами *SLA* підписаних сервісних угод, що ініціюється службою С2.

17. Отримувач даних ІП 9 – **служба організації активізації послуг (С3).**

15.6. Процедура обробки замовлень

На стадії імпліментації послуги здійснюються наступні види

робіт:

- формуються заявки на усі види додаткових ресурсів, що необхідні для забезпечення надання послуги відповідно до умов *SLA*;
- активізуються заявлені ресурси;
- конфігуруються, інсталюються, активізуються та тестуються ресурси мережі, на основі якої буде здійснюватися надання послуги за новою сервісною угодою;
- конфігуруються, інсталюються, активізуються та тестуються механізми служби підтримки якості послуги відповідно до умов нової *SLA*;
- активізується та тестується послуга у цілому в умовах, що максимально наближені до реальних умов її надання.

Кінцевий результат цієї стадії життєвого циклу *SLA* – повністю придатна для користування послуга відповідно до умов нової *SLA*.

Організаційно-технологічна схема відображення процесів, що мають виконуватися технологічними підрозділами оператора електрозв'язку на стадії опрацювання замовлень (тобто, технологічний ланцюг потоків і процесів опрацювання замовлень відповідно до умов SLA), показана у вигляді графа на рис. 15.4.

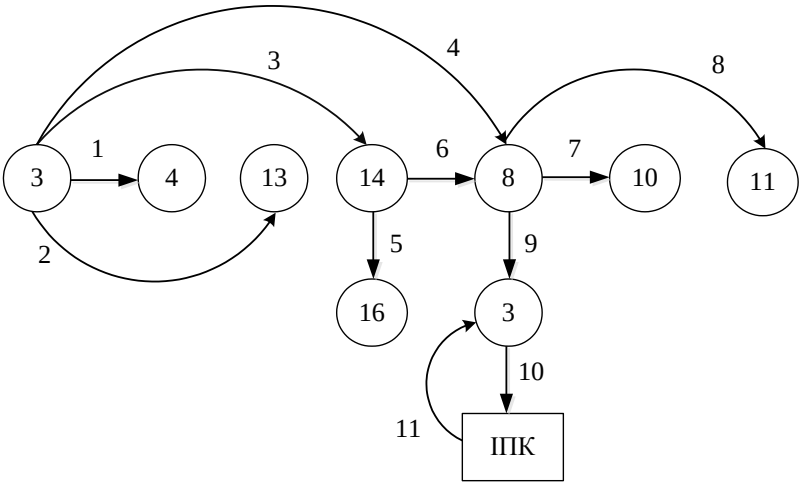


Рис. 15.4 . Процедура опрацювання замовлень

Після того, як сервісна угода набула чинності, протягом відведеного проміжку часу здійснюється підготовка ресурсів мережі та інших ресурсів до набуття стану, коли забезпечується можливість надання послуг у відповідності із умовами сервісної угоди. Здійснюється побудова каналу доступу клієнта до мережної інфраструктури сервіс-провайдера (у разі потреби), виконується конфігурація послуги та мережних ресурсів відповідно до умов *SLA*, інсталюються відповідні параметри *QoS* та показників мережної досконалості, створюються канали обміну інформацією між кінцевим сервіс-провайдером та представниками покупця послуги, тестується обладнання, вмикаються механізми обліку ресурсів, що надаються згідно умов *SLA*, переводяться в активний стан усі ресурси, що пов'язані із забезпеченням надання послуг відповідно до умов сервісної угоди.

Про досягнення активного стану обладнання інформується покупець, разом з котрим виконується заключний етап тестування обладнання на прикладах, максимально наближених до умов використання послуги прикладними застосуваннями покупця.

1. **Служба організації активізації послуг (С3)** інсталює потоки ІП 1, ІП 2 та ІП3 на адресу служб С4, С8, С13 та С14 із заявками на активізацію відповідних ресурсів цих служб.

2. **ІП1** – потік заявок служби С3 на адресу служби С4 із параметрами *SLA*, що є необхідними для організації каналу звітування покупця про стан обслуговування.

3. **ІП2** – потік заявок служби С3 на адресу служби С13 із параметрами *SLA*, що є необхідними для постановки на облік ресурсів, які будуть використовуватися згідно умов SLA.

4. **ІП3** – потік заявок служби С3 на адресу служби С14 із параметрами *SLA*, що є необхідними для забезпечення надання послуг відповідними мережними ресурсами.

5. **ІП4** – потік заявок служби С3 на адресу служби С8 із параметрами *SLA*, що є необхідними для конфігурування та інсталяції послуг.

6. Отримувач даних ІП1 – **служба організаційної підтримки надання послуг (С4).** На основі даних потоку ІП1 ця служба створює канал звітування покупця про стан обслуговування.

7. Отримувач даних ІП2 – **служба обліку мережних ресурсів**

(С13). На основі даних потоку ІП2 ця служба інсталює параметри та активізує механізми обліку ресурсів згідно умов *SLA*.

8. Отримувач даних ІП3 – **служба забезпечення мережними ресурсами (С14).** На основі даних потоку ІП3 ця служба здійснює конфігурування елементів мережі та інсталяцію параметрів мережної досконалості, щоб забезпечити можливість раціонального конфігурування параметрів послуг відповідно до умов *SLA*. Дані щодо виконаних змін у структурі мережних ресурсів заносяться у базу даних **служби управління даними (С16)** потоком **ІП5**.

9. **ІП6** – потік даних, ініційований службою С14 на адресу служби С8, із інстальованими параметрами мережної досконалості відповідно до умов SLA. Ці дані використовуються службою С8 під час конфігурування та інсталяції параметрів послуг.

10. Отримувач даних ІП4 та ІП6 – **служба конфігурування/інсталяції послуг (С8).** На основі даних ІП4 та ІП6 ця служба здійснює конфігурування та інсталяцію параметрів послуг відповідно до умов *SLA*. Дані щодо конфігурації послуг та інстальованих параметрів цих послуг і параметрів показників мережної досконалості надсилаються на адресу служб С10 та С11 потоками ІП7 та ІП8 відповідно. Зконфігуровані послуги активізуються. Про це повідомляється служба С3 потоком ІП9.

11. **ІП7** – потік, ініційований службою С8, на адресу **служби управління механізмами QoS (С10)** із конфігураційними даними інстальованих послуг. Ці дані використовуються службою С10 для настроювання механізмів *QoS*.

12. **ІП8** – потік, ініційований службою С8, на адресу **служби визначення вартості послуг QoS (С11)** із конфігураційними даними інстальованих послуг. Ці дані використовуються службою С11 для настроювання механізмів визначення вартості послуг (зокрема, параметрів білінгових систем) на диференційоване обслуговування з урахуванням умов *SLA* (одержаних преференцій, наданих пріоритетів тощо).

13. **ІП9** – повідомлення, ініційовані службою С8, на адресу служби С3 про активний стан системи обслуговування щодо надання послуг за сервісними угодами, параметри котрих заявлялись службою С3 через потік ІП4.

14. Отримувач даних ІП9 – **служба організації активізації послуг (СЗ).** Отримавши дані через потік ІП9 про досягнення активного стану обладнання згідно умов сервісної угоди, ця служба інформує покупця про готовність розпочати процес обслуговування і, в разі необхідності, організує разом із представниками покупця заключний етап тестування обладнання (потоки **ІП 10** та **ІП 11**) на відповідність вимогам *SLA* на прикладах, максимально наближених до умов використання послуги прикладними застосуваннями покупця.

15.7. Процедура опрацювання проблемних ситуацій

Процес надання послуги (в частині управління якістю обслуговування) складається із:

- контролю відповідності поточних параметрів обслуговування, що визначені у *SLA*;
- звітування про реальний стан обслуговування за сервісною угодою;
- обробки запитів та реакції на запити покупця послуги відповідно до умов *SLA*;
- виявлення подій, що пов'язані із деградацією послуги або відмов у її наданні, та сповіщення спеціалізовані служби про виниклі події.

Організаційно-технологічна схема відображення процесів, що мають виконуватися технологічними підрозділами оператора МПД на стадії опрацювання проблем (тобто, технологічний ланцюг потоків і процесів опрацювання проблем, що виникають під час надання послуг), показана у вигляді графів на рис.15.5 та 15.6.

Рис.15.5 відображає ситуацію опрацювання проблем в процесі надання послуг, коли:

- виникло **ушкодження (*Impairment*),** тобто аномалія або дефект в роботі обладнання, але не його відмова, за умов відсутності переривань в наданні послуг;
- виникло переривання в наданні послуги, але не у більшій мірі, чим це визначено умовами сервісної угоди, тобто виникла ситуація, коли **параметр деградації послуги (*Service Degradation Factor, SDF*)** ще не перевищив можливого ступеню деградації послуги відносно параметрів *QoS*, що зафіксовані у *SLA*.

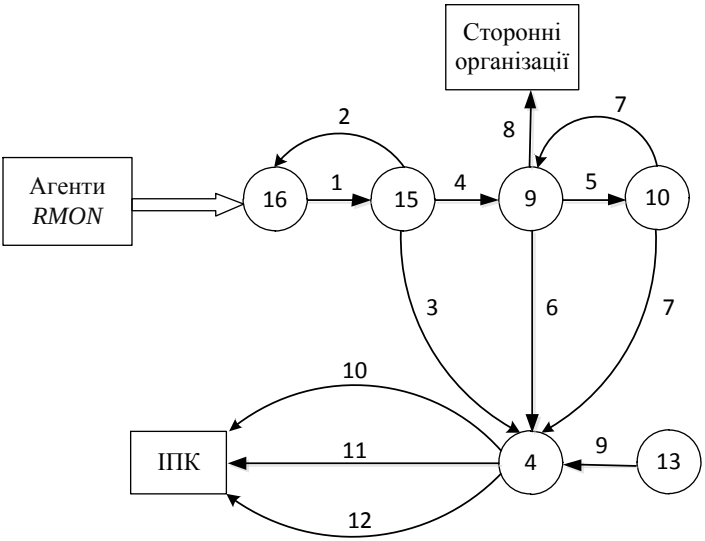


Рис.15.5. Процедура опрацювання проблем у випадку, коли не виникло порушень умов SLA

У цьому випадку у якості джерел **необроблених даних щодо функціонування (*Raw Performance Data*)** (тобто, необроблених первісних даних щодо стану обладнання та поточного рівня обслуговування), а також сигналів тривоги та повідомлень про перетин порогів виступають **агенти *RMON*** системи управління ТЛК-системою.

Модель обслуговування для такого випадку відображається у вигляді нижченаведеної послідовності одиничних векторів.

1. Отримувач необроблених даних щодо функціонування - **служба управління даними (С16).** В процесі надання послуг необроблені первісні дані щодо функціонування телекомунікаційної мережі та служби *QoS*, як правило, в автоматичному режимі збираються від усіх задіяних на мережі джерел генерації даних - на рівні систем управління елементами мережі, мережних серверів, серверів застосувань тощо. Ці дані, у т.ч. дані щодо поточного стану обслуговування, піддаються первісній обробці і накопичуються в базі даних служби С16.

2. **ІП 1** – потік інформації із бази даних служби С16, яка є необхідною для контролю відповідності обладнання.

3. Отримувач даних ІП1 - **служба техобслуговування та ремонту засобів мережі (С15).**

Служба С15 – це служба, яка безпосередньо у реальному часі здійснює нагляд за поточним станом обслуговування – як за станом мережних ресурсів, так і за станом надання послуг (оскільки контрольовані параметри мережної досконалості і якості надання послуг являють собою взаємопов'язану сукупність). Дані потоку ІП1 використовуються службою С15 в процесі контролю стану ресурсів мережі та ресурсів служби *QoS*. Служба С15 у реальному часі відслідковує події, що пов'язані із контролем відповідності усього телекомунікаційного обладнання. Зокрема, відслідковуються:

- індикація тривоги (*Alarm*) – попереджувальна індикація про виниклу подію, яка може привести або вже привела до деградації параметрів послуги або до відмови в наданні послуги (наприклад, відмова мережного елемента, уповільнення роботи прикладного застосування, зменшення функціональності підсистеми керування тощо);

- повідомлення про перетин порогу (*Threshold Crossing Alert*) – повідомлення про виникнення події, коли контрольований параметр досягає або перетинає встановлений поріг гранично припустимого значення цього параметру. Пороги припустимих значень контрольованих параметрів визначаються умовами сервісних угод. Перетин порогу за межі припустимих значень параметру, як правило, означає підвищену ймовірність виникнення перевантажень трафіком або зменшення здатності обладнання у повній мірі виконувати штатні функції.

4. Якщо в процесі надання послуг відповідність оцінок контрольованих параметрів знаходиться в припустимих межах відносно заявлених значень параметрів у розрізі усіх діючих сервісних угод, то служба С15 потоком **ІП2** вносить відповідні дані у базу даних служби С16 і потоком **ІП3** надсилає повідомлення службі С4 про нормальний стан обслуговування.

5. У разі виявлення невідповідності (зокрема, появи сигналу тривоги) служба С15 реалізує процедури локалізації та усунення

виниклої проблеми. На початку цієї процедури вирішуються дві групи питань:

1) з яким видом ресурсів слід пов'язати виниклу проблему? Чи її виникнення обумовлюється некоректною роботою мережних ресурсів, чи її слід пов'язати із роботою механізмів служби *QoS*, чи вона має комплексний характер?

2) наслідком проблеми буде порушення умов діючих сервісних угод, чи стануться погіршення в обслуговуванні у припустимій мірі?

В залежності від отриманої відповіді на поставлені вище питання, вибираються процедури вирішення проблеми.

Якщо виявиться, що виникнення проблеми обумовлюється некоректною роботою мережних ресурсів і не призвело до порушень умов діючих сервісних угод, то служба С15 самостійно за рахунок власних сил вирішує цю проблему. Процедури вирішення проблем у таких випадках, як правило, регламентуються відповідними внутрішньо корпоративними стандартами: інструкціями, регламентами, правилами технічної експлуатації і т. ін..

Якщо виявиться, що виникнення проблеми обумовлено некоректною роботою мережних ресурсів і призвело до порушень умов діючих сервісних угод, то служба С15 діє згідно із процедурою, яка викладена у попередньому підрозділі. Якщо ж виявиться, що проблема має комплексний характер або пов'язана з роботою механізмів надання послуг, то про це повідомляється служба розв'язання проблем в наданні послуг С9. Такі повідомлення передаються потоком ІП 4.

6. **ІП 4** – потік із даними щодо виявленої проблеми в наданні послуг: час появи проблеми, її характер, стан обладнання на той момент, зроблені кроки та пропозиції щодо вирішення проблеми тощо.

7. Отримувач даних ІП4 - **служба розв'язання проблем в наданні послуг (С9).**

На основі даних ІП4 служба С9 вирішує проблеми в наданні послуг. Перш за все, вирішується питання щодо можливості порушень умов діючих сервісних угод.

Якщо в процесі розв'язання проблем виявляться несправності

або похибки у настроюванні параметрів обладнання служби *QoS*, які не призвели до порушень умов діючих сервісних угод, то рекомендації щодо усунення цих проблем надаються службі управління механізмами *QoS* (потоком ІП5). Крім того, після усунення проблеми (або під час усунення проблеми, якщо цей процес затягнувся) служба С9 потоком ІП 6 надає службі С4 усю інформацію, що є необхідною для аналіза наслідків виникнення проблеми у розрізі виконання умов *SLA*, приймання відповідних заходів та інформування покупця послуги – час виникнення та термін існування проблеми, її характеристика, наслідки виникнення проблеми, зокрема її вплив на якість надання послуг у розрізі кожної сервісної угоди і т. ін.

8. **ІП 5 –** потік із рекомендаціями щодо усунення проблем в наданні послуг або змін в управлінні механізмами *QoS*, що надаються службою С9 для служби С10.

9. **ІП 6 –** потік із описом виявлених проблем та їхнього впливу на якість надання послуг, що надаються службою С9 для служби С4.

10. Отримувач даних ІП5 – **служба управління механізмами *QoS* (С10).**

Керуючись інформацією, що надходить потоком ІП 5, служба С10, у разі необхідності, вносить необхідні зміни в управління механізмами *QoS*, після чого здійснює оцінку досягнутого в результаті цих змін рівня надання послуг. Інформація щодо отриманих оцінок параметрів *QoS* та виміряного рівня послуг надається потоком ІП7 службі С9 для прийняття рішень щодо успішності розв'язання виявленої проблеми в наданні послуг і службі С4 для підготовки звітів згідно умов діючих *SLA*.

11. **ІП7** – потік із оцінками параметрів *QoS* та рівнів послуг, що надсилається службою С10 на адресу служб С9 та С4.

12. Отримувач даних ІП 7 – **служба розв'язання проблем в наданні послуг (С9).** На основі даних потоку ІП 7 служба С9 приймає рішення щодо успішності її спроб розв'язати виявлену проблему в наданні послуг.

Якщо спроби виявились невдалими, то служба С9 разом із службами С15 і С10 в діалоговому режимі продовжує намагання вирішити проблему.

Якщо протягом тривалого часу (який визначається у відповідній регламентуючій документації) і ці спроби виявились невдалими, то служба С9 сповіщає про це Дирекцію оператора електрозв'язку і звертається за допомогою до сторонніх спеціалізованих організацій – автосорсінгових компаній або компаній – виробників обладнання (**потік заявок про допомогу сторонніх організацій – ІП 8**).

У будь-якому випадку (успішного або неуспішного вирішення проблем із погіршенням якості надання послуг) служба С9 потоком ІП6 інформує службу С4 про виявлені факти погіршення якості надання послуг (хоч і в припустимих умовами *SLA* межах) і надає їй усю інформацію, яка є необхідною для звітування перед покупцями послуг про поточний стан обслуговування.

13. **ІП 9** – потік із даними щодо використаних мережних ресурсів, що надсилаються **службою обліку мережних ресурсів (С13)** на адресу служби С4 в процесі надання послуг для підготовки відповідних звітів.

14. Отримувач даних ІП3, ІП6, ІП7 та ІП9 – **служба організаційної підтримки надання послуг (С4).**

Дані потоків ІП3, ІП6, ІП7 та ІП9 у повній мірі відображають хід обслуговування за умов, коли порушень умов діючих сервісних угод не виявлено. На основі аналізу цих даних згідно з умовами діючих сервісних угод служба С4 виготовляє **звіти про поточний стан обслуговування (*Performance Report*).**

Звіти представляються окремо щодо кожної точки доступу до послуги або кожної групи точок доступу до послуги. Періодичність звітування обумовлюється окремо для кожного виду звіту в рамках кожної сервісної угоди.

15. **ІП 10** – потік із **звітами про виконання вимог сервісної угоди щодо рівнів наданих послуг (*Service Level Agreement Report*).** Це – стислі експрес-звіти про виконання вимог *SLA* щодо рівнів наданих послуг без деталізації характеристик стану обслуговування. Надсилаються покупцям послуг з метою їхнього оперативного інформування.

16. **ІП 11** - потік із **звітами про якість наданої послуги (*Quality of Service Report*)**. Це – звіти з оцінками досягнутих в процесі обслуговування рівнів якості наданої послуги, зокрема з поточними оцінками параметрів *QoS*. Ціль цього звітування -

надати можливість покупцю послуги порівняти реально досягнуті значення показників якості отриманої послуги з гарантованими параметрами *GoS*, що зафіксовані у *SLA*.

17. **ІП 12** – потік із **звітами про використані мережні ресурси (*Resource Report*)**. Це – звіти про характеристики реального трафіка застосувань покупця мережних ресурсів, що утворюється цими застосуваннями на визначених проміжках часу, а також про кількість і якість використаних покупцем мережних ресурсів за обумовлені проміжки часу.

Рис.15.6 відображає ситуацію опрацювання проблем в процесі надання послуг, коли:

- виявлено переривання в наданні послуг через відмови в роботі обладнання у більшій мірі, чим це визначено умовами сервісної угоди;

- виявлена неприпустима деградація послуги, тобто виявлена ситуація, коли **параметр деградації послуги (*Service Degradation Factor, SDF*)** перевищив припустиму ступень деградації послуги відносно параметрів *QoS*, що зафіксовані у *SLA*.

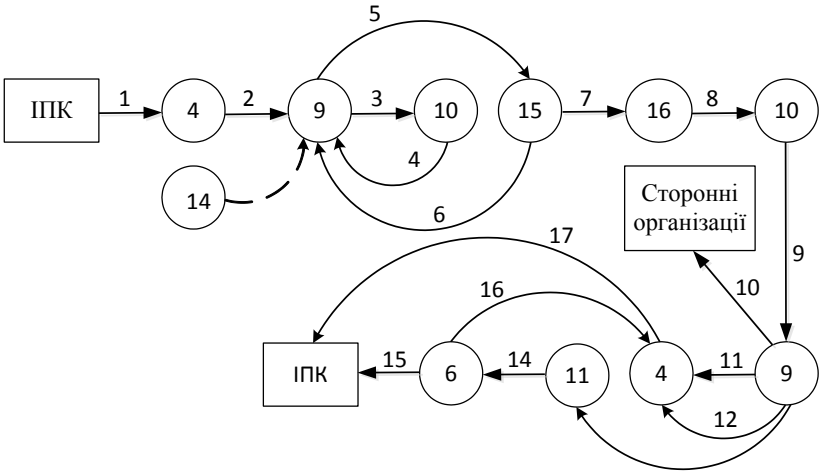


Рис.15.6. Процедура опрацювання проблем у випадку, коли виникло порушення умов SLA

У цьому випадку процедура обслуговування відрізняється від наданої вище процедури опрацювання виявленої проблеми,

починаючи з моменту, коли служба розв'язання проблем в наданні послуг (служба С9) виявила існування порушень умов будь-якої із діючих сервісних угод. Крім того, такі порушення можуть бути виявлені безпосередньо користувачами послуг.

Модель обслуговування для такого випадку відображається у вигляді нижченаведеної послідовності одиничних векторів.

1. Користувач послуги у разі виявлення ознак порушення умов сервісної угоди надсилає через інтерфейс із покупцями послуг відповідне повідомлення, в якому він у доступній для нього формі характеризує виявлені ним ознаки порушення.

2. **ІП1** – потік від користувачів послуг з виявленими ними ознаками порушень діючих сервісних угод.

3. Отримувач даних ІП1 – **служба організаційної підтримки надання послуг (С4).** Ці дані фіксуються службою С4, оброблюються на предмет їхньої легітимності і спрямовуються потоком ІП2 на адресу служби С9.

4. **ІП2** – потік із виявленими ознаками порушень діючих сервісних угод, що надсилаються службою С4 на адресу служби С9.

5. Отримувач даних потоку ІП2 – **служба розв'язання проблем в наданні послуг (С9).**

Отримавши дані ІП2, а також, можливо, самостійно виявивши порушення сервісної угоди на основі повідомлень від служби С14 (див. підрозділ 2.3.6.1), служба С9 намагається власними силами вирішити проблему і відновити надання послуг відповідно до умов порушеної сервісної угоди.

В процесі вирішення проблеми служба С9 взаємодіє із службою С10, якщо проблема пов'язана із некоректною роботою механізмів *QoS*. Потоки **ІП3** та **ІП4** таку взаємодію відображають.

В процесі вирішення проблеми служба С9 взаємодіє із службою С15, якщо проблема має комплексний характер. Потоки ІП5 та ІП6 таку взаємодію відображають.

6. **ІП 5** - потік із специфікаціями змін, які необхідно здійснити у мережній інфраструктурі, щоб відновити надання послуг у рамках умов порушеної сервісної угоди.

7. Отримувач даних ІП5 – **служба техобслуговування та ремонту засобів мережі (С15).** Ця служба здійснює зміни в

мережній інфраструктурі відповідно до отриманих через потік ІП5 специфікацій служби С9.

8. **ІП6** – потік із повідомленнями про виконані зміни у мережній інфраструктурі, які служба С15 надсилає на адресу служби С9.

9. **ІП7** – потік із інформацією щодо виконаних змін у мережній інфраструктурі, яку служба С15 надсилає на адресу служби С16.

10. Отримувач даних ІП7 – **служба управління даними (С16).** Дані потоку ІП7 щодо виконаних змін у мережній інфраструктурі (зокрема, дата проведених змін, значення усіх параметрів *SLA*, що зазнали змін, і т.ін.) оброблюються службою С16 і заносяться до відповідної бази даних. Оброблені дані щодо змін мережної інфраструктури, які виконані в результаті опрацювання виявленої проблеми, надсилаються також потоком ІП8 на адресу служби С10 з тим, щоб ця служба здійснила відповідні зміни у настроюванні параметрів служби *QoS*.

11. **ІП8** – потік із бази даних служби С16, які містять оброблені дані щодо виконаних змін у мережній інфраструктурі під час опрацювання виявлених проблем обслуговування.

12. Отримувач даних ІП8 – **служба управління механізмами QoS (С10)**. Ця служба на основі даних потоку ІП8 здійснює необхідне коригування параметрів настроювання механізмів *QoS*, оцінює поточні рівні надання послуг після коригувань і надсилає потоком ІП9 на адресу служби С9 інформацію про результати своїх дій, зокрема останній варіант набору значень параметрів *QoS* та досягнуті рівні надання послуг після виконаних коригувань.

13. **ІП9** – потік із повідомленнями про результати коригування параметрів QoS під час опрацювання проблем обслуговування, що надсилаються службою С10 на адресу служби С9.

14.Отримувач даних потоків ІП4 та ІП9 – **служба розв'язання проблем в наданні послуг (С9)**. Дані потоків ІП2, ІП4 та ІП9 мають бути достатніми для вирішення службою С9 будь-яких проблем із порушенням виконання умов діючих сервісних угод.

Якщо після тривалих намагань (термін котрих визначено у відповідних регламентуючих документах) не вдається успішно розв'язати виявлену проблему, то служба С9 інформує про це Дирекцію оператора електрозв'язку і звертається за допомогою до спеціалізованих автосорсінгових організацій або до постачальників

задіяного обладнання. **ІП 10** – відповідний потік заявок на адресу сторонніх організацій щодо допомоги у вирішенні виявлених проблем із підтримкою діючих сервісних угод.

Якщо факти порушень умов діючих сервісних угод виявлено, то у будь-якому випадку (успішного або неуспішного вирішення проблем із відновленням якості надання послуг) служба С9 потоком ІП11 інформує службу С4 про виявлені факти порушень умов або якості надання послуг, що зафіксовані у діючих *SLA*, і надає їй усю інформацію, яка є необхідною для звітування перед покупцями послуг про поточний стан обслуговування.

Якщо факти порушень умов діючих *SLA* за ознаками, які містилися у повідомленнях користувачів (потік ІП1), не підтвердилися, то служба С9 потоком ІП12 інформує про це службу С4 із наданням відповідної інформації, що підтверджує зроблений висновок про відсутність фактів порушень.

15. **ІП 13** – потік із даними, що містять результати опрацювання виявлених проблем, які призвели до порушень умов діючих сервісних угод: підтвердження фактів виникнення порушень, тривалість порушень, якісні та кількісні показники, що характеризують порушення – взагалі усе, що має відношення до визначення компенсацій покупцям послуг згідно з умовами порушених сервісних угод.

16. Отримувач даних ІП 13 – **служба визначення вартості послуг (С11)**. Ця служба на основі аналізу даних потоку ІП13 визначає характер і розмір преференцій та (або) компенсацій, на які має право розраховувати покупець послуг у зв'язку із порушенням сервісної угоди, яку цей покупець уклав із Дирекцією оператора електрозв'язку. Відповідні результати такого визначення служба С11 потоком ІП14 направляє до служби фінансового супроводження надання послуг С6.

17. **ІП 14** – потік із даними, що містять визначення характеру та розміри преференцій та (або) компенсацій за порушення умов сервісних угод.

18. Отримувач даних ІП14 – **служба фінансового супроводу надання послуг (С6)**. Ця служба на основі аналізу умов порушених сервісних угод і даних потоку ІП14 визначає конкретні розміри преференцій та (або) компенсацій у розрізі кожної

порушеної сервісної угоди. І з урахуванням зроблених преференцій та (або) компенсацій служба С6 здійснює відповідні взаєморозрахунки із покупцями послуг, що відображається в моделі обслуговування у вигляді потоку **ІП 15**. Крім того, служба С6 потоком ІП 16 інформує службу С4 щодо наданих преференцій та (або) компенсацій для подальшого сповіщення покупців послуг.

19. **ІП16** – потік із даними, що містять інформацію про надані преференції та (або) компенсації покупцям послуг, умови сервісних угод котрих було порушено з вини оператора електрозв'язку.

20. Отримувач даних потоків ІП11, ІП12 та ІП16 – **служба організаційної підтримки надання послуг (С4)**. Дані потоків ІП11, ІП12 та ІП16 містять вичерпну інформацію про стан обслуговування під час опрацювання проблем, що пов'язані із порушеннями умов діючих сервісних угод. Ця інформація оброблюється службою С4 згідно з умовами діючих сервісних угод. Зокрема, виготовляються усі види звітів про поточний стан обслуговування, які потоком **ІП 17** надаються покупцям послуг із визначеними термінами звітування.

15.8. Процедура підтримки узагальнених аналізів та оцінки якості обслуговування

Аналіз та оцінювання результатів надання послуги виконується з метою забезпечення вирішення таких двох задач:

1) аналіз якості надання послуги у розрізі окремої сервісної угоди;

2) інтегральна оцінка та аналіз ефективності функціонування служби QoS.

Аналіз якості надання послуги у розрізі окремої сервісної угоди передбачає оцінювання якості наданої послуги, ступеню задоволеності покупця наданою послугою, потенційних можливостей щодо удосконалення послуги та можливих змін у вимогах покупця до змісту послуги та процесу її надання.

Інтегральна оцінка та аналіз ефективності функціонування служби QoS передбачає визначення:

- інтегральних показників якості надання послуг у розрізі груп користувачів і в цілому по всій клієнтській базі, проблем у системі надання послуг, нових цілей в обслуговуванні та нових шляхів

щодо удосконалення системи надання послуг.

Організаційно-технологічна схема відображення процесів, що мають виконуватися технологічними підрозділами оператора МПД на стадії узагальнених аналізів та оцінки якості обслуговування (тобто, технологічний ланцюг потоків і процесів узагальнених аналізів та оцінки якості обслуговування), показана у вигляді графа на рис.15.7.

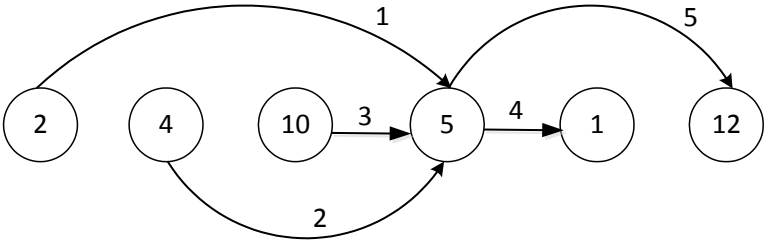


Рис. 15.7. Процедура підтримки узагальнених аналізів та оцінки якості обслуговування

Узагальнені аналізи та оцінки якості обслуговування виконуються в цілях планування розвитку МПД та системи надання послуг із використанням ресурсів цієї мережі. Цю аналітичну роботу забезпечує **служба аналізу та оцінки обслуговування (С5).** Вихідні дані для здійснення узагальнених аналізів та оцінок якості обслуговування надають служби С2, С4 та С10 потоками ІП1, ІП2 та ІП3 відповідно.

1. **ІП 1** – потік із узагальненими звітами **служби узгодження/укладання сервісних угод (С2)** щодо потреб та пропозицій кінцевих користувачів послуг відносно надання нових послуг або модернізації властивостей вже існуючих послуг.

2. **ІП 2** – потік із узагальненими рекомендаціями **служби організаційної підтримки надання послуг (С4)** щодо бажаних змін параметрів надаваних послуг або розробки нових послуг на основі аналізу втрат від надання преференцій та (або) компенсацій під час обслуговування.

3. **ІП 3** – потік із узагальненими рекомендаціями **служби управління механізмами QoS (С10)** щодо бажаних змін

параметрів надаваних послуг або розробки нових послуг на основі аналізу вад в управлінні механізмами *QoS* (наприклад, необгрунтованого надання пріоритетів одних класів трафіку перед іншими).

4. Отримувач даних потоків ІП1, ІП2 та ІП3 - **служба аналізу та оцінки обслуговування (С5)**. Ця служба безпосередньо здійснює узагальнені аналізи та оцінки якості обслуговування. Результати цих аналізів та оцінок направляються у **службу розвитку послуг (С1)** і у **службу планування та інжинірингу мережі (С12)** потоками **ІП4** та **ІП5** відповідно.

Визначення параметрів телекомунікаційного обладнання, що підтримує технологію ДОГС**.** Підтримка заданих у *SLA* показників якості ДОГС забезпечується шляхом адаптивного перерозподілу у реальному часі ресурсів ТКМ, зокрема швидкості передавання диференційованих потоків та виділених для них канальних смуг. Адаптивне керування параметрами каналу потребує однозначного визначення залежності між швидкістю передачі даних і показниками завадостійкості каналу. Бажано, щоб механізм перерозподілу мав змогу оптимальним чином налаштовувати параметри ТКО на підтримку ДОГС відповідно до прийнятого критерію оптимальності. Тому виникла потреба у використанні аналітичних математичних моделей (ММ) каналів передавання даних (КПД), що адекватно відображають реально існуючі функціональні взаємозв'язки між параметрами таких каналів. Параметрична оптимізація цих моделей виявить оптимальні залежності між параметрами ТКО і, отже, дозволить оптимальним чином побудувати механізм адаптивного перерозподілу телекомунікаційних ресурсів між клієнтськими застосуваннями.

Контрольні питання до п'ятнадцятої лекції

1. Які дані відносять до інформаційного забезпечення технологій обслуговування?
2. Поясніть структуру взаємозв'язків між службами та процесами обслуговування?
3. Визначить основні елементи мови відображення процедур обслуговування.

4. Поясніть процедуру підтримки створення та розвитку послуг.

5. Поясніть процедуру підтримки узагальнених аналізів та оцінки якості обслуговування.

Використана література:

1. Г.Ф. Конахович, В.М. Чуприн. Сети передачи пакетной коммутации.–К.: МК-Пресс, 2006. Розділ 6.

ЛЕКЦІЯ №16. ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ОБСЛУГОВУВАННЯ. СЛУЖБА QOS. ІНЖЕНЕРІЯ ПАКЕТНОГО ТРАФІКА

Розглядаються наступні питання:

Лекційне заняття

16.1. Модель служби підтримки якості обслуговування
16.2. Засоби служби підтримки якості на телекомунікаційному вузлі
16.3. Протоколи сигналізації служби підтримки якості
16.4. Алгоритми управління чергами
16.5. Механізми профілювання та формування трафіка

Самостійне заняття. Інженерія пакетного трафіка

16.6. Методи інженерії трафіка
16.7. Механізми реалізації визначених маршрутів
16.8. Інженерія трафіка різних класів

16.1. Модель служби підтримки якості обслуговування

З метою технічного забезпечення системи диференційованого обслуговування з гарантованим сервісом на базі ресурсів телекомунікаційних систем створюється та підтримується в актуальному стані **служба підтримки якості обслуговування** (служба *QoS*). Головне призначення цієї служби – забезпечувати пріоритезацію різних видів трафіка, необхідну смугу пропускання для них, керування величинами затримок та варіацій затримок протокольних блоків даних (*PDU*), а також зменшення відсотку втрат *PDU* під час передавання. Важливо також забезпечити пріоритетність обслуговування для одного або декількох потоків з одночасною можливістю передавання інших потоків.

Базова архітектура служби підтримки якості обслуговування надана на рис.16.1, де відображені три основні її складові:

1) засоби служби підтримки якості надання послуг на вузлі мережі, що здійснюють обробку потоків *PDU* (зокрема, потоків пакетів *IP*), які надходять до цього вузлу відповідно до умов сервісних угод;

2) засоби реалізації протоколів сигналізації служби підтримки якості обслуговування (тобто, протоколів *QoS*-сигналізації), за допомогою яких здійснюється координація роботи мережних елементів в процесі підтримки заданих рівнів послуг при

обслуговуванні “із кінця в кінець”;

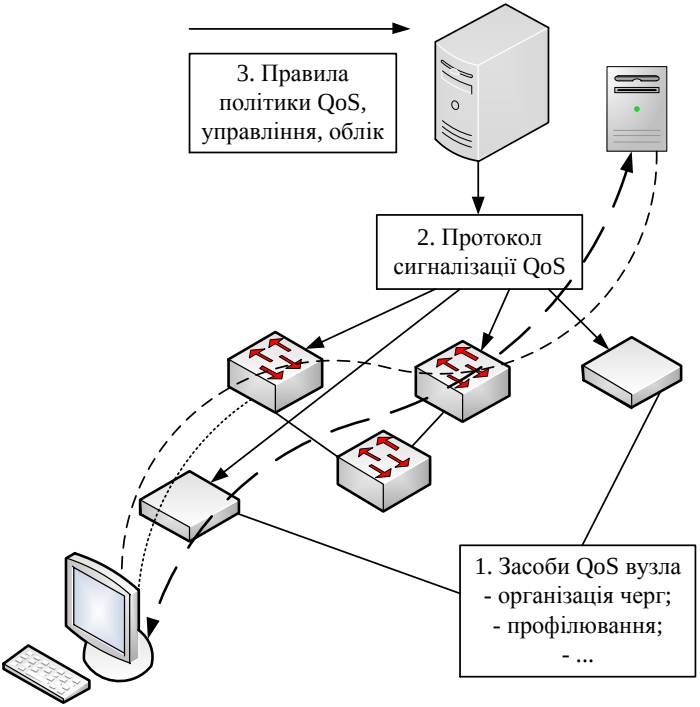


Рис.16.1. Базова архітектура служби підтримки якості надання послуг

3) засоби реалізації централізованих функцій підтримки прийнятих правил забезпечення якості обслуговування (у тому числі, функцій керування механізмами служби *Q₀S* та обліку її ресурсів), що призначені для цілеспрямованого впливу на мережні елементи з метою раціонального розподілу ресурсів мережі між різними видами трафіка відповідно до умов сервісних угод.

Служба *Q₀S* має розподілений характер, оскільки її елементи присутні практично на всіх мережних пристроях, що приймають участь в просуванні та обробці *PDU*. Координація роботи розосереджених елементів цієї служби здійснюється засобами задіяних протоколів *QoS*-сигналізації. Крім того, до

служби підтримки якості включаються засоби централізованого керування, за допомогою яких виконується узгоджене конфігурування механізмів *QoS* на кожному окремому пристрої мережі.

Централізовані функції керування служби підтримки якості не є необхідним елементом архітектури цієї служби, що наведена на рис.16.1. Але на глобальних мережах вони мають застосування, оскільки дозволяють мережним адміністраторам задавати саме ті рівні послуг для окремих користувачів або їхніх застосувань, що зафіксовані у сервісних угодах SLA. Зокрема, ці функції дозволяють адміністраторові створювати правила, згідно з якими мережні пристрої будуть здатними (на підставі заданих адміністратором наборів ознак) розпізнавати окремі типи трафіка і застосовувати до них визначені функції QoS.

16.2. Засоби служби підтримки якості на телекомунікаційному вузлі

Програмно-технічні засоби служби Q_0S ТЛК-вузлу безпосередньо впливають на процес просування *PDU* між увідними та вивідними інтерфейсами комутаторів та (або) маршрутизаторів. Вони визначають внесок кожного мережного пристрою в показники якості обслуговування.

Засоби служби *QOS* вузлу реалізують наступні типи виконавчих механізмів:

- механізми обслуговування черг;
- механізми кондиціонування трафіку;
- механізми керування буферами;
- механізми керування уводом;
- механізми контролю із зворотнім зв’язком.

Механізми обслуговування черг (Queuing and Scheduling) є необхідним елементом ТЛК-пристроїв, що працюють за принципом комутації протокольних блоків даних. Вони можуть підтримувати різні алгоритми обробки *PDU*, що потрапили в чергу, від найпростішого (типу *FIFO*) до досить складного, що у змозі підтримувати одночасну обробку кількох різних за характеристиками класів потоків (наприклад, алгоритм пріоритетного або зваженого обслуговування).

За звичайних умов у ТЛК-пристроях діє алгоритм обробки черг типу *FIFO*, але він є достатнім тільки для реалізації обслуговування, як кажуть, „із максимумом можливого”. Для підтримки диференційованого обслуговування з гарантованим сервісом використовуються більш складні механізми, що функціонують за алгоритмами пріоритетного або зваженого обслуговування.

Механізми кондиціонування трафіка (Traffic Conditioning) використовують в умовах швидко пульсуючого трафіку *PDU*. Ці механізми, зокрема, забезпечують “згладжування” пульсуючого потоку пакетів, що транспортується між вузлами пакетної мережі, таким чином, щоб швидкість “згладженого” потоку пакетів (тобто, пакетів, які після “згладжування” надходять до вузлу безпосередньо на обробку) залишалася трохи меншою, ніж максимально можлива швидкість обробки цього потоку засобами вузлу.

Забезпечення потрібної якості обслуговування завжди означає створення таких умов, коли припустима швидкість обробки *PDU* на вузлі узгоджується, тим чи іншим чином, зі швидкістю їхнього надходження до цього вузлу. Якщо пульсації потоку не призводять до виникнень ситуацій, коли швидкість надходження *PDU* до увідного порту вузла стає більше швидкості його просування через вузол, то реалізація механізмів кондиціонування є недоцільною. Але в багатьох інших випадках швидкість надходження *PDU* до вузлу на певних проміжках часу стає більшою, ніж швидкість їхнього просування через вузол. Як наслідок, виникають черги протокольних блоків даних, які за певних умов можуть перевищувати розмір пам’яті буферного портового пристрою на вузлі, що призведе до втрат пакетів. Механізми кондиціювання розраховані на роботу саме в ці періоди трафікових перенавантажень. Вони “згладжують” пікові значення пульсацій трафіка, але за рахунок збільшення затримки пакетів в чергах. Зрозуміло, що затримки від чекання в чергах повинні укладатися в параметри потоку, що зафіксовані в умовах *SLA*.

Механізм кондиціонування потоку *PDU* за звичайних умов реалізується шляхом виконання наведених нижче функцій.

1) ***Функція класифікації трафіка***, тобто функція

відокремлення із загального потоку різнорідних *PDU*, що надходять до вузла, такої послідовності протокольних блоків даних, до котрих пред'являються однакові вимоги щодо якості обслуговування. Класифікація може виконуватися на основі формальних ознак *PDU*, таких як адреса відправника та/або призначення, ідентифікатори застосувань, значення пріоритету блоку, значення мітки потоку тощо.

2) ***Функція профілювання трафіка на основі визначених правил*** - це конкатенація двох функцій: ***функції перевірки відповідності*** параметрів потоку *PDU,* що надходять до вузла, параметрам його профілю, що зафіксований у *SLA*, та ***функції обробки*** потоку *PDU* (вигляд якої залежить від результату перевірки функції відповідності).

