Кафедра організації та технічного забезпечення
аварійно-рятувальних робіт
Національного університету цивільного захисту України

АВТОМАТИЗОВАНІ СИСТЕМИ УПРАВЛІННЯ ТА ТЕЛЕКОМУНІКАЦІЇ

Курс лекцій

Харків 2023

Підготовлено до друку за рішенням
засідання організації та технічного
забезпечення аварійно-рятувальних
робіт НУЦЗ України
Протокол від 28.08.23 № 1

Укладач: Л.В.Борисова

Рецензенти:
Л.О. Нікітіна, заступник завідувача кафедри систем інформації факультету комп'ютерних та інформаційних технологій Національного технічного університету «Харківський політехнічний інститут» кандидат технічних наук, доцент
В. В. Тютюник, начальник кафедри управління та організації діяльності у сфері цивільного захисту факультету цивільного захисту НУЦЗ України.

Автоматизовані системи управління та телекомунікації: курс лекцій / Укладач Л.В.Борисова – Х.: НУЦЗУ, 2023. – 200 с.

Курс лекцій відповідає змісту навчальної дисципліни «Автоматизовані системи управління та телекомунікації», охоплює описання характеристик, варіантів структурної побудови та архітектурного описання, а також основних технологій і протоколів сучасних телекомунікаційних мережею.

Рівень викладення матеріалу дозволяє використовувати його у навчальному процесі для курсантів, студентів та слухачів під час роботи на посаді інженер, науковець, практичний фахівець, які працюють у сфері пожежної безпеки та цивільного захисту.

ЛЕКЦІЯ 1. ЗВ'ЯЗОК ТА ІНФОРМАТИЗАЦІЯ В ДСНС УКРАЇНИ

План

Вступ

1.1 Нормативне забезпечення організації зв'язку та інформатизації в ДСНС України.

1.2 Сучасний стан телекомунікаційного простору України.

1.3 Інформаційне середовище сучасного суспільства.

1.4 Реформування системи Державної служби України з надзвичайних ситуацій

Висновки

Література

1. Теоретичні основи телекомунікаційних мереж : навч. посіб. /М.М Климаш, Б.М.Стрихалюк, М.В.Кайдан. – Львів : вид-во УАД, 2011. – 496 с.

2. Кривуца В.Г. Система управління сучасними телекомунікаційними мережами / Кривуца В.Г., Беркман Л.Н. та ін. / – К. : Зв'язок, 2009. –352 с.

3. Буров Є. Комп'ютерні мережі / Є.Буров. – Львів : БаК, 1999. – 468 с.

Вступ

Рівень інформатизації будь-якої країни, ступінь її залучення до глобального інформаційного суспільства, визначається розвитком інформаційних комунікацій. Основу інформаційних комунікацій формують інформаційні мережі, які базуються на телекомунікаційних мережах. На шляху еволюційного розвитку телекомунікаційних мереж виокремлюють три етапи: аналоговий, цифровий та етап телекомунікаційно-комп'ютерної інтеграції.

Перший етап характеризує епоху аналогової телефонії, де середовищем передавання переважно були мідні кабелі. Багатоканальні системи передавання будували за принципом частотного розподілу телефонних каналів. Розподіл інформації здійснювався за принципом комутації каналів із використанням електромеханічних (декадно-крокових, координатних) або в кращому випадку квазіелектронних автоматичних телефонних станцій. В Україні до 1991 року також існувала аналогова мережа зв'язку, яка в основному задовольняла потреби населення, народного господарства, громадських інститутів у послугах електричного зв'язку.

Зародження етапу цифрового зв'язку розпочато з моменту формулювання та доведення теореми Котельникова (1933 рік) та розробки основ теорії потенційної завадостійкості (1946 рік). Досягнення мікро-, нано- та оптоелектроніки уможливили створення апаратури цифрового зв'язку. Із появою нових телекомунікаційних технологій, орієнтованих на пакетний спосіб передавання інформації (оптичне волокно, радіочастотний ресурс) та забезпечення мобільності зв'язку, виникла необхідність суттєво підвищити

продуктивність, ефективність та якість обслуговування телекомунікаційних мереж.

Етап телекомунікаційно-комп'ютерної інтеграції означений успіхами як у галузі електроніки, так і комп'ютерних технологій. Інтеграція комп'ютерів з телекомунікаціями у якості термінальних і комунікаційних пристроїв, а також досягнення в галузі інформаційних технологій стали підґрунтям створення інформаційних мереж. Це дало змогу накопичувати в електронному вигляді, зберігати й обробляти значні ресурси інформації та надавати її користувачам за їх запитами у зручний для них час.

На сьогодні розвиток інформаційного суспільства та поширення інформаційно-комунікаційних технологій стали нормою подальшої еволюції суспільства. Завдяки надзвичайно могутнім інформаційним технологіям почався процес переходу від індустріальної епохи, цифрового інформаційного суспільства до суспільства знань, яке характеризується значною кількістю циркулюючої комунікаційними каналами зв'язку інформації, наявністю необхідних засобів її збереження, передавання, оброблення, використання та захисту, обчислювальної техніки, програмного забезпечення. В Індексі розвитку інформаційно-комунікаційних технологій Міжнародного союзу електрозв'язку Індексі, останнє дослідження якого опубліковано за підсумками 2017 року, в списку відповідно за 11 критеріями, в число яких входять як можливість доступу до ІТ-технологій, так і широта їх використання та вміння населення ними користуватися, Україна знаходиться на 79 місці.

Розвиток ДСНС України та цивільного захисту не можливий без постійного технологічного переоснащення та різноманітних інноваційних процесів. Інформаційно-комунікаційні технології сьогодні відіграють важливу роль для підвищення ефективності реагування на надзвичайні ситуації природного та техногенного характеру. Телекомунікаційні системи цивільного захисту – це складні системи як за своєю структурою, так і функціями, які вони виконують. Мережі телекомунікацій можуть охоплювати як окремий підрозділ ДСНС, так і всю земну кулю.

Згідно з Постановою КМУ від 29 червня 2004 р. № 812 «Порядок оперативно-технічного управління телекомунікаційними мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану» (редакція від 06.02.2019) *ДСНС України, як спеціальний споживач телекомунікаційних мереж*, *з метою впорядкування роботи відомчої інформаційно-комунікаційної мережі ДСНС здійснює загальний контроль за готовністю та функціонуванням телекомунікаційних мереж* в умовах надзвичайних ситуацій, надзвичайного та воєнного стану.

Оповіщення та інформування населення згідно до Кодексу Цивільного Захисту України у Розділі IV «Захист населення і територій від надзвичайних ситуацій» (ст. 30) забезпечується шляхом: *централізованого використання телекомунікаційних мереж загального користування, у тому числі мобільного (рухомого) зв'язку, відомчих телекомунікаційних мереж* і телекомунікаційних мереж суб'єктів господарювання в порядку, встановленому Кабінетом Міністрів

України, а також мереж загальнонаціонального, регіонального та місцевого радіомовлення і телебачення та інших технічних засобів передавання (відображення) інформації.

Розвиток інформаційно-комунікаційних технологій встановлює, що межі модернізації програмно-технічного забезпечення не повинні знаходитись у яких-небудь рамках, вони повинні мати можливість гнучко змінюватися з урахуванням вимог та сучасних умов для безперебійного функціонування зв'язку, телекомунікацій та інформатизації в системі ДСНС.

1.1 Нормативне забезпечення організації зв'язку та інформатизації в ДСНС України

Телекомунікаційна система є ієрархічною структурою, що включає в себе підсистеми, кожна з яких потребує встановлення адекватного нормативно-правового регулювання.

Правовою основою, спрямованої на забезпечення діяльності сил ДСНС України, є Конституція України, Кодекс Цивільного захисту України, Постанова КМ України від 27.09.2017 № 733 «Про затвердження Положення про організацію оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій та зв'язку в сфері цивільного захисту», Розпорядження КМ України від 31.01.2018 № 43-р «Про схвалення Концепції розвитку та технічної модернізації системи централізованого оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій», Постанова КМ України від 09.01.2014 № 11 «Положення про єдину державну систему цивільного захисту», накази центрального органу виконавчої влади з питань НС, відповідні розпорядження обласної державної адміністрації та інші акти.

У «Положенні про єдину державну систему цивільного захисту» розкриваються наступні питання:

– здійснення керівництва єдиною державною системою цивільного захисту;

– постійно діючі органи управління цивільного захисту, які функціонують в державі;

– координаційні органи єдиної державної системи цивільного захисту;

– сили цивільного захисту, які входять до складу єдиної державної системи цивільного захисту;

– основні завдання, що виконуються єдиною державною системою цивільного захисту;

– режими функціонування єдиної державної системи цивільного захисту;

– загальні питання організації реагування на надзвичайні ситуації та ліквідації їх наслідків;

– порядок здійснення взаємодії та обміну інформацією у разі загрози або виникнення надзвичайних ситуацій та інші питання.

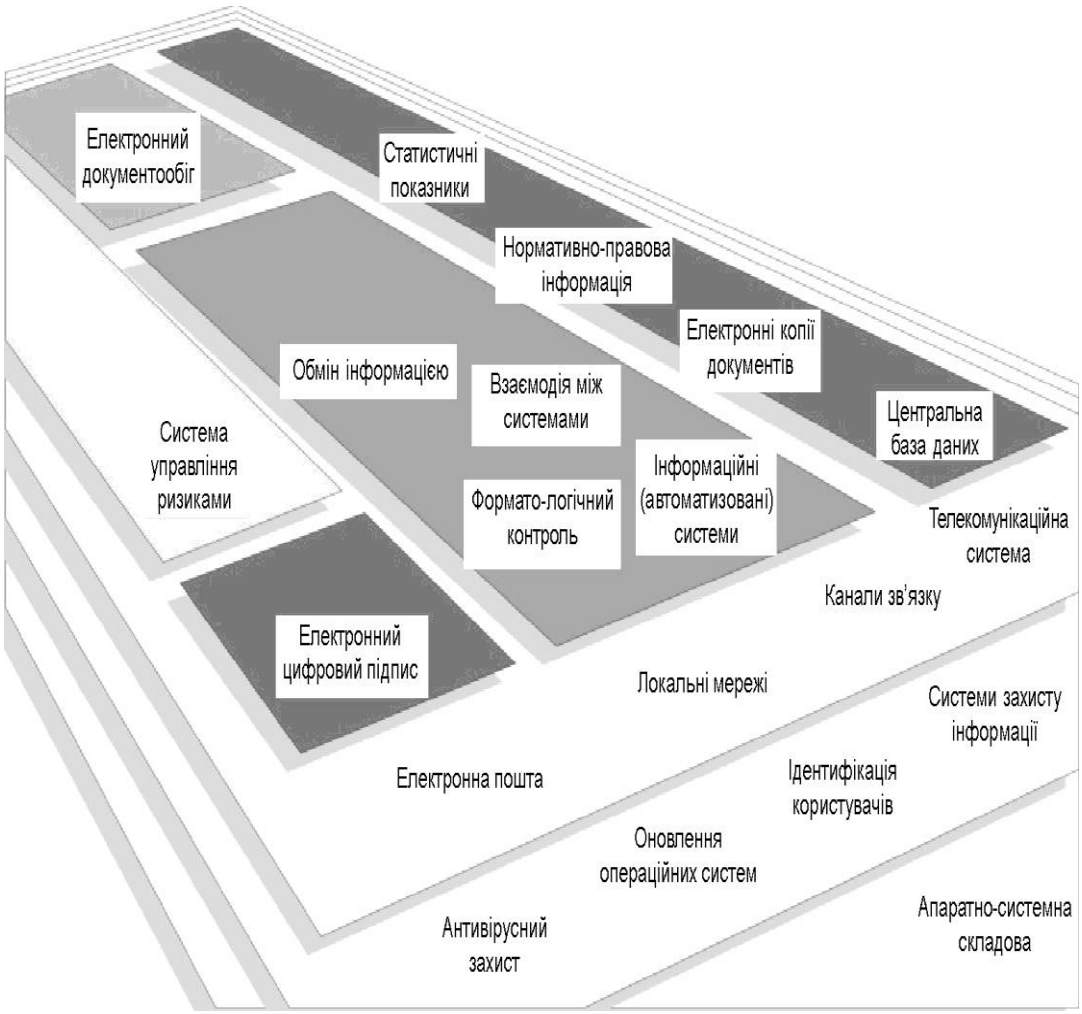


Рисунок 1 – Багатофункціональна інформаційно-комунікаційна система

Багатофункціональною інформаційно-телекомунікаційною системою органу державної влади є сукупність взаємопов'язаних інформаційних, телекомунікаційних і інформаційно-телекомунікаційних систем (рисунок 1), яка включає:

– апаратно-системну складову (сервери, засоби обчислювальної техніки, системне програмне забезпечення тощо);

– системи захисту інформації (інформаційні системи ідентифікації та автентифікації користувачів, моніторингу, антивірусного захисту, оновлення операційних систем тощо);

– телекомунікаційну систему (мережеве устаткування, канали зв'язку, локальні мережі, електронна пошта тощо);

– центральну базу даних, систему електронного документообігу; систему електронного цифрового підпису;

– систему управління ризиками;

– різноманітні відомчі інформаційні системи.

Для забезпечення і регламентування функціонування інформаційно-комунікаційної системи повинні бути розроблені відомчі нормативно-правові

акти як концептуального змісту (першого рівня), так і положення, порядки, регламенти і інструкції (відомчі нормативно-правові акти другого рівня).

У сфері оповіщення

1. Розпорядження КМ України від 31.01.2018 № 43-р «Про схвалення Концепції розвитку та технічної модернізації системи централізованого оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій».
2. Постанова КМ України від 27.09.2017 № 733 «Про затвердження Положення про організацію оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій та зв'язку у сфері цивільного захисту».
3. Наказ МВС України від 05.11.2018 № 884 «Про затвердження технічних вимог до загальнодержавної автоматизованої системи централізованого оповіщення».
4. Наказ МВС України від 08.02.2019 № 93 «Про затвердження Інструкції щодо практик чи процедур проектування, дослідження, введення в експлуатацію, експлуатації та технічного обслуговування (супроводження) автоматизованих систем централізованого оповіщення», зареєстрований у Міністерстві юстиції України 22.04.2019 за № 418/33389.

У сфері інформаційних технологій

Державне агентство з питань електронного урядування України є центральним органом виконавчої влади, діяльність якого спрямовується і координується Кабінетом Міністрів України і який реалізує державну політику у сферах інформатизації, електронного урядування, формування і використання національних електронних інформаційних ресурсів, розвитку інформаційного суспільства.

1. Постанова КМ України від 21. 10. 2015 № 835 «Про затвердження Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних».
2. Постанова КМ України від 8.09.2016 № 606 «Деякі питання електронної взаємодії державних електронних інформаційних ресурсів».
3. Постанова КМ України від 10.09. 2003 № 1433 «Про затвердження Порядку використання комп'ютерних програм в органах виконавчої влади».
4. Наказ ДСНС від 18.08.2014 № 476 «Про використання комп'ютерних програм у ДСНС України».
5. Наказ МНС від 19.11.2012 № 1326 «Про впровадження відомчої системи відеоконференцзв'язку МНС України в експлуатацію».
6. Постанова КМ України від 16.11.2016 № 887 «Про внесення змін до деяких постанов Кабінету Міністрів України щодо діяльності Державного агентства з питань електронного урядування».
7. Постанова КМ України від 10.05.2018 № 357 «Деякі питання організації електронної взаємодії державних електронних інформаційних ресурсів».

8. Постанова КМ України від 21.10.2015 № 851 «Деякі питання використання доменних імен державними органами в українському сегменті Інтернету».

9. Постанова КМ України від 12.06.2019 № 493 «Про внесення змін до деяких постанов Кабінету Міністрів України щодо функціонування офіційних Web-сайтів органів виконавчої влади».

10. Наказ ДСНС від 19.07.2019 № 425 «Про затвердження Порядку використання інформаційних та інформаційно-телекомунікаційних систем і Порядку використання та обліку комп'ютерних програм».

У сфері телекомунікацій

1. Наказ ДСНС від 19.11.2014 № 648 «Про впровадження абонентських комплектів супутникового зв'язку та затвердження тимчасової інструкції».

2. Наказ МНС від 23.02.2012 № 531 «Про заходи щодо побудови та організації дослідної експлуатації відомчої системи IP телефонії».

3. Наказ МНС 02.06.2004 № 42 «Про затвердження Положення про службу радіотехнічного контролю МНС України».

4. Наказ ДСНС від 23.10.2019 № 608 «Про організацію роботи відомчої цифрової телекомунікаційної мережі ДСНС».

У сфері кібербезпеки

1. Закон України від 05.10.2017 № 2163-VIII «Про основні засади забезпечення кібербезпеки України»).

2. Указ Президента України від 13.02.2017 №32/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації».

У сфері технічного захисту інформації

1. Закон України 05.07.1994 № 80/94-ВР «Про захист інформації в інформаційно-телекомунікаційних системах».

2. Указ Президента України від 27.09.1999 № 1229/99 «Про Положення про технічний захист інформації в Україні».

3. Постанова КМ України від 29.03.2006 р. № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах».

4. Наказ ДСНС від 19.12.2014 № 726 «Про забезпечення захисту державних інформаційних ресурсів ДСНС України».

5. Наказ ДСНС від 11.12.2013 № 755 «Про затвердження Положення про технічний захист інформації у Державній службі України з надзвичайних ситуацій».

6. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України, Державного комітету України з питань технічного регулювання та споживчої політики від 25.04.2007 № 75/91 «Про затвердження Правил проведення робіт із сертифікації засобів захисту інформації».

Стандарти

Відповідно до статті 7 Закону України «Про стандартизацію» (від 05.06. 2014 № 1315-VII) національні стандарти приймаються державною мовою або в разі потреби однією з мов відповідних міжнародних або регіональних організацій стандартизації.

1. У галузі зв'язку існує Фонд нормативних документів із стандартизації (Стандарти організації Україна), який функціонує у складі Державного підприємства «Український науково-дослідний інститут зв'язку» (за напрямами «проводовий та поштовий зв'язок») та Державного підприємства «Український науково-дослідний інститут радіо і телебачення» (за напрямами «радіозв'язок і радіомовлення»).

2. Згідно ДСТУ 1.7:2015 (ISO/IEC Guide 21-1:2005, NEQ; ISO/IEC Guide 21-2:2005,NEQ) «Національна стандартизація. Правила та методи прийняття міжнародних і регіональних нормативних документів» для нормативних документів, прийнятих методом підтвердження, передбачено лише оприлюднення підтверджувального повідомлення і не передбачено перекладу або офіційного видання нормативного документа.

3. Електронний каталог НД включає інформацію щодо змін та поправок до НД, терміну чинності, заміни або відміни НД, кодів УКНД та іншої додаткової інформації: URL : http://csm.kiev.ua/nd/nd.php?b=1

4. На даний час в країнах ЄС використовується стандарт Технічного комітету Європейського інституту стандартизації – ETSI 202 057, який стосуються визначення переліку параметрів якості послуг, методів їх вимірювання та оцінювання.

1. СОУ 64.2-00017584-001:2009 Телекомунікаційні мережі фіксованого телефонного зв'язку загального користування. Система показників якості послуг телефонного зв'язку. Загальні положення, який визначає назви показників якості послуг фіксованого телефонного зв'язку.

2. СОУ 64.2-00017584-002:2009 Телекомунікаційні мережі фіксованого телефонного зв'язку загального користування. Телекомунікаційні послуги. Показники якості. Методи випробування.

3. СОУ 64.2- 00017584- 005:2009 Телекомунікаційні мережі рухомого (мобільного) зв`язку загального користування. Система показників якості послуг рухомого (мобільного) зв`язку. Загальні положення.

4. СОУ 64.2-00017584-006:2009 Телекомунікаційні мережі рухомого (мобільного) зв`язку загального користування. Телекомунікаційні послуги. Показники якості. Методи випробування.

5. СОУ 64.2-00017584-008:2010 Телекомунікаційні мережі передачі даних загального користування. Система показників якості послуг з передачі даних та доступу до Інтернет. Загальні положення».

6. СОУ 61-34620942-011:2012 Телекомунікаційні мережі передачі даних загального користування. Телекомунікаційні послуги. Основні показники якості. Методи випробування.

7. ДСТУ ISO/IEC 24759:2015 (ISO/IEC 24759:2014, IDT) Інформаційні технології. Методи захисту. Вимоги до тестування криптографічних модулів.

8. ДСТУ ISO/IEC 24760-1:2016 (ISO/IEC 24760-1:2011, IDT) Інформаційні технології. Методи захисту. Структура керування ідентифікаційною інформацією. Частина 1. Термінологія та поняття.

9. ДСТУ ISO/IEC 24761:2015 (ISO/IEC 24761:2009; Cor 1:2013, IDT) Інформаційні технології. Методи захисту. Контекст автентифікації для біометрії.

10. ДСТУ ISO/IEC 27000:2017 (ISO/IEC 27000:2016, IDT) Інформаційні технології. Методи захисту. Системи менеджменту інформаційної безпеки. Словник термінів.

11. ДСТУ ISO/IEC 27001:2010 (ISO/IEC 27001:2005, IDT) Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги.

12. ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013; Cor 1:2014, IDT) Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги.

13. ДСТУ ISO/IEC 27002:2015 (ISO/IEC 27002:2013; Cor 1:2014, IDT) Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки.

14. ДСТУ ISO/IEC 27006:2015 (ISO/IEC 27006:2011, IDT) Інформаційні технології. Методи захисту. Вимоги до організацій, які надають послуги з аудиту і сертифікації систем управління інформаційною безпекою.

15. ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT) Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки.

16. Стандарт ISO/IEC 15408 Загальні критерії оцінки безпеки інформаційних технологій.

1.2 Сучасний стан телекомунікаційного простору України

Інформаційні технології є фундаментальним наслідком впливу інформації на сучасний світ і полягають у тому, що інформаційна епоха породжує суспільство, яке є не лише глобальним, але ще й мережевим за рахунок інформаційних технологій.

Міжнародний союз електрозв'язку (МСЕ) виділяє триступеневу модель, за якою країни або регіони рухаються у розвитку інформаційного (цифрового) суспільства:

– першим етапом є мережева готовність, яка відображується поширенням інфраструктури інформаційно-комунікаційних технологій (ІКТ) в суспільстві або країні з акцентом на питанні доступу до ІКТ;

– другий етап включає ступінь впровадження ІКТ з наголосом на навичках ефективного використання ІКТ;

– третій етап визначає ефективність використання ІКТ у конкретному суспільстві або регіоні.

В Україні сфера інформаційно-комунікаційних технологій виділена в стратегічний пріоритет, який зафіксований в Стратегії сталого розвитку «Україна – 2020» (2015 рік), де, в розділі 3 «Дорожня карта та першочергові пріоритети реалізації Стратегії», до першочергових реформ віднесені реформа державного управління із застосуванням новітніх інформаційно-комунікаційних технологій та реформа телекомунікаційної інфраструктури.

Парламентські слухання «Реформа галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України» у березні 2016 року показали, що стан розбудови інформаційного суспільства в Україні порівняно із світовими тенденціями є недостатнім. Постановою КМ України від 28.12.2016 №1056 «Деякі питання визначення середньострокових пріоритетних напрямів інноваційної діяльності загальнодержавного рівня на 2017 – 2021 роки» серед пріоритетних напрямів інноваційної діяльності визначений розвиток інформаційно-телекомунікаційної інфраструктури, впровадження новітніх інформаційних технологій.

Нинішній стан телекомунікаційних мереж характеризується конвергенцією мобільної та стаціонарної мереж. Мережі телекомунікацій є складними об’єктами управління для яких характерним є розподільні системи.

Інтелектуалізація мереж телекомунікацій потребує управління такими мережами за протоколами, ґрунтується на розподілі функцій транспорту, комутації та надання послуг, що потребує створення мережі для передавання інформації, забезпечення її розподіленої обробки й збереження, надання традиційних комунікаційних послуг, підтримка послуг і допоміжних програмних продуктів, термінальне устаткування.

У Звіті про роботу Національної комісії, що здійснює державне регулювання у сфері зв’язку та інформатизації за 2018 рік зазначено, що основними тенденціями розвитку телекомунікаційних мереж у 2018 році були:

– продовження розгортання телекомунікаційних мереж рухомого (мобільного) зв’язку четвертого покоління (4G) із застосуванням радіотехнології «Міжнародний рухомий (мобільний) зв’язок ІМТ» в смугах радіочастот 1800 МГц та 2600 МГц;

– активізація процесу впровадження на телекомунікаційних мережах рухомого (мобільного) зв’язку України послуги із перенесення абонентських номерів;

– розпочато процес створення умов для запровадження конвергентних рішень щодо спільного використання фрагментів мереж фіксованого і рухомого (мобільного) зв’язку;

– створення умов для реконструкції та оптимізації телекомунікаційних мереж, шляхом використання сучасного високопродуктивного комутаційного обладнання, здатного обслуговувати декілька зон нумерації; підвищення попиту споживачів на конвергентні телекомунікаційні послуги, послуги

міжмашинної взаємодії (machine-to-machine, M2M) та послуги Інтернету речей (Internet of Things, IoT);

– розпочато процес законодавчого врегулювання питання щодо забезпечення з'єднання головних управлінь Національної поліції України з телекомунікаційними мережами загального користування (ТМЗК) на рівні обласних центрів, що забезпечить централізацію приймання і обробки викликів за скороченим телефонним номером 102;

– забезпечення підготовки та використання телекомунікаційних мереж України в умовах воєнного стану;

– виконання заходів з побудови Національного центру оперативно-технічного управління мережами телекомунікацій України.

Основними проблемами розвитку телекомунікаційних мереж є:

– нерівномірність забезпечення споживачів телекомунікаційними послугами, у тому числі загальнодоступними та послугами широкосмугового доступу до Інтернету в окремих адміністративно-територіальних одиницях України;

– організаційні та технологічні проблеми функціонування телекомунікаційних мереж на тимчасово окупованих територіях, що пов'язано з втручанням у роботу ТМЗК та порушенням майнових прав операторів, провайдерів телекомунікацій України;

– діяльність незаконно створених на тимчасово окупованих територіях суб'єктів господарювання, що не зареєстровані згідно із законодавством України, та які не мають права здійснювати діяльність у сфері телекомунікацій з використанням радіочастотного та номерного ресурсів ТМЗК;

– невиконання вимог Закону України від 7.02.2017 №1834-VIII «Про доступ до об'єктів будівництва, транспорту, електроенергетики з метою розвитку телекомунікаційних мереж» власниками об'єктів інфраструктури, які під всілякими приводами мають наміри обмежити доступ до елементів інфраструктури;

– стала тенденція останніх років до збільшення випадків викрадення та пошкодження кабелів та інших технічних засобів телекомунікацій операторів телекомунікацій, у тому числі викрадення мідних кабелів, що набуло масового характеру.

На сьогодні інформаційно-телекомунікаційній системі притаманні такі риси:

– багатофункціональність, що випливає з необхідності передавання різних видів інформації;

– складність структурної організації і алгоритмів функціонування;

– наявність великої кількості підсистем і елементів, які входять у систему, та їх тісний взаємозв'язок;

– імовірнісний характер процесів функціонування системи, який обумовлений випадковими і навмисними змінами параметрів середовища, а також невизначеним характером потоків інформації;

– великі просторові габарити і динамічність.

Сучасна телекомунікаційна мережа – це інфраструктура, що об’єднує системи передавання інформації за різними технологіями, включаючи новітні.

1.3 Інформаційне середовище сучасного суспільства

Основним завданням розвитку інформаційного суспільства в Україні є сприяння кожній людині на засадах широкого використання сучасних ІКТ можливостей створювати інформацію і знання, користуватися та обмінюватися ними, виробляти товари та надавати послуги, повною мірою реалізовуючи свій потенціал, підвищуючи якість свого життя і сприяючи сталому розвитку країни на основі цілей і принципів, проголошених Організацією Об’єднаних Націй, Декларації принципів та Плану дій, напрацьованих на Всесвітніх зустрічах на вищому рівні з питань інформаційного суспільства (Женева, грудень 2003 р.; Туніс, листопад 2005 р.) та Постанови Верховної Ради України від 1 грудня 2005 р. «Про Рекомендації парламентських слухань з питань розвитку інформаційного суспільства в Україні».

Інформація – один із найважливіших феноменів, органічно і фундаментально «вбудованих» у сучасні парадигми наукового пізнання людини, суспільства, світу.

Інформація є інформація, а не матерія і не енергія. Інформація, за визначенням В. М. Бехтерєва, – «це нематеріальна субстанція, на відміну від речовини або енергії, але від них невід’ємна, як від своїх носіїв». Вставши в один ряд із такими категоріями, як матерія та енергія, інформація перетворилася на надзвичайно широке поняття.

Першим сформулював поняття «інформація» математик Н. Вінер: «Інформація – це визначення змісту, отриманого із зовнішнього світу в процесі нашого пристосування до нього і пристосування до нього наших почуттів. Процес отримання та використання інформації є процесом нашого пристосування до випадковостей зовнішнього середовища нашої життєдіяльності в цьому середовищі».

В. Ровенський, А.Уємов під інформацією розуміють «повідомлення про події, що відбуваються як у зовнішньому по відношенню до системи середовищі, так і в самій системі».

Під інформаційним середовищем розуміють сферу діяльності суб’єктів, пов’язану із створенням, перетворенням і споживанням інформації. Інформаційне середовище умовно поділяється на три основні складові:

– створення і розповсюдження вихідної та похідної інформації;

– формування інформаційних ресурсів, підготовки інформаційних продуктів, надання інформаційних послуг;

– споживання інформації;

– та дві забезпечувальні предметні складові:

– створення і застосування інформаційних систем, інформаційних технологій і засобів їхнього забезпечення;

– створення і застосування засобів і механізмів інформаційної безпеки.

У зв'язку з великомасштабністю інформаційно-комунікаційної системи оцінка її ефективності в методологічному плані повинна базуватися на основних положеннях теорії складних систем, теорії ефективності, теорії ймовірностей, теорії масового обслуговування, теорії дослідження операцій і системного аналізу.

Виникає гостра необхідність застосування основних типів інтелектуальних систем управління:

– інформаційних систем;
– систем підтримки прийняття рішень;
– систем, що навчають;
– експертних систем;
– гібридних систем.

При проектуванні сучасних телекомунікаційних мереж важливими є вимоги надійності та живучості.

Надійність – це функціонування мережі із заданими параметрами протягом певного часу.

Живучість розуміється як здатність мережі нормально функціонувати при дії дестабілізуючих чинників. Оцінка живучості проводиться по максимальній кількості збитку, яку може витримати мережа і система управління нею. Вимога до живучості мережі є базовою в умовах надзвичайних ситуацій.

На телекомунікаційних мережах України працює велика кількість операторів, а це спричиняє проблеми, пов'язані з управлінням мережами, які побудовані з використанням різних технологій і технічних засобів, що створює низку проблем, пов'язаних з їх взаємодією між собою та з Національним центром оперативно-технічного управління телекомунікаційними мережами України (НЦУ) в звичайних умовах і в умовах кризових ситуацій.

За умов надзвичайних ситуацій усі телекомунікаційні мережі на території України мають функціонувати як єдина система телекомунікацій під управлінням НЦУ. Основними за чисельністю елементами Національної системи оперативно-технічного управління телекомунікаційними мережами є головні центри управління усіх телекомунікаційних мереж України – як мереж загального користування (ТМЗК), так і спеціальних телекомунікаційних мереж. Таким чином, НЦУ повинно мати можливість координації ефективного функціонування телекомунікаційних мереж, раціонального використання ресурсів телекомунікацій, включаючи мобільний сегмент.

У зв'язку із збільшенням обсягу обміну інформації в інформаційно-телекомунікаційних мережах, в тому числі і в мережах спеціального призначення, збільшується ризик додаткового навантаження на мережі, що призводить до перевантаження та значного зменшення пропускної здатності мережі, аж до виникнення колапсу, результатом якого є втрата інформації. В зв'язку з цим важливо усвідомити механізм пошуку шляхів протидії

можливому штучному створенню глобального колапсу інформаційно-телекомунікаційних систем.

Перебудова сучасних інформаційних технологій пов'язана з їх переходом на IP-основу, тобто створення єдиного інформаційного середовища, в основі якого лежить принцип мобільного доступу до всіх інформаційних ресурсів.

Сучасні зміни в інформаційно-телекомунікаційних системах поєднується з концепцією мереж нового покоління (Next Generation Network – NGN) – це мультисервісна мережа зв'язку, ядром якої є опорна IP-мережа, що підтримує повну або часткову інтеграцію послуг передачі мови, даних і мультимедіа. Вони створені для того, щоб подолати архітектурні обмеження, властиві традиційним фіксованим телефонним мережам. Це досягається за рахунок реорганізації мережевої архітектури, виділення нового рівня управління послугами, злиття телефонії та інформаційних технологій, та використання відкритих протоколів.

NGN – це мережа на базі пакетів, що здатна надавати служби/послуги телекомунікацій та можливість використання декількох широкосмугових транспортних технологій, які забезпечують якість обслуговування і в яких функції, що належать до служб, не залежать від технологій, які стосуються транспортування.

Основні вимоги до мережі майбутнього:

– створювана мережа повинна мати можливість плавного переходу до нових технологій з комутацією пакетів і переростання в перспективну мережу NGN;

– масштабованість мережі при її розвитку та реконструкції;

– мінімальний вплив ринку послуг на етапність розвитку мережі;

– забезпечення міжмережної взаємодії на різних рівнях мережі з приєднаними мережами інших операторів;

– забезпечення транспортування трафіку, мультимедійних послуг в межах можливостей гарантованої якості.

Відповідно до Концепції розвитку НАН України на 2014-2023 роки з метою подальшої інтеграції установ Академії у великі міжнародні програми створено регіональний офіс підтримки та співробітництва у сфері використання космічної інформації для попередження і екстреного реагування на надзвичайні ситуації (програма UN-SPIDER), здійснено вступ НАН України від імені Національного ГРІДу до NorduGrid колаборації, яка передбачає об'єднання можливостей національних ГРІД-мереж півночі Європи. (URL : http://www.nas.gov.ua/legaltexts/DocPublic/P-131225-187-1.pdf)

1.4 Реформування системи Державної служби України з надзвичайних ситуацій

Метою Стратегії реформування системи Державної служби України з надзвичайних ситуацій, яка була ухвалена розпорядженням КМ України від

25.01.2017 р. № 61р, є реформування системи ДСНС та підвищення її спроможності щодо забезпечення виконання у взаємодії з іншими складовими сектору безпеки і оборони завдань з протидії загрозам національній безпеці у сфері цивільного захисту.

На третьому етапі впровадження Стратегії (2019-2020 роки) передбачається створення та забезпечення функціонування автоматизованої системи управління телекомунікаційними мережами, центру обробки даних, комплексної підсистеми інформаційної підтримки прийняття рішень з питань надзвичайних ситуацій, у тому числі комплексної системи захисту інформації. Виконання Стратегії реформування системи Державної служби України з надзвичайних ситуацій визначено Наказом ДСНС України від 02.03.2017 № 132 «Про затвердження Плану заходів щодо реалізації Стратегії реформування системи Державної служби України з надзвичайних ситуацій».

Основним завданням такої служби є поєднання функціональних можливостей інформаційних і телекомунікаційних систем задля побудови єдиної системи управління службами екстреної допомоги населенню незалежно від відомчого підпорядкування, організацію взаємодії та координацію в он-лайн режимі всіх державних, муніципальних (комунальних), обласних служб, діяльність яких пов’язана з реагуванням на надзвичайні (небезпечні) події, виклики громадян, аварії, стихійні лиха, або ліквідацією їх наслідків, забезпечити інформування (оповіщення) керівного складу та населення, збір, обробку та аналіз всієї інформації, що надходить, в одному місці – єдиній оперативно-черговій службі ОТГ (центральній диспетчерській службі ОТГ).

Актуальною є необхідність забезпечення оперативно-чергової служби апаратурою та високошвидкісним доступом до мережі Інтернет (~100Mb/s), бажано за допомогою сучасних оптичних ліній зв’язку. Таке підключення необхідне по-перше, для забезпечення роботи «хмарної» АТС, а по-друге для здійснення обміну службовою інформацією за допомогою електронної поштової мережі, використання Web-ресурсів, швидкої передачі великих файлі і документів, роботи з мультимедіа, повноцінного використання інтерактивних засобів, інформування в установленому порядку посадових осіб про виїзд аварійно-рятувальних підрозділів та обстановку на місці проведення виникнення НП (НС), порядок та стан проведення робіт з ліквідації надзвичайних подій.

На даний час єдиним загальноєвропейським стандартом цифрового радіозв’язку є стандарт DMR (Digital Mobile Radio). Він позиціонується як відкритий стандарт, тобто передбачається, що обладнання різних виробників буде сумісно між собою. Реалізація рішень стандарту DMR в діапазонах частот 403-0470 МГц повністю забезпечує управління силами й засобами місцевих ланок ЄДС ЦЗ об’єднаних територіальних громад та дозволяє здійснювати обмін інформацією між оперативно-рятувальними підрозділами ДСНС та іншими службами, що взаємодіють. Цифрові мережі технологічного радіозв’язку в стандарті DMR повинні працювати в режимі двочастотного

симплексу або дуплексу. При цьому рознос частот прийому і передачі повинен бути більше 1 МГц.

Схема організації радіозв'язку служб ОТГ з використанням технологій (рішень) стандарту DMR (рисунок 2) повністю інтегрується в єдину систему управління всіма службами та відповідальними посадовими особами, що задіяні у забезпеченні виконання всіх заходів життєзабезпечення громади, будується на базі оперативно-чергової служби МПО, але має надзвичайно високу надійність, достовірність, мобільність та розгалуженість схем організації зв'язку при виникненні будь яких непередбачуваних аварій на загальнодержавних та регіональних (місцевих) мережах зв'язку.

На відміну від засобів аналогового радіозв'язку, стандарт DMR дозволяє здійснити швидке встановлення виклику, він постійно вдосконалюється, реалізуючи функціональний набір раніше не характерний для засобів аналогового радіозв'язку.

Засоби зв'язку на базі стандарту DMR здатні забезпечувати:

– захист радіопереговорів від прослуховування;

– організацію передачі текстових повідомлень разом із голосом;

– збільшення розбірливості мови при сильних навколишніх перешкодах;

– збільшення терміну неперервної роботи акумуляторних батарей та багатьма іншими технічними вимогами.

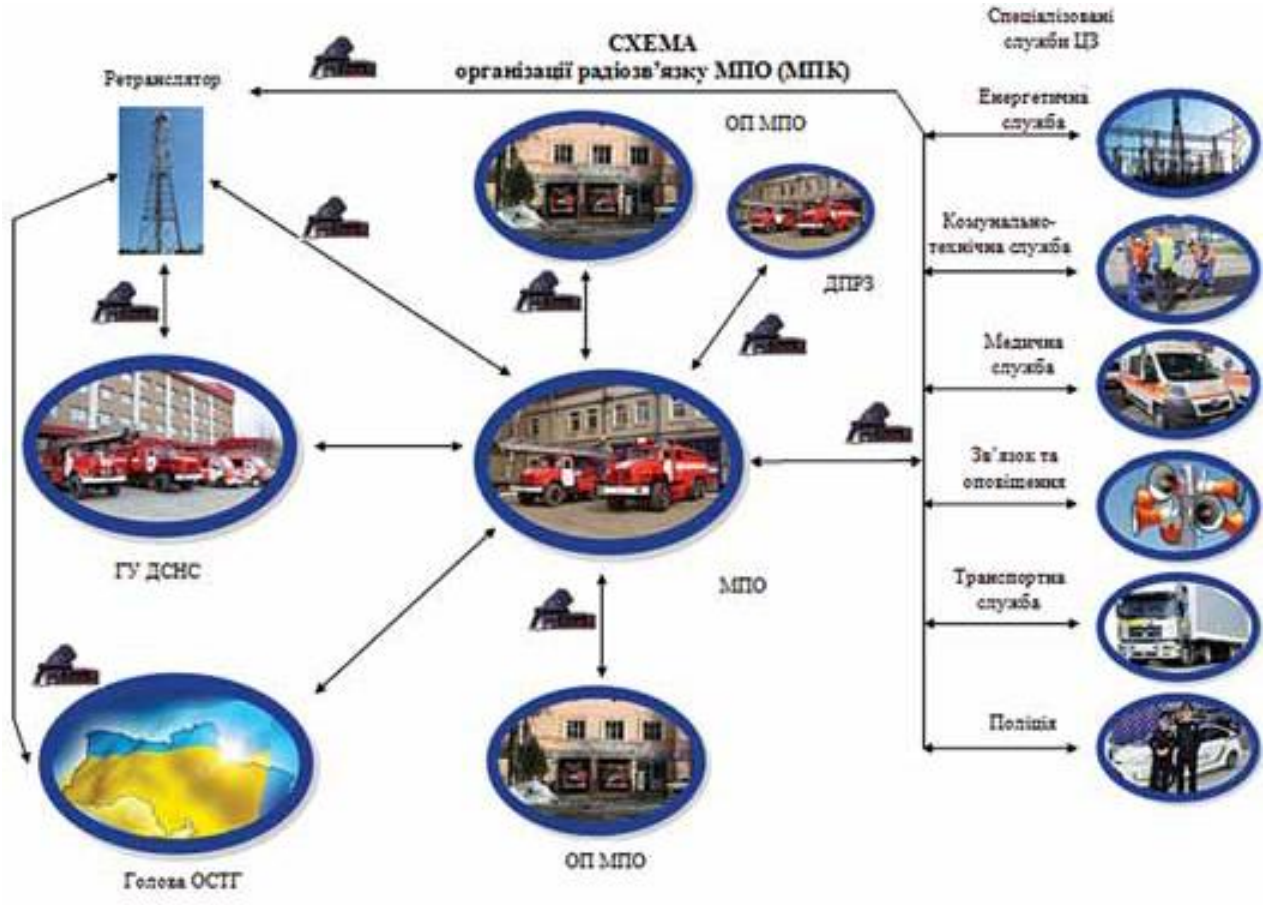


Рисунок 2 – Схема організації зв'язку МПО (МПК)

На відміну від засобів аналогового радіозв’язку, стандарт DMR дозволяє здійснити швидке встановлення виклику, він постійно вдосконалюється, реалізуючи функціональний набір раніше не характерний для засобів аналогового радіозв’язку.

Засоби зв’язку на базі стандарту DMR здатні забезпечувати:

– захист радіопереговорів від прослуховування;

– організацію передачі текстових повідомлень разом із голосом;

– збільшення розбірливості мови при сильних навколишніх перешкодах;

– збільшення терміну неперервної роботи акумуляторних батарей та багатьма іншими технічними вимогами.

До основних функціональних можливостей цифрового стандарту DMR необхідно віднести:

– цифрову обробку сигналу, опціональне шифрування;

– керування акумуляторною батареєю;

– пріоритетний аварійний виклик;

– покращений режим «вільні руки»;

– вбудований приймач GPS сигналів для реалізації додатків по контролю місцезнаходження;

– віддалений контроль;

– одночасну передачу мови та даних (в тому числі пакетних);

– роботу в аналоговому режимі, що актуально при здійсненні зв’язку з аналогови0 ми системами.

Польові випробування радіостанцій на базі стандарту DMR показали суттєву перевагу по відношенню до аналогових засобів зв’язку при використанні радіостанцій в міських умовах. Крім того, якість зв’язку та час автономної роботи портативних радіостанцій збільшилось до 2 разів, що обумовлюється принципами роботи обладнання стандарту DMR.

На виконання розпорядження КМ України від 22 .08.2018 р. № 564-р «Про виділення коштів для здійснення заходів, пов’язаних із зміцненням обороноздатності держави», було проведено процедуру закупівлі та побудовано для пересувний пункт управління (ППУ).

ППУ призначений для забезпечення автономної роботи керівника робіт з ліквідації наслідків надзвичайної ситуації, спеціальної урядової комісії з ліквідації наслідків надзвичайної ситуації, Державної комісії техногенно-екологічної безпеки та надзвичайних ситуацій або штабу з ліквідації наслідків надзвичайної ситуації, поблизу зони надзвичайної ситуації.

ППУ оснащений сучасними засобами радіозв’язку:

– базовою станцією цифрового транкінгового радіозв’язку та портативними радіостанціями стандарту;

– ретрансляторами;

– базовими та портативними станціями;

– радіостанціями для роботи з морськими та повітряними суднами; станцією супутникового зв’язку.

ППУ забезпечує стійкий радіо-, відео- та супутниковий зв'язок з пунктами управління, у тому числі повітряними та морськими, Державним та регіональними центрами управління у надзвичайних ситуаціях та ситуаційними центрами державних органів влади та силами, залученими до ліквідації наслідків НС.

Основні можливості:

– супутниковий, радіо та радіорелейний зв'язок;

– забезпечення проведення відеоконференції;

– проведення повітряної розвідки з використанням безпілотного літального апарата;

– відеотрансляція з місця події в режимі он-лайн;

– забезпечення діяльності органів управління.

У 2018 році проведено підключення 25 територіальних підрозділів ДСНС, Центру оперативного зв'язку, телекомунікаційних систем та інформаційних технологій ДСНС, Центру зв'язку та управління ДСНС та Львівського державного університету безпеки життєдіяльності до телекомунікаційної мережі доступу спеціального призначення.

У рамках виконання щорічних цільових планів Україна-НАТО у сфері планування надзвичайних ситуацій передбачено виконання низки заходів, пов'язаних із:

– реалізацією завдань щодо удосконалення і розвитку системи реагування на надзвичайні ситуації природного та техногенного характеру, участі у заходах Програми «Партнерство заради миру» відповідно до Індивідуальної програми партнерства України з НАТО;

– планування разом з комітетами та управліннями НАТО заходів щодо вдосконалення взаємосумісності під час надзвичайних ситуацій природного і техногенного характеру;

– удосконалення інформаційно-телекомунікаційної системи ДСНС тощо.

Висновки.

Розвиток ДСНС України та цивільного захисту здійсненний за умови постійного технологічного переоснащення та різноманітних інноваційних процесів. Базові напрямки інноваційної стратегії ДСНС України – напрямки, які орієнтовані на формування умов для розвитку виробництва конкурентоспроможної інноваційної продукції для забезпечення функціонування системи ДСНС Україні на базі передових досягнень науки, технологій і техніки та підвищення частки такої продукції в структурі виробництва і системі їх реалізації на вітчизняному та світовому ринках.

Створення і вдосконалення технологічного, математичного, програмного та інформаційного забезпечення автоматизованих систем управління, зв'язку та оповіщення в надзвичайних ситуаціях.

ЛЕКЦІЯ 2. ЗАГАЛЬНІ ПРИНЦИПИ ПОБУДОВИ МЕРЕЖ ЗАГАЛЬНІ ВІДОМОСТІ

План

Вступ
1. Мережі операторів.
2. Інтернет-сервіс-провайдинг.
3. Мережі підприємств і установ.
4. Телекомунікаційна мережа.
5. Параметри ефективності телекомунікаційної мережі.
6. Інформаційна мережа.
7. Конвергенція мереж, технологій та послуг**.**
8. Інфокомунікаційна мережа**.**
9. Глобальна інформаційна інфраструктура.

Висновки

Література

1. Теоретичні основи телекомунікаційних мереж : навч. посіб. /М.М. Климаш, Б.М.Стрихалюк, М.В.Кайдан. – Львів : вид-во УАД, 2011. – 496 с.

2. Стеклов В. К. Телекомунікаційні мережі / В. К. Стеклов, Л. Н. Беркман. – К. : Техніка, 2001. – 392 с.

3. Буров Є. Комп'ютерні мережі / Є.Буров. – Львів : БаК, 1999. – 468 с.

Вступ

В умовах ринкової економіки суб'єктами підприємницької діяльності у галузі телекомунікацій виступають *мережеві оператори та сервіс-провайдери* (постачальники послуг). Вони забезпечують побудову мереж зв'язку *загального користування – публічних мереж.*

Сучасні мережі зв'язку є складними штучними системами. Вивчення та дослідження мереж доцільно здійснювати в двох аспектах:

- *телекомунікаційні мережі;*
- *інформаційні мережі.*

2.1 Мережі операторів

Телекомунікаційна мережа загального користування означає системи передавання і, у відповідних випадках, комунікаційне обладнання та інші ресурси, що дозволяють передавати сигнали між визначеними кінцевими пунктами за допомогою телеграфу, радіо, оптичних чи інших електромагнітних засобів, які використовуються повністю чи частково, для надання загальнодоступних телекомунікаційних послуг. Телекомунікаційна послуга означає послуги, надання яких повністю чи частково полягає в переданні та

маршрутизації сигналів у телекомунікаційних мережах, за винятком радіо- та телевізійного мовлення (Директива Європейського парламенту і Ради від 15 грудня 1997 р. № 97/66/ЄС стосовно оброблення персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі).

Окремим класом виділяють *мережі підприємств*, що належать компаніям та установам, бізнес-інтереси яких, виходять за межі ринку телекомунікацій.

Оператор мережі – це оператор інфраструктури телекомунікацій загального користування, що дозволяє передачу сигналів між визначеними пунктами призначення всередині мережі за допомогою телефонного зв'язку, мікрохвиль, оптичних засобів чи інших електромагнітних засобів [с.15].

Постачальник послуг мережі – це фізична чи юридична особа, яка займається наданням послуг у сфері телекомунікацій загального користування, забезпечення яких цілком або частково полягає в передачі сигналів всередині мережі зв'язку [с.16].

Зв'язок – будь-яке з'єднання (стаціонарне чи тимчасове), яким може передаватися інформація між двома чи більше користувачами системи передачі даних [с.15].

Інформація про передачу даних між пунктом призначення та мережею чи іншим користувачем включає в себе інформацію про передачу, що використовується для встановлення зв'язку та контролю за його розвитком (наприклад, утримання запиту, передача запиту). Інформація про зв'язок також включає в себе інформацію доступну для оператора мережі/постачальника послуг мережі (наприклад, тривалість зв'язку) [с. 17].[1]

Послуги з транспортування інформації, які надаються оператором мережі як кінцевим користувачам мережі, так і іншим операторам мережі, забезпечуючи їх транзитною можливістю з передачі трафіку через свої мережі, називаються *комунікаційними послугами* послугами.

Основним завданням *комунікаційних послуг* є забезпечення можливості віддалено розташованих об'єктів обмінюватися інформаційними повідомленнями. Створюючи мережу загального користування, оператор зобов'язаний забезпечити в будь-якому місці мережі, до якого під'єднанні кінцеві пристрої, *стандартний інтерфейс* (точку з'єднання). Розрізняють операторів *фіксованого* та *мобільного* (стільникового) зв'язку.

Оператори фіксованого зв'язку організовують стаціонарні мережі, в яких комунікаційне обладнання та пристрої користувачів розміщуються в стаціонарних пунктах мережі.

Оператори мобільного зв'язку створюють мережеве покриття території, розміщуючи свої базові станції за стільниковою схемою в стаціонарних або рухомих пунктах, забезпечуючи тим самим можливість вільного переміщення абонентів у зоні покриття.

Серед основних тенденцій розвитку ринку стільникового зв'язку є поява *віртуальних операторів*. Це компанії, не маючи власних мережевих ресурсів,

[1] Офіційний переклад нормативних актів Євросоюзу в сфері інформаційно-комунікаційних технологій. Громадська організація ІНТЕРНЬЮЗ-УКРАЇНА. – Київ, 2000. – 219 с.

займаються маркетинговою діяльністю, реалізуючи клієнтам під своєю торговою маркою у вигляді пакетів популярних послуг на основі гнучкої тарифної сітки. Для операторів фіксованих мереж комплексних рішень щодо розширення послуг є надання мобільного доступу своїм абонентам. Операторові мобільного зв'язку фіксована мережа дозволяє стати постачальником повного набору послуг.

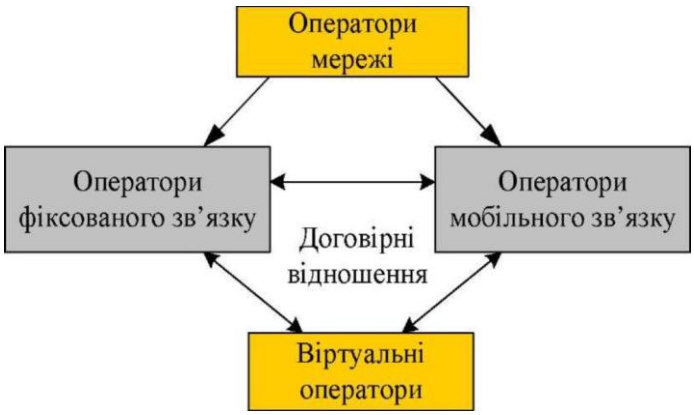


Рисунок 3 – Класифікаційна схема взаємодії між операторами

2.2 Інтернет-сервіс-провайдинг

Розвиток Інтернету сприяв зростанню такому виду мережевих послуг як *інтернет-сервіс-провайдинг*. Унікальність Інтернету (глобальної *інформаційної мережі*) полягає в наповненні інформаційними ресурсами та широкому застосуванні інформаційних технологій, таких як *накопичення, зберігання, обробка інформації* та подання її у формі *Web-сторінок*.

Інформаційні послуги Інтернету полягають у тому, щоб забезпечити користувачів можливістю пошуку в мережі найрізноманітнішої інформації (контенту). В Інтернеті, технологічною особливістю якого є пакетний спосіб передачі інформації, можливою є організація різних служб, найпоширенішою серед яких електронна пошта.

Діяльність сервіс-провайдерів зосереджена на організації сервісних вузлів, за допомогою яких реалізується доступ користувачів до різних мережевих служб та інформаційних ресурсів як даного вузла, так і віддалених вузлів Інтернету. Постачальники послуг (провайдери) також є споживачами телекомунікаційних послуг (послуг з транспортування інформації), які надаються мережевими операторами.

Функціонуюча мережа «провайдерського класу» створюється:

– сервісним вузлом *провайдера місцевого рівня* (рівень III) зовнішнім каналом, орендованим у мережевого оператора, під'єднуються точки мережевої присутності (Point of Presents, POP), у якій розміщується обладнання мережевого доступу регіонального провайдера;

– *регіональним провайдером* (рівень II), який розміщує в своєму регіоні кілька точок мережевої присутності, забезпечуючи користувачів місцевих провайдерів доступом як до своїх інформаційних ресурсів (свого сервісного вузла), так і до зовнішніх ресурсів Інтернету;

– регіональний провайдер, орендуючи канал у мережевого оператора, під'єднується до мережі доступу національного провайдера (рівень I). І тільки національний провайдер має право під'єднання до *точки мережевого доступу* (Network Access Point, NAP). NAP – це міжнаціональні точки доступу в Інтернет.

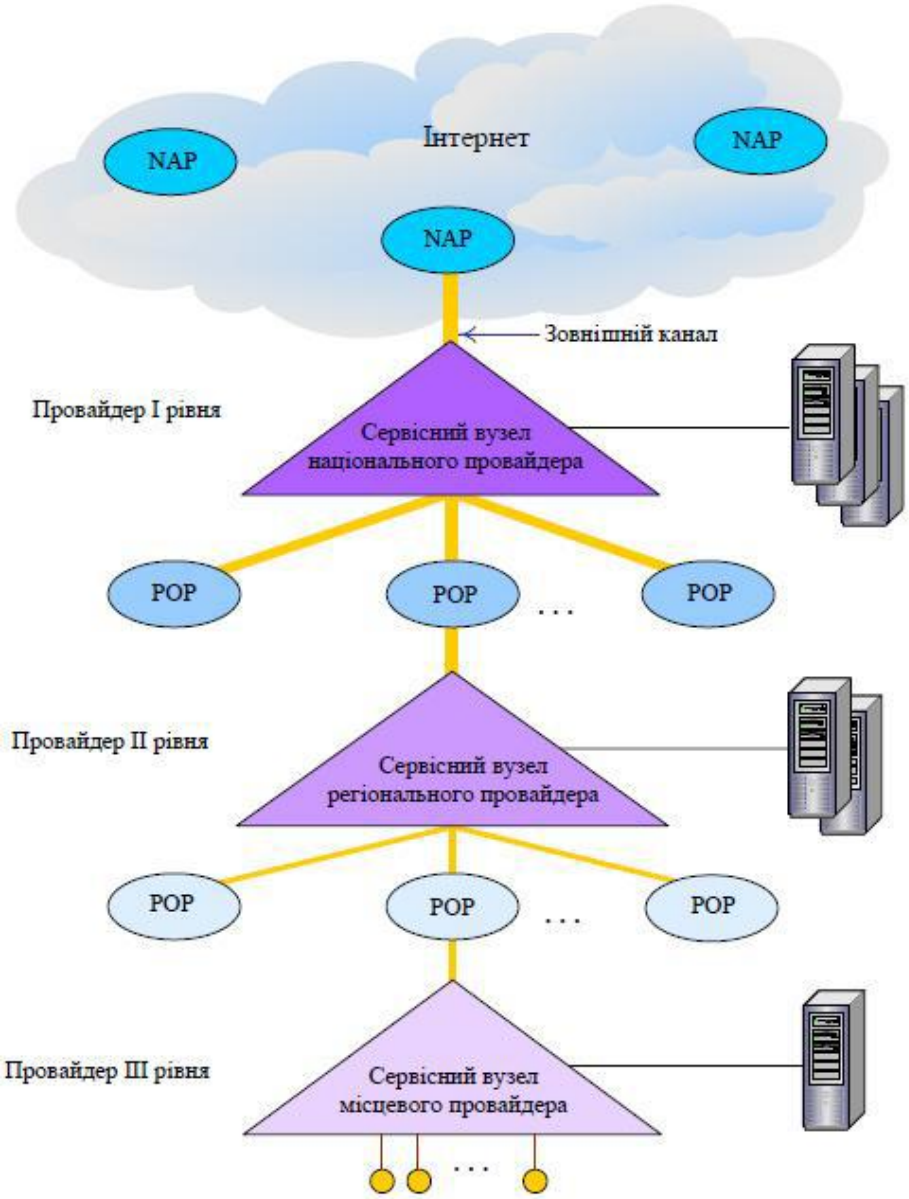


Рисунок 4 – Інтернет-сервіс-провайдер

2.3 Мережі підприємств та установ

Мережами підприємств, або *приватними мережами*, називають мережі, які належать установам і компаніям.

Відмінною особливістю приватних мереж є те, що всі ресурси мережі використовуються виключно співробітниками підприємства, яке є власником мережі. Під терміном «приватна» мережа розуміють також *закриту мережу*, призначену для конфіденційного зв'язку.

Поєднання комп'ютерів у мережу дозволяє підприємству оптимізувати його інформаційну інфраструктуру (роботу програм, устаткування, баз даних, тощо), що в результаті підвищує ефективність процесу в цілому.

Залежно від масштабу виробничого підрозділу, в межах якого діє мережа, розрізняють мережі *робочих груп, мережі відділів, мережі кампусів* (невелике містечко) і *корпоративні мережі*.

Мережі робочих груп зазвичай характеризуються малою кількістю робочих місць (до 10) та використовуються невеликими групами співробітників підприємства, які виконують спільне виробниче завдання. Метою створення мережі в даному випадку є поділ дорогого периферійного обладнання та даних, спільне використання застосувань, а також надання універсальних засобів комунікацій як для внутрішнього, так і зовнішнього зв'язку (рис. 5).

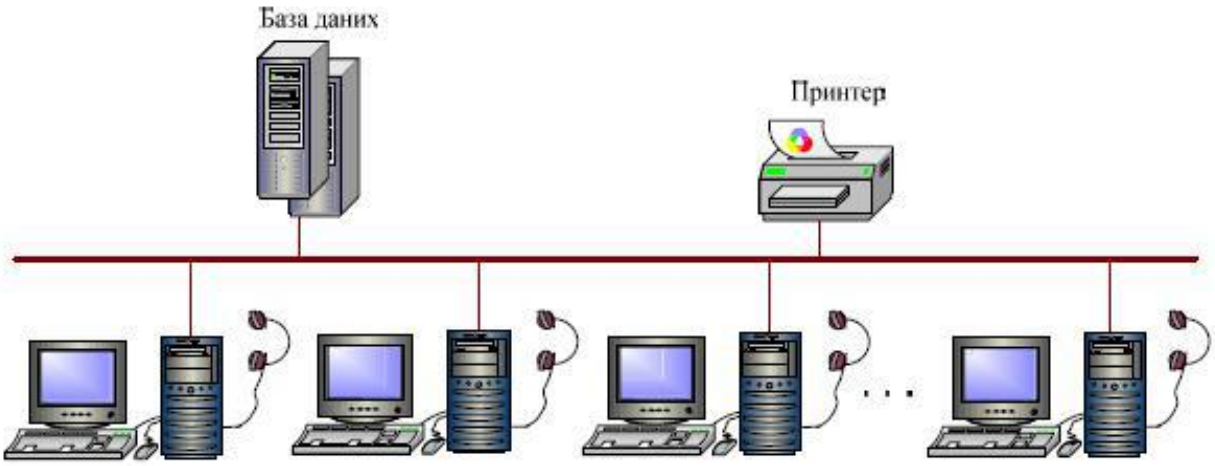


Рисунок 5 – Мережа та робочі групи

Мережі відділів можуть об'єднуватися для забезпечення спільної роботи співробітників одного відділу (рис. 7), співробітники яких вирішують ряд взаємопов'язаних завдань. Завдяки мережі забезпечується робота в режимі розподілу лазерних принтерів, модемів, інформаційних ресурсів відділу та мережевих застосувань.

Комп'ютерно-телефонна інтеграція зумовила появу нових ознак, властивих сучасним мережам відділів: робочі місця співробітників поповнилися спеціалізованими телефонними апаратами, під'єднаними до послідовних портів персональних комп'ютерів (ПК). Крім того з'явилася можливість емуляції телефонного апарата за допомогою плат розширення в стандарті *програмного інтерфейсу телефонного застосування*.

Факс як необхідний елемент офісу або відділу завдяки новим стандартам інтегрувався в телефонно-комп'ютерну систему.

Мережі нового типу засновують як на базі УАТС (з використанням станцій Hicom, Siemens), так і на базі технологій IP-мереж, що забезпечує можливість створення гібридних застосувань, наприклад, уніфікований обмін повідомленнями.

Рисунок 6 – Мережа відділу

Мережа будівлі або кампусу об’єднує мережі різних відділів великого підприємства. Мережі відділів можуть розташовуватися як у межах одного багатоповерхового будинку, так і в декількох будинках, розміщених неподалік один від одного, які утворюють *кампус* (невелике містечко) (рис. 8).