Набір параметрів *QoS*, що характеризує певний потік *PDU,* часто називають профілем цього потоку. Для перевірки відповідності вхідного потоку заданому профілеві механізм кондиціонування здійснює виміри параметрів потоку. У разі порушення параметрів профілю, що виявляється за результатами перевірки відповідності (наприклад, перевищення тривалості пульсації або середньої швидкості), реалізується одна із трьох можливих функцій обробки потоку: формування трафіка, відкидання окремих блоків із потоку або маркування *PDU* цього потоку.

3) ***Функція формування трафіку (Traffic shaping)*** – різновид функції профілювання трафіка з метою придання йому потрібної тимчасової «форми». В основному, за допомогою даної функції прагнуть згладити пульсації потоку пакетів *IP,* щоб вихід пакетів із пристрою обробки був більш рівномірним, чим вхід. Таке згладжування пульсацій буде зменшувати можливі черги в мережних пристроях, що будуть обробляти потік далі за маршрутом. Його також доцільно використовувати для відновлення часових співвідношень між окремими застосуваннями, що працюють із рівномірними потоками (наприклад, між потоками мовних застосувань).

4) ***Функція обмеження трафіка*** (відкидання пакетів потоку, *Traffic policing*). Реалізація цієї функції не потребує буферизації даних за умов, коли потоки користувачів порушують умови

сервісних угод. Відкидання певної частки пакетів знижує інтенсивність потоку і приводить його параметри у відповідність із зазначеними у профілі.

5) ***Функція маркування пакетів потоку***. Маркування пакетів без відкидання потрібне для того, щоб не втратити пакети – "порушники", а обслужити їх (на даному вузлі або у наступному уздовж маршруту транспортування), але з рівнем якості, що, безумовно, буде нижчим за той, що зазначений у профілі потоку (наприклад, буде збільшено значення затримки тощо).

Механізми керування буферами (*Buffer Management*) розподіляють мережні буферні пристрої між даними користувачів. В залежності від ступеню заповнення пам'яті цих пристроїв (а також від характеристик потоків пакетів із даними різних типів, що надходять через вхідні інтерфейси) пакети або знищуються або приймаються до "попередніх" черг на уводах буферів, щоб потім, після чекання у буферах, бути розподіленими за типами черг, які створюються на виводах буферів.

Найбільш відомі механізми керування буферами – **механізм випадкового раннього виявлення переповнення (*RED*)** та його модифікація, що враховує пріоритетність трафіка – **механізм зваженого випадкового раннього виявлення переповнення (*WRED*)**. Принцип їхнього функціонування полягає в наступному: як тільки інформаційний потік перевищує визначений ліміт буферного простору вивідного інтерфейсу, ймовірність знищення його пакетів підвищується. Таким чином здійснюється протидія можливому захопленню смуги пропускання мережного обладнання тими потоками, що не реагують на перенавантаження.

У багатьох випадках механізми керування буферами роблять чутливими до сигналів від протоколів більш високого рівня. Зокрема чутливими до сигналів, що цими протоколами генеруються в моменти, коли вони виявляють підвищену інтенсивність втрачених пакетів.

Механізми керування уводом (*Admission Control*) забезпечують можливість безпосереднього контролю характеристик трафіка, його класифікації і активного впливу на

трафік увідного інтерфейсу з метою недопущення перенавантажень елементів мережного обладнання.

Механізми обмеження трафіка і керування буферами не дозволяють активно впливати на джерела небажаних потоків пакетів, котрі за певних обставин можуть створювати ситуацію постійних перенавантажень на мережі. Тому в таких випадках доцільно використовувати механізми керування уводом, за допомогою яких паразитні потоки у мережі знищуються.

Основний механізм реалізації керування уводом – **фільтрація трафіка**. Фільтрація може базуватися на *IP*-адресах, адресах *TCP*- або *UDP*- портів і т. ін. Потоки, котрі виявляються узгодженими із встановленими фільтрами, пропускаються через увідний інтерфейс, а всі інші – знищуються.

Механізми контролю із зворотнім зв'язком (*Feedback Control*) використовують зворотній зв'язок між вузлами мережі для розповсюдження інформації щодо стану перенавантажень. Зворотній зв'язок може здійснюватися за принципом "із кінця в кінець" або "крок за кроком" і виконуватися на будь-якому протокольному рівні.

На різних ділянках мережної інфраструктури використовуються різні механізми боротьби з перенавантаженнями та підтримки рівнів надання послуг.

На вузлах доступу до магістральної мережі, як правило, здійснюється обмеження трафіка, організація та обробка черг, а також керування буферами. На проміжних вузлах магістральної мережі використання вищезазначених механізмів не є обов'язковим.

На вузлах мереж абонентського доступу, особливо там, де здійснюється надання послуг за диференційованою системою з гарантованим сервісом, використання механізмів кондиціювання трафіку є обов'язковим. Зокрема, на цих вузлах мають бути задіяні механізми керування уводом, класифікації та формування трафіка, організації та обробки черг, керування буферами. На термінальних вузлах в необхідних випадках доцільно здійснювати керування із зворотнім зв'язком "із кінця в кінець".

16.3. Протоколи сигналізації служби підтримки якості

Протоколи сигналізації служби підтримки якості потрібні для координації роботи механізмів *QoS*, функціонуючих у вузлах мережі впродовж усього шляху проходження потоку (див. рис.16.1). Наприклад, за допомогою засобів сигналізації забезпечується можливість для окремого застосування зарезервувати необхідну йому середню пропускну здатність уздовж усього маршруту проходження пакетів (для мереж *IP* цю функцію підтримує протокол *RSVP*).

Один із найбільш розповсюджених засобів сигналізації — маркування пакета ознакою, що несе інформацію про рівень обслуговування, який є необхідним для його обробки. Зазвичай для цього використовується поле пріоритету, що існує у форматах багатьох протоколів. У цьому разі пакет, просуваючись від пристрою до пристрою, переносить уздовж шляху проходження свої вимоги до якості обслуговування, але у досить узагальненій формі — тому що поле пріоритету має усього кілька можливих значень. Це означає, що якість обслуговування за допомогою такого засобу сигналізації може надаватися диференційовано лише небагатьом агрегованим потокам.

Засоби сигналізації *QoS* встановлюються як на магістральних мережах, так і на мережах абонентського доступу. Але в багатьох випадках координацію механізмів *QoS* здійснюють не на усьому шляху проходження потоку, а тільки в межах окремих мереж абонентського доступу. Наприклад, маршрутизатор абонентського доступу на стороні постачальника послуг інсталюється на виконання лише класифікації трафіка та здійснення функції резервування певному потокові визначеної величини пропускної здатності транспортного каналу. Це, звичайно, не сприяє диференційованості у підтримці якості обслуговування у розрізі окремих застосувань клієнтів мережі, але спрощує вимоги до реалізації засобів підтримки якості.

На мережах передачі даних (МПД) загального користування в залежності від конкретних умов надання послуг використовуються як централізована, так і децентралізована системи керування засобами служби підтримки якості. Централізовані системи керування засобами *QoS* іноді називають **службами *QoS*,**

базованими на політиці (policy-based *QoS*).

У певних випадках на мережах абонентського доступу правила політики підтримки якості конфігуруються і зберігаються окремо в кожному активному мережному пристрої. Однак це вимагає від адміністратора такої мережі значних зусиль щодо координації засобів *QoS* і, як наслідок, породжує підвищену кількість помилок, що може призвести до неузгодженої роботи мережних пристроїв.

На магістральних МПД використовується виключно централізована система керування засобами служби підтримки якості (яка і наведена на рис.16.1). В цьому випадку формуються єдині правила політики керування, узгоджені щодо всіх пристроїв мережі, які зберігаються на центральному сервері політики (або в цілях підвищення надійності – на кількох серверах, що реплікують базу даних політики). Адміністратор конфігурує правила політики в одній точці, що знижує витрати його праці і кількість помилок. Потім за допомогою спеціального протоколу *QoS*-сигналізації ці правила поширюються на всі мережні пристрої, котрі мають підтримувати необхідні рівні послуг. Ці мережні пристрої застосовують визначену політику керування засобами служби *QoS*, зокрема для кондиціонування трафіка або керування чергами відповідно до умов сервісних угод.

В багатьох випадках правила політики формуються не тільки для керування засобами *QoS*, але і для координації мережних пристроїв при виконанні інших функцій, наприклад функцій захисту інформації. Тому централізована система керування засобами *QoS* включається у склад централізованої системи підтримки визначеної політики забезпечення правил функціонування мережі і базується на загальній довідковій службі мережі (*Directory Service*), що зберігає всі необхідні для її функціонування облікові дані.

У розрізі прийнятої моделі служби підтримки якості надання послуг функції *QoS*-сигналізації виконує більшість конкретних протоколів підтримки *QoS*, таких як *RSVP*, *DiffServ* (у мережах *TCP/IP*) або протоколів служб *CBR, VBR* і *ABR* (у мережах *ATM*).

16.4. Алгоритми управління чергами

*16.4.1. Умови виникнення черг***.** На рівні окремих мережних

елементів підтримка якості надання послуг заснована на використанні певних алгоритмів обробки черг пакетів. Механізми реалізації таких алгоритмів використовуються в будь-якому мережному пристрої, що працює на основі механізму комутації пакетів, — у маршрутизаторі, у комутаторі локальної або глобальної мережі, в обладнанні кінцевого вузлу і т.ін. Виключення складають тільки повторювачі, які пакетів не розрізняють, а працюють на рівні потоків бітів.

Обробка пакетів у чергах є потрібною під час тимчасових перенавантажень мережних пристроїв, коли вони внаслідок обмеженості пропускної здатності не в змозі просувати через себе пакети у тому темпі, у якому вони надходять до їхніх увідних портів. Якщо причиною перенавантаження є процесорний блок мережного пристрою, то для тимчасового збереження неопрацьованих пакетів використовується вхідна черга, тобто черга, що зв'язана з увідним інтерфейсом. У тім же випадку, коли причина перенавантаження полягає в обмеженій швидкості вивідного інтерфейсу (ця швидкість завжди обмежена теоретично максимальною швидкістю підтримуваного протоколу), то пакети тимчасово зберігаються у вихідній черзі.

Головним за ступенем впливу на виникнення черг фактором є **коефіцієнт навантаження пристрою (*utilization*)** — відношення середньої сумарної інтенсивності вхідного трафіка пристрою до середньої сумарної інтенсивності вихідного трафіка, що вимірюються на певним чином вибраному інтервалі усереднення.

Якщо на інтервалі усереднення інтенсивність вхідного трафіка буде вищою, ніж інтенсивність просування пакетів через пристрій на вивідний інтерфейс, то коефіцієнт навантаження пристрою буде більшим за одиницю. В цьому випадку на увідному інтерфейсі пристрою (точніше, у буферній пам’яті увідного порту цього пристрою) виникне черга, і її довжина за таких умов прагнула б до нескінченності, якби не працювали б механізми обробки виникаючих черг.

Якщо коефіцієнт навантаження менше за одиницю і до увідного порту пристрою надходить рівномірний потік пакетів, то в такій ситуації черг не виникне зовсім. Але якщо у межах інтервалів усереднення існує певна варіація в надходженні пакетів у пристрій,

то за таких умов можуть виникати черги навіть при коефіцієнті навантаження, меншим за одиницю. Більш того, ці черги можуть мати досить значну середню довжину. Чим більша варіація, тим більша середня довжина черги. Тому варіація інтервалів надходження пакетів є важливим, поряд з коефіцієнтом навантаження, фактором, що впливає на поведінку черг.

Пульсуючий характер багатьох типів трафіка, коли коефіцієнт пульсацій на певних проміжках часу дорівнює 100:1 і більше, обумовлює виникнення суттєвих за розміром черг. Практика експлуатації мереж показує, що навіть при значеннях коефіцієнта навантаження сегмента мережі на рівні 0,5 (наприклад, у локальних мережах Ethernet) затримки доступу до мережі бувають значними, що змушує використовувати ці мережі з коефіцієнтом навантаження сегмента не більш 0,3.

Наслідком виникнення черг є погіршення якості обслуговування трафіка. Зокрема, виникають затримки в процесі транспортування пакетів, що мають, до того ж, непостійний характер, тобто спостерігаються варіації затримок. Під час тривалих пульсацій потоку пакетів черги можуть зростати настільки, що пакети не вміщуються в буферну пам'ять мережних пристроїв і губляться.

Щоб зменшити (а в ідеалі, нейтралізувати) негативний вплив наведених вище факторів на якість надання послуг, служба підтримки якості використовує наступні методи:

1) попереднє резервування частки пропускної здатності обладнання для потоків з відомими параметрами *QoS* (наприклад, з відомими значеннями середньої інтенсивності потоку і його пульсації);

2) примусове профілювання вхідного трафіка, що, в деяких випадках, дозволяє підтримувати коефіцієнт навантаження пристрою на потрібному рівні;

3) використання складних алгоритмів керування чергами.

Найчастіше у маршрутизаторах і комутаторах застосовуються наступні алгоритми обробки черг:

- традиційний алгоритм *FIFO*;
- пріоритетне обслуговування (*Priority Queing*);
- зважене обслуговування (*Weighted Queing, WQ*);
- зважене справедливе обслуговування (*Weighted Fair Queuing,*

WFQ).

Кожен із вищеназваних алгоритмів має свою сферу використання. Можливо і комбіноване застосування цих алгоритмів.

*16.4.2. Традиційний алгоритм FIFO***.** Принцип традиційного алгоритму *FIFO* полягає в тому, що під час пікових значень інтенсивності пульсуючого трафіка пакети надсилаються до черг у пристроях буферної пам'яті портів, а під час помірних значень інтенсивності трафіка вони передаються на вивідні порти обладнання безпосередньо у тому порядку, в якому вони надходять до увідних портів, тобто за принципом «першим прийшов — першим пішов» (*First In — First Out, FIFO*). В усіх пристроях з комутацією пакетів *FIFO* – це вбудований алгоритм обробки черг, що автоматично реалізується без втручання адміністраторів мережі. Його перевага – в простоті реалізації, а також у відсутності потреб щодо відповідного конфігурування обладнання. Більшість маршрутизаторів оптимізовані для роботи саме з цим типом черги. Коли параметри мережного обладнання збалансовані із характеристиками більш/менш рівномірних потоків пакетів із короткочасними сплесками трафіка (або існує достатній резерв пропускної здатності цього обладнання), то організація черг необхідна лише для того, щоб запобігти знищенню пакетів під час таких сплесків. За таких умов організація черги *FIFO* може бути ефективною, оскільки глибина черг, найбільш ймовірно, буде невеликою за розміром, а середня затримка пакетів у черзі буде незначною у порівнянні з часом транспортування пакетів „із кінця в кінець". Але коли трафікове навантаження у мережі збільшується, навіть короткочасні сплески збільшують розміри черги, і в певний момент після повного наповнення черги пакети почнуть знищуватися, що веде до деградації якості надання послуг. Крім того, алгоритм *FIFO* з точки зору якості обслуговування має суттєвий недолік — неможливість диференційованої обробки пакетів різних потоків. Усі пакети згідно умов реалізації цього алгоритму оброблюються у загальній черзі на рівних підставах — як пакети чутливого до затримок голосового трафіка, так і пакети нечутливого до затримок, але вельми інтенсивного трафіка резервного копіювання. За таких умов "рівноправності",

наприклад, тривалі пульсації трафіка резервного копіювання можуть надовго затримати пакети голосового трафіка, що неприпустимо.

Тим не менш, можливість створення черг за алгоритмом *FIFO* є необхідною передумовою для нормальної роботи мережних пристроїв, хоч він і не здатний забезпечити підтримку механізмам служб *QoS*.

16.4.3. Пріоритетне обслуговування. Алгоритми пріоритетної обробки черг (*Priority Queuing*) використовуються, коли у суміші потоків пакетів, що транспортуються через канал із даними різнорідних прикладних застосувань, необхідно забезпечити перевагу в обробці одних застосувань над іншими. Зокрема, використовуються ці алгоритми для забезпечення переваги в обробці одного класу трафіка в порівнянні з іншими класами.

Механізм пріоритетної обробки трафіка заснований на поділі усього можливого за даних умов мережного трафіка на невелику кількість класів і призначенні кожному класові числової ознаки — пріоритету. Поділ на класи (класифікація) може здійснюватися різноманітними способами. Правила класифікації пакетів на пріоритетні класи являють собою частину політики керування мережею.

Спосіб класифікації, як правило, не пов'язується безпосередньо з роботою алгоритмів обслуговування на основі пріоритетів — головне, щоб усі пакети, що надходять у чергу, мали ознаки пріоритетів. Пакети можуть розбиватися на пріоритетні класи відповідно до типу мережного протоколу — наприклад, *IP*, *IPX* або *DECnet* (зрозуміло, що такий спосіб класифікації підходить тільки для пристроїв, що працюють на канальному рівні згідно семирівневої моделі *OSI ISO*), або на підставі адрес призначення і відправника, або ідентифікатора застосувань, або будь-яких інших комбінацій ознак, що містяться у полях форматів задіяних мережних протоколів.

Точка класифікації трафіка може розміщатися як у самому пристрої, так і поза ним. Доцільно здійснювати класифікацію трафіка в одному або у кількох пристроях, що розташовані на інтерфейсах “користувач – постачальник послуг”, наприклад у маршрутизаторах абонентського доступу або на стороні покупців

послуг (зокрема, у комутаторах корпоративної мережі, до яких підключаються комп'ютери користувачів). Подібний варіант класифікації вимагає наявності у форматі пакетів спеціального поля для ознаки пріоритету, щоб ним могли скористатися інші мережні пристрої, що обробляють трафік після пристрою, що здійснює функцію класифікації. Таке поле існує у специфікаціях заголовків багатьох мережних протоколів. У тих же випадках, коли специфікація протоколу не передбачає існування спеціального поля пріоритету, в цілях класифікації трафіка використовується додатковий протокол, що вводить новий заголовок з таким полем. Так, наприклад, у форматах більшості варіантів протоколу *Ethernet* поля пріоритету не існує. Тому у випадках їхнього використання в цілях забезпечення можливості класифікації трафіка застосовують спеціально розроблений протокол за специфікацією *IEEE 802.1Q/p,* що має додаткове трьохбітне поле пріоритету.

Пріоритети можуть призначатися не тільки комутатором або маршрутизатором, але і прикладним застосуванням у вузлі-відправнику.

Необхідно також враховувати, що в процесі транспортування пакету будь-який мережний пристрій, через який має просуватися цей пакет, може “не погодитися” з призначеним в іншій точці мережі пріоритетом даному пакетові. У цьому випадку такий мережний пристрій перепише значення пріоритету відповідно до своєї локальної політики. Тому, щоб унеможливити виникнення подібних ситуацій, доцільно впроваджувати засоби підтримки централізованої політики служби *QoS*, що забезпечують скоординовану роботу елементів мережі.

Механізм пріоритетної обробки трафіка функціонує наступним чином. Відповідно до кількості пріоритетних класів на виході буферної пам’яті мережного пристрою створюється кілька черг. Пакет, що надійшов під час перенавантажень, спрямовується до черги, що відповідає його пріоритетному класові.

На рис.16.2 наведено приклад використання чотирьох пріоритетних черг: з високим, середнім, нормальним і низьким пріоритетом. Пріоритети черг визначають абсолютний характер переваги під час обробки пакетів, тобто, поки з більш пріоритетної черги не будуть оброблені усі наявні пакети, пристрій не повинен

переходити до обробки наступної, менш пріоритетної черги.

Тому пакети, що мають середній пріоритет, завжди обробляються тільки тоді, коли черга пакетів з високим пріоритетом - порожня. Відповідно, пакети з низьким пріоритетом обробляються тільки тоді, коли порожні усі більш пріоритетні черги: з високим, середнім і нормальним пріоритетами. Фізично пакети, що очікують обслуговування в чергах, розміщуються у буферній пам'яті портів мережного пристрою. Ця буферна пам'ять має кінцевий розмір. Максимальна довжина буфера визначає максимальну кількість пакетів, що можуть зберігатися в черзі даного пріоритету. Тому під час мережного адміністрування необхідно враховувати можливість переповнення черг і приймати відповідні дії.

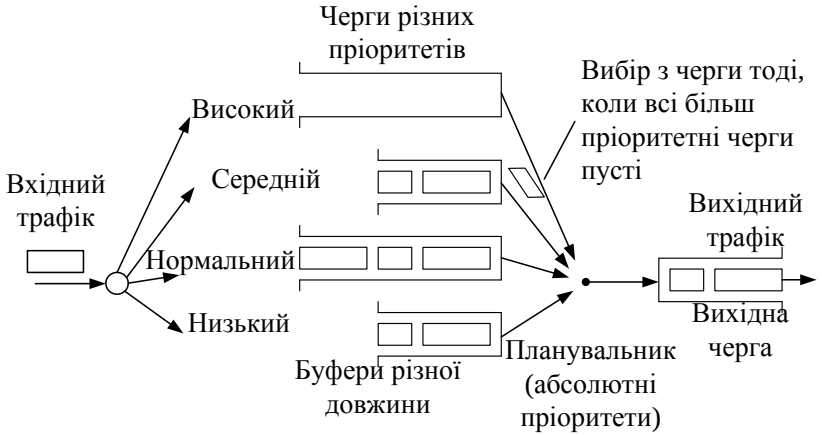


Рис.16.2. Пріоритетне обслуговування черг протокольних блоків даних

На практиці "за замовчуванням" усім пріоритетним чергам приділяються однакові за розміром буфери. Але диференційоване обслуговування передбачає використання механізму створення буферів з індивідуальним для кожної черги розміром пам'яті.

Оптимальний розмір буфера визначається в ідеальному випадку таким чином, щоб його вистачало з деяким запасом для збереження черги середньостатистичної довжини. Однак визначити цей розмір, хоча б приблизно, в реальних умовах досить складно, оскільки характеристики пульсацій трафіка

обумовлюються багатьма, складно передбачуваними, факторами. Тому потрібно постійне і тривале спостереження за роботою мережі. У загальному випадку, розмір буферної пам'яті вибирають, виходячи із таких суб'єктивних міркувань: чим вище цінність трафіка у застосуваннях користувачів, а також чим більше його інтенсивність і пульсації, тим більший розмір буфера потрібно виділити для цього трафіка. У прикладі, наведеному на рис.16.2, для трафіка вищого і нормального пріоритетів обрані великі розміри буферної пам'яті, а для інших двох класів — менші розміри. Мотиви прийнятого рішення щодо вищого пріоритету – очевидні. Щодо трафіка нормального пріоритету, то висунуто припущення, що він має високу інтенсивність і значний коефіцієнт пульсацій.

Пріоритетне обслуговування черг забезпечує високу якість обслуговування для пакетів із черги з найвищим пріоритетом. Якщо середня інтенсивність їхнього надходження у пристрій не перевершує пропускної здатності вихідного інтерфейсу (і продуктивності внутрішніх блоків самого пристрою, що просувають пакети), то пакети вищого пріоритету завжди одержують ту пропускну здатність, яка їм потрібна. Рівень затримок високо пріоритетних пакетів також мінімальний. Однак він не нульовий і залежить, в основному, від характеристик потоку цих пакетів — чим вище пульсації потоку і його інтенсивність, тим вище рівень затримок. Трафік всіх інших пріоритетних класів майже прозорий для пакетів вищого пріоритету. Слово «майже» відноситься до ситуації, коли високо пріоритетний пакет повинен чекати завершення обслуговування низько пріоритетного пакета, тому що його прихід збігся за часом з початком просування низько пріоритетного пакета на вихідний інтерфейс.

Якість обслуговування пакетів інших класів за схемою пріоритетного обслуговування завжди буде нижчою порівняно з якістю обслуговування пакетів найвищого пріоритету. Рівень зниження якості заздалегідь передбачити досить важко. Це зниження може бути істотним, якщо, наприклад, високо пріоритетний трафік починає передавати дані з високою інтенсивністю. Зокрема, треба мати на увазі, якщо коефіцієнт навантаження пристрою обумовлюється трафіком вищого

пріоритетного класу і наближається в якийсь період часу до одиниці, то трафік інших класів на цей час практично буде заморожений. Тобто виникає проблема монополізації ресурсів обслуговування високо пріоритетним трафіком. Саме через це пріоритетне обслуговування на практиці застосовується, в основному, тоді, коли в мережі існує лише один високо пріоритетний клас трафіка, хай і чутливий до затримок, але з невеликою інтенсивністю. За таких умов пріоритетне обслуговування цього класу буде у припустимій мірі впливати на погіршення якості обслуговування трафіка інших класів. Наприклад, за найвищим пріоритетом є можливим обслуговувати голосовий трафік. Він, хоч і чутливий до затримок, але не є інтенсивним - його інтенсивність звичайно не перевищує 8 - 64 кбіт/с.

На жаль, сфера використання пріоритетного обслуговування у чистому вигляді є досить вузькою, оскільки не охоплює багато інших ситуацій, що мають місце на практиці. Наприклад, відеотрафік також потребує пріоритетного обслуговування, але має більш високу інтенсивність, що не дозволяє його пріоритезувати без надання деяких гарантій сумісним з ним низько пріоритетним трафікам.

16.4.4. Зважене обслуговування. Алгоритм зважених черг (Weighted Queuing) розроблений для того, щоб усунути проблему монополізації обслуговування високо пріоритетним трафіком, тобто щоб можна було надавати всім класам трафіка попередньо визначений мінімум пропускної здатності мережних ресурсів або гарантувати виконання певних вимог щодо затримок. Згідно цього алгоритму кожному класу трафіка приписується певна вага, а під вагою класу розуміється відсоток пропускної здатності, що надається цьому класу, відносно повної пропускної здатності вихідного інтерфейсу. Вага класам трафіка може призначатися адміністратором мережі.

Зважене обслуговування також передбачає поділ трафіка на кілька класів, і для кожного класу також створюється окрема черга пакетів. Але в цьому випадку з кожною чергою зв'язується не її пріоритет, а відсоток пропускної здатності вихідного інтерфейсу, надання котрого гарантується даному класові трафіка

у разі перенавантаження цього інтерфейсу.

У прикладі, наведеному на рис.16.3, пристрій підтримує 5 окремих черг для кожного із п'яти класів трафіка. Цим чергам на випадок перенавантажень виділяється відповідно 10%, 10%, 30%, 20% і 30% пропускної здатності вихідного інтерфейсу. При цьому реалізується наступний механізм надання необхідної ваги утвореним чергам: реалізується процедура послідовного і циклічного обслуговування черг, а в кожнім циклі обслуговування з кожної черги на вихідний інтерфейс спрямовується така кількість пакетів (у пропорції до кількості пакетів з інших черг), що відповідає вазі даної черги. Наприклад, якщо цикл перегляду черг дорівнює одній секунді, а швидкість вихідного інтерфейсу дорівнює *100 Мбіт/с*, то у кожнім циклі з першої черги вибирається *10 Мбіт* даних, із другої — теж *10 Мбіт*, із третьої — *30 Мбіт*, з четвертої — *20 Мбіт*, а з п'ятої — *30 Мбіт*.

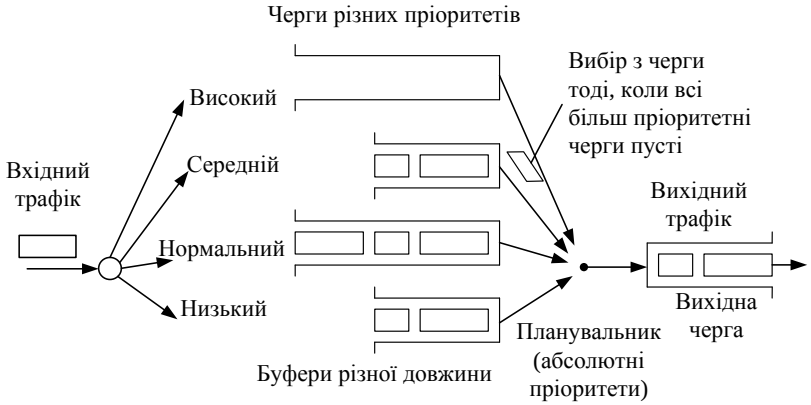


Рис.16.3. Зважене обслуговування черг у пакетній мережі

Як результат, кожному класові трафіка дістається гарантований мінімум пропускної здатності, що в багатьох випадках є більш бажаним результатом, ніж неконтрольоване придушення низько пріоритетних класів трафіка з боку трафіка з високим пріоритетом.

У загальному випадку, зважене обслуговування призводить до більш високих значень затримок пакетів і їх варіацій у порівнянні з

пріоритетним обслуговуванням трафіка найбільш пріоритетного класу. Але для створення більш сприятливих умов обслуговування всіх класів трафіка зважене обслуговування часто буває більш прийнятним.

Якщо розглядати окремо будь-який клас трафіка при зваженому обслуговуванні, то виявляється, що на рівень затримок і варіації затримок в значній мірі впливає коефіцієнт навантаження трафіка даного класу. У цьому випадку коефіцієнт навантаження підраховується як відношення середньої інтенсивності вхідного трафіка даного класу до частки пропускної здатності вихідного інтерфейсу, яка виділена цьому класові відповідно до його ваги. Характер утворення черги цього класу і, відповідно, затримок тут виглядає приблизно так само, як і у випадку черги *FIFO* — чим менший коефіцієнт навантаження, тим менша середня довжина черги і тим менші затримки.

Зважене обслуговування передбачає можливість адміністраторам мережі призначати для різних класів черг різні розміри буферної пам'яті. Зменшення розмірів буферів для черг призведе до росту числа втрат пакетів під час перенавантажень, але через це зменшується час чекання для тих пакетів, що не були відкинуті і потрапили в чергу.

16.4.5. Зважене справедливе обслуговування. Зважене справедливе обслуговування (Weighted Fair Queuing, WFQ) — це комбінований алгоритм, що об'єднує пріоритетне обслуговування черг зі зваженим. Існує велика кількість різних реалізацій WFQ, котрі відрізняються способом призначення ваг і підтримкою різних режимів роботи.

Найбільш розповсюджена схема передбачає існування однієї особливої черги, що обслуговується за пріоритетною схемою. Ця черга призначена для системних та сигнальних повідомлень, а також, іноді, для передачі пакетів найбільш критичних або вимогливих застосувань. Передбачається, що її трафік має невисоку інтенсивність, так що значна частина пропускної здатності вихідного інтерфейсу залишається іншим класам трафіка. Черги інших класів трафіка за цією схемою обробляються послідовно згідно з алгоритмом зваженого обслуговування (див. рис.16.4). Адміністратор може задати вагу

кожного класу трафіка, тобто кількість пакетів з кожної черги, що мають спрямовуватися на вихідний інтерфейс на кожному циклі обробки черг.

Наведена нижче схема обробки черг пакетів пропонується для використання багатьма виробниками комунікаційного устаткування, якщо необхідно об'єднати пріоритетне і зважене обслуговування. Наприклад, за умов, коли існує один клас пріоритетного трафіка, пакети якого мають обслуговуватися в першу чергу. Обслуговування пакетів всіх інших класів повинно починатися тільки тоді, коли пріоритетна черга стає порожньою. При цьому пропонується здійснювати зважене обслуговування всіх інших з урахуванням заданого відсоткового відношення.

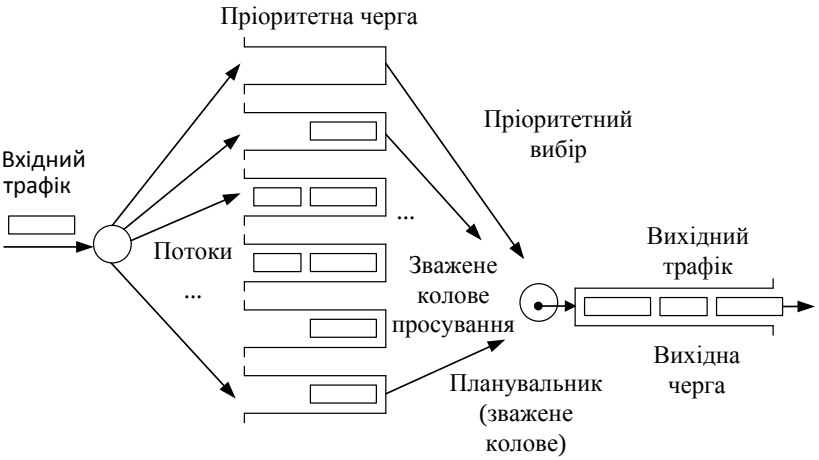


Рис.16.4. Зважене справедливе обслуговування черг у пакетній мережі

16.5. Механізми профілювання та формування трафіка

Служба *QoS* для профілювання і формування трафіка використовує нижченаведені алгоритми.

16.5.1 Алгоритм «дірявого цеберка». Алгоритм "дірявого цеберка" (*leaky bucket*, рос. – "дырявого ведра") розроблений для профілювання пульсуючого трафіка. Алгоритм дозволяє перевірити дотримання породжувачами трафіка узгоджених

значень середньої швидкості і пульсації.

Алгоритм моделює цеберко, знизу котрого зроблена дірка. Якщо дані втікають у цеберко швидше, ніж витікають, то цеберко в кінці кінців переповниться, і виникне ситуація, коли дані, що надходять, будуть відкидатися до тих пір, поки не з'явиться вільне місце для їхнього розміщення у цеберку. Для керування потоком даних використовується два параметри: середня швидкість V_c, тобто середня кількість пакетів у секунду, що "витікають" через дірку у цеберку і передаються в мережу; глибина цеберка S, тобто кількість пакетів, котрим дозволено накопичуватися у цеберку. Крім того, використовуються дві змінних стану: поточний реальний час t_p; віртуальний час $t_в$ (у секундах), що визначається через співвідношення середньої швидкості надходження пакетів та кількості вже накопичених у цеберку пакетів. Наприклад, якщо середня швидкість складає 100 пакетів у секунду, а у цеберку накопичено 1000 пакетів, то віртуальний час буде на 10 секунд перевищувати реальний час.

Згідно з алгоритмом "дірявого цеберка" кожний пакет, що надходить до увідного інтерфейсу, оброблюється за такими правилами (при цьому приймемо такі позначення: R – розмір пакета у байтах; V_n – поточна швидкість надходження пакетів) :

За умов, коли $t_в + R\ (\ V_n / V_c\ ) > \ t_p + S / V_c$, то пакет має бути знищений, а $t_в = max\ (t_в\ ,\ t_p\ )$; у протилежному випадку пакет слід помістити у цеберко, *а* $t_в = t_в + R\ (\ V_n / V_c\ )$.

Існує кілька варіантів реалізації цього алгоритму. Розглянемо варіант, що застосовується для контролю трафіка в мережах *frame relay*.

Процедура реалізації алгоритму передбачає можливість настроювання за наступними параметрами:

T — інтервал усереднення оцінок швидкості потоку пакетів;

CIR (Commited Information Rate) — узгоджена середня швидкість, яка повинна не перевищуватися трафіком на періоді усереднення ;

Bc — припустимий (фактично узгоджений) для передачі обсяг даних користувача, що відповідає узгодженій середній швидкості *CIR* і узгодженому інтервалові усереднення *T*, тобто $Bc = CIR\ x\ T$;

Be — дозволений для передавання додатковий обсяг даних, який

відповідно до умов сервісної угоди може перевищувати *Bc*, але цей обсяг даних буде оброблюватися за іншими правилами (як правило, з більш нижчим рівнем обслуговування).

Робота за алгоритмом полягає в наступному. Кожні *T* секунд здійснюється контроль трафіка. Виміряна середня швидкість трафіка на цьому проміжку часу, якщо користувач хоче мати пріоритетне обслуговування, повинна бути не більше за узгоджену швидкість *CIR*. Швидкість контролюється на основі підрахунку обсягу даних, що надійшли за період *T*. Якщо цей обсяг менше або дорівнює *Bc*, то це свідчить про те, що фактична швидкість трафіка була менше *Bc/T*, тобто менше *CIR*. На практиці трафік користувача може перевищувати узгоджену швидкість *CIR*. Перевищення трафіком узгодженого значення *Bc* на величину, що не є більшою за *Be*, за звичайних умов допускається. Кадри, що входять до складу *Be*, позначаються певною ознакою, але не відкидаються. Але якщо трафік, що надходить до комутатора, перевищує величину *Bc* + *Be*, то обладнання постачальника послуг може бути інстальоване таким чином, щоб відкидати такі кадри.

Механізм профілювання трафіка, що реалізується алгоритмом, заснований на використанні лічильника даних, котрі надходять на увідний інтерфейс комутатора від користувачів. Відлік здійснюється у байтах. Через кожні *T* секунд показник відліку лічильника або зменшується на величину *Bc*, або ж "обнулюється", якщо показник відліку лічильника в момент коригування показника виявляється меншим, ніж *Bc*.

Механізм функціонування за цим алгоритмом часто ілюструють у вигляді уявного «цеберка», з якої дискретно, кожні *T* секунд, "виливаються" дані в обсязі, що дорівнює мінімальному з чисел: *Bc* або поточне значення лічильника *C* (див. рис.16.5).

Усі кадри, дані яких не збільшили значення лічильника понад поріг *Bc*, пропускаються на вихідний інтерфейс комутатора з ознакою поля у форматі кадру *DE = 0*. Кадри з такою ознакою обробляються з найвищим пріоритетом. Кадри, дані яких привели до значення відліку лічильника, більшому за *Bc*, але меншому за *Bc* + *Be*, також пропускаються на вихідний інтерфейс комутатора, але з ознакою *DE = 1*. Такі кадри обслуговуються з меншим рівнем якості.

І, нарешті, кадри, що привели до значення відліку лічильника, більшому за *Bc+Be*, обслуговуються з найменшим пріоритетом або навіть відкидаються комутатором.

Одна з модифікацій алгоритму «дірявого цеберка» за назвою ***Generic Cell Rate Algorithm (GCRA)*** застосовується в мережах *ATM* для контролю наступних параметрів: пікової швидкості, середньої швидкості, варіації інтервалу прибуття чарунок і обсягу пульсації.

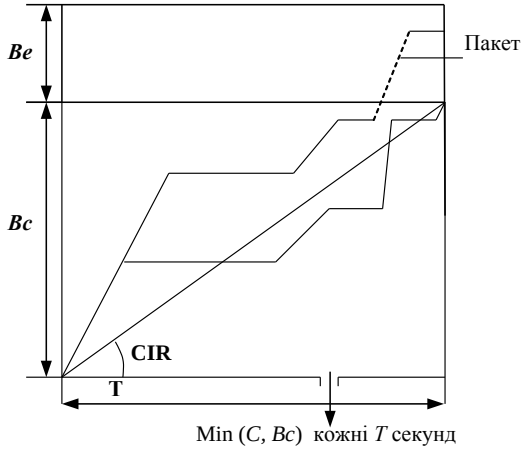


Рис.16.5. Профілювання трафіку за алгоритмом «дірявої цеберки»

*16.5.2. Алгоритм «цеберка жетонів»***.** Алгоритм **«цеберка жетонів»** (*Token Bucket*) застосовується як для профілювання, так і для формування трафіка.

Використовується цей алгоритм в цілях:

- забезпечення можливості пропуску пульсуючого трафіка без згладжування (але з обмеженням його інтенсивності зверху) за умов, коли відсутня конкуренція потоків за мережні ресурси (це сприяє більш ефективному використанню ресурсів мережі в таких умовах);

- зменшення нерівномірності просування пакетів, коли через значну пульсацію вони збиваються в щільні групи.

Робота алгоритму ілюструється на рис.16.6, де відображений сервер, який, поряд з іншим, здійснює функцію обмеження

інтенсивності увідного трафіка за алгоритмом «цеберка жетонів».

На увідному порту сервера створюється черга пакетів, а його внутрішні механізми моделюють так зване “цеберко” і генерують послідовність так званих жетонів, що спрямовуються в “цеберко”.

Під жетоном у даному випадку розуміється певний абстрактний об'єкт - носій «порції» інформації, що використовується для побудови моделі обслуговування трафіка. “Цеберка” має граничну місткість розміром у *b* байт, а довжина жетона складає *m* байт. Генератор жетонів заповнює “цеберко” із швидкістю *r* байт за секунду.

Параметр *r* регулюється адміністратором мережі і встановлюється таким, щоб швидкість надходження жетонів у “цеберко” дорівнювала узгодженій середній швидкості для трафіка, що формується. Тобто потік жетонів являє собою той ідеально усереднений трафік, до форми якого намагаються привести вхідний трафік.

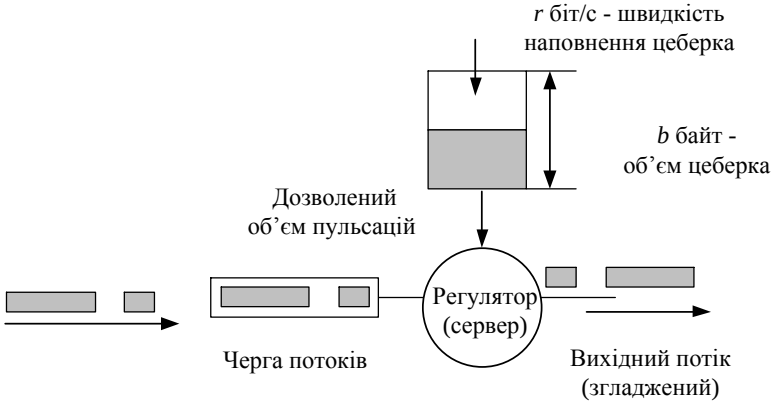


Рис.16.6. Формування трафіка за алгоритмом «цеберка жетонів»

Алгоритм функціонує наступним чином. Пакети надходять у систему і стають у чергу довжиною *K* байт. З виходу черги пакет забирається і просувається далі сервером тільки в той момент, коли «цеберко» заповнюється жетонами до рівня, не нижче за *M*

байт, де *M* — довжина пакета. Якщо ця умова виконується і пакет просувається на вихід, то в момент початку такого просування із «цеберка» викидається така кількість жетонів, яка за сумарною довжиною дорівнює *M* байтам (з точністю до *m* байт). Якщо ж цеберка заповнена недостатньо, то пакети з черги не вибираються, очікуючи надходження потрібного числа жетонів.

У такий спосіб досягається «поліпшення» трафіка: якщо в результаті пульсації в систему прийшла велика пачка пакетів, то навіть за цих умов із черги пакети виходять рівномірно - у темпі, що задається генератором жетонів.

Контрольні питання до шістнадцятої лекції

1. Надайте характеристику моделі служби підтримки якості обслуговування.
2. Яке призначення служби *QoS*?
3. Які основні складові служби *QoS*?
4. Які виконавчі механізми служби *QoS* Ви знаєте?
5. Надайте характеристику функції класифікації трафіка.
6. Надайте характеристику функції профілювання трафіка на основі визначених правил.
7. Надайте характеристику функції формування трафіка.
8. Надайте характеристику функції обмеження трафіка.
9. Надайте характеристику функції маркування пакетів потоку.
10. Які механізми керування буферами Ви знаєте?
11. Які протоколи сигналізації служби підтримки якості Ви знаєте?
12. Надайте характеристику протоколам *QoS*.
13. Які умови виникнення черг?
14. Які алгоритми управління чергами Ви знаєте?
15. Як працює механізм пріоритетної обробки трафіка?
16. Надайте характеристику алгоритму зважених черг.
17. Як працює алгоритм «дірявого цеберка»?

Використана література

1) Г.Ф. Конахович, В.М. Чуприн. Сети передачи пакетной коммутации.–К..: МК-Пресс, 2006. Розділ 5.

САМОСТІЙНЕ ЗАНЯТТЯ ЗА МАТЕРІАЛАМИ ЛЕКЦІЇ №16. ІНЖЕНЕРІЯ ПАКЕТНОГО ТРАФІКА

16.6. Методи інженерії трафіку

Інженерія трафіку – це процес вибору раціональних шляхів проходження трафіку через мережу, де раціональність розуміється як досягнення збалансованого завантаження всіх ресурсів мережі. Якщо ресурси пакетної мережі є збалансованими, то забезпечується можливість її функціонування при високих рівнях коефіцієнту завантаження і створюються умови, коли ризики перенавантаження внаслідок пульсацій трафіку знаходяться у припустимих межах.

Якщо не здійснювати інженерію трафіка, то мережа, скоріш за все, буде функціонувати неефективно. Зокрема і тому, що традиційним протоколам маршрутизації притаманні певні недоліки. Наприклад відомо, що більшість протоколів маршрутизації, у тому числі дистанційно-векторні (такі, як *RIP*) або стану зв'язків (наприклад, *OSPF* чи *IS-IS*), вибирають *найкоротший маршрут* відповідно до вибраної метрики. В простих випадках під час вибору маршруту згідно із специфікаціями цих протоколів враховується лише кількість проміжних маршрутизаторів (точніше, проміжних зв’язків, які називають “хопами”), що розташовані на шляху транспортування пакетів. В інших випадках з метою більш раціонального вибору маршруту враховується також номінальна пропускна здатність каналів зв'язку, а також рівні затримок, що цими каналами вносяться. Однак у будь-якому випадку вибирається єдиний маршрут, якщо не виявлено іншого абсолютно рівнозначного з точки зору вибраної метрики маршруту. На практиці абсолютно рівнозначних маршрутів майже не буває, але досить часто виникає ситуація, коли для вибраного маршруту існують альтернативні шляхи з трохи гіршими характеристиками. Для запобігання перенавантаженням було б доцільно використати усі альтернативні шляхи просування пакетів через вузли мережі. На жаль, традиційні протоколи маршрутизації на таку альтернативу не реагують.

Відомим прикладом неефективності традиційних протоколів маршрутизації є так звана «риба» — мережа з топологією, що

відображена на рисунку 16.7.

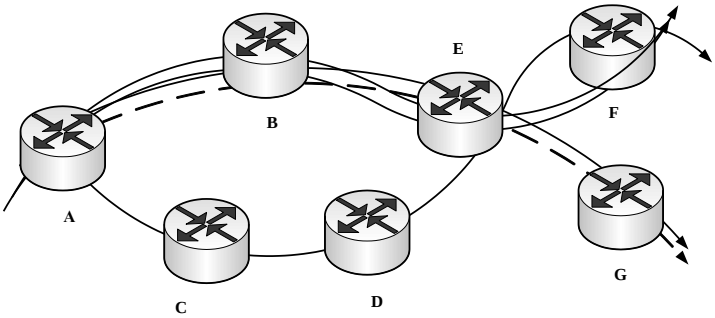


Рис.16.7. Фрагмент пакетної мережі з топологією «риба»

Між маршрутизаторами A та E існує два шляхи — перший, через маршрутизатор B, і другий, лише на один «хоп» більший — через маршрутизатори C і D. Тим не менш, у відповідності з принципами традиційних протоколів весь трафік від маршрутизатора A до маршрутизатора E буде спрямований тільки через маршрутизатор B. І тільки тому, що другий шлях трохи довший, традиційний протокол його ігнорує, хоча він міг би працювати «паралельно» з першим шляхом і розвантажувати маршрутизатор B.

Ще один недолік традиційних методів маршрутизації - шляхи вибираються без урахування ступеню поточного завантаження ресурсів мережі. Тобто, навіть якщо найкоротший шлях уже перенавантажений, пакети все рівно посилаються цим шляхом. Щоб позбавитися розглянутих вище недоліків і забезпечити можливість більш ефективного використання мережних ресурсів застосовується технологія **інженерії трафіку** (*Traffic Engineering, TE*).

Планування роботи мережі.

Невід'ємним елементом інженерії трафіка є робота, яку називають "планування роботи мережі". Таке планування передбачає певну попередню роботу щодо вибору та інсталяції параметрів обладнання мережі з урахуванням умов, що містяться в сервісних угодах з клієнтами - як тих, що вже набули чинність, так

і тих, що плануються до реалізації.

Планування роботи мережі починають з аналізу сервісних угод з клієнтами, що звуться *SLA – Service Level Agreement*. Під час такого аналізу визначають:

1) усі користувальницькі потоки даних та їхні можливі маршрути;

2) статистичні характеристики цих потоків (очікувана середня інтенсивність, можливі затримки пакетів, можливі коефіцієнти пульсацій потоків тощо);

3) вимоги клієнтів до якості обслуговування (бажані показники швидкості, припустимих затримок, ймовірностей втрат пакетів тощо).

Під час планування намагаються визначити параметри мережі, що забезпечують її роботу з максимально можливою ефективністю. Зазвичай прагнуть до найбільш повного завантаження мережних ресурсів — у першу чергу, маршрутизаторів і каналів зв'язку, — щоб передавати якомога більші обсяги даних. Але пульсації трафіка, що завжди існують в пакетних мережах, не дозволяють домогтися якісного обслуговування за умов навантажень, що наближені до максимально можливого рівня. Робота пакетної мережі може вважатися тільки тоді ефективною, коли кожен її ресурс якомога більше завантажений, але не перенавантажений. Усвідомлений вибір величини коефіцієнта завантаження ресурсу з урахуванням тонкої структури умов його використання, включаючи умови сервісних угод, має визначальне значення. Величина цього коефіцієнту безпосередньо впливає на розміри черг пакетів до ресурсу і на час затримки внаслідок перебування пакетів в чергах. Тому в процесі планування роботи мережі слід намагатися знайти розумний компроміс у досягненні двох протилежних цілей. З одного боку, необхідно прагнути до поліпшення якості обслуговування переданого трафіку, тобто намагатися знизити затримки в просуванні пакетів, зменшити втрати пакетів і збільшити інтенсивності потоків трафіку. Таке на практиці досягається, головним чином, за рахунок резервування ресурсів, а для цього потрібно мати додаткові незадіяні на даний момент ресурси мережі. З другого боку, необхідно намагатися максимально збільшити завантаження

всіх ресурсів мережі з метою підвищення економічних показників її експлуатації. Компроміс в досягненні вищезазначених цілей, як показує практика, слід шукати на шляху використання засобів і механізмів боротьби із заторами (*congestion*) у мережі, а саме:

1) здійснювати раціональне настроювання параметрів обладнання з метою обмеження безконтрольного збільшення інтенсивності вхідних потоків;

2) реалізовувати алгоритми керування чергами, що обрані з урахуванням конкретних умов використання мережі;

3) оптимізувати шляхи проходження потоків з користувальницькими даними через вузли мережі.

Загальна характеристика інженерії трафіку. Існують спеціалізовані методи і механізми здійснення інженерії, які спрямовані саме на збалансоване завантаження ресурсів.

Інженерію починають з аналізу таких двох типів характеристик:

1) характеристики транспортної мережі, що може бути використана — її топологія, а також продуктивність (тобто, пропускна здатність) маршрутизаторів і каналів зв'язку, що функціонують у складі цієї мережі (приклад відображення транспортної мережі - на рис.16.8);

2) запропоноване (бажане) навантаження на мережу, тобто дані про бажані значення величин щодо швидкостей потоків між кожною парою маршрутизаторів абонентського доступу, які розташовані на границях магістральної мережі (приклад відображення бажаного навантаження на мережу – на рис.16.9).

Задача інженерії полягає у визначенні шляхів проходження запропонованих потоків через мережу із визначеними характеристиками за умови, що усі ресурси мережі будуть навантажені якомога більш збалансовано.

Вирішити наведену задачу – означає знайти для кожного заданого потоку точну послідовність проміжних маршрутизаторів і їхніх інтерфейсів, що знаходяться на шляху між вхідною і вихідною точками цього потоку. При цьому маршрути потоків мають бути такі, щоб навантаження елементів мережі було якомога більш рівномірним.

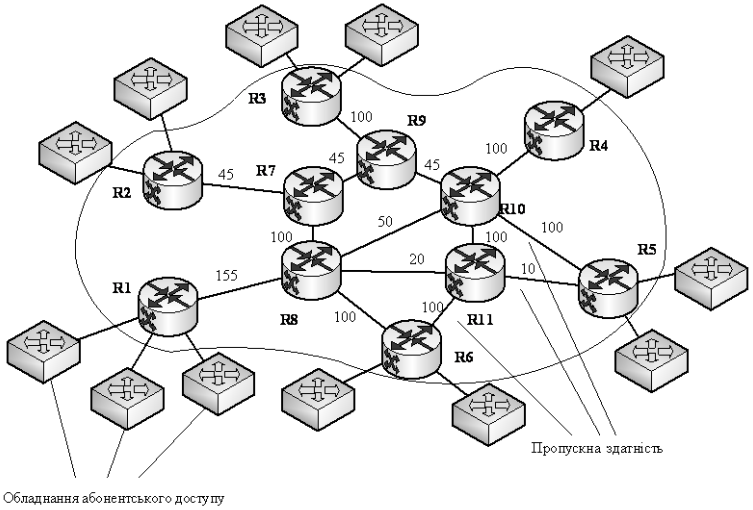


Рис.16.8. Приклад відображення даних щодо топології транспортної мережі і продуктивності її ресурсів

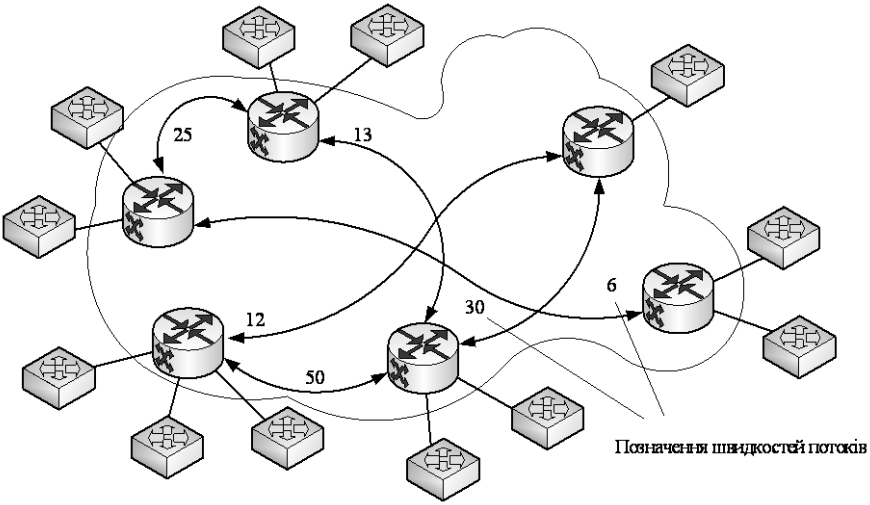


Рис.16.9. Відображення запропонованого навантаження на мережу

Формалізацію умови збалансованості ресурсів здійснюють різними способами. Наприклад, якщо за мету поставити мінімізацію нерівномірності у завантаженні мережних ресурсів при звісній структурі трафіку мережі, то доцільно мінімізувати максимальний коефіцієнт використання того ресурсу, для якого цей коефіцієнт має максимальне значення у розрізі всіх ресурсів мережі. Саме так формулюється задача інженерії в американському стандарті RFC 2702 «*Requirements for Traffic Engineering Over MPLS*». У цьому документі, що містить загальні рекомендації форуму IETF щодо вирішення задач інженерії, цільова функція оптимізації маршрутів має наступний вигляд:

$$min\ (max\ K_t), \qquad (16.1)$$

де K_t — коефіцієнт навантаження t-го ресурсу.

Іншим варіантом постановки задачі інженерії є пошук такого набору маршрутів, за яким значення коефіцієнтів використання усіх елементів мережі не перевищать заданий поріг K_{max}. Такий підхід простіше в реалізації за попередній, оскільки потребує перебору меншої кількості варіантів.

Агрегація потоків. Один із основних прийомів, що використовується під час інженерії трафіка, є **агрегація потоків**, тобто об'єднання потоків окремих користувачів в один загальний потік. При цьому одним агрегованим потоком вважається трафік пакетів, що має загальні вхідну і вихідну точки.

За умов індивідуального розгляду кожного породжуваного користувачами потоку проміжні маршрутизатори повинні зберігати занадто великі обсяги інформації, оскільки індивідуальних потоків може бути дуже багато. Крім того, в цілях маршрутизації доводиться запам'ятовувати адреси кінцевих вузлів (а не проміжних маршрутизаторів) і програмних портів UDP/TCP застосувань, що ще більш ускладнює задачу. Тому агреговане завдання потоків дозволяє спростити задачу вибору маршрутів.

Необхідно, однак, мати на увазі, що агрегація потоків можлива лише тоді, коли всі складові потоки пред'являють однакові вимоги до якості обслуговування (тобто, однакові вимоги до параметрів *QoS*). На практиці в задачах інженерії здебільшого розглядають

кілька потоків, серед котрих частина або навіть всі є агрегованими.

Точність результатів інженерії. Процес інженерії здійснюють з різним ступенем деталізації щодо опису характеристик потоків для яких визначаються маршрути. Чим вища ступінь деталізації, тим точніші результати вибору маршрутів.

Наприклад, для більш тонкої оптимізації мережі під час опису характеристик потоків бажано враховувати величину можливої пульсації трафіка або вимоги до якості обслуговування, зокрема, до припустимої величини затримок, варіації затримок та (або) припустимого відсотка втрат пакетів. Однак за цих умов задача інженерії ускладнюється настільки, що не завжди вдається її вирішити навіть наближеними методами. Тому в багатьох випадках задовольняються більш простими (субоптимальними) рішеннями, коли в процесі визначення шляхів проходження потоків через мережу враховуються тільки їхні середні інтенсивності з умовою, що коефіцієнт навантаження кожного елементу обладнання (маршрутизатору, каналу транспортування тощо) не буде перевищувати попередньо встановленого значення, наприклад 0,65. Крім того, з метою спрощення усі потоки пакетів вважаються рівнозначними, тобто такими, що висувають однакові вимоги до якості обслуговування.

Субоптимальні методи інженерії. Використовуються, в основному, наступні два субоптимальні підходи до вирішення задачі інженерії трафіку:

- автономний пошук раціональних маршрутів без втручання в оперативну роботу протоколів маршрутизації;
- автоматизований пошук раціональних маршрутів в оперативному режимі з використанням розширень протоколів маршрутизації, що працюють на основі так званого алгоритму стану зв'язків.

Автономний пошук раціональних маршрутів виконується завчасно. Слово «завчасно» означає, що спочатку визначаються маршрути потоків (наприклад, у фоновому режимі роботи ТЛК-обладнання), а потім відповідно до отриманих визначень здійснюється ручна маршрутизація потоків. Для автономного пошуку потрібно знати: топологію мережі і продуктивність її елементів, вхідну і вихідну точки кожного потоку, середню

інтенсивність кожного потоку. Необхідно задати також певний припустимий рівень максимального значення коефіцієнта навантаження елементів мережі, неперевищення котрого має бути забезпечено встановленням відповідних параметрів обладнання.

За цих вихідних даних реалізується процедура спрямованого перебору варіантів маршрутизації (зокрема, за допомогою спеціально створеної для цієї цілі комп'ютерної програми). Результатом такого перебору будуть визначені згідно обраного критерію маршрути для кожного потоку з вказівкою на місця розташування всіх проміжних маршрутизаторів у мережі.

Процес завчасного вирішення задачі інженерії трафіка доцільно продемонструвати на наступному прикладі. Для цього в якості вихідних візьмемо дані, що відображені на рис.16.8 та рис.16.9.
На рис.16.10 показано одне з можливих рішень поставленої задачі.

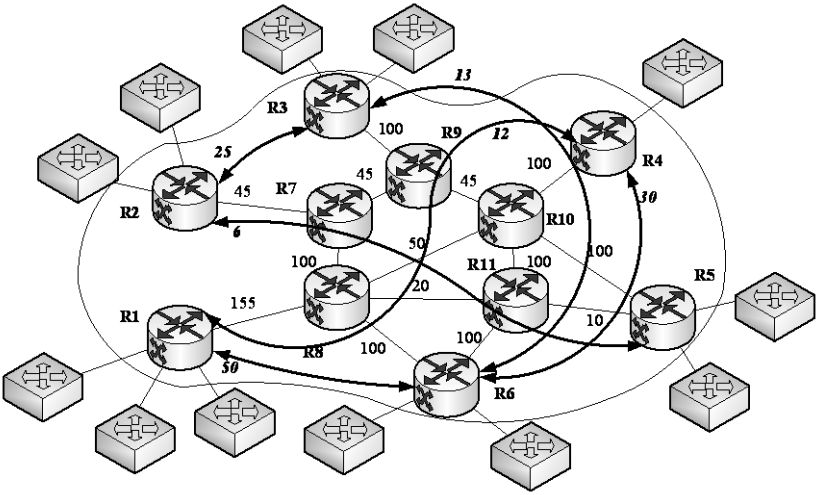


Рис.16.10. Розподіл навантаження на елементи мережі, за результатами автономного пошуку маршрутів

Жирними лініями показано прокладені маршрути. Як бачимо, на кожній ділянці між будь-якими суміжними маршрутизаторами значення коефіцієнту навантаження не перевищує 0,6. Наприклад, на ділянці між R8 та R10 коефіцієнт навантаження визначається як 12/50=0,24, що набагато менше, ніж 0,6. Так що отримані

результати гарантують, що значення коефіцієнту навантаження кожного із елементів мережі не перевищить 0,6.

Автоматизований пошук раціональних маршрутів з використанням розширень протоколів маршрутизації, що працюють на основі алгоритму стану зв'язків, здійснюється засобами мережної маршрутизації в оперативному режимі їхнього функціонування. Для цього використовуються розширення протоколів маршрутизації, що працюють на основі алгоритму стану зв'язків. Наразі такі розширення стандартизовані для протоколів *OSPF* і *IS-IS.* Причина застосування протоколів маршрутизації саме цього класу полягає в тому, що ці протоколи, на відміну від дистанційно-векторних протоколів, до яких відноситься, наприклад, *RIP*, дають маршрутизаторові повну топологічну інформацію щодо мережі. Оголошення цих протоколів містять дані як про внутрішні маршрутизатори досліджуваної мережі, так і про інші зовнішні мережі, а також про всі фізичні зв'язки між ними. Кожний зв'язок характеризується поточним станом щодо працездатності і метрикою, яка є величиною, пропорційною його вартості використання. У традиційному варіанті граф мережі, ребра якого навантажені значеннями метрик, використовується маршрутизатором для вибору найкоротшого (з мінімальною сумарною метрикою) маршруту до кожної із зовнішніх мереж. При цьому із знайденого маршруту в таблиці маршрутизації запам'ятовується тільки наступний "хоп" (тобто, запам'ятовується IP-адреса лише найближчого маршрутизатора), а дані щодо інших проміжних "хопів" відкидаються. Таке здійснюється відповідно до прийнятого у IP-мережах принципу просування пакетів - кожен маршрутизатор приймає рішення тільки про один крок маршруту.

У протоколи *OSPF* і *IS-IS*, щоб надати можливість за їх допомогою вирішувати задачі інженерії трафіку, включені нові типи оголошень, що поширюють каналами мережі додаткову інформацію про номінальну і незарезервовану пропускну спроможність кожного зв'язку. Таким чином, ребра результуючого графа мережі, що створюється в топологічній базі кожного маршрутизатора, ідентифікуються цими двома

додатковими параметрами. Побудувавши такий граф, а також отримавши інформацію про параметри потоків, для яких потрібно знайти раціональні маршрути, маршрутизатор одержує можливість знайти субоптимальне рішення, що задовольняє, наприклад, одному із сформульованих вище обмежень на коефіцієнти навантаження елементів мережі, забезпечивши тим самим збалансоване завантаження мережі.

Для спрощення задачі вибору маршрутів щодо визначеного набору потоків її рішення може здійснюватися поступово по черзі за кілька етапів – спочатку у рамках однієї послідовності каналів визначеного набору, потім іншої послідовності цього набору і т.д. При цьому в якості обмеження виступає сумарне завантаження кожного ресурсу мережі. Зрозуміло, що у будь-якому випадку пропускна здатність маршрутизатора має бути (у середньому) достатньою для обслуговування будь-якого трафіку, який у змозі прийняти інтерфейси цього маршрутизатора. Тому обмеженнями є тільки максимально припустимі значення коефіцієнтів завантаження каналів зв'язку, котрі встановлюються індивідуально для кожного каналу окремо або ж мають однакові значення.

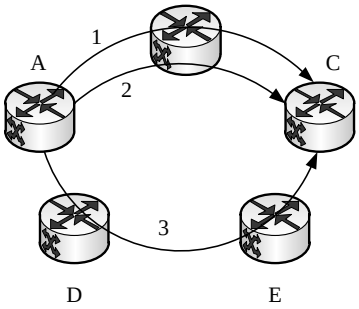
Процедура знаходження маршруту з урахуванням обмежень одержало назву *Constrained-based Routing*, а протокол *OSPF* з відповідними розширеннями — *Constrained SPF* або *CSPF*.

Зрозуміло, що пошук раціональних маршрутів по черзі з послідовним розглядом варіантів агрегації потоків знижує якість рішення, оскільки при одночасному розгляді всіх потоків можна знайти більш раціональний варіант завантаження ресурсів.

Проаналізуємо приклад, що наведений на рисунку 16.11.

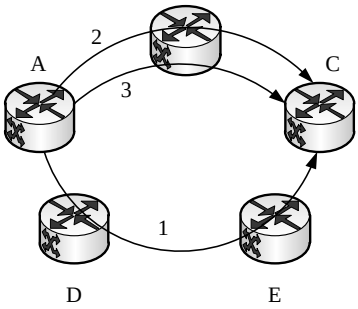
Задано обмеження на максимально припустиме значення коефіцієнта навантаження елементів мережі K_{max}, яке у даному прикладі прийнято рівним 0,65. Задано також результуючий граф досліджуваної мережі, який відображений у верхній частині рис.16.11. Як бачимо, на п’яти вузлах A,B,C,D,E задано три потоки, що починаються на вузлі A і закінчуються на вузлі C. Середні інтенсивності цих потоків N відповідно визначені як 50, 40, 30. Відношення між номінальною пропускною спроможністю та не зарезервованою (тобто, ще не використаною) її частиною N' для

кожного із вузлів - однакове і дорівнює 150/100.



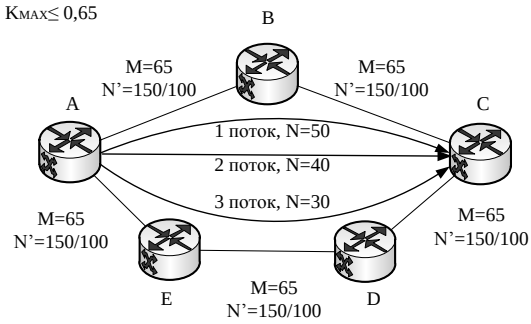
Рішення з варіантом 1: 1 → 2 → 3

K_{MAX}= 0,58



Рішення з варіантом 2: 2 → 3 → 1

K_{MAX}= 0,5



Результуючий граф з вихідними даними

- мережний маршрутизатор

Рис.16.11. Інженерія трафіка з послідовним розглядом варіантів агрегації потоків

Метрика M (яка безпосередньо пов’язана із вартістю користування маршрутом) кожного зв’язку (кожного “хопу”) дорівнює 65 умовних одиниць.

Розглянемо два варіанти вирішення задачі.

У варіанті 1 для першого потоку обираємо маршрут A-B-C, тому що, з одного боку, він задовольняє заданому обмеженню на максимальний коефіцієнт навантаження обладнання мережі (у даному випадку, усі маршрутизатори уздовж маршруту виявляються завантаженими на 50/150 = 0,33, тобто меншими, ніж 0,65), а з іншого боку, він має мінімальну за цих умов метрику: 65 + 65 = 130. Для другого потоку також був обраний шлях A-B-C, тому що у цьому випадку висунуте обмеження також задовольняється, тобто результуючий коефіцієнт використання виявляється рівним (50+40)/150=0,6. За цих умов третій потік може направлятися тільки в напрямку A-D-E-C і завантажувати ресурси каналів A-D, D-E і E-C на 30/150=0,2. Рішення за варіантом 1 хоч і задовольняє висунутій вимозі щодо не перевищення коефіцієнту навантаження будь-якого маршрутизатора значення 0,65, але знайдені маршрути виявились завантаженими нерівномірно (порівняйте отримані коефіцієнти навантаження маршрутів - 0,2 з 0,6).

Краще рішення представлене варіантом 2, згідно з котрим за маршрутом A-B-C спрямовуються потоки 2 і 3, а потік 1 — за маршрутом A-D-E-C. У цьому випадку ресурси першого маршруту виявляються завантаженими на (40+30)/150=0,46, а другого — на 0,33, тобто в наявності більш рівномірне завантаження ресурсів, а максимальний коефіцієнт використання будь-якого елементу мережі не перевищує 0,5.

Займатися задачами інженерії трафіка не є обов’язковою функцією експлуатаційного персоналу. Проте слід відмітити одну позитивну особливість вирішення цих задач: в результаті їхнього вирішення визначається не тільки маршрут до сусіднього маршрутизатора (тобто, запам'ятовується не тільки перший “хоп” маршруту, як це робиться в процедурах класичної IP-маршрутизації), але також інформація про всі проміжні вузли мережі (разом з початковим і кінцевим). Це надає можливість не

займатися маршрутизацією на проміжних вузлах, а здійснювати маршрутизацію тільки на граничних маршрутизаторах дослідженої мережі. Внутрішні маршрутизатори мають надсилати до граничних маршрутизаторів невеликі обсяги необхідної інформації про поточний стан мережі. Такий підхід (реалізація котрого можлива лише після отримання результатів інженерії трафіка) має кілька переваг у порівнянні з розподіленою моделлю пошуку шляхів, що лежить в основі стандартних протоколів маршрутизації IP. По-перше, він дозволяє використовувати так звані «зовнішні» рішення, коли маршрути знаходяться якою-небудь зовнішньою системою оптимізації мережі в автономному режимі, а потім встановлюються в мережі. По-друге, кожний із граничних маршрутизаторів має можливість працювати за власною версією алгоритму пошуку, що спрощує роботу на устаткуванні різних виробників. По-третє, такий підхід розвантажує внутрішні маршрутизатори від роботи з пошуку шляхів.

16.7. Механізми реалізації визначених маршрутів

Після того як задача інженерії трафіку знайшла вирішення і маршрути визначені, необхідно задіяти програмні механізми, які дозволяли б спрямовувати пакети, що відносяться до визначеного маршруту, саме через ті проміжні маршрутизатори, що були обрані.

Ця задача для IP-мереж ускладнюється тим, що основний режим маршрутизації, що підтримується стандартним ТЛК-обладнанням, пропонує лише єдиний «найкоротший» маршрут. В принципі, за цих умов, в IP-мережах існує можливість використати режим маршрутизації від джерела (*Source Routing*), оскільки він дозволяє джерелу пакетів задавати точну послідовність проміжних вузлів уздовж шляху їхнього проходження. Але цьому режимові притаманні суттєві обмеження, через які в експлуатаційній практиці він не отримав значного розповсюдження. По-перше, наразі він підтримується не усіма виробниками устаткування (зокрема, в поточній версії 4 протоколів IP). По-друге, маршрутизація від джерела пов’язана з необхідністю транспортування небажано великої кількості службової інформації (оскільки кожен пакет додатково має

переносити дані щодо всіх адрес проміжних маршрутизаторів, через які пролягає маршрут). По-третє, цей режим надзвичайно уразливий з погляду інформаційної безпеки: саме тому адміністратори під час конфігурування маршрутизаторів, як правило, його відключають.

Отже, для реалізації в мережі маршрутів, знайдених в результаті інженерії трафіка, використовують спеціальний службовий протокол, який, зазвичай, відносять до класу протоколів сигналізації. У якості такого найчастіше в IP-мережах використовується протокол резервування ресурсів *RSVP* (*Resource reSerVation Protocol*). У повідомленнях цього протоколу для визначеного потоку прописується точний маршрут, що встановлюється у вигляді послідовності IP-адрес інтерфейсів проміжних маршрутизаторів, через які просувається потік. Маршрутизатори запам'ятовують встановлені маршрути у спеціальних таблицях, які мають назву “таблиці комутації” (не плутати з таблицею маршрутизації). А для того щоб пакети просувалися не за допомогою таблиць маршрутизації, а за допомогою таблиць комутації, використовується спеціальна технологія просування — *MPLS* (*Multiprotocol Label Switching*).

Основне призначення технології *MPLS* полягає в забезпеченні можливості надання диференційованих послуг *QoS* з гарантованим сервісом. Але з позицій інженерії трафіку істотним є той факт, що ця технологія дозволяє передавати пакети (які належать визначеному потокові) уздовж заздалегідь обраного і встановленого в мережі шляху. При цьому специфіка інженерії полягає в тім, що шляхи вибираються з метою дотримання балансу завантаження ресурсів мережі.

Дотримання верхньої межі завантаження після впровадження результатів інженерії суттєво підвищує упевненість, що середня довжина і варіація черг до кожного мережного ресурсу буде знаходитися у визначених межах, так що затримки пакетів і втрати через недостачу місця у буферній пам'яті також із визначеною імовірністю не будуть перевищувати звісних граничних значень.

Примітка 16.1. Точні значення величин затримок і втрат пакетів тільки на основі додержання обмежень щодо коефіцієнтів навантаження елементів мережі в

реальних умовах експлуатації визначити практично неможливо, хоча цей коефіцієнт і найбільш істотно впливає на якісні показники роботи мережі. Уточнені оцінки значень затримок або відсотків втрат пакетів визначаються в мережі, як правило, шляхом натурних вимірювань. Результати таких вимірювань надаються клієнтам мережі відповідно до умов сервісних угод про рівень обслуговування (тобто, у *SLA*).

16.8. Інженерія трафіка різних класів

В експлуатаційній практиці часто виникає ситуація, коли діяльність покупця послуг мережі пов'язана з генерацією кількох різних класів трафіку, і ці класи відрізняються вимогами до якості обслуговування. Типовим прикладом є необхідність розподілу трафіку, принаймні, на два класи — чутливого і не чутливого до затримок пакетів. До одного класу відносять, наприклад, трафік IP-телефонії й інших мультимедійних інтерактивних застосувань, а також трафік застосувань, які здійснюють функції керування технологічними об'єктами у реальному часі. Інші види трафіку, що не є чутливими до затримок пакетів (наприклад, потоки файлів з програмним забезпеченням), відносять до другого класу.

За умов спрощеного варіанту надання послуг, коли ці два класи трафіка в засобах ТЛК-обладнання не розрізняються і не відокремлюються один від одного, для того щоб гарантувати користувачам неперевищення узгоджених рівнів затримок та варіацій затримок, оператор змушений тримати ресурси своєї мережі недовантаженими, так щоб коефіцієнт навантаження кожного ресурсу не перевищував 0,2-0,3. Тоді для пакетів обох класів будуть створені умови для якісного їхнього транспортування через мережу (якісного – з точки зору мінімізації затримок пакетів). Однак, такий підхід важко назвати раціональним. Якщо ж за цим варіантом надання послуг оператор мережі поставить за мету більш ефективно завантажувати свої ресурси, наприклад, до рівня 0,6-0,7 (оскільки певну частину пропускної здатності необхідно залишити для службового трафіку і врахувати, хоч і на якісному рівні, пульсації трафіку), тоді він зможе обслуговувати тільки тих користувачів, трафік котрих є нечутливим до затримок. В будь-яких інших випадках необхідно розрізняти класи трафіку і вирішувати задачу інженерії з урахуванням їхнього існування.

Якщо здійснюється інженерія трафіку різних класів, то в розширеннях протоколів маршрутизації необхідно забезпечити окреме урахування завантажень кожного елементу мережі у розрізі кожного класу трафіка. При цьому, як показує практика, коефіцієнт завантаження будь-якого мережного ресурсу чутливим до затримок трафіком має не перевищувати 0,2 - 0,3, а щодо іншого класу трафіку – цей коефіцієнт має вибиратися в межах 0,6 - 0,7. Якщо за цих умов чутливий до затримок трафік буде обслуговуватися в єдиній пріоритетній черзі, а інший трафік — за схемою кругового обслуговування типу “з максимальними зусиллями”, то трафік кожного класу з високою ймовірністю отримає необхідний для нього рівень обслуговування. Вищенаведене ілюструється графіком залежності середніх затримок пакетів τ від вибраного коефіцієнта навантаження елементу мережного обладнання K, що відображений на рис.16.12.

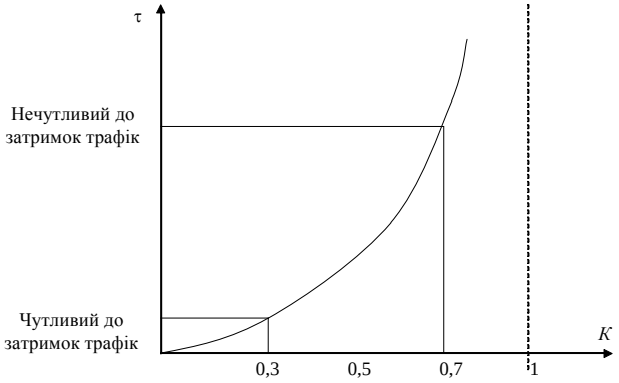


Рис.16.12. Залежність середніх затримок пакетів τ від рівнів завантаження мережного елементу K

Механізм реалізації гарантованого обслуговування двох класів трафіку з наведеними вище характеристиками має функціонувати наступним чином. З кожним елементом мережі, що має засоби впливу на параметри потоків, повинне бути зв'язано два

лічильники завантаження — один для пріоритетного трафіку, а другий для іншого (фонового) трафіку. Якщо необхідно додати до вже існуючого в мережі трафіку додатковий потік пріоритетного класу і, отже, визначити для цього потоку маршрут, то під час перевірки можливості проходження шляху через конкретний мережний елемент середня інтенсивність нового потоку повинна порівнюватися з вільною часткою пропускної здатності цього елементу саме щодо пріоритетного трафіку. Якщо вільна частка ресурсу виявиться достатньо і цей новий потік буде проходити через даний інтерфейс, то значення інтенсивності нового потоку необхідно відняти як з лічильника завантаження пріоритетного трафіку, так і з лічильника завантаження фонового трафіку (тому що пріоритетний трафік завжди буде обслуговуватися раніше фонового і тому він створить додаткове навантаження і для фонового трафіку). Якщо ж необхідно додати до вже існуючого трафіку додатковий фоновий потік, то його інтенсивність порівнюється з вільною інтенсивністю лічильника фонового трафіку, а значення цієї інтенсивності віднімається тільки з лічильника фонового трафіку, тому що для пріоритетного трафіку фоновий трафік є прозорим.

Протоколи маршрутизації з розширеннями в цих умовах повинні поширювати уздовж мережі інформацію про два параметри вільної пропускної здатності — для кожного класу трафіку окремо.

Якщо ж задача узагальнюється для випадку передачі через мережу трафіку кількох класів, то, відповідно, з кожним ресурсом повинне бути зв'язане стільки лічильників, скільки класів трафіку існує в мережі, а протоколи маршрутизації повинні поширювати вектор вільних інтенсивностей відповідної розмірності.

Контрольні питання до самостійного заняття шістнадцятої лекції:

1.Що таке інженерія трафіку?

2. Які недоліки притаманні традиційним протоколам маршрутизації?

3. Наведіть фрагмент пакетної мережі з топологією «риба».

4. Яким чином здійснюється планування роботи мережі?

5. Що таке *SLA*?

6. У чому полягає компроміс при плануванні роботи мережі?

7. З чого починають інженерію трафіка?

8. Що значить вирішити задачу інженерії трафіка?

9. Надайте формальну умову збалансованості ресурсів.

10. Що таке агрегація потоків?

11. Які субоптимальні методи інженерії трафіка Ви знаєте?

12. Чим автономний пошук раціональних маршрутів краще за автоматизований пошук?

13. Які переваги пошуку раціональних маршрутів по черзі з послідовним розглядом варіантів агрегації потоків?

14. Які механізми реалізації визначених маршрутів Ви знаєте?

15. Надайте характеристику режиму маршрутизації від джерела (*Source Routing*).

16. Який спеціальний службовий протокол сигналізації використовують для реалізації в мережі маршрутів, знайдених в результаті інженерії трафіка?

17. Яке основне призначення технології *MPLS*?

18. У чому полягає специфіка інженерії трафіку різних класів?

Література до самостійного заняття шістнадцятої лекції

1) Г.Ф. Конахович, В.М. Чуприна „Мережі передавання пакетних даних”. – К.: „МК-Прес”, 2006. Розділ 7.

МОДУЛЬ №5. ТЕХНОЛОГІЇ ПІДТРИМКИ ПОЛІТИКИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ТЛК-ОБЛАДНАННЯ

ЛЕКЦІЯ №17. СТВОРЕННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ У ТЛК-СИСТЕМАХТА ЇХ ПІДТРИМКА В АКТУАЛЬНОМУ СТАНІ

Розглядаються наступні питання:

Лекційне заняття

17.1. Загальні положення щодо організації технічного захисту інформації у ТЛК-системах

17.2. Розробка політики забезпечення захисту інформаційних ресурсів ТЛК-систем

17.3. Впровадження розробленої політики забезпечення захисту ресурсів ТЛК-систем

17.4. Підтримка впровадженої політики забезпечення захисту в період експлуатації

Самостійне заняття. СТВОРЕННЯ СИСТЕМИ ЗАХИСТУ ТА ОЦІНЮВАННЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ РЕСУРСІВ ПРОГРАМНО-КЕРОВАНОЇ АТС

17.5. Структура АТС з позицій технічного захисту інформації

17.6. Порядок виконання робіт з ТЗІ на АТС

17.7. Оцінка ефективності захисту інформаційних ресурсів АТС

17.1. Загальні положення щодо організації технічного захисту інформації у ТЛК-системах

Інформація, яка підлягає технічному захисту, у процесі функціонування ТЛК-систем може зазнавати впливів загроз, внаслідок чого може виникнути її виток, порушення її цілісності або порушення доступності до неї з боку авторизованих користувачів (див., наприклад, Закон України "Про захист інформації у автоматизованих системах", "Положення про технічний захист інформації в Україні", Рекомендації Ради Європи №№ R (89)2, R (95)4 та ін.). Спроможність системи технічного захисту інформації (ТЗІ) протистояти впливам загроз визначає рівень захищеності інформаційних ресурсів телекомунікаційної

системи. ТЛК-системи, як правило, оснащуються штатними і, при необхідності, додатковими (позаштатними) засобами ТЗІ, які при їхньому спільному використанні утворюють комплекс засобів і механізмів захисту (КЗМЗ), що забезпечує потрібний рівень захищеності інформаційних ресурсів цих систем.

Основні принципи організації ТЗІ полягають у наступному:

1) Принцип легітимності захисту - ТЗІ у телекомунікаційних системах (далі - захист ТКС) повинен ґрунтуватися на положеннях і вимогах чинних в Україні нормативно-правових актів і нормативних документів щодо технічного захисту інформації.

2) Принцип комплексності захисту - захист ТКС повинен забезпечуватися комплексом взаємопов'язаних програмно-технічних засобів і організаційних заходів.

3) Принцип безперервності захисту - захист ТКС повинен забезпечуватися на всіх технологічних етапах та режимах їх функціонування і надання послуг, зокрема при проведенні ремонтних і регламентних робіт.

4) Принцип мінімальної достатності захисту - захист ТКС повинен забезпечувати необхідний рівень захищеності при мінімальних витратах ресурсів.

5) Програмно-технічні засоби захисту не повинні істотно погіршувати основні характеристики ТКС (пропускну спроможність, надійність, можливість зміни конфігурації ТКС і т. ін.).

6) Невід'ємною частиною робіт з ТЗІ у ТЛК-системах є оцінка ефективності засобів захисту, що здійснюється згідно з методиками, які враховують всю сукупність технічних характеристик оцінюваного об'єкта, включаючи технічні рішення і практичну реалізацію засобів захисту.

7) Захист ТЛК-систем повинен передбачати створення систем керування комплексами засобів захисту, що дозволяють здійснювати безперервний контроль ефективності засобів захисту, підтримку необхідного рівня захищеності інформаційних ресурсів цих систем.

Примітка 1. Основні терміни та визначення у сфері організації технічного захисту інформації

Перш ніж перейти до викладу основного змісту лекції наведемо пояснення

основних термінів та визначень (згідно ДСТУ 2615-94, ДСТУ 2621-94 і ДСТУ 3396.2-97), що стосуються проблематики ТЗІ у телекомунікаційних системах. Крім того, уточнимо терміни і визначення щодо проблематики ТЗІ на АТС, що регламентовані положеннями НД ТЗІ 1.1-001-99.

Інформаційний ресурс - це власне інформація або будь-який об'єкт, що є елементом певної інформаційної технології (технічні засоби обчислювальної або телекомунікаційної техніки, програми, дані і т. ін.).

Уразливість інформації - фундаментальна властивість інформації наражатися на небажані з точки зору її власників впливи з боку різного роду несприятливих чинників середовища існування інформаційних ресурсів;

ТЗІ у ТЛК-системах - запобігання за допомогою інженерно-технічних заходів реалізаціям загроз для інформаційних ресурсів цих систем, що створюються через технічні канали, через канали спеціальних впливів та шляхом несанкціонованого доступу.

Канали спеціальних впливів на елементи ТЛК-систем - канали, через які впливи на технічні (апаратні) засоби ТЛК-систем призводять до створення загроз для інформації.

Реалізація загроз для інформації у ТЛК-системах через канали спеціальних впливів можлива з-за:

- кількісної недостатності компонентів ТЛК-систем;
- якісної недостатності компонентів і (або) всієї ТЛК-системи у цілому;
- навмисної або ненавмисної діяльності осіб, які, в свою чергу, впливають на елементи ТЛК-системи з використанням програмних і (або) технічних засобів;
- несправностей апаратних елементів ТЛК-систем;
- виходів за межі припустимих значень параметрів зовнішнього середовища функціонування ТЛК-систем (у тому числі, пов'язаними зі стихійними лихами, катастрофами й іншими надзвичайними подіями);
- помилок і некоректних дій суб'єктів доступу до ресурсів ТЛК-систем на стадії їх промислової експлуатації.

Кількісна недостатність компонентів - фізична недостатність компонентів ТЛК-систем, що не дозволяє забезпечити потрібну захищеність інформаційних ресурсів у розрізі розглянутих показників ефективності захисту.