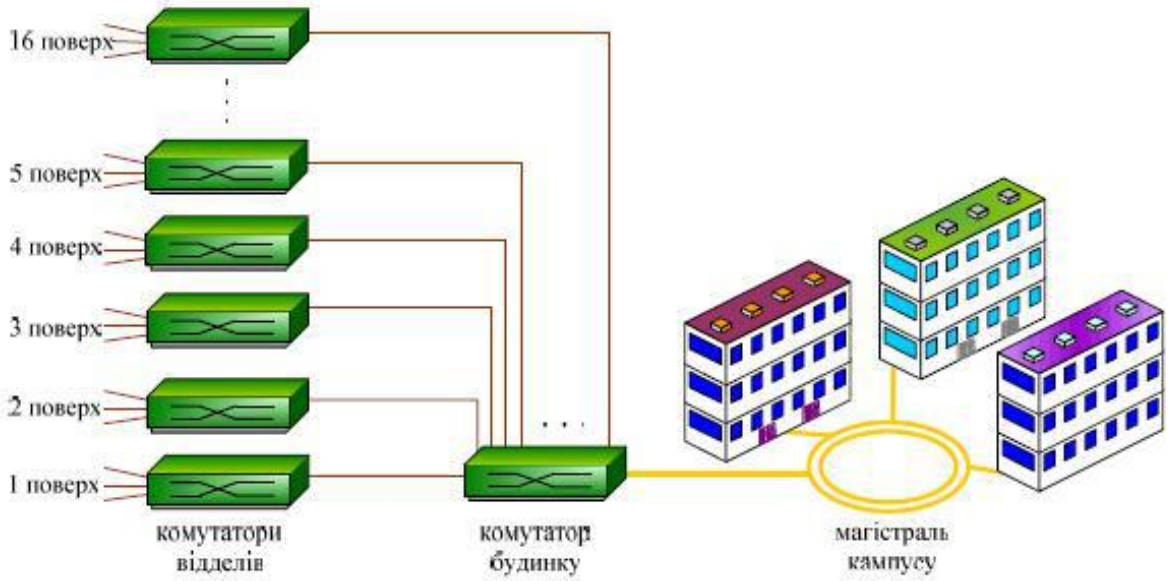


Рисунок 7 – Мережа кампусу

Мережі кампусів налічують декілька сотень комп'ютерів, які використовують спеціальні служби мережевої взаємодії, що забезпечує доступ до загальних баз даних підприємства, високошвидкісних модемів та ін.

Кампусна мережа може складатися з різних типів комп'ютерів, неоднорідного апаратного й програмного забезпечення, різних мережевих технологій, що є прикладом *гетерогенного* мережевого середовища. Це створює проблему, пов'язану зі складністю керування кампусними мережами і вимагає високої кваліфікації мережевих адміністраторів.

Підрозділи ДСНС можуть мати різний масштаб: від малого з одним або кількома працівниками до масштабу кампусу, а тому об'єднання мереж підрозділів є можливим лише з використанням зовнішніх телекомунікацій. Санкціонований доступ до мережі має лише обмежений контингент користувачів, група конкретних осіб.

Мережі ДСНС включають усю комунікаційну інфраструктуру, що забезпечує взаємодію між користувачами: різні типи термінальних пристроїв; кабельні системи в місцях розташування офісів; глобальні комунікації на базі ресурсів мережевих операторів; функціональні елементи керування мережею.

Корпоративні мережі належать великим компаніям, які складаються з головної штаб-квартири (центрального офісу), а також віддалених філій в інших містах, країнах і навіть на різних континентах.

Підрозділи корпорації можуть мати різний масштаб: від малого з одним або кількома працівниками компанії до філії масштабу кампусу, а тому об'єднання мереж корпоративних підрозділів є можливим лише з використанням зовнішніх телекомунікацій які, не належать даному підприємству (рис. 6).

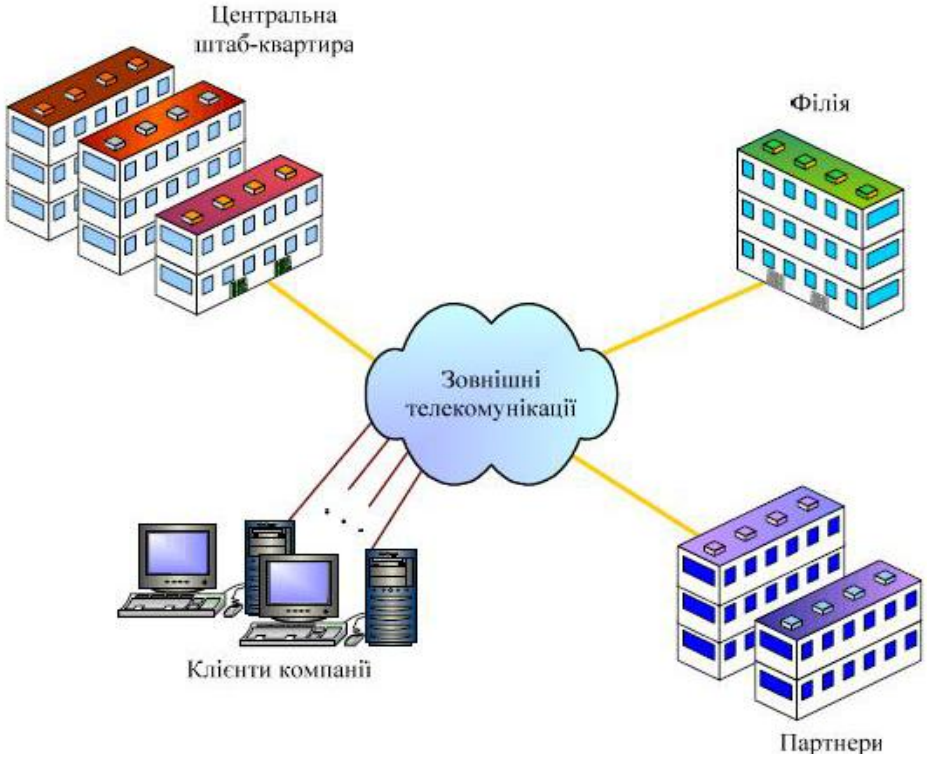


Рисунок 8 – Корпоративна мережа

Корпоративна мережа може обслуговувати не лише підрозділи, але й певну групу користувачів (основні клієнти). Санкціонований доступ до корпоративної мережі має лише обмежений контингент користувачів, група конкретних осіб.

Корпоративні мережі включають усю комунікаційну інфраструктуру, що

- забезпечує взаємодію між користувачами:
- різні типи термінальних пристроїв;
- кабельні системи в місцях розташування офісів;
- глобальні комунікації на базі ресурсів мережевих операторів;
- функціональні елементи керування мережею.

2.4 Телекомунікаційна мережа

Загальне поняття «телекомунікації» базується на уявленні про засоби, які дозволяють організувати зв'язок між двома і більше віддаленими пунктами. «Теле-» в перекладі з давньогрецької означає «далеко».

Телекомунікації – будь-яка передача знаків, сигналів, записів, образів, звуків, інформації чи свідчень будь-якого характеру, що передаються повністю або частково за допомогою телефонного зв'язку, радіо, електромагнітної, фотоелектронної чи фотооптичної системи [с. 17].[2]

Секція телекомунікацій *Міжнародного союзу електрозв'язку* у Рекомендаціях серії I (I.110, I.112) визначає термін «*телекомунікації*» як сукупність засобів, які забезпечують перенесення інформації, поданій у необхідній формі, на значну відстань за допомогою поширення сигналів в одному з середовищ (міді, оптичному волокні, ефірі) або сукупності середовищ.

Засоби телекомунікацій є лінії зв'язку, пристрої з'єднання середовищ, системи передачі, комунікаційні пристрої мережі, обладнання сигналізації, синхронізації та ін.

Ґрунтуючись на цих поняттях, дамо визначення телекомунікаційній мережі.

Телекомунікаційна мережа (ТК) – це системоутворююча сукупність засобів телекомунікацій, що надає територіальновіддаленим об'єктам можливість інформаційної взаємодії шляхом обміну сигналами (електричними, оптичними або радіо).

Об'єктами при цьому можуть виступати:

- термінальні пристрої користувачів;
- кінцеві системи мережі;
- окремі мережі).

Кінцем (інтерфейсною точкою) телекомунікаційної мережі є або телекомунікаційний роз'єм, до якого під'єднано пристрій користувача

[2] Офіційний переклад нормативних актів Євросоюзу в сфері інформаційно-комунікаційних технологій. Громадська організація ІНТЕРНЬЮЗ-УКРАЇНА. – Київ, 2000. – 219 с.

(мережевий інтерфейс), або кінцеве мережеве обладнання, яке забезпечує з'єднання мереж (міжмережевий інтерфейс) (рис. 9)

Транспортування інформації означає перенесення інформації, перетвореної в сигнал з кінця в кінець, тобто від джерела до одержувача. Його слід відрізняти від терміна «передача», під яким розуміється процес поширення сигналу у фізичному середовищі між двома суміжними пунктами мережі.

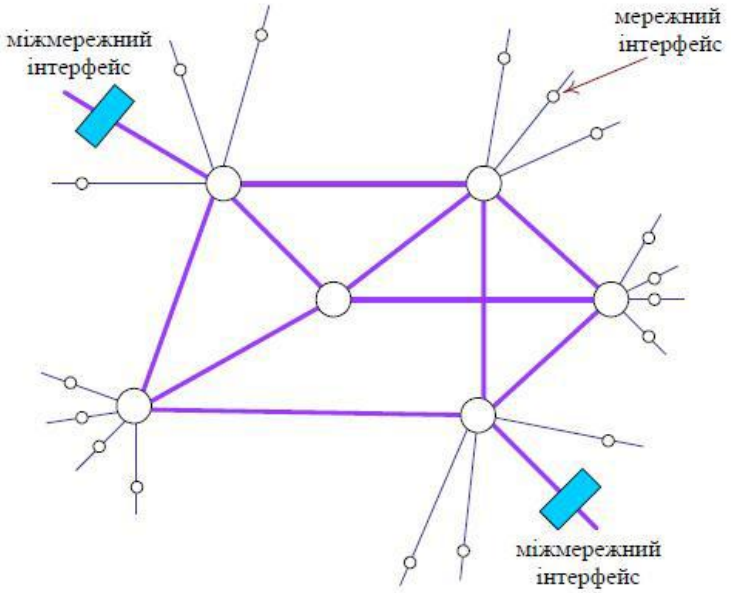


Рисунок 9 – Телекомунікаційна мережа

Транспортуючи інформацію, необхідно контролювати такі важливі мережеві функції, як якість обслуговування з кінця в кінець, керування потоками з метою запобігання перевантажень у мережі та ін.

Телекомунікаційні мережі можна класифікувати за: типом режиму перенесення інформації (синхронні, асинхронні); технологічними характеристиками (середовищем передавання, заданою шириною смуги пропускання, якістю передавання сигналів, швидкістю передавання та ін.).

2.5 Параметри ефективності телекомунікаційної мережі

Телекомунікаційні мережі характеризують за показниками, які відображають у цілому можливість і ефективність транспортування інформації. Можливість транспортування інформації в телекомунікаційній мережі пов'язана зі ступенем її функціональності в часі, тобто виконанням заданих функцій в повному обсязі з необхідним рівнем якості протягом певного періоду експлуатації мережі або в конкретний момент часу.

Працездатність мережі пов'язана з поняттями надійності та живучості.[3]

[3] Різниця між цими поняттями зумовлена відмінностями причин та факторів, які порушують нормальну роботу мережі, та специфікою порушень.

Надійність мережі зв'язку характеризується здатністю забезпечувати зв'язок, зберігаючи в часі значення встановлених показників якості в заданих умовах експлуатації. Вона відображає вплив на працездатність мережі передусім внутрішніх чинників:

– випадкових відмов технічних засобів, спричинених процесами старіння;

– дефектами технології виготовлення;

– помилками обслуговуючого персоналу.

Наприклад, показниками надійності є відношення часу працездатності мережі до загального часу її експлуатації, ймовірність безвідмовного зв'язку та ін.

Важливим показником є також кількість незалежних шляхів передавання інформаційного повідомлення, які можуть бути визначені між парою пунктів мережі.

Живучість мережі зв'язку характеризується здатністю зберігати повну або часткову функціональність під впливом руйнуючих причин, які виникають поза межами мережі й призводять до виходу з ладу чи значних пошкоджень деякої частини її елементів (пунктів і ліній зв'язку). Виокремлюють два типи таких причин: *стихійні й навмисні*.[4]

Живучість мережі характеризують показники, які визначають:

– вірогідність того, що між будь-якою заданою парою пунктів мережі можна передати обмежений обсяг інформації після впливу руйнівних факторів;

– мінімальну кількість пунктів, ліній мережі (або тих та інших), вихід з ладу яких призводить до порушення зв'язності мережі відносно довільної пари пунктів;

– середню кількість пунктів, які залишаються зв'язними при одночасному пошкодженні декількох ліній зв'язку та ін.

Пропускна здатність мережі. У тих випадках, коли мережа не може обслуговувати (реалізувати) необхідне навантаження, говорять про обсяг реалізованого навантаження в мережі.

Величина реалізованого навантаження в мережі визначає її пропускну здатність і в ряді випадків може бути оцінена кількісно. Оцінка пропускної здатності мережі значною мірою пов'язана з параметрами якості обслуговування, тому що реалізація конкретного навантаження має здійснюватися відповідно до заданих параметрів якості.[5]

Якість обслуговування визначається сукупністю показників, які вказують на рівень відповідності телекомунікаційної мережі нормам експлуатації та вимогам користувачів.

[4] До стихійних чинників відносяться: землетрус, повинні та інші форсмажорні обставини, до навмисних – пошкодження мережі в наслідок злочинних дій.

[5] Наприклад, можна визначити величину максимального потоку інформації між двома пунктами (джерело-стік), або пропускну спроможність перетину мережі, що є найвужчим місцем при поділі мережі між джерелом і стоком на дві частини.

2.5 Інформаційна мережа

Поняття «*інформаційна мережа*» передбачає розгляд телекомунікаційної мережі в сукупності зі взаємодіючими за допомогою неї об'єктами. У такому розумінні інформаційна мережа – це «навантажена» телекомунікаційна мережа.

Поняття «інформаційна мережа» відображає інформаційні процеси, які протікають в мережі в результаті взаємодії кінцевих систем, під'єднаних до телекомунікаційної мережі.

Інформаційні процеси в мережі можна поділити на дві групи: прикладні процеси та процеси взаємодії.

Прикладні процеси ініціюються кінцевими системами під час запуску програм користувача, які ще називаються застосуваннями.

Процеси взаємодії – це процеси в мережі, призначені для обслуговування прикладних процесів.[6] Прикладні процеси та процеси взаємодії підтримуються *мережевими операційними системами* (МОС).

Кінцеві системи інформаційної мережі класифікуються таким чином:

– *термінальні системи* – комп'ютери користувачів мережі;

– *хостингові системи* – комп'ютери, на яких розміщено інформаційні та програмні ресурси мережі;

– *сервери* – комп'ютери, на яких інстальоване спеціальне програмне забезпечення, яке дозволяє надавати мережеві сервіси.[7] Серверний комп'ютер, залежно від можливості його операційної системи, може бути налаштований як для роботи в режимі хосту (інформаційний сервер), так і в режимі комунікаційного пристрою (наприклад, шлюзу);

– *адміністративні системи* – комп'ютери, які забезпечують роботу застосувань керування мережею та окремих її частин.

Інформаційні ресурси формуються і використовуються на основі всіх соціальних процесів, усіх форм власності та різних способів організації суспільно корисної діяльності. Процеси перетворення та реалізації знань через матеріалізацію інформаційного ресурсу отримують розвиток за рахунок високих інформаційних технологій, а для отримання і збереження переваг в умовах конкуренції кожна дія в інформаційному середовищі буде мати значний вплив у світі фізичних ресурсів: предметних, фінансових – і в різних абстрактних галузях.

Усе це систематизується в мережевих банках даних, з якими взаємодіють користувачі мережі. Ці ресурси визначають споживчу цінність інформаційної мережі, тому їх необхідно:

– постійно створювати та поповнювати;

– вчасно архівувати та оновлювати;

---

[6] Наприклад, визначення форматів подання інформації для передачі мережею, встановлення режимів передавання даних, визначення маршрутів просування інформації та ін.

[7] Наприклад, керування доступом для великої кількості користувачів до інформаційних ресурсів, пристроями колективного користування (принтерів, плотерів), реєстрація користувачів та контроль за їх правами доступу в мережу та ін.

– користування мережею повинно забезпечувати можливість отримання актуальної інформації саме тоді, коли в ній виникає необхідність.

Ресурси обробки та зберігання даних – це продуктивність процесорів та обсяги пам'яті комп'ютерів, які працюють у мережі, а також час, протягом якого вони використовуються.

Програмні ресурси – мережеве програмне забезпечення (ПЗ):

– мережеві операційні системи, серверне ПЗ, ПЗ робочих станцій;

– прикладне ПЗ;

– інструментальні засоби: утиліти, аналізатори проходження трафіку, засоби мережевого контролю, програми додаткових функцій, основними серед яких є виписка рахунків, облік оплати послуг, навігація (забезпечення пошуку інформації в мережі), обслуговування мережевих електронних поштових скриньок, організація мостів для телеконференцій, перетворення форматів переданих інформаційних повідомлень, криптозахист інформації (кодування й шифрування), автентифікація (електронний підпис документів, що засвідчує їх справжність).

Комунікаційні ресурси – це ресурси, які беруть участь у транспортуванні та перерозподілі потоків інформації в мережі (ресурси телекомунікаційної мережі), основними з яких є пропускні спроможності ліній зв'язку та устаткування вузлових пунктів, а також їх використання під час взаємодії користувача з мережею. Вони класифікуються відповідно до використаного середовища передачі та телекомунікаційної технології. Ресурси інформаційної мережі можуть використовуватися одночасно кількома прикладними процесами, тобто *розділятися в часі*.

Ресурси інформаційної мережі дозволяють:

– виконувати обробку інформації;

– забезпечувати ефективний пошук її в будь-якому місці мережі;

– уможливлюють її накопичення й зберігання.

Отже, під *інформаційною мережею як фізичним об'єктом розуміють сукупність територіально розрізнених кінцевих систем, об'єднаних телекомунікаційною мережею, за допомогою якої забезпечуються взаємодія прикладних процесів, активізованих в кінцевих системах, та їх колективний доступ до ресурсів мережі*.

Уся інтелектуальна робота в інформаційній мережі виконується на перефирії, тобто в кінцевих системах мережі, а телекомунікаційна мережа, займаючи центральне положення є з'єднувальним компонентом (рис. 10) *Телекомунікаційна мережа* у складі інформаційної мережі виконує функції транспортувальної системи.

Поняття інформаційна мережа зосереджує увагу на *інформаційних процесах*, які виникають у мережі під час взаємодії кінцевих систем через телекомунікаційнійну мережу. Опис цієї взаємодії демонструє всю складність організації зв'язку в мережі як у режимі «запит-відповідь», так і в реальному масштабі часу. Основною вимогою, якій має відповідати інформаційна мережа, є забезпечення користувачів *ефективним доступом до ресурсів*, які можуть

розділятися (тобто колективного використовуватися). Усі інші вимоги – пропускна здатність, надійність, живучість – лише забезпечують якісне виконання цієї основної вимоги.

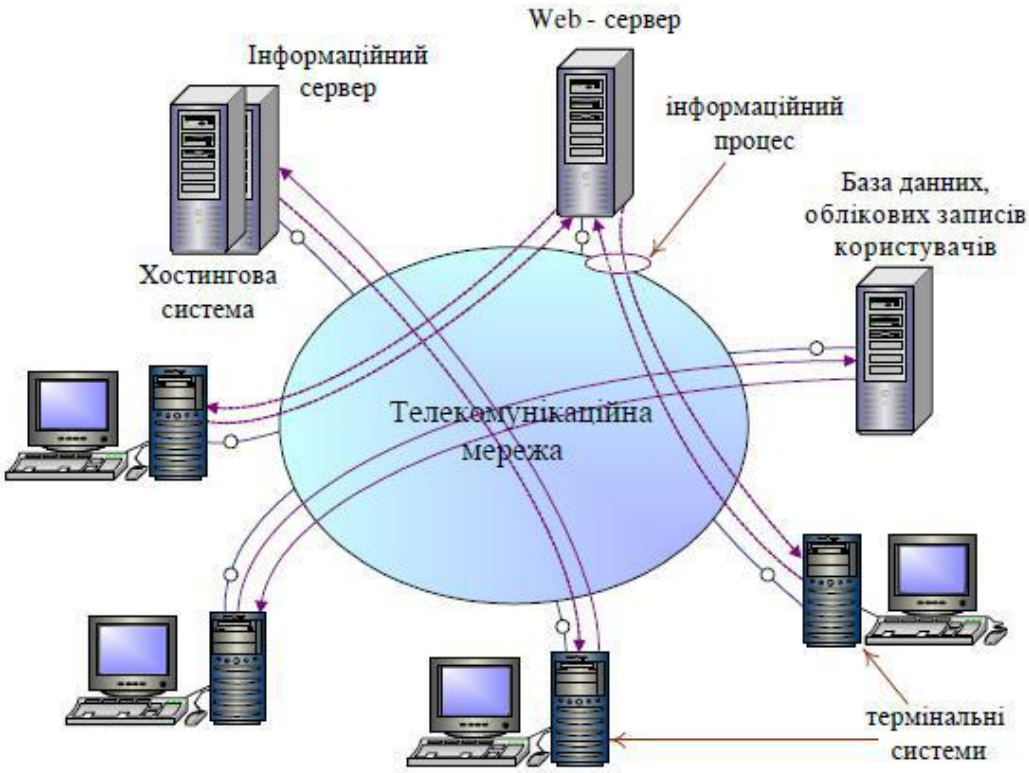


Рисунок 10 – Інформаційна мережа

Параметри оцінки ефективності інформаційної мережі визначаються рівнем продуктивності інформаційної мережі як системи розподільчих ресурсів складаються з:

– часу реакції мережі;
– затримки передачі;
– варіації затримки передачі;
– прозорості.

Час реакції мережі визначається як інтервал часу між поданням запиту користувача до певної мережевої служби (наприклад, передачі файлів) і отримання відповіді на цей запит. Значення цього показника залежать від:

– типу служби, до якої звертається користувач;
– до якої категорії належить користувач;
– продуктивності сервера, куди він звертається;
– ступеня завантаженості елементів мережі через які проходить запит.

Затримка передачі визначається як час між моментом надходження пакету даних на вхід будь-якого мережевого пристрою або фрагмента мережі і моментом виходу з неї тобто визначаються етапи тимчасової обробки пакетів

при проходженні їх мережею. При цьому продуктивність мережі оцінюється максимальною затримкою передачі та варіацією затримки.

Варіація затримки (джитер затримки) характеризує коливання затримки в часі. Великий діапазон в значеннях затримки негативно позначаються на якості наданої користувачеві інформації при передаванні чутливих до затримки видів трафіку таких як відеодані, мовленнєвий трафік.

Прозорість характеризується властивістю мережі приховувати від користувача принципи її внутрішньої організації. Для роботи з віддаленими ресурсами мережі користувач повинен використовувати ті ж самі команди й процедури, що й для роботи з ресурсами свого комп'ютера.

2.6. Конвергенція мереж, технологій та послуг

Мережі зв'язку класифікують відповідно до категорій послуг, які надаються, основними серед яких є такі:

- телекомунікаційні або транспортні послуги;
- інформаційні послуги.

Комп'ютери мережі як розподільчі системи обробки даних забезпечують можливість автоматизованої обробки, накопичення й зберігання в мережі будь-якої інформації, що є продуктом інтелектуальної діяльності суспільства, й видачі її на запит користувача в необхідній формі, розширюючи спектр інформаційних послуг.

Передача комп'ютерних даних засобами телефонних комунікацій або передача мовного трафіку з використанням пакетного режиму переносу інформації ускладнює та видозмінює звичну у минулому класифікацію мереж зв'язку за типом переданих інформаційних повідомлень. Сьогодні відбувається взаємопроникнення різних за походженням і принципами роботи мереж (мережі передачі комп'ютерних даних і мережі передачі мовного (телефонного) трафіку), що свідчить про конвергенцію[8] мереж.

Під *конвергенцією в телекомунікаціях розуміють забезпечення практично однакових наборів послуг різними за технологічними можливостями мереж, або об'єднання кінцевих пристроїв, таких, як телефон, персональний комп'ютер і TV-приймач у єдиний термінал.*

Конвергенція передбачає створення конвергентних систем зв'язку на основі злиття мереж, які відрізняються цілим рядом ознак:

- використання різних телекомунікаційних технології;
- локальні й територіальні мережі;
- проводові та безпроводові мережі;
- стаціонарні та мобільні мережі;
- мережі доступу та транспортні мережі.

[8] Від англ. convergence – зближення, сходження в одну точку. Конвергенція зумовлена прагненням мати однорідну інфраструктуру для тих чи інших послуг, навіть коли ці послуги підтримуються різними технічними рішеннями. Ці рішення можуть бути засновані на телекомунікаційних або інформаційних технологіях.

Конвергенція послуг завжди припускає певний рівень конвергенції в технічних системах, які забезпечують ці послуги.

Конвергенція послуг слугує: до значного збільшення можливостей однієї окремо взятої послуги (наприклад, у мультимедійні комунікації):

– *передачі мови пакетами*: коли окремі сегменти телефонної мережі заміщуються мережами передачі даних, які забезпечують також і транспортування мови; надання Інтернет-послуг через лінії доступу телефонної мережі (взаємодія між телефонною мережею та Інтернетом на межі телефонної мережі);

– *стирання меж між фіксованими та мобільними мережами* (інтеграція комутаторів для проводових і мобільних радіомереж (комбінований комутатор);

– *отримання абонентами послуг* у разі будь-якого доступу до мережі.

Закономірним результатом загальних процесів конвергенції є *комп'ютерно-мережева інтеграція*: саме розвиток обчислювальної техніки та її архітектури став підґрунтям розробки принципів та системних рішень, запроваджених в сучасних мережах.

Помітними також є фактори зворотного впливу. Необхідність передавання даних на значні відстані призвела до *використання існуючих телекомунікацій як транспортного середовища* при об'єднанні локальних обчислювальних мереж (ЛОМ) та взаємодії їх з віддаленими комп'ютерами. Комп'ютер, у свою чергу, використовують не тільки як термінальний пристрій, але й як транзитний вузол телекомунікаційної мережі, який поєднує різних користувачів мережі, використовуючи мережеві процедури маршрутизації.

Доцільним є використання в локальних мережах телекомунікаційної технології асинхронного режиму перенесення (АТМ), що забезпечує передачу різнотипного трафіку необхідної якості.

На сьогодні в комп'ютерно-телефоній інтеграції виокремлено два підходи: комп'ютерний і телефонний:

– *комп'ютерний*, в основі якого лежить концепція підтримки додаткових послуг підвищеної якості для бізнес-користувачів, яка орієнтована на конвергенцію комунікаційних та інформаційних послуг. Комп'ютерний підхід спрямовано на обслуговування великої кількості викликів шляхом організації спеціалізованого операторського центру, що забезпечує інтелектуальні й автоматизовані комунікаційні послуги, які підтримуються за допомогою складних програмних застосувань, інстальованих на спеціальному сервері комп'ютерної телефонії, який взаємодіє з базою даних клієнтів, що знаходиться на окремому сервері (програмний комутатор);

– *телефонний*, якщо забезпечує виконання функцій Call Center комутаційною системою телефонної станції без використання додаткового сервера. Основним завданням є вирішення внутрішніх завдань підприємства: підвищення культури виробництва, інтеграція різних власних баз даних з телефонною системою.

Таким чином, як перший, так і другий підходи мають право на існування.

Концепція IP-телефонії передбачає доставку голосового трафіку пакетами (Voice over Internet Protocol, VoIP) в режимі реального масштабу часу мережами передачі даних за допомогою транспортних механізмів протоколів TCP/IP, що забезпечує можливість інтеграції голосового трафіку й даних в одній мережі, а це дозволяє спростити мережеву інфраструктуру, відмовившись від непотрібних мережевих платформ.

Найбільші можливості в створенні потужного мультисервісного терміналу надає персональний комп'ютер:

– завдяки модульній структурі розширення його функцій зводиться до додавання різноманітних карт і спеціального програмного забезпечення;

– використання ПК як мультисервісного пристрою для отримання послуг зв'язку в різних інформаційних середовищах, використовуючи як мультимедійний термінал, що поєднує текстову, звукову та відеоінформацію в одному сеансі зв'язку.

Тобто, *конвергенція забезпечила перехід до мереж зв'язку наступного покоління*, що якісно змінить усі сфери життя й діяльності людини.

2.7 Інфокомунікаційна мережа

Сукупність ресурсів мережі, задіяних у виробництві та наданні користувачам конкретної послуги або певного набору послуг, прийнято називати платформою надання послуг.

Використовуючи поняття «мережеві ресурси» та «платформа надання послуг», визначимо терміни «інфокомунікації» і «інфокомунікаційна мережа».

Інфокомунікації – це сукупність мережевих ресурсів, призначених для спільної участі у виробництві та наданні телекомунікаційних, інформаційних та інших послуг інформаційного співтовариства.

Інфокомунікації забезпечують:

– можливість перенесення в просторі інформаційних повідомлень;

– взаємодію інформаційних систем;

– виробництво нових послуг та інформації.

Інфокомунікаційна мережа є комплексом термінальних пристроїв користувачів, кінцевих систем мережі та універсальної платформи виробництва та надання послуг, які відповідають різноманітним вимогам користувачів до їх типу та якості.

Інфокомунікаційну мережу як фізичний об'єкт зображено на рис. 11.

Термінальними пристроями користувачів називають пристрої, призначені роботи в мережі, якими є як кінцеві пристрої телекомунікаційних служб: телефонні апарати (стаціонарні, системні, мобільні, IP-телефонії), пристрої телематичних служб (факсимільні апарати, телетекси, відеотермінали тощо), так і багатофункціональні термінали на основі комп'ютерів.

Універсальну платформу надання широкого спектру послуг інфокомунікаційної мережі ще називають мультисервісною мережею,

відмінною рисою якої є *мережеве закінчення з універсальним відкритим інтерфейсом.*

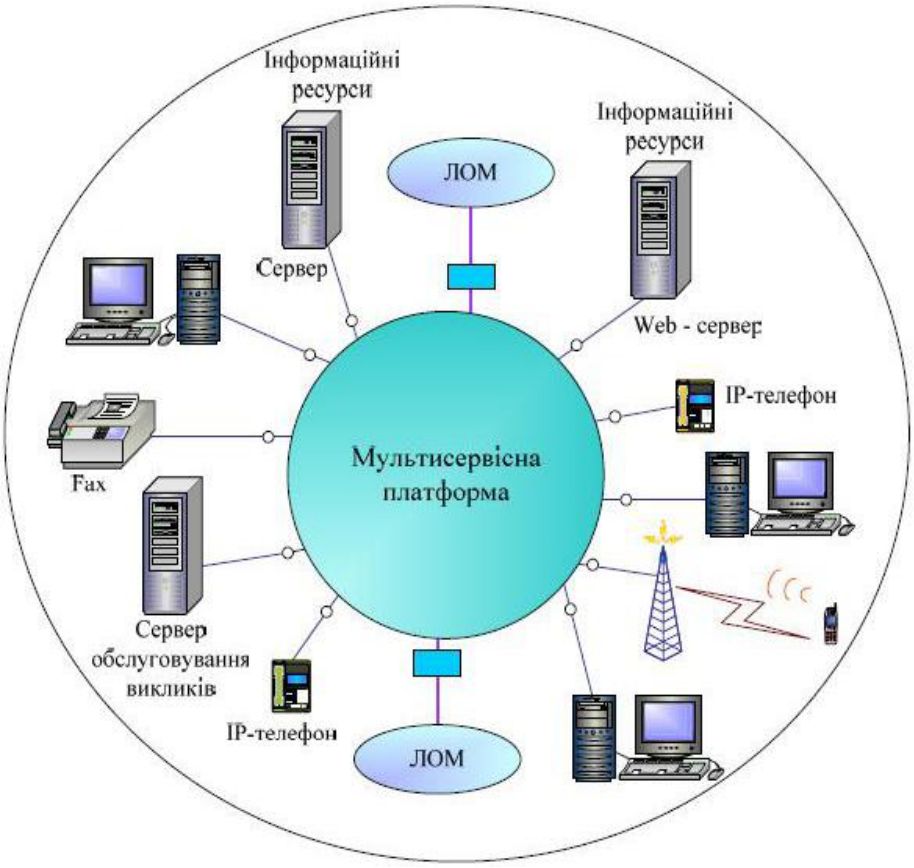


Рисунок 11 – Інфокумунікаційна мережа

Інфокомунікаційна мережа дозволяє вирішувати найбільш актуальні завдання:

– надання користувачам можливості обміну інформаційними повідомленнями різного типу (мова, відео, дані);

– швидке та якісне отримання необхідної інформації з будь-якого віддаленого джерела в мережі;

– автоматизацію процесів обробки, накопичення, зберігання великих обсягів інформації в мережі, самого процесу виробництва інформації.

У результаті конвергенції все сучасне цифрове мережеве та термінальне (користувальницьке) обладнання перетворюється в набір *різнофункціональних комп'ютерів.*

2.8 Глобальна інформаційна інфраструктура

Глобальна інформаційна інфраструктура пропонує користувачам набір комунікаційних послуг, які забезпечують відкриту множинність застосувань, охоплюють усі види інформації та надають можливість її отримання в будь-якому місці, в будь-який час, за прийнятною ціною і з прийнятною якістю.

Створенню глобальної інформаційної інфраструктури сприяють конвергенція технологій, упроваджених у галузі телекомунікацій, комп'ютерів і споживчої електроніки. На Урядовій конференції країн «великої вісімки», проведеній Комісією Європейського Економічного Союзу (ЄЕС) в лютому 1995 року, було узгоджено основні принципи, на яких має базуватися розвиток глобальної інформаційної інфраструктури, серед яких:

– забезпечення відкритого доступу до мереж;

– гарантія забезпечення загального доступу до послуг, а саме:

– *мобільності* – можливості доступу до послуг з різних місць та під час руху. При цьому визначення та локалізація джерела надходження запитів повинні забезпечуватись мережею;

– *номадизму* – можливості вільного переміщення, зберігаючи при цьому доступ до послуг, незалежно від доступності або недоступність цих послуг в місцевому середовищі, тобто безперервність доступу в просторі та часі;

– забезпечення рівних можливостей для користувачів, зважаючи на культурне та мовне розмаїття;

– необхідність міжнародного співробітництва з особливою увагою до найменш розвинених країн; сприяння відкритій конкуренції та заохочення приватних інвестицій.

Висновки

Інформація про передачу даних між пунктом призначення та мережею чи іншим користувачем включає в себе інформацію[9] про передачу, що використовується для встановлення зв'язку та контролю за його розвитком (наприклад, утримання запиту, передача запиту). Інформація про зв'язок також включає в себе інформацію доступну для оператора мережі/постачальника послуг мережі (наприклад, тривалість зв'язку) [с. 17][10].

У спеціальній літературі й міжнародних документах *відомості про проходження інформації* іменуються як «історичні дані», «дані про потоки» або «дані про потоки інформації» і вказують на джерело, призначення, шлях або маршрут, час, дату, розмір, тривалість чи тип мережевого сервісу.

Принципи глобалізації можна реалізувати завдяки:

– розвитку глобальних ринків для мереж, послуг та застосувань;

– гарантії конфіденційності та захисту даних;

– захисту прав інтелектуальної власності;

– співробітництву в науково-дослідницької діяльності та в розробці нових застосувань.

[9] У спеціальній літературі й міжнародних документах відомості про проходження інформації іменуються як «історичні дані», «дані про потоки» або «дані про потоки інформації» і вказують на джерело, призначення, шлях або маршрут, час, дату, розмір, тривалість чи тип мережевого сервісу.

[10] Офіційний переклад нормативних актів Євросоюзу в сфері інформаційно-комунікаційних технологій. Громадська організація ІНТЕРНЬЮЗ-УКРАЇНА. – Київ, 2000. – 219 с.

ЛЕКЦІЯ 3. МОДЕЛІ СИСТЕМНОГО ОПИСУ МЕРЕЖЕВОЇ АРХІТЕКТУРИ

План

Вступ
1. Поняття архітектури мережі.
2. Моделі топологічної структури мережі.
3. Моделі організаційної структури мережі.
4. Моделі логічної структури мережі: протокольної; програмного
5. забезпечення.
6. Компоненти і моделі фізичної структури.

Висновки

Література

1. Теоретичні основи телекомунікаційних мереж : навч. посіб. /М.М. Климаш, Б.М.Стрихалюк, М.В.Кайдан. – Львів : вид-во УАД, 2011. – 496 с.

2. Стеклов В. К. Телекомунікаційні мережі / В. К. Стеклов, Л. Н. Беркман. – К. : Техніка, 2001. – 392 с.

3. Буров Є. Комп'ютерні мережі / Є.Буров. – Львів : БаК, 1999. – 468 с.

Вступ

Вивчаючи питання лекції будемо використовувати узагальнюючі терміни «*мережа зв'язку*» (або просто «*мережа*»), відповідно до контексту, навантажену або ненавантажену телекомунікаційну мережу.

На логічному рівні мережу зв'язку описують такими моделями:

- функціональна модель;
- протокольна модель;
- модель програмного забезпечення.

3.1 Поняття архітектури мережі

Усі мережі зв'язку належать до класу об'єктів, які називають великими чи складними системами.

Складні системи за своїм складом є гетерогенними, тобто характеризуються величезною кількістю неоднорідних елементів і зв'язків між ними. Мережам зв'язку властиво мати всі ознаки складних систем і підпорядковуватися відповідним їм закономірностям.

Ієрархічність – розташування частин та елементів цілого в порядку від вищого до нижчого. Дотримуючись цієї закономірності, ми можемо розчленовувати мережу на окремі підмережі (сегменти) нижчого порядку.[11]

Комунікаційність – закономірність, яка вказує на численність зв'язків (комунікацій) системи: зовнішніх – з навколишнім середовищем і внутрішніх – із власними підсистемами та елементами. Це означає, що мережу будь-якого рівня ієрархії не можна розглядати ізольовано, без урахування факторів, які впливають ззовні (вищерозташованих систем) і не можна розчленовувати її без урахування типу взаємозв'язку підмереж й елементів нижчого порядку.

Емерджентність – закономірність, що полягає в прояві системою інтегрованої риси – цілісності, яка не притаманна окремим її елементам. Наприклад, у мережі можна виокремити такі функціонально важливі й відносно незалежні підсистеми, як система мережевих застосувань, транспортна система, система керування мережею та ін.[12]

Процес побудови ряду окремих структур системи має назву «структуризація». Отримані в результаті структуризації окремі структури системи взаємопов'язані між собою. Щоб відобразити міжструктурні зв'язки, ізольовані структури розташовують у певному порядку, наприклад, ієрархічному, де ієрархія відбудовується відповідно до пріоритету аспектів дослідження системи.

Структуризація складної системи не піддається формалізації і тому її часто ототожнюють з архітектурою.

Архітектура – це багаторівневий опис системи, отриманий шляхом структуризації.

Уявлення про будову та функціонування мережі зв'язку, як складної системи, може бути сформовано в результаті формування та дослідження її архітектури. При цьому доцільним є розгляд таких відокремлених структур:

– *топологічної*, яка визначає розташування пунктів мережі та ліній зв'язку;

– *організаційної*, яка визначає тип, призначення, статус елементів мережі залежно від виконуваних ними функцій;

– *логічної*, яка описує роботу мережі на рівні взаємодії мережевих функцій та правил встановлення зв'язку між кінцевими системами, взаємодіючими через телекомунікаційну мережу;

– *фізичної*, яка відображає фізичні пристрої та програмні засоби, в котрих реалізовано функціональні елементи мережі, фізичні середовища передавання сигналів.

---

[11] Наприклад, глобальна мережа може бути представлена сукупністю територіальних мереж різного масштабу: континентальних, регіональних, міських, локальних та ін.

[12] Жодну з цих систем не можна ототожнити з мережею зв'язку в цілому, і тільки їх взаємо зв'язок відображає це поняття. Системний підхід, системний аналіз, як наукові методи пізнання, засновані на методологічних принципах системології, передбачають усебічний розгляд складної системи в багатьох аспектах. Для кожного аспекту до уваги береться група найбільш типових елементів і визначається різновид зв'язків між ними, які створюють певну, окрему структуру системи.

Кожна з конкретних структур може бути змодельована. Модель дозволяє відобразити найбільш важливі компоненти та зв'язки об'єкта, і не враховувати несуттєві, відповідно до мети дослідження, деталі. Сукупність таких моделей будемо називати системним описом мережевої архітектури (рис. 12).

Рисунок 12 – Системний опис мережевої архітектури

3.2 Моделі топологічної структури мережі

На рівні найбільш узагальненого уявлення, будь-яка мережа складається з сукупності *пунктів* і з'єднуючих їх *ліній*, взаємне розташування яких характеризує зв'язність мережі та здатність забезпечувати інформаційний обмін між різними адресатами. Така відокремлена структура мережі має назву «топологія».

Розрізняють топології *фізичних зв'язків* і *логічних зв'язків*.

Топологія фізичних зв'язків відображає схему з'єднань елементів мережі.

Для дослідження топологічних особливостей мережі її зручно зображувати у вигляді *точок* і з'єднуючих їх *дуг*. Така геометрична фігура має назву *граф*. Точки в графі називають *вершинами*, а дуги, якщо не враховується їх спрямованість, – *ребрами*. Граф є моделлю топологічної структури мережі.

Вибір топології – це завдання, вирішення якого є першочерговим при побудові мережі. Він здійснюється з урахуванням таких вимог, як *економічність* і *надійність зв'язку*.

Задача вибору топології мережі вирішується, якщо відомим є набір типових *топологій (примітивів)*, які можна використовувати як окремо, так і в комбінації.

Розглянемо ряд типових топологій (назвемо їх базовими) та охарактеризуємо їх особливості.

Топологія «точка – точка» уявляє собою сегмент мережі, який зв'язує фізично й логічно два пункти (рис. 13).

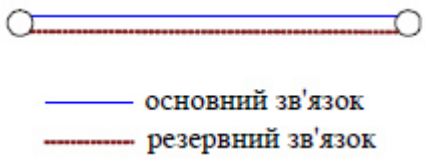


Рисунок 13 – Топологія «точка – точка»

Надійність зв’язку в такому сегменті може бути підвищена за рахунок долучення резервного зв’язку, який забезпечує стовідсоткове резервування, яке називають *«захистом типу 1+1»*. У разі виходу з ладу основного зв’язку мережа автоматично від’єднується до резервного.

Ця базова топологія найбільш широко використовується:

– при передачі великих потоків інформації високошвидкісними магістральними каналами, наприклад, трансокеанськими підводними кабелями, які обслуговують цифровий телефонний трафік;

– як складова частина радіально-кільцевої топології (у якості радіусів).

Топологія «точка – точка» з резервуванням типу 1+1 може розглядатися як варіант топології «кільце».

Деревоподібна топологія може мати різні варіанти (рис.14)

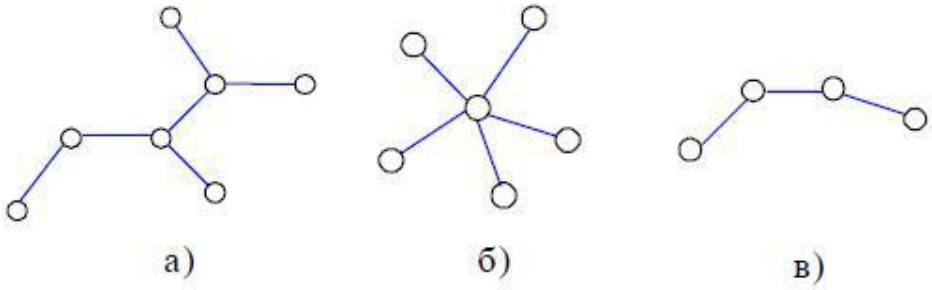


Рисунок 14 – Деревоподібна топологія: а) дерево; б) зірка; в) ланцюг

Особливістю сегменту мережі, що має деревоподібну топологію, будь-якого з перелічених варіантів, є те, що зв’язність п пунктів на рівні фізичної топології тут досягається числом ребер $K = n - 1$, що забезпечує високу економічність такої мережі. На логічному рівні, кількість зв’язних шляхів передавання інформації між кожною парою пунктів у такому сегменті завжди дорівнює $H = 1$. З точки зору надійності, це досить низький показник. Підвищення надійності в таких мережах досягається введенням резервних зв’язків (наприклад, захисту типу 1+1).

Деревоподібна топологія застосовується в локальних мережах, мережах абонентського доступу.

Топологія «кільце» (рис. 15) характеризує мережу, в якій до кожного пункту приєднано дві *(і тільки дві)* лінії. Кільцева топологія використовується в локальних мережах, у сегментах міжвузлових з’єднань територіальних мереж, а

також у мережах абонентського доступу, організованих на базі волоконно-оптичного кабелю.

Число ребер графа, яке відображає фізичну топологію, дорівнює кількості вершин: $K = n$ і вказує на порівняно незначні витрати на мережу.

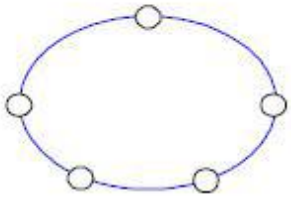


Рисунок 15 – Типологія «кільце»

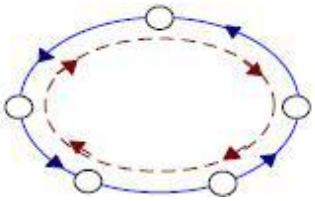


Рисунок 16 – Типологія «подвійне кільце»

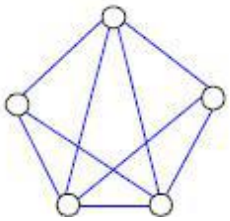


Рисунок 17 – Повнозв'язна типологія

На логічному рівні між кожною парою пунктів можна організувати $к = 2$ незалежних зв'язаних шляхи (прямий та альтернативний), що забезпечує підвищення надійності зв'язку в такому сегменті, особливо при використанні резервування 1+1, так званого *«подвійного кільця»* (рис. 16).

Подвійне кільце утворюється фізичними з'єднаннями між парами пунктів, при яких інформаційний потік направляється в двох протилежних напрямках (східному і західному), причому один напрям використовується як основний, другий – як резервний.

Повнозв'язна топологія (рис. 17) забезпечує фізичне та логічне з'єднання пунктів за принципом «кожен з кожним». Граф, який включає п вершин, містить $K = n(n – 1)/2$ ребер, що впливає на високу вартість мережі. Кількість незалежних зв'язних шляхів між кожною парою пунктів у такому сегменті мережі дорівнює $H = n – 1$.

Повнозв'язна топологія на логічному рівні забезпечує максимальну надійність зв'язку завдяки можливості організовувати велику кількість обхідних шляхів. Така топологія притаманна територіальним мережам при формуванні сегментів базових і опорних (магістральних) мереж. Максимальної надійності зв'язку в сегменті можна досягти, використовуючи на обхідних напрямках альтернативні середовища поширення сигналів (наприклад, волоконно-оптичний кабель і радіорелейна лінія).

Коміркова топологія (рис. 18). Кожен пункт сегмента має безпосередній зв'язок із невеликою кількістю пунктів, найближчих за відстанню. При великій кількості вершин число ребер $R \approx r\ n/2$, де r – кількість ребер, інцидентних кожній вершині. Коміркові сегменти мають високу надійність зв'язку при меншій кількості ребер у порівнянні з повнозв'язним сегментом.

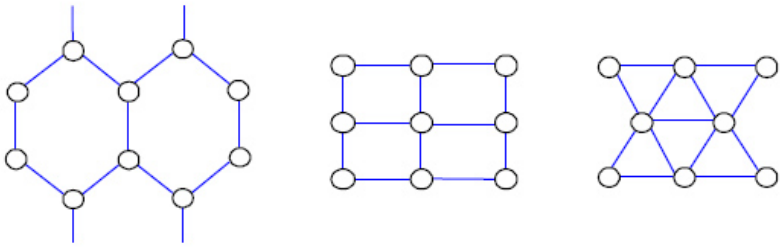


Рисунок18 – Коміркова топологія

Використання повнозв'язної та коміркової топологій є доцільним лише в сегментах із високою концентрацією трафіку, тому що їх реалізація пов'язана із значними витратами.

Складні (змішані) топології. Реальні мережі часто мають складні топології, що є розширеннями та/або комбінаціями базових фізичних топологій (рис. 19). За рахунок використання складних топологій вдається забезпечувати вимоги до розширюваності та масштабованості мереж.

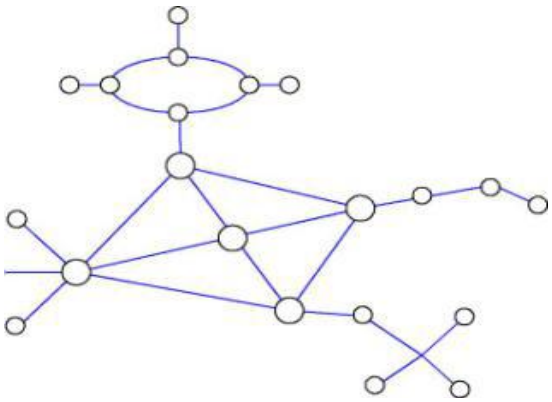


Рисунок 19 – Складна мережева топологія

Топологія логічних зв'язків дає уявлення про шляхи переміщення інформаційних повідомлень у мережі від джерел до одержувачів відповідно до адресної інформації. Зв'язані шляхи можуть бути визначені лише в зв'язних фізичних топологіях (методи знаходження зв'язуючих шляхів із урахуванням різних критеріїв.

Під *зв'язуючим шляхом* розуміють послідовність ліній і вузлових пунктів, через які проходить маршрут перенесення інформації в мережі.

Маршрут вказує на спрямованість шляху (траєкторію перенесення інформації по мережі).

Сукупність потоків інформації (службової та призначеної для користувача), які переміщаються в мережі за певними маршрутами та навантажують мережу протягом певного інтервалу часу, називається *мережевим трафіком*.

Таким чином, *топологія логічних зв'язків є адекватною плану розподілу потоків мережевого трафіку*.

Узагальнено *планом розподілення потоків у мережі* називають суперпозицію (накладання) маршрутів передачі інформації, визначених у мережі для кожної пари джерело – одержувач.

Елементами моделі логічної топології є логічні вузли та маршрути, які їх поєднують.

Логічними вузлами, або далі скорочено *вузлами мережі* на рівні топології логічних зв'язків називаються будь-які фізичні пристрої, яким призначені адресні ідентифікатори.

Вузол може бути комп'ютером (робочою станцією або сервером), комунікаційним пристроєм, мережевим принтером – будь-яким пристроєм з *мережевим інтерфейсом* (встановленою мережевою платою).

Вузол, у якому не передбачено виконання функцій вузлових пунктів (концентрації, мультиплексування, комутації або маршрутизації), називається хостом[13].

Хост – це вузол, який є кінцевою системою мережі і не може виконувати функції транзитного вузлового пункту.

Адресні ідентифікатори підрозділяються на адреси вузлів і мережеві адреси.

Адреси вузлів мають назву локальні[14] чи апаратні адреси.

У локальних сегментах локальні адреси ще називають *фізичними адресами, адресами точки доступу до середовища*. Це унікальні числові значення можуть встановлюватися як програмно, так і апаратно.

У територіальних сегментах локальні розширення ідентифікують мережеві інтерфейси взаємодіючих всередині передбаченої використовуваною телекомунікаційною технологією.

Мережева адреса – це логічна адреса, яка присвоюється адміністрацією (спеціальним міжнародним органом) і визначає сегмент приєднання пристрою. Повна мережева адреса складається зі спільного для всіх вузлів номера мережі й унікального в цій мережі номера вузла.

В інформаційній мережі (як логічній надбудові) застосовуються також *ідентифікатори (адреси) прикладних процесів*, які взаємодіють через мережу.

Моделями топологій логічних зв'язків прийнято вважати:

– логічну шину;

– логічне кільце;

– комутовану топологію.

Принцип побудови тієї чи іншої моделі топологічних зв'язків ґрунтується на виборі механізму, який забезпечує зв'язність вузлів. Топологія логічних зв'язків може збігатися з топологією фізичних зв'язків у мережі або відрізнятися. На основі однієї й тієї ж топології фізичних зв'язків можна побудувати різні топології логічних зв'язків, використовуючи відповідне комунікаційне (мережеве) обладнання.

---

[13] Термін «хост» широко використовується в Інтернеті. Усі комп'ютери з унікальними IP-адресами та доменними іменами, які призначено для виконання програм користувачів та під'єднано до глобальної мережі, традиційно називаються хостами.

[14] Слово «локальний» означає «той, що діє в межах конкретного сегменту».

3.3 Моделі організаційної структури мережі

Організаційна структура мережі зв'язку визначає *рольове призначення* й статус мережевих елементів та утворених ними структурних компонентів залежно від поставленого завдання та займаного місця в мережі. Рольове призначення характеризує, умовно кажучи, *«права та обов'язки»* елементів або виділених структурних фрагментів мережі під час реалізації покладених на них функціональних завдань, а статус – рівень їх значимості відповідно до ієрархічної приналежності.

Елементами моделі організаційної структури є пункти та лінії зв'язку.

Пункти мережі підрозділяються на *кінцеві* і *вузлові*.

Кінцеві пункти (КП) – це пункти, в яких розміщено термінальне обладнання користувачів і кінцеві системи мережі (сервери, на яких зосереджено інформаційні ресурси й застосування, у тому числі застосування системи керування мережею).

Пункти, призначені для розміщення термінального обладнання користувачів, яке забезпечує доступ в мережу, функціонують у ролі *абонентських пунктів* (АП).

Пункти, у яких зосереджено інформаційні ресурси, називаються *інформаційними центрами* (ІЦ), а пункти системи керування відповідно – *центрами керування* (ЦК).

У кінцевих пунктах телекомунікаційна мережа представлена пристроєм *мережевого закінчення* (Network Termination Unit, NTU), або просто *мережевим закінченням* (Network Termination,TU), яке в *організаційній структурі* набуває *статусу точки присутності телекомунікаційної мережі*. Прикладом цього є звичайна телефонна розетка, інформаційна розетка з телекомунікаційним роз'ємом для під'єднання комп'ютера.

Вузловий пункт – це пункт мережі, в якому сходяться дві і більше ліній зв'язку.

У вузловому пункті зазвичай розміщується комунікаційне (мережеве) обладнання, за допомогою якого можуть виконуватися такі функції, як *концентрація, мультиплексування, комутація* та *маршрутизація*.

Концентрація передбачає поєднання декількох невеликих за потужністю вхідних інформаційних потоків з метою отримання більш потужного вихідного потоку. Функція може бути реалізована в спеціалізованому пристрої на основі статистичного ущільнення (асинхронне мультиплексування). В концентраторі для локальних мереж, який має назву «хаб», ця функція виконується досить умовно. Повідомлення, яке надходить на один з входів хаба, передається одночасно на всі виходи.

Розподілення – функція, протилежна концентрації, тобто відгалуження від концентрованого вхідного інформаційного потоку малих за потужністю вихідних потоків і розподіл їх між виходами. Функція реалізується в пристроях, які називаються відгалужувачі.

Мультиплексування забезпечує можливість передачі декількох потоків інформації однією лінією, що здійснюється закріпленням за кожним із них фіксованої частини ресурсу лінії (смуги пропускання або часу зайняття). Фіксований розподіл ресурсу лінії залишається незмінним навіть у періоди відсутності інформації, тобто функція концентрації не спрацьовує. Зворотна функція – *демультиплексування*. Реалізація в комунікаційних пристроях (мультиплексорах) функції мультиплексування завжди поєднується з демультиплексуванням.

Комутація є процесом встановлення зв'язку між входами та виходами комутаційного пристрою на основі аналізу адресної інформації повідомлень і використання інформації відповідних таблиць комутації. Комутація може бути оперативною (на час передачі одного повідомлення) та довготривалою, яка здійснюється шляхом кросування ліній, які сходяться у вузловому пункті.

Маршрутизація – це поєднання процедур пошуку зв'язних шляхів (маршрутів) між вузлами мережі з метою формування таблиць маршрутизації та встановлення зв'язку між входами та виходами пристрою на основі адресної інформації повідомлень та з урахуванням вибору найкращого (за обраним критерієм) маршруту проходження повідомлення мережею.

У комунікаційному пристрої може бути реалізована одна з перерахованих функцій, саме тоді цей пристрій відповідно називається або концентратором, або *мультиплексором*, або *комутатором*, або *маршрутизатором* та ін.

Порядок співвідношення між елементами (їх статус) в моделі організаційної структури визначається рівнями їх ієрархії (рис. 20).

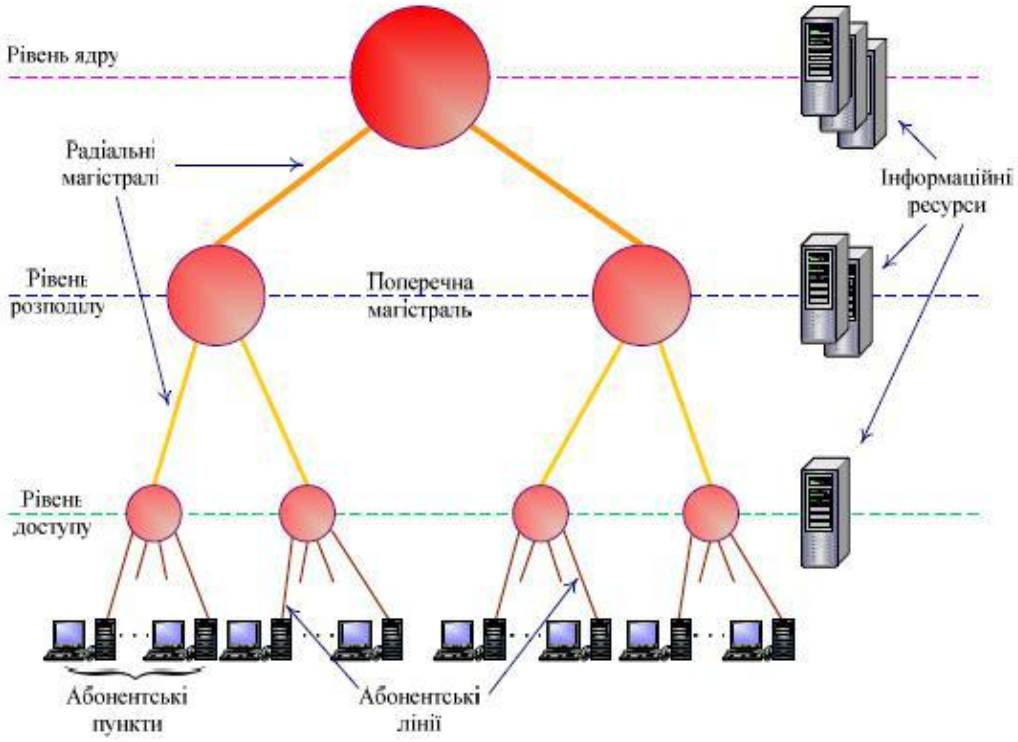


Рисунок 20 – Узагальнена схема організаційної структури мережі

Найнижчий рівень займають АП. Статус вузлових пунктів визначається відповідно рівнем *доступу, розподілу* та *ядра.*

АП під'єднуються до вузлових пунктів рівня доступу. Таким чином для них реалізується право доступу в мережу (до її ресурсів).

Призначення та статус вузлових пунктів рівня розподілу визначається забезпеченням інформаційного обміну між АП, під'єднаними до різних вузлових пунктів рівня доступу. Залежно від способу структуризації мережі, рівень розподілу матиме декілька підрівнів. Вузлові пункти всіх підрівнів розподілу виконують функцію концентрації трафіку у висхідних напрямах і функцію розподілу – у низхідних.

У вузлових пунктах рівня ядра інформаційні потоки досягають максимальної концентрації та перерозподіляються між усіма іншими пунктами мережі. Вузлові пункти рівня ядра мають найвищий статус, оскільки вони забезпечують зв'язність мережі в цілому за рахунок об'єднання вузлових пунктів рівня розподілу.

Точка підключення кінцевих систем (інформаційних центрів мережі) може бути організована у вузловому пункті будь-якого рівня. Це визначається масштабом контингенту користувачів, які мають загальну потребу у зверненні до інформаційного ресурсу. Чим вище рівень підключення ресурсу, тим ширшою є його доступність. Те ж відноситься і до пунктів обладнання системи керування мережею – центрів керування (ЦК). Чим вищим є рівень підключення, тим ширшою зона моніторингу технічного стану елементів мережі.

Лінії зв'язку в моделі організаційної структури також отримують відповідний статус.

Лінії, які з'єднують АП з відповідним вузловим пунктом рівня доступу, мають найнижчий статус і називаються *абонентськими лініями*.

Лінії, які з'єднують вузлові пункти між собою, називаються *магістральними*. Чим вищим є рівень ієрархії з'єднуваних магістралями вузлових пунктів, тим вищим – статус самих магістралей, і, відповідно, вимоги до їх пропускної здатності, надійності.

Магістралі, що з'єднують вузлові пункти, які належать різним рівням ієрархії, називаються *радіальними магістралями*, а ті, що з'єднують вузлові пункти одного рівня, – *поперечними магістралями.*

Призначення вузлових пунктів в моделі організаційної структури відносно кінцевих пунктів, які він обслуговує, незалежно від статусу, може виступати в ролі:

- опорного вузла;
- транзитного вузла;
- опорно-транзитного вузла.

Якщо вузловий пункт забезпечує проходження трафіку тільки між КП конкретної групи, то відносно цих КП він виступає в ролі *опорного вузла*.

Якщо через вузловий пункт проходить трафік від деякої групи КП до будь-яких інших КП мережі, то він виступає в ролі *транзитного вузла*.

Якщо вузловий пункт забезпечує проходження трафіку як внутрішнього, так і зовнішнього обміну деякого конкретного числа КП мережі, то відносно цих КП він виступає у ролі опорно-транзитного вузла.

Для мереж операторів і сервіс-провайдерів актуальними є терміни, що визначають призначення вузлових пунктів відповідно до реалізації функцій доступу.

Функції доступу в територіальних мережах незалежно від рівня ієрархії вузлового пункту прийнято розглядати за наступними аспектами:

– забезпечення доступу користувачів до телекомунікаційних служб та мережевих ресурсів;

– забезпечення доступу при з'єднанні сегментів телекомунікаційної мережі;

– забезпечення доступу до інформаційних ресурсів глобальної мережі Інтернет.

Вузловий пункт, у якому забезпечується доступ користувачів до служб мережі з метою отримання телекомунікаційних та інформаційних послуг, називають сервісним вузлом (вузол рівня доступу, розподілу або ядра).

Вузловий пункт, де забезпечується з'єднання сегментів телекомунікаційної мережі, наприклад, мережі доступу та транспортної мережі, називається вузлом доступу.

Вузловий пункт, у якому забезпечується підключення сервіс-провайдера національного рівня в глобальну інформаційну мережу Інтернет, називається точкою мережевого доступу (Network Access Point, NAP). Це вузловий пункт рівня ядра. Через NAP зорганізується спілкування клієнтів одного національного провайдера з клієнтами інших національних провайдерів.

3.4 Моделі логічної структури мережі

Функціональна модель – це *абстрактний опис мережі зв'язку, що не залежить від принципів її фізичної реалізації*. Вона відображає взаємозв'язок функцій, які виконуються в мережі й які в даному випадку розглядаються як елементи моделі.

Функція – це певний логічний елемент, що виконує конкретне завдання в мережі. Реалізація функцій допустима в таких варіантах:

– у вигляді апаратних засобів;

– у вигляді програмного продукту.

Поняття «функція», що використовується в телекомунікаціях, традиційно передбачало реалізацію зв'язку в апаратному забезпеченні. Однак, завдяки потужному розвитку індустрії програмного забезпечення, виникла можливість реалізації функцій програмним способом. Функції, реалізовані у вигляді програмних продуктів, прийнято називати об'єктами.

Розрізняють такі основні типи функцій мережі зв'язку:

– *прикладні функції* – об'єкти застосувань користувачів;

– *функції обробки та зберігання даних* – об’єкти, що забезпечують виклик об’єктів застосувань, їх взаємодію, а також витяг необхідних даних або розміщення їх у базу даних;

– *функції керування послугами* – об’єкти, що дозволяють формувати послуги, необхідні користувачам, управляти ресурсами мережі, пов’язаними з їх наданням, і взаємодією користувачів з цими послугами;

– *комунікаційні функції* – транспортні функції, функції керування передачею потоків даних, функції керування телекомунікаційними послугами;

– роботою мережі в цілому (моніторинг дієздатності елементів мережі, збір статистики про проходження сигналів, вирішення аварійних і неординарних ситуацій та ін.).

Порядок і правила взаємодії між функціями та об’єктами мережі формують *зв’язки* між елементами у функціональній моделі. Повна специфікація такої взаємодії називається *логічним інтерфейсом*.

Логічний інтерфейс охоплює як набір правил поведінки взаємодіючих елементів, так і формат подання інформації, якою вони обмінюються.

Логічний інтерфейс між об’єктами одного типу називається *протоколом*.

Логічний інтерфейс між комунікаційними функціями отримав назву *еталонної точки телекомунікаційної мережі.*

3.5 Функціональні модулі

Розглядаючи реалізацію функцій та об’єктів доцільно групувати їх в функціональні модулі. Функціональні модулі можуть формуватися як функціональні підсистеми й домени.

У функціональні підсистеми об’єднуються функції та об’єкти, для яких важливою є спільна реалізація. Прикладом утворення функціональної підсистеми є поєднання транспортної функції та функції керування потоками при їх програмно-апаратній реалізації в сегментах телекомунікаційної мережі (рис.21).

Рисунок 21 – Зразок утворення транспортної підсистеми на рівні функціональної моделі I (еталонна точка телекомунікаційної мережі); NTU мережеве закінчення I – інтерфейс (еталонна точка телекомунікаційної мережі); NTU – мережеве закінчення.

У такому контексті телекомунікаційну мережу на рівні функціональної моделі часто називають транспортною підсистемою.

Аналогічно можна виокремити підсистему адміністративного керування мережею, підсистему послуг та програм і менш масштабні підсистеми: підсистему передачі, підсистему розподілу інформації та ін.

Домен – це функціональний модуль, сформований за принципом *приналежності функцій і об'єктів одній групі*. При цьому враховувати їх спільну дію при реалізації в апаратних засобах або програмних продуктах не потрібно. Прикладами можуть бути домен користувача (рис. 22) і домен оператора мережі (рис. 23).

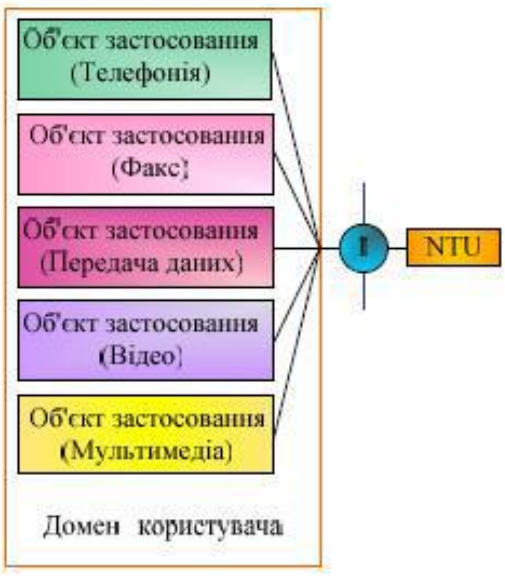


Рисунок 22 – Зразок утворення домену користувача

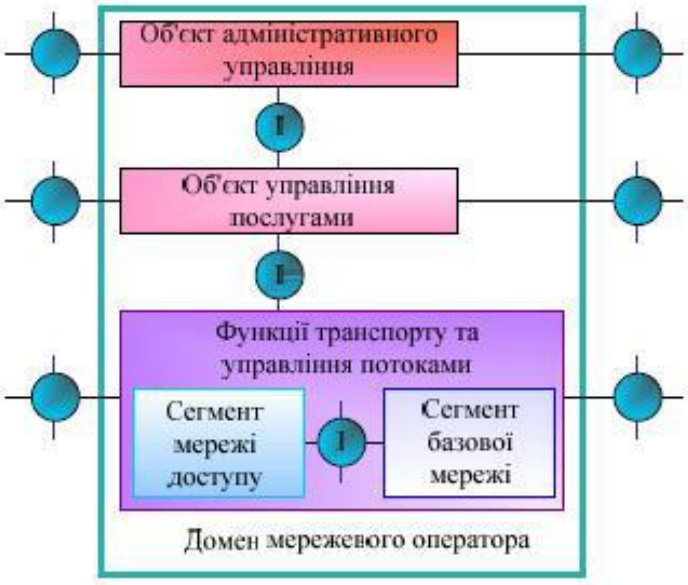


Рисунок 23 – Зразок утворення домену мережевого оператора

Конкретний склад об'єктів (функцій) домену називається *конфігурацією домену*. Конфігурації мережевих операторів можуть бути різними: якщо надання конкретної послуги або набору послуг вимагає участі декількох операторів, їх домени розглядаються на функціональному рівні як об'єднану платформу надання послуг.

Взаємодія функціональних підсистем і доменів реалізується за допомогою логічних інтерфейсів.

Залежно від способу формування функціональних модулів і можливостей їх реалізації (при конкретному рівні науково-технічного прогресу), може *бути сформована одна або інша концепція побудови мережі.*

Наприклад, концепція телефонної мережі полягає в побудові дорогих АТС як єдиної структури, в якій поєднують функції комутації, керування обслуговуваннями викликів, об'єкти послуг та застосувань, а також білінгу. Така АТС у мережі є монолітною, закритою системною структурою та, як правило, не допускає розширення або модернізації з використанням обладнання

інших виробників. Спроба відокремити від АТС підсистему послуг та застосувань породила концепцію інтелектуальної мережі. Це дозволило організувати в телефонній мережі додаткові види обслуговування (розширити конфігурацію домену) та надавати різні послуги за заявками користувачів, формуючи їх з окремих компонентів.

Концепція інтелектуальної мережі припускає наявність таких функціональних модулів (підсистем):

– *модуль розпізнавання викликів*, що вимагається виконанням додаткові види обслуговування (ДВО);

– *модуль формування необхідного сервісу* з незалежних функціональних компонентів;

– *модуль керування мережевими ресурсами* та ін.

При цьому функціонування підсистеми додаткових видів обслуговування є абсолютно незалежним від типу мережі зв'язку. Технологія інтелектуальної мережі може бути реалізована на базі будь-якої комутованої мережі (аналогової або цифрової), а також мережі передачі даних.

Поява Softwitch, добре масштабованого сучасного програмного комутатора, докорінно змінила традиційну закриту систему комутації. Softwitch використовує принципи компонентної побудови мережі та відкриті стандартні інтерфейси між трьома основними функціями: комутація, керування обслуговуваннями викликів, керування послугами та програмами. У такій відкритій розподільчій структурі можуть вільно використовуватися функціональні компоненти різних виробників.

Поділ функцій транспортування інформації та функцій керування її перенесенням мережею, а також відмежування функцій послуг та програм від власне зв'язкових функцій породило концепцію NGN (мереж наступного покоління), в якій зв'язок між компонентами здійснюється виключно через відкриті інтерфейси. З позицій традиційної телефонії вона сприймається як мережа пакетної комутації під керування Softwitch, що підтримує широкосмуговий абонентський доступ і мультисервісне обслуговування трафіку.

3.6 Протокольна модель

Протокольна модель описує роботу мережі зв'язку на рівні правил взаємодії (протоколів) об'єктів (функцій) та функціональних модулів, розосереджених на різних кінцевих системах.

Повний набір протоколів, які забезпечують взаємодію кінцевих систем мережі великий, оскільки при цьому активізується величезна кількість мережевих функцій. При побудові протокольної моделі зручно всі протоколи розбити на групи, відповідно до об'єднання об'єктів у функціональні модулі, кожен з яких вирішує певне коло тісно пов'язаних завдань.

Така група протоколів називається *протокольним рівнем* або *протокольним блоком.* Їх прийнято розташовувати ієрархічно, відповідно до першорядності завдань, які виконуються функціональними модулями (рис. 24).

Ієрархію протокольних рівнів (блоків) протокольної моделі конкретної мережі зв'язку називають *стеком протоколів*.

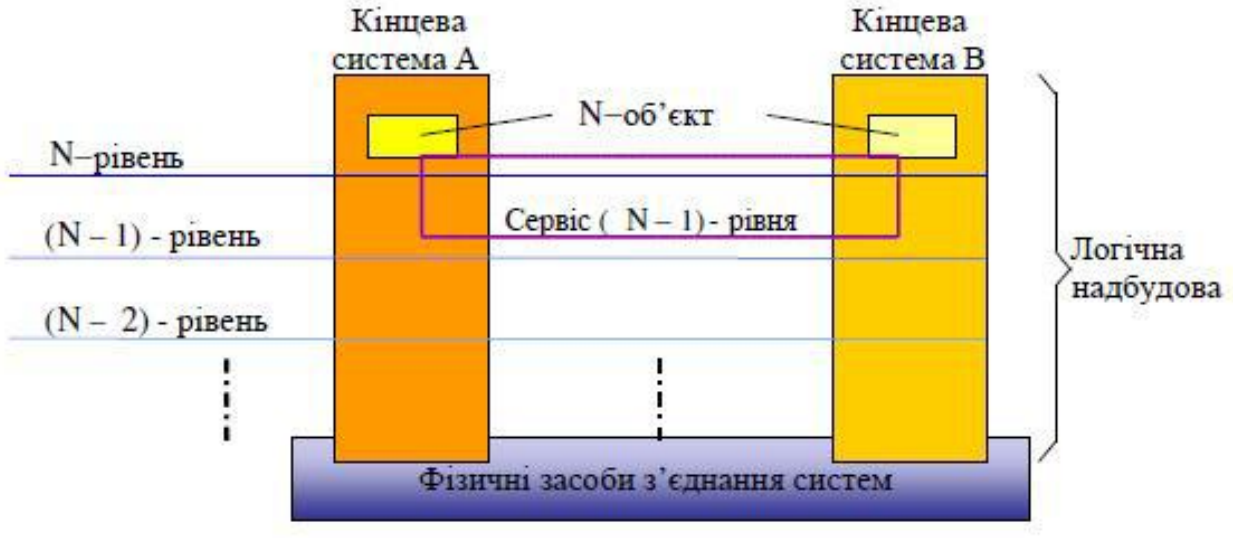


Рисунок 24 – Принцип побудови протокольної моделі

N-об'єкти, виконуючи завдання *N*-рівня, здійснюють локальний комплекс функцій даного рівня.

Протокольні блоки розташовані на рівні таким чином, що можливість виконання завдання *N*-рівня цілком залежить і забезпечується участю об'єктів нижчерозташованого *(N – 1)*-го рівня й так далі.

Таким чином, *N-об'єкти виявляються залученими у взаємодію з (N – 1) – об'єктами, а (N – 1) – об'єкти з (N – 2) – об'єктами і т. д. Тобто, кожен нижчий рівень надає сервіс вищому рівню.*

Будь-який об'єкт *N*-рівня, активізуючись, видає інформацію двох типів:

1) інформацію, яка призначена для *N*-об'єкта іншої кінцевої системи (наприклад, дані користувача) й не пов'язана з операціями підтримання зв'язку об'єктів *N*-го рівня;

2) інформацію керування, яка призначена для об'єкта *(N – 1)*-го рівня, за допомогою якої здійснюється координація процедур «з'єднання» об'єктів *N*-го рівня різних кінцевих систем.

Угоди, які визначають порядок взаємодії об'єктів одного рівня на різних кінцевих системах, називають протоколом, а угоди, які визначають порядок взаємодії об'єктів різних рівнів на одній кінцевій системі – *інтерфейсом*.[15]

[15] Як ілюстрацію того, як відбувається реалізація протоколів і міжрівневих інтерфейсів при ініціалізації взаємодії двох кінцевих систем, проаналізуємо процес ділового інформаційного спілкування між двома користувачами, які знаходяться в різних установах. Особа, яка підготувала інформаційне повідомлення, передає його помічникові з адміністративної роботи (рівень, розташований нижче) та повідомляє ім'я одержувача. Помічник з адміністративної роботи шифрує повідомлення (якщо це необхідно) та форматує його (розміщує на офіційному бланку). Підготовлений документ передається секретареві (наступний нижчий рівень), який, у свою

Підкреслюючи важливість протокольної моделі в реалізації принципів взаємодії кінцевих систем, її називають ще архітектурою зв'язку в мережі. Архітектура зв'язку є основою для розробки мережевих стандартів, які є надзвичайно необхідними для забезпечення взаємодії між обладнанням різних виробників і сумісності мереж різних операторів.

3.7 Модель програмного забезпечення

Функціонування мережі зв'язку – це складний комплекс програмних і апаратних компонентів. Саме програмне забезпечення визначає функціональність мережі зв'язку. Сучасне мережеве програмне забезпечення є *структуризованим*. Основні функції та вся архітектура зв'язку (протокольні моделі) реалізуються в програмному забезпеченні мережі.

Аналіз програмної структури (ПЗ) дозволяє розглянути ієрархію мережевого програмного забезпечення. Елементами цієї структури є програмні модулі, в яких реалізовано об'єкти та логічні модулі мережі.

Ієрархія програмного забезпечення може бути подана таким чином:

– прикладне ПЗ;
– проміжне ПЗ;
– базове ПЗ.

У *прикладному ПЗ* реалізовано об'єкти застосувань.

Розрізняють два типи застосувань, які впливають на структуру організації ПЗ – локально обмежені і розподільчі.

Локально обмежене застосування інсталюється, викликається, керується та виконується в межах однієї кінцевої системи та не вимагає залучення комунікаційних функцій.[16]

Розподільче застосування складається з кількох компонентів, які можуть виконуватися в різних кінцевих системах а, отже, вимагають організації взаємодії цих кінцевих систем.[17]

Компоненти розподільчого застосування можуть неодноразово використовуватися іншими застосуваннями. У цьому випадку вони стають

чергу, кладе його в конверт, додає повну адресу та наклеює поштову марку. Кур'єрський рівень забезпечує фізичну доставку конверта серед іншої кореспонденції за адресою одержувача.

У такій системі відправник не має уявлення про механізм доставки. Він цілком покладається на сервіси нижчих рівнів і не турбується про те, як вони реалізуються. Це принциповий момент, який є необхідним у правильно сформованому стеку протоколів. Будь-який рівень повинен мати можливість змінювати механізм реалізації наданого ним сервісу, не впливаючи на роботу будь-якого іншого рівня. Так, наприклад поштовий кур'єр може доставляти кореспонденцію на велосипеді, автомобілі або поїзді, але це жодним чином не позначиться на роботі інших співробітників апарату. Вони повинні бути впевнені, що кореспонденція буде доставлена адресатові. Або, якщо передані дані в системі обробляються з використанням повного стека протоколів, ми можемо замінити мідне середовище передачі на оптико-волоконне, й це не впливатиме на програмне чи апаратне забезпеченні верхніх рівнів стека.

[16] Прикладом може бути редагування документа при підготовці тексту на комп'ютері користувача (терміналі користувача).

[17] Наприклад, спільне редагування тексту значної за обсягом публікації користувачами, які знаходяться на віддалі.

об’єктами проміжного ПЗ і підтримують послуги, пов’язані з інтелектуальними можливостями мережі.

Проміжне ПЗ реалізує в мережі функції керування послугами та функції адміністративного керування мережею. Об’єкти обох груп ПЗ аналогічно до компонентів розподільчих застосувань взаємодіють за допомогою комунікаційних функцій мережі.

Базове ПЗ призначено для забезпечення об’єктів прикладного ПЗ та проміжного ПЗ виконанням спільних дій з іншими об’єктами за допомогою взаємодії середовища з комунікаційними функціями мережі й логічними інтерфейсами користувачів.

Організація цього середовища здійснюється уніфікованими програмними комплексами, які називаються мережевими *операційними системами*. Від того, які концепції керування ресурсами покладено в основу мережевої ОС, залежить ефективність роботи не тільки об’єктів прикладного та проміжного ПЗ, але й мережі в цілому.

Стандартами мережевих ОС де-факто на сьогодні стали системи UNIX і мережеві версії Windows. Логічні компоненти комунікаційних функцій, реалізованих програмно, які забезпечують підтримання зв’язку між віддаленими об’єктами, також розглядають як функції базового ПЗ.

До *базового ПЗ* належать також об’єкти обробки та зберігання даних, реалізовані в таких програмних комплексах, як СКБД (системи керування базами даних), базове ПЗ сервера обробки транзакцій та ін. Тип взаємодії між об’єктами визначається типом об’єктного інтерфейсу, який є подібним до протоколу та функціональної еталонної точки.

Розрізняють такі типи *об’єктних інтерфейсів* (програмних інтерфейсів):

– *прикладний протокол* – логічний інтерфейс між прикладними об’єктами;

– *інтерфейс прикладних програм* – логічний інтерфейс між прикладними об’єктами та об’єктами проміжного ПЗ, які підтримують прикладні об’єкти;

– *протокол проміжного ПЗ* – логічний інтерфейс між об’єктами проміжного ПЗ;

– *інтерфейс базових програм* – логічний інтерфейс між об’єктами проміжного та базового програмного забезпечення, які підтримують об’єкти проміжного ПЗ;

– *інтерфейс «людина-комп’ютер»* – логічний інтерфейс між користувачем об’єктами базового ПЗ, проте він може включати в себе також логічний інтерфейс з об’єктами проміжного ПЗ і навіть об’єктами застосувань.

Мережеве програмне забезпечення є ресурсом, яке бере участь в організації платформ надання послуг, а з цього випливає, що композиційним принципам об’єднання програмних модулів, як і принципам побудови функціональної моделі мережі, притаманна така ж специфіка динамізму, як і принципам побудови функціональної моделі мережі.

3.8 Компоненти і моделі фізичної структури мережі

Розглянемо елементи мереж зв’язку як фізичних об’єктів.[18]

Апаратура, разом з її кабельної системою з’єднань, утворює *фізичне мережеве середовище.* Воно відображається моделлю, яка називається *фізичною структурою мережі*.

Під *фізичною структурою мережі розуміють склад її активного та пасивного обладнання та топологію його розміщення в просторі*.

Активне мережеве обладнання охоплює весь парк кінцевого й комунікаційного устаткування мережі, функціонування якого забезпечується за рахунок споживання електроенергії від зовнішніх джерел живлення. Активне мережеве обладнання виконує комплекси тих функцій мережі, які реалізуються в апаратурі.

Пасивне обладнання мережі, на відміну від активного, не має потреби в джерелах електроживлення й містить у собі кабельну систему, телекомунікаційні роз’єми, комутаційні панелі, комутаційні шнури, монтажне обладнання тощо.

3.9 Узагальнена модель апаратурної реалізації функцій та об’єктів

Узагальнена модель апаратурної реалізації:

– демонструє як реалізуються ті чи інші функції та об’єкти в активному обладнанні мережі, а також інтерфейси між різними апаратними засобами;

– визначає додаткові інтерфейси між обладнанням від різних постачальників та їх характеристики, які підлягають стандартизації.

Узагальнено під *апаратурою* розуміють активне обладнання, в якому функції можуть бути реалізовані як у вигляді апаратного забезпечення, так і у вигляді програмного забезпечення (рис. 25). Апаратура може мати модульну конструкцію, тобто складатися з певної кількості знімних плат.

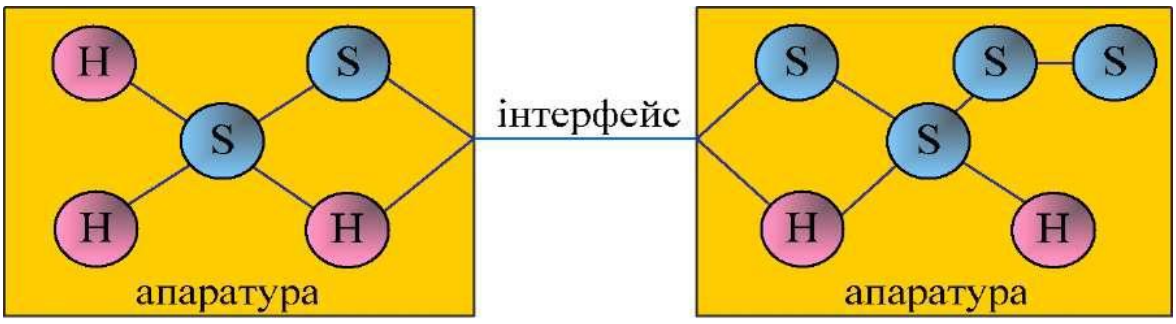


Рисунок 25 – Схема моделі реалізації: H – апаратне забезпечення (Hard ware); S – програмне забезпечення (Soft ware)

[18] Загальна архітектура зв'язку та принципи взаємодії функцій і об'єктів кожного рівня розглянуті раніше.

Елементи моделі апаратурної реалізації є такі:

– *апаратне забезпечення* (Hard ware) – обладнання, в якому одна або декілька функцій реалізовано фізично;

– *програмне забезпечення* (Soft ware) – один або декілька програмних модулів, які представляють собою реалізацію одного або декількох об'єктів;

– *фізичний інтерфейс* (Phisical interface) – фізичне середовище (проводи) для передачі сигналів між різної апаратурою.

Сукупність різних пристроїв, потенційно призначених для використання в мережевих середовищах, називається *парком апаратури активного обладнання мережі.*

Активне обладнання мереж зв'язку складається з:

– пристроїв, які використовуються для організації кінцевих і вузлових пунктів;

– інтерфейсних пристроїв, які забезпечують спряження апаратури з лініями зв'язку.

У технічній літературі набули вжитку такі позначення класів апаратури: DTE, DCE і DTE/DCE.

Усі пристрої в мережі, які функціонують як джерела та приймачі даних на фізичному рівні моделі OSI/ISO, визначаються як клас DTE (Data Terminal Equipment) – кінцева апаратура даних (КАД).

У термінології електрозв'язку дана апаратура називається ще *кінцевим обладнання даних*[19] (КОД).

Разом із функцією формування даних, у реалізації якої в основному бере участь програмне забезпечення, в КАД здійснюється також функція керування потоком даних для узгодження роботи джерела й приймача. Ця функція, як правило, виконується апаратно.

Відмінною особливістю обладнання класу DTE є те, що воно не належить до складу устаткування ліній зв'язку. Для забезпечення обміну даними між пристроями DTE через канали зовнішніх телекомунікацій необхідно використовувати фізичні *інтерфейсні пристрої*, які здійснюють обробку даних з урахуванням вимог передачі каналом певного стандарту. Ці пристрої забезпечують не тільки протокол фізичного рівня, а й фізичні засоби приєднання до середовища передачі, а тому вважаються устаткуванням лінії зв'язку.

Обладнання, що забезпечує сполучення DTE з каналами зв'язку, визначається як клас DCE (Data Communication Equipment) – *апаратура передачі даних* (АПД). Пристрої DCE працюють на фізичному рівні, відповідаючи за передачу й прийом сигналів потрібної форми та потужності в середовищі передачі, й не можуть розглядатися в якості джерел і приймачів даних.

[19] *Дані (інформація)* – представлення інформації відповідним чином для зв'язку, тлумачення, зберігання і обробки відповідним чином [с.15]. Офіційний переклад нормативних актів Євросоюзу в сфері інформаційно-комунікаційних технологій. Громадська організація ІНТЕРНЬЮЗ-УКРАЇНА. – Київ, 2000. – 219 с.

Мережеве обладнання важко розподілити за конкретними класами DTE та DCE. Наприклад, мережевий адаптер можна вважати як складовою комп'ютера (DTE), так і частиною каналу зв'язку (DCE).

У кожному сегменті інформаційної мережі DTE набуває функцій будь-якого джерела даних, поданих у форматі кадру канального рівня, якими можуть бути:

– мережевий адаптер;
– вихідний порт комутатора;
– вихідний порт маршрутизатора.

Хоча кадр даних спочатку продукується мережевим адаптером комп'ютера, а через комутатор або маршрутизатор відбувається його трансляція, для сегменту мережі, під'єднаного до вихідного порту комутатора або маршрутизатора, цей кадр є новим. Отже, вихідний порт комутатора і маршрутизатора стає джерелом кадрів і може розглядатися як вихід пристрою DTE.

Отже, такі комунікаційні пристрої, як мости, комутатори і маршрутизатори розглядають у межах змішаного класу – класу DTE/DCE, де розрізняють відповідні типи портів: DTE або DCE. Для цих портів принципами функціонування є такі:

– для порту DTE сигнал даних передавача є вихідним, а сигнал даних приймача – вхідним;
– для порту DCE – відповідно навпаки.

Пасивне обладнання використовується для побудови телекомунікаційних кабельних систем мережі.

Кабельна система – це складний технічний об'єкт, який будується відповідно жорстким вимогам загальноприйнятих стандартів. До нього належать лінейно-кабельні споруди, кабелі ліній зв'язку, регенераційне обладнання, тощо. Створення й правильна експлуатація такого об'єкта вимагають відповідного рівня кваліфікації проектувальників, монтажників і обслуговуючого персоналу.

Висновки

1. Мережеве програмне забезпечення є ресурсом, яке бере участь в організації платформ надання послуг, а з цього випливає, що композиційним принципам об'єднання програмних модулів, як і принципам побудови функціональної моделі мережі, притаманна така ж специфіка динамізму, як і принципам побудови функціональної моделі мережі.

2. Обладнання кабельних систем для мереж підприємств є набором компонентів і аксесуарів структурованих кабельних систем (СКС) і складається з кабелів, роз'ємів телекомунікаційних та інформаційних розеток, монтажного обладнання, настінних коробів для прокладки кабелів горизонтальної розводку, закладних для прокладання кабелів вертикальної розводки та ін.

ЛЕКЦІЯ 4. СТАНДАРТИ ПРОТОКОЛЬНИХ МОДЕЛЕЙ

План

Вступ

1. Еталонна модель взаємодії відкритих систем ISO/OSI.
2. Принципи інкапсуляції даних в моделі ISO/OSI.
3. Промисловий стандарт стека протоколів TCP/IP.
4. Переваги і недоліки моделі ISO/OSI і TCP/IP.

Висновки

Література

1. Теоретичні основи телекомунікаційних мереж : навч. посіб. /М.М. Климаш, Б.М.Стрихалюк, М.В.Кайдан. – Львів : вид-во УАД, 2011. – 496 с.
2. Буров Є. Комп'ютерні мережі / Є.Буров. – Львів : БаК, 1999. – 468 с.
3. Управління телекомунікаціями із застосуванням новітніх технологій / Кривуца В. Г., Беркман Л. Н., Стеклов В. К. та ін.]. – К.: Техніка, 2007. – 384 с.

Вступ

Завдання побудови мережі – це поєднання різноманітного обладнання, подальша функціональність та спільна робота якого залежить від забезпечення його сумісності, що відображено в стандартах.

Мережева технологія набуває законного статусу, коли її положення закріплюються у відповідному стандарті. Стандарти мереж описують мережі як відкриті системи.

Відкритою системою називається будь-яка система (мережа, програмний продукт, апаратний засіб), яка побудована відповідно до відкритих специфікацій.

Специфікація – це формалізований опис апаратного або програмного компонента мережі, способу його функціонування, взаємодії з іншими компонентами, умов експлуатації й особливих характеристик.

Стандартом стає відкрита специфікація, яка приймається в результаті досягнення згоди після всебічного обговорення всіма зацікавленими сторонами та оприлюднення її у відкритій пресі.

4.1. Еталонна модель OSI/ISO

У 1977 році ISO почала розробку стандартів універсальної архітектури зв'язку, яка отримала назву Еталонної моделі взаємодії відкритих систем (Open System Interconnection, OSI) або скорочено – модель OSI/ISO.

Модель OSI/ISO є концепцією застосування відкритих стандартів, спрямованою на забезпечення сумісності між різними системами, що дозволяє мінімізувати кількість угод, які не мають безпосереднього відношення до організації самого з'єднання між системами. Перша версія стандартів моделі OSI/ISO була випущена як стандарт X.200. Робота зі стандартизації моделі OSI/ISO, спільну участь у якій беруть ISO і ITU-T, триває до сьогодні.

Еталонна модель OSI є визначальним документом для розробки відкритих стандартів з організації з'єднань систем і мереж зв'язку. За основу прийняті такі *принципи*:

– кількість протокольних рівнів не повинна бути занадто великою, щоб розробка мережі та її реалізація не ускладнювалися, водночас ця кількість не має бути занадто малою, щоб не перевантажувати логічні модулі кожного рівня;

– рівні повинні чітко відрізнятися логічними модулями й функціями (об'єктами), які на них виконуються;

– функції та протоколи одного рівня можуть змінюватися, якщо це не порушує інші рівні; кількість інформації, яка передається через інтерфейси між рівнями, повинна бути мінімальною;

– допускається подальше структурування рівнів на підрівні, якщо виникає необхідність локального зосередження на функціях у межах одного рівня. Виокремлення підрівнів є доцільним, якщо постає потреба поділу трудомісткого завдання на окремі, менш складні.

У результаті розроблено еталонну модель, яка містить сім рівнів (рис. 26).

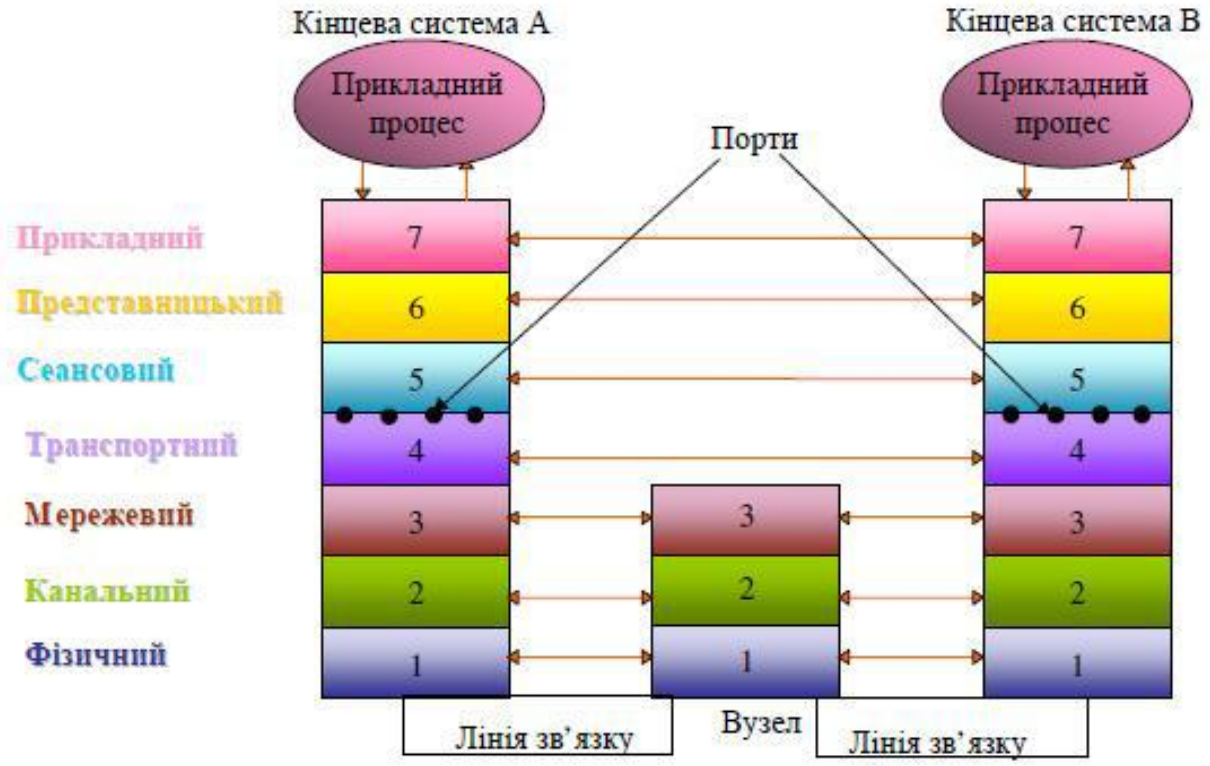


Рисунок 26 – Еталонна модель OSI

Найвищим, сьомим, рівнем моделі OSI є *прикладний рівень*, на якому здійснюється керування терміналами й прикладними процесами в кінцевих системах мережі, які є джерелами та споживачами інформації. Цей *рівень надає сервіси безпосередньо для прикладних програмам* користувачів.

Щоб уникнути несумісності між призначеними для користувача програмами, прикладний *рівень визначає стандартні способи надання сервісів цього рівня*. Це звільняє програмістів від необхідності повторно прописувати одні й ті ж функції в кожній розроблюваній ними мережевій прикладній програмі. Самі сервіси прикладного рівня не є застосуваннями. *Прикладний рівень* надає програмістам *набір відкритих стандартних інтерфейсів прикладного програмування* (Application Programming Interface, API), які можна використовувати для виконання таких функцій мережевого застосування, як передача файлів, віддалена реєстрація та ін. У результаті модулі прикладних програм виходять меншими за розміром і потребують менше пам'яті.

Прикладний рівень для користувачів є найбільш помітною частиною моделі OSI, оскільки він відповідає за запуск програм, їх виконання, введення-виведення даних, адміністративне керування мережею. Протоколи взаємодії об'єктів сьомого рівня отримали назву прикладних.

Представницький рівень здійснює:

– інтерпретацію й перетворення даних, що передаються у мережу, до типу, зрозумілому прикладним процесам;

– забезпечує подання даних в узгоджених форматах і синтаксисі, трансляцію й інтерпретацію програм з різних мов, шифрування й стиснення даних.

Завдяки цьому мережа не обмежує використання різних типів ЕОМ як кінцевих систем. На практиці багато функцій цього рівня групуються з функціями прикладного рівня, тому протоколи представницького рівня не набули належного розвитку й не використовуються в багатьох мережах.

Сеансовий рівень забезпечує виконання функцій:

– керування сеансом зв'язку (сесією), орієнтованим на наскрізну передачу повідомлень, таких, наприклад, як встановлення й завершення сесії;

– керування черговістю й режимом передачі даних (*симплекс, дуплекс, напівдуплекс*);

– синхронізація;

– керування активністю сесії;

– складання звітів про надзвичайні ситуації.

У сесіях із встановленням логічного з'єднання запити встановлення й розриву з'єднання, а також запити передачі даних, пересилаються на розміщений нижче транспортний рівень.

Сеансовий рівень після сесії здійснює поступове, а не раптове завершення, виконує процедуру квитування (відправки службового повідомлення про завершення сеансу зв'язку), що дозволяє запобігти втраті даних у разі, коли одна зі сторін має намір перервати діалог, а інша – ні. Сесії надзвичайно корисні у випадках, коли між клієнтом і сервером в мережі існує

логічне з’єднання. Без встановлення логічного з’єднання сесія є неможливою. Однак, у цього правила є винятки, і деякі мережі підтримують передачу файлів без встановлення з’єднання. Навіть за таких умов сеансовий рівень передбачає виконання деяких корисних функцій для керування діалогом.

Сервіси сеансового рівня є додатковими і корисні лише для окремих застосувань, для більшості – їх наявність не є доцільною. Часто функції сеансового рівня реалізуються на транспортному рівні, тому протоколи сеансового рівня застосовуються обмежено.

Транспортний рівень виконує сегментування повідомлень і керування наскрізним, безпомилковим транспортуванням даних від джерела до споживача. Складність протоколів транспортного рівня зворотно пропорційна надійності сервісів нижчерозташованих рівнів (мережевого, канального й фізичного).

Функція сегментації полягає в розбитті довгих інформаційних повідомлень на блоки даних транспортного рівня – сегменти. Для невеликого за обсягом повідомлення сегмент асоціюється з його розміром.

У керуванні наскрізним транспортуванням даних транспортний рівень підтримує такі функції як:

– адресація; встановлення з’єднання;
– керування потоком даних;
– надання даним пріоритетів;
– виявлення та виправлення помилок;
– відновлення після збоїв, мультиплексування.

Протоколи транспортного рівня поділяються на два види:

– протоколи, орієнтовані на встановлення з’єднання;
– встановлення з’єднання.

Протоколи транспортного рівня без гарантії доставки набувають особливої популярності у випадках коли не потребується гарантована доставка повідомлень або не дозволяється повторення передачі повідомлень у якості метода контролю помилок. Це стосується застосувань, які працюють у реальному масштабі часу, такі як потокове відео або IP-телефонія.

Функція адресації на транспортному рівні, на відміну від адресації на мережевому і канальному рівнях, полягає в приєднанні додаткової унікальної адреси, яка ідентифікує прикладний процес, який здійснюється в кінцевій системі.

Більшість комп’ютерів здатні виконувати одночасно декілька процесів, підтримуючи одночасно роботу декількох застосувань. Однак на мережевому рівні кожен із них, як правило, асоціюється з одним місцем розташування – апаратною адресою порту комп’ютера призначення. Коли пакет (блок даних мережевого рівня) надходить до порту комп’ютера призначення, останньому необхідно знати, для якого процесу його призначено. Саме цю інформацію надає унікальна адреса транспортного рівня. Таким чином, *адреса транспортного рівня є логічною (відповідає програмному порту, пов'язаному з*

конкретним застосуванням), оскільки адресує процес, а не машину (на відміну від адрес канального і мережевого рівнів).

Функція встановлення й розриву з'єднання на запит сеансового рівня між рівноправними об'єктами транспортного рівня реалізується за допомогою процедури *тристороннього квитування*.

Ця процедура дозволяє мінімізувати ймовірність випадкового встановлення помилкового з'єднання, вимагаючи два підтвердження у відповідь на один запит з'єднання. З'єднання встановлюється тільки тоді, коли всі три події (запит, підтвердження отримання запиту, підтвердження отримання підтвердження) відбуваються в заданий часовий проміжок. Це дозволяє переконатися у тому, що обидва об'єкти транспортного рівня готові до сеансу зв'язку. Якщо дії процедури не вкладаються в заданий проміжок часу, наприклад, через затримку або пошкодження службових пакетів, процедура ініціюється заново.

Розрив з'єднання транспортного рівня також контролюється трістороннім квитуванням, що забезпечує його коректність. Розрив з'єднання відбувається окремо в прямому й зворотному напрямках, що виключає можливість втрати даних користувача у разі, коли одна зі сторін завершила передачу даних, а інша ще залишається активною.

Функція керування потоком даних полягає в узгодженні параметрів передачі під час процедури *тристороннього квитування*. Такими параметрами є:

– максимальний розмір сегменту даних для встановленого з'єднання;

– обсяг вільного простору буфера приймача, в якому розміщуватимуться доставлені сегменти;

– розмір групи сегментів, після отримання яких приймач повинен надсилати передавачеві підтвердження про прийом.

Підтвердження не тільки доводить безпомилковість отримання даних, але й визначає кількість наступних сегментів, прийом яких є можливим з урахуванням поточного завантаження приймального буфера.

Функція призначення пріоритетів даних є виключною прерогативою транспортного рівня. Нижчий мережевий рівень не знає про існування пріоритетного трафіку й усі пакети (блоки даних мережевого рівня) він сприймає однаковими.

Більшість протоколів транспортного рівня підтримують два пріоритети: *звичайні* дані та *термінові*. Запит на призначення пріоритету надходить від сеансового рівня. *Ідентифікатор призначеного пріоритету* розміщується в поле службової інформації транспортного рівня, що приєднуються до сегмента.

Для кожного з пріоритетів можуть бути організовані окремі буферні пули. *Алгоритм транспортування при цьому передбачає першочерговість обслуговування буфера термінових даних і тільки після його спустошення – буфера звичайних даних*.

Іншим підходом є групування сегментів термінових і звичайних даних в один блок з розміщенням в полі службової інформації граничного покажчика їх розташування.

Функція виявлення та виправлення помилок виконується багатьма протоколами канального рівня, однак, транспортний рівень її не дублює. Відмінність полягає в тому, що *канальний рівень виявляє й виправляє помилки двійкових розрядів, які виникають на фізичному рівні при передачі біт, а транспортний рівень ліквідує помилки, які виникають в результаті неправильної роботи мережевого рівня (втрата пакетів, несвоєчасна доставка пакетів та ін.).* Крім того у мережах, де канальний рівень не відповідає за виявлення й виправлення помилок у двійкових розрядах або цей рівень зовсім відсутній, транспортний рівень бере на себе ці функції.

Функція транспортного рівня з виявлення помилкових пакетів ґрунтується на впорядкуванні сегментів. Для цього кожному сегменту присвоюється порядковий номер, а в момент відправлення запускається власний таймер. Таймер працює до тих пір, поки не надійде підтвердження (позитивне або негативне) прийому пакета на приймальному кінці. У разі негативного підтвердження, передавач повторює передачу сегмента.

У деяких більш простих реалізаціях протоколів транспортного рівня позитивне підтвердження отримання останнього сегмента повідомлення сприймається як безпомилкове отримання всіх його сегментів. Отримання негативного підтвердження означає, що передавач повинен повторно передати сегменти від тієї точки (сегмента), де виникла помилка. Такий механізм називається передачею з поверненням до N.

Якщо час, відрахований таймером сегмента, закінчується, ініціюється процедура виявлення помилки.

Функція відновлення після збоїв забезпечує можливість відновлення втрачених даних у разі пошкоджень мережі таких, як вихід з ладу лінії зв’язку (як наслідок – втрата віртуального з’єднання), вихід з ладу обладнання мережевого вузла (як наслідок – втрата пакетів у середовищі без встановлення з’єднання) і, нарешті, вихід з ладу комп’ютера, якому адресовано дані.

Якщо вихід з ладу окремих компонентів мережі короткочасний, і швидко вдається встановити новий віртуальний канал або знайти маршрут, який оминає несправний вузол, транспортний рівень, аналізуючи порядкові номери сегментів, точно встановлює, які сегменти вже отримано і які слід передати повторно. При довготривалому пошкодженні мережі транспортний рівень може організувати транспортне сполучення в резервній мережі (якщо така передбачена).

У разі виходу з ладу комп’ютера-передавача або комп’ютера-приймача, робота транспортного рівня припиняється, тому що він функціонує під керуванням інстальованих у них операційних системах. Після відновлення функціональності комп’ютера транспортний рівень починає ініціювати розсилку широкомовних повідомлень усім комп’ютерам, які працюють у мережі, з метою виявлення того з них, який мав активне транспортне з’єднання

з пошкодженим. Таким чином, поновленому комп'ютеру вдається відновити перерване з'єднання за допомогою інформації, збереженої в справних машинах.

Функція мультиплексування дозволяє в одному мережевому з'єднані організувати кілька з'єднань транспортного рівня. *Адреса транспортного рівня дозволяє транспортному* рівню розрізняти сегменти, адресовані різним прикладним процесам. Перевагою такого мультиплексування є зменшення собівартості транспортування даних у мережі. Проте воно є доцільним тільки в режимі роботи мережі, орієнтованій на встановлення з'єднання (віртуального каналу).

Особливостях роботи транспортного рівня в режимі без встановлення з'єднання, який використовується, коли гарантувати наскрізну доставку даних не потрібно:

– процеси обміну даними в реальному масштабі часу (аудіо- або відео-процеси), для яких доставка без затримки є значно важливішою ніж достовірність, яка досягається за рахунок повторних передач сегментів;

– більш ефективне використання мережі, не займаючи її пропускну здатність величезною кількістю службової інформації;

– актуальність функції адресації транспортного рівня, яка забезпечує підтримку декількох одночасно працюючих прикладних процесів на одній машині, що є неможливим без сервісів транспортного рівня.

Мережевий рівень виконує головну телекомунікаційну функцію – забезпечення зв'язку між кінцевими системами мережі. Цей зв'язок реалізовано шляхом надання наскрізного каналу, який комутований з окремими ділянками відповідно до оптимально обраного маршруту, логічного віртуального каналу або безпосередньої маршрутизації блоку даних у процесі його доставки. При цьому мережевий рівень звільняє вищі рівні від знань про те, через які ділянки мережі або через які мережі проходить маршрут передачі інформації. Якщо вищі рівні (прикладний, представницький, сеансовий і транспортний), зазвичай обов'язкові в кінцевих системах, які взаємодіють через мережу, три нижніх рівні (мережевий, канальний та фізичний) є необхідними також для всіх проміжних мережевих пристроїв, розташованих у транзитних пунктах маршруту передачі даних.

Основною *функцією мережевого рівня є маршрутизація*. Вона полягає в прийнятті рішення, через які конкретно проміжні пункти повинен пройти маршрут передавання даних, які направляються з однієї кінцевої системи в іншу, та як має виконуватися комутація (яка відповідає конкретному маршруту) між входами та виходами мережевих пристроїв, розташованих у проміжних пунктах мережі.

Блоки даних, з якими оперує мережевий рівень, називаються пакетами. Пакет утворюється шляхом додавання до сегмента, переданого з транспортного рівня, заголовка, який містить *адресу мережевого рівня*, яка складається з двох частин і ідентифікує як адресу мережі кінцевого користувача, так і самого користувача в ній.

Мережі з різними мережевими адресами з'єднуються між собою маршрутизаторами. Для того, щоб передати пакет від відправника, який знаходиться в одній мережі, до одержувача з іншої мережі, необхідно зробити кілька транзитних «стрибків» – *хопові* (hops) між мережами, вибираючи щоразу найоптимальніший за часом проходження або надійністю маршрут.

Мережевий рівень вирішує також завдання взаємодії мереж з різними технологіями та створення захисних бар'єрів на шляху небажаного трафіку між мережами.

На мережевому рівні використовуються два види протоколів:

– власне мережеві протоколи, які забезпечують просування пакетів через мережу (асоціюють з протоколами мережевого рівня);

– протоколи маршрутизації, які займаються обмобміном маршрутною інформацією, за допомогою яких маршрутизатори збирають інформацію про топологію міжмережевих з'єднань.

Протоколи мережевого рівня виконуються модулями операційної системи, а також програмними й апаратними засобами маршрутизаторів.

На мережевому рівні можуть також працювати протоколи відображення адреси призначення мережевого рівня на адресу канального рівня мережі, де знаходиться кінцевий користувач.

Канальний рівень відповідає за якісну передачу даних між двома пунктами, пов'язаними фізичним каналом з урахуванням особливостей середовища-передавача.

Термін «*передача даних*», на відміну від терміна «переносу інформації» підкреслює саме цей аспект діяльності канального рівня. Якщо з'єднання встановлюється між двома кінцевими системами, не пов'язаними безпосередньо, то воно буде включати декілька незалежно функціонуючих фізичних каналів передачі даних. При цьому фізичні середовища передачі можуть відрізнятися (мідь, оптичне волокно, ефір). Несумісними можуть виявитися й вимоги до формату подання даних у кожному каналі, що називається *лінійним кодуванням.* У цій ситуації канальний рівень бере на себе функції адаптації даних до типу фізичного каналу зв'язку, надаючи вищерозташованим рівням «прозоре з'єднання».

Блок даних на канальному рівні називається *кадром* або *фреймом*. Пакети мережевого рівня, об'єднані в кадр, обрамляються розділовими прапорами (спеціальними послідовностями біт, розміщеними на початку та в кінці блоку пакетів). Крім того, до кадру додається контрольна сума, з використанням якої здійснюється перевірка правильності переданого каналом кадру. У разі виявлення невиправної помилки, приймач надсилає запит до передавача про повторну передачу кадру.

Теорія передачі даних і теорія кодування досить добре розроблені, що дозволяє забезпечити високу ефективність роботи протоколів канального рівня. Необхідно відзначити, що функція виправлення бітових помилок не завжди є обов'язковою для канального рівня, тому в деяких протоколах канального рівня вона відсутня. Іноді в глобальних мережах функції канального рівня

виокремити важко, оскільки в одному й тому ж протоколі вони об'єднуються з функціями мережевого рівня.

Важливими функціями канального рівня є керування доступом до каналу з зв'язку, синхронізація кадрів, керування потоком даних, адресація, встановлення з'єднання й роз'єднання.

Керування доступом до каналу визначається:

– типом фізичного каналу, який з'єднує станції;

– кількістю під'єднаних до нього станцій.

Тип каналу визначається:

– режимом його роботи (дуплексний, напівдуплексний);

– конфігурацією (двоточковою – тільки дві станції, багатоточковою – три і більше станцій.

Керування доступом є актуальним у напівдуплексному режимі роботи каналу з багатоточковою конфігурацією, коли станціям необхідно очікувати момент початку своєї передачі даних.

Синхронізація кадрів забезпечує приймач можливістю точного визначення початку й кінця кадру. Для передачі даних визначено два методи:

– асинхронна передача, орієнтована на символи (зазвичай 8-бітний символ), означає, що передача кожного символу попереджається стартовим бітом і закінчується стоповим бітом;

– синхронна передача, орієнтована на кадри, в якій використовуються прапори початку і кінця кадру як синхронізуючі послідовності.

Керування потоком даних полягає в наданні приймачу можливості повідомляти передавач про свою готовність або неготовність до приймання кадрів. Суть полягає в тому, що виникає запобігання такій ситуації, коли передавач завалює приймач кадрами, які той не в змозі обробити.

Адресація є потрібною при багатоточковій конфігурації каналу з більш ніж двома станціями, щоб ідентифікувати одержувача.

Адреси канального рівня називаються *апаратними*. Поле адреси містить адресу призначення та адресу джерела.

Встановлення та роз'єднання з'єднання – це процедура активації та дезактивації з'єднання на канальному рівні, яка виконується програмним забезпеченням. При цьому станція передачі ініціює з'єднання надсиланням адресату спеціальної команди «старт», а станція приймання підтверджує з'єднання, після чого починається передавання даних. Ця процедура здійснюється також після збоїв і перезапуску програмного забезпечення канального рівня. Є також команда «стоп», яка зупиняє роботу програмного забезпечення.

Фізичний рівень відповідає за розміщення біт інформації у фізичному середовищі. На фізичному рівні можуть використовуватися такі типи середовищ:

– кабель «вита пара»;

– коаксіальний кабель;

– оптичне волокно;

– територіальний цифровий канал;
– ефір.

Основними характеристиками фізичних середовищ передачі є такі параметри:
– смуга пропускання;
– перешкодозахищеність;
– хвильовий опір та ін.

Тут реалізуються фізичні інтерфейси пристроїв з передавальним середовищем та пристроями, між якими виконується передавання бітів.

Основні *характеристики фізичного рівня* можна об'єднати в такі групи.

Механічні. Це характеристики, пов'язані з фізичними властивостями інтерфейсу з передавальним середовищем, тобто роз'ємами, які забезпечують з'єднання пристрою з одним або кількома провідниками. Типи роз'ємів і призначення кожного контакту зазвичай стандартизуються.

Електричні. Визначають вимоги до подання бітів, які передаються в фізичне середовище, наприклад, рівень струму або напруги переданих сигналів, крутизна фронтів імпульсів, типи лінійних кодів, швидкість передачі сигналів.

Функціональні. Визначають функції окремих каналів фізичних інтерфейсів пристроїв, які взаємодіють через передавальне середовище.

Основними схемами взаємодії пристроїв на фізичному рівні є:
– симплексний зв'язок (однобічний);
– дуплексний зв'язок (двобічний, одночасний);
– напівдуплексний зв'язок (почерговий).

При цьому можуть бути реалізовані два варіанти організації зв'язку:
– *«точка-точка»;*
– *«точка-багато точок»*.

У першому варіанті два пристрої розділяють один зв'язок, який, може бути симплексним, напівдуплексним або дуплексним.

У другому варіанті передбачається, що передані дані одним пристроєм приймаються багатьма пристроями. Як правило, такі зв'язки є симплексними (кабельне телебачення) або напівдуплексними (локальна мережа на базі стандарту Ethernet).

В окремих випадках можуть використовуватися також дуплексні зв'язки (мережа на базі технології SONET). Можуть застосовуватися також інші топології фізичного рівня, такі, як шина, зірка, кільце, проте всі вони є варіаціями вже відомих «точка-точка» і «точка-багато точок». Так топологія шина є типовим варіантом «точка-багато точок», топологія зірка – набором зв'язків «точка-точка», топологія кільце – набір колоподібних зв'язків «точка-точка».

Процедурні. Встановлюють правила, за допомогою яких відбувається обмін потоками бітів через фізичне середовище.

Це схеми роботи послідовного та паралельного інтерфейсів. У першому випадку між взаємодіючими пристроями існує тільки один канал зв'язку, яким біти передаються один за одним. Це призводить до обмеження швидкості

передачі й, отже, повільної роботи інтерфейсу. У другому випадку кілька бітів передаються між взаємодіючими пристроями одночасно декількома каналами. Швидкість передачі при цьому зростає.

4.2 Принцип інкапсуляції даних в моделі 0SI/IS0

Підготовка даних, отриманих на прикладному рівні, для транспортування по мережі зв'язку відповідно до протоколів стека OSI ґрунтується на концепції інкапсуляції.

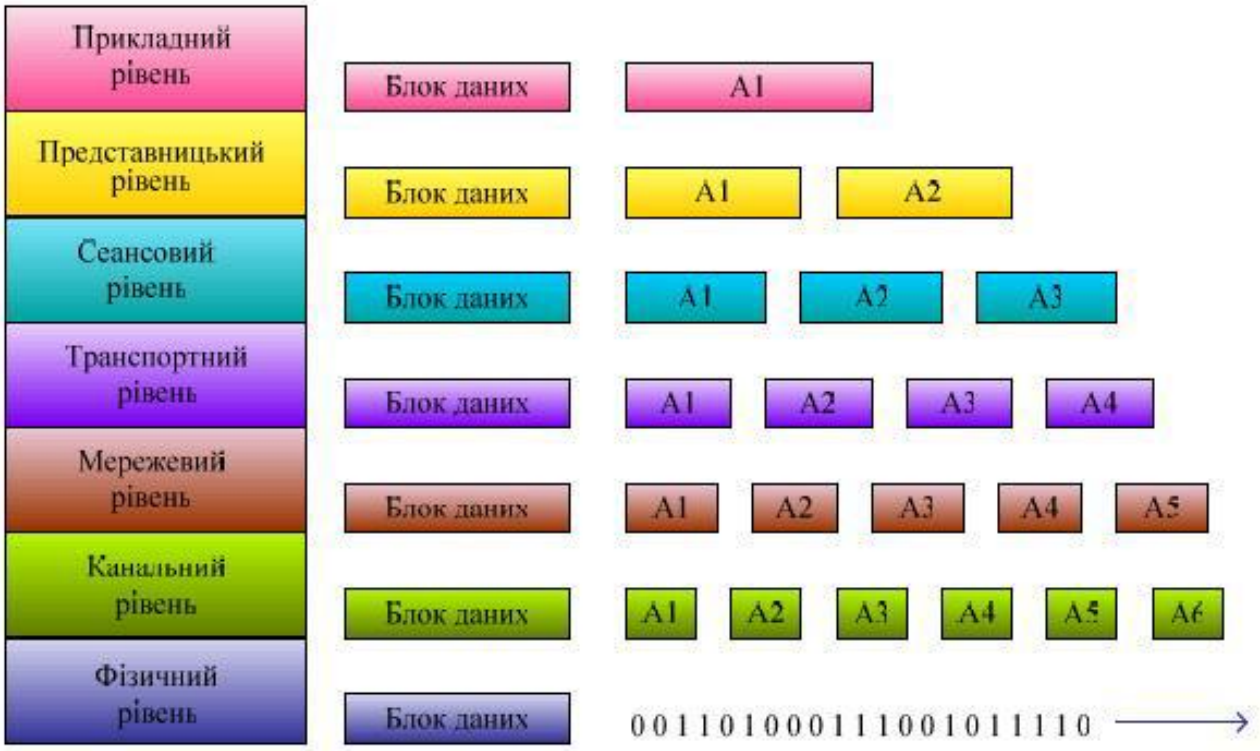


Рисунок 27 – Інкапсуляція даних при проходженні вниз по стеку OSI

A1 – заголовок прикладного рівня
A2 – заголовок представницького рівня
A3 – заголовок сеансового рівня
A4 – заголовок транспортного рівня
A5 – заголовок мережевого рівня
A6 – заголовок канального рівня

Механізм інкапсуляції – це спосіб пакування даних у форматі одного протоколу в формат іншого протоколу, що в даному випадку відповідає послідовному додаванню до даних відповідної службової інформації на кожному рівні стека (рис. 27). У результаті кожний рівень отримує дані від вищого рівня, поміщені в оболонку. Оболонка не відкривається й не зчитується нижчим рівнем, який, у свою чергу, доповнює зовні оболонку своєю

службовою інформацією, яка призначена аналогічному рівню в системі приймання.

Блок інформації, який надходить з вищого рівня на нижчий, завжди має стандартний формат: *заголовок, службова інформація, дані, кінцевик*. При цьому заголовок вищого рівня сприймається нижчерозміщеним як передані дані.

4.3 Промисловий стандарт стека протоколів TCP/IP

Transmission Control/Internet Protocol) (TCP/IP) – це промисловий стандарт стека протоколів, розроблений для глобальних мереж. У протоколі TCP/SH (Transmission Control/Internet Protocol) фіксується механізм того, як передається інформація з датчика особі, яка її приймає (або кільком особам). Для стаціонарних мереж це включає, наприклад, PSTN та ISDN (цифрова мережа інтегрованих послуг). Мережі та послуги комутації пакетів включають в себе, наприклад, GPRS, UMTS (Універсальну систему мобільних телекомунікацій), xDSL, TETRA (Транс'європейський стандарт радіозв'язку з автоматичним розподілом каналів), послуги електронної пошти та інші послуги Інтернет зв'язку.

Стандарти TCP/IP опубліковано в серії документів, названих *Request For Comment (RFC)*.[20] Документи RFC описують внутрішню роботу Інтернету. На рис. 28 наведено структуру стека TCP/IP у співвідношенні з рівнями моделі OSI. Праворуч на рис.25 вказано засоби реалізації різних рівнів.

Протоколи стека TCP/IP поділяються на п'ять рівнів.

Найнижчий – *фізичний рівень* – відповідає фізичному рівню моделі OSI. Цей рівень у стеку TCP/IP спеціально не стандартизовано, а тому допускає використання всіх основних стандартів фізичного рівня, які визначають характеристики передавального середовища, швидкості передачі сигналів та схеми кодування сигналів.

Рівень доступу до мережі, пов'язаний з логічним інтерфейсом між кінцевої системою і мережею, є також нерегламентованим. Наприклад, для з'єднання комп'ютера з мережею може використовуватися будь-який стандарт канального рівня: PPP, Ethernet, ATM і та ін.

Міжмережевий рівень забезпечує функцію маршрутизації при передачі даних від одного хосту до іншого через вузли однієї або декількох логічних мереж.

Основний протокол цього рівня – це *протокол IP* (Internet Protokol), який підтримується усіма кінцевими системами (хостами) й мережевими комунікаційними пристроями, котрі здійснюють функцію маршрутизації.

[20] Документи RFC описують внутрішню роботу Інтернету. Деякі RFC описують мережеві сервіси або протоколи та їх реалізацію, водночас інші узагальнюють умови застосування. Слід зазначити, що стандарти TCP/IP завжди публікуються у вигляді документів, але не всі RFC можна вважати стандартами. Деякі RFC з часом набувають статусу офіційних міжнародних стандартів після їх затвердження організацією зі стандартизації 0SI або ITU-T.

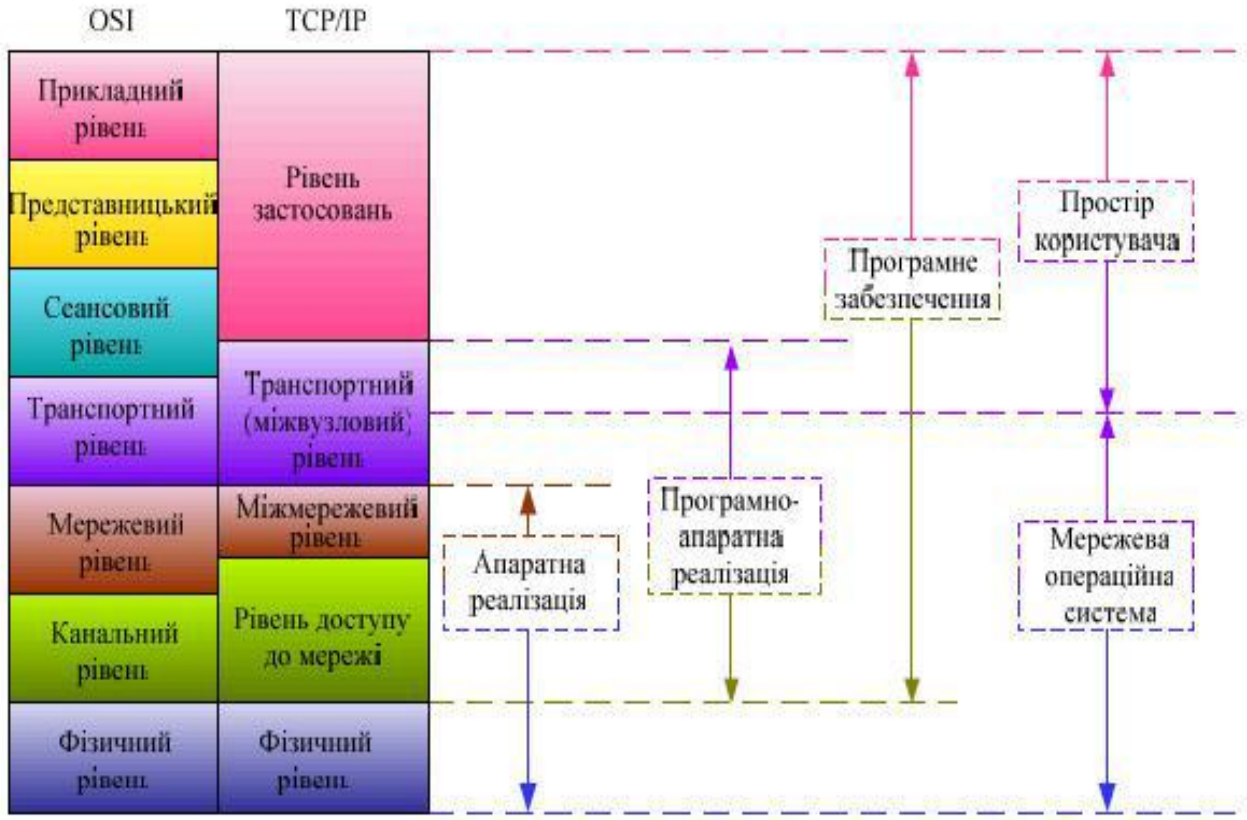


Рисунок 28 – Порівняння архітектур TCP/IP і OSI за засобами реалізації різних

До допоміжних протоколів цього рівня належать такі:

– ICMP (Internet Control Message Protokol) – *протокол керування повідомленнями Інтернет*, забезпечує можливість шлюзів та маршрутизаторів обмінюватися службовими повідомленнями з хостом-відправником у разі виникнення проблемної ситуації при передачі в мережі;

– IGMP (Internet Group Management Protokol) – *протокол керування групами*, надає великій кількості хостів і маршрутизаторів можливість обмінюватися повідомленнями з груповими адресами в широкомовному режимі;

– OSPF (Open Shortest Pash First) – *протокол визначення першого найкоротшого маршруту* при встановленні віртуального (логічного) з'єднання OSI/ISO в інтермережі;

– BGP (Border Gateway Protokol) – *протокол регламентує процедуру маршрутизації* між граничними шлюзами в Інтернет;

– RSVP (ReSerVation Protokol) – *протокол резервування комунікаційних ресурсів* (смуги пропускання ліній зв'язку) з метою надання необхідної якості обслуговування, підтримується хостами й мережевими комунікаційними пристроями;

– RIP (Pouting Protokol) – *протокол збору маршрутної інформації* при топологічних змінах у інтермережі;

– ARP (Address Resolution) – *протокол розв'язування адресів* (встановлює співвідношення між IP-адресом і фізичним адресом вузла).