Якісна недостатність - недосконалість архітектури чи структури ТЛК-систем, організації технологічних процесів їх функціонування, проектних рішень на будь-якому з видів їхнього забезпечення (програмного, апаратного, інформаційного і т.ін.), недоробки функціональних та принципових схем, конструкції компонентів і (або) всієї ТЛК-системи у цілому, внаслідок чого не забезпечується потрібна захищеність інформаційних ресурсів у розрізі розглянутих показників ефективності захисту.

Відмова - порушення працездатності певного елемента ТЛК-системи, що унеможливлює виконання ним своїх функцій.

Збій - тимчасове порушення працездатності певного елемента ТЛК-системи, внаслідок чого з'являється можливість хибного виконання ним у цей момент своїх функцій.

Помилка - хибне (одноразове або систематичне) виконання елементом ТЛК-

системи однієї або кількох функцій, що відбувається внаслідок специфічного (постійного або тимчасового) його стану.

Стихійне лихо - спонтанно виникаюче природне явище, що виявляється як могутня руйнівна сила.

Зловмисні дії - дії людей, що спеціально спрямовані на порушення захищеності інформаційних ресурсів.

Побічне явище - явище, що супроводжує виконання елементом ТЛК-системи своїх основних функцій, внаслідок якого можливе порушення захищеності інформаційних ресурсів цієї системи.

Штатні засоби доступу (до інформаційних ресурсів ТЛК-системи) - системні термінали, термінали обслуговування (у тому числі, віддалені), телефонні комутатори та абонентські прикінцеві пристрої.

Закладний пристрій - позаштатний технічний пристрій, встановлений і замаскований у апаратному середовищі ТЛК-системи з метою реалізації загроз для інформації.

Програмна закладка - позаштатна комп'ютерна програма, встановлена і замаскована у програмному середовищі ТЛК-системи з метою реалізації загроз для інформації.

Програмно-апаратні закладні пристрої (закладки) - закладні пристрої та (або) програмні закладки.

Модель порушника - опис ймовірних дій порушника, рівня його повноважень, ресурсних можливостей, використовуваних ним програмних і (або) апаратних засобів з метою реалізації загроз для інформації у ТЛК-системі.

Модель загроз для інформації у ТЛК-системі - опис способів і засобів здійснення суттєвих загроз для інформаційних ресурсів із зазначенням рівнів гранично припустимих втрат, що пов'язані з їхніми можливими проявами в конкретних або передбачуваних умовах застосування цієї системи.

Сертифікований канал можливої реалізації загроз для інформаційних ресурсів – стандартизований потенційно можливий документально зафіксований у моделях порушників спосіб (метод і (або) механізм) реалізації загроз для інформаційних ресурсів.

Слабке місце у захисті - сертифікований канал можливої реалізації загроз для інформаційних ресурсів, механізми захисту для протидії котрим у системі ТЗІ відсутні.

Вилом у захисті – сертифікований канал можливої реалізації загроз для інформаційних ресурсів, механізми захисту для протидії котрим у системі ТЗІ присутні, але перебувають у непрацюючому стані.

Функціональна послуга захисту (ФПЗ) - взаємопов'язана множина виконуваних ТКС елементарних функцій, яка дозволяє протистояти певним загрозам для інформації.

Засіб захисту - програмний і (або) технічний засіб, який безпосередньо реалізує певну ФПЗ.

Механізм захисту - процедура або частина процедури реалізації певної ФПЗ.

Стійкість (потужність) механізму захисту - його здатність протистояти прямим атакам, тобто спробам його безпосереднього злому.

Модель захисту - опис взаємопов'язаної множини ФПЗ із зазначенням необхідних рівнів стійкості реалізованих механізмів захисту, у випадку реалізації якої забезпечується потрібний рівень захисту інформації у ТЛК-системі.

База захисту ТЛК-системи - сукупність всіх елементів системи ТЗІ (методологічних, методичних, проектних, програмних, апаратних, організаційних і т.ін.), що мають відношення до організації протидії загрозам для інформаційних ресурсів у ТЛК-системі.

Комплекс засобів і механізмів захисту (КЗМЗ) - взаємопов'язаний набір засобів і механізмів ТЗІ, що реалізують обрану модель захисту інформаційних ресурсів у ТЛК-системі.

Гарантії захисту на певній стадії життєвого циклу ТЛК-системи - сукупність вимог до реалізації організаційно-технічних заходів на цій стадії життєвого циклу системи, що спрямовані на підвищення захищеності інформації у ТЛК-системі.

КАЗЛ - підсистема комутації абонентських і з'єднувальних ліній зв'язку у системі з комутацією каналів.

ПРД - правила розмежування доступу.

СРД - система розмежування доступу.

Неформальний опис – опис на звичайній мові, що не підлягає будь-яким обмеженням, за винятком необхідності використання звичайних умовностей граматики та синтаксису мови, яка використовується (при цьому багатозначність щодо трактування опису не виключається).

Напівформальна специфікація – специфікація, яка потребує використання обмежувальних позначень (наприклад, діаграм структур даних або процесів, мови специфікацій SDL і т. ін.) при додержанні певних умовностей, котрі мають неформальний опис (при цьому багатозначність щодо трактування опису суттєво обмежується, але повністю не виключається).

Формальна специфікація - специфікація, яка потребує використання лише формальної системи правил та позначень, побудованої на обгрунтованій математичній концепції (при цьому ймовірність багатозначності щодо трактування специфікації визначається ступенем обгрунтованості математичної концепції, що використовується).

Тест на проникнення - опис (специфікація) процедури штатних дій санкціонованого користувача або експерта, що імітує дії потенційного порушника з метою перевірки ефективності системи захисту ("глибина" тесту на проникнення визначається ступенем наближення дій, що імітуються, до реально можливих дій порушника та ресурсними можливостями порушника).

Гарантії захисту на певній стадії життєвого циклу ТЛК-системи - сукупність вимог до реалізації організаційно-технічних заходів на цій стадії життєвого циклу системи, що спрямовані на підвищення захищеності інформації у ТЛК-системі.

Заявник - юридична або фізична особа, що є ініціатором проведення робіт з ТЗІ;

Експерт - фізична особа, яка має високу кваліфікацію, спеціальні знання, безпосередньо здійснює експертизу і несе персональну відповідальність за

достовірність та повноту аналізу, обгрунтованість рекомендацій відповідно до вимог завдання на проведення експертизи.

Оцінка ТЛК-системи за критеріями ТЗІ - комплекс спеціалізованих дослідницько-аналітичних та експериментальних робіт, що виконуються з метою визначення відповідності системи захисту інформації у ТЛК-системі до вимог (специфікацій) нормативних документів з ТЗІ.

Експертиза ТЛК-системи за критеріями ТЗІ - діяльність, метою якої є дослідження, перевірка, аналіз та оцінка науково-технічного рівня системи захисту інформації у ТЛК-системі, а також підготовка обгрунтованих висновків для прийняття рішення щодо рівня захищеності інформаційних ресурсів цієї системи в описаних Заявником умовах експлуатації ТЛК-системи та рівня довіри до результатів оцінки.

Зміст і послідовність робіт з протидії загрозам та їх нейтралізації повинні відповідати вказаним у ДСТУ 3396.0-96 і ДСТУ 3396.1-96 етапам створення системи захисту інформації (див. рис.17.1) і полягати у:

- розробці технічної політики забезпечення захисту інформаційних ресурсів ТЛК-системи, що знаходиться в експлуатації (охоплює стадії розробки моделі загроз інформаційним ресурсам ТЛК-системи, розробки технічного та робочого проектів системи ТЗІ у ТЛК-системі – опції 1.1 – 1.7 та опції 2.1 – 2.2 рис.17.1);
- впровадження розробленої технічної політики забезпечення захисту інформаційних ресурсів ТЛК-системи в експлуатаційну практику (охоплює стадію реалізації техно-робочого проекту системи ТЗІ – опції робіт 3.1-3.5);
- підтримка впровадженої технічної політики забезпечення захисту інформаційних ресурсів ТЛК-системи в процесі її експлуатації (охоплює стадію оцінки ТЛК-системи за критеріями ТЗІ).

Технічну політику забезпечення захисту інформаційних ресурсів іноді скорочено називають політикою безпеки (ПБ). Зазвичай розробка ПБ полягає у розробці та реалізації техно-робочого проекту системи ТЗІ у ТЛК-системі.

На початковому етапі для вперше створюваних ТЛК-систем (таких, наприклад, як інформаційні мережі з розподіленим керуванням і з розподіленим опрацюванням даних або таких, як системи комутації телефонних каналів зв'язку), у складі яких планується використання ТЛК-системи, розроблюється підрозділ технічного завдання на створення ТЛК-системи за назвою "Вимоги до ТЗІ у ТЛК-системі". Цей підрозділ включається до складу розділу технічного завдання (ТЗ), що відображає вимоги з ТЗІ у ТЛК-системі у цілому, і оформлюється згідно з ГОСТ 34.602-89. Крім того, в інших розділах ТЗ на ТЛК-систему, мають бути враховані вимоги з ТЗІ.

Для вже введених в експлуатацію ТЛК-систем, але не

атестованих за критеріями ТЗІ, технічні вимоги (ТВ) до системи ТЗІ у ТЛК-системі розроблюються у вигляді окремого документу згідно з ГОСТ 34.602-89.

Середовище функціонування ТЛК-системи

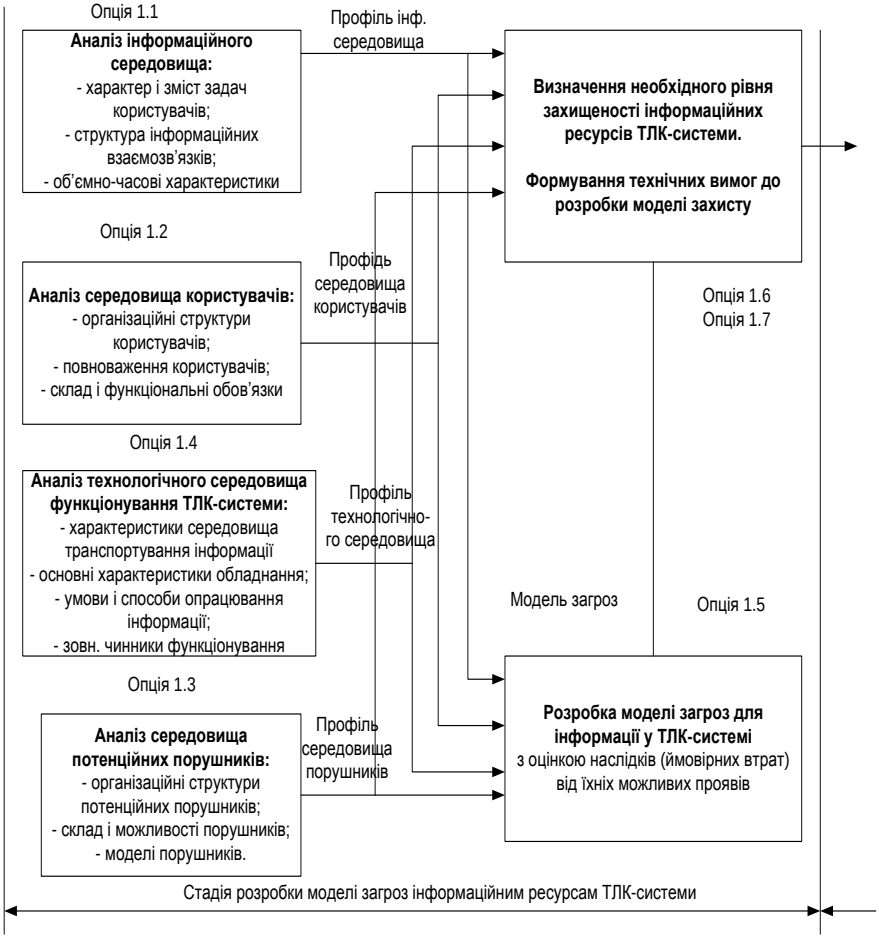


Рис. 17.1. Схема організації робіт з ТЗІ у ТЛК-системі

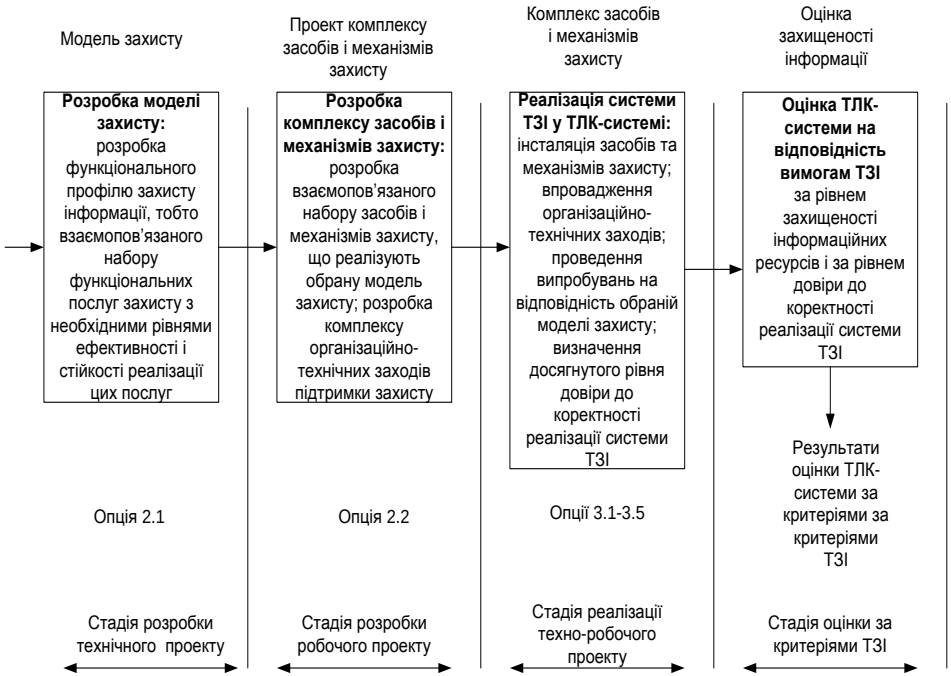


Рис.17.1 (продовження). Схема організації робіт з ТЗІ у ТЛК-системі

Підтримка впровадженої ТБ полягає у періодичних оцінках досягнутого рівню захищеності інформаційних ресурсів ТЛК-системи та спостереженням за можливими відхиленнями параметрів середовища експлуатації ТЛК-системи від тих значень, що зазначені у проекті системи ТЗІ. Якщо такі відхилення мали місце, то вони повинні бути усунуті або ж необхідне коригування проекту системи ТЗІ.

17.2. Розробка технічної політики забезпечення захисту інформаційних ресурсів ТЛК-систем

17.2.1. Розробка технічного завдання на створення системи ТЗІ у ТЛК-системах

Зазвичай розробку технічної політики захисту (політику безпеки, ПБ) починають з розробки технічного завдання (ТЗ) або

технічних вимог до створюваної системи захисту.

У процесі розробки ТЗ на систему ТЗІ у ТЛК-системах:

– аналізуються інформаційні потоки через ТКС, характер і зміст розв'язуваних її користувачами задач, рівень цінності (у т.ч., ступінь конфіденційності) інформації користувачів;

– оцінюються характеристики технологічного середовища експлуатації ТКС, що підлягає захисту;

– створюються моделі порушників;

– виявляються дестабілізуючі чинники і загрози для інформаційних ресурсів;

– прогнозуються імовірності прояву загроз, потенційно можливі і припустимі втрати власників та користувачів ТКС, що пов'язані з такими проявами;

– будується модель загроз;

– задаються вимоги до необхідного рівня захищеності інформаційних ресурсів у ТКС.

Відповідно до принципу мінімальної достатності (див. НД ТЗІ 1.1-001-99) система захисту повинна бути спроектована таким чином, щоб здійснювалася протидія тільки тим загрозам, що мають суттєве значення для Замовника системи ТЗІ, і тільки у тій мірі, у котрій необхідно нейтралізувати (послабити, зменшити) наслідки прояву таких суттєвих загроз, для того щоб втрати від їхніх можливих реалізацій не перевищували гранично припустимих рівнів. Тому необхідний рівень захищеності інформації у ТЗ або у ТВ визначається, виходячи із необхідності нейтралізації врахованих загроз.

У процесі аналіза інформаційних потоків через ТКС, характеру і змісту розв'язуваних її користувачами задач, як правило, керуються матеріалами, що викладені в підрозділах стандарту на створення ТЗ для розроблюваних автоматизованих систем (АС) ГОСТ 34.602-89, зокрема "Вимоги до функцій (задач), що виконуються системою" і "Вимоги до видів забезпечення", звертаючи особливу увагу на вимоги до інформаційного забезпечення. Рівень цінності (у т.ч., ступінь конфіденційності) інформації, що циркулює у ТКС, визначається Розроблювачем ТЗ і Замовником спільно.

Оцінка характеристик ТКС і технологічного середовища її експлуатації, виявлення дестабілізуючих чинників і загроз для

інформаційних ресурсів, оцінка імовірностей їхньої прояви і втрат, що пов'язані із можливими реалізаціями загроз, виконуються Розроблювачем на основі теоретичних і спеціальних експериментальних досліджень як самої ТКС, так і середовища її функціонування.

Оцінка припустимих втрат і розробка вимог до необхідного рівня захищеності інформаційних ресурсів ТКС виконується Замовником ТЗ на основі наданих Розроблювачем ТЗ матеріалів, що містять аналіз задач користувачів ТКС із позицій ТЗІ, аналіз загроз для інформаційних ресурсів і потенційних втрат, пов'язаних із їхніми можливими реалізаціями.

На стадії розробки ТЗ на систему ТЗІ у ТКС (далі - ТЗ) виконуються наступні види робіт, що називаються опціями (див. рис.16.1):

- аналіз інформаційного середовища, створеного або створюваного на базі використання ТКС, що потребує захисту (опція 1.1);
- аналіз середовища користувачів ТКС (опція 1.2);
- аналіз середовища потенційних порушників (опція 1.3);
- оцінка основних характеристик технологічного середовища функціонування штатних засобів ТКС до проведення заходів захисту (опція 1.4);
- побудова моделі загроз для інформації у ТКС, включаючи аналіз ризиків, що пов'язані із можливими реалізаціями загроз (опція 1.5);
- визначення необхідного рівня захищеності інформаційних ресурсів ТКС (опція 1.6);
- формування основних технічних вимог до розробки моделі захисту ТКС, яке здійснюється на стадії технічного проектування (опція 1.7).

Розробка ТЗ являє собою двохетапний процес (див. рис.17.2).

Метою робіт, що здійснюються на першому етапі розробки ТЗ, є визначення необхідного рівня довіри до коректності створюваної системи ТЗІ оскільки зміст і обсяг потрібних вихідних даних, виконуваних спеціальних досліджень і аналізів, рівень глибини (деталізації, формалізації) необхідних обгрунтувань однозначно залежать від потрібного рівня довіри до коректності системи

захисту (див. НД ТЗІ 2.5 - 003 - 99).

Змістом робіт, що здійснюються на першому етапі розробки ТЗ, є послідовне виконання опцій 1.1 - 1.6. Аналіз передбачуваних середовищ функціонування ТКС (див. опції1.1 - 1.4) виконується на якісному рівні в загальному вигляді, враховуються основні характеристики об'єктів й особливості взаємовідносин суб'єктів у досліджуваних середовищах.

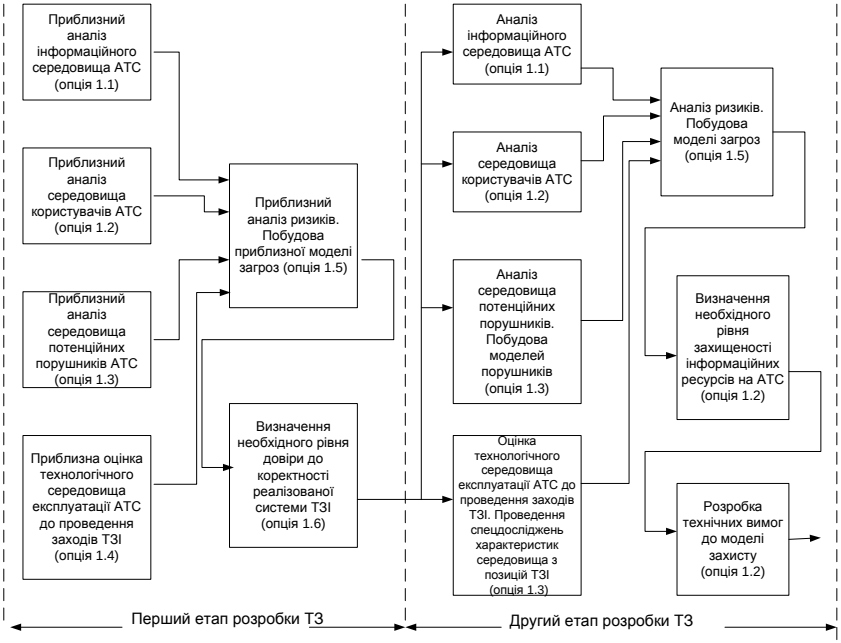


Рис. 17.2 Порядок розробки технічного завдання на систему ТЗІ для АТС

На першому етапі розробки ТЗ визначаються:

– призначення ТКС, що потребує захисту, і основні розв'язувані на її базі задачі;

– обсяги і ступінь важливості (цінності, у т.ч., конфіденційності) оброблюваної і транспортованої інформації;

– структура основних інформаційних взаємозв'язків;

– основні характеристики технологічного середовища експлуатації ТКС, включаючи основні умови, режими і способи опрацювання і транспортування інформації;

– передбачувані межі зон, що потребують захисту;

– рівні інформативних випромінювань і навідів від побічних явищ;

– основні види загроз для інформації і технічні канали реалізації цих загроз;

– основні характеристики організаційних структур потенційних порушників.

У процесі захисту об'єктів особливої важливості вже на першому етапі розробки ТЗ може виникнути необхідність у проведенні спеціальних досліджень з метою експериментальної оцінки реальних характеристик передбачуваного середовища експлуатації ТКС, якщо в результаті попереднього аналізу важко зробити висновки щодо передбачуваних значень параметрів досліджуваного середовища. У таких випадках спецдослідження виконуються відповідно до відомих спеціалізованих методик.

У рамках опцій 1.5 і 1.6 визначаються найбільш суттєві загрози в передбачуваних умовах застосування ТКС, оцінюється співвідношення ресурсних можливостей захисту і потенційних порушників і з оглядом на цінність циркулюючої у ТКС інформації приймається рішення щодо необхідного рівня довіри до коректності створюваної системи ТЗІ.

Вихідними даними для робіт, що виконуються в процесі розробки ТЗ, є:

- підрозділ "Вимоги до функцій (задач), що виконуються системою" і підрозділ "Вимоги до видів забезпечення" технічного завдання на вперше створювані і (або) вже створені автоматизовані системи, в складі яких використовується або планується використання ТКС, що потребує захисту (див. ГОСТ 34.602-89);

- організаційно-розпорядницька й експлуатаційна документація на фрагмент (ділянку) телекомунікаційної мережі, у складі якої використовується або планується використання ТКС, що потребує захисту;

- документи, що містять описи організаційних структур

користувачів (у т.ч., абонентів) ТКС, що потребує захисту;

- документи, що містять описи організаційних структур потенційних порушників;

- комплект технічної документації, включений до складу поставленої конфігурації ТКС;

- нормативні документи ТЗІ.

Результатом виконання першого етапу розробки ТЗ є обране значення необхідного рівня довіри до коректності створюваної системи ТЗІ.

Цілями робіт, що здійснюються на другому етапі розробки ТЗ, є:

– визначення необхідного рівня захищеності інформаційних ресурсів ТКС, що потребує захисту;

– розробка основних технічних вимог до забезпечення ТЗІ з метою їх використання в процесі техно-робочого проектування системи захисту.

Змістом робіт, що здійснюються на другому етапі розробки ТЗ, є виконання опцій 1.1 - 1.7. При цьому зміст і обсяг необхідних вихідних даних, запроваджуваних спеціальних досліджень і аналізів, рівень деталізації і формалізації виконуваних обгрунтувань однозначно залежать від необхідного рівня довіри до коректності системи ТЗІ.

За високих рівнів довірчих оцінок, починаючи з рівня Е4 (для АТС) і вище, необхідно розробити модель політики безпеки і, отже, повною мірою виконати аналіз середовищ функціонування АТС, створити моделі порушників, створити і проаналізувати модель загроз, виконати аналіз ризиків, обгрунтувати необхідний рівень захищеності інформаційних ресурсів ТКС для конкретних або передбачуваних умов її експлуатації.

Результатами виконання другого етапу розробки ТЗ є:

– отриманий перелік суттєвих потенційних загроз для інформаційних ресурсів ТКС із зазначеними гранично припустимими рівнями втрат від їхніх можливих реалізацій (тобто, визначений необхідний рівень захищеності інформаційних ресурсів ТКС);

– основні технічні вимоги до розробки моделі захисту.

У процесі аналізу інформаційного середовища ТКС досліджується:

- характер і зміст задач користувачів і персоналу телекомунікаційної системи;

- структура інформаційних взаємозв'язків;

- об'ємно-часові характеристики і ступінь важливості (цінності, у т.ч., конфіденційності) інформації, що циркулює у ТКС.

Результатом робіт в опції 1.1 є опис профілю інформаційного середовища ТКС, обумовленого як структурований набір можливо різнорідних визначень, показників і параметрів, що характеризує інформаційне середовище ТКС із позицій ТЗІ.

У процесі аналізу середовища користувачів ТКС досліджуються:

- організаційні структури користувачів (абонентів і персоналу системи);

- склад і функціональні обов'язки користувачів;

- повноваження користувачів.

Результат робіт в опції 1.2 - опис профілю середовища користувачів, який задається як структурований набір визначень, показників і параметрів, що характеризує середовище користувачів ТКС із позицій ТЗІ.

У процесі аналізу технологічного середовища ТКС досліджуються:

- основні характеристики ТКС, що потребує захисту;

- характеристики середовища транспортування інформації;

- умови і способи опрацювання інформації штатними засобами ТКС, що потребує захисту із позицій ТЗІ;

- зовнішні чинники середовища експлуатації ТКС (у т.ч., спецдослідження) із позицій ТЗІ.

Результат робіт в опції 1.3 - опис профілю технологічного середовища, який задається як структурований набір визначень, показників і параметрів, що характеризує технологічне середовище експлуатації штатних засобів ТКС.

У процесі аналізу середовища потенційних порушників досліджуються:

- організаційні структури потенційних порушників;

- склад і можливості потенційних порушників, що реалізують загрози для інформації у ТКС;

- моделі потенційних порушників.

Результат робіт в опції 1.4 - опис профілю середовища потенційних порушників, що реалізують загрози для інформації через технічні канали, який задається як структурований набір моделей порушників.

У процесі аналізу середовища функціонування ТКС виконується:

- аналіз ризиків, пов'язаних із можливими реалізаціями загроз, тобто оцінка частостей (імовірностей) проявів потенційних загроз і можливих рівнів втрат, пов'язаних із їхніми проявами, в умовах застосування штатних засобів ТКС до проведення заходів захисту;

- побудова моделі загроз.

Результат робіт в опції 1.5 - побудована модель загроз для інформаційних ресурсів ТКС, що потребують захисту.

За результатами побудови моделі загроз визначається необхідний рівень захищеності інформаційних ресурсів ТКС.

Результат робіт в опції 1.6 - набір суттєвих загроз, стосовно котрих необхідно організувати протидію, з вказівкою гранично припустимих втрат від їхніх можливих реалізацій. Такі вказівки потрібні для визначення рівнів протидії суттєвим загрозам.

На заключному етапі визначаються основні технічні вимоги до розробки моделі захисту ТКС.

Результат робіт в опції 1.7 - основні технічні вимоги до розробки моделі захисту.

17.2.2. Розробка та реалізація техно-рабочего проекту системи ТЗІ у ТКС

У процесі техно-робочого проектування системи ТЗІ у ТКС послідовно розроблюються (див. рис.17.1):

- технічний проект - модель захисту інформаційних ресурсів ТКС (опція 2.1);

- робочий проект - проект комплексу засобів і механізмів захисту (опція 2.2).

На стадії технічного проектування розроблюється модель захисту інформаційних ресурсів ТКС, реалізація якої дозволить забезпечити заданий у ТЗ рівень захищеності інформаційних ресурсів цієї телекомунікаційної системи.

Вибір моделі захисту здійснюється Розроблювачем технічного

проекту і являє собою рішення задачі з мінімізації ресурсів захисту при забезпеченні наведеного в технічному завданні рівня захищеності інформаційних ресурсів ТКС. У результаті визначена сукупність функціональних послуг захисту (ФПЗ), що пропонуються для реалізації в системі ТЗІ, оформлюється у вигляді технічних вимог до розробки КЗМЗ.

Порядок розробки технічного проекту системи ТЗІ показаний на рис.17.3.

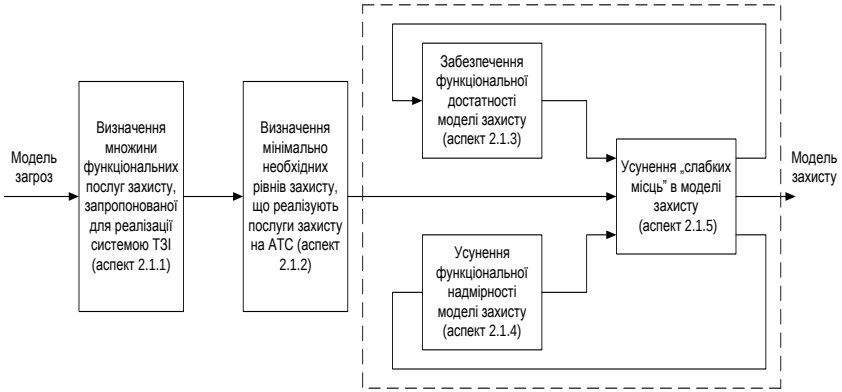


Рис. 17.3 Порядок розробки технічного проекту на систему ТЗІ для АТС

Створення моделі захисту містить у собі проробку наступних аспектів у рамках опції 2.1:

– визначення множини функціональних послуг захисту, які у необхідній мірі протидіють загрозам, що включені в модель загроз (для АТС див. НД ТЗІ 2.5-001-99);

– визначення мінімально необхідних рівнів стійкості механізмів захисту, що реалізують послуги захисту з обраної множини функціональних послуг;

– оптимізація проекта моделі захисту за критеріями дієвості (для АТС див. НД ТЗІ 3.7-002-99);

– забезпечення функціональної достатності моделі захисту;

– усунення функціональної надмірності моделі захисту.

З метою спрощення процесу проектування системи ТЗІ і полегшення сприйняття результатів оцінки захищеності інформації

у ТКС за аналогією з Європейськими Критеріями безпеки (ITSEC) доцільно специфікувати перелік так званих стандартних профілів захищеності інформації у ТКС для різних умов їхнього застосування. Кожний із стандартних профілів характеризується певним набором ФПЗ з визначеними рівнями стійкості їхніх реалізацій обраними механізмами захисту і визначеними рівнями гарантованості коректності як моделі захисту, так і системи ТЗІ в цілому.

У процесі проектування системи ТЗІ за основну (базову) сукупність ФПЗ зручно вибрати специфікований стандартний профіль захищеності інформації, який найкраще відповідає прийнятій моделі захисту, щоб потім доповнити цю сукупність (якщо виникне потреба) відсутніми засобами і механізмами захисту з метою найбільш повного врахування нюансів конкретного застосування ТКС.

Старанність (глибина проробки, ступінь формалізації і деталізації) виконання технічного проекту однозначно залежить від потрібного рівня довіри до коректності розроблювальної системи ТЗІ і визначається специфікаціями, що для АТС наведені в НД ТЗІ 2.5 - 002 - 99 та НД ТЗІ 2.5-003-99.

Результатом технічного проектування є модель захисту інформації у ТКС.

На стадії робочого проектування розроблюється комплекс засобів і механізмів захисту (КЗМЗ), що реалізує обрану модель захисту. Порядок розробки робочого проекту показаний на рис. 17.4.

Для вперше створюваних АС, у складі котрих планується використання ТКС, спочатку виконується вибір ТКС з оглядом на реалізовані у ній ФПЗ таким чином, щоб мінімізувати вартість робіт із створення додаткових механізмів захисту (якщо в цьому виникає потреба). У сукупності зі штатними додаткові механізми повинні забезпечити зазначений у ТЗ рівень захищеності інформації. Іншими словами, необхідно вибрати таку ТКС, штатні засоби захисту котрої (з урахуванням забезпечених гарантій захисту) за інших рівних умов найбільш повним чином реалізовували б отриману за результатами технічного проектування модель захисту. Якщо ТКС вже обрана, то виконується оцінка реалізованих у ній штатних ФПЗ на

відповідність наведеній у технічному проекті моделі захисту. Відсутні послуги реалізуються за допомогою додаткових засобів і механізмів захисту.

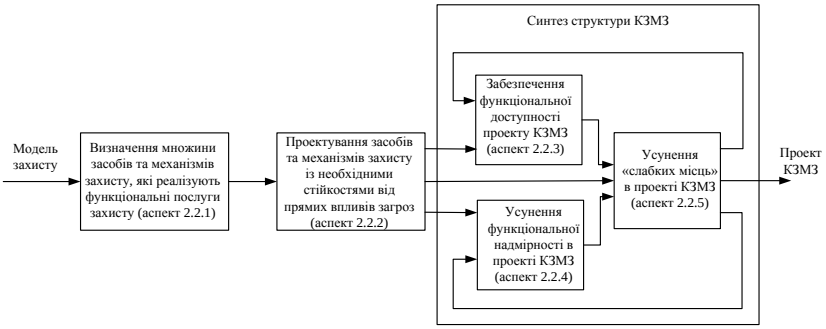


Рис.17 4. Порядок розробки робочого проекту на систему ТЗІ для АТС

Створення проекта КЗМЗ містить у собі проробку в рамках опції 2.2 таких аспектів:

– визначення множини засобів і механізмів захисту, які коректно реалізують функціональні послуги, що включені в модель захисту;

– проектування (вибір) засобів та механізмів захисту із заданими стійкостями (див. НД ТЗІ 1.1-001-99) від прямих впливів загроз;

– усунення "слабких місць" у проекті КЗМЗ з урахуванням передбачуваних умов експлуатації комплексу;

– забезпечення функціональної достатності проекта КЗМЗ;

– усунення функціональної надмірності в проекті КЗМЗ.

Старанність (глибина проробки, рівень обгрунтувань) виконання робочого проекта однозначно залежить від потрібного рівня довіри до коректності розроблювальної системи ТЗІ і для АТС визначається специфікаціями, що наведені в НД ТЗІ 2.5 - 002 - 99 та НД ТЗІ 2.5 - 003 - 99.

Необхідними даними для проектування КЗМЗ є модель захисту, яка розроблена в рамках опції 2.1. Результатом робочого проектування є проект КЗМЗ у КТС, що потребує захисту.

17.3. Впровадження розробленої технічної політики

забезпечення захисту

У процесі реалізації техно-робочого проекту системи ТЗІ у ТКС виконуються наступні види робіт:

- програмна і (або) апаратна реалізація розробленого КЗМЗ, який забезпечує наведений у ТЗ рівень захищеності інформаційних ресурсів ТКС (опція 3.1);
- випробування реалізованого КЗМЗ на відповідність нормативним специфікаціям і проектній документації (опція 3.2);
- оцінка реальних характеристик технологічного середовища функціонування захищеної ТКС після проведення заходів захисту (опція 3.3);
- оцінка ефективності нейтралізації "слабких місць" у захисті (опція 3.4);
- оцінка досягнутого рівня довіри до коректності реалізованої системи ТЗІ у ТКС, що потребує захисту (опція 3.5).

17.3.1. Інсталяція комплекса засобів та механізмів захисту

Для виконання робіт у опціях 3.2 - 3.4 створюється програма та методика випробувань. Зміст програми та методики повинен відповідати ГОСТ 2.106-96.

Механізми захисту, які включені в проект КЗМЗ, але не реалізовані штатними засобами ТКС, що потребує захисту, створюються на базі програмних і (або) апаратних засобів і включаються до складу поточної конфігурації ТКС.

Деякі механізми захисту відповідно до проекту КЗМЗ реалізуються закупними засобами захисту, які повинні бути включені у відомість (перелік) закупних виробів системи ТЗІ.

Рівень захищеності інформації в середовищі виготовлення КЗМЗ однозначно залежить від потрібного рівня довіри до коректності створюваної системи ТЗІ і для АТС визначається специфікаціями, наведеними в НД ТЗІ 2.5 - 002 - 99, НД ТЗІ 2.5 - 003 - 99.

Результатом робіт в опції 3.1 є реалізований КЗМЗ.

17.3.2. Випробування КЗМЗ

Метою робіт, проведених у рамках опції 3.2, є одержання впевненості в тому, що реалізований КЗМЗ відповідає

нормативним специфікаціям (для АТС згідно з НД ТЗІ 2.5-002-99 та НД ТЗІ 2.5-003-99) і проектній документації. Змістом робіт, виконуваних у рамках опції 3.2, є випробування реалізованого КЗМЗ на відповідність нормативним специфікаціям і проектній документації. Обсяг і глибина запроваджуваних випробувань, а також повнота охоплення випробуваннями елементів ТКС залежить від потрібного рівня довіри до коректності системи ТЗІ і визначається специфікаціями, що для АТС наведені в НД ТЗІ 2.5-003-99.

Результат випробувань - підтвердження потрібного рівня довіри до того, що реалізований КЗМЗ відповідає нормативним специфікаціям (для АТС специфікаціям НД ТЗІ 2.5-003-99) і проектній документації.

17.3.3. Оцінка характеристик технологічного середовища функціонування захищеної ТКС

Метою робіт, що здійснюються у рамках опції 3.3, є одержання впевненості в тому, що реальні характеристики технологічного середовища функціонування захищеної ТКС після проведення заходів захисту знаходяться в припустимих діапазонах значень, що вказані у НД. Змістом робіт, виконуваних у рамках опції 3.3, є визначення, у тому числі й експериментальним шляхом згідно із спеціалізованими методиками вимірів сигналів та полів від побічних явищ, реальних характеристик і параметрів середовища функціонування захищеної ТКС і порівняння отриманих оцінок із нормованими припустимими значеннями відповідно до розробленої програми та методики проведення вимірювань.

Обсяг виконуваних спецдосліджень середовища, а також повнота охоплення дослідженнями елементів середовища залежить від потрібного рівня довіри до коректності системи ТЗІ і визначається специфікаціями, що для АТС наведені в НД ТЗІ 2.5-003-99.

Результат оцінки - підтвердження впевненості в тому, що реальні характеристики технологічного середовища функціонування захищеної АТС після проведення заходів захисту знаходяться в припустимих діапазонах значень.

17.3.4. Оцінка ефективності нейтралізації "слабких місць" у захисті

Метою робіт, здійснюваних у рамках опції 3.4, є одержання впевненості в тому, що "слабкі місця" в захисті інформаційних ресурсів ТКС належною мірою задокументовані і нейтралізовані. Змістом робіт, виконуваних у рамках опції 3.4, є:

– випробування захищеної ТКС на можливість виявлення "слабких місць" у конструкції й у методах експлуатації (в тому числі, реалізація тестування "на проникнення");

– випробування реалізованого КЗМЗ на коректність і ефективність нейтралізації виявлених "слабких місць" і "виломів" у захисті.

Оцінка "слабких місць" у захисті повинна здійснюватися відповідно до розробленої програми та методики. Зміст програми та методики - згідно з ГОСТ 2.106-96. Обсяг і глибина випробувань "слабких місць" у захисті однозначно залежать від потрібного рівня довіри до коректності системи ТЗІ і визначаються специфікаціями, що наведені в НД ТЗІ 2.5-003-99. Результат випробувань "слабких місць" - підтвердження впевненості в тому, що в захисті АТС відсутні "виломи", а виявлені "слабкі місця" належним чином задокументовані і нейтралізовані.

17.3.5. Оцінка досягнутого рівня довіри до реалізованої системи захисту

Метою робіт, що здійснюються в рамках опції 3.5, є підтвердження наведеного у ТЗ рівня довіри до коректності реалізованої системи ТЗІ у ТКС, що потребує захисту. Змістом робіт, виконуваних у рамках опції 3.5, є оцінка рівня довіри до коректності реалізованої системи ТЗІ. Для АТС - за методикою, викладеною в НД ТЗІ 3.7-002-99. Ця методика базується на специфікаціях довірчих оцінок, визначених у НД ТЗІ 2.5-003-99. Результат оціночних робіт в межах опції 3.5 - підтвердження того, що отримана оцінка рівня довіри відповідає очікуваному рівню, який наведений у ТЗ.

17.4. Підтримка впровадженої технічної політики забезпечення захисту в період експлуатації ТКС

Одне з основних завдань персоналу, що експлуатує ТКС, у сфері ТЗІ - оцінити достатність і ефективність побудованої моделі захисту, а також повноту, коректність і ефективність реалізації створеним комплексом КЗМЗ функціональних послуг захисту (ФПЗ) у реальних умовах функціонування ТКС.

У процесі виконання оціночних робіт на основі матеріалів ТЗ на систему ТЗІ аналізуються умови, в яких повинна працювати ТКС, оцінюється слушність вибору необхідного рівня захищеності інформаційних ресурсів, структурованого за видами загроз (тобто, оцінюється відповідність між припустимим рівнем втрат, пов'язаних із можливими реалізаціями конкретної множини загроз, і обраною моделлю захисту), і далі на основі матеріалів техно-робочого проекта на систему ТЗІ, технічної документації на ТКС (особливо в частині опису комплекса засобів захисту), програми, методики і протоколів випробувань системи ТЗІ перевіряється ефективність і коректність реалізації обраної моделі захисту.

При цьому під ефективністю реалізації моделі розуміється:

- взаємна узгодженість відображених у моделі ФПЗ між собою;
- спроможність механізмів захисту, що реалізують на практиці задані у моделі ФПЗ, протистояти прямим атакам;
- неможливість практичного використання слабкостей в архітектурі ТКС, тобто відсутність способів відключення, обходу, ушкодження й обману ФПЗ;
- неможливість практичного використання слабкостей в експлуатаційному середовищі КТС, тобто відсутність способів відключення, обходу, ушкодження й обману механізмів захисту експлуатаційного середовища;
- неможливість небезпечного конфігурування або використання ТКС в умовах, коли засоби, що інформують персонал про перехід станції в небезпечний стан, відсутні або дають помилкові показання.

Під коректністю реалізації моделі захисту розуміється кон'юнкція наступних подій:

– проект КЗМЗ містить реалізації усіх без винятку ФПЗ, що включені у модель захисту;

– система ТЗІ, що реально створена на ТКС, містить у собі всі без винятку засоби і механізми захисту, які відображені у проекті КЗМЗ;

– технічний проект системи ТЗІ містить опис ФПЗ, що відповідає нормуючим специфікаціям (для АТС – це НД ТЗІ 2.5-001-99);

– робочий проект системи ТЗІ містить опис механізмів захисту, що відповідає нормуючим специфікаціям (для АТС – це НД ТЗІ 2.5-001-99);

– механізми захисту, що включені в скад КЗМЗ, реально функціонують згідно з специфікаціями робочого проекту та нормуючими специфікаціями (за результатами випробувань системи ТЗІ, зокрема її тестування у процесі екплуатації).