Транспортний рівень відповідає за *виконання функції наскрізної передачі даних* і тому реалізується лише в кінцевих системах. Протоколи цього рівня приховують від рівня застосувань подробиці про мережу або мережі, якими транспортуються дані. На цьому рівні виконуються два основні протоколи:

– TCP (Transmission Control Protokol) – *протокол керування передачею*, орієнтований на логічне з'єднання та послідовну передачу блоків даних, котрий містить механізми забезпечення надійності, які дозволяють відстежувати блоки даних і тим самим гарантувати їх коректну доставку застосування адресантові;

– UDP (Ustr Datagram Protokol) – *протокол датаграм користувачів*, який забезпечує швидку, але ненадійну передачу блоків даних, які самостійно переміщуються мережею без встановлення логічного з'єднання.

Рівень застосувань забезпечує зв'язок між прикладними процесами та застосуваннями взаємодіючих хостів.

Основні протоколи цього рівня:

– FTP (File Transfer Protokol) – *протокол передачі файлів*;

– HTTP (Hyper Text Transfer Protokol) – *протокол передачі гіпертекстових файлів;*

– SMTP (Simple Mail Transfer Protokol) – *простий протокол передачі пошти;*

– TELNET – *протокол видаленого входу в систему;*

– SNMP (Simple Network Management Protokol) – *простий протокол мережевого керування;*

– DNS (Domain Name System) – служба імен доменів або прикладний сервіс в Інтернет-мережі, який дозволяє хостам перетворювати Інтернет-імена в IP-адреси;

– MIME (Multipurpose Internet Mail Extensions) – *багатоцільові розширення Інтернет-пошти*, які підтримують обмін мультимедійними повідомленнями, визначаючи процедури, які дозволяють користувачеві приєднувати до повідомлення електронної пошти файли різних форматів (тексти, зображення, аудіо, відео та цілі програмні застосування).

На рівні застосувань працюють також багато навігаційних програм (Google, Gopher, Wais, WWW), які забезпечують пошук потрібної інформації в мережі.

4.4 Переваги та недоліки моделі ISO/OSI і TCP/IP

Переваги моделі OSI

Модель OSI сьогодні є еталонною багаторівневою моделлю архітектури зв'язку інформаційних мереж і основою для розробки стандартів нових протоколів.

Модель ISO/OSI дозволяє визначити межі телекомунікаційної та інформаційної мереж у загальній архітектурі зв'язку, а саме:

– фізичний, канальний, мережевий і транспортний рівні відображають принцип роботи телекомунікаційної мережі;

– сеансовий, представницький і прикладний – інформаційної мережі.

Чітке *визначення інтерфейсів за рівнями дозволяє заміняти один протокол рівня на інший без зміни стандартів протоколів суміжних рівнів.* У цьому полягає *основна цінність моделі OSI*.

Модель ISO/OSI є корисною для теоретичних досліджень і розробок нових мереж, хоча протоколи OSI не отримали широкого розповсюдження.

Недоліки моделі OSI

За архітектурою OSI закріпився статус приписної моделі. Це відбулося, по-перше через несвоєчасність появи стандартних протоколів OSI (до моменту їхньої появи розповсюдилися конкуруючі з ними протоколи стеку TCP/IP), а по-друге – через складність і недосконаліть моделі (представницький і сеансовий рівні порожні, а мережевий і канальний – перевантажені).

Переваги моделі TCP/IP

Стек TCP/IP є лідером, що пояснюється такими його властивостями:

– це найбільш апробований, і у той же час популярний стек протоколів, який став стандартом де-факто;

– майже всі існуючі великомасштабні мережі функціонують на основі стека TCP/IP;

– це основний спосіб отримання доступу в Інтернет;

– усі сучасні операційні системи підтримують стек TCP/IP;

– стек TCP/IP знайшов застосування при створенні корпоративних мереж, які використовують транспортні послуги Інтернету і гіпертекстову технологію;

– стек TCP/IP є основою гнучкої технології для поєднання різнорідних систем і мереж, як на рівні реалізації транспортної функції, так і на рівні взаємодії прикладних процесів;

– стек TCP/IP забезпечує добре масштабоване середовище для застосувань клієнт-сервер.

Недоліки моделі TCP/IP

Моделі TCP/IP та її протокол не позбавлені певних недоліків:

– відсутність розмежувань концептуальних понять інтерфейсу, протоколу та рівневого сервісу, що досить чітко зроблено в моделі ISO/OSI. Внаслідок цього модель TCP/IP не може застосовуватися для розробки нових мереж;

– за допомогою моделі TCP/IP неможливо описати жоден інший стек протоколів, окрім TCP/IP;

– у моделі не диференційовано фізичний та канальний рівні, хоча вони абсолютно різні, що в коректній моделі обов'язково враховується;

– найбільш ретельно продумано й опрацьовано протоколи IP і TCP;

– стек TCP/IP не може розглядатися як повноцінна модель, однак самі протоколи добре апробовані та надзвичайно популярні.

Висновки

Використання відкритих специфікацій (стандартів) дозволяє випускати сумісні між собою мережеві компоненти, а мережевим операторам створювати мережі з продуктів різних виробників і забезпечувати сумісність своїх мереж з мережами інших операторів. Відкритий характер стандартів є важливим:

– для пристроїв і програм, які випускаються для побудови мереж;

– для комунікаційних протоколів.

Отже, дотримання відкритих стандартів надає такі переваги:

можливість побудови мереж з апаратних і програмних засобів різних виробників;

– безпроблемну заміну одних компонентів мережі іншими, більш

– досконалими, що дозволяє забезпечити розвиток мережі з мінімальними

– витратами;

– вільне сполучення однієї мережі з іншою.

У результаті конвергенції мереж та об’єднання інформаційних потоків різних служб у спільний передавальний потік гетерогенного трафіку, виникає необхідність ідентифікації його змісту.

ЛЕКЦІЯ 5. ПРИНЦИПИ ПОБУДОВИ ТЕЛЕКОМУНІКАЦІЙ

План

Вступ

1. Сегментний підхід в побудові мереж.

2. Виокремлення сегментів за масштабом охоплюваної території, на основі декомпозиції транспортної функції, за технологічною ознакою.

3. Побудова сегментів.

4. Узагальнені характеристики сегментів.

5. Поєднання сегментів мережі.

Висновки

Література

1. Теоретичні основи телекомунікаційних мереж : навч. посіб. /М.М. Климаш, Б.М.Стрихалюк, М.В.Кайдан. – Львів : вид-во УАД, 2011. – 496 с.

2. Буров Є. Комп’ютерні мережі / Є.Буров. – Львів : БаК, 1999. – 468 с.

3. Управління телекомунікаціями із застосуванням новітніх технологій / Кривуца В. Г., Беркман Л. Н., Стеклов В. К. та ін.]. – К.: Техніка, 2007. – 384 с.

Вступ

Принципи побудови телекомунікаційної мережі як складного об’єкта базуються на способах її декомпозиції. Цей процес полягає у виділенні в мережі відносно незалежних структурних фрагментів, так званих сегментів. Будь-який сегмент глобальної мережі можна розглядати як самостійну мережу більш низького рівня.

Сегментний підхід слід розглядати не стільки як спосіб декомпозиції мережі, скільки як спосіб її синтезу (що нагадує принцип «дитячого конструктора»), метою якого є визначення принципів утворення сегментів і правил поєднання сегментів між собою. Основним завданням сегментації слід вважати максимізацію частки трафіку, який замикається всередині сегментів, та мінімізацію тієї його частини, яка циркулює між сегментами.

5.1 Сегментний підхід в побудові мереж

5.1.1 Виокремлення сегментів за масштабом охоплюваної території

Виокремлення сегментів за масштабно-територіальною ознакою представлено ієрархією, наведеною на рис. 29. До виділеного сегмента можна вжити термін «мережа», який не суперечить загальноприйнятій термінології, а для повноти ієрархії логічно ввести поняття глобальної мережі.

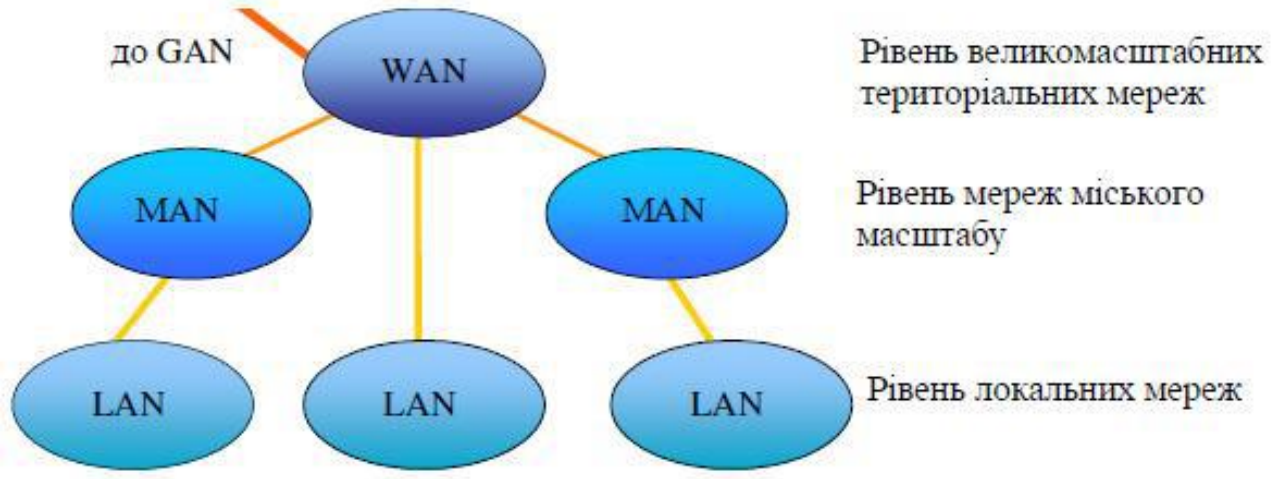


Рисунок 29 – Ієрархія мереж

Глобальна мережа (Global Area Network, GAN) – це загальнопланетарна мережа, яка об’єднує всі країни та континенти, забезпечує доступ користувачів мережі в будь-якій точці земної кулі.

Великомасштабна територіальна мережа (Wide Area Network, WAN) – сегмент, призначений для об’єднання мереж міського масштабу або сільських

районів, розташованих на території великого регіону, держави, континенту, а також на різних континентах.

Мережа мегаполісу (Metropolitan Area Network, MAN) – сегмент, що охоплює територію міста, сільського району, області або регіону.

Локальна мережа (Local Area Network, LAN) – сегмент, у якому основна частина трафіку замикається всередині невеликої території, установи, промислового підприємства і т. п. Сегментами типу LAN також є мережі, утворені поєднанням декількох локальних мереж, розташованих на невеликій відстані один від одного (мережі кампусів).

Класифікація сегментів за масштабно-територіальною ознакою представляє інтерес при *декомпозиції задач синтезу мережі.*

Телекомунікаційні технології, які в них застосовуються, суттєво відрізняються один від одного. Зважаючи на відмінність технологій локальних і глобальних мереж, неважко зрозуміти, чому до недавнього часу локальні й територіальні мережі обслуговувалися різними фахівцями.

В умовах тенденції до зближення локальних і територіальних мереж (конвергенції мереж), а також конвергенції технологій, що застосовуються, ситуація суттєво змінилась. Сьогодні виділення будь-яких сегментів розглядається як фрагментація єдиної глобальної мережі.

5.1.2 Виокремлення сегментів на основі декомпозиції транспортної функції

Основне призначення телекомунікаційної мережі – це реалізація транспортної функції, тобто перенесення інформації, поданої у формі сигналу з кінця в кінець між інтерфейсами мережі.

Мережева активність при транспортуванні інформації різними ділянками телекомунікаційної мережі визначаються інтенсивністю створеного в них мережевого трафіку.

Принцип розподілу інтенсивності трафіку на різних ділянках телекомунікаційної мережі може бути основою декомпозиції транспортної функції. Така декомпозиція передбачає виділення трьох типів сегментів, які вирішують відносно самостійні функціональні підзавдання, а саме: транспортні мережі, мережі доступу і розподільчі мережі.

Транспортна мережа – це сегмент з високим ступенем концентрації трафіку, за допомогою якого здійснюється інформаційний обмін між сегментами з більш повільним трафіком і в якому транспортне середовище для передавання будь-якого типу інформації забезпечується використанням єдиних технологічних принципів і встановлених стандартів з надання ширини смуги пропускання (рис. 30).

Мережею доступу називається сегмент телекомунікаційної мережі, в якому формуються інформаційні потоки, спрямовані в транспортну мережу.

З'єднання мереж доступу з транспортною мережею здійснюється у вузлах доступу до транспортної мережі.

Мережі доступу узагальнено поділяються на:

– мережі проводового доступу;

– стаціонарні мережі безпроводового доступу;

– мережі мобільного доступу.

Мережа доступу з боку користувача має пристрій мережевого закінчення, який ще називається просто *мережевим закінченням*, а на іншому кінці – *інтерфейс вузла доступу до транспортної мережі*.

Ділянка мережі між мережевим закінченням NT, до якого під'єднаний термінальний пристрій користувача, й інтерфейсом сервісного вузла, де абоненту надається необхідна послуга, визначається *терміном мережа абонентського доступу.*

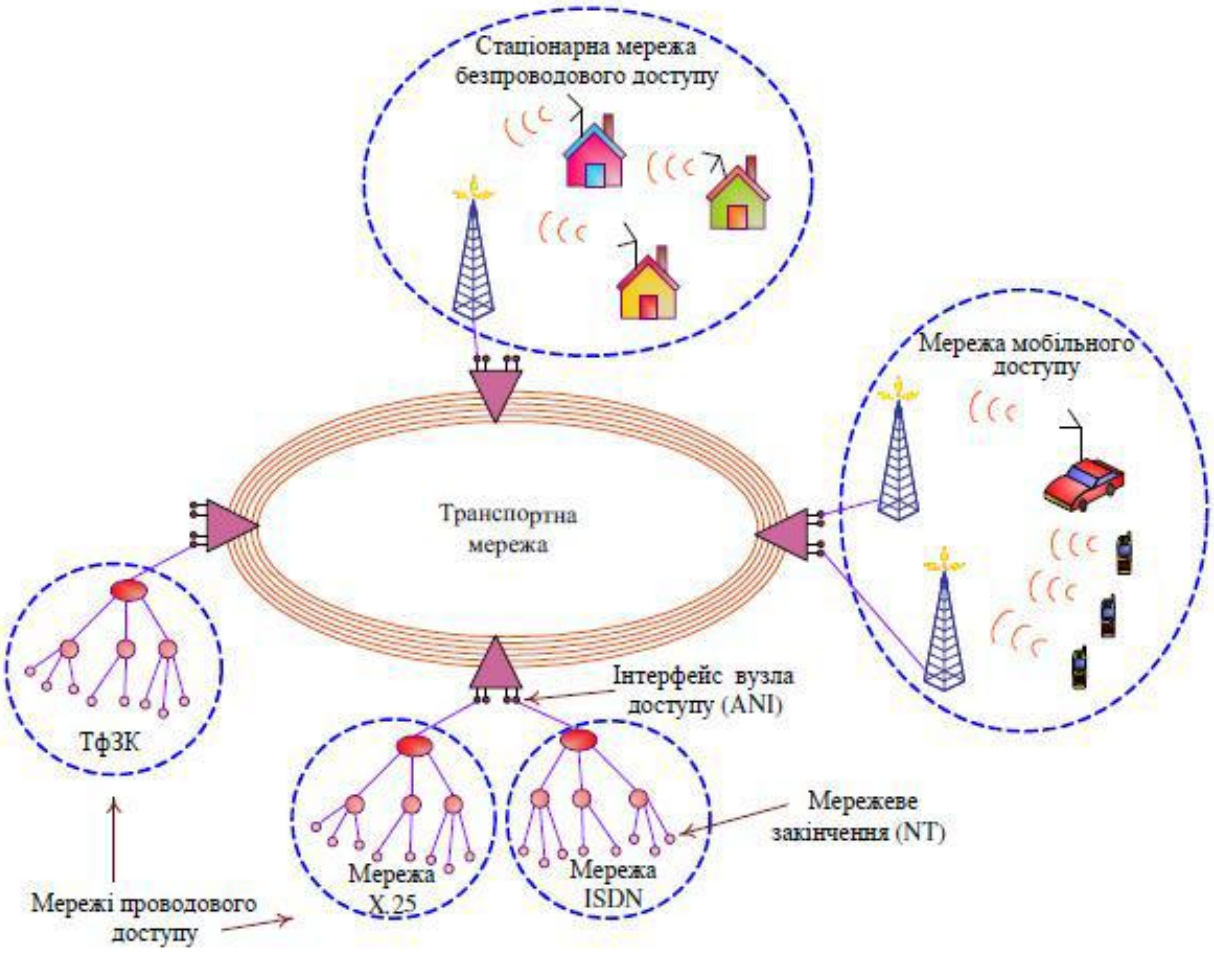


Рисунок 30 – Транспортна мережа та мережі доступу

Мережею доступу називається сегмент телекомунікаційної мережі, в якому формуються інформаційні потоки, спрямовані в транспортну мережу. З'єднання мереж доступу з транспортною мережею здійснюється у вузлах доступу до транспортної мережі. Мережі доступу узагальнено поділяються на:

– мережі проводового доступу;
– стаціонарні мережі безпроводового доступу;
– мережі мобільного доступу.

Мережа доступу з боку користувача має пристрій мережевого закінчення, який ще називається просто мережевим закінченням, а на іншому кінці – *інтерфейс вузла доступу до транспортної мережі*.

Ділянка мережі між мережевим закінченням NT, до якого під'єднаний термінальний пристрій користувача, й інтерфейсом сервісного вузла, де абоненту надається необхідна послуга, визначається терміном *мережа абонентського доступу.*

Мережі доступу, у загальному випадку, мають багаторівневу архітектуру, що включає вузли рівнів доступу, розподілу і ядра.

Опорні вузли мереж абонентського доступу формують рівень доступу.

Вузли рівня розподілу забезпечують агрегацію інформаційних потоків, що надходять від опорних вузлів абонентського доступу, і магістралями направляють агреговані потоки у вузли доступу до транспортної мережі.

У вузлі доступу до транспортної мережі відбувається концентрація всіх інформаційних потоків від приєднаних вузлів рівня розподілу. Вузол доступу до транспортної мережі, таким чином, переміщується на рівень ядра в мережі доступу. Якщо територіальна протяжність є значною, мережа доступу може розглядатися як самостійний сегмент MAN.

Розподільчою мережею називають сегмент телекомунікаційної мережі, за допомогою якого концентрований потік, який надходить з транспортної мережі, перерозподіляється та надходить до споживачів.

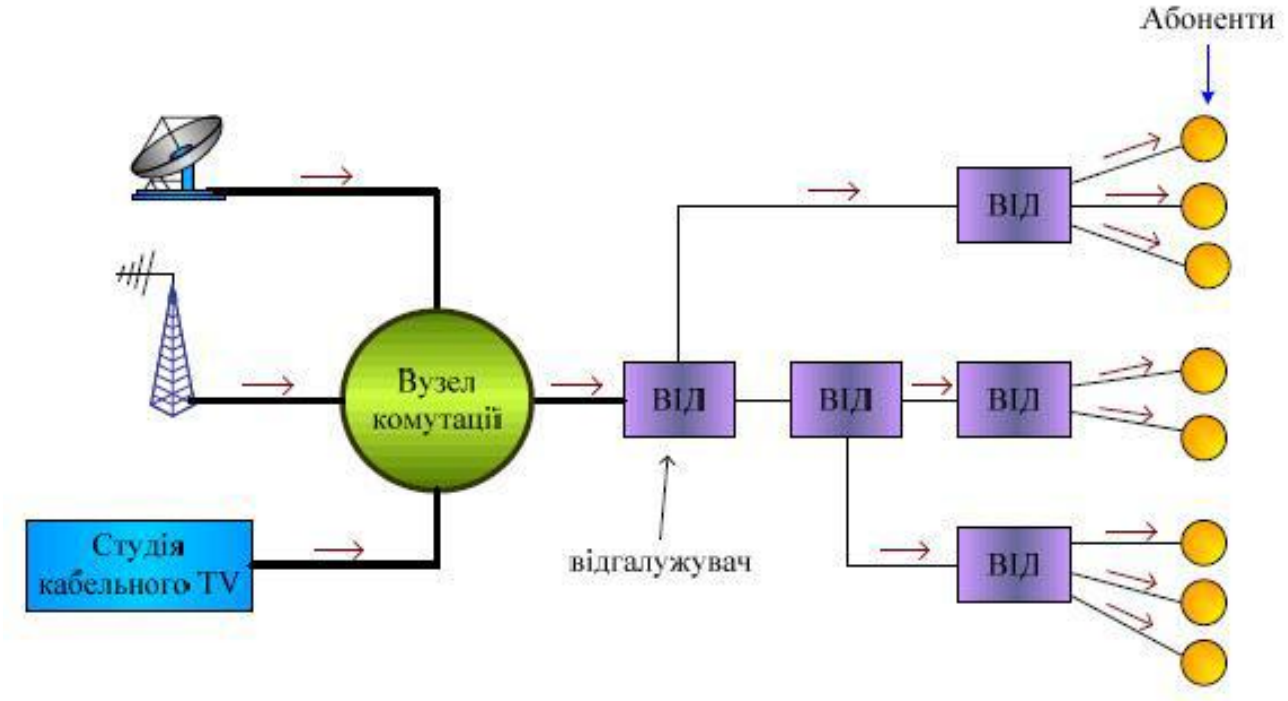


Рисунок 31 – Розподільча мережа

На практиці функції мережі доступу та розподільчої мережі часто поєднуються в одному сегменті. Класичним прикладом власне розподільчої мережі є тільки мережа оператора кабельного телебачення (рис. 31).

5.2 Виокремлення сегментів за технологічною ознакою

Телекомунікаційну мережу розглядають як сукупність сегментів, різниця між якими зумовлена телекомунікаційними технологіями, що застосуються в них. Причому розміри таких сегментів можуть досягати масштабів LAN, WAN, MAN мереж.

Визначаючи сегменти за ознаками телекомунікаційної технології, вживають поняття, яке пов'язано з назвою відповідного технологічного стандарту або протоколу, наприклад, «мережа ATM», «IP-мережа» та ін.

Принцип технологічної однорідності дозволяє виокремлення сегментів, до яких вживається термін *хмара*.

Хмара – це територіальна телекомунікаційна мережа з *однорідними зовнішніми інтерфейсами*, внутрішня будова якої при організації через неї транспортування інформаційних потоків не деталізується і не розглядається.

Цей термін вживається в контексті опису схем взаємодії двох і більше віддалених локальних мереж через телекомунікаційні мережі операторів. Прикладом цього є корпоративна мережа, в якій мережі центральної штаб-квартири та філій об'єднуються за допомогою зовнішніх телекомунікацій.

5.3 Побудова сегментів

5.3.1 Побудова сегментів фізичного рівня

Сегмент фізичного рівня розглядається як сукупність пунктів і ліній, які їх з'єднують, що утворює відносно незалежний структурний фрагмент мережі.

З'єднаність усіх пунктів у сегменті на фізичному рівні досягається використанням *окремих ліній зв'язку* для кожної пари кінцевих пунктів (повнозв'язна топологія «кожен з кожним»), спільним комунікаційним середовищем або вузлоутворенням.

Повнозв'язна топологія

Використання в сегменті топологій «точка-точка» для зв'язку всіх пар кінцевих пунктів не завжди є економічно доцільним. Проте саме в такому сегменті досягається максимальна надійність, а це виправдовує використання дорогих топологій у сегментах з високим ступенем концентрації трафіку (магістральних мережах).

Спільне комунікаційне середовище – це фізичне середовище передачі, в якому з'єднаність кінцевих пунктів забезпечується принципом «точка-багато точок» (шинна топологія).

Пари пунктів можуть взаємодіяти у спільному середовищі, не заважаючи одна одній, тільки почергово, тому що спільне комунікаційне середовище є єдиним приладом, який обслуговує запити на обмін інформацією різних кореспондуючих пар пунктів.

Сегменти, побудовані на базі спільного середовища передачі, мають такі недоліки:

– дефіцит пропускної здатності та зниження продуктивності сегмента при збільшенні кількості під'єднаних кінцевих пунктів;

– обмеження фізичної довжини сегмента, обумовлене загасанням сигналів у фізичному середовищі передачі.

Оскільки спільне комунікаційне середовище як єдиний канал зв'язку в одному часовому інтервалі може використовуватися тільки однією взаємодіючою парою пунктів, його ще називають *розподільчим середовищем передачі* (мається на увазі розподіл у часі).

Використовуючи мультиплексування, в спільному комунікаційному середовищі можна організувати кілька незалежних каналів, розділивши його смугу пропускання на канали меншої пропускної здатності. Кожен з них можна використовувати або за принципом єдиного розподільчого середовища для під'єднання декількох кінцевих пунктів, або як незалежні канали двоточкового з'єднання для підключення окремих пар пунктів.

Обмеженням є дефіцит пропускної спроможності спільного середовища передачі, використання якого, незважаючи на зазначені недоліки, завжди є економічно вигідним рішенням.

Основна перевага спільного комунікаційного середовища – простота фізичної топології мережі, а також відносно недороге комунікаційне обладнання, в якому не потрібно аналізувати адресну інформацію повідомлень, що передаються. Це завдання перекладається на обладнання кінцевих пунктів, де аналізується адреса кожного надісланого повідомлення та обробляється лише те з них, яке адресовано даному пункту.

Вузлоутворення є компромісом між двома розглянутими вище способами організації зв'язних фізичних сегментів. Воно передбачає структуризацію сегмента зі встановленою ієрархією вузлових пунктів, в яких розміщується активне комунікаційне устаткування, що забезпечує зв'язність з'єднаних в них ліній.

У побудові сегментів фізичного рівня у вузлових пунктах використовується обладнання, в якому не передбачено обробку адресної інформації повідомлень, що передаються. Це устаткування фізичного рівня моделі OSI/ISO, наприклад, повторювачі, концентратори, мультиплексори.

Реалізація принципу вузлоутворення в сегменті називається його фізичною структуризацією, оскільки вузлові пункти можуть мати різний статус і таким чином формувати ієрархію. Фізично структурований сегмент залишається сегментом зі спільним комунікаційним середовищем і в ньому зберігаються всі притаманні йому недоліки.

5.3.2 Побудова сегментів канального рівня

Розміщення в вузлових пунктах сегмента устаткування, *здатного аналізувати адресну інформацію кадрів*, що передаються (комунікаційного обладнання канального рівня моделі (OSI/ISO), і на її основі виконувати функцію комутації вхідних і вихідних ліній зв'язку, дозволяє будувати структуровані сегменти з *комутованою топологією*, в даному випадку – сегменти канального рівня.

Такий принцип вузлоутворювання в сегментах отримав назву *логічна структуризація.*

У логічно структурованому сегменті у вузлових пунктах відбувається розділ спільного комунікаційного середовища на менші за розміром фізичні сегменти, у межах яких властиві йому недоліки мінімізуються або є зовсім відсутніми.

Можливість одночасного встановлення в комутаторі декількох внутрішніх зв'язків (вхід-вихід) для паралельного проходження декількох кадрів дозволяє значно підвищити продуктивність сегмента, що в цілому виправдовує деякі втрати у вартості комутованої топології в порівнянні з розподільчим комунікаційним середовищем.

Використання комутованої топології дозволяє вирішити ряд найважливіших завдань, таких, як підвищення продуктивності сегмента і забезпечення його оптимальною масштабованістю.

5.3.3 Побудова сегментів мережевого рівня

Проблемою великомасштабних сегментів стає необхідність обмеження широкомовного службового трафіку, що формується мережевими адаптерами хостів. Комунікаційні пристрої мережі, які працюють на фізичному й канальному рівнях моделі OSI/ISO, є прозорими для широкомовного трафіку, який складають кадри без конкретної фізичної адреси порту призначення (MAC-адреси).

Широкомовним кадрам службового трафіку належить значна частина трафіку при функціонуванні мережі, а це створює додаткове навантаження на магістральні лінії зв'язку.

Можливими є також ситуації, коли інтенсивність такого трафіку раптово зростає внаслідок програмних або апаратних збоїв. Наприклад, протокол верхнього рівня або мережевий адаптер починають працювати некоректно, генеруючи кадри з широкомовними адресами. Такий режим називається затопленням мережі, або широкомовним штормом.

Вирішити зазначені проблеми можна за рахунок поділу великомасштабного сегмента канального рівня на ряд сегментів мережевого рівня моделі OSI/ISO. Сегментом мережевого рівня є певна сукупність логічних вузлів, виокремлених за принципом домену.

Доменний принцип передбачає спосіб групування вузлів в поіменовані групи – домени. У даному випадку ім'ям для кожного домену є спільний для вузлів, що належать до нього, номер – адреса мережевого рівня. Група вузлів, які мають єдиний мережевий номер, називається логічною мережею.

Обмін трафіком двох і більше логічних мереж називають міжмережевою взаємодією. Прикордонним комунікаційним пристроєм, який виконує процедуру міжмережевої взаємодії, є маршрутизатор (обладнання мережевого рівня OSI/ISO). Він здатен не тільки розрізняти мережеві адреси, а й виконувати фільтрацію трафіку, спрямованого у відповідні логічні мережі.

Маршрутизатор обробляє пакети, які дістаються із кадрів, на основі мережевої адреси і не аналізує MAC-адресу. Тим самим він перешкоджає потраплянню службового широкомовного трафіку з однієї логічної мережі в іншу. У зв'язку з цим логічну мережу ще називають *доменом широкомовного трафіку*.

Використання в маршрутизаторах спеціальних алгоритмів маршрутизації з використанням адресної інформації пакетів забезпечує ще й можливість вибору оптимального, відповідно до заданих критеріїв, маршруту їх переміщення між вузлами.

5.4 Узагальнені характеристики сегментів

Узагальненими характеристиками будь-якого сегменту є *розмір, масштаб* і *структура внутрішньосегментного трафіку*.

Розмір сегмента визначається фізичною відстанню між найбільш віддаленими точками.

Масштаб сегмента визначається *кількістю об'єднаних* у ньому *хостів*.

Внутрішньосегментний трафік у загальному випадку складається з *локального трафіку, вихідного, вхідного і транзитного відносно сегменту*, який розглядається.

Локальним називається трафік, який формується в результаті інформаційного обміну хостів в межах сегменту.

Розподіл локального трафіку в сегменті називається *замиканням трафіку в сегменті.*

Вихідним називається трафік, який генерується хостами сегмента і є спрямованим за межі даного сегмента до хостів інших сегментів.

Вхідним називається трафік, генерований хостами інших сегментів і призначений хостам даного сегмента.

Транзитним відносно сегмента називається трафік, генерований хостами інших сегментів та адресований хостам, розташованим поза даним сегментом.

Відповідно до перерахованих складових внутрішньосегментного трафіку будемо розрізняти наступні види сегментів.

Сегмент замикання локального трафіку (СЗЛТ) – сегмент, у якому циркулює тільки локальний трафік. Це приклад закритої, ізольованої мережі.

Топологія логічних зв’язків у такому сегменті є повнозв’язною для кореспондуючих пунктів.

Існують «*плоскі*» і «*опуклі*» СЗЛТ.

Плоский СЗЛТ відповідає фізичному сегменту зі спільним комунікаційним середовищем, де рівень замикання локального трафіку припадає безпосередньо на фізичне середовище.

Опуклий СЗЛТ відповідає сегменту з комутованою топологією, де трафік замикається через логічний вузол (обладнання канального або мережевого рівня).

Такий вузол виконує обов’язки опорного вузла. Наприклад, та ж мережа робочої групи, що має топологію «зірки», але з використанням комутатора в центральному пункті.

Опорний вузол, через який хости обмінюються повідомленнями локального трафіку сегмента, визначає рівень замикання трафіку в опуклому сегменті.

Сегмент формування вихідного трафіку (СФВихТ) – сегмент, хости якого генерують трафік, спрямований за межі сегменту.

Сегмент розподілення вхідного трафіку (СРВхТ) – сегмент, у якому є лише трафік, який надходить від зовнішніх відносно нього, хостів.

У СФВихТ і СРВхТ не завершено процес перенесення інформації з кінця в кінець (від джерела до одержувача), і це визначає особливості топологій їх логічних зв’язків.

Топологією логічних зв’язків таких сегментів є «*дерево з корінням*». У разі СФВихТ траєкторії руху трафіку спрямовано від хостів до вузла – «кореня дерева», в якому концентрується вихідний трафік, а в разі СРВхП – навпаки. Вузол, який є «корінням дерева», у зазначених сегментах виступає у ролі *транзитного вузла*.

Оскільки на практиці всі мережі побудовано як відкриті системи, то припускається, що в багатьох випадках один і той же сегмент виконує відразу декілька функцій з формування трафіку (рис. 32).

Структурований СЗЛТ відображено як сукупність вкладених один в одного сегментів з поєднанням функцій СЗЛТ, СФВихТ і СРВхТ (рис. 33).

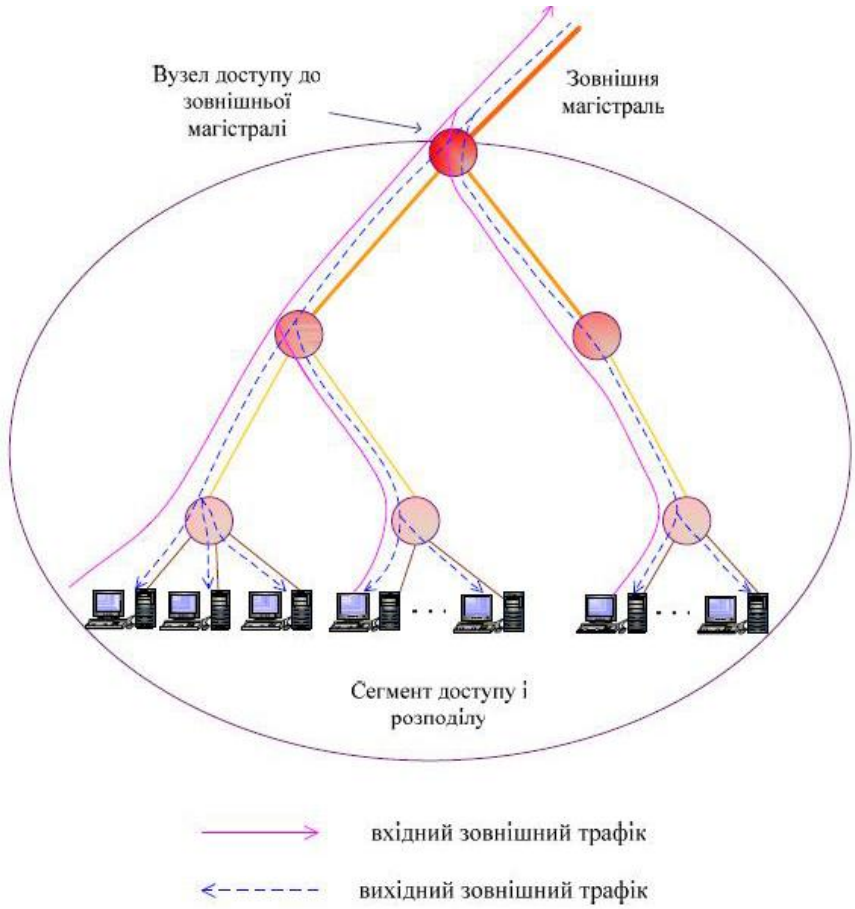


Рисунок 32 – Поєднання функцій СФВихТ і СРВхТ в одному сегменті

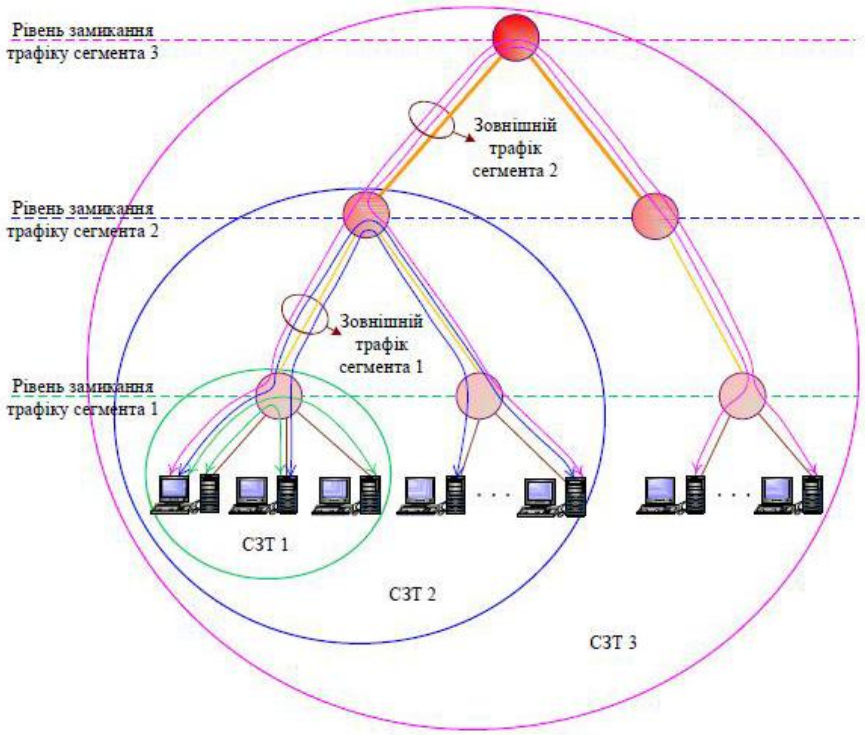


Рисунок 33 – Поєднання функцій СЗЛТ, СФВихТ і СРВхТ в одному сегменті

У такому сегменті існує декілька рівнів замикання трафіку, кожен з яких визначається статусом відповідного опорного вузла. Прикладом може бути мережа великого відділу, яка складається з рівня замикання локальних трафіків робочих груп і рівня замикання трафіку відділу.

Вузол, який виконує функції опорного вузла в поєднанні з функціями транзитного вузла, має назву *опорно-транзитного вузла*.

Сегментом формування транзитного трафіку (СФТТ) називається сегмент, у якому є концентрований трафік від хостів зовнішніх сегментів. СФТТ має особливий статус. Це магістральний сегмент, який об'єднує опорні, опорно-транзитні або власне транзитні вузли і визначає рівень замикання трафіку, оскільки перерозподіляє трафік між усіма об'єднаними ним сегментами, що мають нижчий статус.

Відмінною особливістю такого сегменту є підвищення вимог до пропускної спроможності магістральних ліній і продуктивності вузлів.

У мережевій термінології такий сегмент називається *магістральною мережею.*

5.5 Поєднання сегментів мережі

Поєднання сегментів здійснюється на фізичному, канальному й мережевому рівнях моделі OSI/ISO з використанням відповідного комунікаційного обладнання. При цьому можуть бути задіяні механізми *розширюваності* й *масштабованості* сегментів.

Під *розширюваністю* розуміють можливість збільшення розміру сегмента шляхом порівняно нескладного долучення нових структурних фрагментів.

Поняття розширюваності пов'язують зазвичай з фізичними сегментами, побудованими на основі спільного розподільчого середовища передачі. Масштаб такого сегмента та його фізичний розмір обмежені, тому що починаючи з якогось певного моменту, додавання чергового хосту або структурного фрагмента призводить до різкого зниження технологічних характеристик мережі (продуктивності, збільшення загасання переданих сигналів).

Механізми, які забезпечують розширюваність сегмента, – це поєднання невеликих за розміром фізичних сегментів в сегмент більшого розміру з використанням комунікаційного устаткування фізичного рівня. Масштаб розширюваного фізичного сегмента завжди має обмеження, що накладаються спільним комунікаційним середовищем.

Великомасштабні сегменти не можуть бути побудовані на базі нерозривного комунікаційного середовища з причин структурованості. Способи фізичної структуризації можуть варіюватися від простого поділу спільного кабелю на сегменти меншої довжини та поєднання їх за допомогою повторювачів (плоска структуризація) до побудови багаторівневої ієрархічної композиції на базі концентраторів (опукла структуризація).

На рис. 34 наведено приклад розширення локальної мережі, що використовує для з’єднання комп’ютерів загальний кабель (методом проколювання). Збільшення довжини сегмента здійснено нарощуванням додаткових ділянок, приєднаних повторювачами.

Рисунок 34 – Плоска фізична структуризація

Для мережі невеликого відділу, підприємства можна скористатися опуклою (багаторівневої) структуризацією, адекватною його адміністративному улаштуванню (рис. 35).

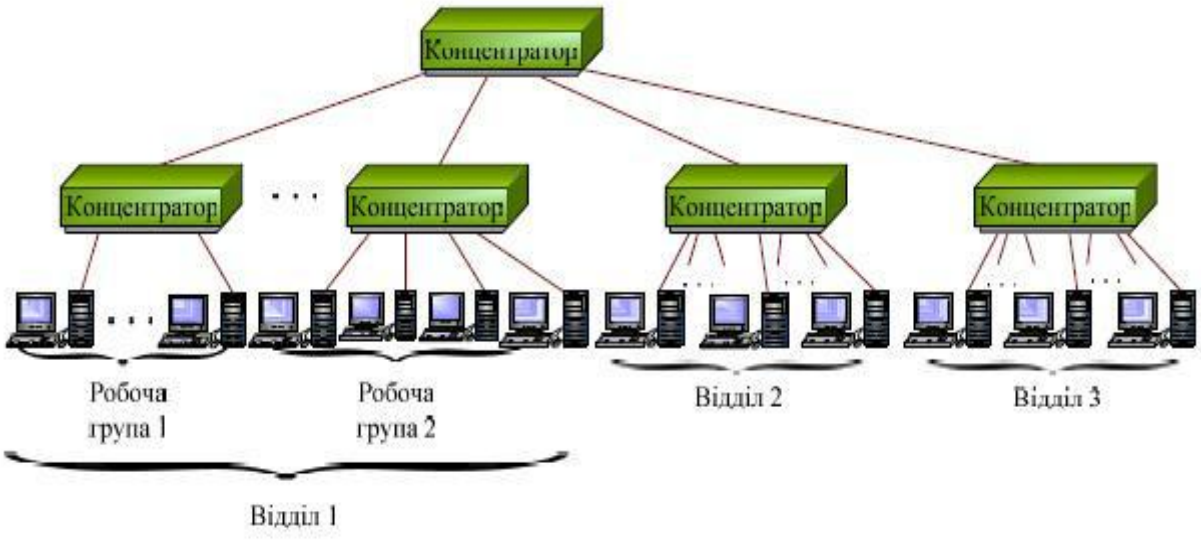


Рисунок 35 – Опукла фізична структуризація

Комутована топологія з використанням комунікаційного устаткування не нижче канального рівня, на відміну від спільного розподільчого середовища, дозволяє забезпечити оптимальну масштабованість сегмента.

Під *масштабованістю* розуміють можливість необмеженого під’єднання хостів і цілих сегментів, що не впливає на продуктивність мережі в цілому.

Збільшення масштабу сегменту відбувається шляхом додавання вузлового пункту на будь-якому рівні структуризації (доступу, розподілу або ядра). При цьому, чим вищим є рівень доданого вузла, тим ширшими можливості збільшення масштабу сегмента. Правильна масштабованість є

однією з найважливіших вимог, дотримання яких у сучасних мереж є необхідною.

У загальних випадках об'єднання сегментів, які генерують вихідний трафік, виконують із використанням СФТТ. З'єднання будь-якого сегмента з магістральним сегментом зазвичай відбувається у вузлі, який набуває ролі опорно-транзитного або транзитного.

Визначаючи рівень ієрархії вузлів, на якому доцільною є організація СФТТ, слід брати до уваги такий фактор як масштаб формованої мережевої інфраструктури.

Об'єднання сегментів на мережевому рівні розглядається як забезпечення *міжмережевої взаємодії*, тобто засіб обміну даними між логічними мережами з використанням комунікаційного обладнання і протоколів третього рівня моделі OSI/ISO. Таке об'єднання логічних мереж набуло назву інтермережа (internetwork, internet).

У мережах, які використовують стек протоколів TCP/IP, взаємодія логічних мереж здійснюється на основі *протоколу межмережевої взаємодії* (Internet Protokol, IP). У зв'язку з тим, поряд з терміном «інтермережа», використовуються також терміни IP-мережа, TCP/IP-мережа (за назвою протоколу і стека відповідно).

Термін *інтермережа*, на відміну від назви глобальної мережі Інтернет, завжди пишеться малими літерами, хоча за принципом організації вони ідентичні.

У межах однієї мережі масштабу LAN можна організувати інтермережу, наприклад, у разі необхідності забезпечення спільної роботи груп вузлів, які використовують різне системне програмне забезпечення. Для цього групи вузлів необхідно зробити логічними мережами, додавши їм відповідні номери (мережеві адреси) й організувати шлюз для їхньої взаємодії. Роль шлюзу може виконувати комп'ютер з відповідним програмним забезпеченням мережевого рівня або маршрутизатор. Іншим прикладом є обмеження масштабу логічної мережі її адресним простором (множиною адрес, які є допустимими в рамках прийнятої схеми адресації).

Наприклад, для IP-протоколу – це 255 хостів для мереж класу C – найбільш доступного. У цьому випадку необхідно також організувати інтермережу з декількома IP-адресами.

Висновки

Сегментний підхід при синтезі мережі забезпечує вирішення таких завдань:

– *підвищення* загальної продуктивності мережі, оскільки відділення локального трафіку розвантажує магістральні зв'язки;

– *спрощення* процесу керування мережею, оскільки основні проблеми частіше виникають і локалізуються всередині сегментів;

– *підвищення* гнучкості мережі, оскільки будь-який сегмент завжди можна адаптувати до специфічних потреб групи об'єднаних у ньому користувачів;

– можливість забезпечення в різних сегментах різних швидкостей передачі та мережевих технологій.

ЛЕКЦІЯ 6. МАТЕМАТИЧНІ МОДЕЛІ ТА МЕТОДИ СИНТЕЗУ ТА АНАЛІЗУ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

План

Вступ

1. Загальне поняття про задачі синтезу та аналізу.
2. Моделювання зв'язувальної мережі як об'єкта синтезу та аналізу.
3. Задачі синтезу телекомунікаційних мереж.
4. Синтез зв'язувальної мережі мінімальної вартості.
5. Визначення оптимального місця розташування опорного вузла в кабельній мережі абонентського доступу.
6. Визначення оптимального місця розташування базової станції в мережі стаціонарного радіо доступу.
7. Визначення циклу найменшої довжини для організації транспортного кільця.
8. Задачі аналізу телекомунікаційних мереж.
9. Знаходження найкоротшого шляху в зв'язувальній мережі.
10. Визначення множини шляхів заданої транзитності.

Висновки

Література

1. Теоретичні основи телекомунікаційних мереж : навч. посіб. /М.М. Климаш, Б.М.Стрихалюк, М.В.Кайдан. – Львів : вид-во УАД, 2011. – 496 с.

2. Буров Є. Комп'ютерні мережі / Є.Буров. – Львів : БаК, 1999. – 468 с.

3. Управління телекомунікаціями із застосуванням новітніх технологій / Кривуца В. Г., Беркман Л. Н., Стеклов В. К. та ін.]. – К.: Техніка, 2007. – 384 с.

Вступ

Для синтезу мережі є заданим географічне розташування пунктів мережі, які слід об'єднати в зв'язну мережу (саме). При цьому топологія ліній зв'язку є невідомою характеристикою, яку необхідно з'ясувати, й яка може варіюватися залежно від оптимізації економічних показників. Це дає змогу розглядати мінімум витрат на лінії зв'язку як цільовий критерій оптимального синтезу мережі.

6.1 Загальне поняття про задачі синтезу та аналізу

Усі задачі, які виникають у процесі побудови та експлуатації телекомунікаційних мереж діляться на два класи: *задачі синтезу* й *аналізу зв'язувальних мереж*.

Задача синтезу зв'язувальної мережі постає як у процесі побудови нової мережі, так і під час реконструкції та розвитку наявних мереж. задача є техніко-економічною, тому що найчастіше треба знайти рішення, оптимальне за економічними показниками: мінімум капіталовкладень, максимум рентабельності та ін.

На конфігурацію ліній зв'язку між пунктами мережі може бути накладено обмеження, зокрема заборона окремих географічних трас, наприклад, якщо вони перетинають водні або гірські перешкоди.

У класі задач аналізу розглядають питання визначення структурних характеристик як мережі в цілому, так і окремих її елементів. Конкретними задачами є такі:

– розв'язування яких – це вибір оптимальної топології фізичних зв'язків на певних ділянках мережі;

– підвищення надійності та живучості мережі;

– вибір оптимальної кількості й місця розташування вузлових пунктів та ін.

Задачі аналізу є актуальними для наявних, тобто вже синтезованих зв'язувальних мереж. Такі задачі спрямовано на:

– знаходження екстремальних шляхів передавання інформаційних потоків;

– визначення сукупності шляхів заданої транзитності;

– оцінювання пропускної здатності мережі;

– ймовірності підтримання зв'язку між пунктами та ін.

Для того, щоб вирішити конкретне завдання синтезу або аналізу телекомунікаційної мережі, її необхідно *формалізувати*, тобто записати у вигляді схеми: що дано, що необхідно визначити і з якими обмеженнями.[21]

Здійснення формалізації вимагає не тільки розуміння самої проблеми, а й вибору адекватної моделі об'єкта (телекомунікаційної мережі). Моделювання об'єкта синтезу або аналізу дає змогу з'ясувати та відтворити найбільш істотні, відповідно до поставленого завдання, елементи об'єкта та зв'язки між ними, не відволікаючись на деталі.

Для модельного відтворення зв'язувальної мережі найчастотніше застосовують графи. На основі моделі об'єкта та її параметрів (кількості пунктів та ліній мережі, відстаней між пунктами, пропускної здатності вузлів і ліній мережі, вартісних параметрів та ін.) можна побудувати математичну

[21] Формалізацію можна виконати словесно (таку форму називають вербальною моделлю завдання) або у вигляді математичної моделі, яка описує завдання термінами тієї чи іншої теорії (наприклад, теорії графів, теорії множин, теорії оптимальних рішень та ін.)

модель, яка відображає залежність між параметрами, що відшукуються, та незалежними змінними завдання.

У задачах синтезу та аналізу зв'язувальних мереж найчастіше використовують *оптимізаційні математичні моделі*, де критерій оптимізації записують як цільову функцію, для якої необхідно знайти екстремум (мінімум або максимум). На вхідні в цільову функцію параметри накладають обмеження, які вказують, у яких межах можуть змінюватися значення параметрів, що відшукуються. Обмеження записують як рівняння та нерівності, що містять деякі логічно пов'язані сукупності цих параметрів. Таку систему рівнянь або нерівностей називають *системою обмежень задачі*.

Задачі, в яких треба відшукати екстремум (мінімум або максимум) деякої цільової функції, що відображає критерій оптимальності рішення, називають *екстремальними*.

Особливістю екстремальних задач синтезу та аналізу телекомунікаційних мереж є їх велика розмірність. Формулювання цих завдань термінами графових та мережевих моделей дає змогу отримати значну кількість ефективних (зважаючи на подолання обчислювальної складності) методів та алгоритмів їх вирішення, орієнтованих на застосування ЕОМ.

Під *алгоритмом* розуміють формалізовану покрокову процедуру, що забезпечує знаходження рішення завдання, виконання якого можна доручити ЕОМ.

Розрізняють алгоритми точні та наближені, так звані евристичні.

Точні алгоритми завжди гарантують знаходження оптимального рішення (глобального оптимуму цільової функції). Наприклад, алгоритм повного перебору всіх можливих рішень з вибором найкращого серед них, є точним алгоритмом.

Точні алгоритми досить трудомісткі, тому у практиці часто використовують більш прості алгоритми, що забезпечують швидке вирішення з прийнятною точністю. Такі алгоритми будують, використовуючи раціональні *правила знаходження рішення.* Ці правила називають *евристиками*. Розв'язування задачі можна повторити, використовуючи інші евристики.

Евристичний алгоритм дає змогу знайти рішення, близьке до оптимального. Евристичні алгоритми використовують у тих випадках, коли побудувати точний алгоритм не вдається через складність математичної моделі задачі (її нелінійність, дискретність та ін.).

6.2 Моделювання зв'язувальної мережі як об'єкта синтезу та аналізу

Зв'язувальна мережа як об'єкт синтезу та аналізу – це сукупність розосереджених у просторі пунктів і ліній, які їх з'єднують. Математичною моделлю такого об'єкта може бути граф.

Означення. *Графом* називають певну сукупність точок, з'єднаних лініями.

Точки графа називають *вершинами*, а лінії – *дугами*.

Граф математично позначають як *G(N,V)*, де *N* – кінцева множина вершин потужністю n, а *V* – кінцева множина дуг потужністю *m.*

Вершини можна позначити малими латинськими літерами (*i, i,* k, l, s) або арабськими цифрами (1, 2, 3, 4, 5), а дуги – відповідно парами: {(*i,j*), (o,k), (*k,l*),...} або {(1,2), (2,3), (3,4),...}, де перший індекс визначає *початок дуги*, а другий – *кінець дуги* (рис. 36).

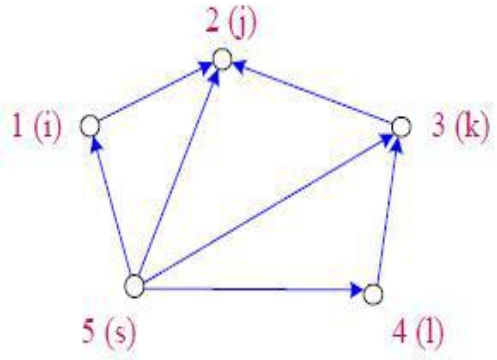


Рисунок 36 – Графова модель мережі

Граф, у якому задано напрямок дуг стрілками, називають о*рієнтованим*, у протилежному випадку – *неорієнтованим*. Неорієнтовані дуги називають *ребрами*.

Між двома вершинами, з'єднаними дугою (ребром), існує відношення *суміжності* (для орієнтованого графа вершини і та j суміжні, лише якщо дуга починається в і та направлена в *j*.

Між вершиною та суміжними з нею дугами (ребрами) існує відношення *інцидентності*.

Вершина і дуга інцидентні одне одному, якщо вершина є для цієї дуги кінцевою або початковою точкою.

Граф, кожній дузі (ребру) якого відповідатимуть деякі числові характеристики, називають *зваженим графом*, а самі характеристики називають *вагами*.

Ваговими характеристиками зв'язувальної мережі можуть бути відстані, пропускна здатність, вартість та ін. У разі необхідності ваги можуть бути приписані також вершинам графа.

Зважений граф прийнято називати *мережею* (в даному випадку мається на увазі ще одна модель зв'язувальної мережі, а не фізичний об'єкт).

Крім геометричного зображення у вигляді точок і ліній, граф можна відтворити дискретно.

Саме таку форму використовують у програмній реалізації алгоритмів для розв'язування задач із застосуванням графових моделей в ЕОМ. Однією з найбільш поширених дискретних форм графа є *матриця суміжностей*.

Матрицю суміжності графа наведено на рис. 37.

$$A=\begin{vmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \end{vmatrix}$$

Рисунок 37 – Матриця суміжності

Для зберігання в пам'яті ЕОМ матриці суміжності, як бачимо, необхідно n^2 комірок.

У неорієнтованому графі матриця суміжності є симетричною до основної діагоналі, отже, в пам'яті ЕОМ може зберігатися лише один з її трикутників (верхній або нижній), що економить пам'яті, але ускладнює її оброблювання в ЕОМ. Якщо перенумерувати довільно дуги (ребра) графа С і проставити ці номери відповідно до номерів рядків деякої матриці B = [], а номери стовпців залишити, як і раніше, відповідними номерам вершин графа, то в такій матриці можна відобразити відношення інцидентності елементів графа *G*. Елементи матриці можуть набувати значень {0, 1}.

Якщо перенумерувати дуги графа, наведеного на рис. 34, так : (*i,j*) – 1; (j, *k*) –2; (k, l) –3; (*l, s*) – 4; (*s, i*) –5; (*s, j*) – 6; (*s, k*) – 7, то матриця інцидентності набуде вигляду (рис. 38):

$$B=\begin{vmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{vmatrix}$$

Рисунок 38 – Матриця інцидентності

Орієнтованість графа в цій матриці, на відміну від матриці суміжностей, не відображається.

Якщо граф є *розрідженим* (має малу кількість дуг (ребер)), то можливим є більш компактне подання графа G, а саме списком дуг (ребер). Цей список можна реалізувати двома одновимірними масивами *(R1* і *R2*) розмірністю т, у першому з яких записано початкові вершини дуг (ребер), а в другому – кінцеві, або двовимірним масивом R розмірністю (*2,m*).

6.3. Задачі синтезу телекомунікаційних мереж

Розв'язування будь-якої задачі синтезу телекомунікаційної мережі обов'язково складається з визначення топології фізичних зв'язків (проводових або безпроводових) для деякої заданої сукупності пунктів, розосереджених у просторі. Неважко уявити, що кількість топологічних варіантів можливих фізичних зв'язків у цьому випадку, може бути доволі значною величиною. Закономірно постає питання про вибір такого варіанту, який відповідатиме деякому заздалегідь визначеному критерію оптимальності. Таким чином, задачі синтезу зв'язувальних мереж є екстремальними, для вирішення яких можна застосовувати точні та евристичні алгоритми.

Чим більшою є розмірність мережі, тим складнішим є застосування точних методів і алгоритмів. Однак сегментний підхід у побудові телекомунікаційних мереж дає змогу здійснювати декомпозицію загальної задачі синтезу мережі на ряд підзадач оптимального синтезу її сегментів, які виконують відносно самостійні завдання щодо забезпечення основної телекомунікаційної функції – транспортування інформаційних потоків. Отже, говорять про оптимальний синтез мережі абонентського доступу, транспортної мережі та ін.

Сучасна теорія графів пропонує витончені методи та алгоритми рішення завдань оптимального синтезу топологій фізичних зв'язків для сегментів телекомунікаційних мереж.

6.4. Синтез зв'язувальної мережі мінімальної вартості

Ситуація, в якій деяку множину точок необхідно поєднати так, щоб кожна пара точок стала зв'язною (безпосередньо або через інші точки), а загальна вагова характеристика зв'язків виявилася мінімальною, спонукає до *розв'язування задачі синтезу мережі мінімальної вартості*.

Приклад: є ряд точок, у яких можуть бути розташовані пункти телекомунікаційної мережі.

Відомо: відстані між парами точок і вартість прокладання одного кілометра лінії зв'язку.

Необхідно: визначити сукупність ліній зв'язку, які забезпечують зв'язність усіх пунктів мережі й мінімальну сумарну вартість їх прокладки.

З теорії графів і мереж відомо, що рішенням поставленого завдання є мережа з топологією фізичних зв'язків типу «дерево», тобто такого графа, в якому відсутні *цикли*. Граф містить *цикли*, якщо в ньому можна відшукати замкнуті контури. Відсутність циклів визначає особливість графа типу «дерево», яка полягає в тому, що між будь-якою парою його вершин існує лише один єдиний шлях їх сполучення, тобто параметр зв'язності $k = 1$. Кількість ребер у дереві є завжди на одиницю меншою від кількості його вершин.

Означення. Граф типу «дерево», в якому для кожної пари вершин існує шлях, який їх з'єднує, називають *покривним деревом*.

Математично задача синтезу мережі мінімальної вартості зводиться до знаходження *мінімального покривного дерева*. Цю задачу формулюють наступним чином.

Нехай задано неорієнтований граф *G (N,V*), де множині вершин *N* відповідає множина пунктів мережі, загальне число яких дорівнює *n*, а множина ребер *V* – відстаням між парами пунктів.

Відома вартість організації одиниці довжини (наприклад, одного кілометра) лінії зв'язку між пунктами *i* та *j*.

Необхідно знайти деяке покривне дерево *(N*), для якого досягається мінімум цільової функції:

Для вирішення поставленої задачі існує ряд ефективних алгоритмів знаходження покривного дерева. Наведемо один із них, відомий за прізвищем автора як *алгоритм Пріма*.

Алгоритм Пріма можна реалізувати шляхом надання позначок вершинам, які вводяться в відшукуваний граф (*N*), і послідовного введення в нього мінімальних за вагою ребер. При цьому, як зазначено вище, загальна кількість ребер не повинна перевищувати (*n–1*) і між усіма п вершинами покривного дерева має бути зв'язність.

Надамо процедуру виконання алгоритму Пріма у покроковій формі.

Крок 0. Мережа (*N*), яку треба визначити, початково містить п вершин і не має ребер. Вибирають одну довільну вершину *I* та позначають як «вибрану». Решта (*n –1*) вершин є «невибраними».

Крок 1. Відшукують ребро (*i, j*), яке належить *G (N,V)* з мінімальною вагою, у якого вершина і належить підмножині «вибраних» вершин, а вершина j – підмножині «невибраних» вершин.

Крок 2. Ребро (*i, j*) розміщують у мережі (*N*), яку треба визначити, а вершину і, вилучаючи з підмножини «невибраних», розташовують у підмножині «вибраних» вершин. Якщо підмножина «невибраних» вершин виявилася порожньою, то роботу алгоритму завершено. Інакше – перехід до кроку 1.

На кроці 0 граф , який треба знайти, містить сім вершин і не містить ребер. Вибираємо вершину 3 та позначаємо її як «вибрану» (рис. 39).

На кроці 1 вибираємо ребро (l_{35}) як ребро з найменшою вагою, у якого вершина і = 3 належить підмножині «вибраних» вершин (воно поки що містить лише одну вершину 3), а вершина j = 5 – підмножині «невибраних» вершин (зараз це всі інші вершини).

На кроці 2 ребро l_{35} уводимо у шуканий граф , а вершину 5 вилучаємо з підмножини «вибраних» вершин (рис. 40.).

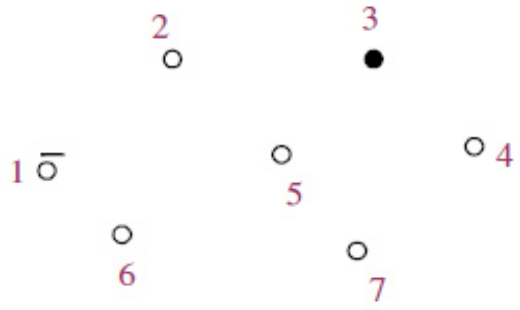


Рисунок 39

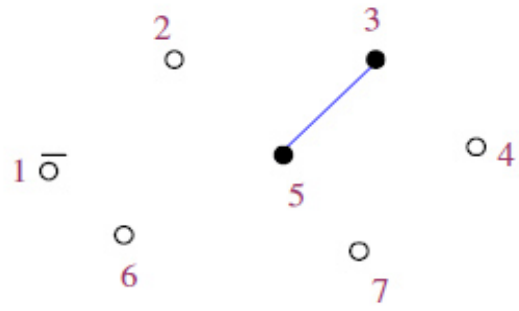


Рисунок 40

Оскільки підмножина «невибраних» вершин – порожня, повторюємо крок 1. Для цього знаходимо ребро мінімальної ваги, перебираючи сполучення кожної пари «вибраної» та «невибраної» вершин. Таким виявилося ребро l_{34} (рис. 41), яке розміщуємо у графі G. Вершина 4 стає «вибраною».

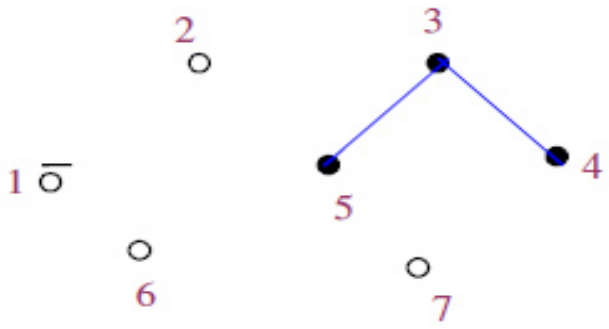


Рисунок 41

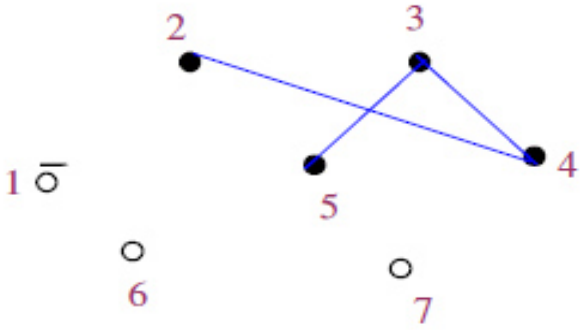


Рисунок 42

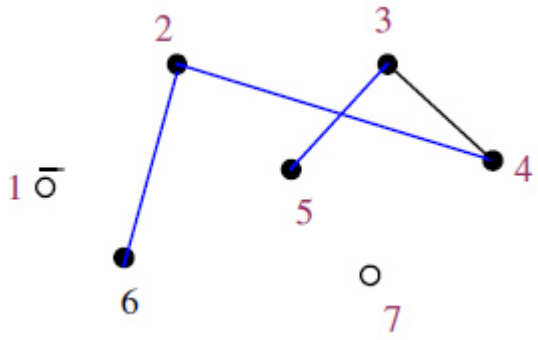


Рисунок 43

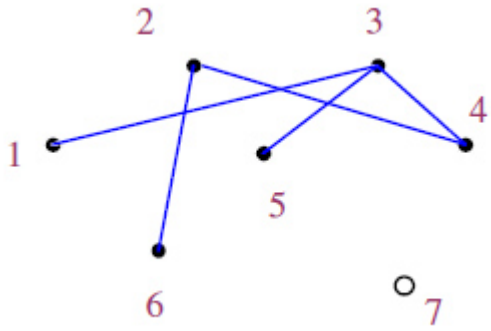


Рисунок 44

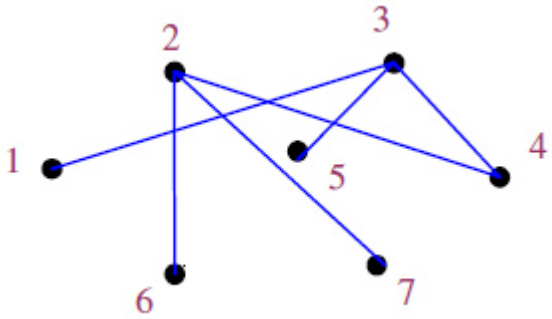


Рисунок 45

Наступними вибираємо ребра: l_{24} (рис. 42); l_{26} (рис. 43); l_{27} (рис.44). На цьому робота алгоритму закінчується, тому що всі вершини позначені як «вибрані» (тобто підмножина «невибраних вершин» стала порожньою).

Знайдено відшукуваний граф (N), який є покривним деревом, тому що він містить усі вершини, а число ребер на одиницю є меншим кількості вершин ($n = 7$, $V = 6$) та забезпечує зв'язність кожної пари вершин.

Знаходження мінімального покривного дерева є однією з класичних задач оптимізації на графах і мережах, оригінальні розв'язування якої запропоновано багатьма авторами. Більш ефективним, з урахуванням швидкості обчислень, є алгоритм, запропонований Краскелом.

Алгоритм Краскела відрізняється тим, що ребра в ньому проглядають у порядку зростання ваг і лиш одноразово. Звісно, це передбачає виконання попередньої процедури впорядкування ребер у порядку збільшення їх вагових характеристик. У разі однакових ваг ребра розташовують довільно.

Ідея алгоритму ґрунтується на процесі «фарбування» ребер і формуванні «букетів» із вершин. Проаналізуємо цю ідею.

Для фарбування ребер, які формуватимуть мінімальне покривне дерево, використовуємо, наприклад, зелений колір, а для тих, що поза ним – помаранчевий. Якщо чергове незабарвлене ребро, взяте з упорядкованого списку, *не утворює цикл* з ребрами зеленого кольору, його забарвлюємо у зелений колір, а з його вершини утворюємо «букет» вершин мінімального покривного дерева, яке будується. Інакше – ребро забарвлюємо у помаранчевий колір. Ребро може утворювати цикл у мінімальному покривному дереві лише в тому випадку, коли його вершини належать до одного «букету». Якщо ж вершини належать різним «букетам», то ребро забарвлюють в зелений колір, а букети зливаються.

Процедуру завершують, коли кількість зелених ребер досягає *(n –1),* або коли всі ребра будуть, не зважаючи на колір, пофарбованими.

Сформулюємо процедуру алгоритму Краскела покроково.

Крок 0. Упорядкувати ребра за збільшенням ваги. Усі ребра є непофарбованими. Букети відсутні. Вибрати перше з упорядкованого списку ребро (воно має мінімальну вагу), пофарбувати його в зелений колір і сформувати з його вершин перший букет.

Крок 1. Вибрати наступне за списком незабарвлене ребро. Можливим є один із таких варіантів:

а) обидві вершини належать одному букету – пофарбувати ребро в оранжевий колір;

б) одна з вершин належить букету, а інша ні – пофарбувати ребро в зелений колір, вершину долучити до того ж букет;

в) обидві вершини не належать жодному букету – пофарбувати ребро в зелений колір і сформувати з його вершин новий букет;

с) вершини належать різним букетам – пофарбувати ребро в зелений колір, а обидва букета об’єднати в один.

Перейти до кроку 2.

Крок 2. Якщо кількість зелених вершин дорівнює (п –1), або всі вершини пофарбовано – кінець роботи алгоритму. Інакше – повернутися до кроку 1.

6.5 Визначення оптимального місця розташування опорного вузла в кабельній мережі абонентського доступу

Розглянемо наступне завдання. Нехай граф *G(N,V)* відображає деяку зв’язувальну мережу, тотожну кабельній мережі абонентського доступу, яка охоплює п абонентських пунктів. Вага кожного ребра (*i, j*), яке належить *V,*

відповідає довжині або вартості прокладки кабелю, котрий з'єднує пункти *i* та *j*. Необхідно визначити деяку вершину *m*, що належить *N*, у якій доцільно розмістити опорний вузол (наприклад, районну АТС) з урахуванням мінімізації загальної довжини кабелю, який з'єднує абонентські пункти з опорним вузлом.

6.6 Визначення оптимального місця розташування базової станції в мережі стаціонарного радіодоступу

Припустимо, що задано розташування пунктів мережі, в якій реалізовано абонентський стаціонарний радіодоступ до базової станції (БС). Необхідно знайти місце розташування базової станції, яка по радіоканалах зв'язується з абонентськими пунктами (АП).

Бажано, щоб відстань від БС до будь-якого АП була мінімальною, що забезпечить стійкий радіо зв'язок з урахуванням меншої потужності передавача БС. Такий критерій задовольнити майже неможливо. Тому будемо мінімізувати відстань до найбільш віддаленого від БС абонентського пункту, решта АП в цьому випадку автоматично знаходиться ближче до БС.

Закономірно, що БС (якщо це можливо) повинна займати центральне положення відносно всіх АП. Задача знаходження пункту, в якому доцільно розташувати БС, може бути зведена до задачі знаходження центра графа.

Означення. Нехай G (N,V)є графом, де N – множина вершин, а V – множина відстаней між усіма вершинами. *Вершину s називають центром графа G* (*N*,*V*) якщо вона не суперечить умові *max* < *max* для будь-якої *i*; *1* < *j* < *n*.

Алгоритм знаходження центра графа (вершини s) випливає з самого визначення. Мінімізувавши відстань від точки *s* до найвіддаленішої вершини, забезпечується до всіх інших вершин гарантовано менша відстань.

6.7 Визначення циклу найменшої довжини для організації транспортного кільця

Кільцеві топології фізичних зв'язків часто використовують для побудови сегментів телекомунікаційних мереж, особливо транспортних мереж. У термінах теорії графів кільцеву топологію визначають як *цикл* або *контур*.

Під *циклом* розуміють послідовність дуг (ребер) графа, що складають шлях, який починається й закінчується в одній і тій же вершині, а під *контуром* – послідовність вершин графа, які входять у такий цикл.

Пошук циклу (контуру) є доцільний лише в «надлишковому» відносно деревоподібного графа, тобто в графі, кількість ребер якого є більшою від числа *n* його вершин. Власне кажучи, в задачах синтезу в такому сенсі вихідний граф допустимих зв'язків між вершинами завжди є надлишковим. У такому графі можна утворити *n!* циклів, які містять дуги (ребра) різної ваги, серед яких

можна відшукати цикл найменшої сумарної ваги дуг (ребер). Розв'язавши подібну задачу можна оптимізувати витрати на побудову транспортної мережі.

Задача про знаходження циклу найменшої довжини в теорії графів є відомою як «задача комівояжера». Вона може бути формалізована наступним чином. Дано граф *G (N,V)* вершини якого – це міста в зоні обслуговування комівояжера, а дуги – відповідно зв'язки між парами міст. Маршрутом комівояжера називається контур, який містить всі вершини графа *G*. Необхідно знайти маршрут найменшої довжини.

Не важко переконатися, що ефективність обчислювальної процедури для вирішення цього завдання точним методом різко зменшується зі збільшенням числа *n* вершин графа. Як доводить практика, ефективність можна вважати задовільною, якщо кількість вершин у графі не більша від 30. У зв'язку з цим для розв'язування задачі про знаходження *гамільтонового контуру* часто використовують *евристичні алгоритми*.

Наближений алгоритм для розв'язання задачі про комівояжера можна отримати, наприклад, використовуючи евристики: – «*на кожному кроці рухаємося тільки до найближчого пункту*». Використання такої евристики дає змогу одержати прийнятне рішення за час, необхідний для побудови тільки одного контуру.

6.8 Задачі аналізу телекомунікаційних мереж

Задачі аналізу телекомунікаційної мережі, як уже зазначено вище, ґрунтуються на синтезованої топології фізичних зв'язків, і найчастіше зводяться до з'ясування оптимальних топологій логічних зв'язків. Це стосується побудови оптимальних планів розподілу інформаційних потоків у мережі, вибору найкращих маршрутів передавання інформаційних повідомлень, підвищення надійності та живучості мережі та ін.

Задачі синтезу та аналізу дуже пов'язані між собою, оскільки можливості оптимізації топології логічних зв'язків обмежуються топологією фізичних зв'язків у мережі. Якщо неможливо виконати умови оптимальної побудови топології логічних зв'язків, доводиться повертатися до синтезу інших топологій фізичних зв'язків. У результаті побудова телекомунікаційної мережі та її сегментів перетворюється на ітераційний процес.

Нижче розглядаємо окремі класичні задачі аналізу зв'язувальних мереж, що засновані на *графових моделях*.

6.9 Знаходження найкоротшого шляху в зв'язувальній мережі

Задача про знаходження найкоротшого за довжиною шляху в зв'язувальній мережі є фундаментальною задачею комбінаторної оптимізації. За її допомогою можна вирішити широке коло практичних завдань, які

виникають у процесі керування телекомунікаційними мережами, впровадження нових телекомунікаційних технологій, методів маршрутизації та ін. Закономірно, що як «довжини» можуть розглядатися будь-які інші вагові характеристики елементів графа.

Одним з найбільш ефективних алгоритмів, які вирішують поставлене завдання, є *алгоритм Дейкстри*. Особливістю цього алгоритму є те, що в процесі його виконання одночасно будують найкоротші шляхи з заданої вершини *s* до усіх інших вершин мережі. Це пояснюється тим, що будь-яка вершина і *N* може виявитися проміжною на найкоротшому шляху з *s* до *i*. Після закінчення роботи алгоритму вершина s стає з'єднаною з усіма іншими вершинами зв'язувальної мережі *G*, зокрема і з вершиною і, найкоротшими шляхами, а дуги (ребра), які увійшли до них, утворюють деяку підмережу без циклів, тобто «дерево» з коренем у вершині *s*.

6.10 Визначення множини шляхів заданої транзитності

Серед обмежень, які накладаються у процесі знаходженні шляхів у зв'язувальних мережах, можна розглядати обмеження на їх транзитність.

Під *транзитністю шляху* розуміють кількість проміжних пунктів, які входять до нього (без урахування початкового s і кінцевого t пунктів), або кількість ліній зв'язку, які з'єднують на шляху тільки транзитні пункти. Кількість проміжних пунктів називають *параметром транзитності T на шляху*.

Обмеження за транзитністю на шляху надсилання повідомлення залежать від вимог до якості обслуговування у мережі (наприклад, до часу проходження повідомлення мережею, часу оброблювання повідомлення у вузлах та ін.).

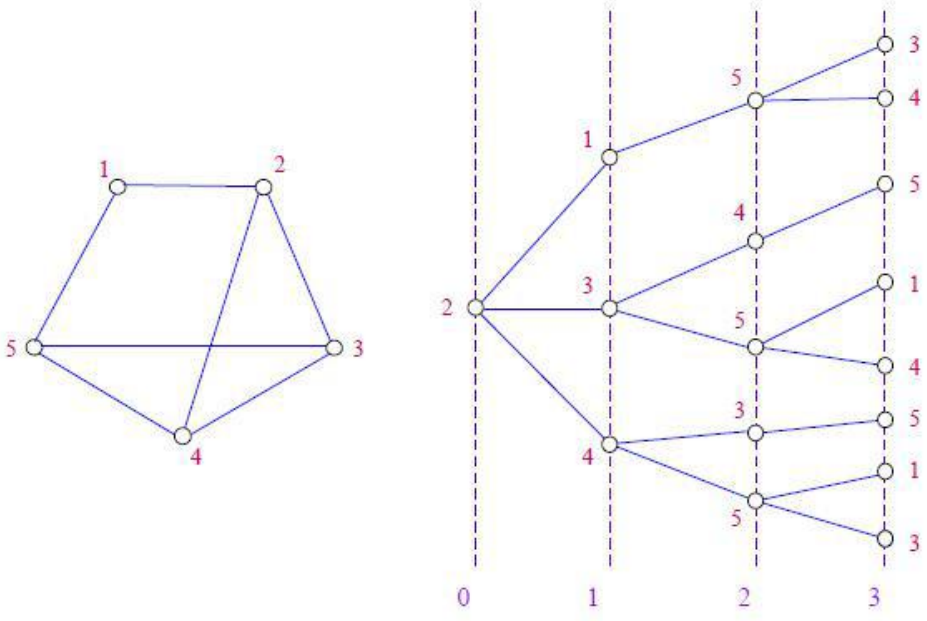


Рис. 46 – Ілюстрація роботи алгоритму побудови ярусного дерева

Алгоритм побудови «ярусного дерева» складається з таких кроків.

Крок 0. Утворити підмножини нульового ярусу, який міститиме єдиний елемент – вершину *s*. Використовуючи матрицю суміжності, виписати номери стовпців у рядку з номером 8, елементи якого дорівнюють *1*. Таким чином, отримано підмножину вершин першого ярусу, утворену вершиною *s*.

Крок 1. Утворити підмножину вершин наступного ярусу. Для цього:

а) почергово вибирають вершини попереднього ярусу, для кожної з яких вибирають рядок з однойменною номером у матриці суміжності;

б) для кожного рядка виписують номери стовпців, визначені ненульовим елементами;

в) з кожної з утворених підмножин вилучають номери вершин (номери стовпчиків), відносно яких утворювалися підмножини вершин у попередніх ярусах. Усі не викреслені елементи (номери стовпчиків) утворюють підмножини наступного ярусу.

Крок 2. Якщо номер ярусу дорівнює $(T_0 + 1)$ – кінець. Інакше – перейти до кроку 1.

Спеціальні технічні можливості комутаційного обладнання іноді дають змогу вибирати додаткові напрями (обхідні) у разі зайнятості напрямку першого вибору. Порядок вибору напрямків визначають маршрутної матрицею, кількість рядків якої відповідає числу шляхів, нумерація рядків – призначеному порядку їх зайняття, а число стовпців – адресами пунктів призначення.

Елементом маршрутної матриці є номер порту вихідної лінії на шляху відповідного вибору з даного транзитного пункту до пункту призначення.

Висновки

Алгоритми знаходження екстремальних шляхів (найкоротших за довжині, за транзитністю) застосовують для визначення оптимальних маршрутів як у мережах із пакетною комутацією, так і в мережах із комутацією каналі каналів. Результати їхньої роботи зводять до побудови маршрутних матриць, які зберігаються в транзитних пунктах телекомунікаційних сегментів із комутованої топологією. Вони призначені для визначення вихідного порту під час комутації вхід-вихід, наприклад, у маршрутизаторах, комутаційних телефонних станціях.

ЛЕКЦІЯ 7. БАЗОВІ ТЕЛЕКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

План

Вступ

1. Поняття технології в телекомунікаціях.

2. Технології синхронного перенесення: синхронне часове мультиплексуваня; комутація каналів; технологія ISDN.

Висновки

Література

11. Теоретичні основи телекомунікаційних мереж : навч. посіб. /М.М. Климаш, Б.М.Стрихалюк, М.В.Кайдан. – Львів : вид-во УАД, 2011. – 496 с.

2. Буров Є. Комп'ютерні мережі / Є.Буров. – Львів : БаК, 1999. – 468 с.

3. Управління телекомунікаціями із застосуванням новітніх технологій / Кривуца В. Г., Беркман Л. Н., Стеклов В. К. та ін.]. – К.: Техніка, 2007. – 384 с.

Вступ

Під терміном «метод передавання» (на відміну від «режим перенесення») розуміють спосіб організації взаємодії приймача й передавача в процесі обміну сигналами між двома суміжними вузлами мережі, безпосередньо з'єднаними лінією зв'язку (проводовою або безпроводовою). Ці методи ґрунтуються на теорії передавання сигналів і в даному розділі не розглядаються.

7.1. Поняття технології в телекомунікація

Поняттям *технологія* у сфері телекомунікацій позначають *спосіб реалізації режиму перенесення інформації в мережі, який забезпечує користувачів певним гарантованим рівнем якості обслуговування.*

Термін *режим перенесення* узагальнено розуміють як *сукупність методів мультиплексування, передавання та комутації, за допомогою яких у телекомунікаційній мережі уможливлюється транспортування інформації з кінця в кінець, тобто від джерела до одержувача.*

Фізичною основою будь-якої телекомунікаційної технології є лінії зв'язку та комунікаційне (мережеве) устаткування.

Лінії зв'язку – це узагальнене поняття, яке, залежно від застосування певної телекомунікаційної технології, можна конкретизувати таким чином:

– *ланка, лінк* – це фізичний сегмент, який забезпечує передавання сигналів між суміжними вузлами без використання проміжного комунікаційного обладнання мультиплексування й комутації;

– *канал* – це частина пропускної здатності ланки, яка незалежно використовується під час комутації. Канали в ланці можуть бути утворені за допомогою демультиплексора або апаратури ущільнення (наприклад, ланка з 30 каналів, кожен з яких має пропускну здатність 64 Кбіт/с);

– *комутований канал* – це складений канал, який утворюється в сегменті з комутованою топологією з окремих проміжних ланок або каналів та комутаційного обладнання вузлів;

– *тракт передавання* – це всі пристрої та споруди, які беруть участь в утворенні шляху проходження інформації з кінця в кінець. Тракт утворюють засоби кросової комутації декількох каналів у транзитних вузлах мережі.

Лінії зв'язку є середовищем передавання сигналів, безпосередньо підтримуючи технології фізичного рівня моделі OSI/ISO. Комунікаційне обладнання залежно від функціональності можна поділяти на обладнання фізичного, канального та мережевого рівнів моделі OSI/ISO.

Режим перенесення інформації в мережі можна організувати *синхронним* способом або *асинхронним*.

Синхронний режим перенесення ґрунтується на принципі синхронного часового мультиплексування та часового розділення каналів у процесі передавання інформації від одного вузла комутації до іншого. При цьому всі ланки тракту передавання інформації з кінця в кінець працюють синхронно. Таку синхронізацію забезпечують спеціальні синхронні технології, основані на використанні генераторів тактових сигналів, які працюють від єдиного еталонного джерела в мережі.

Для *асинхронного режиму перенесення* достатньо забезпечити синхронне передавання інформації лише між суміжними об'єктами (передавачем і приймачем вузлів, безпосередньо з'єднаних лінією зв'язку). У транзитному вузлі інформаційні блоки зберігаються деякий час у пристрої запам'ятовування, а потім передаються в наступний вузол мережі. При цьому швидкості у вхідному та вихідному каналах вузла можуть відрізнятися. Таким чином, *при асинхронному режимі інформація переміщується мережею естафетним способом.*

Відповідно до цього телекомунікаційні технології можна класифікувати як *технології синхронного* та *асинхронного режимів* перенесення. Технологічний рівень розвитку мережі того чи іншого режиму перенесення залежить від двох факторів: рівня розвитку науково-технічного прогресу; потреб людства в послугах зв'язку певного типу та відповідної якості.

Телекомунікаційна технологія є одним з основних факторів, який характеризує телекомунікаційну мережу з точки зору можливостей з транспортування інформації.

7.2. Технології синхронного режиму перенесення

7.2.1. Синхронне часове мультиплексування

Режим комутації часових каналів, який ґрунтується на принципі синхронного часового мультиплексування під час передавання інформації від одного вузла комутації до іншого, відомий як синхронний режим перенесення STM (Synhrounus Transfer Mode).

Під *мультиплексуванням* у цифрових мережах розуміють поєднання п низькошвидкісних цифрових потоків у один високошвидкісний потік. Мультиплексування застосовують з метою більш ефективного використання пропускної здатності лінії зв'язку, що зумовило вживання у термінології понять *ущільнення, розподілення лінії зв'язку*.

Вихідні цифрові потоки, які формуються в результаті роботи різних мережевих застосувань (від різних служб), можуть істотно відрізнятися за своєю природою. Це передавання:

– постійного бітового потоку;

– файлів даних;

– мовленнєвих і відеосигналів в цифровій формі.

Мультиплексування забезпечує *адаптацію середовища передавання лінії зв'язку* до великої кількості різнорідних мережевих додатків.

Цифровий потік кожного застосування є сигналом, що відповідає критеріям та показникам певного інформаційного повідомлення, яке необхідно передати. Часове синхронне мультиплексування полягає в тому, що вся смуга середовища поширення сигналів в лінії зв'язку на короткий проміжок часу, тривалістю τ, почергово надається сигналам п застовувань.

Зазначений проміжок часу називають *тайм-слотом*, інтервал $Тц = nr$, який відповідає n тайм-слотам, називають *циклом передавання*.

Характерною особливістю *синхронного часового мультиплексування* є те, що в мультиплексному сигналі кожному початковому сигналу відповідає тайм-слот із чітко фіксованим порядковим номером у межах циклу передавання $Тц$.

Слід зазначити, що завдяки мультиплексуванню для сигналу мультимедійного застосування (голос + відео + дані) надають відразу декілька тайм-слотів.

Пристрій, який приймає декілька потоків від різних застовувань (голос, відео, дані) й передає їх у лінію у вигляді мультиплексного сигналу, називають *мультиплексором* (MUX), а пристрій, який виконує зворотну функцію на іншому кінці лінії, – *демультиплексором* (DEMUX). MUX і DEMUX повинні працювати синхронно і синфазно, так як тайм-слоти відносно Тц на вході й на виході лінії зв'язку повинні збігатися. З цією метою використовують пристрої з високим стандартом частоти, які називають *таймерами*.

Зазвичай, у системах двобічного (дуплексного) зв'язку функції мультиплексування й демультиплексування поєднують в одному пристрої, який також називають *мультиплексором*.

Сучасні мультиплексори розподілення часу є каналоутворювальним обладнанням. Їх відмінність від традиційних систем ущільнення з імпульсно-кодовою модуляцією полягає в тому, що:

– мультиплексори дають змогу передавати в лінію цифрові потоки різних швидкостей (від різних джерел), тому вони ще називаються *гнучкими мультиплексорами;*

– мультиплексори, які мають властивість «*долучення/виокремлення*», дозволяють відокремити від загального потоку частину сигналів або додавати

сигнали до спільного лінійного потоку. Це дає змогу будувати мережі складної топології.

Мультиплексування мовленнєвих сигналів за своєю природою є аналоговим, і для передавання в інформаційній мережі його перетворюють у цифровий. Відомо, що основну смугу частот мовленнєвого сигналу оптимізовано за індексом артикуляції (прийнятному – 0,7), що відповідає рівню чіткості слів 85-90% і складає 3100 Гц. Цю смугу розміщено в діапазоні 0,3-3,4 кГц, що відповідає стандартизованій смузі каналу тональної частоти (ТЧ).

Зважаючи на те, що зазначену смугу необхідно фільтрувати реальним аналоговим смуговим фільтром, який має кінцеву крутизну спаду частотної характеристики в перехідній смузі, запропоновано використовувати смугу 4 кГц як розрахункову ширину смуги стандартного каналу тональної частоти, що забезпечує захисну смугу між двома сусідніми каналами 900 Гц.

Схема цього перетворення складається з таких етапів:

1. Дискретизування аналогового сигналу. Відповідно до теореми Котельникова частота дискретизування аналогового сигналу, яка забезпечує його відновлення без спотворення, дорівнює подвоєнню максимальної частоти спектру сигналу. З урахуванням верхньої межі діапазону мовленнєвого сигналу, частота дискретизації

$$Fд = 2 \text{ х } 4 \text{ кГц} = 8 \text{ кГц},$$

що відповідає періоду дискретизування = 1/8 = 125 мкс.

2. Квантування амплітуд дискретних відліків сигналу за рівнем є поділ миттєвої амплітуди на певне число рівнів (рівнів квантування). Для якісного передавання мовлення приймають 256 рівнів квантування.

Величиною амплітуди дискретного відліку мовленнєвого сигналу вибирають найближчий до її значення рівень квантування. Різницю між значеннями амплітуди сигналу та найближчим рівнем квантування визначає похибка перетворення мовленнєвого сигналу в цифрову форму, яку називають *помилкою квантування Δ*.

3. Кодування квантованих амплітуд дискретних відліків мовленнєвого сигналу. Якщо номери рівнів квантування подати в двійковому коді, то процес кодування зводиться до вибору номера найближчого до значення дискретної амплітуди сигналу рівня квантування.

Номер рівня квантування в двійковому коді передається в лінію. Кількість позицій двійкового коду цифрового номера рівня квантування дорівнює 8 (один байт), що дає змогу закодувати номер найвищого рівня квантування 255 – 11111111.

Кодову комбінацію, яка відповідає одному дискретного відліку амплітуди мовленнєвого сигналу, називають вибіркою.

Зважаючи на те, що вибірки мовленнєвого сигналу надходять у лінію з частотою 8 кГц, послідовно одна за одною, отримуємо цифровий зі швидкістю С = 8 біт х 8 кГц = 64 кбіт/с.

Швидкість 64 кбіт/с визначено Міжнародним союзом електрозв'язку (ITU-T) швидкістю основного цифрового каналу, який ще називають потоком нульового рівня DSO (Digital Service /Signal of Level 0).

Імпульсно-кодова модуляція є основою для побудови цифрових систем передавання (ЦСП). Існує декілька реалізацій цифрових систем, визнаних стандартними:

ІКМ-30/32 (СНД) – 30-канальна;
CEPT (Європа) – 30-канальна;
Bell D1 (США) – 24-канальна;
D 2 (Bell, США) – 24-канальна;
U.K. (Англія) – 24- канальна.

Принцип побудови ЦСП зображено на рис. 47.

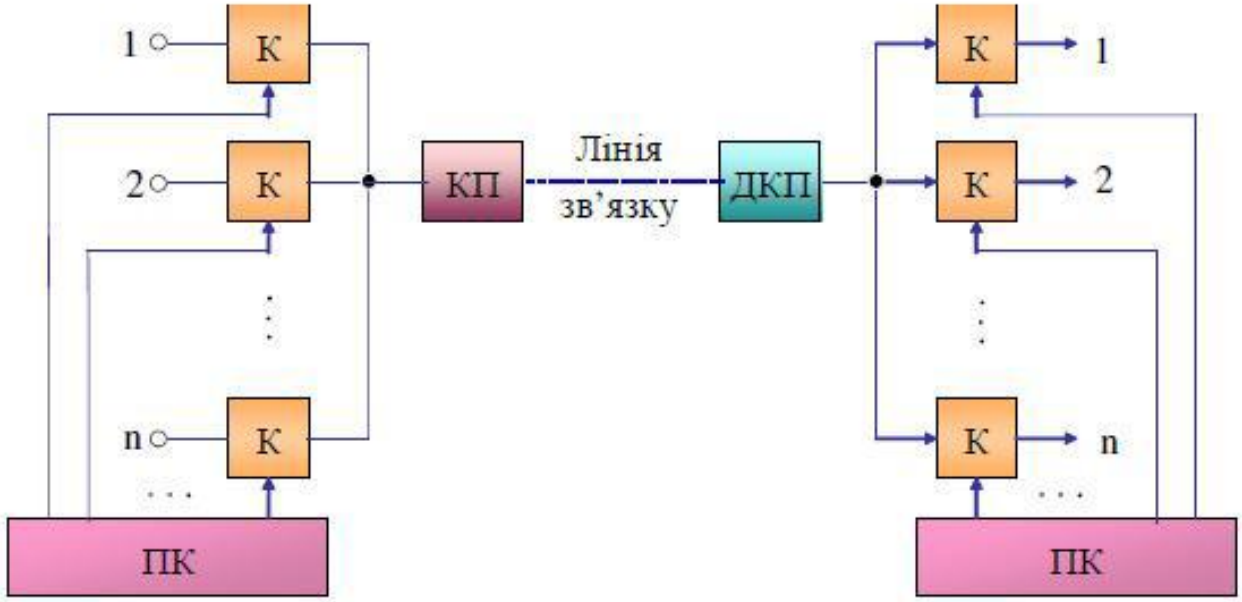


Рисунок 47 – Структурна схема ЦСП: К – електронні ключі, які забезпечують дискретизацію безперервних інформаційних сигналів; ПК – пристрої керування станом (замкненого, розімкнутого) ключів; КП – кодувальний пристрій, в якому груповий сигнал підлягає квантуванню й кодуванню; ДКП – декодер, який зворотно перетворює ІКМ- сигнал у груповий амплітудно-імпульсний сигнал

Функціонування такої системи пов'язано з розмежуванням часу передавання на повторювані цикли тривалістю . Кожний цикл, у свою чергу, розбивають на тайм-слоти, число яких дорівнює кількості організованих у лінії каналів.

Розглянемо структуру (формат) багатоканального сигналу на виході 30-канального ЦСП.

Апаратура ІКМ-30/32 утворює в лінії 32 цифрові канали, з яких 30 призначено для передавання інформаційних сигналів, один – для синхронізації, один – для сигналізації (передавання службових сигналів перед сеансом зв'язку).

Час циклу Тц у ІКМ-30/32 відповідає період дискретизації = 125 мкс. Для того, щоб упродовж цього часу передати 32 цифрові потоки зі швидкостями 64 кбіт/с кожен, у лінії зв'язку необхідно забезпечити швидкість Сл = 64 кбіт/с х х 32 = 2048 кбіт/с.

Загальна тривалість тайм-слоту при цьому т = 125 мкс/32 = 3,90625 мкс. Упродовж цього часу послідовно в кожному з 32-х тимчасових каналів передається 1 байт.

Протягом циклу Тц передається відповідно: 8 біт х 32 = = 256 байт. Формат сигналу в 256 байт показано на рис. 48. Його називають *кадром*, або *фреймом.*

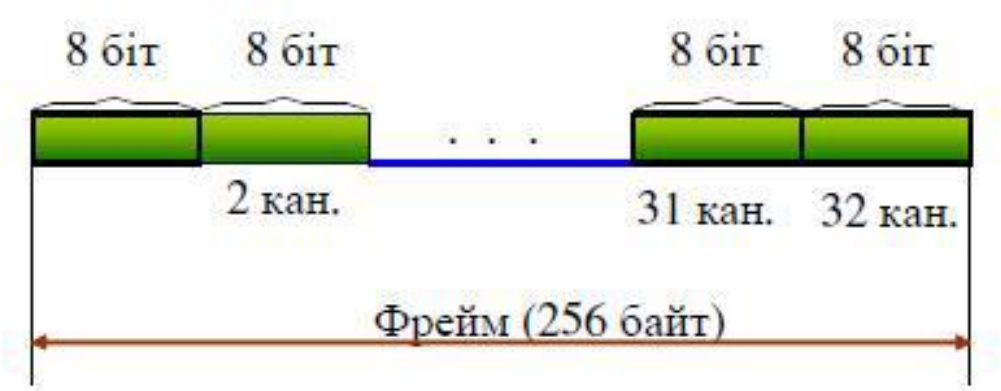


Рисунок 48 – Формат лінейного сигналу ІКМ-30/32

Кількість біт, яка відповідає конкретному часовому каналу (тайм-слоту) в загальному форматі фрейму, називають полем, або ніблом (nibble).

Положення кожного поля чітко фіксується в структурі фрейму. Це уможливлено застосуванням у ЦСП синхронізації. Синхронізація здійснюється передаванням спеціального синхросигналу (наприклад, 11111111) каналом синхронізації (наприклад, 31-м). Сигнал синхронізації в даному випадку передається зовнішнім (відносно до інформаційного) каналом, а тому вважають, що виконується ідеальне мультиплексування.

Під час часового мультиплексування потоків даних на входи мультиплексора подаються п двійкових потоків даних, походження яких не пов'язано з формуванням вибірок для відліків амплітуд безперервних сигналів. Тому з вхідних каналів можна вибрати будь-яку логічно осмислену послідовність біт як вибірку сигналів при формуванні фрейму.

Такий процес формування вибірок називають інтерлівінгом. байт-інтерлівінг (чергування байтів по одному з кожного каналу); символьний інтерлівінг (чергування декількох бітів, необхідних для кодування одного символу переданого тексту, з кожного каналу. Наприклад, під час передавання

файлу з комп'ютерним алфавітом ASCII міжнародної версії, довжина поля коду одного символу становить 8 біт, а американської версії – 7 біт); блок-інтерлівінг (чергування блоків по кілька байт із кожного каналу).

Сигнали синхронізації та сигналізації у процесі формуванні фрейму можуть передаватися як окремими виділеними часовими каналами (ідеальне мультиплексування), так і інформаційними каналами.

Узагальнено в мультиплексуванні потоків даних розрізняють такі види синхронізації:

– за окремими полями (часовими каналами);
– за фреймом у цілому;
– за кожним бітом у межах кожного поля.

Для синхронізації в структуру фрейму після будь-якої з перерахованих груп додають по одному або кілька бітів. Можна сформувати й більш складну повторювану структуру, складену з m-фреймів і k полів синхронізації, так званий мультифрейм.

Без урахування синхронізації мультиплексор створює регулярний потік фреймів. Синхронізація цю регулярність порушує.

Сигналізація також може бути виконана в окремому каналі або розміщенням бітів сигналізації в полях вибірок зі зменшенням при цьому розрядної сітки поля, наприклад, на 1 біт.

Навіть зважаючи на все можливе розмаїття, структура фрейму (його формат) для конкретної системи передавання є фіксованою. За аналогією до тривалості циклу передавання $T_Ц$ в ідеальному мультиплексуванні, у даному випадку можна говорити за період повторення фрейму – часу, що витрачається на один повний цикл, та доданому часу передавання долучених бітових груп синхронізації та сигналізації.

7.2.2. Комутація каналів

Надання зв'язку абонентам-кореспондентами на основі методу комутації каналів (Switching Circuits, SC) складається з трьох фаз.

1. Налаштування дуплексного каналу. Для цього в мережу передається службова інформація, яка містить закодовані адреси абонента. На основі цієї інформації встановлюється маршрут передавання інформаційного повідомлення, який з'єднує опорні вузли через ланцюг проміжних вузлів комутації. Службова інформація формується самим абонентом (набором номера абонента) або його терміналом і передається каналами сигналізації або інформаційними каналами.

2. Здійснення сеансу зв'язку. Після налаштування каналу абоненти можуть починати процес обміну інформаційними повідомленнями. При цьому ресурси мережі, які забезпечують даний сеанс зв'язку, повністю закріплені за налаштованим каналом зв'язку і, в разі пауз у процесі передавання інформації, не можуть бути надані для організації інших з'єднань.

3. Від’єднання каналу. Після відповідної команди про припинення сеансу зв'язку від однієї з опорних станцій каналом сигналізації проходить сигнал роз'єднання, в результаті чого зайняті ресурси вивільняються в мережу.

Для налаштування каналу комутаційна система повинна забезпечити взаємні з’єднання будь-яких каналів.

Для комутації кожного вхідного часового каналу з кожним вихідним необхідно мати можливість перестановки вибірки, яка визначає амплітуду мовленнєвого сигналу (байти інформації) з одного часового інтервалу в будь-який інший.

У даний час використовують два принципи побудови комутаційних блоків (КБ): просторовий та часовий. Просторовий принцип побудови КБ. З’єднання здійснюється в одній і тій же часовій позиції каналів вхідної ущільненої лінії (ВхУЛ) з каналами вихідної ущільненої лінії (ВихУЛ).

У цьому випадку 8-розрядна вибірка надходить з каналу і ВхУЛ в канал і ВихУЛ. Структурну схему просторового однокаскадного КБ зображено на рис. 49.

У певні моменти часу з пристрою керування (ПК) подаються сигнали для замикання відповідних точок комутації. Ці точки можуть бути реалізовані на електронних елементах (електронних ключах).

Очевидно, що за такої побудови КБ комутуються цифрові канали ВхУЛ з цифровими каналами ВихУЛ тільки в одній і тій же часовій позиції (в однойменних тайм-слотах), тобто в процесі комутації немає можливості змінити часову позицію. Здійснити таку можливість дає змогу часовий принцип побудови КБ.

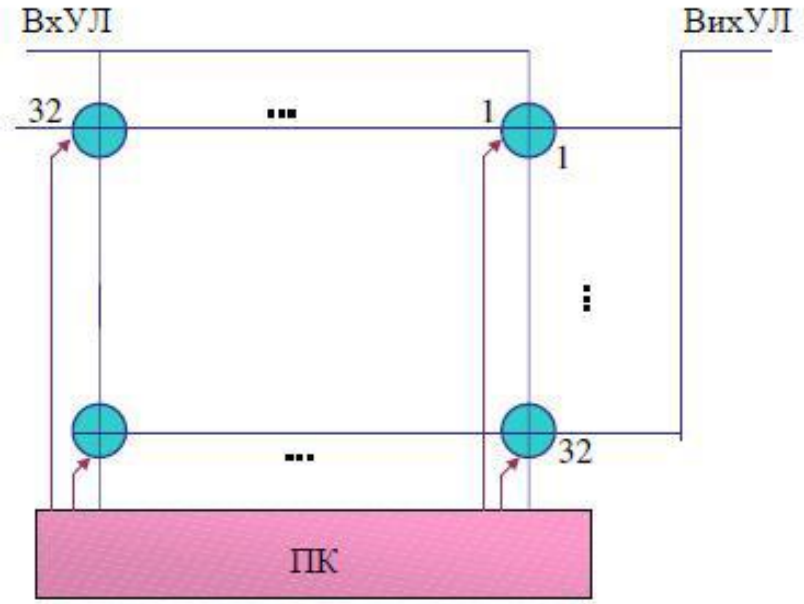


Рисунок 49 – Просторовий однокаскадний КБ

Часовий принцип побудови КБ засновано на налаштуванні зв'язку входу з виходом через буферний запам'ятовуючий пристрій (БЗП) (рис. 50).

Канальні вибірки, які послідовно надходять з ВхУЛ в результаті демультиплексування, через допоміжну комірку ДК1, куди накопичується 8-розрядна кодова комбінація при побітовому її надходженні, розміщуються в БЗП у комірку з адресою, яка відповідає номеру часового каналу.

Протягом часу одного тайм-слоту проводиться один запис у БЗП канальної вибірки, яка надходить із ВхУЛ, і одне зчитування канальної вибірки з БЗП, яке направляється в ВихУЛ. У зв'язку з цим канальний інтервал (тайм-слот) розділяється на дві фази. У першій здійснюється запис, у другій – читання.

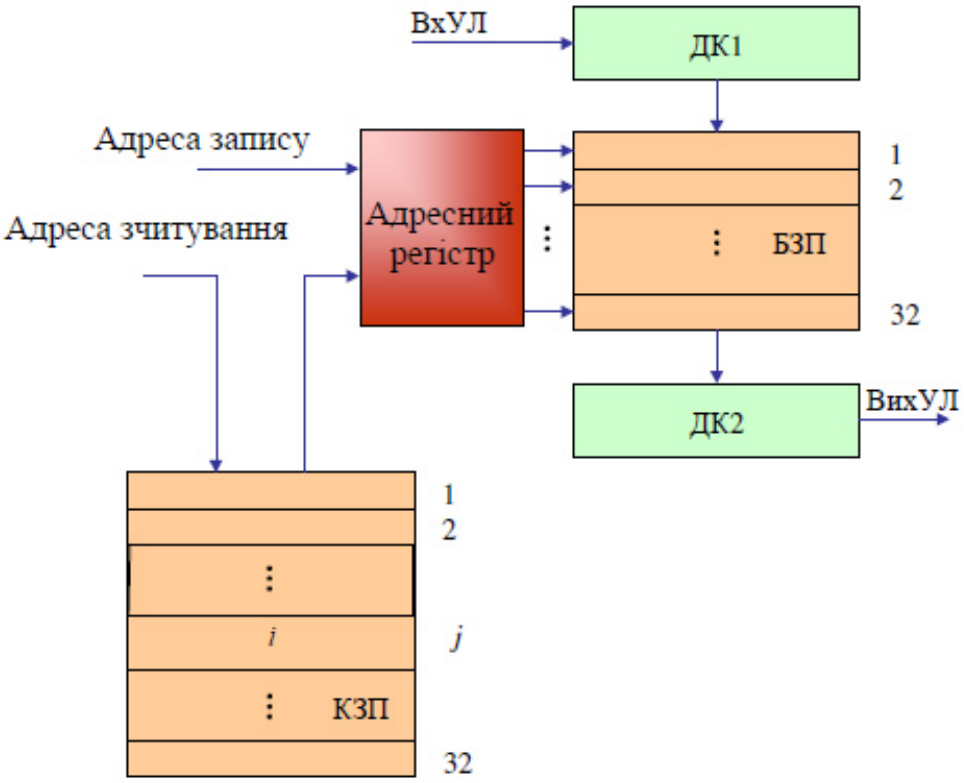


Рисунок 50 – Комутаційний блок з тимчасовою комутацією

Зчитування вибірок здійснюється за допомогою управляючого запам'ятовуючого пристрою (КЗП). У ньому на етапі налаштування зв'язку за допомогою службових сигналів записується інформація в номерах вихідних часових каналів, з якими повинні бути скомутовані послідовно вхідні часові канали.

Якщо вхідний канал і комутується з вихідним каналом і, то в j – у комірку КЗП записується число і. У другій фазі тайм-слоту з номером і подається сигнал адреси зчитування і з комірки і КЗП вибирається число і. Воно розміщується в адресний регістр, у результаті чого вміст комірки з номером і з

БЗП зчитується у допоміжну комірку ДК2. З ДК2 кодова комбінація побітово передається в канал ВихУЛ.

7.3 Технологія ISDN

Традиційна комутація каналів з часовим розподіленням є дуже негнучкою процедурою, так як тривалість тайм-слоту однозначно визначає швидкість передавання в каналі зв'язку. У технології ISDN зроблено першу реальну спробу безпосередньо надати послуги передавання не тільки голосової, а й відеоінформації та даних кінцевим користувачам у єдиній цифрової мережі.

Цифрова мережа інтегрального обслуговування ISDN (Integrated Services Digital Network) є інтегрованою системою зв'язку з різноманітним комплексом послуг. Вимоги різних служб до швидкості передавання різні – від дуже низьких (1 кбіт/с – для телеметрії) до надвисоких (140 Мбіт/с – TV високої чіткості). Для задоволення цих вимог було розроблено варіант поєднання комутації каналів з мультиплексуванням, який забезпечує широкий діапазон швидкостей передавання даних.

У системі передавання з високошвидкісною комутацією каналів використовується той самий метод часового мультиплексування, що й у системі зі звичайною комутацією каналів. Проте в одному з'єднанні (широкосмуговому каналі) може використовуватися п (п > 1) цифрових каналів Б80 (64 кбіт/с). Отже, кожне під'єднання може бути кратним швидкості 64 кбіт/с.

Системи комутації, які забезпечують багатошвидкісну комутацію каналів, є більш складними в порівнянні з системами зі звичайною комутацією цифрових каналів, так як всі канали окремих з'єднувальних ланок є синхронними.

Важливою *проблемою для систем з багатошвидкісною комутацією каналів є вибір базової швидкості передавання*.

ITU-T визначив основними два інтерфейси доступу до ISDN:

– базовий доступ (Basic Rate Acces) 144 кбіт/с, який забезпечує два мовленнєвих канали типу В зі швидкістю 64 кбіт/с і один сигнальний канал типу D зі швидкістю передавання 16 кбіт/с (2 В +D);

– первинний доступ PRA (Pгimaгy Rate Acces), який дає змогу працювати з каналами Т1 (1,5 Мбіт/с) і Е1 (2 Мбіт/с), які розділено на 23 і 30 каналів типу В відповідно, і, крім цього, мають один сигнальний D канал зі швидкістю 64 кбіт/с (23В + D або 30В +D).

Виділена лінія може використовувати як окремий канал В, так і їх комбінацію для досягнення збільшення швидкості. Як налаштування, так і роз'єднання зв'язку між абонентами здійснюються через сигнальний канал і відбуваються майже миттєво.

Обрана швидкість каналу має дорівнювати або перевищувати пікову швидкість передавання джерела під час усього сеансу зв'язку, хоча середня

швидкість передавання може бути дуже низькою. Це принципово важливо для передавання мовлення, а особливо – відео.

Зміна швидкості передавання у даному випадку характеризується *вибуховим (пачковим) режимом роботи джерела*, на відміну від рівномірного, так званого ізохронного потоку28.

Таким чином, вибуховий трафік не забезпечує ефективне використання пропускної здатності каналу навіть у процесі багатошвидкісної комутації каналів.

Цифрові мережі ISDN виникли як альтернатива традиційним аналоговим мережам із застосуванням модемів, виділених ліній, іншим службам глобальних мереж. Маючи значно більшу гнучкість у порівнянні з простою комутацією каналів, технології ISDN все ж зберігають фундаментальне обмеження: хоча користувач має можливість вибору швидкості передавання, сам набір швидкостей залишається цілком визначеним (фіксованим).

Системи комутації, розроблені для багатошвидкісної комутації каналів, складаються з набору окремих комутаторів, кожен із яких здійснює комутацію каналів з певною швидкістю. Інформація з абонентської лінії до надходження на різні комутатори демультиплексується, а інформація від комутатора до абонентського лінії, навпаки, мультиплексується.

Незважаючи на всі переваги технології ISDN, мережеві ресурси продовжують використовуватися неефективно. Так, наприклад, якщо всі низькошвидкісні комутатори зайнято, то додаткове низькошвидкісне під’єднання не відбудеться, незважаючи на те, що високошвидкісні комутатори у цей час є вільними.

Отже, телекомунікаційна технологія є одним з основних факторів, який характеризує телекомунікаційну мережу з точки зору можливостей з транспортування інформації.

7.4 Технології асинхронного режиму перенесення

7.4.1 Принцип комутації пакетів

Низька ефективність використання каналів у мережі з комутацією каналів пояснюється тим, що після налаштування з’єднання між кінцевими пристроями ресурс (пропускна здатність) скомутованого каналу та його складових частин на час сеансу зв’язку є недоступним для інших застосувань, навіть у тому випадку, коли дані тимчасово не передаються.

Використовуючи такі телекомунікаційні мережі для передавання даних між комп’ютерами, виявлено, принаймні, два недоліки: з’єднання типу термінал-хост (наприклад, у процесі взаємодії ПК користувача з мережевим комп’ютером) звільняє канал на значний час, але телекомунікаційна мережа не може використовувати його в цей час для іншого застосування; мережа з комутацією каналів забезпечує передавання даних з постійною швидкістю. Це

означає, що будь-*якій парі термінал-хост надано однакову фіксовану швидкість, що обмежує можливості мережі для під'єднання хостів і терміналів різної продуктивності.*

Упровадження телекомунікаційної мережі з асинхронним режимом перенесення може усунути ці недоліки шляхом використання так званого естафетного способу передавання повідомлень (або його частин) від вузла до вузла за маршрутом перенесення інформації в мережі. При цьому не потрібно жорсткого закріплення ресурсів ліній зв'язку, через які проходить маршрут.

Комп'ютерні повідомлення (дані), згідно зі стеком протоколів моделі OSI/ISO, розподіляються на невеликі блоки, які, досягаючи мережевого рівня, перетворюються на пакети, отримуючи заголовок Зп, який містить адреси джерела й споживача інформації, номер блоку в повідомленні та вказівку на його приналежність до даних повідомлень (рис. 51).

Перед відправленням у лінію пакет оформлюються у вигляді фрейму. Фрейм – це сегмент повідомлення із заголовками канального рівня. Таке формування прийнято ще називати кадром. Заголовок кадру ЗФ, містить інформацію, яка використовується для ідентифікації адреси порту призначення кадру (фрейму).

Для того, щоб на приймальному кінці лінії зв'язку відокремити один фрейм від іншого у процесі побітового передавання їх каналом, між фреймами вставляються розділові прапори.

Прапор (Ф) – це поле, яке містить 8 біт, наприклад, 01111110. На приймальному вузлі прийнята послідовність бітів групується у фреймі, прапори видаляються, а з фрейму витягується пакет. Він розміщується в запам'ятовуючий пристрій (ЗП) вузла та обробляється: перевіряється на відсутність помилок та перекручень. У разі виявлення помилок і неможливості їх виправити, приймальний вузол повторює передавання фрейму.

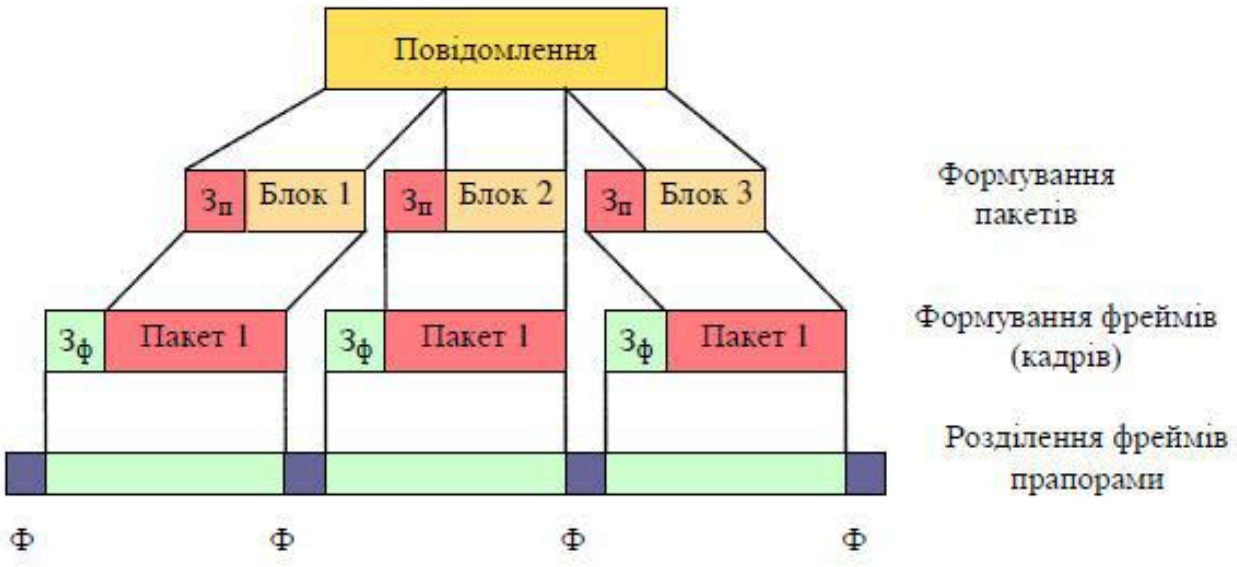


Рисунок 51 – Передавання повідомлення пакетами

Вилучений з ЗП пакет відповідно до таблиці адрес, збереженої на вузлі комутації, прямує у вихідну лінію та оформлюється в новий фрейм. Таким естафетним способом сегмент інформаційного повідомлення передається мережею до вузла призначення (вхідного вузла).

На вхідному вузлі пакети накопичуються, з них витягуються сегменти, з яких далі збираються повідомлення. Таким чином, *функція розбиття повідомлення на сегменти здійснюється на вихідному вузлі, а збирання – на вхідному.*

Незважаючи на те, що лініями зв'язку пакети передаються у вигляді фреймів (кадрів), у проміжних вузлах відбувається комутація саме пакетів. Тому такий *метод комутації у вузлах мережі отримав назву комутація пакетів*, а мережі, відповідно, *– з комутацією пакетів*.

Комутація пакетів (КП) має кілька переваг над комутацією каналів (КК):

– ефективність використання ліній при КП є набагато вищою, оскільки ресурси ліній та вузлів мережі можуть динамічно розподілятися між багатьма пакетами від різних застосувань;

– у мережі з комутацією пакетів може здійснюватися перетворення швидкості передавання даних. Це дає змогу обмінюватися повідомленнями абонентських пунктів, під'єднаних до мережі каналами різної пропускної здатності (смуги пропускання);

– користувачам гарантовано під'єднання навіть, якщо мережу перевантажено. При цьому лише можуть виникнути затримки з доставкою пакетів або зменшення швидкості передавання;

– у мережах з КП можна використовувати систему пріоритетів. Пакети з високим пріоритетом доставлятимуться з меншими затримками.

7.4.2 Способи передавання пакетів у телекомунікаційній мережі

Передавання пакетів між вузлами телекомунікаційної мережі можна реалізувати по-різному, а саме:

– за допомогою датаграм;

– з використанням віртуального виклику;

– з використанням віртуального каналу;

– з використанням віртуального зєднання.

Датаграмний спосіб полягає у тому, що кожен пакет рухається мережею самостійно, без урахування того, як просуваються пакети, які йдуть до або після нього. Кожен вузол комутації (ВК), на основі адресної інформації полів заголовка пакета й власних відомостей про наявність незайнятих вихідних каналів, до сусідніх ВК вибирає наступний ВК, на який спрямовується пакет.

У результаті пакети одного й того ж повідомлення з однією й тією ж адресою можуть слідувати від місця відправлення до місця призначення різними маршрутами й прийти у переплутаному порядку (рис. 52 а).

Вхідний ВК (кінцевий вузол маршруту) відновлює правильну послідовність пакетів і вже в цій послідовності передає їх до пункту призначення.

Використання віртуального виклику. Особливістю є те, що датаграмний спосіб доповнюється віртуальним викликом. Попередньою до фази передавання пакетів повідомлення є фаза посилки службового пакету в АП одержувача із зазначенням повного обсягу повідомлення для того, щоб зарезервувати достатній буферу пам’яті для його прийому.

Після резервування пам’яті в АП у зворотний бік надсилається службовий пакет з підтвердженням про готовність до прийому повідомлення. Сеанс передавання пакетів розпочинається лише після отримання пакету про підтвердження прийому.

Обмін службовими пакетами перед сеансом передавання повідомлення називається посилкою віртуального виклику.

Спосіб віртуального виклику зменшує ймовірність блокування роботи окремих вузлів комутації (ВК) і, отже, ймовірність виникнення безвихідних ситуацій у мережі, які гальмують проходження датаграм, а також додаткових витрат часу на посилку віртуального виклику.

Використання віртуального каналу. Цей спосіб характеризується тим, що фазі передавання пакетів повідомлення від одного АП до іншого АП передує фаза налаштування логічного з’єднання між ними, яке називається віртуальним каналом (рис. 52б).

Фаза налаштування віртуального каналу містить обмін службовими пакетами, при якому, як і в попередньому способі, здійснюється резервування пам’яті для прийому повідомлення в АП одержувача, а також визначається фіксований маршрут прямування мережею пакетів переданого повідомлення. Кожен пакет забезпечується ідентифікатором віртуального каналу, який розміщується в поле заголовка.

Проміжні ВК, через які проходить маршрут віртуального каналу, у даній ситуації не приймають самостійних рішень щодо маршрутизації пакетів, а спрямовують пакети згідно з ідентифікаторами віртуального каналу. Оскільки пакети рухаються за фіксованим маршрутом, то, у випадку зайнятості вихідного напрямку, вони затримуються в ВК і накопичуються у вихідних буферах.

Якщо вихідний буфер переповнюється, виникає блокування ВК. Блокування можуть викликати неприпустимі затримки пакетів у мережі, а також безвихідну ситуацію, яка зупиняє роботу всієї мережі. Цей недолік усувається за допомогою організації віртуального з’єднання, в якому забезпечується резервування ресурсів пам'яті в усіх проміжних ВК маршрутом проходження пакетів переданого повідомлення.

Використання віртуального з’єднання. Спосіб характеризується тим, що в фазі налаштування віртуального каналу здійснюється резервування буферів до ЗП ВК, які входять у маршрут передавання пакетів, достатніх для проходження пакетів без затримок (рис. 52в).

Цей спосіб є подібним за принципом налаштування зв’язку до методу комутації каналів проходження датаграм, а також додаткових витрат часу на посилку віртуального виклику.

Використання віртуального каналу. Цей спосіб характеризується тим, що фазі передавання пакетів повідомлення від одного АП до іншого АП передує фаза налаштування логічного з’єднання між ними, яке називається віртуальним каналом (рис. 43б). Фаза налаштування віртуального каналу містить обмін службовими пакетами, при якому, як і в попередньому способі, здійснюється резервування пам’яті для прийому повідомлення в АП одержувача, а також визначається фіксований маршрут прямування мережею пакетів переданого повідомлення. Кожен пакет забезпечується ідентифікатором віртуального каналу, який розміщується в поле заголовка.

Проміжні ВК, через які проходить маршрут віртуального каналу, у даній ситуації не приймають самостійних рішень щодо маршрутизації пакетів, а спрямовують пакети згідно з ідентифікаторами віртуального каналу. Оскільки пакети рухаються за фіксованим маршрутом, то, у випадку зайнятості вихідного напрямку, вони затримуються в ВК і накопичуються у вихідних буферах.

Якщо вихідний буфер переповнюється, виникає блокування ВК. Блокування можуть викликати неприпустимі затримки пакетів у мережі, а також безвихідну ситуацію, яка зупиняє роботу всієї мережі. Цей недолік усувається за допомогою організації віртуального з’єднання, в якому забезпечується резервування ресурсів пам'яті в усіх проміжних ВК маршрутом проходження пакетів переданого повідомлення.

Використання віртуального з’єднання. Спосіб характеризується тим, що в фазі налаштування віртуального каналу здійснюється резервування буферів до ЗП ВК, які входять у маршрут передавання пакетів, достатніх для проходження пакетів без затримок (рис. 43в).

Цей спосіб є подібним за принципом налаштування зв’язку до методу комутації каналів (КК). Якщо налаштування зв’язку супроводжуватиметься резервуванням тайм-слотів у транзитних лініях, то відмінність від КК полягатиме лише в розмірі пакета та способі коректування помилок (при КК це робиться на вхідному ВК, а при КП – на всіх ВК, які складають маршрут віртуального каналу).

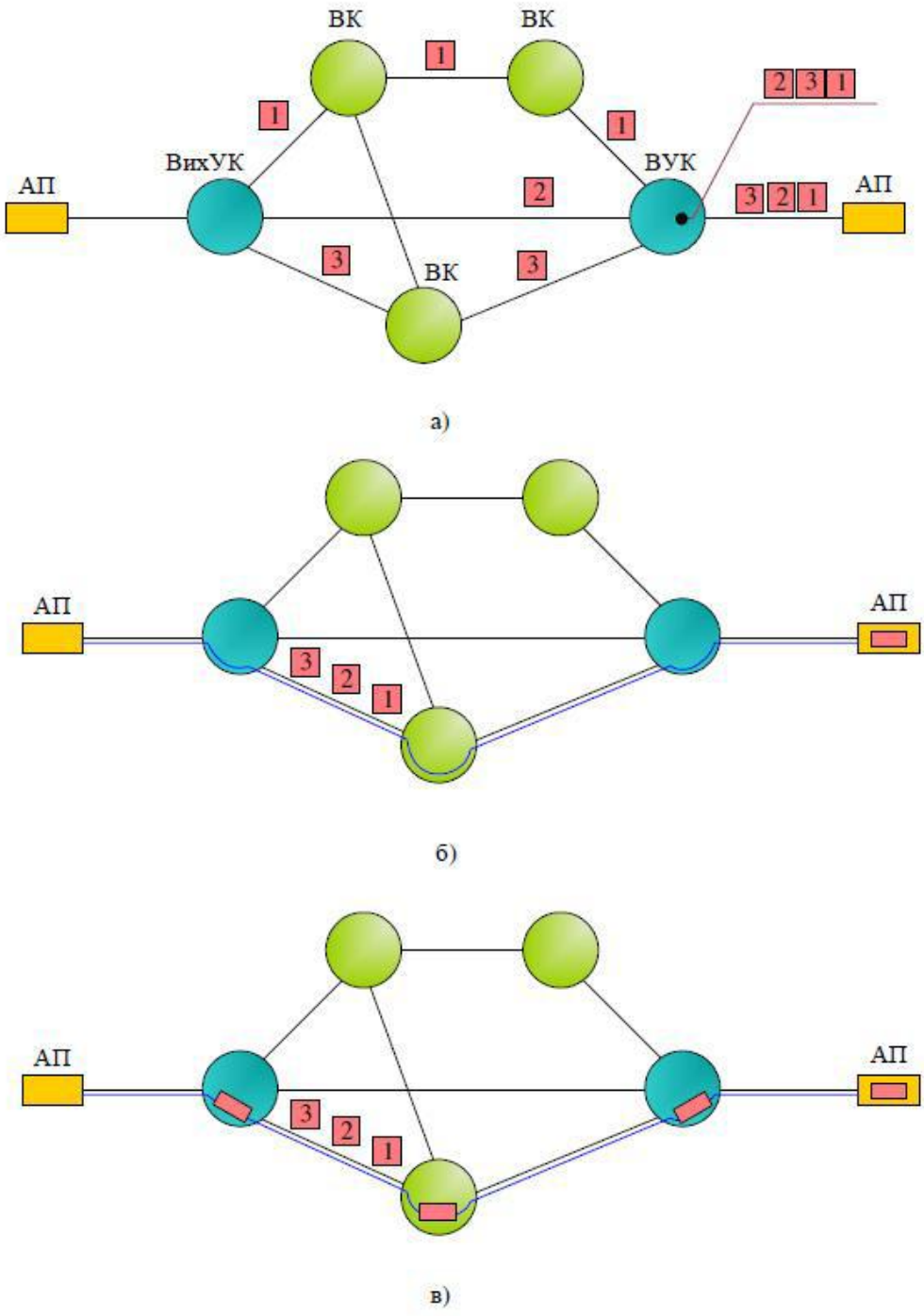


Рисунок 52. Способи комутації пакетів: а – датаграмний; б – віртуального каналу; в – віртуального з’єднання

7.5 Технологія X.25

Міжнародна організація зі стандартизації (ISO) та IU-T уперше затвердили метод передавання й комутації пакетів у вигляді Рекомендацій X.25. Зазначений метод (протокол) дістав назву технологія X.25. Крім пакету розміром 128 байт, який приймається усталено, допускаються також інші розміри пакету: 16, 32, 256, 512, 1024, 2048, 4096 байт. Крім довжин пакетів,

рекомендовано також формати пакетів і кадрів (фреймів), а також протокол їх передавання та приймання.