Аналіз слабких місць робиться в контексті забезпечення необхідного рівня захищеності інформаційних ресурсів. Наприклад, можливо примиритися з наявністю таємних каналів передачі інформації, якщо відсутні вимоги до навмисних порушень конфіденційності. Слабкість конкретного захисного механізму стосовно певного виду загроз може не мати значення, якщо вона компенсується іншими засобами забезпечення безпеки.

Якщо в результаті виконання оціночних робіт зроблено висновок про те, що система ТЗІ, яка створена на ТКС, що потребує захисту, реалізована коректно, то необхідно визначити ступінь впевненості в слушності такого висновку. Тут мається на увазі, що висновок про коректність системи ТЗІ може бути зроблений на базі різної повноти і глибини знань про неї. Тому і рівень довіри до результатів оцінки коректності може бути різний.

Наприклад, у НД ТЗІ 2.5 - 003 - 98 для АТС визначаються сім можливих рівнів гарантованості коректності - від ЕО до Е6 (у порядку зростання вимог до глибини оцінки). Рівень ЕО означає відсутність гарантій коректності. На рівні Е1 аналізується лише загальна архітектура АТС - вся інша впевненість у коректності системи захисту повинна бути наслідком функціонального тестування. На рівні Е4 до аналізу залучаються вихідні тексти

програм і схеми апаратури. На рівні Е6 потрібно мати формальний опис загальної архітектури АТС і обраної моделі політики безпеки. Відповідно до принципу безперервності захисту (див. НД ТЗІ 1.1 - 001 - 98) при перевірці коректності аналізується весь життєвий цикл АТС - від проектування до стадії промислової експлуатації включно.

Контрольні питання до сімнадцятої лекції:

1. Через які канали спеціальних впливів можлива реалізація загроз для інформації у ТКС?
2. Що таке якісна недостатність компонентів системи ТЗІ?
3. Що таке закладний пристрій?
4. Що таке модель порушника?
5. Що таке модель загроз для інформаційних ресурсів ТКС?
6. Що таке сертифікований канал можливої реалізації загроз для інформаційних ресурсів ТКС?
7. Що таке слабке місце у захисті?
8. Що таке база захисту ТКС?
9. Що таке тест на проникнення?
10. Викладіть зміст і послідовність робіт з протидії загрозам інформаційним ресурсам та їх нейтралізації у ТКС.
11. У чому полягає розробка політики безпеки (ПБ)?
12. Що складає зміст технічного завдання (ТЗ) на розробку системи ТЗІ?
13. Надайте характеристику процесу розробки моделі захисту.
14. Надайте характеристику процесу розробки комплексу засобів та механізмів захисту (КЗМЗ)?
15. Яким чином впроваджується політика безпеки?
16. Яким чином підтримується політика безпеки?

Література до сімнадцятої лекції:

1)ДСТУ 3396.0-96 - Захист інформації. Технічний захист інформації. Основні положення;
2)ДСТУ 3396.1-96 - Захист інформації. Технічний захист інформації. Порядок проведення робіт;
3)ДСТУ 3396.2-97 - Захист інформації. Технічний захист інформації. Терміни і визначення;

4)НД ТЗІ 3.7-002-99 - Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова);

5)НД ТЗІ 2.5-001-99 - Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту;

6)НД ТЗІ 2.5-002-99 - Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту;

7)НД ТЗІ 2.5-003-99 - Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту;

8)НД ТЗІ 2.7-001-99 - Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт.

САМОСТІЙНЕ ЗАНЯТТЯ ЗА МАТЕРІАЛАМИ ЛЕКЦІЇ №17 . СТВОРЕННЯ СИСТЕМИ ЗАХИСТУ ТА ОЦІНЮВАННЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ РЕСУРСІВ ПРОГРАМНО-КЕРОВАНОЇ АТС

Об'єкти, цілі та основні організаційно-технічні положення щодо технічного захисту інформації (ТЗІ) на телефонних системах з комутацією каналів визначаються положеннями нормативного документу (НД) Державної служби спеціального зв”язку та захисту інформації (ДССЗЗІ) України НД ТЗІ 1.1-001-99.

Об'єктом технічного захисту у системах з комутацією каналів (КС), зокрема на програмно-керованих АТС, є конфіденційна, а також відкрита, але важлива для особи, суспільства і держави інформація, яка зберігається та циркулює на цих КС. Метою створення системи ТЗІ у КС є запобігання за допомогою інженерно-технічних заходів здійсненню загроз інформаційним ресурсам (далі - загроз для інформації) КС.

17.5. Структура АТС з позицій технічного захисту інформації

17.5.1. Структура КС, зокрема АТС, що відображена на рис.16.5,

з позицій ТЗІ розподіляється на дві відносно незалежні підсистеми - підсистема керування станцією та підсистема комутації абонентських і з'єднувальних ліній зв'язку (КАЗЛ).

Підсистема керування станцією містить у собі:

– спеціалізовані пристрої керування, що реалізують принцип програмного керування і складаються, здебільшого, з процесорів, пристроїв внутрішньої і зовнішньої пам'яті, периферійних пристроїв, спеціалізованих модулів керування сигналізацією, опрацюванням викликів, наданням послуг і деяких інших програмно-апаратних компонентів, які є характерними для комп'ютерної техніки;

– термінали обслуговування, що під'єднані до пристроїв керування через канали технологічного обслуговування КС і до підсистеми КАЗЛ - через канали інформаційного обслуговування абонентів.

–

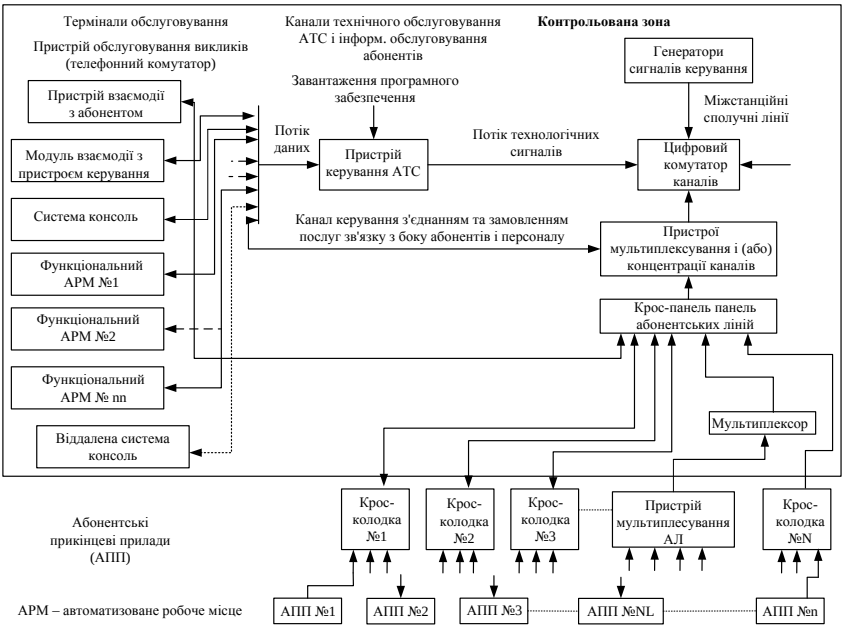


Рис.17.5. Структурна схема системи комутації каналів (КС) з позицій ТЗІ

Підсистема КАЗЛ містить у собі пристрої, що реалізують процеси комутації, мультиплексування та концентрації абонентських і міжстанційних з'єднувальних ліній, а також компоненти устаткування абонентських ліній зв'язку - абонентські прикінцеві пристрої, фізичні лінії зв'язку, пристрої мультиплексування абонентських ліній, станційні абонентські комплекти і т. ін. На виходах підсистеми керування утворюються в реальному часі потоки технологічних сигналів, за допомогою яких має місце процес керування підсистемою КАЗЛ. З іншого боку, абонентські прикінцеві пристрої мають можливість обмінюватися керуючою інформацією з підсистемою керування КС через канали керування з'єднанням і замовленням послуг.

Незалежність вищезгаданих підсистем керування комутаційною системою і КАЗЛ розуміється в тому сенсі, що підмножина загроз для інформації, яка характерна для підсистеми керування, не перетинається з підмножиною загроз, яка характерна для підсистеми КАЗЛ, за передумовою відсутності механізмів реалізації загроз на підсистемі керування з боку підсистеми КАЗЛ і, навпаки, - на підсистемі КАЗЛ з боку підсистеми керування КС.

Коректність такої декомпозиції структури системи з комутацією каналів обумовлена прийнятими щодо них проектними рішеннями, що не передбачають:

- можливостей штатних впливів на підсистему керування з боку абонентських прикінцевих пристроїв, за винятком можливості запуску абонентом задач із фіксованого набору, що реалізують заздалегідь передбачені функції замовлення абонентом додаткових видів послуг, які надаються комутаційною системою;

- можливостей штатних впливів на інформацію в розмовних трактах із боку підсистеми керування, за винятком можливості штатних під'єднань до вже встановлених з'єднань (наприклад, із боку телефонного комутатора або абонентських прикінцевих пристроїв у режимі конференцзв'язків), однак з обов'язковим оповіщенням учасників розмови про всі додаткові підключення до їхніх розмовних трактів (зокрема, фоновими тональними сигналами).

Відносність незалежності вищезгаданих підсистем розуміється в

тому сенсі, що за певних умов внаслідок помилок або некоректних (зокрема, зловмисних) дій, які були допущені на передексплуатаційних стадіях життєвого циклу КС (наприклад, при установці програмних закладок або апаратних закладних пристроїв), або внаслідок якісної недостатності КС, тим не менш, можливі реалізації загроз на підсистемі керування з боку підсистеми КАЗЛ, і, навпаки, - на підсистемі КАЗЛ з боку підсистеми керування КС. Тому для обгрунтування коректності розподілу структури КС на дві вищезгадані підсистеми необхідно надати докази щодо коректності реалізації проекту КС. Такі докази виконуються, як правило, на стадії розробки технічного проекту системи ТЗІ.

17.5.2. Загрози для інформації на КС

Розрізняють наступні види загроз для інформації на КС:

- порушення конфіденційності (тобто, ознайомлення з інформацією обмеженого доступу неавторизованими особами);
- порушення цілісності (тобто, несанкціонована законним власником зміна, підміна або знищення інформації);
- порушення доступності або відмова в обслуговуванні (тобто, позаштатні обмеження в реалізації авторизованими користувачами штатних процедур доступу до інформаційних ресурсів);
- порушення спостережності або керованості (тобто, порушення штатних процедур ідентифікації і (або) автентифікації, контролю доступу і контролю дій користувачів, повна або часткова втрата керованості комутаційною системою);
- несанкціоноване користування інформаційними ресурсами КС (зокрема, несанкціоноване користування послугами, що надаються КС і т. ін.).

Такий вид загроз як витік інформації (тобто, неконтрольоване поширення інформації, що веде до несанкціонованого її одержання) розглядається як окремий випадок прояву порушень конфіденційності.

Такий вид загроз як блокування інформації (тобто, порушення можливості санкціонованого доступу до інформації) розглядається як окремий випадок прояву порушень доступності.

Загрози для інформації на КС можуть здійснюватися:

– шляхом несанкціонованого доступу (НСД) до інформаційних ресурсів КС, коли порушуються встановлені правила розмежування доступу (ПРД) і (або) правові норми з метою реалізації будь-якої з видів загроз для інформації на КС через канал спеціального неприпустимого регламентом впливу за допомогою штатних засобів доступу на устаткування, програми, дані та процеси (див. далі за текстом);

– через канал спеціального неприпустимого регламентом впливу із застосуванням штатних основних або додаткових програмних і (або) технічних засобів КС (але не штатних засобів доступу) на устаткування, програми, дані і процеси, що утворений з метою реалізації будь-якої з видів загроз для інформації на КС;

– через канал спеціального неприпустимого регламентом впливу на параметри середовища функціонування КС, що утворений з метою порушень доступності до інформації на КС;

– через канал спеціального впливу позаштатними програмними і (або) програмно-технічними засобами на елементи устаткування, програми, дані і процеси на КС, встановленими на передексплуатаційних стадіях і в процесі її експлуатації, з метою реалізації будь-якої з видів загроз для інформації на КС;

– через канал спеціального впливу на компоненти КС за допомогою закладних пристроїв і (або) програмних закладок, впроваджених у середовище функціонування КС на передексплуатаційних стадіях і в процесі її експлуатації з метою реалізації будь-яких з видів загроз для інформації на КС;

– через канал побічних електромагнітних випромінювань і навідів (ПЕМВН) із метою порушень конфіденційності інформації на КС;

– через канал побічних акусто-електричних перетворень інформативних сигналів на прикінцевому устаткуванні ліній зв'язку з метою порушень конфіденційності інформації на КС;

– через кількісну і (або) якісну недостатність компонентів і (або) всієї КС у цілому з метою реалізації будь-якої з видів загроз для інформації на КС;

– за рахунок використання випадкових збоїв і відмов у роботі устаткування КС з метою реалізації будь-яких з видів загроз для інформації на КС;

– за рахунок використання помилок і некоректних (зокрема, зловмисних) дій відповідальних осіб при збереженні критичної інформації на фізичних носіях з метою реалізації будь-яких з видів загроз для інформації на КС.

17.5.3. Моделі порушників

За порушників на КС розглядаються суб'єкти, внаслідок навмисних або випадкових дій котрих, і (або) випадкові події, внаслідок настання яких можливі реалізації загроз для інформації.

Розглядаються три групи моделей порушників на КС. Перша група містить у собі моделі порушників, що реалізують загрози на одній підсистемі КС з боку іншої підсистеми. Друга група містить у собі моделі порушників, що реалізують загрози на підсистемі керування КС. Третя група містить у собі моделі порушників, що реалізують загрози на підсистемі КАЗЛ КС.

Передбачається, що порушник - суб'єкт є кваліфікованим фахівцем, володіє всією технічною інформацією про КС і, зокрема, про системи і можливі засоби її захисту, а порушник - випадкова подія має найгірший (із позицій власників інформації, що захищається) закон розподілу.

Кодифікатор моделей порушників на КС наданий у таблиці 16.1.

Таблиця 16.1

Код моделі порушника	Найменування моделі порушника
	Перша група моделей (для порушників, які створюють загрози на одній підсистемі КС при впливах з боку іншої підсистеми)
МН1.01	Модель порушника ПРД до інформаційних ресурсів підсистеми керування КС,який діє з боку абонентських ліній
МН1.02	Модель порушника, який використовує помилки або некоректні дії суб'єктів, що допущені на будь-якій із стадій життєвого циклу КС, з метою реалізації загроз на підсистемі керування шляхом впливу на

Код моделі порушника	Найменування моделі порушника
	інформацію з боку підсистеми КАЗЛ
МН1.03	Модель порушника, який використовує програмні і (або) технічні позаштатні пристрої, що встановлені на підсистемі керування комутаційною системой, шляхом їхньої активізації через спеціальні канали впливу з боку підсистеми КАЗЛ
МН1.04	Модель порушника, який використовує програмно-технічні позаштатні пристрої, що встановлені на підсистемі КАЗЛ КС, шляхом їхньої активізації через спеціальні канали впливу з боку підсистеми керування
МН1.05	Модель порушника, який використовує якісну недостатність інформаційно-уразливих режимів, функцій і послуг, що надоються КС, для реалізації загроз на підсистемі КАЗЛ з боку підсистеми керування
	Друга група моделей (для порушників, які створюють загрози на підсистемі керування КС)
МН2.01	Модель порушника ПРД
МН2.02	Модель порушника, який реалізує неприпустимі впливи через штатні засоби КС (але не штатні засоби доступу) на елементи підсистеми керування комутаційною системою
МН2.03	Модель порушника, який реалізує неприпустимі впливи на параметри середовища експлуатації КС з метою порушень доступності до підсистеми керування
МН2.04	Модель порушника, що впливає позаштатними засобами на елементи підсистеми керування КС
МН2.05	Модель порушника, який використовує закладні пристрої і (або) програмні закладки, що встановлені на елементах підсистеми керування
МН2.06	Модель порушника через канали ПЕМВН
МН2.07	Модель порушника через канали побічних акусто-

Код моделі порушника	Найменування моделі порушника
	електричних перетворень на терміналах обслуговування КС
МН2.08	Модель порушника, який використовує помилки або некоректні дії суб'єктів доступу до підсистеми керування або її документації, що допущені на передексплуатаційних стадіях життєвого циклу КС
МН2.09	Модель порушника, який використовує помилки або некоректні дії персоналу КС при збереженні критичної інформації на фізичних носіях
МН2.10	Модель порушника, який використовує випадкові збої і відмови в роботі підсистеми керування КС
	Третя група моделей (для порушників, які створюють загрози на підсистемі КАЗЛ КС)
МН3.01	Модель порушника, який реалізує неприпустимі впливи через штатні засоби станції на елементи підсистеми КАЗЛ КС
МН3.02	Модель порушника, який реалізує неприпустимі впливи на параметри середовища експлуатації КС з метою порушень доступності до елементів підсистеми КАЗЛ КС
МН3.03	Модель порушника, який впливає позаштатними засобами на елементи підсистеми КАЗЛ АТС
МН3.04	Модель порушника, який використовує програмні закладки і (або) апаратні закладні пристрої, що встановлені на підсистемі КАЗЛ КС
МН3.05	Модель порушника через канали ПЕМВН
МН3.06	Модель порушника через канали побічних акусто-електричних перетворень в абонентських прикінцевих пристроях.
МН3.07	Модель порушника, який використовує помилки або некоректні дії суб'єктів доступу до підсистеми КАЗЛ або її документації, що допущені на передексплуатаційних стадіях життєвого циклу КС

Код моделі порушника	Найменування моделі порушника
МН3.08	Модель порушника, який використовує випадкові збої і відмови в роботі елементів підсистеми КАЗЛ КС

17.5.4. Рівні можливостей порушників

Рівні можливостей порушника для моделі МН1.01

Передбачається, що порушник намагається порушити встановлені ПРД до ресурсів підсистеми керування КС з боку підсистеми КАЗЛ, маючи в розпорядженні штатний абонентський прикінцевий пристрій. Порушник має при цьому єдиний рівень можливостей - можливість вибору прикладної задачі і ведення в її середовищі діалогу, як-от: запуску задач (програм) із фіксованого набору, що реалізують заздалегідь передбачені функції (послуги) щодо опрацювання інформації; діалогу в процесі виконання активних задач; реконфігурації прикінцевого устаткування і наданих послуг засобами прикладного програмного забезпечення.

Для порушника в рамках розглянутої моделі виключається можливість:

- створення і запуску власних програм;
- керування функціонуванням КС (зокрема, реконфігурацією устаткування) засобами системного програмного забезпечення;
- включення до складу устаткування підсистеми керування КС позаштатних програмних і (або) технічних засобів.

Рівні можливостей порушників для моделі МН1.02

У рамках моделі МН1.02 розрізняють порушника - джерела помилок або некоректних дій і порушника - реалізатора загроз для інформації на підсистемі керування КС, що діє з боку підсистеми КАЗЛ.

Передбачається, що порушник -джерело помилок або некоректних дій може мати статус авторизованого користувача з будь-яким припустимим рівнем повноважень і може мати можливість доступу до будь-яких штатних механізмів взаємодії авторизованого користувача із середовищем розробки, виготовлення і (або) експлуатації КС на будь-якій із стадій її

життєвого циклу. Порушник - реалізатор загроз також може мати статус авторизованого користувача з будь-яким припустимим рівнем повноважень, але діє тільки на стадії експлуатації КС.

17.5.5. Основні способи реалізації загроз для інформації

До основних способів порушень у рамках моделі МН1.01 відносяться:

- безпосереднє звертання до об'єктів доступу шляхом ушкодження системи ідентифікації й автентифікації користувачів (наприклад, шляхом добору вірного пароля і т.ін.);

- маніпуляція штатними засобами доступу підсистеми КАЗЛ, що дозволяє внаслідок кількісної і (або) якісної недостатності компонентів КС (або недосконалості архітектури або конструкції КС у цілому) здійснити доступ до об'єктів підсистеми керування комутаційною системою (зокрема, шляхом створення каналів доступу до інформаційних ресурсів в обхід засобів і механізмів захисту);

- модифікація засобів захисту на підсистемі КАЗЛ, що дозволяє здійснити НСД до об'єктів на підсистемі керування.

До основного способу порушень у рамках моделі МН1.02 відноситься маніпуляція штатними і (або) спеціально встановленими програмними і (або) технічними засобами на підсистемі КАЗЛ КС, що дозволяє внаслідок помилок або некоректних дій суб'єктів доступу до середовищ проектування, виготовлення або експлуатації КС реалізувати загрози для інформації.

До основного способу порушень у рамках моделі МН1.03 відноситься установка позаштатних апаратних і (або) інсталяція позаштатних програмних засобів у підсистемі керування на передексплуатаційних стадіях життєвого циклу КС з наступною їхньою активізацією через спеціальні канали впливу з боку підсистеми КАЗЛ на стадії промислової експлуатації системи з метою реалізації будь-якої з видів загроз.

До основного способу порушень у рамках моделі МН1.04 відноситься установка програмно-апаратних позаштатних пристроїв на підсистемі КАЗЛ КС на будь-якій із стадій життєвого циклу КС з наступною їхньою активізацією через спеціальні

канали впливу з боку підсистеми керування на стадії промислової експлуатації системи з метою реалізації будь-якої з видів загроз.

До основного способу порушень у рамках моделі МН1.05 відноситься використання "слабких місць" в захисті або модифікація з боку підсистеми керування порядку (або умов) роботи інформаційно-уразливих режимів, функцій і послуг, що надаються комутаційною системою, з метою реалізації загроз на підсистемі КАЗЛ.

До основних способів порушень у рамках моделі МН2.01 відносяться:

- безпосереднє звертання до об'єктів доступу шляхом ушкодження системи ідентифікації й автентифікації користувачів (наприклад, шляхом добору вірного пароля і т.ін.);

- штатна маніпуляція штатними засобами підсистеми керування, що дозволяє внаслідок кількісної і (або) якісної недостатності компонентів КС (або недосконалості архітектури або конструкції КС у цілому) здійснити доступ до об'єктів підсистеми керування системою;

- позаштатна маніпуляція штатними засобами підсистеми керування, що дозволяє здійснити доступ до об'єктів на підсистемі керування (зокрема, шляхом створення каналів доступу до інформаційних ресурсів, що захищаються, в обхід засобів захисту);

- модифікація засобів захисту на підсистемі керування системою, що дозволяє здійснити НСД до об'єктів на підсистемі керування.

До основного способу порушень у рамках моделі МН2.02 відноситься неприпустимий вплив через штатні засоби КС (але не штатні засоби доступу – системні термінали, віддалені засоби доступу через модеми і т.ін.) на елементи системи керування системою з метою реалізації будь - якої із загроз.

До основного способу порушень у рамках моделі МН2.03 відноситься маніпуляція засобами впливу на параметри середовища експлуатації КС з метою організації навмисних збоїв і відмов у роботі КС шляхом виводу параметрів устаткування підсистеми керування сиситемою за межі штатних значень.

До основного способу порушень у рамках моделі МН2.04 відноситься вплив позаштатними технічними або програмно-

технічними засобами на елементи підсистеми керування КС з метою реалізації будь-якої з видів загроз.

До основного способу порушень у рамках моделі МН2.05 відноситься установка апаратних закладних пристроїв і (або) інсталяція програмних закладок на підсистемі керування на будь-якій із стадій життєвого циклу КС з наступною їхньою активізацією на стадії промислової експлуатації системи з метою реалізації будь-якої із основних видів загроз на КС.

До основного способу порушень у рамках моделі МН2.06 відноситься прийом і виділення інформативних параметрів ПЕМВН від елементів підсистеми керування системою (зокрема, від терміналів обслуговування, периферійних пристроїв і т.ін.).

До основних способів порушень у рамках моделі МН2.07 відносяться:

- зняття інформативних сигналів із комунікаційних ліній, що утворюються на виході терміналів обслуговування КС внаслідок побічних акусто-електричних перетворень;

- модуляція штучно створюваного несучого коливання інформативними сигналами в лінії ("ВЧ -накачка") з метою полегшення процесу транспортування знятих сигналів за межі контрольованої зони.

До основного способу порушень у рамках моделі МН2.08 відноситься маніпуляція штатними і (або) спеціально встановленими програмними і (або) технічними засобами на підсистемі керування системою, що дозволяє внаслідок помилок або некоректних дій суб'єктів доступу реалізувати будь-яку із основних видів загроз на КС.

До основних способів порушень у рамках моделі МН2.09 відносяться:

- несанкціоноване ознайомлення із критичною інформацією, що зберігається на фізичних носіях, з метою реалізації будь-якої із загроз;

- порушення цілісності критичної інформації.

До основного способу порушень у рамках моделі МН2.10 відноситься маніпуляція штатними і (або) спеціально встановленими програмними і (або) технічними засобами на підсистемі керування КС, що дозволяє використовувати випадкові

збої і відмови в роботі КС з метою реалізації будь-якої із основних видів загроз.

До основного способу порушень у рамках моделі МН3.01 відноситься позаштатний вплив штатними технічними або програмно-технічними засобами на елементи підсистеми КАЗЛ КС з метою реалізації будь-якої із видів загроз.

До основного способу порушень у рамках моделі МН3.02 відноситься маніпуляція засобами впливу на параметри середовища експлуатації КС з метою організації навмисних збоїв і відмов у роботі КС шляхом виводу параметрів устаткування підсистеми КАЗЛ КС за межі штатних значень.

До основного способу порушень у рамках моделі МН3.03 відноситься безпосереднє під'єднання (гальванічне, індуктивне, ємнісне і т.ін.) апаратури прослуховування до абонентської лінії або крос-панелі з наступним записом знятої інформації на фізичні носії і (або) її передачею за межі контрольованої зони через схований канал передачі.

До основного способу порушень у рамках моделі МН3.04 відноситься установка програмних закладок і (або) апаратних закладних пристроїв на підсистемі КАЗЛ на будь-якій із стадій життєвого циклу КС з наступною їхньою активізацією через канали спеціального впливу на стадії промислової експлуатації станції з метою реалізації будь-якої із видів загроз на КС.

До основних способів порушень у рамках моделі МН3.05 відносяться:

- прийом і виділення інформативних параметрів побічних електромагнітних випромінювань від елементів підсистеми КАЗЛ (в основному, від цифрових абонентських ліній) як усередині, так і поза межами контрольованих зон;

- прийом і виділення інформативних параметрів побічних електромагнітних навідів від елементів підсистеми КАЗЛ (зокрема, від цифрових абонентських ліній) у ланцюгах електроживлення, пожежної й охоронної сигналізації і т. ін.;

- зняття інформативних сигналів - електромагнітних навідів від джерел інформативних випромінювань, що знаходяться в зонах прикінцевих абонентських пристроїв, на абонентських лініях зв'язку КС.

До основних способів порушень у рамках моделі МН3.06 відносяться:

- зняття інформативних сигналів з аналогових абонентських ліній, що утворюються на виході прикінцевих пристроїв в результаті побічних акусто-електричних перетворень у режимі чекання телефонного виклику (у режимі "покладеної трубки");

- модуляція штучно створюваного несучого коливання інформативними сигналами в аналоговій абонентської лінії ("ВЧ-накачка") з метою полегшення процесу транспортування знятих сигналів за межі контрольованої зони;

- демодуляція інформативної обгинаючої сигналів лінійного коду в цифрових абонентських лініях, утвореної через побічні акусто-електричні перетворення в цифрових прикінцевих пристроях, із наступним записом знятої інформації на фізичні носії і (або) її передачею за межі контрольованої зони через схований канал передачі.

До основного способу порушень у рамках моделі МН3.07 відноситься маніпуляція штатними і (або) спеціально встановленими програмними і технічними засобами на підсистемі КАЗЛ, що дозволяє внаслідок помилок або некоректних дій суб'єктів доступу реалізувати будь-яку із видів загроз.

До основного способу порушень у рамках моделі МН3.08 відноситься маніпуляція штатними і (або) спеціально встановленими програмними і (або) технічними засобами на підсистемі КАЗЛ КС, що дозволяє використовувати випадкові збої і відмови в роботі КС з метою реалізації будь-якої із видів загроз.

17.5.6. Види забезпечення систем ТЗІ на КС

Забезпечення систем ТЗІ на КС здійснюється:

- сукупністю технічних і (або) програмних підсистем захисту, що функціонують на стадії її промислової експлуатації;

- системою організаційно-технічних заходів;

- системою ліквідації наслідків реалізованих загроз для інформації на КС;

- системою керування засобами ТЗІ.

Підсистеми захисту на КС класифікуються за способами здійснення загроз і в сукупності повинні забезпечувати реалізацію

на практиці обраної моделі захисту.

Система організаційно-технічних заходів, що здійснюється на всіх стадіях життєвого циклу КС, повинна знизити рівні кількісної і якісної недостатності компонентів і всієї КС у цілому до можливих і (або) припустимих значень.

Система ліквідації наслідків реалізованих загроз для інформації, що являє собою сукупність програмно-апаратних засобів і відповідних організаційних заходів, повинна знизити рівень втрат від реалізованих загроз для інформації до можливих і (або) припустимих меж.

Система керування засобами ТЗІ повинна забезпечувати безперервний контроль і підтримку певного рівня захищеності інформації на КС на стадії її промислової експлуатації.

Шляхи реалізації систем ТЗІ залежать від конкретних особливостей застосування КС, а ресурси, що пов'язані з ТЗІ, включаються в об'єкти доступу і, отже, потребують захисту.

17.5.7. Функції систем захисту

Системи ТЗІ у КС виконують функції, що забезпечують реалізацію визначеної номенклатури функціональних послуг захисту згідно з ISO 7498-2 (Рекомендацією X.800 МСЕ-Т) та НД ТЗІ 2.5-001-99.

Основними функціями підсистем захисту від несанкціонованих впливів через штатні засоби доступу є:

- реалізація ПРД суб'єктів і їхніх процесів із боку моніторів обслуговування до програм, даних, процесів і пристроїв, що встаноалені на підсистемі керування КС;
- реалізація ПРД суб'єктів і їхніх процесів із боку телефонних комутаторів і прикінцевих абонентських пристроїв до сервісних функцій і послуг КС;
- контроль доступу до підсистеми керування комутаційною системою з боку віддалених терміналів обслуговування;
- ізоляція програм, що виконуються в інтересах суб'єкта, від інших суб'єктів;
- керування потоками даних і команд з метою запобігання помилкових з'єднань, помилкового надання послуг і відмов в обслуговуванні;

- ідентифікація й упізнання (автентифікація) суб'єктів;

- реєстрація дій суб'єкта і його процесу;

- надання можливостей вилучення або включення нових суб'єктів і об'єктів доступу , а також зміни повноважень суб'єктів;

- реакція на спроби НСД, наприклад, сигналізація, блокування, знищення ресурсу, відновлення після НСД;

- шифрація інформаційних ресурсів;

- тестування засобів захисту від НСД;

- очищення робочих областей пам'яті ЕОМ після завершення роботи з даними, що захищаються;

- облік вихідних друкарських і графічних форм і твердих копій;

- контроль цілісності програмної й інформаційної частин системи розмежування доступу (СРД).

Основними функціями підсистем захисту від позаштатних впливів через штатні основні або додаткові програмні і (або) технічні засоби КС є:

- виявлення позаштатних впливів на елементи устаткування, програми, дані і процеси;

- реєстрація позаштатних впливів;

- реакція на спроби позаштатних впливів, наприклад, сигналізація, блокування, знищення ресурсу, відновлення після позаштатних впливів;

- моніторинг з метою виявлення позаштатних впливів;

- ідентифікація і розпізнавання процесів;

- реалізація ПРД до інформаційних ресурсів не тільки для процесів, що ініціюються з боку терміналів обслуговування, телефонних комутаторів і прикінцевих абонентських пристроїв, але і для процесів, що ініціюються з боку потенційно небезпечних місць позаштатних впливів через штатні основні або додаткові програмні і (або) технічні засоби КС;

- контроль цілісності програмної й інформаційної частин засобів захисту від позаштатних впливів;

- тестування засобів захисту від позаштатних впливів.

Основними функціями підсистем захисту від позаштатних впливів на параметри середовища експлуатації КС є:

- виявлення позаштатних впливів на параметри середовища експлуатації КС;

- реєстрація таких позаштатних впливів;

- реакція на спроби таких позаштатних впливів, наприклад, сигналізація, блокування, відновлення після позаштатних впливів;

- моніторинг з метою виявлення позаштатних впливів;

- введення в дію засобів протидії непередбаченим змінам параметрів середовища експлуатації КС;

- керування засобами нейтралізації позаштатних впливів на параметри середовища експлуатації КС (вмикання /вимикання і т.ін.);

- контроль цілісності апаратної, програмної й інформаційної частин засобів захисту від позаштатних впливів;

- тестування засобів захисту від позаштатних впливів.

Основними функціями підсистем захисту від впливів з використанням позаштатних технічних і (або) програмно-технічних засобів на елементи устаткування в процесі експлуатації КС є:

- виявлення впливів позаштатними засобами на елементи устаткування;

- реєстрація таких позаштатних впливів;

- реакція на спроби таких позаштатних впливів, наприклад, сигналізація, блокування, нейтралізація спроб реалізації загроз, знешкодження (вивід із працездатного стана) атакуючої апаратури, відновлення після позаштатних впливів;

- керування засобами нейтралізації позаштатних впливів на елементи устаткування КС (умикання/вимикання і т.ін.);

- контроль цілісності апаратної, програмної й інформаційної частин засобів системи захисту;

- тестування засобів системи захисту.

Основними функціями підсистем захисту від впливів позаштатними програмними і (або) програмно-технічними засобами на програми, дані і процеси на КС, що встановлені в процесі її експлуатації, є:

- виявлення впливів позаштатними засобами на програми, дані і процеси на КС;

- реєстрація таких позаштатних впливів;

- реакція на спроби таких позаштатних впливів, наприклад, сигналізація, блокування, відновлення після позаштатних впливів;

- моніторинг з метою виявлення позаштатних впливів;

- ідентифікація і розпізнавання процесів;

- реалізація ПРД до інформаційних ресурсів КС для процесів, що ініціюються позаштатними програмними і (або) програмно-технічними засобами;

- контроль цілісності апаратної, програмної й інформаційної частин засобів підсистеми захисту;

- тестування засобів підсистеми захисту.

Основними функціями підсистем захисту від впливів закладних пристроїв і програмних закладок є:

- виявлення закладних пристроїв і програмних закладок; - реєстрація впливів закладних пристроїв і програмних закладок;

- нейтралізація (знешкодження) закладних пристроїв і програмних закладок;

- реакція на впливи закладних пристроїв і програмних закладок, наприклад, сигналізація, блокування, нейтралізація спроб реалізації загроз, відновлення після впливів;

- контроль цілісності засобів підсистеми захисту;

- тестування засобів підсистеми захисту.

Основними функціями технічних або програмно-технічних підсистем захисту від витоків інформації через канали ПЕМВН є:

- виявлення ПЕМВН від елементів КС (головним чином, випромінювань від абонентських ліній і терміналів обслуговування);

- виявлення електромагнітних навідів в елементах КС (головним чином, в абонентських лініях) від джерел інформативних випромінювань у зонах розміщення елементів КС;

- придушення (ослаблення, екранування) ПЕМВН від елементів КС;

- придушення електромагнітних навідів в елементах КС від джерел інформативних випромінювань у зонах розміщення елементів КС;

- нейтралізація інформативних складових ПЕМВН (наприклад, маскуючим шумоподібним сигналом) від елементів КС;

- нейтралізація електромагнітних навідів в елементах КС від джерел інформативних випромінювань у зонах розміщення елементів КС;

- моніторинг з метою виявлення перевищень припустимих

значень ПЕМВН;

- тестування засобів підсистеми захисту від витоку через канали ПЕМВН.

Основними функціями технічних засобів захисту від витоків інформації через канали побічних акусто-електричних перетворень є:

- виявлення інформативних сигналів - продуктів побічних акусто-електричних перетворень на виході прикінцевих пристроїв аналогових абонентських ліній в режимі чекання виклику;

- виявлення інформативних сигналів акусто-електричних перетворень у цифрових абонентських лініях (як цифрових, так і аналогових складових);

- виявлення інформативних сигналів - продуктів побічних акусто-електричних перетворень на виході термінальних пристроїв підсистеми керування станцією;

- виявлення сторонніх високочастотних коливань (так званих сигналів "ВЧ-накачки") в абонентських і термінальних лініях зв'язку;

- виявлення випромінювань при "ВЧ-накачці" від абонентських ліній;

- придушення (ослаблення) сигналів акусто-електричних перетворень в аналогових абонентських лініях;

- придушення сигналів акусто-електричних перетворень у цифрових абонентських лініях(як цифрових, так і аналогових складових);

- придушення сигналів акусто-електричних перетворень у термінальних лініях зв'язку підсистеми керування станцією;

- придушення сигналів " ВЧ-накачки" і випромінювань при "ВЧ-накачці" від абонентських ліній;

- нейтралізація інформативних сигналів акусто-електричних перетворень в аналогових абонентських лініях у режимі чекання виклику;

- нейтралізація інформативних сигналів акусто-електричних перетворень у цифрових абонентських лініях (як цифрових, так і аналогових складових);

- нейтралізація інформативних сигналів акусто-електричних перетворень у термінальних лініях підсистеми керування станцією;

- моніторинг з метою виявлення сигналів "ВЧ-накачки" в абонентських лініях зв'язку;

- моніторинг з метою виявлення випромінювань при "ВЧ - накачці" від абонентських ліній зв'язку;

- тестування засобів підсистеми захисту від витоку через канали побічних акусто-електричних перетворень.

Основними функціями підсистем захисту від якісної недостатності інформаційно уразливих режимів, функцій і послуг, що надаються КС, є:

- ідентифікація і виявлення моментів активізації інформаційно уразливих режимів, функцій і послуг;

- сигналізація (оповіщення суб'єктів) про активний стан інформаційно уразливих режимів, функцій і послуг;

- придушення каналів витоку інформації в інформаційно уразливих режимах, функціях і послугах;

- контроль цілісності програмної й інформаційної частин засобів підсистеми захисту від якісної недостатності;

- тестування засобів підсистеми захисту від якісної недостатності.

Основними функціями підсистем захисту від збоїв і відмов у роботі АТС є:

- виявлення збоїв і відмов;

- реєстрація збоїв і відмов;

- аварійне завершення активних процесів;

- керування надлишковими ресурсами з метою протидії збоям і відмовам у роботі АТС;

- контроль цілісності програмної й інформаційної частин засобів підсистеми захисту від збоїв і відмов;

- тестування засобів підсистеми захисту від збоїв і відмов.

Основними функціями програмних і (або) технічних підсистем захисту від загроз у системах збереження інформації на фізичних носіях є:

- виявлення спроб несанкціонованого впливу на інформацію;

- реєстрація спроб впливу на інформацію;

- реакція на спроби несанкціонованих впливів, наприклад, сигналізація, відмова в доступі, знищення інформації, відновлення після впливів;

- ідентифікація й автентифікація суб'єктів доступу;
- реалізація ПРД до інформаційних ресурсів на фізичних носіях;
- шифрація інформаційних ресурсів;
- контроль цілісності програмної й інформаційної частин засобів підсистеми захисту;
- тестування засобів підсистеми захисту.

Основними функціями систем ліквідації наслідків реалізованих загроз для інформації на КС є:
- виявлення фактів реалізації загроз;
- реєстрація фактів реалізації загроз;
- реакція на факти реалізації загроз, наприклад, індикація, оповіщення, локалізація і (або) нейтралізація наслідків;
- відновлення після реалізації загроз;
- контроль цілісності програмної й інформаційної частин системи ліквідації наслідків реалізованих загроз;
- класифікація реалізованих загроз і їхнього статистичного опрацювання за певні періоди функціонування КС;
- тестування засобів системи ліквідації наслідків реалізованих загроз.

Основними функціями систем керування засобами ТЗІ є:
- досягнення відповідності прийнятих (затверджених) моделей порушників до реальних загроз для інформаційних ресурсів, які можуть мати місце у конкретних поточних умовах застосування КС;
- досягнення адекватності прийнятої (затвердженої) моделі захисту прийнятим (затвердженим) моделям порушників;
- керування засобами ТЗІ в реальному масштабі часу з метою підтримки певного рівня захищеності інформаційних ресурсів КС;
- виявлення моментів появи дестабілізуючих чинників, спроб реалізації загроз для інформаційних ресурсів КС;
- реакція на появу дестабілізуючих чинників і спроби реалізації загроз (наприклад, оповіщення, реєстрація, вмикання засобів захисту т.ін.);
- тестування інформаційних ресурсів і засобів ТЗІ, включаючи засоби керування системою ТЗІ;
- моніторинг інформаційних ресурсів і засобів ТЗІ;
- контроль цілісності засобів ТЗІ, включаючи засоби керування

системою ТЗІ.

17.5.8. Функціональні послуги захисту, що надаються КС

Функціональна послуга захисту (ФПЗ) являє собою взаємопов'язаний набір виконуваних у середовищі експлуатації КС елементарних функцій, що дозволяє протистояти певній множині загроз для інформації.

У найпростішому випадку ФПЗ є одна елементарна функція, спрямована на протидію визначеній одній загрозі.

З позицій ТЗІ КС разом із реалізованою на ній системою захисту розглядається як набір ФПЗ.

Нормовані специфікації ФПЗ, структуровані за видами загроз для інформації і за способами здійснення цих загроз, наведені в НД ТЗІ 2.5-001-99 .

У ТЗ та ТУ на КС повинні бути наведені вимоги до ФПЗ згідно з НД ТЗІ 2.5-001-99.

17.5.9. Засоби і механізми захисту, що реалізуються на КС

ФПЗ на КС здійснюються за допомогою конкретних засобів і механізмів. Засоби і механізми захисту необхідно розглядати в двох аспектах - із позицій їхньої ефективності і коректності. При цьому під ефективністю засобу або механізму захисту розуміється його спроможність протистояти як прямим атакам, так і всіляким лазівкам, що пов'язані з роботою засобу або механізму захисту в конкретних умовах застосування (зокрема, спроможність протистояти відключенням, обходам, ушкодженням, обманам, провокуванням і т.ін.). Під коректністю засобу або механізму захисту розуміється його спроможність правильно реалізувати визначену ФПЗ.

Спроможність механізму захисту протистояти прямим атакам (тобто, спробам його безпосереднього злому) називається стійкістю (потужністю) механізму. З метою оцінки захищеності КС специфікуються три рівня стійкості механізмів захисту (базовий, середній і високий). Нормовані специфікації рівнів стійкості механізмів захисту наведені в НД ТЗІ 2.5 - 001 - 99 .

17.6. Порядок виконання робіт з ТЗІ на АТС

Порядок виконання робіт з ТЗІ на КС, зокрема на АТС, регламентується ДСТУ 3396.1-96 і НД ТЗІ 2.7-001-99.

17.7. Оцінка ефективності захисту інформаційних ресурсів АТС

Для одержання впевненості в тому, що інформаційні ресурси КС , зокрема АТС, захищені з очікуваною якістю від витоку, спеціальних впливів і НСД, необхідно підтвердження досягнутого рівня ефективності такого захисту з боку незалежного оцінювача.

Згідно з критеріями ITSEC та НД ТЗІ 2.3 - 001 - 99 оцінка захищеності інформації на КС робиться у двох напрямках.

Перший напрямок містить у собі оцінку коректності (тобто, слушності) створеної на КС системи ТЗІ, включаючи оцінку коректності моделі захисту, реалізованого комплексу засобів і механізмів захисту, результатів аналізу на відсутність "слабких місць" у захисті.

Другий напрямок містить у собі оцінку рівня довіри до коректності реалізованої на КС системи ТЗІ. Така оцінка виконується на базі різної повноти і глибини знань про середовище створення та експлуатації КС, а також про систему ТЗІ до неї.

Умови, вимоги і показники, згідно яких оцінюється коректність системи ТЗІ, називаються критеріями дієвості. Це основні функціональні критерії, що дозволяють оцінити ефективність захисту.

Критерії дієвості надані в НД ТЗІ 3.7-002-99 і грунтуються на специфікаціях ФПЗ, які, у свою чергу, викладені в НД ТЗІ 2.5-001-99 .

Рівень довіри до коректності системи ТЗІ специфікується за сьома можливими градаціями: Е0, Е1, Е2, Е3, Е4, Е5 і Е6. Найнижчий рівень довірчої оцінки - Е0 означає недостатню довіру до коректності системи ТЗІ на оцінюваній АТС. Рівень довіри Е1 є початковим рівнем, нижче якого раціональна довіра не зберігається. Рівень Е6 специфікує вищий ступінь довіри. Інші рівні є проміжними.

У НД ТЗІ 2.5-003-99 надані специфікації довірчих оцінок коректності (тобто, нормовані вимоги і умови) для всіх шести

градацій рівнів довіри (крім рівня Е0) до коректності системи ТЗІ, що створена на С.

Деякі специфікації довірчих оцінок базуються на специфікаціях гарантій захисту, які, у свою чергу, викадені в НД ТЗІ 2.5-002-99 .

Контрольні питання до самостійного заняття сімнадцятої лекції:

1. Яка структура АТС з позицій технічного захисту інформації?
2. Які основні види загроз для інформації на АТС?
3. Яким чином можуть здійснюватися загрози для інформації на АТС?
4. Розгляньте три основні групи моделей порушників на АТС.
5. Розгляньте рівні можливостей порушників у рамках кожної групи моделей порушників.
6. Які основні види забезпечення систем ТЗІ на АТС?
7. Назвіть основні функції систем захисту на АТС.
8. Який порядок виконання робіт з ТЗІ на АТС?
9. Яким чином здійснюється оцінка ефективності захисту інформаційних ресурсів АТС?

Література до самостійного заняття сімнадцятої лекції:

1)НД ТЗІ 3.7-002-99 - Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова);

2)НД ТЗІ 2.5-001-99 - Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту;

3)НД ТЗІ 2.5-002-99 - Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту;

4)НД ТЗІ 2.5-003-99 - Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту;

5)НД ТЗІ 2.7-001-99 - Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт.

ЛЕКЦІЯ №18. ТЕХНОЛОГІЇ ОЦІНЮВАННЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ РЕСУРСІВ ТЛК-ОБЛАДНАННЯ

Розглядаються наступні питання:
Лекційне заняття

18.1. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу
18.2. Методика оцінки захищеності інформації в АТС

18.1. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу

На цій лекції розглянуто основні положення нормативного документу (НД) під назвою „Критерії оцінки захищеності інформації в комп"ютерних системах від несанкціонованого доступу" (далі – Критерії) (НД ТЗІ 2.5-004-99), що установлює критерії оцінки захищеності інформації, оброблюваної в комп'ютерних, у т.ч. телекомунікаційних системах з комутацією пакетів, від несанкціонованого доступу. Критерії є методологічною базою для визначення вимог із захисту інформації у вищеназваних системах від несанкціонованого доступу (НСД), створення захищених комп'ютерних та телекомунікаційних систем і засобів захисту від НСД, оцінки захищеності інформації у цих системах та їхньої придатності для обробки критичної інформації (тобто, інформації, що вимагає захисту). Критерії можуть застосовуватися до комп'ютерних та телекомунікаційних систем з пакетною комутацією, включаючи однорідні системи, багатопроцесорні системи, бази даних, вбудовані системи, розподілені системи, мережі, об'єктно-орієнтовані системи та ін.

Виклад матеріалу цієї лекції базується на використанні термінів та визначень, що відповідають встановленим НД ТЗІ 1.1-003-99 "Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу". Зокрема використано наступні позначення та скорочення.

Загальні терміни:
АС — автоматизована система;

КС — комп'ютерна система;
КЗЗ — комплекс засобів захисту;
НСД — несанкціонований доступ;
ОС — обчислювальна система;
ПЗ — програмне забезпечення;
ПЗП — постійний запам’ятовуючий пристрій;
ПРД — правила розмежування доступу.

Позначення послуг, що надаються КС або ТЛК-системою:
КД — довірча конфіденційність;
КА — адміністративна конфіденційність;
КО — повторне використання об'єктів;
КК — аналіз прихованих каналів;
КВ — конфіденційність при обміні;
ЦД — довірча цілісність;
ЦА — адміністративна цілісність;
ЦО — відкат;
ЦВ — цілісність при обміні;
ДР — використання ресурсів;
ДВ — стійкість до відмов;
ДЗ — гаряча заміна;
ДВ — відновлення після збоїв;
НР — реєстрація;
НИ — ідентифікація і автентифікація;
НК — достовірний канал;
НО — розподіл обов'язків;
НЦ — цілісність КЗЗ;
НТ — самотестування;
НВ — автентифікація при обміні;
НА — автентифікація відправника;
НП — автентифікація одержувача

18.1.1. Побудова та структура критеріїв захищеності інформації

В процесі оцінки спроможності ТЛК-системи забезпечувати захист оброблюваної інформації від НСД розглядаються вимоги двох видів:

- вимоги до функціональності послуг безпеки, що надаються ТЛК-системою;

- вимоги до забезпечення гарантій захисту.

В контексті Критеріїв ТЛК-система розглядається як система, що надає користувачам певний набір функціональних послуг із захисту інформації (іноді ці послуги називають послугами безпеки, ПБ). При цьому упевненість щодо коректності надання цих послуг має підтверджуватися результатами перевірки дотримання певних гарантій забезпечення захисту. Надання кожної послуги підтримується певним набором функціональних можливостей ТЛК-обладнання, використання котрих дозволяє протистояти певній множині загроз. Кожна послуга в залежності від потреб користувача може надаватися з різним рівнем ефективності. (Мається на увазі ефективність щодо протидії можливим загрозам інформації). Зрозуміло, що чим більш ефективна послуга, то тим більша вартість її реалізації на практиці. Тому вкрай бажано надати можливість проектувальникам систем захисту вибирати послуги безпеки із різними рівнями ефективності. Тому що не є економічно доцільним проти несуттєвих загроз надавати послуги із високим рівнем ефективності. Нормативні специфікації більшості можливих послуг із захисту інформації визначають для кожної із цих послуг кілька можливих рівнів ефективності їхнього використання. Тобто, уведено поняття рівня послуги (іноді кажуть: „рівня якості послуги" або „рівня ефективності послуги"). Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз. Рівні послуг мають ієрархію за повнотою захисту, проте не обов'язково являють собою точну підмножину один одного. Рівні починаються з першого (1) і зростають до значення *n*, де *n* — - унікальне для кожного виду послуг.

Функціональні послуги із захисту інформації у Критеріях, що наведені у НД ТЗІ 2.5-004-99, розбиті на чотири групи, кожна з

яких описує вимоги до послуг, що забезпечують захист від загроз одного із чотирьох основних видів.

Конфіденційність. Загрози, що відносяться до несанкціонованого ознайомлення з інформацією, становлять загрози конфіденційності. Якщо для якоїсь ТЛК-системи існують вимоги щодо обмеження можливості ознайомлення з інформацією, то специфікації відповідних послуг треба шукати в розділі "Критерії конфіденційності" (див. НД ТЗІ 2.5-004-99). У цьому розділі НД описані наступні послуги: довірча конфіденційність, адміністративна конфіденційність, повторне використання об'єктів, аналіз прихованих каналів, конфіденційність при обміні (експорті/імпорті).

Цілісність. Загрози, що відносяться до несанкціонованої модифікації інформації, становлять загрози цілісності. Якщо існують вимоги щодо обмеження можливості модифікації інформації, то відповідні послуги треба шукати в розділі "Критерії цілісності". У цьому розділі описані наступні послуги: довірча цілісність, адміністративна цілісність, відкат і цілісність при обміні.

Доступність. Загрози, що відносяться до порушення можливості використання ТЛК-систем або оброблюваної інформації легальними (авторизованими, санкціонованими) користувачами, становлять загрози доступності. Якщо існують вимоги щодо забезпечення захисту легальних користувачів від можливих порушень їхнього доступу до інформаційних ресурсів ТЛК-системи (у т.ч., і через можливі несправності обладнання – збої, відмови, помилки і т.ін.), то відповідні послуги треба шукати в розділі "Критерії доступності". У цьому розділі описані наступні послуги: використання ресурсів, стійкість до відмов, горяча заміна, відновлення після збоїв.

Спостереженість. Ідентифікація, автентифікація, авторизація користувачів ресурсами ТЛК-системи, контроль за діями користувачів, забезпечення керованості ТЛК-системи становлять предмет послуг спостереженості і керованості. Якщо при побудові системи захисту висуваються вимоги щодо контролю за діями користувачів або за легальністю доступу, а також за спроможністю комплексу засобів захисту (КЗЗ) виконувати свої функції, то

відповідні послуги треба шукати у розділі “Критерії спостереженості”. У цьому розділі описані наступні послуги: реєстрація, ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність комплексу засобів захисту, самотестування, автентифікація при обміні, автентифікація відправника (невідмова від авторства), автентифікація одержувача (з метою отримання гарантій щодо невідмови від одержання).

Крім специфікацій вищезазначених функціональних послуг безпеки у Критеріях НД ТЗІ 2.5-004-99 містяться також критерії гарантій, що дозволяють оцінити коректність реалізації системи захисту інформаційних ресурсів ТЛК-системи. Специфікації критеріїв гарантій включають вимоги до архітектури комплексу засобів захисту, середовища розробки, послідовності розробки, випробування комплексу засобів захисту, середовища функціонування і експлуатаційної документації. У Критеріях уведено сім рівнів гарантій щодо коректності реалізації системи захисту (Г-1, ..., Г-7), які є ієрархічними. Ієрархія рівнів гарантій відбиває поступово наростаючу міру упевненості в тому, що реалізовані у ТЛК-системі послуги дозволяють протистояти певним загрозам, що механізми, які їх реалізують, в свою чергу, коректно реалізовані і можуть забезпечити очікуваний споживачем рівень захищеності інформації під час експлуатації ТЛК-системи.

Структуру критеріїв показано на рис.18.1.

Аналізуючи функціональність представлених послуг безпеки, можливо упевнитись, що більшість послуг є незалежними одна від одної. Тобто реалізація окремої послуги у складі створюваної системи захисту не залежить від того, чи були реалізовані якісь інші послуги безпеки. Проте існує кілька залежних послуг, тобто послуг, реалізація котрих неможлива без одночасної реалізації певних інших послуг безпеки.

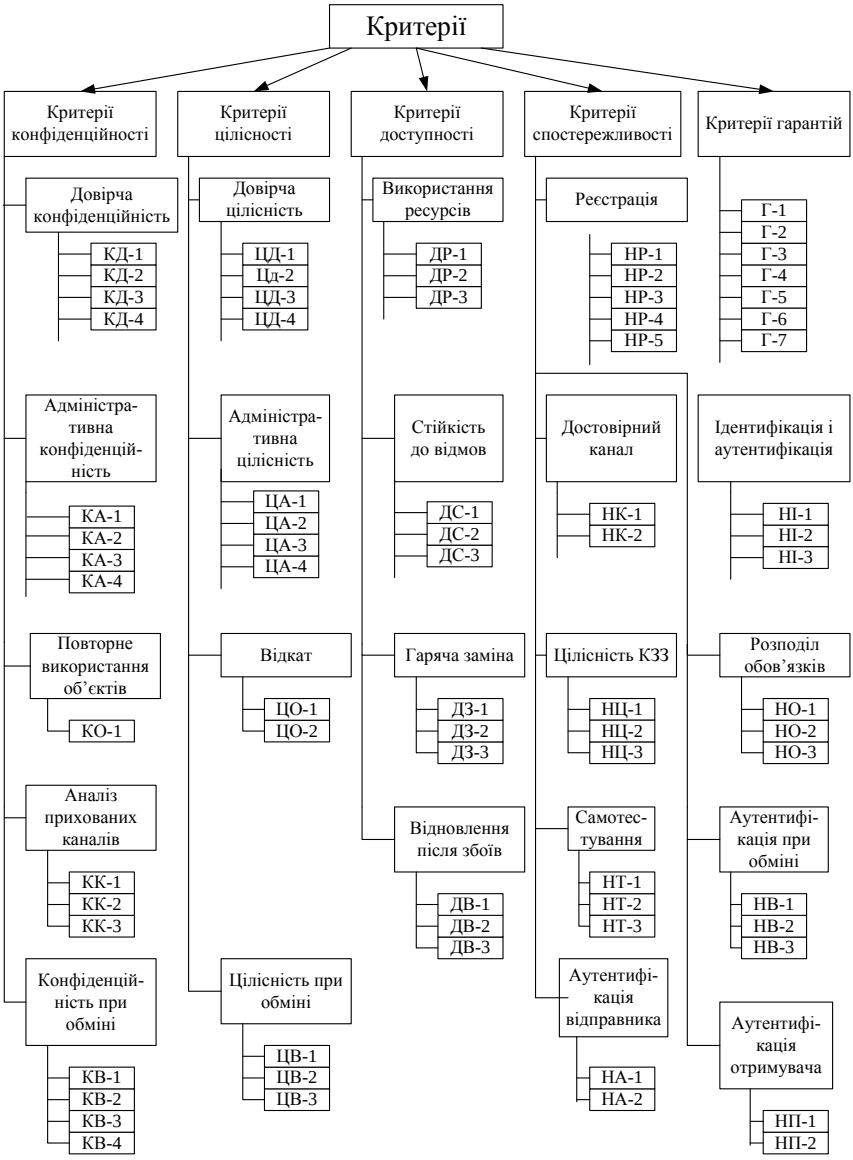


Рис. 18.1 Структура критеріїв

Якщо для якоїсь послуги така залежність існує, то цей факт відбивається у відповідних специфікаціях НД ТЗІ 2.5-004-99 як необхідні умови для реалізації такої залежної послуги. Слід звернути увагу, що залежність між функціональними послугами безпеки і критеріями гарантій відсутня. Виняток складає послуга „*аналіз прихованих каналів"*. Крім того, слід зазначити, що необхідною умовою користування будь-якими функціональними послугами безпеки (незалежно від рівня їхньої ефективності) є обов"язкова реалізація послуги „*цілісність комплексу засобів захисту"* хоча б на першому рівні її ефективності (тобто, необхідність реалізації послуги НЦ-1).

Порядок оцінки будь-якої ТЛК-системи на предмет відповідності Критеріям (див. НД ТЗІ 2.5-004-99) визначається відповідними НД з ТЗІ. Експертна комісія, яка проводить оцінку ТЛК-системи за вищезазначеними Критеріями, визначає, які послуги безпеки і на якому рівні реалізовані в оцінюваній ТЛК-системі, і як дотримані вимоги гарантій. Результатом оцінки опис упорядкованого набору реально перевірених послуг безпеки і відповідних гарантій коректності їхньої реалізації, що називається профілем захищеності оцінюваної ТЛК-системи. Позначення профілю захищеності являє собою так званий рейтинг захищеності ТЛК-системи - упорядкований ряд (перелічення) буквено-числових комбінацій, що позначають рівні реалізованих послуг, в поєднанні з рівнем гарантій. Комбінації упорядковуються в порядку опису послуг у Критеріях. Для того, щоб до рейтингу ТЛК-системи міг бути включений певний рівень послуги чи гарантій, повинні бути виконані усі вимоги, що перелічені у критеріях для даного рівня послуги або гарантій.

Розглянемо послуги, функціональність котрих спрямована на забезпечення захисту інформації від несанкціонованого ознайомлення з нею (тобто, забезпечення захисту від компрометації інформації). Специфікації цих послуг надані в одному із розділів Критеріїв (див. НД ТЗІ 2.5-004-99). Згідно Критеріїв конфіденційність забезпечується наступними послугами: довірча конфіденційність (КД), адміністративна конфіденційність (КА), повторне використання об'єктів (КО), аналіз прихованих каналів (КК), конфіденційність при обміні (КВ). Кожна із цих

послуг має різні рівні ефективності застосування.

Які саме послуги слід використовувати при побудові системи захисту і з якими саме рівнями ефективності – визначається прийнятою політикою забезпечення конфіденційності (яка, в свою чергу, розглядається як складовий елемент загальною політикою забезпечення захисту інформаційних ресурсів ТЛК-системи).

Послуги „Довірча конфіденційність" та „Адміністративна конфіденційність" разом із послугами „Довірча цілісність" та „Адміністративна цілісність" (а також, деякою мірою, послуга повторного використання ресурсів) є класичними послугами, що безпосередньо реалізують ту частину політики безпеки, яка визначає порядок розмежування доступу (ПРД) зацікавлених суб"єктів до об"єктів ТЛК-системи, що потребують захисту.

Основні особливості і відмінність довірчого і адміністративного керування доступом розглянуті в НД ТЗІ 1.1-004-99 "Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу". Система, яка реалізує адміністративне керування доступом, повинна гарантувати, що потоки інформації всередині системи встановлюються адміністратором і не можуть бути змінені звичайним користувачем. З іншого боку, система, яка реалізує довірче керування доступом, дозволяє звичайному користувачеві модифікувати, в т. ч. створювати нові потоки інформації всередині системи.

18.1.2.1. Довірча конфіденційність

Послуга „Довірча конфіденційність" дозволяє користувачеві керувати потоками інформації від захищених об'єктів, що належать його домену безпеки, до інших об"єктів (зокрема, процесів) ТЛК-системи. Як правило, під об'єктами, що належать домену безпеки користувача, маються на увазі об'єкти, власником яких є користувач (тобто, ці об"єкти створені користувачем або від його імені).

Для відображення функціональності системи захисту, що пов"язана із побудовою ПРД, використовується концепція матриці доступу. Матриця доступу являє собою таблицю, уздовж кожного виміру якої відкладені ідентифікатори об'єктів ТЛК-системи, а в якості елементів матриці виступають дозволені або заборонені

режими доступу. Матриця доступу може бути двовимірною (наприклад, типу „користувачі/пасивні об'єкти”) або тривимірною (користувачі/процеси/пасивні об'єкти). Матриця доступу може бути повною (тобто, містити вздовж кожної координати матриці ідентифікатори усіх існуючих на даний час об’єктів ТЛК-системи даного типу) або частковою. Повна тривимірна матриця доступу дозволяє точно описати хто (завдяки ідентифікатору користувача), через що (завдяки ідентифікатору процеса), до чого (завдяки ідентифікатору пасивного об'єкта) та який вид доступу може отримати.

Рівні послуги „Довірча конфіденційність” ранжируються за ступенем повноти захисту та за рівнем вибірковості керування. Маємо наступні рівні послуги „Довірча конфіденційність”.

Мінімальна довірча конфіденційність (КД-1). Щоб уяснити функціональність цієї послуги, слід мати на увазі, що кожний легальний користувач ТЛК-системи має особистий домен безпеки, в межах якого знаходяться приналежні йому об”єкти. Послуга КД-1 пов”язана із створенням обмежень на можливості ознайомлення легальним користувачем домену з інформацією, що передається від об”єктів інших доменів до об”єктів його домену через активізовані у ТЛК-системі процеси. Обмежується список процесів, до яких дозволено користувачу організовувати потоки інформації від об”єктів свого домена. Точніше, у розрізі кожного об”єкта домена обмежуються списки процесів, які можуть одержувати інформацію від цих об'єктів. Тобто дозволено ініціювати потоки інформації від об'єкта тільки до визначених процесів. Інші процеси, що існують у ТЛК-системі, не є доступними для цього об”єкта і, отже, легальний користувач цього об”єкту не може отримати легальний доступ до усіх процесів, окрім тих, що внесені у список. Проте легальний користувач домену безпеки для кожного об”єкту, що входить у цей домен, має змогу змінювати список дозволених процесів. І, отже, при бажанні зможе отримати доступ до бажаного процесу. Однак факт зміни списку буде зареєстровано механізмами системи захисту, тобто буде поміченим головним адміністратором системи. Зрозуміло, що це слабка міра захисту від несанкціонованого ознайомлення з інформацією, оскільки не накладаються обмеження на те, хто саме може активізувати поток

інформації від об”єкта до дозволеного процесу, тобто хто може одержувати інформацію. Комплекс засобів захисту (КЗЗ), що реалізує послугу КД-1, обмежує потоки інформації шляхом обмеження списків процесів, грунтуючись на атрибутах доступу об'єктів і процесів. Для такої системи можна побудувати часткову або повну матрицю доступу процесів до захищених об'єктів.

Базова довірча конфіденційність (КД-2). В системі, яка реалізує послугу довірча конфіденційність на рівні КД-2, атрибути доступу об'єктів і користувачів повинні містити інформацію, що використовується КЗЗ для розмежування доступу до об'єктів з боку конкретного користувача. Додатково повинна існувати можливість встановлювати, які користувачі можуть активізувати конкретний процес, що дозволяє одержати можливість обмеженого керування потоками інформації. Керування правами доступу на даному рівні має невисоку вибірковість. Користувач, домену якого належить об'єкт (процес) може вказати, які групи користувачів і, можливо, які конкретні користувачі мають право одержувати інформацію від об'єкта (ініціювати процес). Для такої системи можна побудувати часткову матрицю доступу користувачів до захищених об'єктів і процесів. Прикладом реалізації даного рівня послуги є реалізоване в ОС UNIX керування доступом на підставі тріад „власник / група / всі інші”.

Повна довірча конфіденційність (КД-3). Основна відміна від попереднього рівня це те, що КЗЗ повинен забезпечувати більш високу вибірковість керування тим, які саме користувачі можуть одержати інформацію від об'єкта або ініціювати процес. Користувач, домену якого належить об'єкт, може вказати права доступу для кожного конкретного користувача і групи користувачів. Є можливим включати або вилучати користувачів із списку доступу. Для такої системи можна побудувати повну матрицю доступу користувачів до захищених об'єктів і процесів. Така вибірковість керування може бути одержана, наприклад, за рахунок використання списків доступу.

Абсолютна довірча конфіденційність (КД-4). Даний рівень забезпечує повне керування потоками інформації у ТЛК-системі. Атрибути доступу користувача, процесу і об'єкта повинні містити інформацію, що використовується КЗЗ для визначення

користувачів, процесів і пар процес/користувач, які можуть отримати інформацію від об'єкта. Таким чином гарантується, що інформація надсилається об’єктом потрібному користувачеві через авторизований процес. Вимоги до вибірковості керування залишаються такими ж самими, як і для попереднього рівня. Для такої системи можна побудувати повну матрицю доступу користувачів, процесів і пар користувач/процес до захищених об'єктів і процесів.

Для всіх рівнів даної послуги необхідною умовою є обов”язковість реалізації послуги „Ідентифікація і автентифікація” рівня НИ-1, що цілком очевидно. Для послуги довірчої конфіденційності рівнів КД-3 і КД-4 необхідною умовою є реалізація послуги „Повторне використання об'єктів” рівня КО-1, оскільки, якщо при виділенні об'єкта користувачеві в цьому об'єкті міститься інформація, що залишилась від попереднього користувача, то це може призвести до витоку інформації, і всі зусилля щодо реалізації даних рівнів послуги будуть марні.

Специфікація послуги „Довірча конфіденційність” наведена в табл.18.2.

18.1.2.2. Адміністративна конфіденційність

Послуга адміністративна конфіденційність дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів до користувачів (див. специфікації в табл.18.4).

Згідно з політикою адміністративної конфіденційності об'єкту присвоюються атрибути доступу, що визначають домен, якому повинні належати ті користувачі або процеси, які намагаються одержати інформацію. Найбільше розповсюдження отримав механізм, коли у вигляді атрибутів доступу використовуються мітки, що визначають рівень конфіденційності інформації (об'єкта) і рівень допуску користувача. Таким чином КЗЗ на підставі порівняння міток об'єкта і користувача може визначити, чи є користувач, що здійснює запит на доступ до інформації, авторизованим користувачем.

Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування повністю аналогічне рівням послуги

довірча конфіденційність з тією відмінністю, що тільки адміністратор або авторизований адміністратором користувач має право включати і вилучати користувачів, процеси і об'єкти до/з конкретних доменів або піддоменів.

Критерії конфіденційності

Для того, щоб ТЛК-система могла бути оцінена на предмет відповідності критеріям конфіденційності, КЗЗ оцінюваної ТЛК-системи повинен надавати послуги з захисту об'єктів від несанкціонованого ознайомлення з їх змістом (компрометації). Конфіденційність забезпечується такими послугами: довірча конфіденційність, адміністративна конфіденційність, повторне використання об'єктів, аналіз прихованих каналів, конфіденційність при обміні.

Довірча конфіденційність

Ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Таблиця 18.1

Специфікації послуги довірчої конфіденційності

<table>
<tr><th>КД-1. Мінімальна довірча конфіденційність</th><th>КД-2. Базова довірча конфіденційність</th><th>КД-3. Повна довірча конфіденційність</th><th>КД-4. Абсолютна довірча конфіденційність</th></tr>
<tr><td colspan="2">Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься</td><td colspan="2">Політика довірчої конфіденційності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС</td></tr>
<tr><td colspan="4">КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу</td></tr>
<tr><td>процесу і захищеного</td><td colspan="2">користувача і захищеного об'єкта</td><td>користувача, процесу і захищеного</td></tr>
</table>

<table>
<tr><td>об'єкта</td><td colspan="2"></td><td>об'єкта</td></tr>
<tr><td colspan="4">Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта</td></tr>
<tr><td colspan="4">КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити</td></tr>
<tr><td>конкретні процеси і/або групи процесів, які мають право одержувати інформацію від об'єкта</td><td>конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта</td><td>конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта</td><td>конкретних користувачів і процеси (і групи користувачів і процесів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта</td></tr>
<tr><td rowspan="2">—</td><td colspan="3">КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити</td></tr>
<tr><td>конкретних користувачів і/або групи користувачів, які мають право ініціювати процес</td><td colspan="2">конкретних користувачів (і групи користувачів), які мають, а також тих, що не мають права ініціювати процес</td></tr>
<tr><td colspan="4">Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації. Як частина політики довірчої конфіденційності повинні бути представлені правила збереження атрибутів доступу об'єктів під</td></tr>
</table>

час їх експорту та імпорту	
НЕОБХІДНІ УМОВИ: НИ-1	НЕОБХІДНІ УМОВИ: КО-1, НИ-1

Адміністративна конфіденційність

Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів до користувачів. Рівні даної послуги ран жируються на підставі повноти захисту і вибірковості управління.

Таблиця 18.2

Специфікації послуги адміністративної конфіденційності

КА-1. Мінімальна адміністративна конфіденційність	**КА-2. Базова адміністративна конфіденційність**	**КА-3. Повна адміністративна конфіденційність**	**КА-4. Абсолютна адміністративна конфіденційність**
Політика адміністративної конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься		Політика адміністративної конфіденційності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС	
КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу			
процесу і захищеного об'єкта	користувача і захищеного об'єкта		користувача, процесу і захищеного об'єкта
Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження			
КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити			

конкретні процеси і/або групи процесів, які мають право одержувати інформацію від об'єкта	конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта	конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта	конкретних користувачів і процеси (і групи користувачів і процесів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта
—	КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного процесу через керування належністю користувачів і процесів до відповідних доменів визначити		
	конкретних користувачів і/або групи користувачів, які мають право ініціювати процес	конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права ініціювати процес	
П рава доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної конфіденційності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту			
НЕОБХІДНІ УМОВИ: НО-1, НИ-1		НЕОБХІДНІ УМОВИ: КО-1, НО-1, НИ-1	

Як і для послуги довірча конфіденційність, для всіх рівнів даної послуги необхідною умовою є реалізація рівня НИ-1 послуги ідентифікація і автентифікація, а для рівнів КА-3 і КА-4 — рівня КО-1 послуги повторне використання об'єктів. Додатковою необхідною умовою для всіх рівнів даної послуги є реалізація рівня НО-1 послуги розподіл обов'язків, оскільки в системі повинні бути

визначені ролі звичайного користувача і адміністратора.

18.1.2.3. Повторне використання об'єктів

Вважається, що ТЛК-система забезпечує послугу „Повторне використання об'єктів", якщо перед наданням користувачеві або якомусь процесові прав доступу до об'єкту, до якого організується доступ, не залишається інформації, що пов"язана із попередньою роботою цього об"єкту, а також якщо скасовуються попередні права доступу до цього об'єкту. Реалізація даної послуги дозволяє забезпечити захист від атак типу "збирання сміття". Ця послуга має один рівень ефективності – КО-1. Специфікації цієї послуги табл.18.4.

Критерії не встановлюють, коли саме має виконуватися очищення об'єкта від інформації, що використовувалася на попередній стадії роботи цього об"єкту. Залежно від реалізованих механізмів можна виконувати очищення об'єкта або під час його звільнення черговим користувачем або безпосередньо перед його наданням наступному користувачу. Повторне використання об'єкта може бути реалізовано також шляхом шифрування інформації, що міститься в об'єктах, і використання керування криптографічними ключами замість знищення інформації.

18.1.2.4. Аналіз прихованих каналів

Аналіз прихованих каналів виконується з метою виявлення і вилучення потоків інформації, що існують, але не контролюються іншими послугами. Специфіковано три рівні цієї послуги – КК-1, КК-2 та КК-3.

Повторне використання об'єктів

Ця послуга дозволяє забезпечити коректність повторного використання розділюваних об'єктів, гарантуючи, що в разі, якщо розділюваний об'єкт виділяється новому користувачу або процесу, то він не містить інформації, яка залишилась від попереднього користувача або процесу.

Таблиця 18.3

Повторне використання об'єктів

КО-1. Повторне використання об'єктів
Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною
НЕОБХІДНІ УМОВИ: НЕМАЄ

Аналіз прихованих каналів

Аналіз прихованих каналів виконується з метою виявлення і усунення потоків інформації, які існують, але не контролюються іншими послугами. Рівні даної послуги ран жируються на підставі того, чи виконується тільки виявлення, контроль або перекриття прихованих каналів.

Таблиця 18.4

Специфікації послуг повторного використання об”єктів та аналізу прихованих каналів

КК-1. Виявлення прихованих каналів	КК-2. Контроль прихованих каналів	КК-3. Перекриття прихованих каналів
Повинен бути виконаний аналіз прихованих каналів		
Всі приховані канали, які існують в апаратному і програмному забезпеченні, а також в програмах ПЗП, повинні бути документовані Має бути документована максимальна пропускна здатність кожного знайденого		Всі (затверджена підмножина) знайдені під час аналізу приховані канали повинні бути усунені

прихованого каналу, одержана на підставі теоретичної оцінки або вимірів Для прихованих каналів, які можуть використовуватися спільно, повинна бути документована сукупна пропускна здатність		
—	КЗЗ повинен забезпечувати реєстрацію використання затвердженої підмножини знайдених прихованих каналів	
НЕОБХІДНІ УМОВИ: КО-1, Г-3	НЕОБХІДНІ УМОВИ: КО-1, НР-1, Г-3	НЕОБХІДНІ УМОВИ: КО-1, Г-3

Рівні даної послуги ранжируються на підставі того, які саме операції виконуються для аналізу прихованих каналів: лише тільки виявлення цих каналів або також і їхній контроль або, тим більш, ще і перекриття прихованих каналів. Специфікації цієї послуги надано в табл.18.4. Ніякого обмеження на смугу пропускання прихованих каналів і ніякої різниці між прихованими каналами з пам'яттю і тимчасовими прихованими каналами не робиться. Проте це не означає, що смуга пропускання прихованих каналів не повинна обмежуватись.

На практиці, наприклад, може виявитись даремною реалізація послуг конфіденційності на рівнях КД-4 і КА-4, якщо в системі існують приховані канали із смугою пропускання у декілька сотень кілобайт за секунду.

Необхідною умовою для реалізації всіх рівнів даної послуги є рівень гарантій забезпечення захисту не нижче Г-3, оскільки розробник повинен виконати аналіз прихованих каналів на етапі проектування системи, а також реалізація послуги „Повторне використання об'єктів" рівня КО-1, оскільки можливість

одержання інформації, що залишилась в об'єкті від попереднього користувача, сама собою може розглядатися як прихований канал.

18.1.2.5. Конфіденційність при обміні

У ТЛК-системах із розподіленою архітектурою у загальному випадку можуть взаємодіяти різні КЗЗ, які реалізують різні політики забезпечення захисту інформації. Наприклад на одному вузлі ТЛК-системи реалізована не така політика безпеки (ПБ), як ПБ, що реалізована на іншому вузлі мережі. Послуги захисту інформації при обміні інформацією між різними доменами безпеки із різними ПБ і КЗЗ (як-от, конфіденційність при обміні, цілісність при обміні, ідентифікація і автентифікація при обміні, автентифікація відправника і автентифікація одержувача) дозволяють забезпечити безпеку обміну інформацією між різними КЗЗ через незахищене середовище транспортування інформації.

Вважається, що КЗЗ розглядає ресурси ТЛК-системи в якості об'єктів захисту і управляє взаємодією цих об'єктів відповідно до реалізованої політики безпеки інформації. Як об'єкти ресурси характеризуються двома аспектами: логічним поданням (тобто, змістом, семантикою, значеннями) і фізичним поданням (тобто, формою та синтаксисом). Зокрема об'єкт характеризується своїм станом (змістом), котрий, в свою чергу, характеризується атрибутами і поводженням, яке визначає засоби зміни стану.

Локалізований КЗЗ (наприклад, операційна система з функціями захисту) розглядає тільки логічне подання об'єктів. Фізичне подання об'єктів захищене тільки від внутрішніх об'єктів, а не від впливу з боку зовнішніх сутностей (агентів). Захист від зовнішніх щодо ТЛК-системи загроз реалізується організаційними заходами і заходами фізичного захисту. До зовнішніх впливів схильні об'єкти, що зберігаються в енергонезалежній пам'яті (на зовнішніх носіях).

У розподіленому оточенні не можна гарантувати, що зовнішній агент не може отримати доступ до фізичного подання об'єктів. Особливо це відноситься до ліній зв'язку (каналів взаємодії). Таким чином, необхідно, щоб об’єкти були захищені під час їх експорту із фізично безпечного оточення.

Специфікації послуги „Конфіденційність при обміні”, що має чотири рівні ефективності (від КВ-1 до КВ-4), наведені в

табл.18.5.

Послуга конфіденційність при обміні дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що в них міститься, під час їх експорту/імпорту через незахищене середовище. Найчастіше дана послуга реалізується з використанням криптографічних перетворень.

Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Конфіденційність при обміні

Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ран жируються на підставі повноти захисту і вибірковості керування.

Таблиця 18.5

Специфікації послуги конфіденційності при обміні

<table>
<tr><th>КВ-1. Мінімальна конфіденційність при обміні</th><th>КВ-2. Базова конфіденційність при обміні</th><th>КВ-3. Повна конфіденційність при обміні</th><th>КВ-4. Абсолютна конфіденційність при обміні</th></tr>
<tr><td colspan="2">Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів і інтерфейсних процесів, до яких вона відноситься</td><td colspan="2">Політика конфіденційності при обміні, що реалізується КЗЗ, повинна відноситись до всіх об'єктів і існуючих інтерфейсних процесів</td></tr>
<tr><td colspan="4">Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуються, і спроможність користувачів і/або процесів керувати рівнем захищеності</td></tr>
<tr><td colspan="4">КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається</td></tr>
<tr><td>—</td><td colspan="3">Запити на призначення або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження</td></tr>
</table>

—	Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу	
	—	і приймальника об'єкта
—	Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу	
	—	і джерела об'єкта
—	Представлення захищеного об'єкта має бути функцією атрибутів доступу інтерфейсного процесу, самого об'єкта, а також його джерела і приймальника	
		Політика конфіденційності при обміні повинна включати опис інформації , яку можливо отримати шляхом сумісного аналізу ряду одержаних об'єктів Повинен бути виконаний аналіз прихованих каналів обміну. Всі знайдені приховані канали обміну і максимальна пропускна здатність

			кожного із них мають бути документовані. Повинна бути забезпечена реєстрація використання затвердженої підмножини знайдених прихованих каналів, їх часткове перекриття або усунення
НЕОБХІДНІ УМОВИ: НЕМАЄ	НО-1	НО-1, НВ-1	НО-1, НВ-1, НР-1, Г-3

Під повнотою захисту в даному випадку розуміють множину типів загроз, від яких забезпечується захист. Під ступенем захищеності об'єктів, що експортуються, як правило, розуміють криптостійкість використовуваних алгоритмів шифрування.

Так, реалізація даної послуги на рівні КВ-1 забезпечує захист від несанкціонованого ознайомлення за рахунок пасивного спостереження за лініями зв'язку або розкрадання носіїв інформації. Прикладом реалізації може служити програмне шифрування файлів перед їх передачею каналами зв'язку або прозоре шифрування файлів перед їх записуванням на диск.

Реалізація даної послуги на рівні КВ-2 дозволяє керувати засобами експорту і імпорту об'єктів і додатково забезпечує захист від помилок користувача та інших випадкових помилок, а також від витоку інформації при підключенні несанкціонованих користувачів.

Реалізація даної послуги на рівні КВ-3 дозволяє забезпечити криптографічне розділення каналів обміну і є необхідною для забезпечення взаємодії КЗЗ, що підтримують обробку інформації рівня секретної або реалізують різні політики безпеки.

Реалізація даної послуги на рівні КВ-3 дозволяє забезпечити захист від компрометації за рахунок аналізу трафіку і від витоку інформації прихованими каналах обміну, що існують. Для реалізації даного рівня від розробника вимагається виконання аналізу прихованих каналів.

18.1.3. Функціональні послуги із протидії порушенням цілісності

Вважається, що цілісність, як і конфіденційність, забезпечується через додержання вимог політики безпеки щодо безпечного переміщення інформації від об'єкта до користувача або до процесу. Правильне (припустиме) переміщення може здійснюватися лише авторизованим користувачем або процесом.

Розглянемо послуги, функціональність котрих спрямована на забезпечення захисту інформації від несанкціонованої модифікації (зокрема, від її знищення). Специфікації цих послуг надані в одному із розділів Критеріїв (див. НД ТЗІ 2.5-004-99). Згідно Критеріїв цілісність забезпечується наступними послугами: довірча цілісність (ЦД), адміністративна цілісність (ЦА), відкат (ЦО), цілісність при обміні (ЦВ). Принципи, що лежать в основі реалізації послуг, визначаються політикою забезпечення цілісності. Кожна із цих послуг має різні рівні ефективності застосування. Які саме послуги слід використовувати при побудові системи захисту і з якими саме рівнями ефективності – визначається прийнятою політикою забезпечення цілісності (яка, в свою чергу, розглядається як складовий елемент загальною політикою забезпечення захисту інформаційних ресурсів ТЛК-системи).

18.1.3.1. Довірча цілісність

Послуга „Довірча цілісність" дозволяє авторизованому користувачеві керувати потоками інформації, що надходять від інших користувачів до захищених об'єктів, які належать його домену захисту. Рівні ефективності даної послуги ранжируються в залежності від повноти захисту і вибірковості керування.

Мінімальна довірча цілісність (ЦД-1). На даному рівні послуги користувач може накладати обмеження на доступ з боку інших користувачів до об'єктів, які належать його домену. Мається на увазі забезпечення цілісності об"єктів, що належать домену захисту

цього користувача. Функціональність послуги ЦД-1 передбачає, що керування правами від імені власника домену має грубу вибірковість (тобто, власник домену має можливість лише розподіляти потоки інформації між групами користувачів). Для такої системи можна побудувати лише часткову матрицю доступу користувачів до захищених об'єктів.

Базова довірча цілісність (ЦД-2). Більш ефективним методом запобігання неавторизованій модифікації об"єктів домену є накладення обмежень на те, який процес або група процесів може модифікувати об'єкт. Користувач, домену якого належить об'єкт, може накладати обмеження на доступ до об'єктів з боку процесів і груп процесів. На основі використання послуги ЦД-2 можна побудувати лише часткову матрицю доступу процесів до захищених об'єктів.

Повна довірча цілісність (ЦД-3). Основна відмінність між рівнями ЦД-2 і ЦД-3 полягає в тому, що на даному рівні надається більш висока вибірковість керування, а саме забезпечується можливість визначення, які саме процеси можуть або не можуть модифікувати об'єкт. Для такої системи можна побудувати повну матрицю доступу процесів до захищених об'єктів.

Абсолютна довірча цілісність (ЦД-4). Реалізація послуги „Довірча цілісність" з ефективністю ЦД-4 забезпечує можливість повного керування потоками інформації всередині домену безпеки. Атрибути доступу користувача, процесу і об'єкта повинні містити інформацію, що використовується комплексом КЗЗ для визначення користувачів, процесів і пар „процес/користувач", яким надані права модифікувати об'єкт. Це гарантує, що модифікація об'єкта здійснюється авторизованим користувачем за допомогою авторизованого процесу. Для такої системи можна побудувати повну матрицю доступу користувачів, процесів і пар „користувач/процес" до захищених об'єктів і процесів.

Для всіх рівнів послуги „Довірча цілісність" необхідною умовою є реалізація послуги „Ідентифікація і автентифікація" рівня НИ-1, що цілком очевидно. Для рівнів ЦД-3 і ЦД-4 необхідною умовою є реалізація послуги „Повторне використання об'єктів" рівня КО-1, оскільки її відсутність може призвести до того, що під час подання об'єкта користувачеві у цьому об'єкті буде міститися

інформація, джерело якої не визначено.

Специфікації послуги „Довірча цілісність" наведені в табл.18.6.

18.1.3.2. Адміністративна цілісність

Послуга **„**Адміністративна цілісність" (ЦА) дозволяє адміністратору чи авторизованому користувачу керувати потоками інформації від користувачів і процесів до захищених об'єктів.

Специфікації послуги „Адміністративна цілісність" наведені в табл.18.7.

Критерії цілісності

Для того, щоб ТЛК-система могла бути оцінена на предмет відповідності критеріям цілісності, комплекс засобів захисту (КЗЗ) оцінюваної ТЛК-системи повинен надавати послуги із захисту оброблюваної інформації від несанкціонованої модифікації. Цілісність забезпечується наступними послугами: довірча цілісність, адміністративна цілісність, відкат, цілісність при обміні.