Технологія X.25 – це технологія передавання даних з комутацією пакетів, яка дає змогу вирішувати проблеми «поганих» каналів зв'язку з великим рівнем перешкод, якими, наприклад, є аналогові телефонні лінії.

Для забезпечення необхідної достовірності передавання інформації в технології X.25 упроваджено багаторівневу систему виявлення й коректування помилок. Кожен ВК мережі X.25 на шляху руху пакета перевіряє цілісність пакету, читає контрольну суму, розміщену в заголовку пакету, обчислює її нове значення й порівнює їх.

Якщо кількість помилок є незначною, ВК здатний відновити пакет і передати його далі. При цьому вузол надсилає підтвердження попереднього вузла про коректний прийом пакету. Якщо ж відновити пакет неможливо, робиться запит про його повторне передавання.

Розбиття повідомлення на пакети й складання повідомлення з пакетів в технології X.25 прийнято називати *функцією розбиття/збірки* (Packet Assembler and Disassembler, PAD). Функція PAD може виконуватися в будь-якому мережевому пристрої або вузлі, який забезпечує доступ до мережі X.25. Слід зазначити, що якщо джерелом повідомлення є ЕОМ (робоча станція), функція PAD може виконуватися безпосередньо в ній.

Високий рівень перешкод на лініях призводить до зменшення швидкості передавання, а тому гранична швидкість передавання в мережах X.25 складає 64 кбіт/с. Крім того, ця швидкість не залишається постійною величиною й залежить від рівня перешкод і викликаних ними помилок.

Метод передавання й комутації пакетів реалізовано не тільки в протоколі X.25, але і, наприклад, у стеку протоколів TCP/IP, який вперше застосовано також у мережі АКРА29. Надалі АКРА перетворилась в Інтернет.

7.5.1 Особливості формування пакетів мовних повідомлень

Мовних повідомлення, подане в цифровій формі (ІКМ сигнал), є послідовністю байтів (вибірок дискретних відліків амплітуд), які в часовому каналі йдуть один за одним через 125 мкс. Особливість реалізації функції PAD при цьому полягає в тому, що, формуючи блок, довжина якого більша від одного байта, необхідно накопичити потрібну кількість байтів. У цьому випадку відбувається затримка всіх байтів, які містить пакет, окрім останнього (рис. 53), на час = 125(n – *1*) мкс, де п – кількість байтів у блоці. Перехід до пакета та трафіку залишається тим же.

На приймальному кінці (вхідного ВК) для правильного відновлення повідомлення відбувається перетворення в *ІКМ*-сигнал з відповідним рознесенням у часі окремих байтів. Крім того, здійснюється узгодження в часі байтів різних блоків. Очевидно, що наявність часових затримань у процесі

передавання й отримання пакетів може суттєво спотворити мовних повідомлення.

Щоб запобігти цьому, для передавання мовлення пакетами необхідно використовувати високошвидкісні канали, в яких мовленнєві пакети передаватимуться пріоритетно серед інших даних.

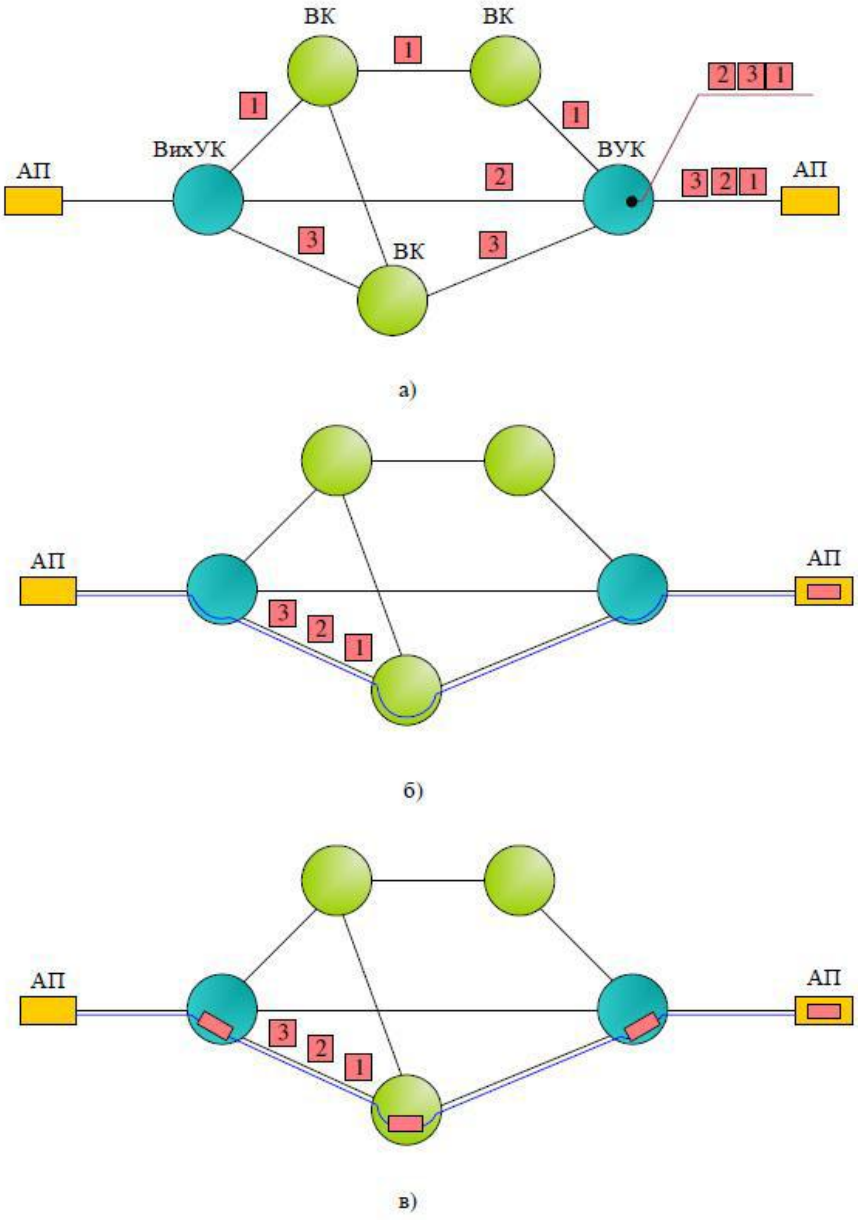


Рисунок 53 – Формування пакета мовленнєвого сигналу:
К1, К2, К3 – кадри

7.6 Технологія ретрансляції фреймів (Frame Relay)

У швидкісних телекомунікаційних мережах, які використовують волоконно-оптичне середовище для передавання даних, рівень помилок є набагато нижчим, порівняно з каналами аналогової телефонії. Тому надмірність

кодування (застосування складних кодів для виявлення й виправлення помилок) пакетів стає непотрібною, спрощується система заголовків, якою була перенасичена обсягами інформації для відновлення пакетів.

У 90-х рр. ITU-T затверджує новий протокол із сімейства протоколів X.25, який отримав назву протоколу ретрансляції фреймів (кадрів) – (Frame Relay, FR).

У цьому протоколі немає тієї надмірності, яка була характерною для протоколу X.25, по-перше, тому, що він спеціально розроблявся для використання на лініях зв'язку з низьким рівнем перешкод, по-друге, в ньому усунуто систему контролю помилок всього фрейму. Замість цього лише перевіряється цілісність отриманого фрейму, й тільки для адресного поля здійснюється контроль помилок. Завдяки всьому цьому Frame Relay забезпечує під'єднання користувачів до телекомунікаційної мережі на швидкості 2 Мбіт/с і вищій. Основною перевагою технології Frame Relay стала низька надлишковість службової інформації в пакеті, що помітно збільшило продуктивність передавання даних у мережі. За іншими критеріями протокол Frame Relay є подібним до протоколу X.25.

Розміри фреймів можуть мати змінну довжину, оскільки самі пакети допускають використання різних довжин і, як наслідок, варіації затримок у процесі передавання фреймів. Це не зовсім прийнятно для передавання мовленнєвих та відеоповідомлень, які вимагають регулярних швидкостей.

Сферою більш ефективного застосування технології Frame Relay є взаємодія локальних мереж LAN через глобальні телекомунікаційні мережі, а також забезпечення високошвидкісних користувальницьких інтерфейсів UNI. Оскільки Frame Relay є різновидом протоколів X.25, він добре поєднується з мережами X.25. Передавання фреймів мережею уможливлюється завдяки використанню віртуального каналу, віртуального під'єднання, а також датаграмного режиму.

З метою керування потоками фреймів у перевантажених мережах, на мережах FR застосовується система так званих «кредитів». Кредит CIR (Committed Intormation Rate) видається користувачеві, та є своєрідним дозволом на передавання даних зі швидкістю, яка не перевищує вказану. При цьому CIR, який вимірюється в кілобітах на секунду, визначається термінами дозволеного обсягу даних B, який можна надіслати користувачем у мережу за час T: CIR = B/T.Значення CIR є середнім гарантованим мережею значенням швидкості передавання даних за умови неперевантажень мережі. Кредит СІК видає адміністрація мережі, він може бути однаковим для всіх користувачів або враховувати запит конкретного користувача.

7.6.1 Передавання й комутація комірок. Технологія ATM

Технологія ATM (Asynchronous Transfer Mode) є провідною у порівнянні з розглянутими вище пакетними технологіями. Дану технологію ще називають

асинхронним режимом перенесення, що закріплено рекомендаціями ІТГ-Т. На сьогодні АТМ є єдиною технологією, яка дає змогу повноцінно передавати інтегральний трафік (голос, відео, дані), одночасно задовольняючи абсолютно несумісні вимоги до умов передавання.

Сутність технології АТМ полягає в транспортуванні всіх видів інформації пакетами фіксованої довжини в 53 байта, з яких 48 байтів визначають розмір інформаційного поля, а 5 байтів відводиться для заголовка. Такий пакет отримав назву комірка (cell).

Комірки передаються без додаткового оформлення в кадр (фрейм), а для їх обробляння використовують більш прості протоколи, на відміну від передавання пакетами за протоколом Х.25. Крім того, фіксована довжина й регулярність створюваного ними потоку не вимагають використання прапора між ними для відокремлення однієї комірки від іншої. Комірки фіксованої довжини передаються каналом безперервно.

У тому випадку, коли інформаційні комірки відсутні, каналом передаються порожні комірки стандартної величини, тобто комірки, які не містять даних у полі інформації, що зазначено в заголовку. Порожні комірки необхідно передавати для того, щоб не порушити покоміркову дискретизацію в каналі.

Покоміркова дискретизація нагадує часову дискретизацію в синхронному режимі передавання. Однак, якщо у синхронному режимі тривалість тайм-слоту (часового каналу) залежала від швидкості передавання бітів каналом, то в асинхронному режимі тривалість часу, витрачена для передавання комірки, залежить тільки від кількості бітів, необхідних для її передавання, але не від швидкості. Таким чином, за допомогою комірок здійснюється своєрідна часова дискретизація в каналі, у зв’язку з чим асинхронний режим передавання ще називають асинхронним часовим мультиплексуванням.

Відмінність асинхронного часового мультиплексування (АЧМ) від синхронного часового мультиплексування (СЧМ) полягає в тому, що комірки, які належать різним інформаційним повідомленням, можуть слідувати довільно, а тайм-слоти СЧМ для передавання різних повідомлень розташовуються на осі часу (в структурі кадру) в чітко фіксованому порядку відносно початку циклу дискретизації (початок кадру) (рис. 54).

Передавання комірок мережею здійснюється завдяки віртуальному з’єднанню, у зв’язку з чим фазі передавання передує фаза налаштування віртуального з’єднання, під час якої перевіряється достатність обсягу мережевих ресурсів як для якісного обслуговування вже наявних віртуальних з’єднань, так і для новостворюваного.

Якщо мережевих ресурсів недостатньо, налаштування з’єднання не відбудеться.

Таким чином, у мережі АТМ реалізується функція контролю й захисту від перевантажень.

Щоб зменшити часові затримання комірок у вузлах комутації, функції заголовка пакету АТМ обмежують. Основною функцією заголовка стає

ідентифікація віртуального з’єднання та забезпечення гарантії правильної маршрутизації. Заголовок також дає змогу мультиплексувати різні віртуальні з’єднання в одному цифровому тракті. Оскільки помилка в заголовку може призвести до неправильної маршрутизації, передбачено виявлення й виправлення помилок у заголовку пакету АТМ.

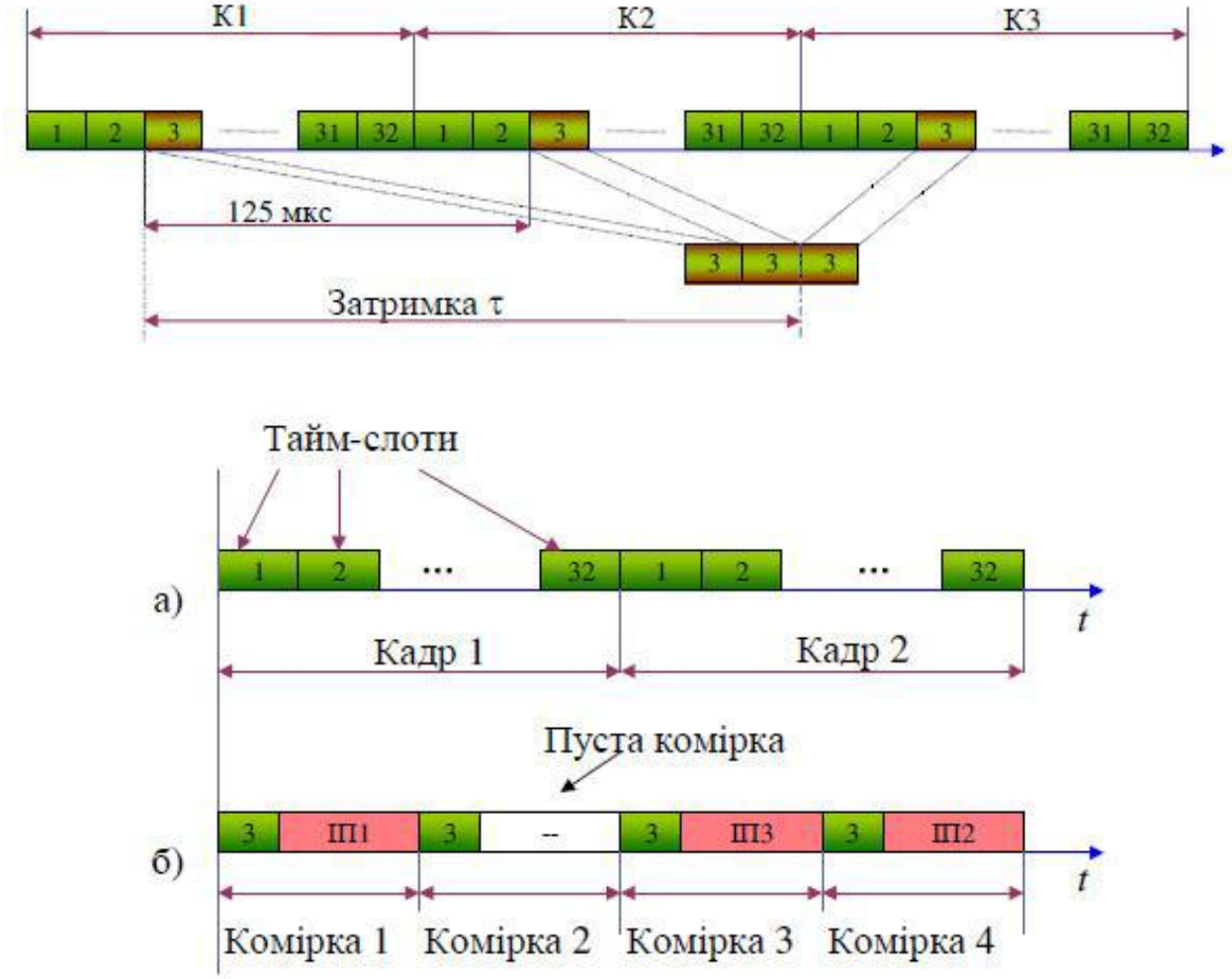


Рис. 54 – Принцип асинхронного мультиплексування:
а – синхронне мультиплексування; б – асинхронне мультиплексування;
ІП1, ІП2, ІП3 – інформаційні повідомлення

Передавання комірок мережею здійснюється завдяки віртуальному з’єднанню, у зв’язку з чим фазі передавання передує фаза налаштування віртуального з’єднання, під час якої перевіряється достатність обсягу мережевих ресурсів як для якісного обслуговування вже наявних віртуальних з’єднань, так і для новостворюваного.

Якщо мережевих ресурсів недостатньо, налаштування з’єднання не відбудеться.

Таким чином, у мережі АТМ реалізується функція контролю й захисту від перевантажень.

Щоб зменшити часові затримання комірок у вузлах комутації, функції заголовка пакету ATM обмежують. Основною функцією заголовка стає ідентифікація віртуального з'єднання та забезпечення гарантії правильної маршрутизації. Заголовок також дає змогу мультиплексувати різні віртуальні з'єднання в одному цифровому тракті. Оскільки помилка в заголовку може призвести до неправильної маршрутизації, передбачено виявлення й виправлення помилок у заголовку пакету ATM.

Через обмеження функцій, які виконує заголовок пакета ATM, його обробка є відносно простою процедурою й може здійснюватися на дуже високих швидкостях, що забезпечує незначне затримування комірок у чергах буферних пристроїв комутаторів ATM. Продуктивність комутаторів ATM досягає 10 Гбіт/с. Якщо мережевих ресурсів недостатньо, налаштування з'єднання не відбудеться.

Комутатори ATM є основними пристроями мережі ATM, основними функціями яких є: налаштування віртуального з'єднання між кінцевими пристроями користувачів; забезпечення так званого режиму якісного обслуговування (Quality of Service, QoS) для цього з'єднання.

Параметри режиму QoS задають користувачі в заявці на під'єднання в фазі формування віртуального з'єднання.

У рекомендаціях ITU-T передбачено такі типи QoS:

– CBR (Constant Bit Rate) – виокремлення каналу з фіксованою пропускною здатністю, гранично допустимим затримуванням та іншими характеристиками, замовленими користувачем. Такий вид QoS в основному використовують для передавання мовлення;

– RT-VBR (Real Time Variable Bit Rate) – виокремлення каналу з пропускною здатністю в заданих межах (min-max) з жорсткими вимогами до затримування та іншими параметрами, замовленими користувачем;

– RT-VBR є ідеальним для передавання відео й мовлення;

– NRT-VBR (Not Real Time Variable Bit Rate) – VBR з послабленими вимогами до затримування у передаванні – застосовується для відео та мовлення, які не потребують режиму реального часу;

– ABR (Availeble Bit Rate) – надання користувачеві залишково вільної частини фізичного каналу. Підключаючись, користувач встановлює лише межі допустимих змін швидкості передавання. Величина затримувань є контрольованою. Даний режим застосовують для передавання даних; UBR (Unspecified Bit Rate) – найбільш низькопріоритетний режим передавання, особливість якого в тому, що надається для користування певний канал без будь-яких гарантій якості передавання; UBR+ – модифікований UBR, який передбачає припинення передавання комірок повідомлення у разі виникненні перевантаження мережі. Застосування UBR+ дає змогу розвантажити фізичні канали.

Забезпечення режиму QoS принципово відрізняє технологію ATM від усіх наявних мережевих технологій. Особливого значення вона набуває в процесі інтегрування даних відео й мовлення, надзвичайно чутливих до

затримування під час передавання. Єдиним протоколом, який забезпечує QoS у комутаторах ATM, є протокол PNNT Phase 1.0 (Private Network – to – Network Interface). Протокол досить складний, для його роботи потрібно вдесятеро більше процесорного часу, ніж для відомого протоколу визначення найкоротшого шляху (OSPF), який використовується в маршрутизаторах.

ЛЕКЦІЯ 8. МЕРЕЖЕВІ КОНЦЕПЦІЇ. ДИНАМІКА РОЗВИТКУ МЕРЕЖ

План

Вступ
1. Концепція Єдиної автоматизованої мережі зв'язку.
2. Концепція цифрової мережі інтегрального обслуговування ISDN.
3. Концепція інтелектуальної мережі (IN).
4. Основні тенденції розвитку телекомунікацій.
5. Мережі абонентського проводового і доступу.
6. Технології та обладнання цифрової абонентської лінії.
7. Мережі абонентського безпроводового доступу.
8. Мережі мобільного доступу.
9. Узагальнена архітектура та модель мережі доступу.
10. Ієрархія мереж доступу.

Висновки

Література

1. Теоретичні основи телекомунікаційних мереж : навч. посіб. /М.М. Климаш, Б.М.Стрихалюк, М.В.Кайдан. – Львів : вид-во УАД, 2011. – 496 с.
2. Буров Є. Комп'ютерні мережі / Є.Буров. – Львів : БаК, 1999. – 468 с.
3. Управління телекомунікаціями із застосуванням новітніх технологій / Кривуца В. Г., Беркман Л. Н., Стеклов В. К. та ін.]. – К.: Техніка, 2007. – 384 с.

Вступ

Концепція побудови мережі відтворює систему поглядів на те, як повинна функціонувати мережа зв'язку, яка задовольняє певні потреби користувачів, і уявлення про те, як це можна практично реалізувати. Формування певної мережевої концепції ґрунтується, насамперед, на конкретизації переліку функцій, виконання яких передбачено в мережі, способі їх поєднання й групування в функціональні модулі та способі реалізації цих функціональних модулів (програмний, апаратний, програмно-апаратний). З'ясовуючи перспективи впровадження тієї чи іншої мережевої концепції, враховують

рівень науково-технічного прогресу в суспільстві, якість розробок телекомунікаційних технологій та потреби суспільства в певному наборі послуг зв'язку.

8.1 Концепція Єдиної автоматизованої мережі зв'язку (ЄАМЗ)

Особливістю початкового етапу розвитку мереж зв'язку, як глобальних об'єктів, є побудова окремих мереж для кожного виду інформації, яку необхідно було передати.

Помітний прогрес у розвитку технічних засобів доставки різних видів інформації надала концепція *Єдиної Автоматизованої мережі зв'язку* (ЄАМЗ), яка виникла на початку 90-х років минулого століття, основною ідеєю якої стало об'єднання мереж, структурно й функціонально відмінних і призначених для передавання різної інформації, у єдину мережу зв'язку, побудовану з максимальним використанням спільних систем передавання й розподілення інформації. Доцільність злиття мереж електрозв'язку було зумовлено також стрімким прогресом у сфері систем комутації, спрямованому на об'єднання комутаційних станцій різного призначення в єдині системи комутації зі спільним керуванням.

Концепція ЄАМЗ ґрунтувалася на виокремленні сукупності мережевих вузлів, мережевих станцій та ліній передавання, які утворюють мережу типових каналів передавання та типових лінійних трактів – первинну мережу ЄАМЗ. Ця мережа з відповідними пристроями керування й експлуатацією стала своєрідним «кістяком» загальної мережі, типові канали якої виділялися для створення різних, так званих, вторинних мереж. Вторинні мережі розділялись за типом інформації, що передавалася, та відомчої приналежності.

У межах сформульованої концепції до складу ЄАМЗ входять наступні вторинні мережі:

– телефонного зв'язку загального користування (ТфЗК), яку одночасно можна використовувати для передавання даних, факсимільної передачі, повільного відеотелефона;

– телеграфного зв'язку загального користування (ТлгЗК) між підприємствами зв'язку;

– абонентського телеграфу між підприємствами та установами;

– загальнодержавної мережі передавання даних;

– передавання програм телемовлення;

– фототелеграфного передавання газет;

– факсимільного зв'язку;

– різних відомств.

Концепція ЄАМЗ ґрунтувалася на виокремленні сукупності мережевих вузлів, мережевих станцій та ліній передавання, які утворюють мережу типових каналів передавання та типових лінійних трактів – первинну мережу ЄАМЗ. Ця мережа з відповідними пристроями керування й експлуатацією стала

своєрідним «кістяком» загальної мережі, типові канали якої виділялися для створення різних, так званих, *вторинних мереж*. Вторинні мережі розділялись за типом інформації, що передавалася, та відомчої приналежності.

У межах сформульованої концепції до складу ЄАМЗ входять наступні вторинні мережі:

– можна використовувати для передавання даних, факсимільної передачі, повільного відеотелефона;

– телеграфного зв'язку загального користування (ТлгЗК) між підприємствами зв'язку;

– абонентського телеграфу між підприємствами та установами; загальнодержавної мережі передавання даних;

– передавання програм телемовлення;

– фототелеграфного передавання газет;

– факсимільного зв'язку; різних відомств.

На базі первинної мережі ЄАМЗ, заснованої на аналогових системах передавання з частотним розподілом каналів, можна було утворювати також широкосмугові канали для звукового мовлення та звукового супроводу програм телебачення та ін.

Створення єдиної універсальної інтегрованої та уніфікованої мережі зв'язку залишається одним з пріоритетних завдань і саме концепцією ЄАМЗ вважають першим кроком у цьому важливому напрямку.

8.2 Концепція цифрової мережі інтегрального обслуговування ISDN

Поява програмно-керованих електронних АТС, систем ІКМ з часовим розподілом каналів (ЧПК), а також перехід до наскрізних цифрових трактів передавання в мережі з кінця в кінець дало змогу створити *інтегровані цифрові мережі зв'язку*, якими розпочато другий – цифровий етап розвитку телекомунікаційних мереж. *Інтеграція комутаційного* й *каналоутворювального обладнання* визначили концептуальну сутність цифрової інтегрованої мережі.

Розробка методу комутації пакетів і створення перших мереж ЕОМ з пакетною комутацією уможливили появу гібридних мереж, у яких інтегровано метод комутації каналів (КК) і метод комутації пакетів (КП).

Гібридні та інтегровані цифрові мережі забезпечили на початку 80-х років минулого століття перехід до *цифрової мережі інтегрального обслуговування*. ITU-T в Рекомендації I.112 подано таке визначення цієї мережі: «*ISDN – це мережа, яка забезпечує надання декількох різних видів обслуговування зв'язком і передбачає цифрові з'єднання між інтерфейсами користувач-мережа*».

У ISDN на основі єдиних принципів побудови й функціонування інтегровано не тільки комутаційне й передавальне обладнання, а й різні типи переданої інформації (мова, дані і т.д.), методи комутації (КК, КП), різні види обслуговування (скорочений номер, зворотний виклик, переадресація виклику та ін.)

Користувачі ISDN отримали можливість позбутися незручностей, пов’язаних з необхідністю мати кілька абонентських ліній спеціалізованих вторинних мереж і декілька абонентських номерів одного й того ж абонентського пункту для передавання різних видів інформації.

Окрім однієї абонентської лінії й одного абонентського номера, очевидними перевагами ISDN є також: наявність багатофункціональних терміналів; потужна пакетна систему сигналізації № 7 (СС-7), яка забезпечує ефективне використання засобів зв’язку.

Відповідно до рекомендацій ITU-T ISDN поділяють на два види: вузькосмугові (Рекомендація I.120); широкосмугові (Рекомендація I.121).

N-ISDN – це такі мережі, в яких швидкість передавання від 64 Кбіт/с до 2,048 Мбіт/с, а

B-ISDN – такі, в яких використовують широкосмугові канали із швидкістю передавання понад 2 Мбіт/с.

8.2.1 Термінали ISDN. Еталонна конфігурація інтерфейсу «користувач-мережа»

Розрізняють два типи терміналів в ISDN:

– *термінальне обладнання типу 1* (TE1) – це спеціалізовані цифрові телефонні апарати, термінали ISDN (цифрування аналогового мовного сигналу відбувається безпосередньо в апараті). Термінали TE1 під’єднують до мережі ISDN через цифрову лінію зв’язку з чотирьох скручених пар проводів;

– *термінальне обладнання типу 2* (TE2) під’єднують до мережі ISDN через спеціальні термінальні адаптери.

На рис. 55 зображено еталонну конфігурацію інтерфейсу «користувач-мережа» (Рекомендація I.411), яка забезпечує під’єднання користувачів до мережі ISDN.

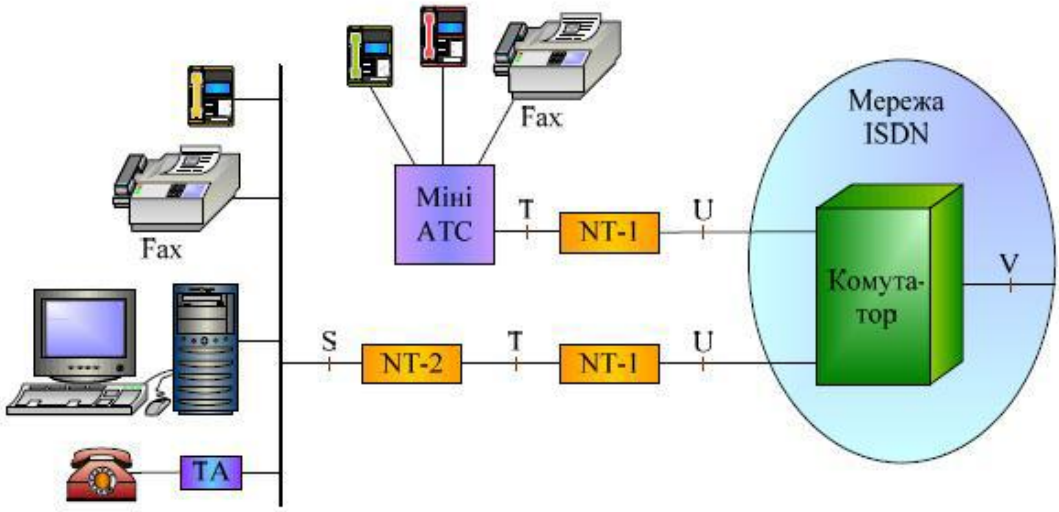


Рисунок 55 – Еталонна конфігурація інтерфейсу «користувач-мережа»

Вона складається з таких елементів, як термінальне обладнання (TE1 і TE2), термінальний адаптер (TA), кінцеве обладнання мережі (мережеві закінчення КТ1 і КТ2) та інтерфейсні еталонні точки (R, S, T, U, V).

Еталонна точка R забезпечує узгодження терміналу TE2 з термінальним адаптером (TA ISDN). Терміналами можуть бути аналоговий телефонний апарат, факсимільний, телетексний, відеотексний та інші апарати, а також персональні ЕОМ. TA ISDN може бути або автономним пристроєм, або платою всередині TE2. Якщо TE2 реалізовано як автономний пристрій, то він підєднується до TA через стандартний інтерфейс фізичного рівня.

Еталонна точка S реалізує взаємодію терміналу TE1 або TA ISDN, якщо даний термінал не є терміналом ISDN, і мережевого закінчення NT2. До однієї абонентської лінії ISDN можна під'єднувати (до чотирипроводової шини S на основі інтерфейсу S) до восьми терміналів. Уважають, що мережа починається з NT2. У NT2 виконуються функції другого та третього рівнів моделі OSI. Опції NT2 може здійснювати міні-АТС з функціями ISDN, яка обслуговує свої термінали. У цьому випадку вона відразу під'єднується до мережевого закінчення КТ1 через еталонну точку Т.

Еталонна точка T забезпечує взаємозв'язок NT2 з NT1, у якій реалізуються функції першого (фізичного) рівня моделі OSI. Фактично NT1 є пристроєм (лінійним терміналом), який утворює дуплексний канал з відповідним пристроєм, налаштованим на території оператора мережі.

Еталонна точка U забезпечує взаємозв'язок з абонентською лінією NT1, яка знаходиться на стороні абонента з аналогічним пристроєм на вході комутатора. U-інтерфейс (вита пара) призначено для роботи з віддаленим користувачами (до 4 - 7 кілометрів).

Еталонна точка V – це інтерфейс для з'єднання з іншими комутаторами. Цей інтерфейс цікавить тільки оператора мережі ISDN.

Основним призначенням N-ISDN є передавання телефонного трафіку. Тому за основу адреси ISDN було взято формат міжнародного телефонного плану номерів, описаного у Рекомендації E.163 (ITU-T). Для підтримки більшої кількості абонентів і для використання адрес інших мереж, наприклад X.25, формат було розширено. Стандарт адресації в мережах ISDN отримав номер E.164.

У мережах ISDN розрізняють номер абонента та адресу абонента. Номер абонента відповідає точці Т під'єднання всього призначеного для користувача устаткування до мережі. Наприклад, уся офісна МІНІ-АТС може ідентифікуватися одним номером ISDN.Номер ISDN складається з 15 десяткових цифр та містить, як і телефонний номер, за стандартом E.163 поле «Код країни» (від 1 до 3 цифр), поле «Код міста» і поле «Номер абонента». Адреса ISDN містить номер плюс до 40 цифр підадреси. Підадресу використовують для нумерації термінальних пристроїв за інтерфейсом користувачів, тобто під'єднаних до шинного інтерфейсу – точки S.

8.2.2 Еталонна конфігурація інтерфейсу «користувач-мережа»

Еталонну конфігурацію N-ISDN з невеликими змінами та доповненнями визнано також придатною для B-I8БК що закріплено Рекомендацією I. 413 (ITU-T).

Еталонну конфігурацію інтерфейсу «користувач- мережа» для B-ISDN наведено на рис. 56.

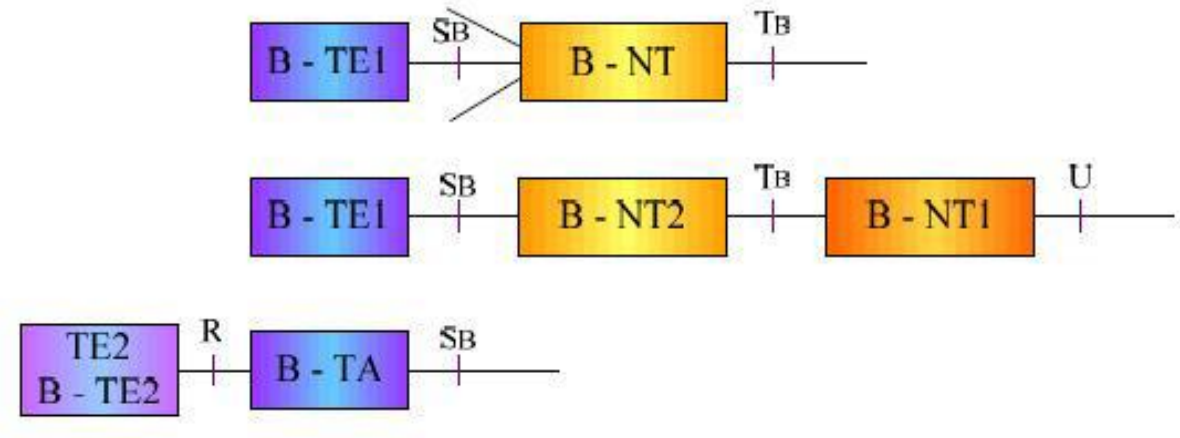


Рисунок 56 – Еталонна конфігурація інтерфейсу «користувач-мережа» для B- ISDN

Широкосмугові термінали B-TE1 під'єднують до широкосмугового мережевого закінчення B-NT, яке забезпечує під'єднання терміналів до мережі ATM, а також можливість спільного використання абонентської лінії декількома B-TE1.

Можливим є також поділ B-NT на два типи мережевих закінчень:

– B-TE1 – широкосмугове мережеве закінчення для під'єднання терміналів зі стандартним для B-ISDN інтерфейсом;

– B-TE2 – широкосмугове мережеве закінчення для під'єднання терміналів з нестандартним для B- ISDN інтерфейсом.

У B-ISDN виділяють, за аналогією до K-ISDN інтерфейсні еталонні точки доступу: K, SB, TB та еталонну точку доступу до широкосмугової абонентської лінії – UB.

У B-ISDN застосовують структуру під'єднання «зірка» за SB-інтерфейсом до мережевого закінчення B-NT.

Мережеве закінчення B-KT2 виконує функції як фізичного рівня, так і більш високих рівнів моделі OSI, основними серед яких є:

– адаптація до різних інтерфейсів фізичних середовищ (мідь, оптичне волокно) й топологій;

– мультиплексування або концентрація трафіку джерел;

– контроль параметрів користувача;

– керування протоколами сигналізації та ін.

Мережеве закінчення B-KT2 може бути відсутнім за умов, коли можливим є пряме з'єднання терміналу B-TE1 з широкосмуговим мережевим закінченням B-KT1. Еталонна точка TB є інтерфейсом між B-NT2 і B-NT1.

У комутаційній системі забезпечується комутація як широкосмугових, так і вузькосмугових каналів (для K-ISDN). Широкосмуговий доступ орієнтовано на стандартні швидкості передавання 155 Мбіт/с і 622 Мбіт/с. У еталонних точках SB і TB підтримуються всі види широкосмугового сервісу.

Сигнальна інформація та інформація користувачів передаються по окремих віртуальних каналах. Сигнальне повідомлення із запитом на налаштування віртуального каналу може додатково містити статистичні параметри потоку інформації, що передається та необхідну якість обслуговування.

8.2.3 Еталонна модель протоколів B-ISDN

Розбиття на рівні (рівнева архітектура) є центральною ідеєю створення будь-якої протокольної моделі і еталонної моделі протоколів B-ISDN зокрема.

Загальний вигляд еталонної моделі протоколів на технології ATM подано на рис. 57.

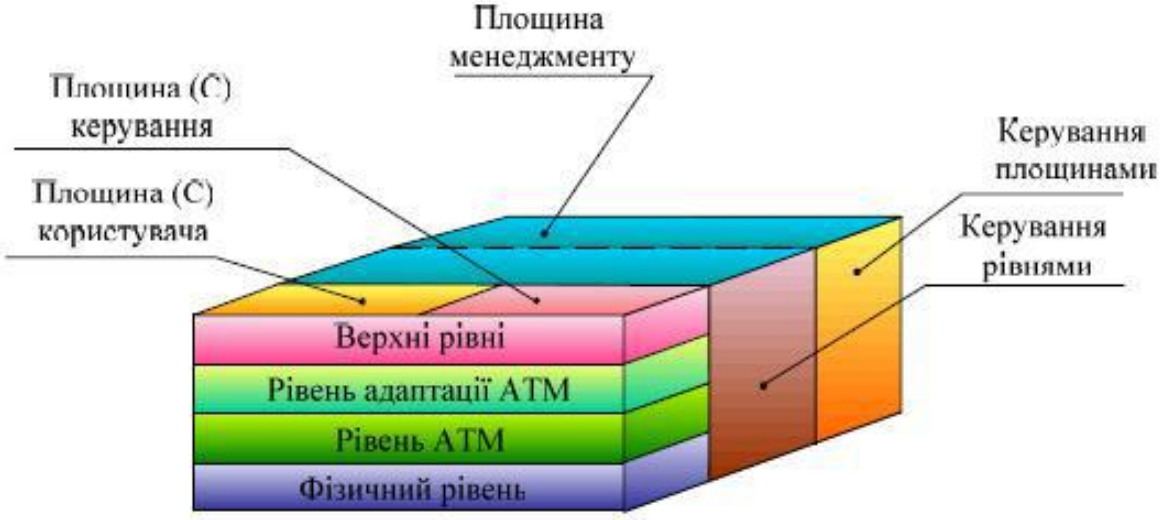


Рисунок 57– Еталонна модель протоколів B- ISDN

Відповідно до Рекомендації I.321 (ITU-T), модель містить у собі три площини:

- площину користувача;
- площину керування;
- площину менеджменту.

Площина користувача (U-plane) забезпечує транспортування всіх видів інформації з відповідними механізмами захисту від помилок, контролю й

керування потоком, обмеження навантаження та ін. Площина користувача має рівневу структуру.

Площина керування (C-plane) визначає протоколи налаштування, контролю й роз'єднання з'єднань; виконує функції сигналізації. Площина керування також має рівневу структуру.

Площина менеджменту (M-plane) забезпечує виконання функцій двох типів: адміністративне керування площинами й рівнями. Адміністративне керування площинами здійснює координацію між усіма «гранями» моделі протоколів і всієї B-ISDN пов'язуючи її в єдине ціле. Сфера керування площинами не має рівневої структури.

Функціями керування рівнями є:

– розподілення мережевих ресурсів;

– узгодження їх з параметрами трафіку;

– обробляння інформації, експлуатації та технічного обслуговування; керування мережею.

Керування рівнями має рівневу структуру. Опції рівневої еталонної моделі протоколів B-ISDN визначено в Рекомендаціях I.321 і I.413 (ITU-T). Фізичний рівень відповідає першому рівню еталонної моделі OSI/ISO, рівень ATM і частина рівня адаптації ATM відповідають другому рівню OSI/ISO та вищим. Мережі B-ISDN на основі технології ATM розраховано на використання в локальному секторі, міських і глобальних мережах для передавання різних видів трафіку: аудіо, відео на вимогу, телебачення високої чіткості. B-I8БК фактично є першою мультисервісною мережею.

8.3 Концепція інтелектуальної мережі (IN)

Наявність програмного керування в комутаційних системах дала змогу реалізувати нову, в порівнянні з попередніми мережевими концепціям, *функціональну модель мережі*. З'явилася можливість відокремити *функції керування з'єднаннями від функцій пов'язаних з логікою формування послуг* і, таким чином, *відобразити функціональну модель мережі дворівневою архітектурою* (рис. 49).

Це дозволило реалізувати зазначені функції в окремому обладнанні та забезпечити до нього віддалений доступ з метою спільного використання всіма комутаційними вузлами мережі зв'язку.

Програмну реалізацію принципу формування послуг, наприклад, переадресація виклику, обмеження потоку викликів, телефонні картки та ін., можна розглядати як наділення мережі «інтелектуальністю».

Керування з'єднаннями (комутація) ITU-T у Рекомендаціях Q.1201 і Q.1290 дає таке визначення терміна «інтелектуальна мережа».

Інтелектуальна мережа є архітектурною концепцією, яку застосовують для мереж електрозв'язку, передбачає чітко визначений набір гнучко

використовуваних засобів, які сприяють створенню та долученню в мережі зв'язку нових послуг, зокрема послуг, керованих користувачем.

Рисунок 58 – Архітектура інтелектуальної мережі

Концепція ІК таким чином, встановлює набір правил, відмінною рисою яких є те, що вони не залежать від створюваної послуги й від структури мережі, яка надає цю послугу. Більшу частину логіки, що є частиною програмного забезпечення АТС, для реалізації інтелектуальної мережі перенесено на невелику кількість спеціалізованих комп'ютерів. Послуги IN підтримуються шляхом інформаційного обміну між комутаційними станціями, зазначеними комп'ютерами та деякими іншими спеціалізованими пристроями (призначення яких розглядатимемо далі). Концепцію Ш у принципі можна реалізувати також у аналоговій мережі, але її реалізація на базі цифрової інтегрованої мережі є значно ефективнішою.

8.3.1 Елементи мережі

На рис. 59 зображено структурну модель інтелектуальної мережі, яку складають компоненти Ш і зв'язки між ними.

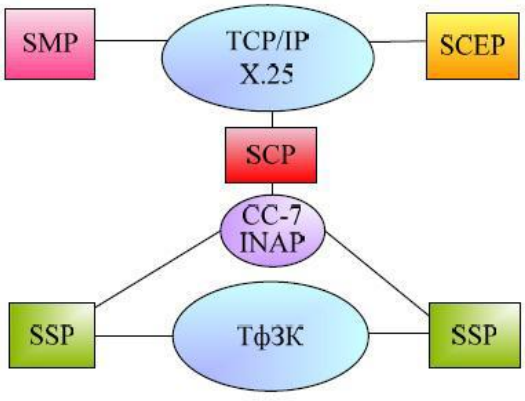


Рис. 59 – Структурна модель інтелектуальної мережі

SSP (Service Switching Point) – *вузол комутації послуг*, котрий є звичайною комутаційною станцією, в якій збережено всі функції керування процесом надання основних послуг зв'язку та додаткові програмні засобами, що надають змогу підтримувати діалог з абонентом (запрошення абонента до набору додаткових цифр, розпізнавання мови і т.д.). SSP з'ясовує, чи вимагає прийнятий ним від абонента виклик звернення до послуг IN, а у разі потреби спрямовує відповідний запит у вузол керування послугами SCP.

Таким чином, SSP забезпечує доступ абонентів мережі зв'язку до послуг IN та підтримує протоколи взаємодії з іншим елементами IN. Запити на послуги передають мережею СС-7, використовуючи спеціальний протокол прикладного рівня INAP (Intellegent Network Application Protocol), який визначає синтаксис та семантику операцій, призначення та порядок їх обробки. Цей протокол прикладного рівня, який підтримує система СС-7, забезпечує взаємодію між прикладними процесами у вузлах IN.

SCP (Service Control Point) – *вузол керування послугами*, який містить програми, що централізовано реалізують логіку послуг, системне програмне забезпечення, а також базу даних реального часу. SCP приймає запит від SSP та направляє йому інструкції для подальшої обробки дзвінка відповідно до необхідної послуги.

SMP (Service Manedgment Point) – *система експлуатаційного керування* та SCEP (Service Creation Enviroment Point) – *середовище створення послуг* надають змогу оператору мережі контролювати та керувати параметрами й конфігурацією послуг IN.

Середовище створення послуг містить засоби конструювання, модифікації та тестування послуг до початку комерційної експлуатації та засоби завантаження відповідних програм у SMP. SMP забезпечує експлуатаційне керування наявними послугами, підготовкою нових послуг та їх долученням. У якості протоколів взаємодії між SMP, SCEP і SCP використовують X.25 і стек TCP/IP.

8.3.2. Модель обслуговування IN-виклику

Модель IN-виклику детально описано в Рекомендації МСЕ Q.1214. Вона складається з SSP (Service Switching Point) – *вузол комутації послуг*, котрий є звичайною комутаційною станцією, в якій збережено всі функції керування процесом надання основних послуг зв'язку та додаткові програмні засобами, що надають змогу підтримувати діалог з абонентом (запрошення абонента до набору додаткових цифр, розпізнавання мови і т.д.).

SSP з'ясовує, чи вимагає прийнятий ним від абонента виклик звернення до послуг IN, а у разі потреби спрямовує відповідний запит у вузол керування послугами SCP. Таким чином, SSP забезпечує доступ абонентів мережі зв'язку до послуг *IN* та підтримує протоколи взаємодії з іншим елементами *IN*.

Запити на послуги передають мережею СС-7, використовуючи спеціальний протокол прикладного рівня INAP (Intellegent Network Application Protocol), який визначає синтаксис та семантику операцій, призначення та порядок їх обробки. Цей протокол прикладного рівня, який підтримує система СС-7, забезпечує взаємодію між прикладними процесами у вузлах IN.

SCP (Service Control Point) – *вузол керування послугами*, який містить програми, що централізовано реалізують логіку послуг, системне програмне забезпечення, а також базу даних реального часу. SCP приймає запит від SSP та направляє йому інструкції для подальшої обробки дзвінка відповідно до необхідної послуги.

SMP (Service Manedgment Point) – *система експлуатаційного керування* та SCEP (Service Creation Enviroment Point) – середовище створення послуг надають змогу оператору мережі контролювати та керувати параметрами й конфігурацією послуг IN.

Середовище створення послуг містить засоби конструювання, модифікації та тестування послуг до початку комерційної експлуатації та засоби завантаження відповідних програм у SMP. SMP забезпечує експлуатаційне керування наявними послугами, підготовкою нових послуг та їх долученням. У якості протоколів взаємодії між SMP, SCEP і SCP використовують X.25 і стек TCP/IP.

8.3.3 Модель обслуговування IN-виклику

Модель IN-виклику детально описано в Рекомендації МСЕ Q.1214. Вона складається з двох частин: моделі вихідної сторони (А); моделі вхідної сторони (В).

На рис. 60 показано модель IN-виклику для вихідної сторони (А). Модель вхідної сторони (В) є подібною.

Модель містить послідовність точок, які відображають фази станів базового процесу, виконуваного комутаційною станцією під час налаштування з’єднання, через які проходить процес обслуговування виклику з моменту, коли абонент зняв слухавку, до закінчення сеансу зв’язку.

Між точками базового процесу можуть бути точки звернень до послуг IN або подій, які становлять інтерес з точки зору логіки послуги IN. Ці точки називають *тригерними точками*.

Якщо в процесі обслуговування виклику виявлено активну тригерну точку, то процес призупиняється до того часу, поки SSP і SCP не завершать обмін інформацією, в результаті якого визначаться параметри наступного стану базового процесу.

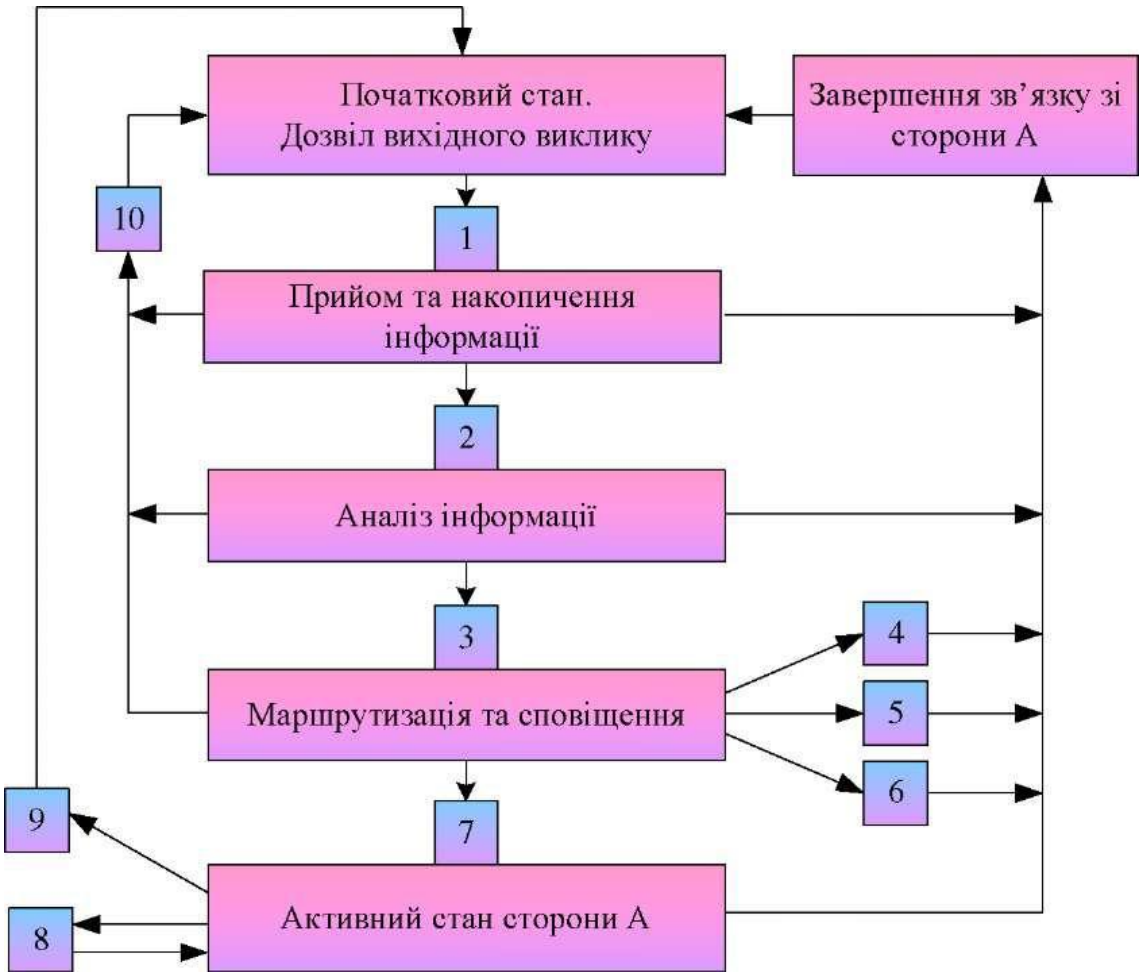


Рисунок 60 – Модель IN-виклику для вихідної сторони

Тригерні точки: 1– Вихідний виклик дозволено; 2 – Інформація накопичена 3 – Інформація проаналізована; 4 – Маршрут не знайдено; 5 – Зайнята сторона, що викликається; 6 – Сторона, що викликається, не знайдена; 7 – Відповідь сторони, що викликається; 8 – Втручання у фазу розмови сторони А; 9 – Роз'єднання сторони А; 10 – Відмова від зв'язку сторони А

Модель містить чотири розташованих одна над іншою площини, кожна з яких є абстрактним поданням (зі своїм ступенем деталізації) тих можливостей, якими володіє інтелектуальна мережа.

Зміни, пов'язані з тією або іншою послугою функції, відображено на кожній площині відповідними об'єктами, причому функціональні об'єкти сусідніх площин заданим способом співвідносяться один з одним.

За допомогою поданої концептуальної моделі можна проектувати послуги та моделювати їх подання для мереж ІМ, які мають різну структуру та різні принципи організації.

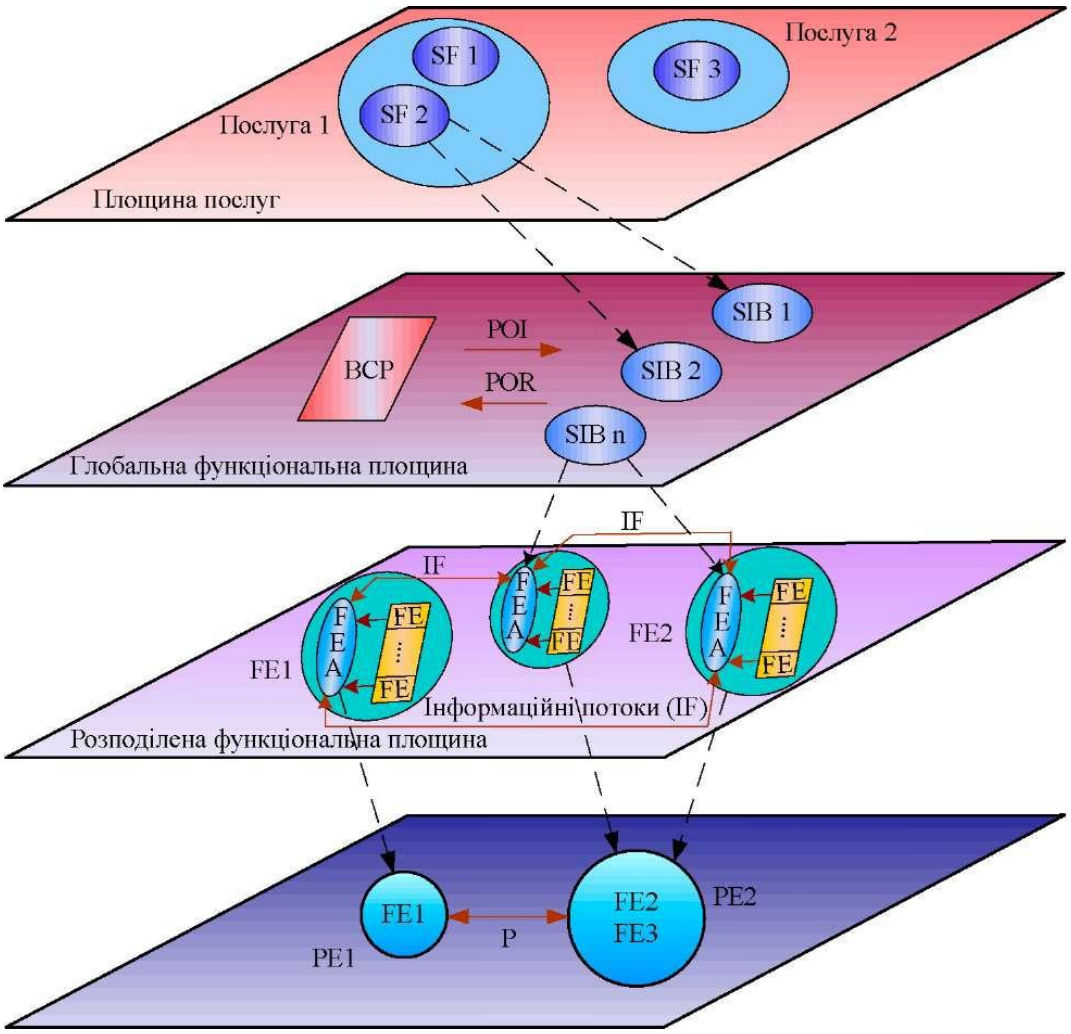


Рисунок 61–Концептуальна модель *IN*

Розглянемо, чим відрізняються площини моделі та яким є їх призначення.

Площина послуг. Верхня площина моделі репрезентує послуги так, як їх сприймає кінцевий користувач. Таке подання не містить інформації про способи та деталі реалізації послуги в мережі. На цій площині послуга компонується з однієї або декількох різних стандартизованих складових. Кожну з цих складових користувач сприймає як один із атрибутів послуги.

Стандартом визначено як сукупність таких складових, так і правила їх використання.

Глобальна функціональна площина відображає мережу *IN* у вигляді єдиного функціонального об’єкта. На цій площині подано незалежні від послуг функціональні блоки, узагальнено названі «*конструктивними блоками*» (SIB).

Одним із таких блоків (SIB) є блок, який реалізує *базовий процес обслуговування виклику* (BCP). Він виконує традиційні для звичайної комутаційної станції функції:

– налаштування з’єднання;
– роз’єднання;
– зберігання оперативних даних;

– виявляти запити послуги IN;

– звертатися до інших блоків.

Звернення BCP до інших SIB відбувається за допомогою логічного інтерфейсу, так званої *точки ініціалізування* (POI).

Після завершення процесу надання послуги IN (у іншому блоці), відбувається повернення в BCP, який продовжує роботу, використовуючи дані, отримані після повернення. Повернення здійснюється через інший логічний інтерфейс, який називають *точкою повернення* (POR).

Необхідність специфікації точок POI та POR зумовлена тим, що одна й та ж сукупність SIB може надавати абсолютно різні послуги залежно від того, з яких точок BCP здійснено запит.

Розподільча функціональна площина відображає те, як реалізацію послуги IM шляхом розподілення здійснюють програмні засоби. Кожен об'єкт (FE) на цій площині може виконувати декілька призначених ньому дій.

Блоки SIB подано на розподільчій функціональної площині у вигляді послідовності дій, які виконують об'єкти FE. Деякі з таких дії пов'язані з обміном інформацією між FE, що відображено на цій площині у вигляді інформаційних потоків.

Фізичну площину відображають фізичні елементи мережі (PE), в якій реалізується концепція IM. Такими PE можуть бути комутаційні станції, спеціалізовані комп'ютери або бази даних. На фізичній площині показано у яких PE розміщено ті чи інші PE.

Концептуальна модель IN є засобом для розмежування етапів проектування послуг та послідовності дій на кожному з них. Моделюючи процедури керування зв'язками користувачів на розподільчій функціональній та фізичній площинах цієї моделі, можна проаналізувати та порівняти можливі варіанти архітектури IN з урахуванням їх економічної доцільності та ефективності функціонування.

Декларований у стандартах для IN принцип незалежності її архітектури від типу мережі зв'язку є чинним, оскільки міжнародними стандартами однозначно визначено функціональні модулі платформи IN та взаємозв'язку між компонентами *IN*. Принцип організації доступу до платформи IN залежить в якій абонентів мережі загального користування є доступними послуги IN, а також від кількості на мережі цифрових комутаційних станцій, способів маршрутизації, систем сигналізації та ін.

8.3.4 Концепції мереж наступного покоління (NGN)

Швидкий розвиток у XXI столітті цифрових мультисервісних мереж зумовив виникнення нової мережевої концепції – *концепції мереж наступного покоління* (Next Generation Network, NGN).

У Рекомендації Y.2001 (ITU-T) NGN визначено як концепцію побудови мереж зв'язку, які надають необмежений набір послуг (зокрема й

широкосмугових) з гнучкими можливостями щодо їх керування, персоналізації та створюють нові послуги за рахунок уніфікації мережевих рішень з використанням мультисервісної транспортної мережі, винесенням функцій надання послуг в кінцеві вузли мережі та можливістю інтеграції з традиційними мережами зв'язку.

Визначення NGN можна доповнити такими характеристиками:

– *універсальна мобільність* передбачає, що для користувачів і будь-яких рухомих об'єктів надання послуг є безперервним та повсюдним, тобто взаємодія та доступ до послуг не залежатимуть від змін місцезнаходження або технічних умов. Рівень доступу до послуг обумовлюється лише технологічними можливостями мережі доступу, узгодженням рівнів обслуговування між мережею реєстрації користувача та візитною мережею;

– *можливість широкосмугового передавання з наскрізним QoS* передбачає досягнення угод з різними кінцевими системами щодо забезпечення *необхідної якості обслуговування з кінця в кінець*, щодо використання наборів параметрів протоколу верхнього рівня для керування нижнім рівнем, а також досягнення угод про механізми QoS рівня доступу та транспорту;

– забезпечення безлічі технологій для мереж доступу;

– повна захищеність інформації в мережі; незалежність функцій, пов'язаних з послугами, від внутрішніх транспортних технологій;

– забезпечення відкритих інтерфейсів для взаємодії з традиційними мережами; різноманітні схеми ідентифікації користувачів та уніфіковані (за оцінкою користувача) характеристики одних і тих самих послуг у різних мережах.

Отже, основним принципом концепції NGN є відокремлення:

– функцій транспортування;

– функцій керування викликами;

– функцій керування послугами.

Багаторівневу архітектури концепції NGN подано на рис.62.

Рисунок 62 – Багаторівнева архітектура концепції NGN

Основними завданнями *транспортного рівня* є прозоре передавання інформаційних потоків, а також підтримка взаємодії з наявними мережами зв'язку.

На *рівні керування викликами* обробляють інформацію сигналізації та керування комутацією й передаванням.

Рівень керування послугами забезпечує керування логікою послуг та застосувань.