Довірча цілісність

Ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену. Рівні даної послуги ран жируються на підставі повноти захисту і вибірковості керування.

Таблиця 18.6

Специфікації послуги „Довірча цілісність"

ЦД-1. Мінімальна довірча цілісність	**ЦД-2. Базова довірча цілісність**	**ЦД-3. Повна довірча цілісність**	**ЦД-4. Абсолютна довірча цілісність**
Політика довірчої цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів ТЛК-системи, до яких вона відноситься		Політика довірчої цілісності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів ТЛК-системи	
КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу			
користувача і захищеного об'єкта	процесу і захищеного об'єкта		процесу, користувача і

			захищеного об'єкта
Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта			
КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити			
конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт	конкретні процеси і/або групи процесів, які мають право модифікувати об'єкт	конкретні процеси (і групи процесів), які мають, а також тих, що не мають права модифікувати об'єкт	конкретних користувачів і процеси (і групи користувачів і процесів), які мають, а також тих, що не мають права модифікувати об'єкт
—	КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити		
	конкретних користувачів і/або групи користувачів, які мають право ініціювати процес	конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права ініціювати процес	
Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і			

імпорту	
НЕОБХІДНІ УМОВИ: НИ-1	НЕОБХІДНІ УМОВИ: КО-1, НИ-1

Адміністративна цілісність

Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від користувачів до захищених об'єктів. Рівні даної послуги ранжируються в залежності від ступеню повноти захисту та вибірковості керування.

Таблиця 18.7

Специфікації послуги „Адміністративна цілісність"

ЦА-1. Мінімальна адміністративна цілісність	**ЦА-2. Базова адміністративна цілісність**	**ЦА-3. Повна адміністративна цілісність**	**ЦА-4. Абсолютна адміністративна цілісність**
Політика адміністративної цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів ТЛК-системи, до яких вона відноситься		Політика адміністративної цілісності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів ТЛК-системи	
КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу			
користувача і захищеного об'єкта	процесу і захищеного об'єкта		процесу, користувача і захищеного об'єкта
Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження			

<table>
<tr><td colspan="4">КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити</td></tr>
<tr><td>конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт</td><td>конкретні процеси і/або групи процесів, які мають право модифікувати об'єкт</td><td>конкретні процеси (і групи процесів), які мають, а також тих, які не мають права модифікувати об'єкт</td><td>конкретних користувачів і процеси (і групи користувачів і процесів), які мають, а також тих, які не мають права модифікувати об'єкт</td></tr>
<tr><td rowspan="2">—</td><td colspan="3">КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного процесу шляхом керування належністю користувачів і процесів до відповідних доменів визначити</td></tr>
<tr><td>конкретних користувачів і/або групи користувачів, які мають право ініціювати процес</td><td colspan="2">конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права ініціювати процес</td></tr>
<tr><td colspan="4">Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під</td></tr>
</table>

час їх експорту і імпорту	
НЕОБХІДНІ УМОВИ: НО-1, НИ-1	НЕОБХІДНІ УМОВИ: КО-1, НО-1, НИ-1

Згідно з політикою адміністративної цілісності (у повній аналогії з адміністративною конфіденційністю) об'єкту привласнюються атрибути доступу, що визначають домен, якому повинні належати ті користувачі чи процеси, які намагаються модифікувати об’єкт. Рівні даної послуги ранжируються в залежності від повноти захисту і вибірковості керування аналогічно рівням послуги „Довірча цілісність” з тією відмінністю, що тільки адміністратор або авторизований адміністратором користувач має право включати і вилучати користувачів, процеси і об'єкти до/з конкретних доменів або піддоменів.

Як і для послуги „Довірча цілісність” для всіх рівнів даної послуги необхідною умовою є реалізація послуги „Ідентифікація і автентифікація” на рівні не менш ніж НИ-1, а для рівнів послуги КА-3 та КА-4 — послуги „Повторне використання об'єктів” рівня ДО-1. Додатковою необхідною умовою використання будь-якого із рівнів даної послуги є реалізація послуги „Розподіл обов'язків” рівня НО-1, оскільки політика забезпечення захисту будь-якої ТЛК-системи повинна визначати ролі звичайного користувача і адміністратора цієї системи.

18.1.3.3. Відкат

Послуга „Відкат” забезпечує можливість відновлення роботи ТЛК-системи після помилок користувачів, після збоїв програмного забезпечення (ПЗ) або апаратних засобів цієї системи, дозволяє підтримувати цілісність баз даних, прикладних застосувань, побудованих на транзакціях і т. ін. Дана послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути (тобто, „відкатити”) захищений об’єкт до попереднього стану. Рівні ефективності даної послуги ранжируються в залежності від множини операцій, для яких забезпечується відкат.

Мається на увазі, що відкат — завжди доступна автоматизована послуга. Підкреслимо, що використання відкладеного

резервування, що вимагає втручання користувача у роботу ТЛК-системи для завантаження резервного носія, не розглядається як реалізація послуги відкату. Якщо ТЛК-система реалізує дану послугу, то її політика безпеки має передбачати необхідність фіксації актів її використання у відповідному журналі. Відміна операції відкату не повинна приводити до видалення із цього журналу запису про операцію, яка пізніше була відмінена.

Необхідною умовою для реалізації всіх рівнів даної послуги є реалізація послуги „Ідентифікація і автентифікація" рівня НИ-1.

Специфікації послуги „Відкат" наведені в табл.18.8.

18.1.3.4. Цілісність при обміні

Послуга „Цілісність при обміні" (ЦВ) дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час експорту/імпорту цих об"єктів через незахищене середовище. Найчастіше ця послуга реалізується з використанням механізмів криптографічного захисту, наприклад як складова при реалізації цифрового підпису. Рівні даної послуги ранжируються в залежності від необхідного ступеню повноти захисту і вибірковості керування. Під повнотою захисту, як і для послуги „Конфіденційність при обміні", треба розуміти множину видів загроз, від яких забезпечується захист. Під ступенем захищеності об'єктів, що експортуються, як правило, слід розуміти криптостійкість використовуваних алгоритмів шифрування. Специфікації послуги „Цілісність при обміні" наведені в табл.18.9.

Рівень ЦВ-1 даної послуги забезпечує мінімальний захист. На включення послуги ЦВ-1 в свій рейтинг може претендувати, наприклад, система, що забезпечує можливість перевірки цілісності ПЗ на підставі цифрового підпису, або система електронної пошти, що забезпечує цифровий підпис повідомлень.

Відкат

Ця послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об'єкт до попереднього стану. Рівні даної послуги ранжируються на підставі множини операцій, для яких забезпечується відкат.

Таблиця 18.8

Специфікації послуги „Відкат"

ЦО-1. Обмежений відкат	ЦО-2. Повний відкат
Політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів ТЛК-системи, до яких вона відноситься	
Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити	
певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу	всі операції, виконані над захищеним об'єктом за певний проміжок часу
НЕОБХІДНІ УМОВИ: НИ-1	

Цілісність при обміні

Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту або імпорту через незахищене середовище. Рівні даної послуги ранжируються в залежності від необхідного ступеню повноти захисту і вибірковості керування.

Таблиця 18.9

Специфікації послуги „Цілісність при обміні"

ЦВ-1: Мінімальна цілісність при обміні	ЦВ-2: Базова цілісність при обміні	ЦВ-3: Повна цілісність при обміні
Політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів ТЛК-системи і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності		
КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається		
—	а також фактів його видалення або дублювання	
	Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу	

	—	і приймальника об'єкта
—	Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу —	і джерела об'єкта
—	Запити на присвоєння або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження	
—		Представлення захищеного об'єкта має бути функцією атрибутів доступу інтерфейсного процесу, самого об'єкта, а також його джерела і приймальника
НЕОБХІДНІ УМОВИ: НЕМАЄ	НО-1	НО-1, НВ-1

Реалізація послуги „Цілісність при обміні" на рівні ЦВ-2 дозволяє, додатково до вищезазначеної можливості, керувати засобами експорту/імпорту об'єктів, забезпечувати захист від помилок користувача та інших випадкових помилок, а також забезпечувати захист від модифікації інформації у разі підключення несанкціонованих користувачів.

Реалізація даної послуги на рівні ЦВ-3 додатково дозволяє забезпечити виявлення випадкових або навмисних порушень цілісності не тільки щодо окремих повідомлень, але і щодо потоків

повідомлень в цілому.

18.1.4. Функціональні послуги із протидії порушенням доступності

Для того, щоб ТЛК-система могла бути оцінена на відповідність критеріям доступності, КЗЗ цієї системи повинен надавати послуги щодо забезпечення можливості авторизованим користувачам на певному проміжку часу мати безперешкодний доступ до ресурсів ТЛК-системи в цілому, до окремих її функцій, зокрема до оброблюваної інформації, і гарантувати спроможність ТЛК-системи функціонувати у разі відмови її компонентів. Доступність може забезпечуватися у ТЛК-системі наступними послугами: „Використання ресурсів", „Стійкість до відмов", „Гаряча заміна", „Відновлення після збоїв".

18.1.4.1. Використання ресурсів

Дана послуга дозволяє контролювати використанням послуг ТЛК-системи та її ресурсів. Рівні ефективності даної послуги ранжируються в залежності від необхідного ступеню повноти захисту і вибірковості керування доступністю ресурсів для авторизованих користувачів.

Найм"якшою формою контролю за використанням ресурсів є застосування так званих квот. Усі захищені об'єкти ТЛК-системи (наприклад, дисковий простір, тривалість сеансу користування ресурсами, час використання центрального процессора і т. ін.) повинні ідентифікуватись і контролюватись диспетчером доступу шляхом накладення обмежень на максимальний обсяг даного ресурсу, що може бути виділений користувачу. На рівні ДР-1 (Квоти) послуги „Використання ресурсів" немає гарантій, що користувач не зможе повністю захопити решту певного ресурсу (тобто, більше, ніж виділена квота), обмежуючи тим самим доступ до нього інших користувачів.

Рівень ДР-2 (Недопущення захоплення ресурсів) послуги „Використання ресурсів" являє собою реалізацію досконалішої форми квот. У рамках функціональності ДР-2 квоти використовуються таким чином, щоб гарантувати, що жоден користувач не зможе захопити решту певного ресурсу, дозволяючи

виділяти менші обсяги ресурсів, ніж максимальна квота користувача, гарантуючи таким чином іншому користувачеві доступ до розділюваного ресурсу.

Рівень ДР-3 (Пріоритетність використання ресурсів) послуги „Використання ресурсів" додатково дозволяє управляти пріоритетністю використання ресурсів. Користувачі групуються адміністратором так, щоб визначити пріоритетні групи. Таким чином, у разі високого завантаження ТЛК-система може знаходитись у стані, коли тільки користувачі, які мають високий приорітет, можуть мати доступ до системи (зрозуміло, що за рахунок інших користувачів).

Необхідною умовою для реалізації всіх рівнів даної послуги є реалізація послуги „Розподіл обов'язків" рівня НО-1 (і як наслідок, — необхідність реалізації послуги „Ідентифікація і автентифікація" рівня НИ-1).

Специфікації послуги „Використання ресурсів" наведено в табл.18.10.

18.1.4.2. Стійкість до відмов

Послуга „Стійкість до відмов" забезпечує доступність ТЛК-системи (зокрема, можливість використання її інформаційних ресурсів, окремих функцій чи ТЛК-системи у цілому) після відмови її компонентів. Специфікації послуги „Стійкість до відмов" наведено в табл. 18.11.

Критерії доступності

Для того, щоб ТЛК-система могла бути оцінена на відповідність критеріям доступності, КЗЗ оцінюваної ТЛК-системи повинен надавати послуги щодо забезпечення можливості використання ТЛК-системи в цілому, окремих функцій або оброблюваної інформації на певному проміжку часу і гарантувати спроможність ТЛК-системи функціонувати у випадку відмови її компонентів. Доступність може забезпечуватися у ТЛК-системі наступними послугами: використання ресурсів, стійкість до відмов, гаряча заміна, відновлення після збоїв.

Використання ресурсів

Ця послуга дозволяє користувачам керувати використанням послуг і ресурсів. Рівні даної послуги ранжируються на підставі

повноти захисту і вибірковості керування доступністю послуг ТЛК-системи.

Таблиця 18.10

Специфікації послуги „Використання ресурсів”

<table>
<tr><th>ДР-1. Квоти</th><th>ДР-2. Недопущення захоплення ресурсів</th><th>ДР-3. Пріоритетність використання ресурсів</th></tr>
<tr><td>Політика використання ресурсів, що реалізується КЗЗ, повинна визначати множину об'єктів ТЛК-системи, до яких вона відноситься</td><td colspan="2">Політика використання ресурсів, що реалізується КЗЗ, повинна відноситися до всіх об'єктів ТЛК-системи</td></tr>
<tr><td colspan="3">Політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються</td></tr>
<tr><td colspan="2">окремому користувачу</td><td>окремому користувачу і довільним групам користувачів</td></tr>
<tr><td colspan="3">Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження</td></tr>
<tr><td>—</td><td colspan="2">Повинна існувати можливість встановлювати обмеження таким чином, щоб КЗЗ мав можливість запобігти діям, які можуть призвести до неможливості доступу інших користувачів до функцій КЗЗ або захищених об'єктів. КЗЗ повинен контролювати такі дії, здійснювані з боку</td></tr>
<tr><td></td><td>окремого</td><td>окремого</td></tr>
</table>

	користувача	користувача і довільних груп користувачів
НЕОБХІДНІ УМОВИ: НО-1		

Стійкість до відмов

Стійкість до відмов гарантує доступність ТЛК-системи (можливість використання інформації, окремих функцій або ТЛК-системи в цілому) після відмови її компонента. Рівні даної послуги ранжируються на підставі спроможності КЗЗ забезпечити можливість функціонування ТЛК-системи в залежності від кількості відмов і послуг, доступних після відмови.

Таблиця 18.11

Специфікації послуги „Стійкість до відмов»

ДС-1. Стійкість при обмежених відмовах	**ДС-2. Стійкість з погіршенням характеристик обслуговування**	**ДС-3. Стійкість без погіршення характеристик обслуговування**
Розробник повинен провести аналіз відмов компонентів ТЛК-системи		
Політика стійкості до відмов, що реалізується КЗЗ, повинна визначати множину компонентів ТЛК-системи, до яких вона відноситься, і типи їх відмов, після яких КС в змозі продовжувати функціонування	Політика стійкості до відмов, що реалізується КЗЗ, повинна відноситися до всіх компонентів ТЛК-системи	

Повинні бути чітко вказані рівні відмов, при перевищенні яких відмови призводять до зниження характеристик обслуговування або недоступності послуги	
Відмова одного захищеного компонента не повинна призводити до недоступності всіх послуг, а має в гіршому випадку проявлятися в зниженні характеристик обслуговування	Відмова одного захищеного компонента не повинна призводити до недоступності всіх послуг або до зниження характеристик обслуговування
КЗЗ повинен бути спроможний повідомити адміністратора про відмову будь-якого захищеного компонента	
НЕОБХІДНІ УМОВИ: НО-1	

Рівні ефективності послуги „Стійкість до відмов” ранжируються в залежності від ступеню спроможності КЗЗ забезпечити можливість продовження функціонування ТЛК-системи після відмови (зокрема, в залежності від кількості відмов і послуг, доступних для користувачів після відмови).

Необхідною умовою для реалізації всіх рівнів даної послуги є реалізація послуги „Розподіл обов'язків” рівня НО-1 (і, як наслідок, — послуги „Ідентифікація і автентифікація” рівня НИ-1).

18.1.4.3. Гаряча заміна

Послуга „Гаряча заміна” (ДЗ) дозволяє гарантувати доступність ресурсів ТЛК-системи (зокрема, можливість використання її інформаційних ресурсів, окремих функцій або ТЛК-системи у цілому) не тільки після, але і в процесі заміни окремих компонентів цієї системи. Рівні ефективності даної послуги ранжируються в залежності від необхідного ступеню забезпечення повноти захисту. Основна мета, яка досягається внаслідок реалізації цієї послуги, полягає в тому, що на проміжках часу, коли встановлюється нова версія ПЗ у ТЛК-системі або коли здійснюється заміна несправного компонента системи, забезпечується безперервність захисту, тобто

протягом цих проміжків часу усувається можливість потраплення системи до стану, коли політика безпеки, що реалізується нею, стане скомпрометованою.

Необхідною умовою для реалізації всіх рівнів ефективності даної послуги є забезпечення реалізації послуги „Розподіл обов'язків" хоча б рівня НО-1 (і, як наслідок, — необхідність реалізації послуги „Ідентифікація і автентифікація" рівня НИ-1). Окрім того, обов"язковою умовою реалізації рівнів ДЗ-2 або ДЗ-3 послуги „Гаряча заміна" є необхідність реалізації послуги „Стійкість до відмов" рівня ДС-1, оскільки для того, щоб забезпечити можливість гарячої заміни компонента, система повинна забезпечувати свою працездатність у разі відмови даного компонента. Специфікації послуги „Гаряча заміна" наведено в табл.18.12.

Гаряча заміна

Ця послуга дозволяє гарантувати доступність ресурсів ТЛК-системи (тобто, можливість використання її інформаційних ресурсів, окремих функцій або ТЛК-системи у цілому) в процесі заміни окремих її компонентів. Рівні ефективності даної послуги ранжируються в залежності від необхідного ступеню повноти її реалізації.

Таблиця 18.12

Специфікації послуги „Гаряча заміна»

ДЗ-1. Модернізація	**ДЗ-2. Обмежена гаряча заміна**	**ДЗ-3. Гаряча заміна будь-якого компонента**
Політика гарячої заміни, що реалізується КЗЗ, повинна визначати політику проведення модернізації ТЛК-системи	Політика гарячої заміни, що реалізується КЗЗ, повинна визначати множину компонентів ТЛК-системи, які можуть бути замінені без	Політика гарячої заміни, що реалізується КЗЗ, повинна забезпечувати можливість заміни будь-якого компонента без переривання обслуговування

	переривання обслуговування	
Адміністратор або користувачі, яким надані відповідні повноваження, повинні мати можливість провести модернізацію (upgrade) ТЛК-системи. Модернізація ТЛК-системи не повинна призводити до необхідності ще раз проводити інсталяцію ТЛК-системи або до переривання виконання КЗЗ функцій захисту	Адміністратор або користувачі, яким надані відповідні повноваження, повинні мати можливість замінити будь-який захищений компонент	
НЕОБХІДНІ УМОВИ: НО-1	НЕОБХІДНІ УМОВИ: НО-1, ДС-1	

18.1.4.4. Відновлення після збоїв

Послуга „Відновлення після збоїв” (ДВ) забезпечує повернення ТЛК-системи до відомого захищеного стану після відмови або після переривання обслуговування. Рівні ефективності даної послуги ранжируються в залежності від рівня автоматизації процесу відновлення. В одних випадках процесс відновлення після збоїв може вимагати втручання оператора, а в інших більш високих рівнів ефективності реалізації цієї послуги. У цих випадках КЗЗ має бути здатним продукувати відновлення працездатності автоматично без втручання оператора.

Якщо відновлення неможливе, то КЗЗ повинен переводити ТЛК-систему до стану, з якого її може повернути до нормального функціонування тільки адміністратор.

Необхідною умовою реалізації всіх рівнів даної послуги — необхідність реалізація послуги „Розподіл обов'язків” рівня НО-1 (і, як наслідок, необхідність реалізації послуги „Ідентифікація і автентифікація” рівня НИ-1).

Специфікації послуги „Відновлення після збоїв” наведено в табл. 18.13.

Відновлення після збоїв

Ця послуга забезпечує повернення ТЛК-системи у відомий захищений стан після відмови або переривання обслуговування. Рівні даної послуги ранжируються в залежності від необхідного ступеню автоматизації процесу відновлення.

Таблиця 18.13

Специфікації послуги „Відновлення після збоїв”

ДВ-1. Ручне відновлення	**ДВ-2. Автоматизоване відновлення**	**ДВ-3. Вибіркове відновлення**
Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов ТЛК-системи і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція ТЛК-системи		
Після відмови ТЛК-системи або після переривання в обслуговуванні КЗЗ повинен перевести ТЛК-систему до стану, із якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження	Після відмови ТЛК-системи або переривання обслуговування КЗЗ має бути здатним визначити, чи можуть бути використані автоматизовані процедури для повернення ТЛК-системи до нормального функціонування безпечним чином. Якщо такі процедури можуть бути	Після будь-якої відмови ТЛК-системи або переривання обслуговування, що не призводить до необхідності заново інсталювати ТЛК-систему, КЗЗ повинен бути здатним виконати необхідні процедури і безпечним чином повернути ТЛК-систему до нормального функціонування або, в гіршому випадку, функціонування в

	використані, то КЗЗ має бути здатним виконати їх і повернути ТЛК-систему до нормального функціонування	режимі з погіршеними характеристиками обслуговування
—	Якщо автоматизовані процедури не можуть бути використані, то КЗЗ повинен перевести ТЛК-систему до стану, з якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження	
Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути ТЛК-систему до нормального функціонування		повернути ТЛК-систему з режиму з погіршеними характеристиками обслуговування в режим нормального функціонування
НЕОБХІДНІ УМОВИ: НО-1		

18.1.5. Функціональні послуги із забезпечення спостереженості

Для того, щоб ТЛК-система могла бути оцінена на відповідність критеріям спостереженості, КЗЗ повинен надавати послуги щодо забезпечення відповідальності користувача за свої дії і щодо підтримки спроможності КЗЗ виконувати свої функції. Спостережність у ТЛК-системах забезпечується наступними послугами: реєстрація (аудит), ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність КЗЗ, самотестування, ідентифікація і автентифікація при обміні, автентифікація відправника, автентифікація отримувача.

18.1.5.1. Реєстрація

Послуга „Реєстрація" (HP) дозволяє контролювати небезпечні з точки зору захисту інформації дії щодо ТЛК-системи. Рівні ефективності цієї послуги ранжируються в залежності від повноти та вибірковості контролю, складності засобів аналізу даних журналів реєстрації і спроможності виявлення потенційних порушень. Специфікації послуги „Реєстрація" наведено в табл.18.14.

Реєстрація — це процес розпізнавання, фіксування і аналізу дій і подій, що пов'язані з дотриманням політики безпеки інформації. Використання засобів перегляду і аналізу журналів, а особливо засобів налагодження механізмів фіксування подій, має бути прерогативою спеціально авторизованих користувачів.

Вибір фізичного носія, що використовується для зберігання даних реєстрації, повинен відповідати способу використання і обсягу даних. Будь-яке переміщення таких даних має виконуватись способом, що гарантує їх безпеку. Одним із найбезпечніших, хоч і досить дорогих рішень, є використання носіїв з одноразовим записом. В будь-якому випадку рівень захищеності даних реєстрації має бути не нижче, ніж рівень захищеності даних користувачів, яку забезпечують реалізовані послуги конфіденційності і цілісності. Повинні бути вироблені угоди щодо планування і ведення архівів даних реєстрації.

Критерії спостереженості

Для того, щоб КС могла бути оцінена на предмет відповідності критеріям спостереженості, КЗЗ оцінюваної ТЛК-системи повинен надавати послуги з забезпечення відповідальності користувача за свої дії і з підтримки спроможності КЗЗ виконувати свої функції. Спостереженість забезпечується наступними послугами: реєстрація (аудит), ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність КЗЗ, самотестування, ідентифікація і автентифікація при обміні, автентифікація відправника, автентифікація отримувача

Реєстрація

Реєстрація дозволяє контролювати небезпечні для ТЛК-системи дії. Рівні даної послуги ранжируються залежно від повноти і вибірковості контролю, складності засобів аналізу даних журналів

реєстрації і спроможності вияву потенційних порушень.

Таблиця 18.14

Специфікація послуги „Реєстрація”

<table>
<tr><th>HP-1. Зовнішній аналіз</th><th>HP-2. Захищений журнал</th><th>HP-3. Сигналізація про небезпеку</th><th>HP-4. Детальна реєстрація</th><th>HP-5. Аналіз в реальному часі</th></tr>
<tr><td colspan="5">Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються</td></tr>
<tr><td colspan="3">КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки</td><td colspan="2">КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє або непряме відношення до безпеки</td></tr>
<tr><td colspan="5">Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події</td></tr>
<tr><td>КЗЗ має бути здатним передавати журнал реєстрації в інші системи з використанням певних механізмів захисту</td><td colspan="4">КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування. Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації</td></tr>
<tr><td colspan="2">—</td><td colspan="3">КЗЗ має бути здатним контролювати одиничні або повторювані реєстраційні події, які можуть свідчити про прямі (істотні) порушення політики безпеки</td></tr>
</table>

	ТЛК-системи. КЗЗ має бути здатним негайно інформувати адміністратора про перевищення порогів безпеки і, якщо реєстраційні небезпечні події повторюються, здійснити неруйнівні дії щодо припинення повторення цих подій	
	—	КЗЗ має бути здатним виявляти і аналізувати несанкціоновані дії в реальному часі
НИ-1	НЕОБХІДНІ УМОВИ: НИ-1, НО-1	

Для жодного з рівнів послуги реєстрації не встановлюється ніякого фіксованого набору контрольованих подій, оскільки для кожної конкретної ТЛК-системи їхній перелік може бути специфічним. Критична для безпеки подія визначається як подія, що пов'язана із звертанням до якої-небудь послуги безпеки або до результатів виконання якої-небудь функції КЗЗ. Критичною визначається також будь-яка інша подія, яка хоч прямо і не пов'язана з функціонуванням механізмів, які реалізують послуги безпеки, але може призвести до порушення політики безпеки. Остання група подій визначається як така, що має непряме відношення до безпеки. Для визначення ступеню небезпеки таких подій часто необхідним має бути їх аналіз у контексті інших подій, що відбулися.

Для реалізації найбільш високих рівнів ефективності даної послуги необхідна наявність засобів аналізу журналу реєстрації, де фіксуються небезпечні події. Засоби аналізу — це засоби, що виконують більш складну, ніж перегляд зафіксованих подій,

обробку даних журналу реєстрації з метою виявлення можливих порушень політики безпеки. Ці засоби повинні надавати адміністратору можливість виконання сортування і фільтрації даних за певними критеріями, а також здійснення інших подібних операцій. КЗЗ повинен надавати адміністратору можливість вибирати із всієї сукупності виниклих подій саме ті події, що підлягають реєстрації. Це може бути досягнено шляхом реалізації процедури "передвибірки" або "поствибірки". Передвиборка подій, що реєструються, дозволяє виділити під час функціонування ТЛК-системи із всієї множини доступних для реєстрації подій підмножину тих, що необхідно реєструвати в журналі. Використовуючи передвибірку, адміністратор може зменшити кількість реально реєстрованих подій і, отже, розмір остаточного журнального файла. Недоліком предвибірки є те, що ті події, які не були вибрані, не можуть уже пізніше бути проаналізовані, навіть, якщо постає така необхідність. Перевага поствибірки полягає в гнучкості можливості аналізу "пост-фактум", проте така організація ведення журнального файла вимагає виділення значного обсягу пам'яті для даних реєстрації.

Для реалізації найбільш високого рівня послуги реєстрації (НР-5) необхідно, щоб аналіз даних реєстрації здійснювався у реальному часі.

Необхідною умовою реалізації даної послуги з будь-яким рівнем ефективності є обов”язкова реалізація послуги „Ідентифікація і автентифікація” рівня НИ-1, а для реалізації цієї послуги вище рівня НР-1 — необхідно реалізувати також послугу „Розподіл обов'язків” рівня НО-1.

18.1.5.2. Ідентифікація і автентифікація

Послуга „Ідентифікація і автентифікація” (НИ) дозволяє КЗЗ визначити і перевірити особистість користувача (фізичної особи), який намагається одержати доступ до ресурсів ТЛК-системи. Хоч поняття „ідентифікація” відрізняється від поняття „автентифікація”, на практиці обидва ці процеси важко буває поділити. Важливо, щоб в кінцевому підсумку були підстави стверджувати, що система має справу з конкретним відомим їй користувачем. За результатами ідентифікації і автентифікації

користувача ТЛК-система (точніше, - КЗЗ), по-перше, приймає рішення про те, чи дозволено даному користувачеві увійти у систему, і, по-друге, використовує одержані результати надалі для здійснення розмежування доступу на підставі атрибутів доступу користувача, що увійшов.

Рівні ефективності даної послуги ранжируються залежно від числа задіяних механізмів автентифікації. Зазвичай використовують на практиці один із трьох основних принципів автентифікації: коли в якості паролю використовують щось таке, що відоме користувачеві; або - щось таке, чим володіє користувач; або щось властиве тільки користувачеві.

Пароль, персональний унікальний номер або інша подібна інформація є прикладом того, що називається "дещо, що відоме користувачеві". Даний тип автентифікації є простим у реалізації і достатньо ефективним. Проте його ефективність обмежена через відносно невеликі зусилля, які треба здійснити, щоб домогтися можливості його повторення: існує можливість обчислення або вгадання інформації автентифікації, а для її дублювання не вимагається спеціального устаткування чи можливостей.

Такі фізичні об'єкти як смарт-карта, магнітна картка, генератор запитів-відповідей, електронний ключ або фізично прошитий криптографічний ключ є прикладами того, що називається "дещо, чим володіє користувач". Основною перевагою даного типу автентифікації є складність або висока вартість дублювання інформації автентифікації. З іншого боку, втрата пристрою автентифікації може стати причиною потенційної компрометації. Проте, в більшості випадків достатньо просто установити факт втрати такого пристрою і попередити адміністратора безпеки про необхідність зміни інформації автентифікації.

Результати біометричних вимірювань, таких як відбитки пальців, параметри райдужної оболонки ока або геометрія руки служать прикладами того, що називають "дещо, що властиве користувачеві". Реалізація даного типу автентифікації повинна забезпечувати значно сильнішу автентифікацію, ніж два попередніх типи. Основною перешкодою для використання даного механізму є відносно висока вартість пристроїв автентифікації. Крім того, використання цих засобів автентифікації не гарантує

безпомилкової роботи. Рівень (ймовірність) помилок першого і другого роду для таких пристроїв може утруднити їхнє використання для деяких застосувань.

Для підвищення ефективності захисту від специфічних загроз несанкціонованого доступу для найбільш високого рівня даної послуги (НИ-3) вимагається використання комбінації мінімум двох різних типів автентифікації, наприклад уведеного з клавіатури пароля та за допомогою магнітної картки.

Для реалізації послуги „Ідентифікація і автентифікація" на рівнях НИ-2 та НИ-3 необхідна умова - реалізація послуги „Достовірний канал" рівня НК-1.

Специфікації послуги „Ідентифікація і аутентифікація" наведено в табл.18.15.

Ідентифікація і автентифікація

Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до ресурсів ТЛК-системи. Рівні даної послуги ранжируються залежно від числа задіяних механізмів автентифікації.

Таблиця 18.15

Специфікації послуги „Ідентифікація і автентифікація"

НИ-1. Зовнішня ідентифікація і автентифікація	**НИ-2. Одиночна ідентифікація і автентифікація**	**НИ-3. Множинна ідентифікація і автентифікація**
Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ		
Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен		
з використанням захищеного механізму одержати від деякого зовнішнього	автентифікувати цього користувача з використанням захищеного механізму	автентифікувати цього користувача з використанням захищених механізмів двох або більше типів

джерела автентифікований ідентифікатор цього користувача		
—	КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування	
НЕОБХІДНІ УМОВИ: НЕМАЄ	НЕОБХІДНІ УМОВИ: НК-1	

18.1.5.3. Достовірний канал

Послуга „Достовірний канал" (НК) дозволяє гарантувати, що користувач взаємодіє безпосередньо з КЗЗ і ніякий інший користувач або процес не може втручатись у взаємодію (підслухати або модифікувати інформацію, що передається). Рівні ефективності даної послуги ранжируються в залежності від того, чи має КЗЗ можливість ініціювати захищений обмін, чи це є прерогативою користувача.

Реалізація даної послуги є необхідною умовою для реалізації рівнів НИ-2 та НИ-3 послуги „Ідентифікація і автентифікація".

Специфікації послуги „Достовірний канал" наведено в табл.18.16.

18.1.5.4. Розподіл обов'язків

Послуга „Розподіл обов"язків" (НО) дозволяє знизити ймовірність навмисних або помилкових неавторизованих дій користувача або адміністратора і, отже, величину потенційних збитків від таких дій. Рівні ефективності даної послуги ранжируються на підставі вибірковості керування можливостями користувачів і адміністраторів.

Специфікації послуги „Розподіл обов'язків" наведено в табл.18.17.

Система, що претендує на включення даної послуги до рейтингу, повинна передусім забезпечувати існування ролей для адміністратора і звичайного користувача (рівень НО-1).

Для наступного рівня даної послуги вимагається, щоб система підтримувала дві або більше адміністративних ролей зі

специфічними наборами адміністративних обов'язків. Одна з цих ролей повинна бути роллю адміністратора безпеки (ця роль може бути поділена на ролі адміністратора реєстрації (аудиту) і адміністратора каталогів або облікових карток користувачів).

Достовірний канал

Ця послуга дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ. Рівні даної послуги ранжируються залежно від гнучкості надання можливості КЗЗ або користувачу ініціювати захищений обмін.

Таблиця 18.16

Специфікації послуги „Достовірний канал"

НК-1. Однонаправлений достовірний канал	**НК-2. Двонаправлений достовірний канал**
Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ	
Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем	Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації та у випадках, коли необхідний прямий зв'язок користувач/КЗЗ або КЗЗ/користувач. Зв'язок з використанням даного каналу повинен ініціюватися користувачем або КЗЗ
—	Обмін з використанням достовірного каналу, що ініціює КЗЗ, повинен бути однозначно ідентифікований як такий і має відбутися тільки після позитивного підтвердження готовності до обміну з боку користувача
НЕОБХІДНІ УМОВИ: НЕМАЄ	

Розподіл обов'язків

Ця послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Рівні даної послуги ранжируються на підставі вибірковості керування можливостями користувачів і адміністраторів.

Таблиця 18.17

Специфікації послуги „Розподіл обов”язків”

<table>
<tr><th>НО-1. Виділення адміністратора</th><th>НО-2. Розподіл обов'язків адміністраторів</th><th>НО-3. Розподіл обов'язків на підставі привілеїв</th></tr>
<tr><td colspan="3">Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції</td></tr>
<tr><td>—</td><td colspan="2">Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі</td></tr>
<tr><td colspan="2">—</td><td>Політика розподілу обов'язків повинна визначати множину ролей користувачів</td></tr>
<tr><td colspan="3">Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі</td></tr>
<tr><td colspan="3">НЕОБХІДНІ УМОВИ: НИ-1</td></tr>
</table>

Роль адміністратора безпеки повинна бути визначена так, щоб обов'язки, що мають відношення до безпеки, могли бути виконані тільки в цій ролі. Ролі не обов’язково мають бути абсолютно взаємовиключаючими, оскільки деякі функції або команди можуть знадобитись і адміністратору, і користувачу, або різним адміністраторам і т.ін.

Основною відмінністю рівня НО-3 від рівня НО-2 є необхідність визначення ролей для звичайних користувачів.

18.1.5.5. Цілісність комплексу засобів захисту

Послуга „Цілісність комплексу засобів захисту” (НЦ) визначає міру спроможності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

Жодна ТЛК-система не може вважатися захищеною, якщо самі засоби її захисту є об'єктом для несанкціонованого впливу. У зв'язку з цим рівень НЦ-1 даної послуги є необхідною умовою реалізації абсолютно всіх рівнів усіх інших послуг.

Для рівня НЦ-1 даної послуги необхідно, щоб КЗЗ мав можливість перевіряти свою цілісність і в разі виявлення її порушення переводити систему в стан, з якого її може вивести тільки адміністратор.

Для рівня НЦ-2 необхідно, щоб КЗЗ підтримував власний домен виконання, відмінний від доменів виконання всіх інших процесів, захищаючи себе від зовнішніх впливів. Дана вимога є однією з вимог до реалізації диспетчера доступу. Як правило, реалізація даної вимоги повинна забезпечуватися можливостями апаратного забезпечення ОС.

Для рівня НЦ-3 необхідно, щоб КЗЗ забезпечував керування захищеними ресурсами таким чином, щоб не існувало можливості доступу до ресурсів, минаючи КЗЗ. Дана вимога є другою функціональною вимогою до реалізації диспетчера доступу.

Необхідною умовою реалізації рівня НЦ-1 даної послуги є реалізація рівня НО-1 послуги „Розподіл обов'язків” і рівня НР-1 послуги „Реєстрація”, оскільки КЗЗ повинен мати можливість ставити до відома адміністратора про факти порушення своєї цілісності.

Специфікації послуги „Цілісність комплексу засобів захисту”

наведено в табл.18.18.

18.1.5.6. Самотестування

Послуга „Самотестування” (НТ) дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій ТЛК-системи. Рівні ефективності даної послуги ранжируються на підставі можливості виконання тестів за ініціативою користувача в процесі запуску або штатної роботи.

Необхідною умовою реалізації будь-якого із рівнів даної послуги є реалізація рівня НО-1 послуги „Розподіл обов'язків”.

Специфікації послуги „Самотестування” наведено в табл.18.19.

18.1.5.7. Ідентифікація і автентифікація при обміні

Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ранжируються на підставі повноти реалізації.

Реалізація рівня НВ-1 даної послуги дозволяє виключити можливість несанкціонованого зовнішнього підключення і є необхідною умовою для реалізації високих рівнів послуг конфіденційності і цілісності при обміні.

Реалізація рівня НВ-2 даної послуги дозволяє виключити можливість несанкціонованого використання встановленого авторизованого підключення.

Реалізація рівня НВ-3 даної послуги дозволяє виключити можливість деяких видів внутрішнього шахрайства.

Специфікації послуги „Ідентифікація і автентифікація при обміні” наведено в табл.18.20.

Цілісність комплексу засобів захисту

Ця послуга визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

Таблиця 18.18

Специфікації послуги „Цілісність комплексу засобів захисту”

НЦ-1. КЗЗ з	НЦ-2. КЗЗ з	НЦ-3. КЗЗ з

контролем цілісності	**гарантованою цілісністю**	**функціями диспетчера доступу**
Політика цілісності КЗЗ повинна визначати склад КЗЗ і механізми контролю цілісності компонентів, що входять до складу КЗЗ	Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів	
В разі виявлення порушення цілісності будь-якого із своїх компонентів КЗЗ повинен повідомити адміністратора і або автоматично відновити відповідність компонента еталону або перевести КС до стану, з якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження	КЗЗ повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування	
Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ		КЗЗ повинен гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів

	контролюються КЗЗ
НЕОБХІДНІ УМОВИ: НР-1, НО-1	НЕОБХІДНІ УМОВИ: НЕМАЄ

Самотестування.

Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій ТЛК-системи. Рівні даної послуги ранжируються на підставі можливості виконання тестів у процесі запуску або штатної роботи.

Таблиця 18.19

Специфікації послуги „Самотестування”

НТ-1. Самотестування за запитом	**НТ-2. Самотестування при старті**	**НТ-3. Самотестування в реальному часі**
Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ		
КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження,		
—	при ініціалізації КЗЗ —	і в процесі штатного функціонування
НЕОБХІДНІ УМОВИ: НО-1		

Ідентифікація і автентифікація при обміні

Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні ефективності цієї послуги ранжируються в залежності від досягнутої повноти реалізації.

Таблиця 18.20

Специфікації послуги „Ідентифікація і автентифікація при обміні”

НВ-1: Автентифікація вузла	НВ-2: Автентифікація джерела даних	НВ-3: Автентифікація з підтвердженням
Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму. Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації		
—	КЗЗ повинен використовувати захищені механізми для встановлення джерела кожного об'єкта, що експортується та імпортується	
—		Використовуваний протокол автентифікації повинен забезпечувати можливість однозначного підтвердження джерела об'єкта незалежною третьою стороною
НЕОБХІДНІ УМОВИ: НЕМАЄ		

18.1.5.8. Автентифікація відправника

Послуга „Автентифікація відправника" (НА) дозволяє протидіяти відмовам від авторства і однозначно встановлювати належність певного об'єкта певному користувачу, тобто той факт, що об'єкт був створений або відправлений даним користувачем. Рівні ефективності цієї послуги ранжируються в залежності від можливості підтвердження результатів перевірки незалежною третьою стороною.

Найширше для реалізації даної послуги, як і послуги автентифікації одержувача, використовується цифровий підпис,

оскільки використання несиметричних криптоалгоритмів (на відміну від симетричних) дозволяє забезпечити захист від внутрішнього шахрайства і автентифікацію за умов взаємної недовіри сторін.

Необхідною умовою для реалізації всіх рівнів даної послуги є реалізація рівня НИ-1 послуги „Ідентифікація і автентифікація".

Специфікації послуги „Автентифікація відправника" наведено в табл.18.21.

18.1.5.9. Автентифікація одержувача

Послуга „Автентифікація одержувача" (НП) дозволяє протидіяти відмовам від одержання і дозволяє однозначно встановити факт одержання певного об'єкта певним користувачем. Рівні ефективності цієї послуги ранжируються в залежності від можливості підтвердження результатів перевірки незалежною третьою стороною.

Необхідною умовою для реалізації всіх рівнів даної послуги є реалізація рівня НИ-1 послуги „Ідентифікація і автентифікація".

Специфікації послуги „Автентифікація одержувача" наведено в табл.18.22.

Автентифікація відправника

Ця послуга дозволяє забезпечити захист від відмови від авторства і однозначно встановити належність певного об'єкта певному користувачу, тобто той факт, що об'єкт був створений або відправлений даним користувачем. Рівні даної послуги ранжируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною.

Таблиця 18.21

Специфікації послуги „Автентифікація відправника"

НА-1: Базова автентифікація відправника	**НА-2: Автентифікація відправника з підтвердженням**
Політика автентифікації відправника, що реалізується КЗЗ, повинна визначати множину властивостей і атрибутів об'єкта, що передається, користувача-відправника і інтерфейсного процесу, а також процедури, які дозволяли б однозначно встановити, що даний об'єкт був відправлений (створений) певним користувачем	

—	Додатково повинні бути визначені ті властивості, атрибути і процедури, які можуть використовуватися для однозначного підтвердження належності об'єкта незалежною третьою стороною
Встановлення належності має виконуватися на підставі затвердженого протоколу автентифікації	
—	Використовуваний протокол автентифікації повинен забезпечувати можливість однозначного підтвердження належності об'єкта незалежною третьою стороною
НЕОБХІДНІ УМОВИ: НИ-1	

Автентифікація отримувача

Ця послуга дозволяє забезпечити захист від відмови від одержання і дозволяє однозначно встановити факт одержання певного об'єкта певним користувачем. Рівні даної послуги ранжируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною.

Таблиця 18.22

Специфікації послуги „Автентифікація отримувача"

НП-1: Базова автентифікація отримувача	**НП-2: Автентифікація отримувача з підтвердженням**
Політика автентифікації одержувача, що реалізується КЗЗ, повинна визначати множину властивостей і атрибутів об'єкта, що передається, користувача-одержувача і інтерфейсного процесу, а також процедури, які дозволяли б однозначно встановити, що даний об'єкт був одержаний певним користувачем	
—	Додатково повинні бути визначені ті властивості, атрибути і процедури, які можуть використовуватися незалежною третьою стороною для

	однозначного підтвердження факту одержання об'єкта
Встановлення одержувача має виконуватися на підставі затвердженого протоколу автентифікації	
—	Використовуваний протокол автентифікації повинен забезпечувати можливість однозначного підтвердження незалежною третьою стороною факту одержання об'єкта
НЕОБХІДНІ УМОВИ: НИ-1	

18.1.6. Процес оцінки системи захисту

В процесі оцінки захищеності ТЛК-системи від НСД розглядаються вимоги двох видів:

- вимоги до функцій (послуг) забезпечення безпеки;
- вимоги до рівня гарантій.

Виконання вимог першого виду забезпечується Розробником системи захисту в процесі її проектування (розробки) і перевіряється Експертною комісією в процесі оцінки її якості. Виконання вимог другого виду забезпечується як діями Розробника, проте вже на всіх стадіях життєвого циклу ТЛК-системи, так і спільними діями Розробника і Експертної комісії в процесі оцінки. Наведені в критеріях гарантій вимоги регламентують передусім дії Розробника. Дії Експертної комісії регламентуються іншими документами.

Специфікації послуг безпеки були розглянуті вище. Більшість з вимог критеріїв гарантій являють собою конкретизацію положень стандартів серії ДСТУ ISO 9000 щодо створення КЗЗ у ТЛК-системах і для їх викладення використовується термінологія з області керування якістю продукції (ДСТУ 3230-95).

Перевірка виконання Розробником вимог критеріїв гарантій вимагає активної роботи Експертної комісії не тільки на етапі оцінки, але, можливо, і на більш ранніх етапах. Якщо використовувані Розробником процедури і методики (наприклад, супроводження проекту) відрізняються від стандартних чи загальноприйнятих, то вони вимагають перевірки і затвердження

Експертною комісією. Чим вищий припустимий рівень гарантій, тим вища складність використовуваних процедур і методик і, отже, тим вищий рівень зусиль, які необхідно докласти Експертній комісії, що зумовлює в свою чергу необхідність більш тісної взаємодії Розробника з Експертною комісією, починаючи з найбільш ранніх етапів проектування.

В залежності від конкретної ТЛК-системи та інших умов Експертна комісія має право конкретизувати і поглиблювати певні вимоги критеріїв гарантій.

18.1.7. Гарантії забезпечення захисту

18.1.7.1. Гарантії коректності архітектури КЗЗ

У багатьох випадках виникає потреба отримати гарантії того, що побудований КЗЗ у змозі повністю реалізувати прийняту політику безпеки. Ці гарантії рахуються отриманими, якщо архітектура КЗЗ (перш за все, його ПЗ) задовольняє певним вимогам, які у вигляді відповідних специфікацій показані в табл.18.23. Додержання цих вимог забезпечується розробником на стадіях проектування КЗЗ.

Передусім, вимоги до архітектури покликані забезпечити структурованість КЗЗ відповідно до принципів так званого “хорошого" проектування ПЗ (модульність, інкапсуляція і приховування даних).

Для самих низьких рівнів забезпечення гарантій коректності архітектури КЗЗ від Розробника вимагається лише описати складові компоненти КЗЗ та їх призначення.

Для більш високих (проміжних) рівнів забезпечення гарантій вимагається логічне поділення вихідного коду на окремі незалежні компоненти (модулі), що ідентифікуються, та ізоляція компонентів КЗЗ, що є критичними з точки зору забезпечення безпеки. Внутрішні деталі і дані, що використовуються всередині кожного модуля, повинні бути приховані від усіх зовнішніх об'єктів. Послуги КЗЗ повинні бути доступні тільки через зовнішній документований інтерфейс.

Для самих верхніх рівнів забезпечення гарантій Розробник під час проектування ПЗ повинен зосередити зусилля на зменшенні

обсягу КЗЗ до мінімального набору компонентів. Мінімізація обсягу є однією з вимог концепції диспетчера доступу, що дозволяє виділити у складі КЗЗ ядро захисту.

Критерії гарантій

Критерії гарантій включають вимоги до архітектури КЗЗ, середовища розробки, послідовності розробки, середовища функціонування, документації і випробувань КЗЗ. В цих критеріях вводиться сім рівнів гарантій, які є ієрархічними. Вимоги викладаються за розділами. Для того, щоб система захисту ТЛК-системи одержала певний рівень гарантій (якщо вона не може одержати більш високий), повинні бути задоволені всі вимоги, визначені для даного рівня в кожному з розділів.

Архітектура

Вимоги до архітектури забезпечують гарантії того, що КЗЗ у змозі повністю реалізувати політику безпеки.

Таблиця 18.23

Специфікації гарантій коректності архітектури системи захисту

Вимоги	**Г-1**	**Г-2**	**Г-3**	**Г-4**	**Г-5**	**Г-6**	**Г-7**
КЗЗ повинен реалізовувати політику безпеки. Всі його компоненти повинні бути чітко визначені	+	=	=	=	=	=	=
КЗЗ повинен складатися з добре визначених і максимально незалежних компонентів. Кожний з компонентів повинен бути спроектований відповідно до принципу мінімуму повноважень	-	-	+	=	=	=	=
Критичні для безпеки компоненти КЗЗ повинні бути захищені від не критичних для безпеки за рахунок використання механізмів захисту, які надаються програмно-апаратними засобами більш	-	-	-	+	=	=	=

низького рівня							
З боку Розробника мають бути вжиті зусилля, спрямовані на виключення з КЗЗ компонентів, що не є критичними для безпеки. Мають бути наведені підстави для включення до КЗЗ будь-якого елемента, який не має відношення до захисту	-	-	-	-	+	=	=
Розробка ПЗ переважно має бути спрямована на мінімізацію складності КЗЗ. КЗЗ має бути спроектований і структурований так, щоб використовувати повний і концептуально простий механізм захисту з точно визначеною семантикою. Цей механізм повинен відігравати центральну роль в реалізації внутрішньої структури КЗЗ. Під час розробки КЗЗ значною мірою повинні бути задіяні такі підходи як модульність побудови і приховання (локалізація) даних	-	-	-	-	+	=	=

* В таблицях використовуються такі позначення: “-” — вимога відсутня; “+” — вимога з'являється; “=“ — вимога зберігається.

18.1.7.2. Середовище розробки

Виконання вимог до середовища розробки ТЛК-системи, що викладені в табл.18.24, забезпечують гарантії того, що процеси розробки і супроводження цієї системи є повністю керованими з боку Розробника.

Процес розробки. Від Розробника вимагається визначити всі стадії життєвого циклу ТЛК-системи, розробити, запровадити і підтримувати в робочому стані документально оформлені методики своєї діяльності на кожній стадії. Мають бути

документовані всі етапи кожної стадії життєвого циклу та їх граничні вимоги (вимоги, що повинні бути виконані раніше, ніж можна приступати до наступного етапу).

Крім того, у проектних документах мають бути вказані усі стандарти, які використовувались під час розробки ПЗ для ТЛК-системи. Використані під час розробки мови програмування і компілятори мають відповідати вимогам національних, міждержавних або міжнародних стандартів. В іншому випадку слід надати повне визначення і опис мови, яка використовувалась. Додатково має бути документовано використання залежних від реалізації або апаратури опцій мови програмування.

Для більш високих рівнів гарантій безпеки середовища розробки вимоги до цього середовища включають вимоги необхідності документування використаних під час розробки методик фізичної, технічної, організаційної і кадрової безпеки.

Керування конфігурацією. Керування конфігурацією є необхідною і невід'ємною частиною робіт із створення будь-якої ТЛК-системи. Додержання вимог щодо керування конфігурацією ТЛК-систем, які також відображені в табл.18.24, дозволяє забезпечити впевненість в тому, що Розробник здатний керувати конфігурацією створеної ТЛК-системи.

Розробник повинен розробити, запровадити і підтримувати в дієздатному стані документовані методики керування конфігурацією ТЛК-системи на всіх стадіях її життєвого циклу. При цьому Розробник може розробити і використати систему керування конфігурацією, що найкраще відображає як складність ТЛК-системи, так і розміри організації Розробника. Критерії керування, необхідність використання тих чи інших засобів автоматизації, належний рівень формалізації процедур і перевірок визначаються Розробником. Цей рівень має бути сумісним з іншими компонентами середовища розробки, наскільки це можливо. Важливо, щоб усі процедури, ролі і відповідальність персоналу, задіяного в керуванні конфігурацією, були чітко визначені і документовані.

Система керування конфігурацією повинна бути орієнтована на вирішення чотирьох основних завдань: визначення конфігурації, регулювання конфігурації, облік стану і перевірка якості

конфігурації.

Визначення конфігурації. ТЛК-система повинна ідентифікуватися в термінах своєї конфігурації: апаратне забезпечення, програмне забезпечення, програми ПЗП і документація на ТЛК-систему (наприклад, функціональні специфікації, технічний і робочий проекти, документація з тестування). Кожний елемент конфігурації одержує унікальне і значиме ім'я (ідентифікатор), під яким він існує у ТЛК-системі протягом всього її життєвого циклу. Повинні використовуватися загальні для всього проекту угоди щодо позначення, маркірування, нумерації і каталогізації елементів конфігурації Особливу увагу слід приділяти угодам щодо ПЗ (наприклад, для визначення того, є елемент вихідним чи об'єктним кодом).

Розмір елементів конфігурації може варіюватися відповідно до їх складності та очікуваної частоти зміни. Шляхом ретельного вибору розміру кожного елемента конфігурації система керування конфігурацією може краще ізолювати ті елементи, що змінюються частіше від тих, що змінюються рідше, ізолювати ті елементи, що є критичними для безпеки від тих, що не є такими, і групувати окремі малі елементи ТЛК-системи в єдиний великий елемент конфігурації для зменшення загального числа елементів конфігурації Ефективність контролю за змінами залежить від вдалого виділення елементів конфігурації: має досягатись рівновага між керуванням великим числом малих елементів конфігурації і групуванням надто великого числа елементів ТЛК-системи в один елемент конфігурації.

Регулювання конфігурації. Керування (контроль за) внесенням будь-яких змін у ТЛК-систему є основною функцією системи керування конфігурацією. Керування внесенням змін до конфігурації ТЛК-системи слід здійснювати протягом всього життєвого циклу цієї системи. Процес внесення змін і набір використаних процедур мають бути визначені і документовані. Необхідно мати відповідальних осіб, роль і відповідальність яких має бути документована, які відповідали б за оцінку і затвердження запропонованих змін і безпосередньо за їх внесення. Це дозволяє гарантувати, що в разі необхідності елементи конфігурації можуть бути зафіксовані в певному стані і що ефекти від пропонованих

змін будуть враховані раніше, ніж будуть затверджені дані зміни.

Облік стану. Завдання керування конфігурацією щодо обліку стану включає в себе фіксування інформації за статусом кожного елемента конфігурації. Вона включає і вихідне визначення елемента, і будь-які зміни, внесені до елемента (наприклад, поширення, усунення помилок) протягом всього життєвого циклу. При збереженні записів за кожним елементом конфігурації поточний стан (статус) кожного елемента може бути доступним зацікавленому персоналу, а також можуть бути одержані архівні дані для використання в процесі перевірки конфігурації.

Перевірка якості конфігурації. Контроль за конфігурацією здійснюється шляхом взаємозв'язаних переглядів і перевірок інформації за станом всіх елементів конфігурації з метою одержання впевненості, що система керування конфігурацією працює належним чином. Контроль за конфігурацією робить можливим наступну адаптацію і настроювання процесу керування конфігурацією відповідно до умов, що змінюються (вхідними вимогами). Перегляди і перевірки також дають гарантію того, що стандарти, політика і процедури, прийняті в організації, присутні і в системі керування конфігурацією.

Відповідно до Критеріїв система керування конфігурацією включає в себе технічні та організаційні заходи. Система керування конфігурацією повинна охоплювати розробку і супроводження програмного, апаратного, програмно-апаратного забезпечення, розробку документації, тестів і т.ін.

Для найнижчих рівнів забезпечення гарантій середовища розробки у Розробника має бути базова система керування конфігурацією, що дозволяє ідентифікувати оцінювану ТЛК-систему, керувати внесенням змін і вести архів цих змін. Система керування конфігурацією повинна включати технічні або організаційні документовані методики керування програмним, апаратним, програмно-апаратним забезпеченням, опрацюванням документації і тестів у необхідному обсязі.

Для більш високих рівнів гарантій система керування конфігурацією повинна додатково мати можливість генерувати версію КЗЗ із вихідного коду і відзначати будь-які відмінності. Частиною системи мають бути засоби генерації звітів про помилки

та інші проблеми, а також про їх усунення. Для цих рівнів гарантій система керування конфігурацією повинна використовувати засоби автоматизації та організаційні процедури, що їх доповнюють.

Для найбільш високих рівнів критеріїв гарантій система керування конфігурацією повинна додатково забезпечувати керування всіма засобами (наприклад, мовами програмування, компіляторами, бібліотеками часу виконання і т. ін.), які використовувались в процесі розробки ТЛК-системи.

Специфікації гарантій середовища розробки наведено в табл.18.24.

Середовище розробки

Вимоги до середовища розробки забезпечують гарантії того, що процеси розробки і супроводження оцінюваної ТЛК-системи є повністю керованими з боку Розробника.

Таблиця 18.24

Специфікації гарантій середовища розробки

Вимоги	**Г-1**	**Г-2**	**Г-3**	**Г-4**	**Г-5**	**Г-6**	**Г-7**
Процес розробки							
Розробник повинен визначити всі стадії життєвого циклу ТЛК-системи, розробити, запровадити і підтримувати в робочому стані документально оформлені методики своєї діяльності на кожній стадії. Мають бути документовані всі етапи кожної стадії життєвого циклу і їх граничні вимоги	+	=	=	=	=	=	=
Розробник повинен описати стандарти кодування, яким необхідно додержуватися	-	-	+	=	=	=	=

в процесі реалізації, і повинен гарантувати, що всі вихідні коди компілюються відповідно до цих стандартів. Будь-яка з використовуваних під час реалізації мов програмування має бути добре визначена. Всі залежні від реалізації параметри мов програмування або компіляторів повинні бути документовані							
Розробник повинен розробити, запровадити і підтримувати в робочому стані документально оформлені методики забезпечення фізичної, технічної, організаційної і кадрової безпеки	-	-	-	+	=	=	=
Керування конфігурацією							
Розробник повинен розробити, запровадити і підтримувати в робочому стані документовані методики щодо керування конфігурацією ТЛК-системи на всіх стадіях її життєвого циклу. Система керування конфігурацією повинна забезпечувати керування внесенням змін в апаратне забезпечення, програми	+	=	=	+ *	=	=	=

ПЗП, вихідні тексти, об'єктні коди, тестове покриття і документацію. Система керування конфігурацією повинна гарантувати постійну відповідність між всією документацією і реалізацією поточної версії КЗЗ							
Система керування конфігурацією також повинна використовуватися для генерації КЗЗ з вихідного коду і обліку всіх змін з появою нових версій	-	-	-	+	=	=	=
Система керування конфігурацією повинна бути здатна видавати звіти про стан елементів конфігурації	-	-	-	+	=	=	=
Повинна використовуватися система заходів технічної, фізичної, організаційної і кадрової безпеки, спрямованих на захист усіх засобів і матеріалів, використовуваних для генерації КЗЗ, від несанкціонованої модифікації або руйнування	-	-	-	-	-	+	=

* Починаючи з рівня Г-4 система керування конфігурацією повинна базуватися на автоматизованих засобах.

18.1.7.3. Послідовність розробки

Вимоги до процесу проектування забезпечують гарантії того, що на кожній стадії розробки (проектування) існує точний опис ТЛК-системи, а реалізація ТЛК-системи точно відповідає вихідним вимогам (політиці безпеки).

Рівні деталізації. Вимоги до процесу проектування передбачають наявність чотирьох основних рівнів деталізації ТЛК-системи у процесі її створення: функціональна специфікація, проект архітектури, детальний проект, реалізація. У процесі перевірки дотримання вимог виконується аналіз коректності опису ТЛК-системи для кожного рівня деталізації і його відповідності опису попереднього рівня. В документах, в яких наведені описи для кожного рівня деталізації, можуть використовуватись посилання на інші документи.

Стиль специфікації. В залежності від рівня гарантій і рівня деталізації передбачається можливість використання трьох способів (стилів) специфікації: неформалізований, частково формалізований і формалізований Неоднозначність специфікацій зменшується з використанням більш високого рівня формалізації.

Неформалізована специфікація має стиль текстового документа мовою повсякденного спілкування (російська, українська). Для неформалізованої специфікації вимагається представити визначення термінів, що використовуються в контексті, які відрізняються від звичайних, що використовуються у повсякденній мові.

Частково формалізована специфікація складається мовою з обмеженим синтаксисом і доповнюється поясненнями, написаними мовою повсякденного спілкування. Мова з обмеженим синтаксисом може являти собою повсякденну мову з жорсткою структурою речення і ключовими словами, що мають спеціальне значення, або бути діаграматичною (наприклад, діаграми потоків даних, станів або переходу). Для побудови частково формалізованої специфікації як на базі діаграм, так і на базі мови повсякденного спілкування, необхідно сформулювати набір угод, що визначають обмеження синтаксису.

Формалізовані специфікації мають представлення, яке базується на добре встановлених математичних концепціях, і

супроводжуються поясненнями звичайною мовою. Ці математичні концепції використовуються для визначення синтаксису і семантики подань і несуперечливих правил доказу, які підтримуються логічними посиланнями. Властивості, критичні для безпеки, повинні виражатися мовою формалізованої специфікації. Формалізовані представлення повинні дозволяти описати і ефект (результат) виконання функції, і всі зв'язані з нею виняткові або помилкові умови. Якщо використовуються ієрархічні специфікації, то необхідно показати, що кожний рівень включає властивості, встановлені для попереднього рівня.

Вимоги до відповідності специфікацій рівня. Критерії гарантій щодо послідовності розробки включають вимоги до відповідності специфікацій рівня деталізації. Рівень зусиль, необхідних для досягнення такої відповідності, зростає разом з рівнем гарантій. Для його характеристики використовують терміни "показати", “продемонструвати" або "довести".

Якщо від Розробника вимагається показати повну відповідність між представленнями ТЛК-системи, це означає, що є необхідністю наявність відповідності тільки між основними елементами кожної специфікації. Прикладом може бути використання таблиці, елементи якої відображають відповідність, або використання належного представлення діаграми проекту.

Якщо від Розробника вимагається продемонструвати повну відповідність між представленнями ТЛК-системи, то вимагається наявність відповідності між більш дрібними елементами кожної специфікації. Демонстрація відповідності виконується на основі аналізу з використанням структурованого наукового підходу, що дає переконливі аргументи на користь того, що існує повна відповідність між елементами двох специфікацій.

Якщо від Розробника вимагається довести повну відповідність між представленнями ТЛК-системи, то необхідним є наявність відповідності між ще більш дрібними елементами кожної специфікації. Відповідність між елементами має бути виражена формально.

Функціональні специфікації. Функціональні специфікації повинні описувати, які послуги надає ТЛК-система у разі мінімуму або повної відсутності інформації про те, як вони представлені.

Послуги безпеки описуються у формі політики безпеки і моделі політики безпеки.

Політика безпеки описує ТЛК-систему як набір послуг безпеки. Кожна послуга описується відповідно до вимог функціональних критеріїв для певного рівня даної послуги і з урахуванням необхідних умов. Для всіх рівнів гарантій політика безпеки подається у стилі неформалізованої специфікації і показується її відповідність більш деталізованій специфікації. Фактично, політика безпеки може бути визначена в технічному завданні на ТЛК-систему.

Модель політики безпеки дозволяє точніше виразити вимоги політики безпеки. Стиль специфікації моделі політики безпеки варіюється залежно від рівнів гарантій від неформалізованого до формалізованого. Для всіх рівнів гарантій показується відповідність моделі політики безпеки більш деталізованій специфікації.

Проект архітектури. Проект архітектури є старшим або верхнім рівнем специфікації проекту, який відображає функціональну специфікацію в основні компоненти проекту ТЛК-системи. Для кожного з основних компонентів ТЛК-системи проект архітектури описує його призначення і функції, визначає послуги безпеки, що реалізуються ним. Взаємодія всіх компонентів також визначається на даному етапі. Ця взаємодія представляється на рівні зовнішніх інтерфейсів, потоків даних, керування і т. ін. Проект архітектури описує, яку функцію виконує кожний компонент. Опис того, як компонент виконує свої функції всередині, не вимагається.

Детальний проект. Детальний проект є нижнім і найбільш детальним рівнем специфікації, який поділяє проект архітектури на менші за обсягом проекти його компонент. Детальний проект повинен мати достатню міру деталізації, щоб дозволити почати реалізацію. Для кожного компонента детальний проект повинен містити опис його призначення і функцій. Має бути визначений порядок взаємодії всіх компонентів. Ця взаємодія представляється на рівні зовнішніх інтерфейсів потоків даних, керування і т. ін. Детальний проект описує і те, яку функцію виконує кожний компонент, і те, як він це робить, включаючи алгоритми і

внутрішні інтерфейси. Для детального проекту допускається наявність деяких проміжних специфікацій, кожна з яких характеризується більшим рівнем деталізації порівняно з попередніми.

Реалізація. Реалізація є завершальним представленням ТЛК-системи, що складається з програмного, програмно-апаратного і апаратного забезпечення. Кожний компонент реалізації повинен бути створений і документований відповідно до вимог процесу проектування. Інтерфейси та інші компоненти, що згадуються, повинні бути описані в документації. Для найбільш високих рівнів гарантій вимагається представлення обраних дільниць вихідного коду.

Специфікації гарантій послідовності розробки представлені в табл.18.25.

Послідовність розробки

Вимоги до процесу проектування (послідовності розробки) забезпечують гарантії того, що на кожній стадії розробки (проектування) існує точний опис ТЛК-системи, а реалізація ТЛК-системи точно відповідає вихідним вимогам (політиці безпеки).

Таблиця 18.25

Специфікації гарантій послідовності розробки

Вимоги	**Г-1**	**Г-2**	**Г-3**	**Г-4**	**Г-5**	**Г-6**	**Г-7**
Функціональні специфікації (політика безпеки)							
На стадії розробки технічного завдання Розробник повинен розробити функціональні специфікації ТЛК-системи. Представлені функціональні специфікації повинні включати неформалізований опис політики безпеки, що реалізується КЗЗ. Політика безпеки повинна містити перелік і	+	=	=	=	=	=	=

опис послуг безпеки, що надаються КЗЗ							
Функціональні специфікації (модель політики безпеки)							
Відповідність політиці безпеки	-	Показ		Демонстрація			
Функціональні специфікації повинні включати модель політики безпеки	-	+	=	=	=	=	=
Стиль специфікації: неформалізована	-						
частково формалізована	-						
формалізована	-						
Проект архітектури							
Відповідність моделі політики безпеки	-	Показ			Демонстрація	Доказ	
На стадії розробки ескізного проекту Розробник повинен розробити проект архітектури КЗЗ. Представлений проект повинен містити перелік і опис компонентів КЗЗ і функцій, що реалізуються ними. Повинні бути описані будь-які використовувані зовнішні послуги безпеки. Зовнішні інтерфейси КЗЗ повинні	+	=	=	=	=	=	=

бути описані в термінах винятків, повідомлень про помилки і кодів повернення							
Стиль специфікації: неформалізована							
частково формалізована							
формалізована							
Вимоги	**Г-1**	**Г-2**	**Г-3**	**Г-4**	**Г-5**	**Г-6**	**Г-7**
Детальний проект							
Відповідність проекту архітектури	-	Показ				Демонстрація	Доказ
На стадіях розробки технічного проекту або робочого проекту Розробник повинен розробити детальний проект КЗЗ. Представлений детальний проект повинен містити перелік всіх компонентів КЗЗ і точний опис функціонування кожного механізму. Повинні бути описані призначення і параметри інтерфейсів компонентів КЗЗ	+	=	=	=	=	=	=
Стиль специфікації: неформалізована		Весь КЗЗ *					

частково формалізована							
формалізована							
Реалізація							
Відповідність детальному проекту	-	-	Показ				Демонстрація
Розробник повинен подати вихідний код: частини КЗЗ	-	-	+	=	=	=	=
всього КЗЗ	-	-	-	-	+	=	=
всіх бібліотек часу виконання	-	-	-	-	-	-	+

* Для рівня Г-1 вимагається детальний проект компонентів КЗЗ, що мають безпосереднє відношення до безпеки.

18.1.7.4. Середовище функціонування

Вимоги до середовища функціонування ТЛК-системи забезпечують гарантії того, що ТЛК-система поставляється замовнику без несанкціонованих модифікацій, а також інсталюється і ініціалізується замовником так, як це передбачається Розробником. Оцінка ТЛК-системи забезпечує гарантії того, що ТЛК-система правильно реалізує політику безпеки і правильно функціонує, і будується на припущенні, що функціонування ТЛК-системи починається з безпечного стану. Дотримання вимог даного розділу критеріїв гарантій дозволяє забезпечити впевненість, що це припущення є правильним для всіх оцінюваних ТЛК-систем.

По-перше, Розробник повинен гарантувати, що конфігурація ТЛК-системи, яка поставляється замовнику, є сертифікованою конфігурацією.

По-друге, під час постачання Розробник повинен забезпечити захист ТЛК-системи від несанкціонованої модифікації. Цей захист за своєю природою може бути технічний, організаційний або фізичний. Технічний захист може полягати, наприклад, у

використанні шифрування або криптографічних контрольних сум, паролів, що відкривають доступ до критичного ПЗ, перевірок на відповідність ПЗ еталону і т. ін. Організаційний захист може полягати, наприклад, у перевірці конфігурації для досягнення впевненості в тому, що замовнику поставлена потрібна версія, для чого можуть застосовуватися процедури керування якістю, задіяні Розробником при пакуванні ТЛК-системи. Фізичний захист може полягати, наприклад, у використанні вакуумної упаковки компонент ПЗ і документації і використанні інших оболонок, що запобігають або фіксують спроби фізичного доступу.

По-третє, коли ТЛК-система доставлена і її цілісність перевірена, замовнику необхідні інструкції з інсталяції і ініціалізації ТЛК-системи. Наведені вказівки повинні описувати всі параметри конфігурування і можливі обмеження.

Специфікації гарантій середовища функціонування наведені в табл.18.26.

Середовище функціонування

Вимоги до середовища функціонування забезпечують гарантії того, що ТЛК-система поставляється Замовнику без несанкціонованих модифікацій, а також інсталюється і ініціюється Замовником так, як це передбачається Розробником.

Таблиця 18.26

Специфікації гарантій середовища функціонування

Вимоги	**Г-1**	**Г-2**	**Г-3**	**Г-4**	**Г-5**	**Г-6**	**Г-7**
Розробник повинен представити засоби інсталяції, генерації і запуску ТЛК-системи, які гарантують, що експлуатація ТЛК-системи починається з безпечного стану. Розробник повинен	+	=	=	=	=	=	=

представити перелік усіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації і запуску							
Повинна існувати система технічних, організаційних і фізичних заходів безпеки, яка гарантує, що програмне і програмно-апаратне забезпечення КЗЗ, яке поставляється Замовнику, точно відповідає еталонній копії	-	-	+	=	=	=	=
Для підтримки відповідності між КЗЗ, що поставляється Замовнику, і еталонною копією повинна існувати система керування розповсюдженням захищеної ТЛК-системи	-	-	-	-	-	+	=

Документація

Вимоги до документації є загальними для всіх рівнів гарантій.

У вигляді окремих документів або розділів (підрозділів) інших документів Розробник повинен подати опис послуг безпеки, що реалізуються КЗЗ, настанови адміністратору щодо послуг безпеки, настанови користувача щодо послуг безпеки.

В описі функцій безпеки повинні бути викладені основні, необхідні для правильного використання послуг безпеки, принципи політики безпеки, що реалізується КЗЗ оцінюваної ТЛК-системи, а також самі послуги.

Настанови адміністратору щодо послуг безпеки мають містити опис засобів інсталяції, генерації і запуску ТЛК-системи, опис всіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації і запуску ТЛК-системи, опис властивостей ТЛК-системи, які можуть бути використані для періодичної оцінки правильності функціонування КЗЗ, а також інструкції щодо використання адміністратором послуг безпеки для підтримки політики безпеки, прийнятої в організації, що експлуатує ТЛК-систему.

Настанови користувачу щодо послуг безпеки мають містити інструкції щодо використання функцій безпеки звичайним користувачем (не адміністратором).

Назва документів (розділів) не регламентується. Опис послуг безпеки може відрізнятися для користувача і адміністратора. Настанови адміністратору і настанови користувачу можуть бути об'єднані в настанови з установлення і експлуатації.

18.1.7.5. Документація

Для того, щоб замовник зміг повною мірою використати послуги безпеки, що надаються ТЛК-системою для реалізації політики безпеки, встановленої в його організації, йому необхідна відповідна документація, в якій були б описані ці послуги і дані вказівки щодо їх використання.

У складі експлуатаційної документації Розробник повинен подати опис послуг безпеки, що реалізуються КЗЗ оцінюваної ТЛК-системи, настанови адміністратору щодо послуг безпеки і настанови користувачу щодо послуг безпеки. Зміст цих документів

залежить від політики безпеки, що реалізується ТЛК-системою. Ніяких особливих вимог до назв, формату або структур документів дані Критерії не ставлять.

Документація може бути загальною або в ній можуть бути явно виділені документи (розділи), призначені для адміністратора безпеки і для звичайного користувача. В будь-якому випадку наведеної в документації інформації повинно бути достатньо для того, щоб і адміністратор, і звичайні користувачі мали змогу виконувати свої функції.

18.1.7.6. Випробування комплексу засобів захисту

Для демонстрації того, що КЗЗ оцінюваної ТЛК-системи піддавався випробуванням, і доказу повноти цих випробувань Розробник повинен мати документально оформлені результати випробувань. При організації випробувань послуг безпеки і механізмів захисту і документуванні їх результатів треба керуватися вимогами ДСТУ 2853-94, ДСТУ 2851-94 та ін. Вимоги до випробувань визначають такі основні елементи планування і проведення випробувань Розробником: план випробувань, програма і методика випробувань і результати випробувань (журнал випробувань, звіт, протокол випробувань).

В плані випробувань повинна бути викладена стратегія випробувань Розробника. План повинен надавати детальний опис всіх тестованих частин КЗЗ. Сюди входять зовнішні інтерфейси КЗЗ, всі політики, привілеї, механізми послуг захисту і специфічних викликів системних функцій, бібліотечного ПЗ і т. ін. План має також відображати середовище випробувань, будь-які особливі умови, що створюються для проведення випробувань, і засоби випробувань. Повинні бути наведені аргументи на користь повноти тестового покриття.

Програма і методика випробувань повинна визначати процедури тестування кожного елемента, визначеного у плані випробувань (наприклад, системних викликів). Для кожного окремого тесту має бути докладно описано використання засобів випробувань, необхідне оточення і особливі умови. Рівень деталізації процедур випробувань має бути достатнім для наступного повторення

випробувань. Розробник повинен також описати очікувані результати кожного тесту.

Інформація, що міститься в документах, які представляють результати випробувань, дозволяє оцінити реальну ефективність і повноту проведених випробувань, їх відповідність плану, програмі і методиці, а також організувати проведення сертифікаційних випробувань.

Специфікації вимог щодо проведення випробувань комплексу засобів захисту наведені в табл.18.27.

Випробування комплексу засобів захисту.

Таблиця 18.27

Специфікації вимог щодо проведення випробувань комплексу засобів захисту

Вимоги	**Г-1**	**Г-2**	**Г-3**	**Г-4**	**Г-5**	**Г-6**	**Г-7**
Розробник повинен подати для перевірки програму і методику випробувань, процедури випробувань усіх механізмів, що реалізують послуги безпеки. Мають бути представлені аргументи для підтвердження достатності тестового покриття	+	=	=	=	=	=	=
Розробник повинен подати докази тестування у вигляді детального переліку результатів тестів і відповідних процедур тестування, з тим, щоб отримані результати могли бути перевірені шляхом повторення тестування	+	=	=	=	=	=	=

Розробник повинен усунути або нейтралізувати всі знайдені “слабкі місця” і виконати повторне тестування КЗЗ для підтвердження того, що виявлені недоліки були усунені і не з'явилися нові “слабкі місця ”	-	+	=	=	=	=	=
Розробник повинен виконати тести з подолання механізмів захисту і довести, що КЗЗ відносно або абсолютно стійкий до такого роду атак з боку Розробника	-	-	-	+	=	+	=

18.2. Методика оцінки захищеності інформації в АТС

18.2.1. Порядок оцінки захищеності інформаційних ресурсів АТС

На етапі оцінки захищеності інформаційних ресурсів АТС послідовно виконуються такі види робіт (див. рис.18.28):

- перевірка коректності побудованої моделі загроз;

- перевірка коректності побудованої моделі захисту;

- перевірка коректності проекту КЗМЗ;

- перевірка коректності реалізації КЗМЗ;

- перевірка виконання нормативних вимог до конструкторської й експлуатаційної документації на систему ТЗІ для оцінюваної АТС відносно заявленого рівня довіри;

- перевірка дотримання нормативних гарантій забезпечення захищеності інформації в технологічних середовищах створення й

експлуатації оцінюваної АТС, включаючи систему ТЗІ, відносно заявленого рівня довіри.

Цілями оцінки АТС за критеріями ТЗІ є:

- підтвердження ефективності і коректності розробленої і реалізованої на АТС системи ТЗІ;

- підтвердження заявленого рівня довіри до висновку про коректність системи ТЗІ в оцінюваній АТС.

Процес оцінки АТС за критеріями ТЗІ регламентований базовою методикою оцінки ефективності захисту, викладеною в НД ТЗІ 2.3 - 001 - 99 . Ця методика ґрунтується на специфікаціях ФПЗ (див. НД ТЗІ 2.5-001-99), специфікаціях гарантій захищеності інформації (див. НД ТЗІ 2.5-002-99) і специфікаціях довірчих оцінок коректності реалізації захисту (див. НД ТЗІ 2.5 - 003 - 99).

Крім того, у процесі оціночних робіт використовуються окремі спеціалізовані методики оцінки якості ТЗІ від НСД, витоків та спеціальних впливів.

Ступінь впевненості в коректності створеної системи ТЗІ у вигляді заявленого до оцінки рівня довіри (будь-якого із шести градацій - від Е1 до Е6) і рівень захищеності інформаційних ресурсів у вигляді певної множини функцій безпеки, для яких зазначені рівні стійкості створених механізмів захисту, вказуються Заявником у процесі оформлення заявки на виконання оціночних робіт. Така заявка направляється на адресу уповноваженого державою експертного органа.

Процес оцінювальних робіт у випадку сертифікації АТС за критеріями ТЗІ регламентується нормативними документами УкрСЕПРО - зокрема, ДСТУ 3413-96.

Розглянувши заявку, експертний орган надає Заявнику поштові реквізити оцінювачів - незалежних від Заявника організацій (як правило, випробувальних лабораторій або центрів), що мають право і здатні виконувати роботи з оцінки захищеності інформаційних ресурсів АТС на тому рівні довіри до результатів оцінки, який влаштовує Замовника.

Далі, відповідно до правил, що регламентовані в ДСТУ 3413-96, укладається договір між Заявником, що виступає за Замовника, і Оцінювачем, що виступає за Виконавця, на проведення оціночних робіт із метою одержання позитивного або негативного висновку про те, чи дійсно система ТЗІ на оцінюваній АТС коректно забезпечує заявлений (очікуваний) рівень захищеності інформаційних ресурсів АТС, і у випадку підтвердження коректності системи захисту, чи дійсно ступінь довіри до висновку про коректність системи захисту перебуває на одному із нормованих рівнів, що зазначив Заявник у заявочних документах.

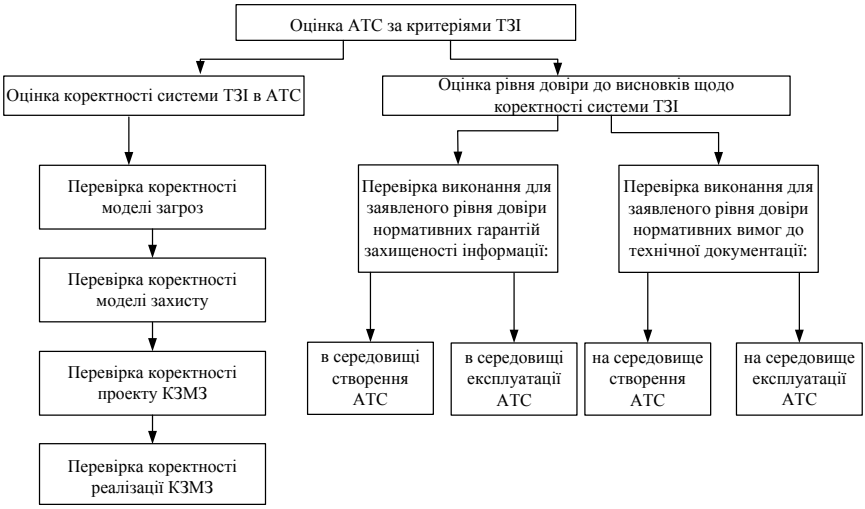


Рис. 18.9 – Порядок оцінки АТС за критеріями ТЗІ

У процесі оціночних робіт може з'ясуватися, що який-небудь аспект оціночного рівня не виконується, наприклад, через відсутність необхідної інформації або внаслідок того, що реальна характеристика оцінюваного об'єкта не відповідає специфікаційним вимогам. У такому випадку Заявнику надається право в заздалегідь обумовлені строки усунути зауваження (наприклад, надати відсутню інформацію, виправити помилку, доробити елемент захисту і т. ін.). У протилежному випадку, оцінюваний об'єкт буде мати результат оцінки на рівні ЕО.

За результатами оцінки Оцінювач надає Заявнику звіт, в якому

вказується результат оцінки.

У випадку негативного висновку в звіті докладно і конкретно з посиланнями на відповідні НД наводяться аргументи і пояснюються причини, що спонукали Оцінювача зробити вивід про невідповідність результатів оцінки до очікуваної цілі.

У випадку позитивного висновку Оцінювачем і Заявником спільно готуються відповідні документи (див. додатки до НД ТЗІ 3.2- 002-99) для подання в експертний орган із метою одержання формального юридично дієвого документа, що підтверджує коректність зазначеної в ньому структури системи ТЗІ на АТС із рівнем довіри, що відповідає зазначеному нормативному рівню довіри.

Таким чином, у названому вище документі вказується:

– структура створеної на АТС системи ТЗІ у вигляді множини функцій безпеки з реалізованими рівнями стійкості механізмів захисту, коректність якої підтверджується;

– підтверджене значення рівня довіри (у межах від Е1 до Е6) до коректності зазначеної в документі структури системи ТЗІ.

Для того, щоб оцінка була виконана ефективно і з мінімальними витратами, Оцінювач може співробітничати із Заявником і (або) Розроблювачем системи ТЗІ, проте Оцінювач повинний бути незалежним (не приймати участі у розробці системи ТЗІ для оцінюваної АТС).

Для виконання оціночних робіт Заявник повинен надати Оцінювачу можливість проведення спеціальних експериментальних досліджень програмних і технічних засобів оцінюваної АТС на розгорнутому працездатному зразку виробу (системи), штатні контрольно-вимірювальні і діагностичні засоби, необхідну технічну й організаційно-розпорядницьку документацію.

Зміст і обсяг проведених у процесі оцінки експериментальних досліджень, перелік, зміст і форма необхідних для аналізу документів, рівень старанності (формалізації, деталізації, строгості) обгрунтувань і доказів, наданих Заявником щодо різних аспектів реалізованої на АТС системи ТЗІ, однозначно залежать від заявленого рівня довіри до коректності системи захисту. Така залежність відображена у відповідних специфікаційних вимогах НД ТЗІ 2.5 - 003 - 99.

Заявник несе повну відповідальність за працездатність наданого у розпорядження Оцінювача зразка виробу (системи), за працездатність і своєчасну перевірку штатних контрольно-вимірювальних і діагностичних засобів, за точність (слушність) наданої документації.

У базовій методиці НД ТЗІ 2.3 - 001 - 99 для кожного оціночного рівня визначені вимоги до переліку, змісту і форми документів, що повинний передати Заявник у розпорядження Оцінювача, і, отже, заздалегідь їх підготувати ще до проведення оціночних робіт.

У процесі оцінювання за вищими рівнями довіри виникає необхідність у розробці і виготовлені спеціальних схем дослідження "слабких місць", глибоких тестів " на проникнення", моделюванні дій "хакерів", формального опису політики безпеки. Всю вище перераховану роботу повинний узяти на себе Заявник і відповідати за повноту і коректність її виконання. Оцінювач може взяти на себе роботу з перегляду наданих Заявником тестів, моделей, схем, аналізів, обґрунтувань і доказів, має право їх доповнювати й удосконалювати, досліджувати власними методами і засобами слабкі місця у захисті.

Для всіх оціночних рівнів, за винятком Е1, Оцінювач повинний переважно перепровіряти результати випробувань і аналізу, які Заявник надав у його розпорядження.

На оціночному рівні Е1 оцінка може робитися тільки за результатами аналізу документації користувача. Заявник у цьому випадку може і не давати результати випробувань створеної на АТС системи ТЗІ.

Контрольні питання до вісімнадцятої лекції

1.Яка побудова та структура критеріїв захищеності інформації у НД ТЗІ 2.5-004-99 ?

2. Назвіть функціональні послуги із протидії порушенням конфіденційності.

3. Назвіть функціональні послуги із протидії порушенням цілісності.

4. Назвіть функціональні послуги із протидії порушенням доступності.

5. Назвіть функціональні послуги із забезпечення спостереженості.

6. Назвіть вимоги щодо забезпечення гарантії коректності архітектури КЗЗ.

7. Назвіть вимоги щодо забезпечення гарантії коректності середовища розробки.

8. Назвіть вимоги щодо забезпечення гарантії послідовності розробки.

9. Назвіть вимоги щодо забезпечення гарантії коректності середовища функціонування.

10. Які вимоги до документації на ТЛК-систему?

11. Які специфікації вимог щодо проведення випробувань комплексу засобів захисту.

Навчальне видання

КОНАХОВИЧ Георгій Филимонович,
ЧУПРИН Володимир Михайлович
ТКАЛІЧ Олег Петрович
МАЧАЛІН Ігор Олексійович
ЕКСПЛУАТАЦІЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

ПІДРУЧНИК

Технічний редакторА.І. Лавринович
Коректор Л.М. Романова

Підп. до друку _____ Формат 60х84/16. Папір офс.
Офс.друк. Ум. друк арк. _____.Обл.-вид. арк._____
Тираж_____ пр. Замовлення №_____. Вид. №_____.

иуніверситету «НАУ-друк»

03058. Київ-58, навта Комарова, 1.

Свідоцтво про внесення до Державного реєстру ДК № 977 від 05.07.2002