Такий функціональний розподіл дає змогу уніфікувати завдання, пов'язані з керуванням викликами, відокремивши їх від особливостей застосовуваних транспортних технологій, та використовувати однакову логіку формування послуги незалежно від типу транспортної мережі та мережі доступу.

Мовлення (в даному випадку медіа-трафік) і сигнальна інформація для керування обслуговуванням виклику в NGN передають різними маршрутами та обробляють різні мережеві пристрої, а не єдиний вузол комутації каналів (АТС), як у традиційній ТфЗК.

Медіа-трафік проходить безпосередньо між шлюзами доступу або транспортними шлюзами.

Сигналізація управління викликом проходить через інший пристрій – спеціальний *програмний комутатор*, але завжди не там, де проходить медіа-трафік. Маршрути медіа-трафіку і сигналізації сходяться в *прикордонному контролері сеансів* – ще одному спеціальному пристрої, який застосовують у NGN.

З функціями комунікаційного обладнання (мультиплексорів, комутаторів і маршрутизаторів) до складу NGN входять:

– контролери сигналізації;

– шлюзове обладнання різного призначення.

Особливе місце тут займає програмний комутатор, який дає змогу надавати мовленнєві послуги у процесі взаємодії мереж з синхронним режимом перенесення (класична телефонія) та з асинхронним (середовища з пакетною комутацією).

Приклад побудови мережі NGN подано на рис. 63.

AG (Access Gateway) – шлюз доступу;

MG (Media Gateway) – транспортний шлюз;

SG (Signaling Gateway) – шлюз сигналізації;

AS (Application Gateway) – сервер застовувань;

SSw (Softswitch) – програмний комутатор.

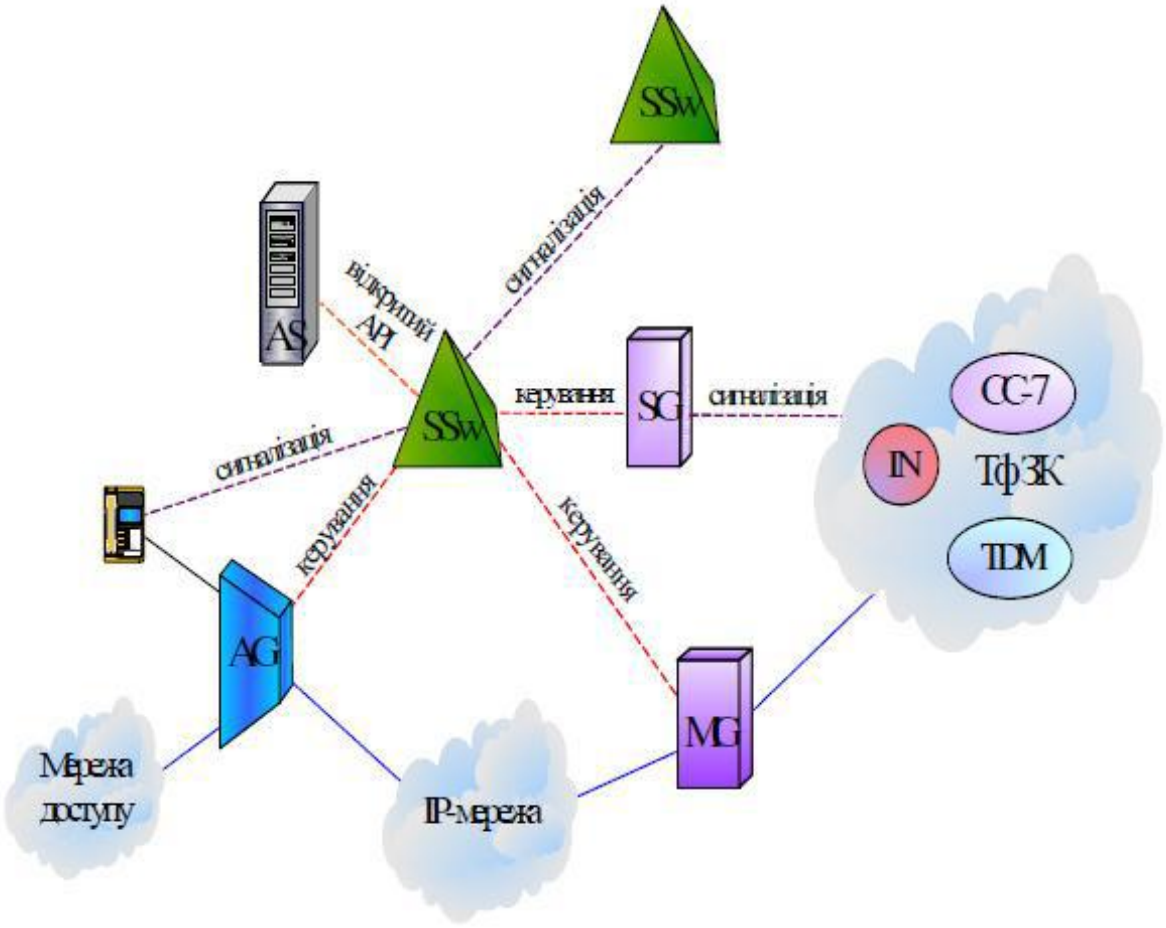


Рисунок 63 – Приклад мережі NGN

Softswitch виконує функції керування обслуговуванням викликів і обробляє всю сигналізацію, керує всіма шлюзами (AG, MG, SG), надає інформацію про маршрутизації виклику, визначає стан обробляння кожного виклику в шлюзі й стан інформаційних каналів, передає інформаційні повідомлення користувачів між транспортними шлюзами, а також між IP-телефонами та іншими терміналами, виконує функції обліку вартості послуг.

Сервер застовувань AS реалізує логіку послуг. Виклик, який вимагає додаткової послуги, або може бути переданий від Softswitch до шлюзу доступу для подальшого керування цією послугою, або сам Softswitch може отримувати від шлюзу доступу інформацію, необхідну для виконання логіки послуги.

На *транспортний шлюз MG* надходять потоки мовленнєвої інформації з боку ТфЗК, він перетворює цю інформацію в пакети й передає її за протоколом IP у мережу з маршрутизацією пакетів, і все це виконує під керуванням Softswitch.

Шлюз доступу AG є інтерфейсом між IP-мережею та мережею доступу (проводовою або безпроводовою), передає сигнальну інформацію до Softswitch, перетворює призначену для користувача інформацію й передає її або до іншого порту цієї ж IP-мережі, або в іншу мережу (з комутацією пакетів або каналів).

Сигнальний шлюз SG забезпечує доставку до Softswitch сигнальної інформації, яка надходить від ТфЗК, а також перенесення сигнальної інформації в зворотному напрямку.

Провідне місце в мережах NGN займає спеціальний *протокол ініціалізування сеансів зв'язку* (Session Initiation Protokol, SIP). SIP є текстово орієнтованим протоколом прикладного рівня, який призначено для організації, модифікації та завершення різних сеансів з зв'язку, зокрема мультимедійних конференцій, телефонних з'єднань, широкомовної розсилки мультимедійної інформації та з'єднань користувачів з різними інфокомунікаційними застосуваннями. SIP використовують для взаємодії Softswitch між собою. Крім того, за допомогою SIP користувачі можуть брати участь у вже активних сеансах зв'язку, а також бути запрошеними іншими користувачами до участі у новостворюваному сеансі.

Отже, NGN – це повноцінна платформа для швидкого створення нових комунікаційних послуг. Значну роль у цьому процесі відіграє Softswitch, який забезпечує нові можливості завдяки *інтерфейсам прикладного програмування*, що ґрунтуються на відкритих стандартах.

ITU-T ініціював процес стандартизації мереж нового покоління в рамках Проекту Глобальної інформаційної інфраструктури (GII), що обумовило створення ряду рекомендацій з GII серії Y.

8.4 Основні тенденції розвитку телекомунікацій

У перспективі розвитку телекомунікацій помітними є тенде тенденції до:

– мультисервісності, тобто незалежності технологій надання послуг від транспортних технологій;

– широкосмуговості, яка забезпечить гнучкі та динамічні зміни швидкості передавання інформації в широкому діапазоні відповідно до поточних потреб користувача;

– мультимедійності, тобто здатності мережі передавати багатокомпонентну інформацію (мовлення, дані, відео, аудіо та ін.) з необхідною синхронізацією цих компонентів у реальному часі й використанням складних конфігурацій сполучень;

– інтелектуальності – можливості керувати послугою, викликом і з'єднанням користувачами або постачальниками послуг;

– інваріантності доступу, тобто можливості організувати доступ до послуг незалежно від технології, яку використовують;

– багатооператорності, тобто участі декількох операторів у процесі надання послуги та розмежування їх відповідальності відповідно до сфер їх діяльності.

Реалізація перерахованих тенденцій дасть змогу вийти на телекомунікаційний ринок мереж з пакетною комутацією для надання як традиційних послуг зв'язку, так і мультимедійних. Традиційними послугами,

реалізованими зараз засобами IP, є: передавання мовлення через Інтернет VoIP потокове відео, інтерактивні ігри, Інтернет-радіо та ін.

У процесі передавання мультимедійного трафіку через Інтернет, разом з мережевим і нижніми рівнями, починають діяти також верхні рівні обладнання користувача, у яких виконуються протоколи контролю перенесення мультимедійного трафіку «з кінця в кінець», алгоритми стискання та кодування інформації.

У цілому, перехід на IP-основу зводиться до розподілу функцій перенесення інформації та функцій керування перенесеннями інформації через мережу, а також відокремленні функцій послуг та застосувань від телекомунікаційних функцій.

Еволюція телекомунікаційних мереж у напрямку NGN відбуватиметься шляхом об'єднання транспортних мереж та мереж доступу як на апаратному рівні, так і на програмному.

Складність переходу до NGN пов'язана з тим, що в наявних мережах використовують різне програмне забезпечення. Для того, щоб усунути таке протиріччя, розроблено концепцію відкритого доступу до послуг OSA (Open Servict Access), що передбачає використання інтерфейсних пристроїв, які забезпечують взаємодію різних мереж.

Процес конвергенції мереж прискорює розвиток фундаментальних тенденцій у телекомунікаціях, а саме:

– кардинальна зміна мережевих архітектур, відмова від жорсткої ієрархії мереж, прикметної для концепції ЄАМЗ;

– фундаментальний поділ рівнів транспортування інформації та рівня формування послуг;

– перехід від телекомунікацій до інфокомунікацій;

– рівноправна участь у інформаційному процесі всіх учасників: користувачів, мережевих операторів і контент-провайдерів.

8.5 Мережі абонентського проводового і доступу

На рис. 64 наведено схему традиційної мережі абонентського доступу, мережеві закінчення (КТ) якої можна знайти в кожному домі. Вона містить фрагмент розподільчої мережі, яка класифікується як СРВхТ, через яку абонент отримує послуги кабельного телебачення та фрагменти організації доступу в територіальні та глобальні мережі.

Особливістю цих фрагментів є:

– поєднання у собі функції СФВихТ і СРВхТ;

– виконання функції сегмента замикання локального трафіку (СЗЛТ), оскільки опорний вузол (ОВ) мережі абонентського доступу – це перший рівень замикання трафіку, на якому здійснюється інформаційний обмін між під під'єнаними до нього абонентськими пунктами (АП).

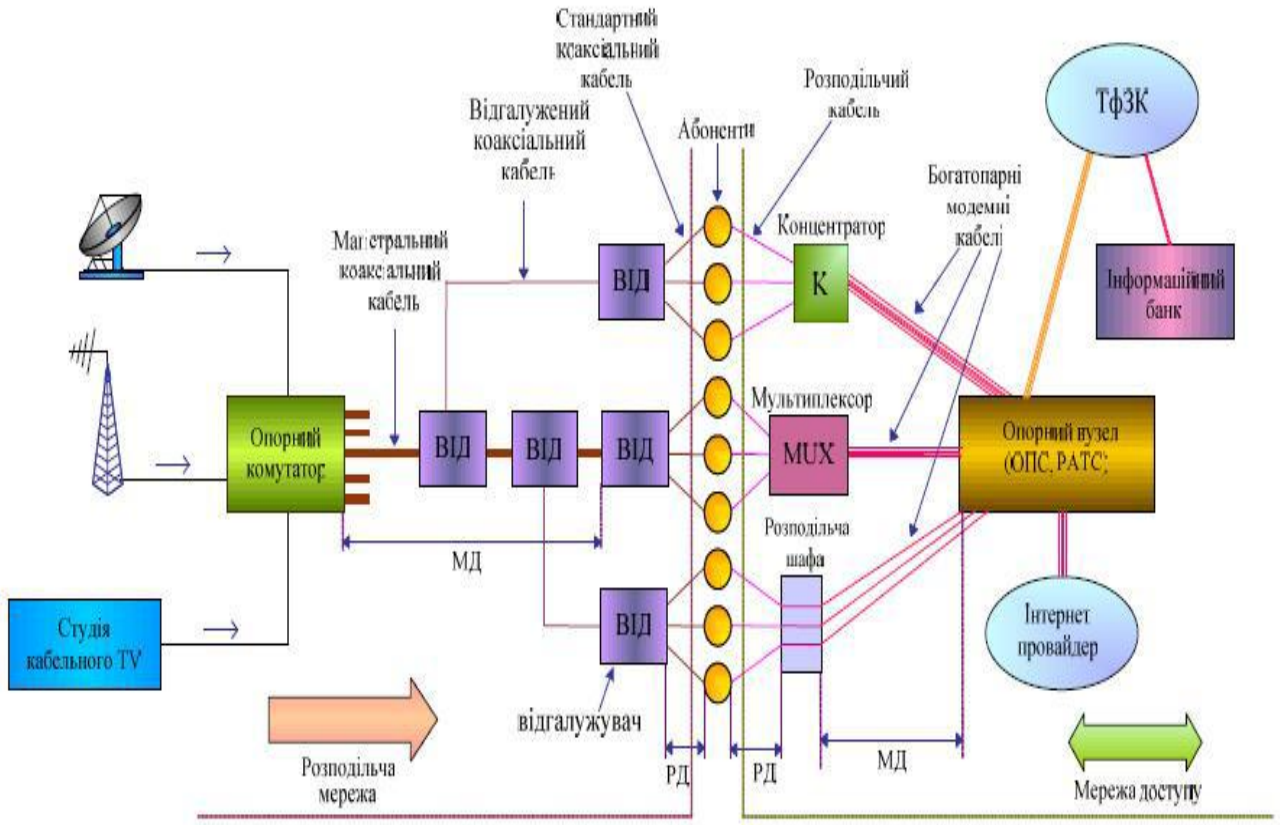


Рисунок 64 – Схема традиційного абонентського доступу

Територія, на якій зосереджено АП, під’єднані до відповідного ОВ, є сферою обслуговування ОВ. Межі сфери обслуговування ОВ залежать від абонентської щільності й комутаційних можливостей вузла. Відносно АП своєї сфери обслуговування, опорний вузол виконує функцію комутації, забезпечуючи налаштування зв’язків усередині. Водночас у ньому здійснюється функція концентрації інформаційних потоків, які направляються в глобальні мережі.

Лінії зв’язку, за допомогою яких АП під’єднуються до ОВ, називаються абонентськими лініями (АЛ). Це, як правило, кабелі з мідними жилами. Абонентську мережу на ділянці від ОВ до АП називають «останньою милею» телекомунікаційної мережі.

Проблема «останньої милі» полягає в численності абонентських ліній, що становить значну частку загальномережевих витрат. Вирішують цю проблему, організовуючи додаткові вузлові пункти (розподільчі вузли), які є інсталяційною базою для розміщення таких пристроїв, як розподільчі коробки, розподільчі шафи, мультиплексори, концентратори, відгалужувачі.

Отже, мережа абонентського доступу складається з двох ділянок: розподільчої ділянки (РД) (це, в основному, окремі мідні пари); магістральної ділянки (МД), на якій використовують спільний багатожильний кабель.

8.6 Технології та обладнання цифрової абонентської лінії

Цифрова абонентська лінія (Digital Subscriber Line, DSL) надається абонентові безпосередньо після підєднання до мережі ISDN. Усі послуги цієї мережі засновано на передаванні інформації в цифровому вигляді. Інтерфейс користувача (BRI, PRI) також є цифровим, тобто всі абонентські пристрої (телефон, факс, комп'ютер) повинні бути цифровими й спрямовувати в мережу цифрові дані.

Альтернативою цифрового абонентського закінчення ISDN. Ця альтернатива є сімейством технологій із загальною назвою xDSL і складається з таких технологій:

– асиметричне цифрове абонентське закінчення – Рекомендація С.992.1 (ITU);

– у комерційних пропозиціях мережевих операторів і провайдерів цю технологію часто називають широкосмуговим доступом;

– високошвидкісна цифрова абонентська лінія – Рекомендація 0.991.1 (ITU);

– симетричне цифрове абонентське закінчення – Рекомендація 0.991.2 (ITU);

– надшвидке цифрове абонентське закінчення – Рекомендація 0.993 (ITU);

– цифрове закінчення з адаптувальною швидкістю – Рекомендація 0.992.1 (ITU).

Технології xDSL засновано на методах, які дають змогу стиснути спектр сигналу й зосередити основну частину його енергії на ділянках більш низьких частот, що узгоджує електричні характеристики кабелю з параметрами сигналу. Подібних перетворень спектру сигналу досягають, використовуючи спеціальні методи модуляції та кодування (ці питання детально вивчають інші дисципліни).

8.7 Мережі абонентського безпроводового доступу

Використання безпроводового абонентського доступу має такі переваги: швидку реалізацію та введення об'єкта в експлуатацію; порівняно нескладну реконфігурацію мережі, що дає змогу відстежувати зміни попиту на послуги; у деяких випадках через неможливість прокласти оптичний кабель, безпроводовий доступ стає єдино можливим способом нарощування й модернізації абонентської мережі.

До безпроводового абонентського доступу також застосовують терміни «безпроводове абонентське закінчення» і «абонентський радіодоступ».

Мережу абонентського безпроводового доступу зображено на рис. 65. Незважаючи на відсутність кабелю на розподільчій ділянці (РД), абоненти, як і раніше, залишаються «прив'язаними» до конкретної стаціонарної географічній

точки – базової станції (BS). Базова станція з опорним вузлом може бути пов’язана як за допомогою кабелю (потоком E1 0703, модемною технологією HDSW), так і безпроводовим способом (цифровий РРЛ, супутникових систем зв’язку).

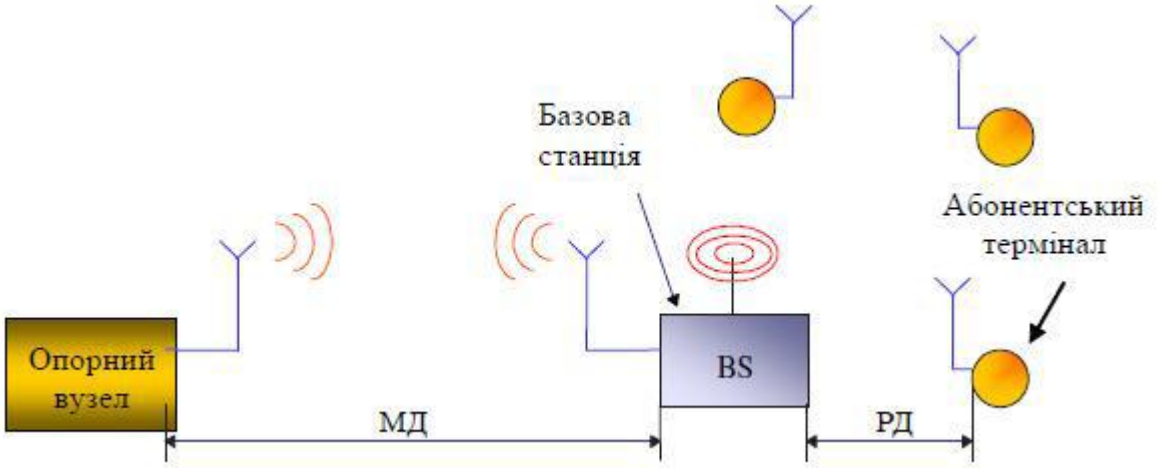


Рис. 65 – Стаціонарний радіодоступ

Абонентський термінал (АТ) є радіоблоком з компактною направленою або ненаправленою антеною. Залежно від типу антени й потужності передавача, допустиме віддалення АТ від базової станції може становити від 5 до 12 км.

Існують вузькосмугові т широкосмугові безпроводові абонентські закінчення. Вузькосмугові безпроводові закінчення забезпечують передавання тільки низькошвидкісного комп’ютерного (до 128 Кбіт/с) та телефонного трафіку. Типовою технологією вузькосмугового абонентського закінчення є технологія DECT.

Сфери застосування стандарту DECT – це системи мікростільникового зв’язку для бізнесу, безпроводові АТС для середніх і великих компаній, пристрої абонентського доступу до телекомунікаційної мережі загального користування, альтернатива стандартному проводовому під’єднанню WLL, мікростільникові радіотелефони для дому й малих офісів.

Стандарт базується на цифровому радіопередаванні даних між базовими радіостанціями й радіотелефонами за технологією множинного доступу з часовим розподілом, TDMA.

Повністю дуплексний зв’язок забезпечується за допомогою часового дуплексування TDD. Діапазон радіочастот, використовуваних для приймання/передавання, – 1880-1900 Мгц. Робочий діапазон (20 Мгц) розподілено на 10 радіоканалів, кожен – по 1,728 МГц. Обмін інформацією проводиться кадрами; за допомогою часового розподілення в кожному кадрі створюються 24 часові слоти; 24 слоти забезпечують 12 дуплексних каналів для приймання/передавання голосу.

Широкосмугові безпроводові абонентські закінчення засновано на системах поширення телевізійного сигналу, які працюють у високочастотному діапазоні й забезпечують передавання всіх трьох видів трафіку, причому

комп’ютерні дані можуть передаватися зі швидкостями кілька мегабіт в секунду. Системами останнього типу є служба багатоканального багатоточкового розподілення, яка працює на частоті 30 ГГц в Америці та 40 ГГц – в Європі.

Важливий аспект використання цієї служби полягає в тому, що вона пропонує альтернативу високошвидкісним орендованим лініях для бізнесу, забезпечує високошвидкісний доступ до Інтернету та телебачення високої чіткості (HDTV).

Стандарт IEEE 802.16 є більш придатним, оскільки визначає загальні принципи використання частотного діапазону, методи мультиплексування й надані послуги, що дає змогу врахувати інтереси різних виробників обладнання WLL та забезпечити гнучкість таких систем. У даний час інтенсивно освоюються діапазони 2.5, 3.5 і 5.8 Ггц.

Специфікація IEEE 802.16 стала стандартом для побудови мереж широкосмугового доступу наступного покоління, які дають змогу не тільки покрити всі зони «останньої милі», але й охопити безпроводовим зв’язком цілі регіони.

8.8 Мережі мобільного доступу

Мобільний доступ абонентам надають оператори стільникового зв’язку.

Стандарт CDMA в системі UMTS еволюціонує від вузькосмугового до широкосмугового зі швидкістю передавання до 2.4 Мбіт/с.

Радіоінтерфейс WCDMA містить канали трьох рівнів: логічного; транспортного; фізичного.

Логічні канали визначають тип інформації, яка передається в мережі. Вони організовуються в мережі лише в потрібні моменти часу для виконання конкретних завдань. Транспортні канали визначають, яким чином перетворюється й здійснюються обмін інформацією між елементами мережі.

Фізичні канали забезпечують реальне передавання сигналів у мережі радіодоступу. З фізичними каналами працюють базові станції, а контролери мережі радіодоступу розрізняють і працюють тільки з транспортними каналами. У мережі UMTS передбачено також такі фізичні канали, які виконують функції сигналізації і не містять інформацію транспортних каналів.

Лінії зв’язку в UMTS складаються з ліній «вгору» US-BS – від абонентського обладнання до базової станції та ліній «униз» BS-US – від базової станції до абонентського обладнання.

Транспортні канали радіо інтерфейсу WCDMA в лініях US-BS і BS-US мають певні відмінності. Безпроводовий мобільний доступ до Інтернету надають переважно оператори мобільних телефонних мереж з використанням для передавання пакетного трафіку протоколу служби пакетного радіозв’язку загального призначення, який працює в рамках стандарту GSM (General System for Mobile Communication) в діапазоні 1800 МГц . Мобільні мережі третього

покоління 3G задекларовано ITU в концепції IMT-2000 (International Mobile Telecommunications). Їх відмінною рисою є значне перевищення трафіку даних над голосовим трафіком. Роботу над стандартами 3G зосереджено на розширенні займаної смуги частот та удосконаленні принципів побудови радіоінтерфейсу.

У мережах 3G забезпечено такі швидкості передавання даних:

– для абонентів, які рухаються зі швидкістю 120 км/год, - 144 кбіт/с;
– для абонентів, які рухаються зі швидкістю до 3 км/год, - 384 кбіт/с;
– для стаціонарних абонентів – до 2 Мбіт/с.

Для роботи в мережах мобільного доступу використовують абонентські багатофункціональні пристрої (АБП), що є повноцінними продуктами конвергенції, якими є мобільний телефон, плата для комп'ютера, блок, інтегрований в ноутбук. Важливим напрямком розвитку АБП є їх конвергенція з іншими технологіями безпроводового доступу, наприклад, використання SIM-картки пристрою, призначеного для роботи в мережі GMS, в пристроях що працюють за технологією Wi-Fi.

8.9 Узагальнена архітектура та модель мережі доступу

Мережі доступу та транспортні мережі є засобом отримання телекомунікаційних та інформаційних послуг.

Узагальнену архітектура та модель мережі доступу визначено ITU-T у Рекомендації 0.902 (11/95). На рис. 66 наведено узагальнену архітектуру мережі доступу, описану в цій рекомендації.

Елементами узагальненої архітектури мережі доступу є:

TMN – мережа керування телекомунікаціями;

UNI – інтерфейс користувач- мережа; AN – мережа доступу; SNI – інтерфейс сервісного вузла;

SN – сервісний вузол; TN – транспортна мережа;

Q3 – інтерфейс керування.

На мережу керування телекомунікаціями ТМК покладено завдання підтримувати функціональність усіх елементів мережі, що здійснюється шляхом постійного контролювання інтерфейсом Q3 операційних систем керування, конфігурації та координації ресурсів, контролювання безпеки. Опції повномасштабного керування повинні охоплювати мережі доступу різних операторів на великих територіях (у межах міст, областей).

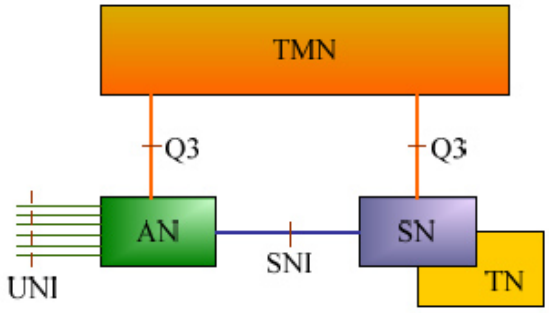


Рисунок 66 – Узагальнена архітектура мережі доступу

Транспортна мережа ТК забезпечує можливість доступу до різних сервісним вузлів.

Функціями інтерфейсів користувачів є:

– під’єднання терміналів користувачів;
– аналогово-цифрове та цифрово-аналогове перетворення;
– перетворення сигналів (інтерфейсів);
– активація/дезактивація;
– тестування;
– контроль, керування та обслуговування.

Прикладами функцій інтерфейсів сервісних вузлів SNI є:

– під’єднання мереж доступу до сервісних вузлів;
– концентрація функцій контролю;
– керування;
– обслуговування в мережах доступу;
– тестування; управління;
– контроль та обслуговування інтерфейсів.

Зразками типів сервісних вузлів SN є:

– вузли телефонного зв’язку;
– вузли N-ISDN, вузли B-ISDN, вузли виокремлених ліній;
– вузли пакетної комутації;
– вузли пакетного передавання через виділені лінії;
– вузли відео- та радіопрограм аналогового мовлення;
– вузли відео та радіопрограм цифрового мовлення;
– вузли відео- та радіопрограм на запит;
– вузли Інтернет.

На рис. 67 відтворено узагальнену модель мережі доступу, в якій відображено її основні ділянки, елементи, блоки та системи.

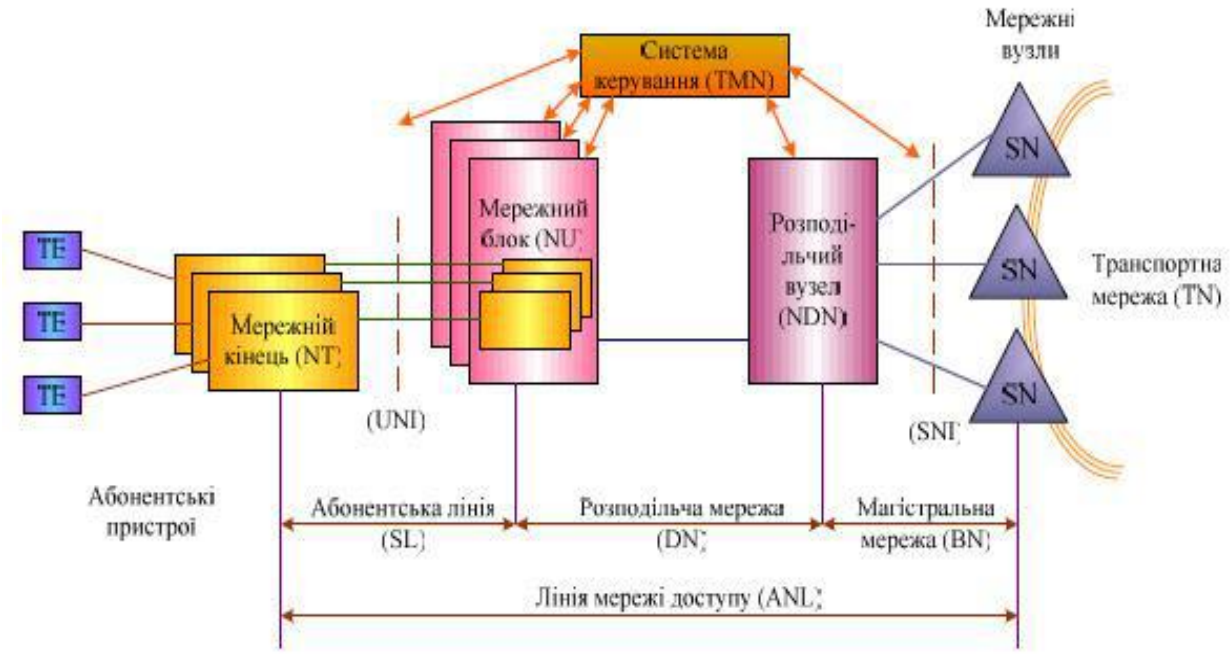


Рисунок 67 – Модель мережі доступу

На цій моделі мережа доступу є сукупністю абонентських ліній та обладнання (станцій) місцевої мережі, які забезпечують доступ абонентських терміналів до транспортної мережі та місцевий зв'язок без виходу в транспортну мережу. Мережеве закінчення NT дає змогу під'єднувати один або декілька користувацьких терміналів TE. Мережевий блок N забезпечує первинний доступ через мультиплексування й концентрацію трафіку та каналів, а розподільчий вузол DN – доступ абонентських пристроїв TE до сервісних вузлах SN. У даній узагальненій моделі мережі доступу ITU-T уперше вводиться поняття «лінія мережі доступу». Це лінія, яка з'єднує мережеве закінчення NT з сервісним вузлом SN і проходить через усю мережу доступу. Вона може бути утворена фізичним ланцюгом (колом), каналом (аналоговим або цифровим), складовим каналом, віртуальним каналом або декількома каналами для однакових або різних послуг. ALN проходить через абонентську лінію SL, інтерфейс UNI мережевий блок NU, розподільчу мережу DN, мережевий розподільчий вузол NDN та магістральну (транспортну) мережу BN.

Модель мережі доступу, визначена ITU-T, відрізняється від звичної схеми мережі абонентського доступу на базі міської телефонної мережі. Для реалізації універсальних можливостей мережі доступу використовуються розглянуті вище системи передавання мідними лініями з застосуванням широкосмугових технологій, оптичного зв'язку та радіосистеми.

8.10 Ієрархія мереж доступу

З точки зору мережевого оператора, мережі доступу можна класифікувати відповідно до ієрархії сегментів: LAN, MAN, WAN. На рис. 86 наведено схему такої структурованої мережі доступу.

Структуризація мережі доступу ґрунтується на принципі побудови ієрархічної моделі організаційної структури мережі. Ця модель відображає ієрархію рівнів доступу, розподілу та ядра.

Перераховані рівні, відповідно до побудови мереж доступу, можна розглядати як; рівні замикання трафіку в процесі організації внутрішньосегментних зв'язків через опорні вузли; рівні розташування сервісних вузлів. Функції розподільчих вузлів при цьому покладено на опорні вузли відповідних рівнів.

Таким чином, побудова мережі доступу зводиться до організації сегмента формування вихідного трафіка СФВихТ від мережевих закінчень КТ до опорного вузла того рівня, до якого під'єднано відповідні сервісні вузли. Якщо оператор поєднує свою діяльність з діяльністю провайдера послуг, він може зосередити функції розподільчого вузла та сервісного вузла (вузлів) у одному опорному вузлі.

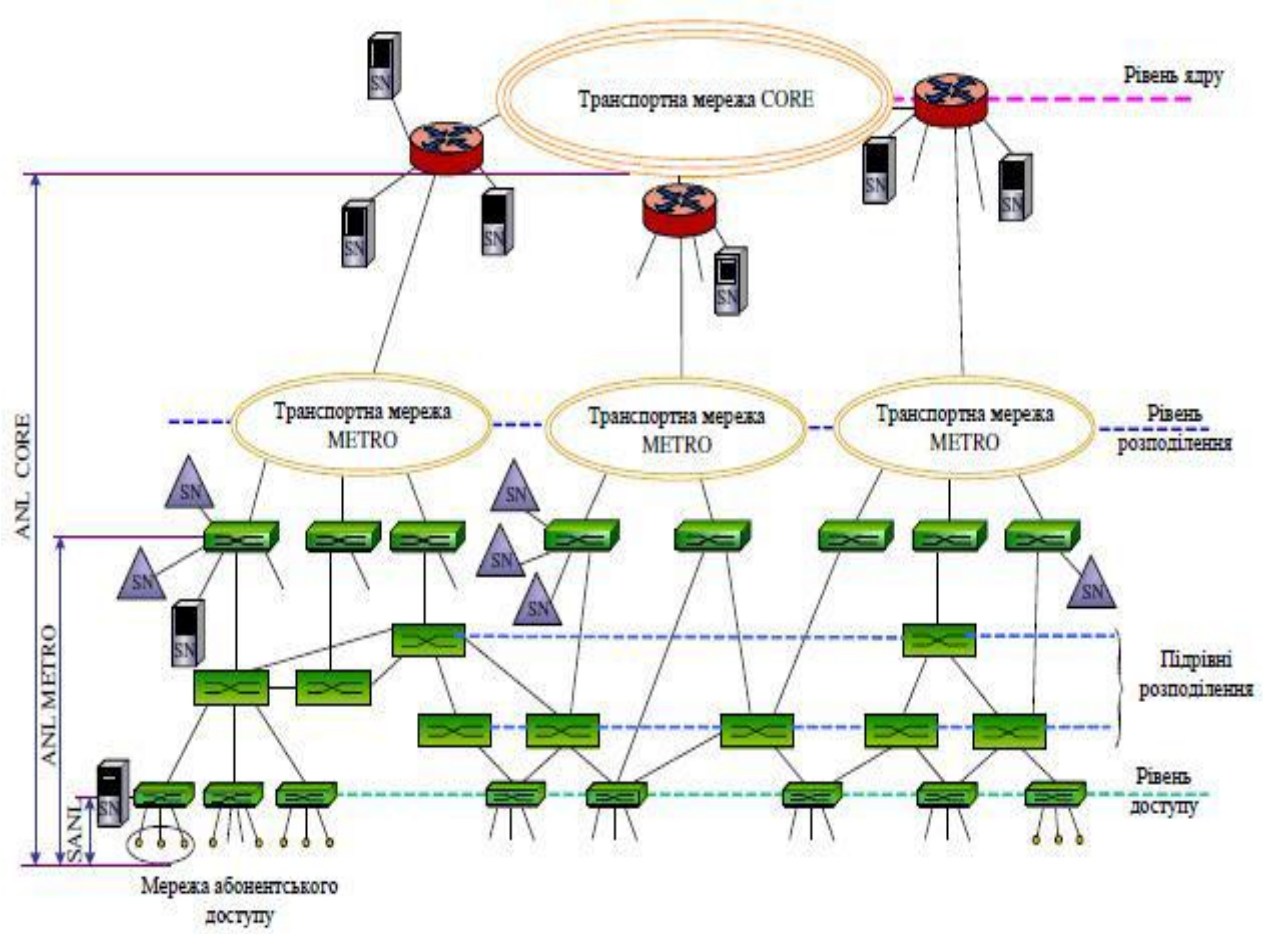


Рисунок 68 – Схема структурованої мережі доступу

Сервісні вузли SN різних провайдерів розосереджені в мережі. У загальному випадку, доступ до них можна здійснювати через транспортні мережі різних рівнів (METRO, CORE). Хоча канали транспортних мереж забезпечують досить широку смугу пропускання, канали мереж доступу залишаються розрахованими на меншу швидкість.

Ієрархічна модель організаційної структури мережі допускає подання рівня розподілу кількома підрівнями, кількість яких залежить від ступеню агрегації інформаційних потоків, які доправляються в транспортну мережу. Малопотужні потоки об'єднуються в комутаційних вузлах підрівнів розподілу до необхідного ступеня агрегації та остаточно концентруються у вузлах доступу – терміналах транспортної мережі. Ступінь концентрації залежить від технології мультиплексування, яку застосовують.

Ділянки мереж доступу, утворені використанням комутаційних вузлів підрівнів розподілу, можуть розглядатися як самостійні сегменти та мають назву «мережі міжвузлового зв'язку». Топологія фізичних зв'язків у сегментах NCN визначається на основі загальних правил побудови сегментів, а також вимог надійності та живучості мережі.

Вузли підрівнів розподілу є суто транзитними вузлами, а лінії зв'язку, які забезпечують їх поєднання, називають з'єднувальними лініями.

Традиційно мережі міжвузлового зв'язку NCN масштабу MAN класифікують як:

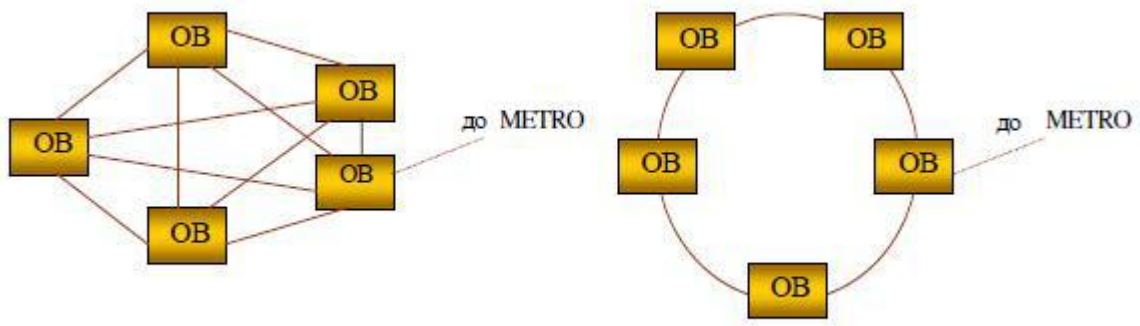
– нерайоновані;

– районовані без вузлування;

– районовані з вузлуванням (термінологія телефонних мереж), що, характеризує ступінь розгалуженості мережі.

Нерайонована NCN є зоною, в якій мережа NCN спростилася до розміру одного опорного вузла, що, крім своїх основних функцій, забезпечує доступ до транспортної мережі METPO.

Районована NCN без вузлування характеризується наявністю декількох районів обслуговування абонентів на її території, в кожному з яких знаходиться свій ОВ. Усі ОВ об'єднуються між собою для організації міжрайонного зв'язку, наприклад, за принципом «кожний з кожним» або в «кільце» (рис. 69 а, 69 б). Вихід у транспортну мережу організовується в одному з вузлів, який виконує функцію опорно-транзитного.



а) б)

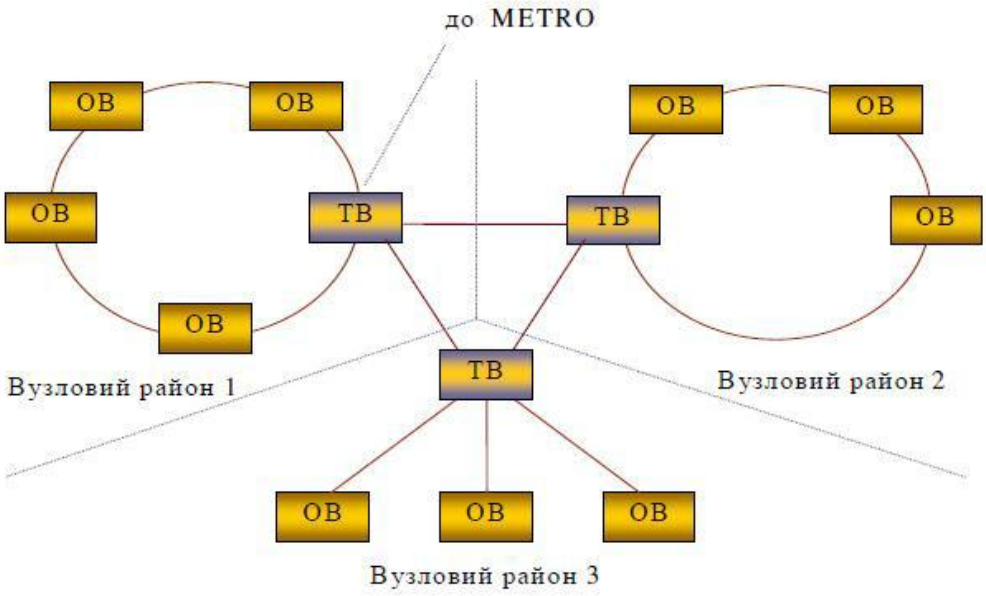


Рисунок 69 – Районована мережа NCN без вузлування: а – на основі мідного кабелю, б – на основі ВОК

Районована NCN з вузлуванням припускає наявність у мережі NCN транзитних вузлів (ТВ), через які можна організувати зв'язок міжрайонного обміну. Це вузли наступного за ієрархією підрівня розподілу. Наявність транзитних вузлів припускає утворення для кожного з них свого вузлового району, який містить певне число ОВ. Один з ТВ забезпечує вихід до транспортної мережі METRO.

Мережа міжвузлового зв'язку може містити сегменти, в яких використовуються різні телекомунікаційні технології, реалізовані на основі мідних кабелів і ВОК. Об'єднання таких сегментів здійснюється шляхом використання «шлюзів». Ці функції, як правило, покладаються на транзитні вузли.

ЛЕКЦІЯ 9. СИСТЕМА ОПЕРАТИВНО-ТЕХНІЧНОГО УПРАВЛІННЯ ТЕЛЕКОМУНІКАЦІЙНИМИ МЕРЕЖАМИ В УМОВАХ НАДЗВИЧАЙНИХ СИТУАЦІЙ

План

Вступ

1. Організація оперативно-технічного управління взаємозв'язаними телекомунікаційними мережами України.
2. Призначення, принципи побудови відомчої цифрової телекомунікаційної мережі ДСНС України.
3. Мережі доступу ВЦТМ ДСНС
4. Використання відомчої VPN

5. Сфери відповідальності за роботу ВЦТМ

6. Вимоги до організації Wi-Fi точок доступу до Інтернет (ВЦТМ)

7. Правила побудови мережі в центральних, окремих вузлах 1-го та 2-го рівня ВЦТМ (для проведення перевірок)

8. Питання безпеки ВЦТМ

9. Вимоги до пріоритетності та якості сервісів ВЦТМ ДСНС (QoS)

10. Вимоги до інженерної інфраструктури технологічних приміщень (серверних) для розміщення серверного та телекомунікаційного обладнання ВЦТМ *(для проведення перевірок)*

Висновки

Література

1. Теоретичні основи телекомунікаційних мереж : навч. посіб. /М.М. Климаш, Б.М.Стрихалюк, М.В.Кайдан. – Львів : вид-во УАД, 2011. – 496 с.

2. Система управління сучасними телекомунікаційними мережами / Кривуца В. Г., Беркман Л. Н., Климаш М. М. та ін.. – К. : ДУІКТ, 2009. – 352 с.

3. Буров Є. Комп'ютерні мережі / Є.Буров. – Львів : БаК, 1999. – 468 с.

Вступ

Для створення і розвитку системи оперативно-технічного управління телекомунікаційними мережами використовуються сучасні телекомунікаційні та інформаційні технології із застосуванням методів обробки інформації, аналізу та прогнозування розвитку ситуацій у реальному часі, методів експертних оцінок і колективного прийняття рішень з урахуванням рекомендацій Міжнародного союзу електрозв'язку щодо принципів управління телекомунікаціями.

9.1 Організація оперативно-технічного управління взаємозв'язаними телекомунікаційними мережами України

Згідно з Постановою КМУ від 29 червня 2004 р. № 812 «Порядок оперативно-технічного управління телекомунікаційними мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану» (редакція від 06.02.2019) *ДСНС України, як спеціальний споживач телекомунікаційних мереж, з метою впорядкування роботи відомчої інформаційно-телекомунікаційної мережі ДСНС здійснює загальний контроль за готовністю та функціонуванням телекомунікаційних мереж* в умовах надзвичайних ситуацій, надзвичайного та воєнного стану.

Цією постановою визначено:

– структуру та склад Системи оперативно-технічного управління (СОТУ);

– основні завдання СОТУ;

– основні завдання та функції Національного центр управління (НЦУ);[22]

– завдання та функції центрів управління мережами (ЦУМ);

– умови взаємодії НЦУ, ЦУМ, спеціальних споживачів та телерадіомовних компаній;

– обсяги та порядок подання інформації до НЦУ;

– вимоги до захисту інформації та гарантування безпеки СОТУ.

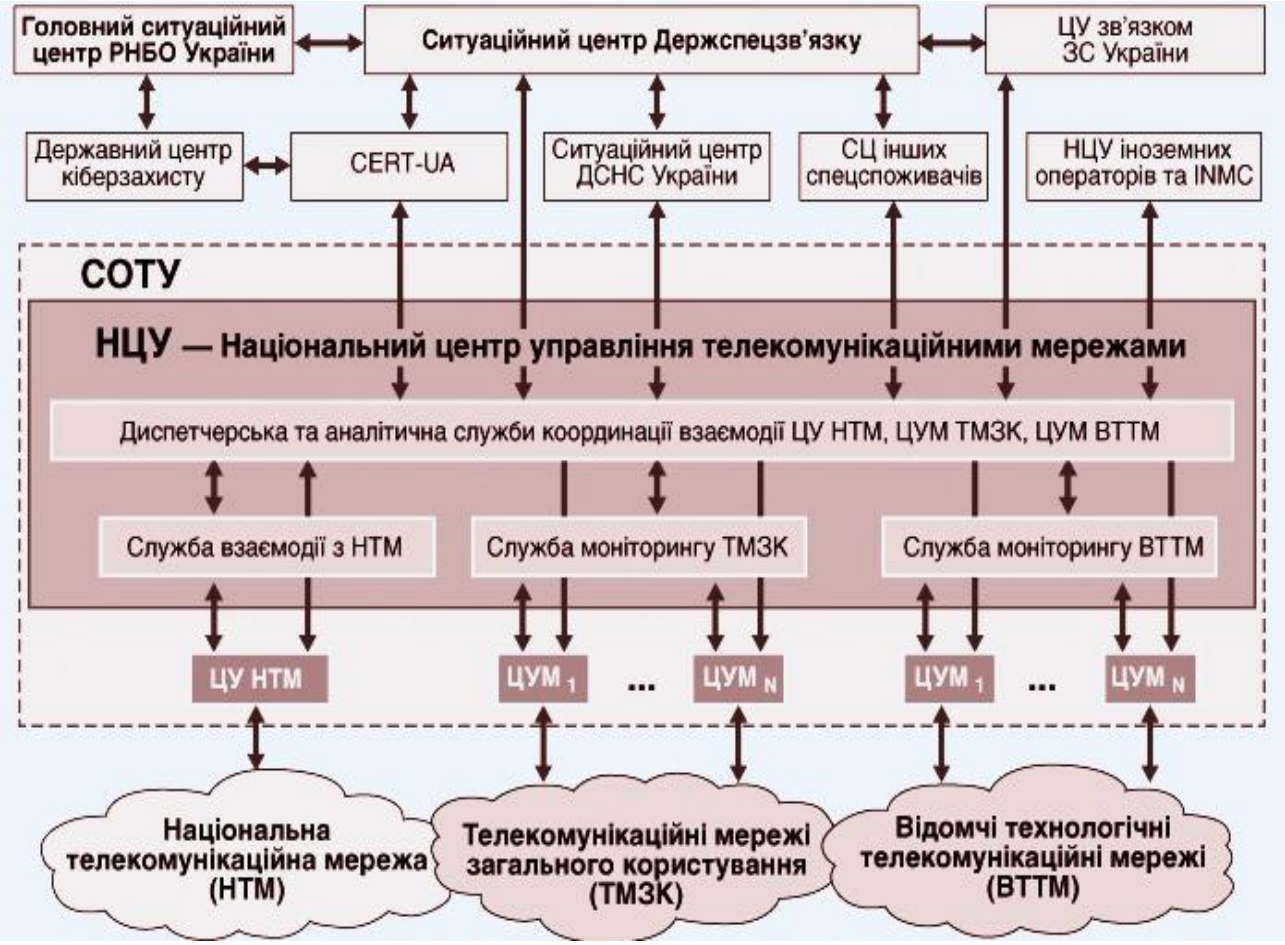


Рисунок 70 – Організація оперативно-технічного управління взаємозв'язаними телекомунікаційними мережами України

[22] Рішенням № 579 від 03.12.2019 Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації погоджено проект наказу Адміністрації державної служби спеціального зв'язку та захисту інформації України «Про затвердження Основних вимог до форми і строків подання інформації до Національного центру оперативно-технічного управління мережами телекомунікацій», що забезпечить ефективну взаємодію операторів телекомунікацій, центральних органів виконавчої влади (крім спеціальних споживачів), підприємств, установ та організацій, у власності, користуванні, господарському віданні чи оперативному управлінні яких є засоби та мережі телекомунікацій з НЦУ.

Для управління сучасними телекомунікаційними мережами розроблено структурну (функціональну), інформаційну та фізичну модель СОТУ, визначено її складові: телекомунікаційні мережі – об'єкти управління в СОТУ, ЦУМ операторів телекомунікацій та НЦУ – суб'єкти управління в СОТУ; визначено організаційні та технічні вимоги до складових СОТУ, які подано на інфограмі (рис.70).

До складу *системи оперативно-технічного управління електронними комунікаційними мережами (СОТУ) входять*, в т.ч. Центр (служба, підрозділ) управління електронними комунікаційними мережами (ЦУМ) – підрозділ постачальника електронних комунікаційних мереж та/або послуг, який виконує визначені функції безпосереднього оперативно-технічного управління власними електронними комунікаційними мережами та взаємодіє з НЦУ і центрами (службами) управління електронними комунікаційними мережами інших постачальників електронних комунікаційних мереж та/або послуг.

Постачальники електронних комунікаційних мереж та/або послуг повинні забезпечити взаємоз'єднання власних мереж та ЦУМ з НЦУ для забезпечення їхньої взаємодії та обміну інформацією управління. Оператори електронних комунікацій повинні забезпечити взаємоз'єднання власних мереж та ЦУМ з НЦУ для їхньої взаємодії та обміну інформацією управління.

Функцією НЦУ як головної складової Системи оперативно-технічного управління телекомунікаційними мережами України (СОТУ) *є накопичення вихідних даних про мережі, моніторинг стану мереж, забезпечення живучості, реагування на зміни стану мереж, оцінки їх готовності до роботи в умовах надзвичайних ситуацій (у тому числі при кібератаках на системи управління телекомунікаційними мережами) та в умовах надзвичайного і воєнного стану*.

Основні критерії для визначення *телекомунікаційних мереж об'єктами управління СОТУ* такі:

– розгалуженість цих мереж та покриття всієї території України або значної її частини, велика потужність та достатні надійність і живучість;

– сучасний технологічний рівень і постійний розвиток;

– висока якість телекомунікаційних послуг та велика абонентська база;

– наявність достатнього мережевого ресурсу, зокрема незадіяного (волокон, каналів, трактів), який можна використати в умовах надзвичайних ситуацій і який забезпечить мобілізаційну готовність в особливий період;

– наявність власних центрів управління мережами, високий рівень технічної експлуатації.

Розташування *функцій управління НЦУ* дозволяє:

– забезпечити незалежність функціонування операторів телекомунікацій від НЦУ;

– реалізує функції управління мережними ресурсами операторів з боку НЦУ в умовах особливого періоду шляхом створення двох стандартних інтерфейсів.

Організація системи управління мережними ресурсами дозволяє функції управління, яка властива НЦУ, виділити в окремий прошарок, розташований

між спільними та індивідуальними функціями управління, дає можливість НЦУ в разі необхідності здійснювати централізоване управління мережними ресурсами, тому що функції верхнього шару є індивідуальними для кожного оператора. НЦУ не впливає безпосереднього на функції верхнього рівня ієрархії управління.

Розташування функцій НЦУ у вигляді відповідного прошарку дозволяє використовувати НЦУ для здійснення незалежного контролю за якістю послуг, що надаються.

СОТУ – це принципи функціонування НЦУ та автоматизація процесів управління багаторівневою системою СОТУ з усіма її складовими для виконання:

– забезпечення накопичення вихідних даних про мережі;

– моніторингу стану мереж;

– оцінки готовності мереж у надзвичайних ситуаціях забезпечити живучість;

– реагування на зміни стану мереж;

– автоматизації аналітичного оброблення даних;

– прогнозування можливих проблемних та критичних ситуацій;

– моделювання варіантів розв'язання проблем та підготовки прийняття оперативних рішень щодо виходу з кризових ситуацій і доведення цих рішень (команд) до центрів управління мережами (ЦУМ) для подальшого виконання у межах мереж, ресурсами яких вони управляють.

Дії НЦУ спрямовуються на організацію ефективної взаємодії усіх учасників СОТУ та в будь-яких умовах гарантоване забезпечення спеціальних споживачів, органів державного управління, служб централізованого оповіщення, екстреної допомоги і населення телекомунікаційними ресурсами та телекомунікаційними послугами.

Реалізація функцій НЦУ потребує створення єдиного стандартизованого інтерфейсу між НЦУ і верхніми рівнями управління індивідуальних систем управління операторів телекомунікацій, а також інтерфейсу між НЦУ і мережною інфраструктурою цих операторів (тобто нижніми, спільними рівнями управління).

Технічна основа НЦУ:

– серверне обладнання, бази даних, автоматизовані робочі місця посадових осіб;

– структурована кабельна система;

– телекомунікаційне обладнання внутрішніх та зовнішніх комунікацій;

– обладнання інженерної інфраструктури (систем енергоживлення, заземлення, охолодження, вентиляції, пожежної та охоронної сигналізації, захисту інформації, пожежогасіння тощо);

– реагування на зміни стану мереж;

– автоматизації аналітичного оброблення даних;

– прогнозування можливих проблемних та критичних ситуацій;

– моделювання варіантів розв’язання проблем та підготовки прийняття оперативних рішень щодо виходу з кризових ситуацій і доведення цих рішень (команд) до центрів управління мережами (ЦУМ) для подальшого виконання у межах мереж, ресурсами яких вони управляють;

– загальне та спеціальне програмне забезпечення для аналітичної обробки, моделювання, прогнозування та підготовки рішень управління;

– інформаційно-лінгвістичне забезпечення для побудови підсистем центру;

– пристрій відображення колективного користування відеостіна, на якій відображаються основні параметри роботи мереж.

9.2 Призначення, принципи побудови відомчої цифрової телекомунікаційної мережі ДСНС України

9.2.1 Призначення відомчої цифрова телекомунікаційної мережі ДСНС України

Відомча цифрова телекомунікаційна мережа ДСНС (ВЦТМ) – логічна цілісна мультисервісна багаторівнева телекомунікаційна мережа, яка здійснює взаємодію із загальнодержавними телекомунікаційними мережами спеціального зв’язку та загального користування і включає в себе сукупність технічних засобів й обладнання телекомунікаційної мережі доступу і транспортної телекомунікаційної мережі для забезпечення інформаційної взаємодії між суб’єктами ВЦТМ як у мирний час, так і в особливий період.

Суб’єкт ВЦТМ – територіальні органи, заклади освіти, установи та підприємства, які підпорядковуються ДСНС.

Вузол ВЦТМ – сукупність технічних засобів телекомунікацій, які забезпечують доступ до ВЦТМ.

Сервіси ВЦТМ – сукупність телекомунікаційних послуг, які надаються за допомогою ВЦТМ.

Локальна телекомунікаційна мережа – комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень і звуків або повідомлень будь-якого виду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням у межах в межах адміністративної будівлі (комплексу адміністративних будівель) суб’єкта ВЦТМ.

ВЦТМ ДСНС організується для:

– забезпечення оперативного управління силами і засобами ДСНС;

– оперативної доставки інформації в процесі повсякденної діяльності всіх галузевих служб і підрозділів;

– оперативної взаємодії з органами державного управління та місцевого самоврядування, іншими міністерствами і відомствами.

ВЦТМ ДСНС України створюється як відомча спеціалізована захищена телекомунікаційна мережа з національним покриттям та інтеграцією служб.

Відомчий характер ВЦТМ ДСНС визначається її призначенням для оперативного управління органами управління ДСНС, його підрозділами і установами, а також оперативної обробки та передачі встановленої інформації, директив та розпоряджень під час виконання поставлених задач та в повсякденній діяльності, оперативної взаємодії з органами державного управління та місцевого самоврядування, іншими міністерствами і відомствами.

Спеціалізованість послуг ВЦТМ ДСНС означає:

– чітке визначення категорій та номенклатури користувачів послугами мережі і гарантоване їх обслуговування у визначені терміни та у відповідності до наданих пріоритетів;

– визначення видів і якості послуг, що включають набір спеціалізованих послуг, в тому числі із забезпеченням необхідного рівня захищеності (телефонний и документальний фіксований зв'язок, одночасну передачу мови та даних, передачу графічної інформації, конференцзв'язок, всі види передачі зображення, доступ до послуг Internet и Intranet).

Захищений статус ВЦТМ ДСНС – це можливість забезпечення передачі нетаємної, але важливої відомчої інформації, порушення конфіденційності, цілісності і (або) доступності до якої може нанести відповідні збитки ДСНС внаслідок її витоку. Захищеність передбачає здійснення протидії несанкціонованому доступу до інформаційних та системних ресурсів, технологічним базам даних і підсистемам управління вузловими комутаторами і всією мережею в цілому, наявність механізмів захисту інформації в каналах зв'язку, автентифікації суб'єктів і ідентифікації об'єктів інформаційного обміну.

Національний статус ВЦТМ ДСНС визначається її розповсюдженням на всі регіони України і можливістю її інтеграції в Єдину національну мережу зв'язку України.

Інтеграція служб в ВЦТМ ДСНС передбачає:

– реалізацію в межах єдиного технологічного простору (на єдиній технічній платформі) всіх передбачених нормативними документами видів зв'язку та інформаційного забезпечення, а саме:

– диспетчерського зв'язку ДСНС зі службою аварійного телефонного виклику «01» (112);

– відомчого телефонного зв'язку;

– відомчих систем документального, факсимільного зв'язку і передачі даних;

– відомчої системи зв'язку з рухомими об'єктами;

– відомчої системи розпоряджувально-пошукового зв'язку та оповіщення;

– системи телевізійного контролю;

– систем пожежно-охоронної сигналізації тощо;

– пристосованість до роботи з різноманітним спектром сучасних абонентських пристроїв, що побудовані з використанням широкого набору телекомунікаційних стандартів інформаційної взаємодії (в тому числі з різними типами телефонів, факсів, модемів, комп'ютерів тощо);

– передачу мультимедійної інформації, тобто можливість передачі і обробки сигналів, які суттєво відрізняються за своїми характеристиками (наприклад, графіки, аудіо, комп'ютерні дані, відео тощо);

– надання користувачам широкого спектру телекомунікаційних послуг, які відрізняються своєю структурою, фізичною природою, а також якістю сервісу, що надається (документальний, аудіо-, відео- конференцзв'язок, локальна мобільність, наскрізний телефонний персональний номер, голосова пошта, системи обробки викликів Call-центрів тощо).

9.2.2 Принципи побудови ВЦТМ ДСНС України

Головним принципом побудови ВЦТМ ДСНС є створення на базі існуючих транспортних мереж національної телекомунікаційної мережі України корпоративної телекомунікаційної мережі з національним покриттям за рахунок використання сучасних систем проводового і безпроводного доступу, засобів захисту інформаційних і системних ресурсів.

Топологія ВЦТМ ДСНС

Топологію ВЦТМ визначає територіальне розміщення органів та підрозділів ДСНС, а саме:

– центральний апарат ДСНС України в м. Києві;

– міські управління Києва, обласні управління, що підпорядковані ДСНС України;

– міські та районні управління, що підпорядковані обласним управлінням ДСНС України;

– сили швидкого реагування, що підпорядковані ДСНС України.

За *топологією мережа будується за дворівневою радіальною схемою*, в якій реалізується:

1-й рівень – центральний апарат ДСНС України в м. Києві, обласні управління, міські управління Києва, сили швидкого реагування центрального підпорядкування;

2-й рівень – Обласні управління, міські управління міст Києва – підпорядковані міські та районні підрозділи.

На всіх рівнях повинно бути забезпечене включення в телефонну мережу загального користування, а також в відомчі телефонні мережі взаємодіючих структур – органів державного управління та місцевого самоврядування, перелік яких визначається відповідними нормативними документами ДСНС України.

Топологія ВЦТМ ДСНС набуває реалізації в *транспортній мережі* на базі каналів зв'язку ДСНС, в мережах доступу операторів (провайдерів) телекомунікацій та державних каналів зв'язку.

Транспортна мережа ВЦТМ ДСНС

Транспортна мережа ВЦТМ ДСНС реалізується з використанням як цифрових технологій і забезпеченням швидкості передачі с фіксованою смугою пропускання (швидкістю передачі), так і традиційних симетричних аналогових кабелів і радіорелейних ліній.

Транспортний рівень призначений для організації мультисервісного трафіка між елементами мережі, а також трафіка з іншими взаємодіючими мережами (загального користування, корпоративними тощо). Її реалізація здійснюється на умовах оренди каналів діючої інфраструктури приватних операторів (провайдерів) телекомунікацій, що надають послуги з доступу до мережі Інтернет та застосування каналів зв'язку ДСНС, державних каналів зв'язку спеціального призначення – національна телекомунікаційна мережа, телекомунікаційна мережа спеціального призначення.

Схема організації такої транспортної мережі може бути реалізована за дворівневим радіально-кільцевим принципом (рис. 71).

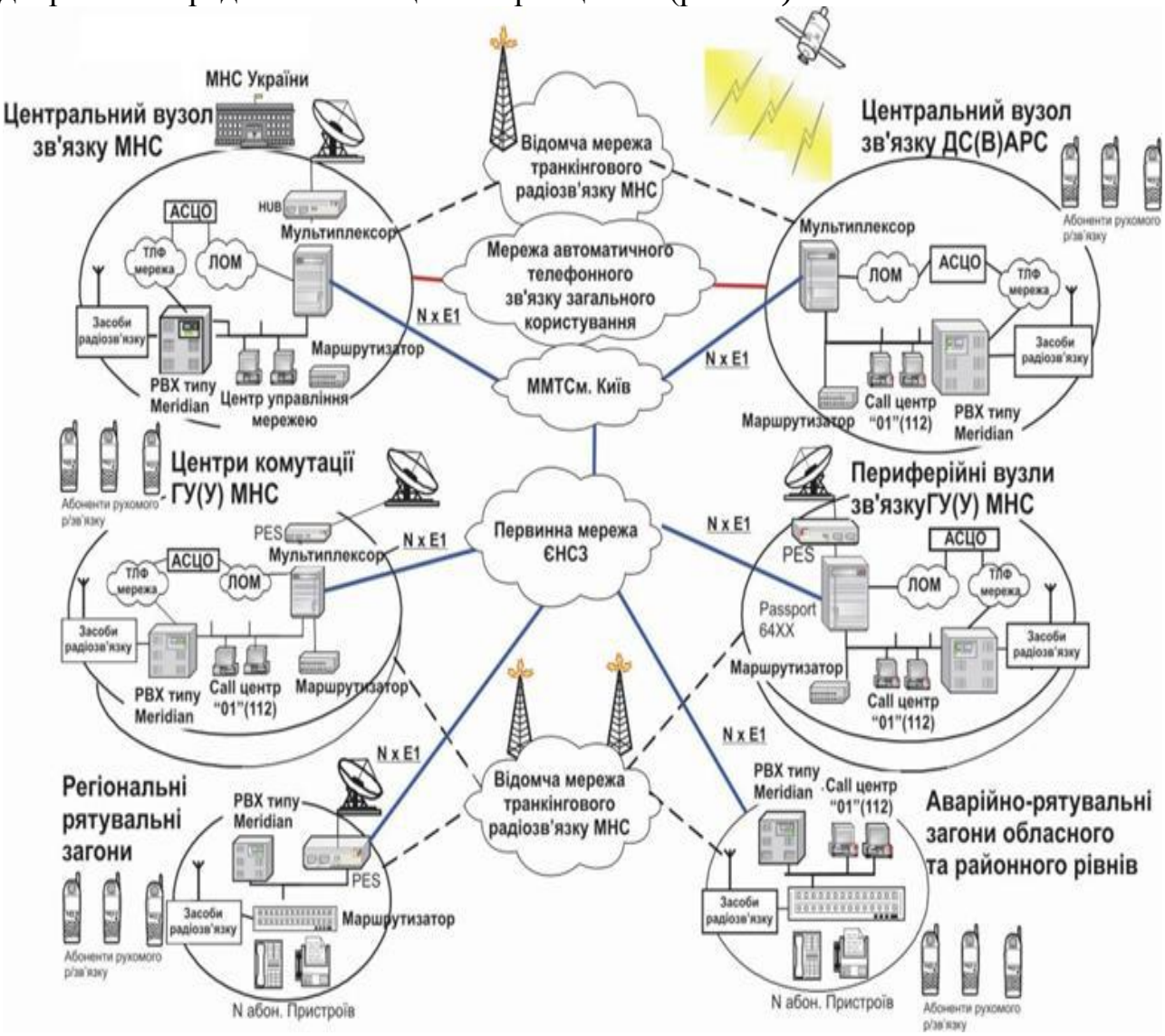


Рисунок 71 – Схема транспортної мережі ВЦТМ ДСНС

Це об’єктивно необхідним при застосуванні сил ДСНС поза межами пунктів постійної дислокації для ліквідації наслідків техногенних аварій та стихійних лих, а також у випадках аварій на проводових транспортних мережах.

9.3 Мережі доступу ВЦТМ ДСНС

9.3.1 Порядок організації роботи ВЦТМ ДСНС

ВЦТМ складається з центральних вузлів (основний і резервний), окремих вузлів 1-го і 2-го рівнів.

Центральний вузол ВЦТМ розміщено в адміністративній будівлі ДСНС.

Резервний центральний вузол ВЦТМ розміщено в будівлі, яка належить до сфери відповідальності Центру зв’язку та управління ДСНС України. На резервному центральному вузлу ВЦТМ здійснюється резервування сервісів ВЦТМ і створено резервний центр обробки даних.

Територіальні органи, підрозділи центрального підпорядкування, заклади освіти, підприємства, організації та установи, які безпосередньо підпорядковуються ДСНС, виступають *окремими вузлами ВЦТМ 1-го рівня* (окремі вузли ВЦТМ) і мають власну IP-адресацію.

Фіксована IP-адресація поширюється на підрозділи ДСНС, розташовані в населених пунктах будь-якого типу та їх районах. Підрозділи ДСНС, які не підпорядковуються безпосередньо апарату ДСНС, виступають окремими вузлами 2-го рівня.

Окремі вузли 2-го рівня підключаються до ВЦТМ через окремі вузли ВЦТМ.

ВЦТМ поєднує як самостійні підмережі територіальних органів, підрозділів центрального підпорядкування, закладів освіти, підприємств, організацій та установ сфери управління ДСНС із центральними вузлами ВЦТМ, так і може надавати можливість здійснювати обмін даними між окремими вузлами ВЦТМ без залучення обладнання центральних вузлів ВЦТМ.

Канали зв’язку між вузлами ВЦТМ будуються на базі:

– каналів зв’язку ДСНС;

– каналів зв’язку операторів (провайдерів) телекомунікацій, що надають послуги з доступу до мережі Інтернет та мають чинні атестати відповідності системи захисту інформації захищених вузлів доступу, видані Державною службою спеціального зв’язку та захисту інформації України;

– державних каналів зв’язку спеціального призначення – національна телекомунікаційна мережа, телекомунікаційна мережа спеціального призначення тощо.

Доступ до ВЦТМ підрозділів, які підпорядковані територіальним органам ДСНС, здійснюється через територіальні органи ДСНС.

Схему організації ВЦТМ наведено на рис. 72 .

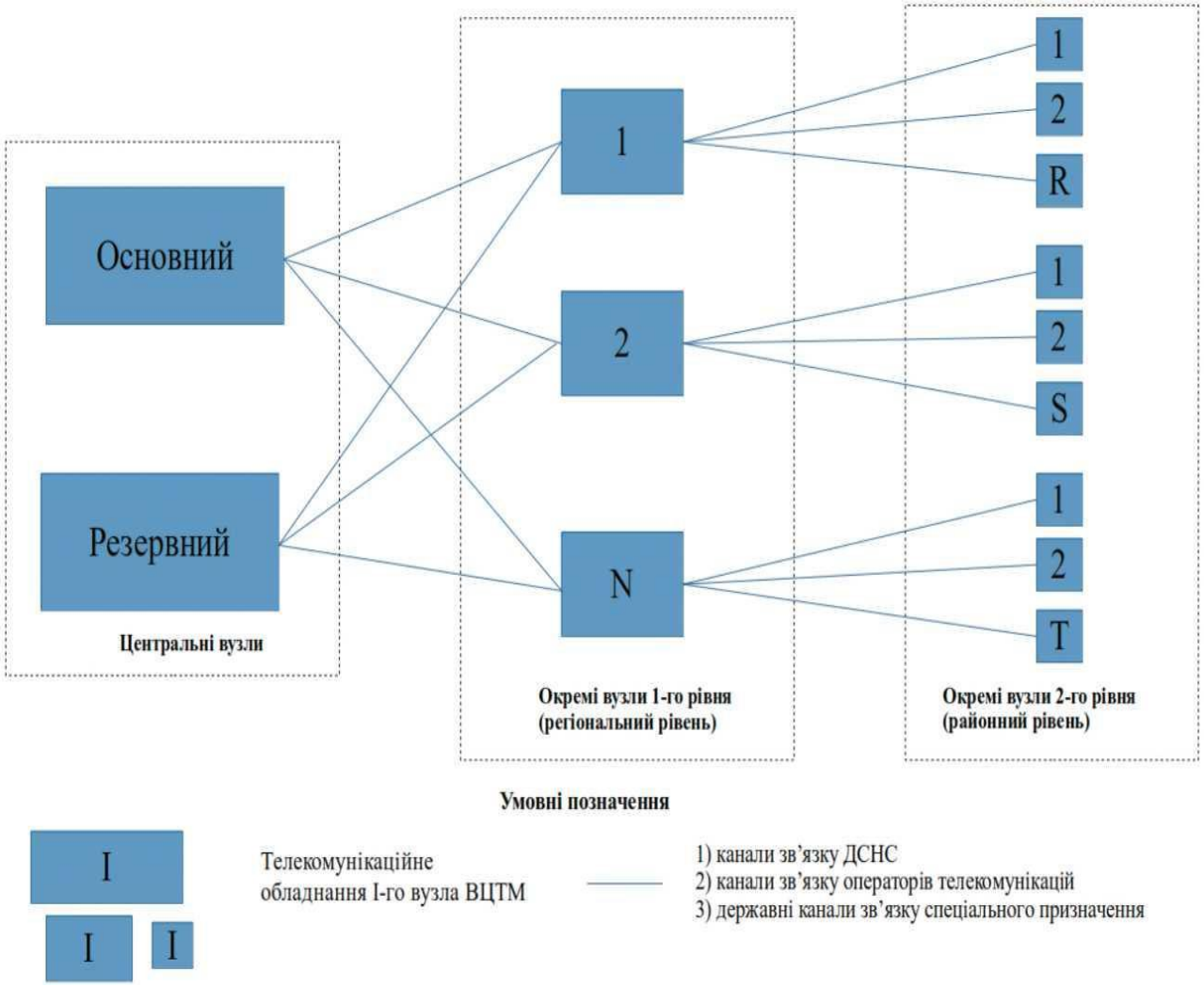


Рисунок 72 – Схема організації ВЦТМ

Топологію мережі центральних вузлів ВЦТМ наведено у рис. 73.

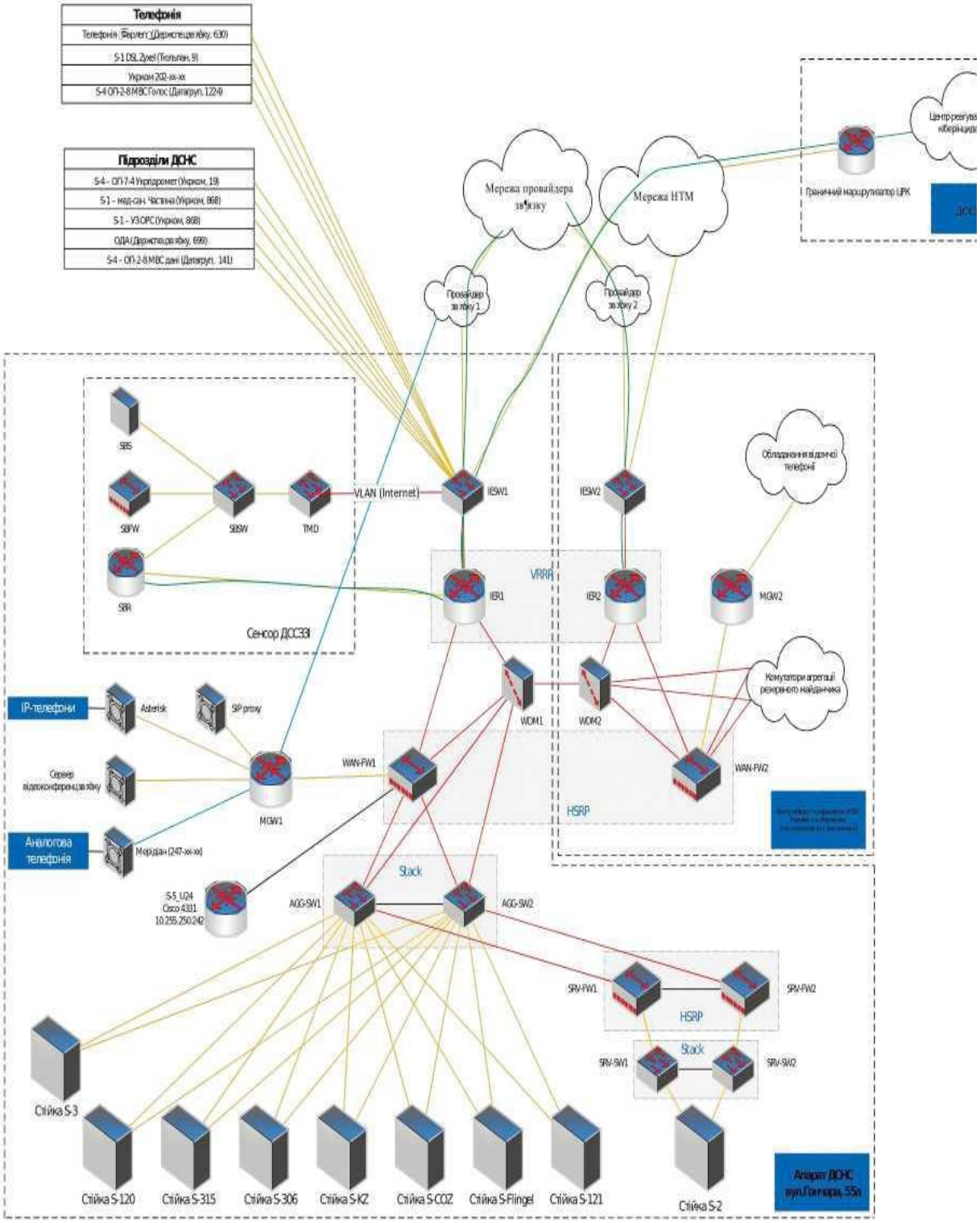


Рисунок 73 – Топологія мережі центральних вузлів ВЦТМ

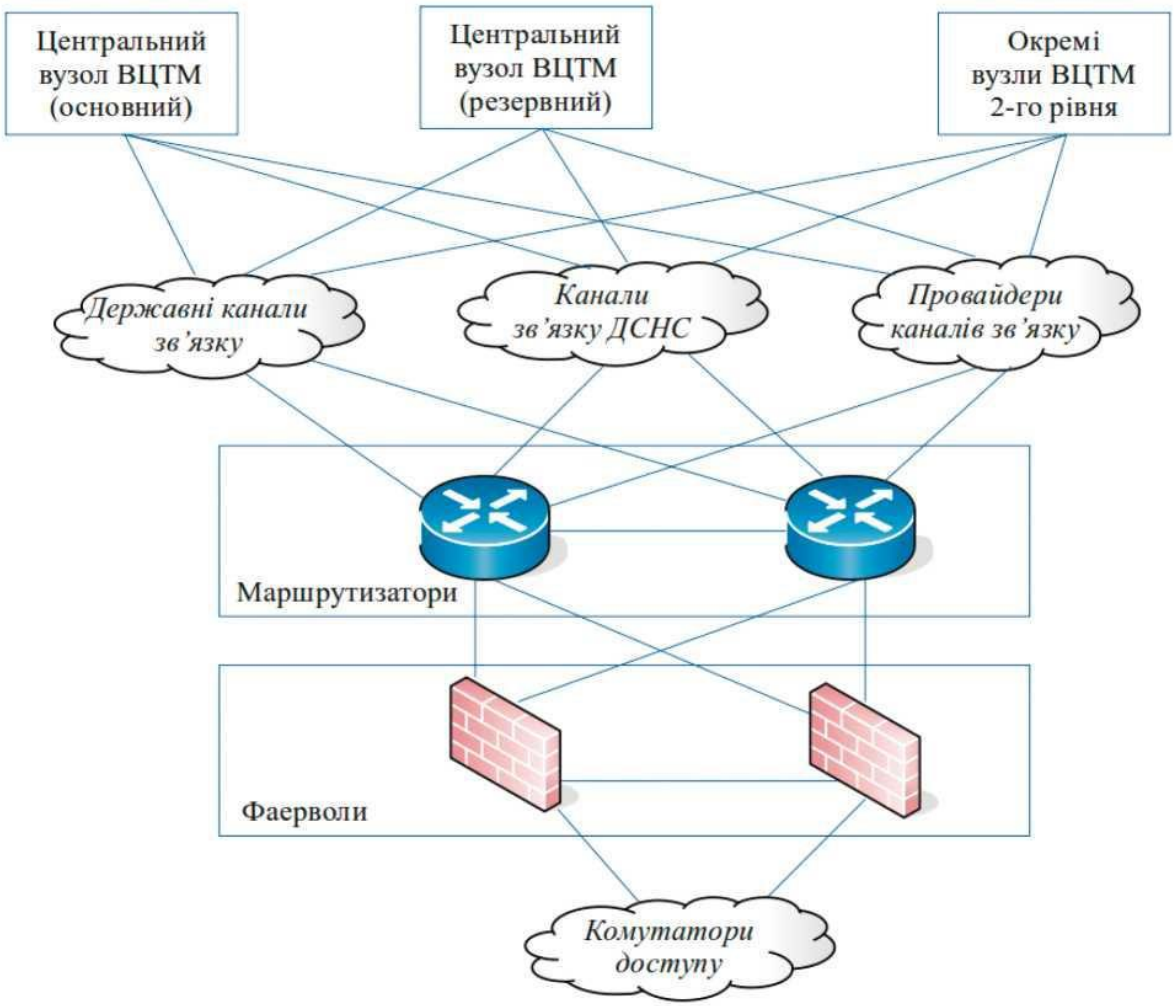


Рисунок 74– Схема підключення окремих вузлів ВЦТМ

Модернізацію, вибір обладнання вузлів ВЦТМ необхідно здійснювати за погодженням з апаратом ДСНС.

9.4 Використання відомчої VPN

Окремим способом підключення до ВЦТМ виступає під'єднання через відомчий сервер для організації віртуальної приватної мережі (VPN). VPN виступає складовою ВЦТМ.

Усі абоненти відомчої VPN мають бути ідентифіковані та отримувати фіксовані IP-адреси. Абонентам відомчої VPN надається обмежений доступ до сервісів ВЦТМ (відповідно до визначених потреб).

Відповідно до наданої заявки на отримання доступу до ВЦТМ через відомчу VPN адміністратором ВЦТМ створюється облікові записи VPN доступу до ВЦТМ з терміном дії на 1 рік. Для продовження дії облікового запису VPN доступу до ВЦТМ подається повторна заявка у першій декаді останнього місяця дії облікового запису VPN доступу до ВЦТМ. У разі неподання повторної заявки термін дії облікового запису VPN доступу до

ВЦТМ по закінченню терміну 1 рік припиняється. Кількість облікових записів для одного структурного підрозділу обмежена з урахуванням обґрунтованої службової необхідності.

Кінцевим обладнанням для термінації відомчих VPN виступає фаєрвол центрального вузла ДСНС, що поєднує в собі функцію VPN-концентратора та надає обмежений доступ до сервісів ВЦТМ (відповідно до визначених потреб).

9.5 Сфери відповідальності за роботу ВЦТМ

1. Налаштуванням мережевого обладнання вузлів відомчої телекомунікаційної мережі в апараті ДСНС та граничних маршрутизаторів та фаєрволів у підпорядкованих підрозділах займаються адміністратори центральних вузлів ВЦТМ.

2. У підпорядкованих підрозділах ДСНС адміністратори під мереж ВЦТМ визначаються власними наказами.

3. Розробленням та супроводом робочої документації ВЦТМ, впровадженням засобів захисту обладнання займається адміністратор відповідної підмережі ВЦТМ.

4. До основної документації на підмережі ВЦТМ відноситься:

– наказ про визначення адміністраторів;

– схема мережі рівня L1 з позначенням усіх комутаторів, фізичних серверів (файлових сховищ) та місць під'єднання всіх провайдерів, що надають телекомунікаційні послуги (рис.75);

– схема побудови телекомунікаційної мережі із підпорядкованими підрозділами ДСНС (із зазначенням моделей комутаторів, маршрутизаторів, провайдерів телекомунікаційних послуг та гарантованої швидкості каналів) (рис. 40);

– схема розташування мережевого обладнання (комутатори, маршрутизатори, модеми, сервери, мережеві принтери, WiFi-точки доступу) і розеток локальної мережі ДСНС та інших організацій по кабінетах на планах поверхів адміністративної будівлі з позначенням розмірів будівлі. У схемі мають бути позначені номери всіх кабінетів та мережевих розеток (рис.76);

– таблиця комутації мережевих пристроїв із зазначенням призначення всіх портів комутаторів та маршрутизаторів додаток;

– схеми організації електроживлення серверного приміщення (рис. 77);

– план поділу підмережі на VLAN додаток;

– перелік санкційованих мережевих пристроїв із зазначенням MAC-адрес;

– журнал обліку доступу технічних співробітників до серверних приміщень.

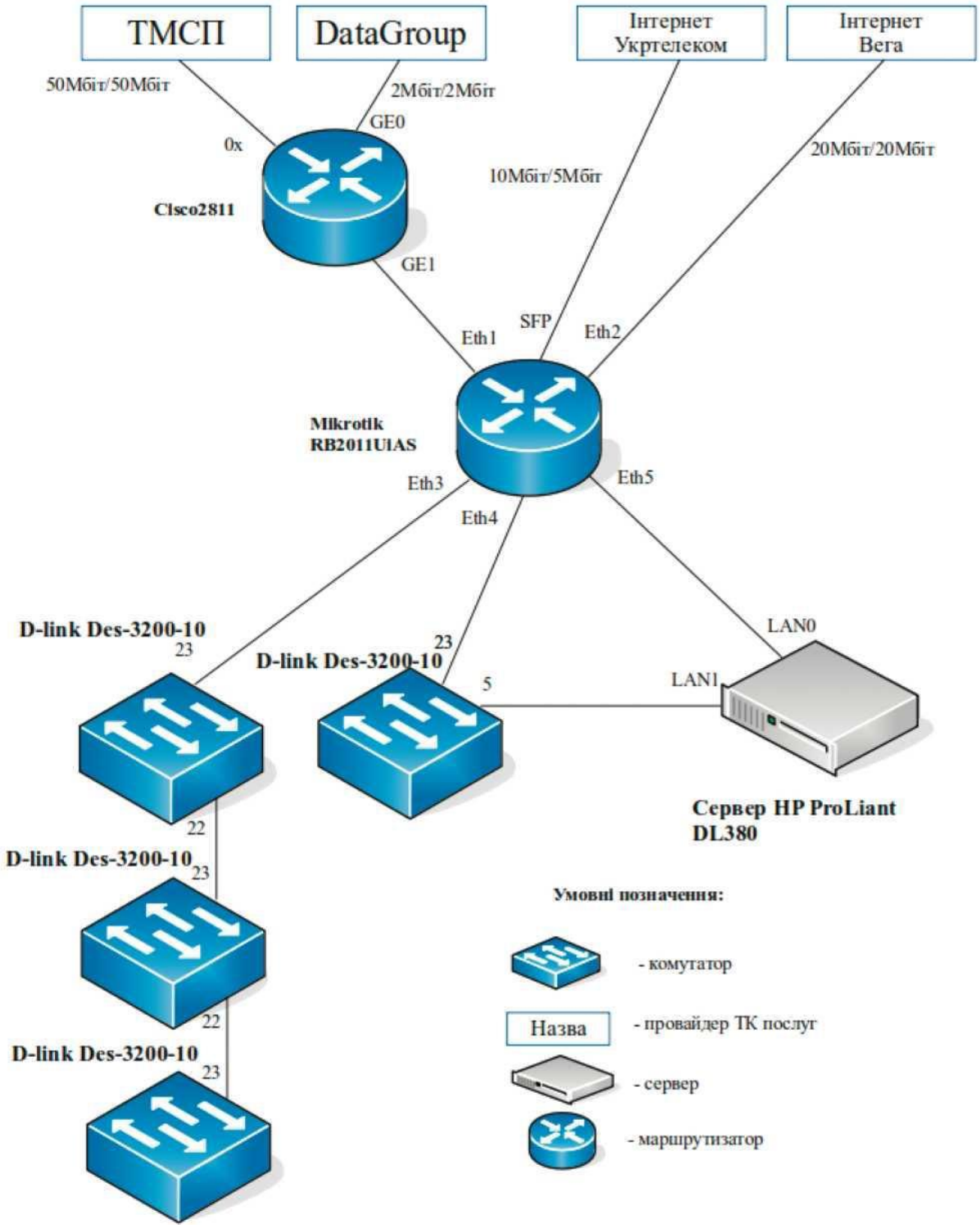


Рисунок 75 – Приклад оформлення схеми рівня L1

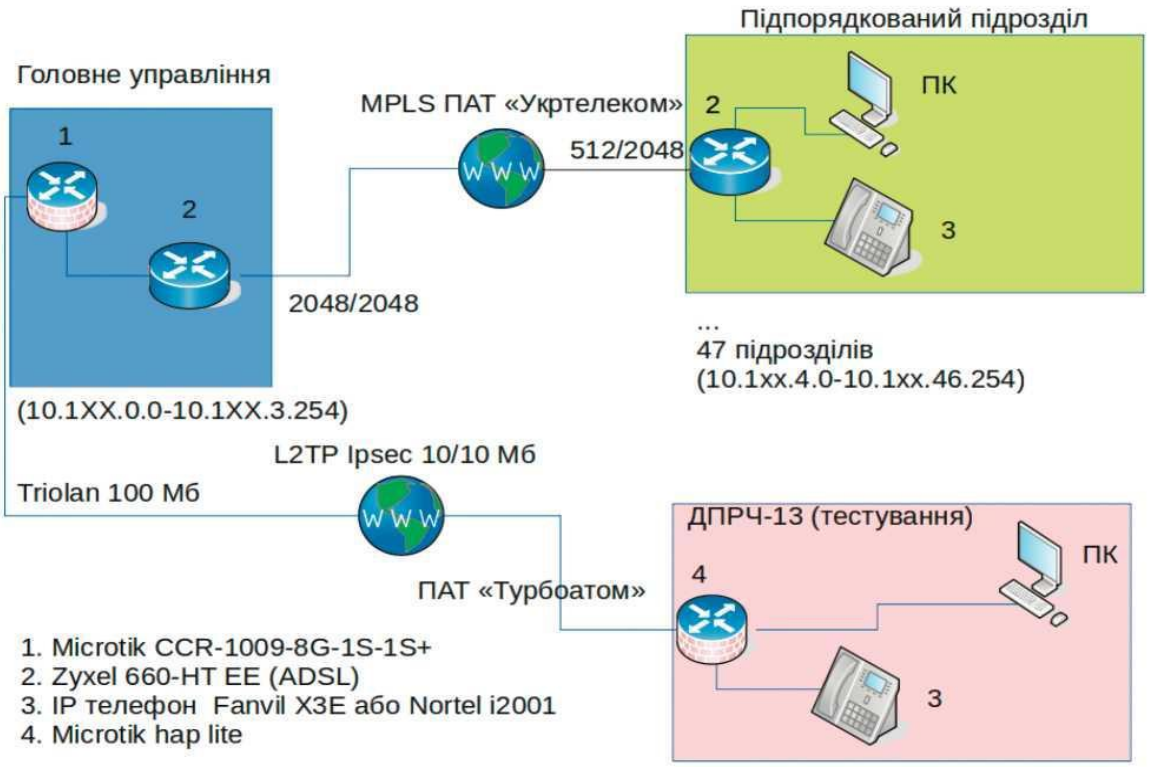


Рисунок 76 – Приклад оформлення схеми організації мережі між окремими вузлами ВЦТМ та їх підпорядкованими підрозділами

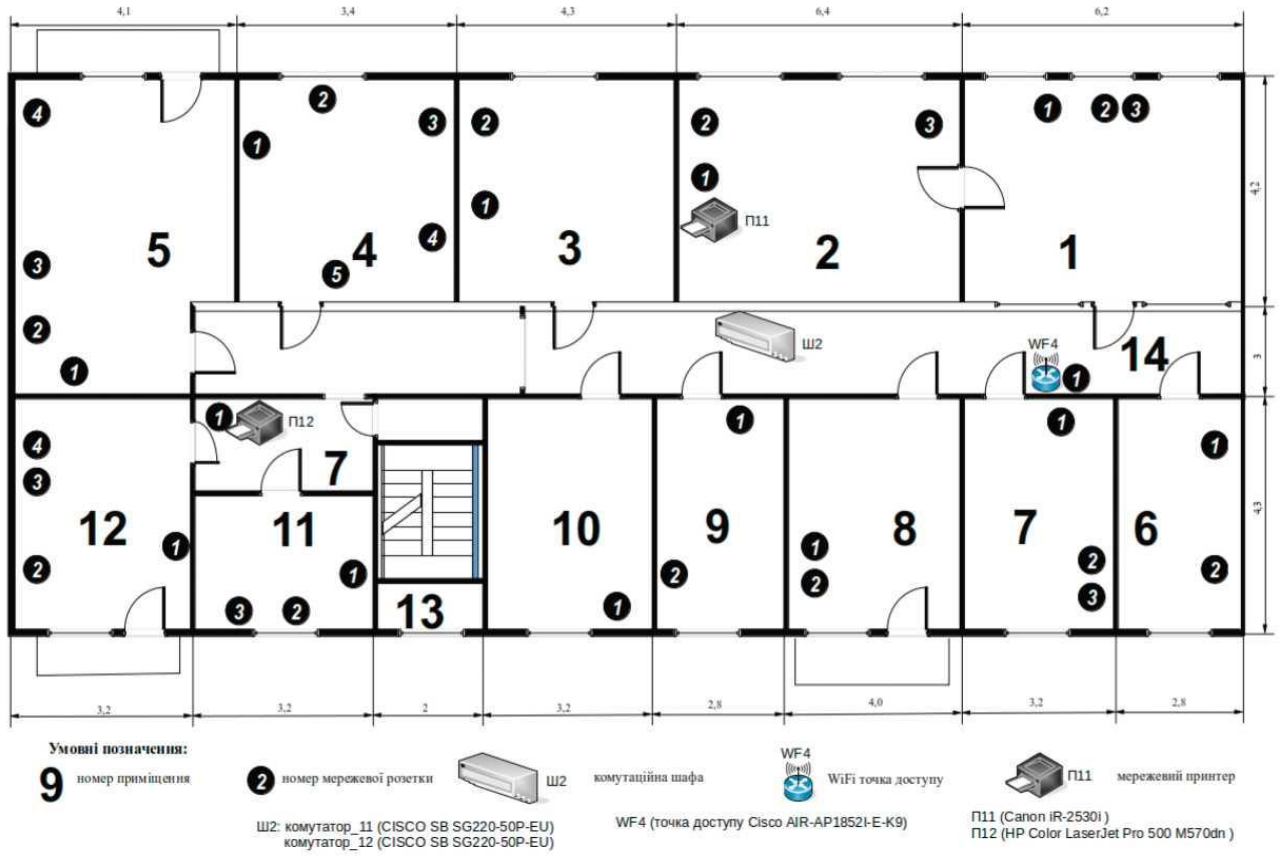


Рисунок 77 – Приклад оформлення схеми розташування мережевого

Обладнання в підрозділах ДСНС

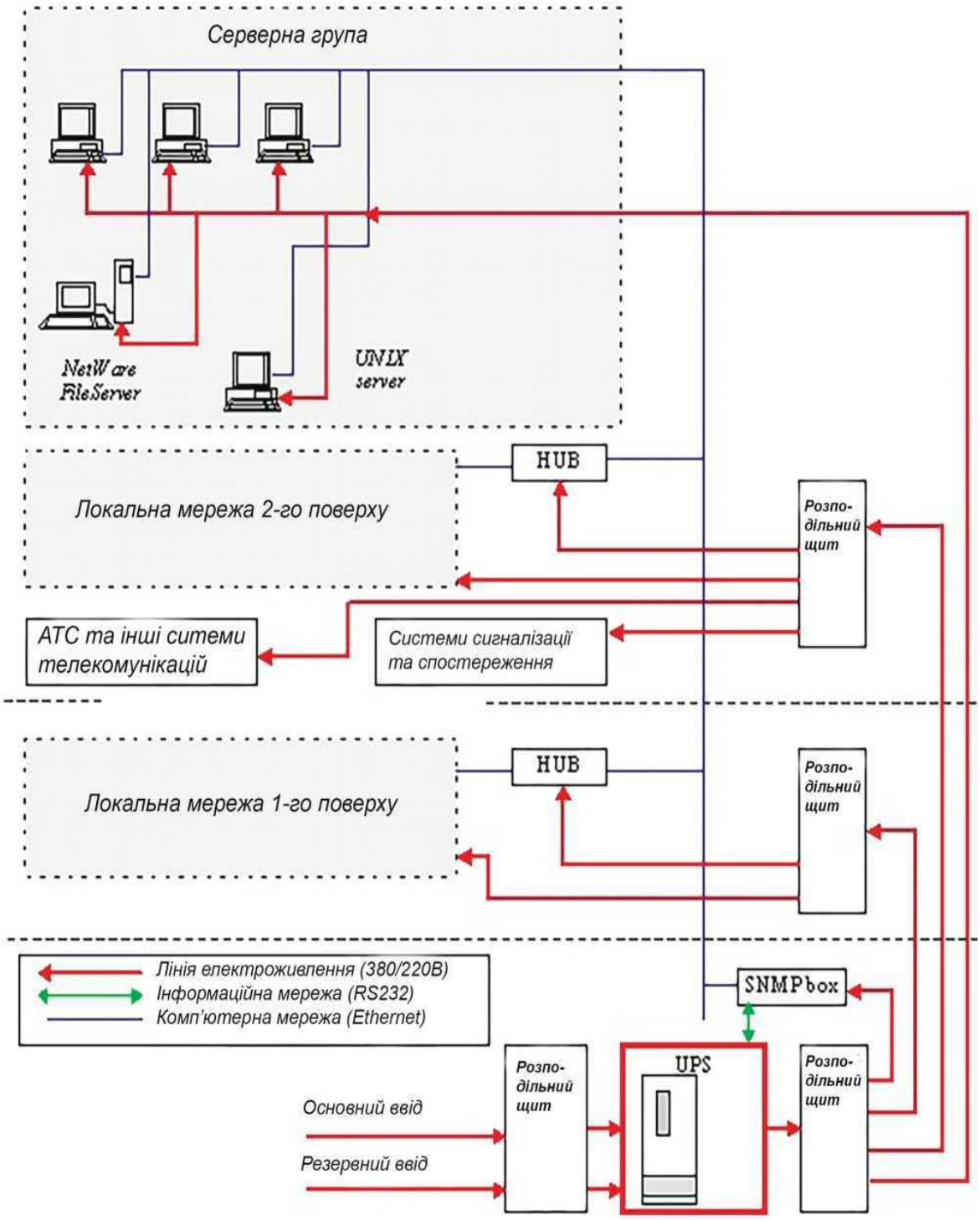


Рисунок 78 – Приклад оформлення схеми організації електроживлення серверного приміщення

5. Рекомендується здійснювати безпосереднє підключення до необхідних пристроїв лише за допомогою захищених протоколів, а саме SSH, SFTP та HTTPS.

9.6 Вимоги до організації Wi-Fi точок доступу до Інтернет (ВЦТМ)

1. Безпроводова мережа Wi-Fi має бути розгорнута в окремому сегменті мережі, який відокремлений та не перетинається із внутрішньою мережею ДСНС.

2. При налаштуванні обладнання Wi-Fi точок доступу необхідно встановлювати наступні параметри:

- приховати ідентифікатор мережі (SSID): ввімкнено;
- фільтрація пристроїв по MAC адресами: ввімкнено;
- тип автентифікації та шифрування: WPA2 PSK;
- функція WPS: заборонено.

2. За погодженням з апаратом ДСНС може бути дозволено організацію доступу до ВЦТМ через Wi-Fi.

9.7 Правила побудови мережі в центральних, окремих вузлах 1-го та 2-го рівня ВЦТМ (для проведення перевірок)

Структурована кабельна система має відповідати вимогам ДСТУ ISO/IEC 11801-1 та ДСТУ ISO/IEC 11801-2.

При проектуванні локальної мережі до кожного робочого місця має закладатися щонайменше по 2 мережевих кабелі вита пара.

Максимальна відстань горизонтальної проводки не має перевищувати 90 метрів.

Мережеве обладнання та мережеві кабелі мають відповідати категорії CAT5e та вище.

Телефонне обладнання та ПЕОМ дозволяється підключати одним мережевим кабелем через вбудований у телефон комутатор.

Усі мережеві кабелі від абонентів мережі мають підключатися до керованих комутаторів рівня доступу, розташованих на поверхах будівлі.

Керовані комутатори необхідно розташовувати таким чином, щоб мінімізувати загальну довжину мережевих кабелів від абонентів підмереж.

Від кожного комутатора рівня доступу має бути прокладено по два оптоволоконних магістральних кабелі до серверного приміщення.

Здійснювати закупівлю комутаторів доступу із функцією PoE.

Використання некерованих комутаторів при побудові мережі заборонено.

Прокладання кабелю в коридорах має здійснюватися за фальш стелею, за відсутності – в спеціальних кабель-каналах. У приміщеннях підведення мережевого кабелю до робочих місць має здійснюватися у спеціалізованих кабель каналах.

Структурована кабельна мережа має забезпечувати швидку перекомутацію ліній горизонтальної проводки та магістральних кабелів.

9.8 Питання безпеки ВЦТМ

На комутаторах рівня доступу та агрегації мають використовуватися такі технології:

– деактивація незалучених інтерфейсів на активному обладнанні;

– обмеження дозволених для транслювання MAC-адрес та фільтрації MAC-адрес;

– ARP фільтрація;

– Port Security;

– використання списків доступу ACL.

На фаєрволах у центральному вузлі ДСНС та територіальних вузлів зв'язку:

– застосування механізму DAI;

– використання Anti DDoS лічильників, що обмежують кількість оброблюваних широкомовних пакетів;

– використання захищених методів передачі даних, наприклад, IPsec тунелі;

– використання списків доступу ACL;

– блокування TCP/UDP, що не використовуються у повсякденній роботі; застосування фільтрації URL-адрес;

– використання захищених протоколів, що передають дані у шифрованому вигляді: HTTPS, SSH, SFTP.

В інформаційно-телекомунікаційних мережах (ІТМ) необхідно здійснювати такі адміністративно-організаційні заходи щодо організації безпеки:

– використання міжмережевих екранів (фаєрволів);

– розмежування корпоративної та публічної мереж;

– логування на обладнанні дій персоналу, який обслуговує обладнання ІТМ;

– розмежування рівнів доступу співробітників;

– надання кожному із співробітників, який займається адмініструванням ІТМ особистого облікового запису для авторизації на обладнанні;

– розробка і дотримання правил щодо складності паролів облікових записів.

Надання доступу до мережі Інтернет необхідно організовувати через фаєрвол з використанням проксі сервера. Використання прямого («прозорого») доступу до мережі Інтернет не рекомендується.

Строк зберігання логів мережевого обладнання – не менше 6 місяців.

Усі абоненти ВЦТМ маються бути ідентифіковані.

Доступ до мережі Інтернет абонентам ВЦТМ має бути обмежено за портами (виключно за потребами пов'язаними з виконанням службових обов'язків).

Адміністративні паролі доступу до пристроїв ВЦТМ мають оновлюватися щонайменше раз у квартал та кожного разу при зміні адміністраторів підмереж ВЦТМ. Адміністративний пароль має складатися щонайменше з 10 символів різного регістру, включно із літерами, цифрами та символами.

У підмережах ВЦТМ мають використовуватися засоби моніторингу мережі, система запобігання вторгненням та фільтрації трафіка по протоколах і портам. *Необхідно здійснення фільтрації http/https трафіка*.

При модернізації мережі перевага має надаватися апаратним засобам захисту мережі.

Підмережі ВЦТМ має бути поділено на окремі сегменти (VLAN) по функціональному призначенню та/або територіальному розміщенню (будівлям, поверхам, кабінетам). Мінімально має бути створено:

– VLAN для управління мережевою інфраструктурою;
– VLAN для серверів;
– VLAN для пристроїв телефонії;
– VLAN для пристроїв фінансового (бухгалтерського) структурного підрозділу, підрозділів по роботі з персоналом, підрозділів служби діловодства та інших.

При модернізації ІТМ необхідно розгорнути загальну систему моніторингу ІТМ з можливістю реалізації такого функціоналу:

– моніторинг доступності каналів зв’язку в режимі реального часу;
– моніторинг завантаженості каналу зв’язку, у тому числі з аналізом типу мережевого трафіка;
– моніторинг стану обладнання та активних аварій; опитування обладнання по протоколу SNMP.

Необхідно щонайменше щороку оновлювати вбудований у мережеве обладнання програмний код (firmware).

9.9 Вимоги до пріоритетності та якості сервісів ВЦТМ ДСНС (QoS)

Пріоритетність обслуговування сервісів під час передачі даних у ВЦТМ ДСНС за пріоритетністю у порядку спадання:

– відомча IP-телефонія;
– відомча система відеоконференцзв’язку;
– системи оперативного диспетчерського управління;
– відомча електронна пошта;
– системні мережеві сервіси;
– службові інформаційні системи;
– довідкові інформаційні системи;
– резервування даних;
– доступ до публічної мережі Інтернет.

9.10 Вимоги до інженерної інфраструктури технологічних приміщень (серверних) для розміщення серверного та телекомунікаційного обладнання ВЦТМ *(для проведення перевірок)*

Телекомунікаційне обладнання ВЦТМ має бути розміщено в окремих спеціально облаштованих серверних приміщеннях (серверні), що складається із зон для розміщення:

– серверного та телекомунікаційного обладнання; складових елементів системи електропостачання;

– складових елементів систем забезпечення мікроклімату, технічної електробезпеки, технічного захисту інформації, газового пожежогасіння (вогнегасників) та інше обладнання.

Ці приміщення має бути оснащене такими системами:

– система контролю доступу;

– система відеоспостереження;

– система автономного електроживлення;

– система пожежегасіння;

– система клімат-контролю (вентиляція, температура, вологість);

– структурованої кабельної системи;

– системи гарантованого електропостачання.

Розміри серверного приміщення визначаються в залежності від кількості серверних стійок та іншого габаритного обладнання.

При виконанні оздоблювальних робіт повинні застосовуватися матеріали, що відповідають санітарним нормам та правилам пожежної безпеки:

– за групами горючості;

– поширення вогню;

– димоутворювальної здатності;

– токсичності продуктів горіння та займистості у відповідності з категорією щодо вогнестійкості.

Стелі повинні мати гідроізоляцію для виключення можливості протікання води у приміщення серверної.

Не рекомендується використання в серверному приміщенні підвісної (фальш) стелі.

Приміщення серверної рекомендовано обладнувати фальш підлогою для розміщення комунікацій, конструкція якої повинна:

– бути виконана плитами з антистатичним покриттям з негорючих матеріалів або матеріалів відповідних груп горючості і ступенем вогнестійкості;

– мати висоту підпільного простору для прокладання в ньому комунікацій не менше 0,2 м;

– забезпечувати вільний доступ до комунікацій під час обслуговування; мати стійкість до горизонтальних зусиль при частково знятих плитах; давати можливість вирівнювання поверхонь підлоги за допомогою регульованих опорних елементів;

– гарантувати взаємозамінність плит.

Система забезпечення мікроклімату складається з підсистем вентиляції (за необхідності) та кондиціювання.

Структурована кабельна система складається з:

– підсистеми організації кабельних комунікацій;

– підсистеми розміщення монтажних шаф.

Системи протипожежного захисту складається з:

– системи пожежної сигналізації;

– автоматичної системи газового пожежогасіння (первинними засобами пожежогасіння);

– підсистеми димовидалення (за необхідністю).

Приміщення серверної згідно з ДБН В.2.5-56 обов'язково підлягають обладнанню системою пожежної сигналізації, тип застосовуваного обладнання системи та місця установки датчиків визначається на етапах технічного проектування відповідно до вимог ДБН В.2.5-56, ДСТУ EN 54-14, ДСТУ EN 54-13.

Приміщення серверних, які не підлягають обладнанню згідно з ДБН В.2.5-56 автоматичними системами газового пожежогасіння, мають бути оснащені первинними засобами пожежогасіння (пересувними або переносними газовими вогнегасниками).

Кліматичні умови в серверних приміщеннях характеризуються такими показниками: температура повітря та відносна вологість повітря.

У серверному приміщенні необхідно контролювати температуру і вологість, щоб вони постійно перебували в межах рекомендованих робочих діапазонів відповідно ДСН 3.3.6.042-99 і ANSI/TIA-942-A: температура повітря: від 20°C (68°F) до 25°C (68°F); відносна вологість повітря: від 40 % до 60 %.

Система гарантованого електропостачання складається з:

– підсистеми силової розподільної мережі (силове обладнання), підсистеми безперебійного електропостачання та розподілу електроенергії;

– підсистеми резервного електропостачання;

– підсистем заземлення (функціональне та захисне заземлення) та блискавкозахисту.

Система електропостачання серверної за своїм функціональним призначення відноситься до електроприймачів критичної (особливої) групи з неперервним режимом роботи та за ступенем надійності електропостачання належить до електроприймачів першої категорії згідно з ДБН В.2.5-23.

Систему електропостачання необхідно забезпечувати електроенергією від двох незалежних взаєморезервуючих джерел живлення. Переривання їх електропостачання, в разі порушення електропостачання від одного з джерел живлення, можна допускати лише на час автоматичного відновлення живлення.

Для електроприймачів особливої групи першої категорії надійності електропостачання необхідно передбачити додаткове живлення від третього незалежного взаєморезервованого джерела живлення, що забезпечує електропостачання визначеної тривалості. Джерелом живлення можуть бути

згідно з ДБН В.2.5-23 джерела безперебійного живлення або дизельна (бензинова) електростанція.

Електропостачання серверної згідно з ДБН В.2.5-23 повинно виконуватися від мережі з глухозаземленою нейтраллю 380/220 В та із системою заземлення типу TN-S, яка забезпечує найвищий рівень електробезпеки людей і обладнання.

Опір заземлювального пристрою не повинен перевищувати 4 Ом і 8 Ом відповідно для лінійних напруг 380В і 220В джерела трифазного струму або 220В і 127В джерела однофазного струму згідно з Правилами улаштування електроустановок, затвердженими наказом Міністерства енергетики та вугільної промисловості України від 21.07.2017 № 476. Цей опір необхідно забезпечувати з урахуванням використання всіх заземлювачів, приєднаних до робочого заземлення.

Заземлювальні пристрої мають бути механічно міцними та динамічно стійкими до струмів замикання на землю і не повинні термічно пошкоджуватися за час протікання зазначених струмів. Матеріал і переріз заземлювачів мають забезпечувати їх стійкість до корозії на весь період експлуатації.

Заземлювальний пристрій, який використовують для заземлення, протягом усього періоду експлуатації серверної повинен відповідати всім вимогам до заземлення: захисту людей від ураження електричним струмом у разі пошкодження ізоляції, умовам режимів роботи мереж, захисту електрообладнання від перенапруги, електромагнітної сумісності обладнання, тощо.

Комутатори локальної мережі окремих вузлів ВЦТМ, які під’єднуються до мережевого обладнання в серверному приміщенні, мають бути розміщені в спеціалізованих серверних шафах із замками.

Телекомунікаційне обладнання абонентського доступу встановлюється в телекомунікаційних шафах із замками, які розміщуються на поверхах будівель в коридорних або окремих приміщеннях та живляться від системи резервного (гарантованого) електроживлення.

Серверні приміщення відносять до режимних. Повинно бути визначено внутрішніми наказами перелік осіб, які мають доступ до цих приміщень. Відвідування приміщень має відбуватись із занесенням у журнал інформації про всіх осіб, час та мету їх відвідування.

ЛЕКЦІЯ 10. ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ДСНС УКРАЇНИ

План

Вступ

1. Організація телекомунікаційних систем та інформаційних технологій у ДСНС
2. Призначення і завдання телекомунікацій
3. Призначення і завдання інформатизації
4. Організаційні заходи стосовно впровадження програмного забезпечення та його облік
5. Організація роботи електронної поштової системи
6. Організація адміністрування систем телекомунікацій та інформатизації
7. Система управління інформаційною безпекою
8. Види робіт з ТЗІ, які можуть виконуватися підрозділами ТЗІ
9. Організація діяльності підрозділів ТЗІ
10. Умови та порядок надання повноважень на проведення робіт з технічного захисту інформації
11. Створення та впровадження комплексних систем захисту інформації
12. Створення та впровадження комплексів технічного захисту інформації
13. Кіберзахист та організація протидії кіберзагрозам
14. Організація заходів протидії кіберзагрозам
15. Система управління інформаційною безпекою
16. Автоматизована система оповіщення
17. Забезпечення функціонування апаратури і технічних засобів автоматизованих систем централізованого оповіщення та зв'язку, контроль за їх станом
18. Функціональна структура Системи 112

Висновки

Література

1. Теоретичні основи телекомунікаційних мереж : навч. посіб. /М.М. Климаш, Б.М.Стрихалюк, М.В.Кайдан. – Львів : вид-во УАД, 2011. – 496 с.

2. Буров Є. Комп'ютерні мережі / Є.Буров. – Львів : БаК, 1999. – 468 с.

3. Управління телекомунікаціями із застосуванням новітніх технологій / Кривуца В. Г., Беркман Л. Н., Стеклов В. К. та ін.]. – К.: Техніка, 2007. – 384 с.

Вступ

Організація телекомунікаційних систем та інформаційних технологій має відповідати вимогам чинних нормативно-правових актів. Перелік основних нормативних документів стосовно телекомунікаційних систем та інформаційних технологій розміщено на Порталі обстеження ІТ-систем органів виконавчої влади. Мова інтерфейсу програмних продуктів і документації інформаційних систем – українська, а у разі відсутності україномовного інтерфейсу – англомовна.

10.1 Організація телекомунікаційних систем та інформаційних технологій у ДСНС

Створення і впровадження нових телекомунікаційних систем та інформаційних технологій у ДСНС відбувається за погодженням зі структурним підрозділом, що відповідає за напрям інформаційні технології в апараті ДСНС.

Усі програмні, програмно-технічні (зокрема, вихідний код програмних засобів і команди компілятора, алгоритми, структури і формати даних тощо) та організаційні (регламенти, вимоги, інструкції, обмеження тощо) проектні рішення, які можуть застосовуватися для підтримки потрібного рівня експлуатаційних характеристик (якості) в процесі експлуатації й супроводу телекомунікаційних систем та інформаційних технологій, мають бути узгоджені, затверджені та передані замовнику виконавцем робіт (розробником) у задокументованому вигляді, необхідному для опису повної сукупності прийнятих проектних рішень і достатньому для їхнього незалежного використання (без звернення до розробника). Застосування недокументованих рішень заборонено.

10.2 Призначення і завдання телекомунікацій

Найважливішими завданнями телекомунікацій у ДСНС є:

– забезпечення оперативного та якісного прийому і передачі інформації про НС (НП);

– забезпечення стійкого і безперервного зв’язку для управління силами та засобами при виконанні завдань за призначенням;

– організація взаємодії та передачі інформації з іншими центральними органами виконавчої влади та місцевого самоврядування;

– забезпечення передачі інформації як між апаратом ДСНС, його територіальними підрозділами, підприємствами, організаціями та установами сфери управління ДСНС, так і всередині них між окремими структурними підрозділами та їх співробітниками.

10.3 Призначення і завдання інформатизації

Упровадження інформаційних технологій (ІТ) в діяльність підрозділів ДСНС відбувається шляхом автоматизації процесів управління діяльністю ДСНС, оперативного рішення завдань щодо забезпечення пожежної та техногенної безпеки, адміністративно-господарської діяльності і реалізується через засоби інформатизації, що забезпечує рішення завдань за призначенням.

Основним призначенням упровадження ІТ у ДСНС є автоматизація обробки інформації за напрямками діяльності ДСНС.

Основним завданням ІТ у ДСНС є:

– автоматизація системи оперативно-диспетчерського управління;

– впровадження та підтримка функціонування системи електронного документообігу;

– автоматизація основних напрямків адміністративно-управлінської діяльності (матеріально-технічне забезпечення, фінансово-господарська діяльність, і т.д.);

– підтримка функціонування Інтернет-ресурсів ІТС та ТС в ДСНС.

– Інформаційні технології повинні забезпечувати:

– взаємодію інформаційних потоків усіх рівнів;

– збереження цілісності інформаційних баз даних;

– оперативність та достовірність інформації;

– ефективне й надійне функціонування інформаційних систем та захист від несанкціонованого доступу та кіберзахист.

Використання ресурсів мережі Інтернет (каналів передачі даних, серверів і наданих ними сервісів та інформації, одержуваної з їхньою допомогою) має відбуватися відповідно до вимог нормативних документів щодо правил та порядку використання цих ресурсів.

10.4 Організаційні заходи стосовно впровадження програмного забезпечення та його облік

У системі ДСНС структурні підрозділи (або визначені посадові особи) за напрямом телекомунікаційних систем та інформаційних технологій відповідають за дотримання вимог законодавства з питань правової охорони комп'ютерних програм під час їх придбання, встановлення, використання, обліку та інвентаризації. У системі ДСНС використання не ліцензійного програмного забезпечення заборонено. У системі ДСНС пріоритетним є використання комп'ютерних програм вільного використання.

Користувач отримує доступ до тих видів інформаційних ресурсів, використання яких в повній мірі забезпечує виконання ним своїх службових обов'язків через комп'ютер, котрий має унікальне ім'я в локальній мережі.

Перелік комп'ютерних програм, які дозволені для встановлення на серверах та комп'ютерах користувачів системи ДСНС, зокрема, що знаходиться на позабалансовому обліку затверджується відповідними наказами ДСНС. Використання інших комп'ютерних програм має відбуватися за погодженням із підрозділом, що відповідає за напрямом інформаційних і телекомунікаційних технологій апарату ДСНС.

Облік програмного забезпечення здійснюється відповідно до вимог нормативних документів в електронному вигляді.

10.5 Організація роботи електронної поштової системи

Відомча електронна поштова система ДСНС застосовується для обміну службовими документами каналами телекомунікаційних мереж ДСНС, а також мережею Інтернет.

До складу Відомчої електронної поштової системи входить центральний поштовий сервер апарату ДСНС та власні поштові сервери головних управлінь (управлінь) ДСНС України в областях та м. Києві, які побудовано на базі серверного програмного забезпечення, рекомендованого для використання апаратом ДСНС, та функціонують на під доменах dsns.gov.ua.

Відомча поштова система використовується в інформаційних цілях, у тому числі з метою інформування, організації роботи, забезпечення внутрішніх та зовнішніх комунікацій.

Обмін електронними повідомленнями в ДСНС та з зовнішніми адресатами здійснюється лише з використанням електронних поштових скриньок в домені dsns.gov.ua.

Закладам освіти, Державному центру сертифікації ДСНС України та Українському гідрометеорологічному центру дозволяється здійснювати обмін електронними повідомленнями в ДСНС та з зовнішніми адресатами з поштових скриньок у під доменах edu.ua та доменах dcs.gov.ua, meteo.gov.ua відповідно.

10.6 Організація адміністрування систем телекомунікацій та інформатизації

Завдання організації адміністрування систем телекомунікацій та інформатизації призначені для виконання таких функцій:

– налаштування загальносистемних серверів та мережевого обладнання

– (операційних систем);

– контроль та надання дозволу на підключення комп’ютерів та периферійної техніки, користувачів до локальної мережі;

– усунення несправностей технічних засобів локальної мережі;

– розмежування прав доступу користувачів;

– організація доступу до загальних ресурсів та мережі Інтернет;

– здійснення заходів із антивірусного захисту;

– організація системи захисту від несанкціонованого проникнення із локальної мережі та мережі Інтернет;

– налагодження та підтримка системи резервного копіювання у мережі критично важливих даних, визначених відповідним наказом керівника установи.

Основними елементами адміністрування є сервер, телекомунікаційна мережа та комп’ютери користувачів.

До обов’язків адміністратора входить;

– технічна підтримка функціонування ІТС згідно регламенту;

– проведення профілактичних заходів;

– організація резервування ІТС та періодичне формування резервних копій даних;

– проведення заходів із кіберзахисту ІТС;

– забезпечення функціонування засобів телекомунікації.

Рекомендовано виконати розмежування рівнів доступу адміністраторів мережевого обладнання таким чином:

– надання адміністраторам центрального вузла ДСНС повного доступу до мережевого обладнання у центральному вузлі ДСНС та в регіональних підрозділах для можливості моніторингу мережі та своєчасного виявлення ризиків;

– надання адміністраторам регіональних підрозділів ДСНС обмеженого рівня доступу до мережевого обладнання, еквівалентного рівню базової конфігурації обладнання.

Рекомендовано здійснювати безпосереднє підключення до необхідних пристроїв лише за допомогою захищених протоколів.

10.7 Система управління інформаційною безпекою. Технічний захист інформації

Організаційно-технічні принципи, порядок здійснення заходів із технічного захисту інформації (ТЗІ), порядок контролю в цій сфері, характеристики загроз для інформації, норми та вимоги з технічного захисту інформації, порядок атестації та експертизи комплексних систем захисту інформації та комплексів технічного захисту інформації визначаються нормативно-правовими актами.

До об’єктів ТЗІ належить інформація, вимога щодо захисту якої встановлена законом. До об’єктів захисту в телекомунікаційних системах та інформаційних технологіях відноситься програмне забезпечення, що призначене для обробки цієї інформації.

Організаційно-технічні принципи, порядок здійснення заходів щодо ТЗІ, порядок контролю у цій сфері, характеристики загроз для інформації, норми та вимоги з ТЗІ визначаються нормативно-правовими актами з питань ТЗІ.

Дія Положення про технічний захист інформації у Державній службі України з надзвичайних ситуацій не поширюється на системи і засоби, що базуються на криптографічних методах захисту інформації.

Організація заходів протидії технічним розвідкам у ДСНС України регламентується нормативними документами Державної служби спеціального зв’язку та захисту інформації України.

Комплекси системи захисту інформації на об’єктах інформаційної діяльності від витоку технічними каналами створюються власними силами та із залученням організацій, що мають відповідні ліцензії (дозволи). Розроблення і впровадження заходів з ТЗІ використовують засоби, дозволені Державною службою спеціального зв’язку та захисту інформації України для застосування та включені до відповідних переліків.

Організація ТЗІ в органах ДСНС, щодо яких здійснюється ТЗІ, покладається на їх керівників. Підрозділи ТЗІ органів та підрозділи ДСНС здійснюють організацію, методичне забезпечення та контроль за впровадженням в органах та підрозділах ДСНС заходів ТЗІ.

Захист інформації в системах розглядається в контексті критично важливих секторів; захист інформаційної інфраструктури передбачає забезпечення гарантії того, що подібні та мережі стійкі до ризиків інформаційної безпеки, мережевої безпеки, Інтернет, так само як і ризиків кібербезпеки.

Напрямки захисту інформації формуються виходячи із конкретних особливостей інформаційної системи як об'єкту захисту. Виходячи з типової структури ІС і історично складених висновків робіт по захисту інформацією, можна виділити наступні напрямки:

– захист об'єктів інформаційних систем;
– захист процесів, процедур і програм обробки інформації;
– захист каналів зв'язку;
– пригнічення побічних електромагнітних наведень;
– управління системою захисту.

Забезпечення діяльності щодо заходів ТЗІ досягається:

– створенням комплексних систем захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах ДСНС на об'єктах інформаційної діяльності ДСНС;

– забезпечення сталого функціонування впроваджених в експлуатацію комплексних систем захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах ДСНС на об'єктах інформаційної діяльності ДСНС.

Виконання заходів кібербезпеки та ТЗІ є елементами системи управління інформаційною безпекою. За впровадження та функціонування системи управління інформаційною безпекою (СУІБ) відповідає керівник установи.

Основні функції системи управління інформаційною безпекою:

– виявлення та аналіз ризиків інформаційної безпеки;

– планування та практична реалізація процесів, спрямованих на мінімізацію

– ризиків ІБ;
– контроль цих процесів;

– внесення в процеси мінімізації інформаційних ризиків необхідних коригувань.

10.8 Види робіт з ТЗІ, які можуть виконуватися підрозділами ТЗІ

Розроблення, впровадження, випробування, обслуговування на об'єктах інформаційної діяльності комплексів (систем) ТЗІ, носіями якої є акустичні поля.

Розроблення, впровадження, випробування, обслуговування на об’єктах інформаційної діяльності комплексів (систем) ТЗІ, носіями якої є електромагнітні поля та електричні сигнали.

Розроблення, впровадження, випробування, супроводження комплексів технічного захисту інформації в інформаційних системах, інформаційних технологій із захистом інформації від несанкціонованого доступу.

Виявлення та блокування витоку мовної та видової інформації через закладні пристрої на об’єктах інформаційної діяльності.

10.9 Організація діяльності підрозділів ТЗІ

У системі ДСНС роботи з технічного захисту інформації проводяться підрозділами ТЗІ відповідно до Дозволу на проведення робіт з технічного захисту інформації для власних потреб, наданого ДСНС у встановленому порядку, та повноважень на проведення відповідних видів робіт відповідно до наказу ДСНС. Роботи з ТЗІ у системі ДСНС також можуть проводити організації, які мають ліцензію на проведення відповідних видів робіт з технічного захисту інформації та спеціальний дозвіл на провадження діяльності, пов’язаної з державною таємницею.

Повноваження підрозділу ТЗІ на проведення відповідних видів робіт з ТЗІ надаються наказом ДСНС. Координацію, облік проведених робіт та контроль за діяльністю підрозділів ТЗІ підрозділів здійснює Управління зв’язку та оповіщення ДСНС. Основні завдання, функції, обов’язки та відповідальність підрозділу ТЗІ визначаються Положенням про підрозділ ТЗІ, яке затверджується керівником підрозділу. Впровадження заходів ТЗІ в підрозділі, до складу якої входить Підрозділ ТЗІ, організовується керівником підрозділу.

Безпосередній контроль за виконанням завдань підрозділом ТЗІ покладається на керівника підрозділу зв’язку та інформатизації підрозділу. Організація заходів ТЗІ у центральному апараті ДСНС здійснюється Управлінням. Інструментальний контроль виконання вимог та норм технічного захисту інформації на об’єкті інформаційної діяльності, де розроблено та впроваджено підрозділом ТЗІ комплекс технічного захисту інформації, може здійснюватися Центром ТЗІ Вузла зв’язку та автоматизації ДСНС.

10.10 Умови та порядок надання повноважень на проведення робіт з технічного захисту інформації

Для одержання повноважень підрозділу ТЗІ на проведення окремих видів робіт або усього зазначеного переліку необхідно мати:

Призначених наказом керівника підрозділу спеціалістів для проведення обраних видів робіт, які мають повну чи базову вищу освіту за напрямом підготовки «Інформаційна безпека» або інженерно-технічну освіту фахового

спрямування, відповідного обраному виду роботи, з додатковою підготовкою на курсах перепідготовки та підвищення кваліфікації фахівців з питань ТЗІ чи стажем роботи у галузі ТЗІ за обраним видом роботи не менше 3 років, а також мають оформлені у встановленому порядку допуски до державної таємниці.

Нормативно-правові акти та нормативні документи з ТЗІ, необхідні для проведення обраних видів робіт.

Повірені в установленому порядку засоби вимірювань і контролю (як власні, так і залучені на договірних засадах), а також засоби ЕОТ в обсязі, що забезпечує проведення обраних видів робіт.

Приміщення, у яких впроваджено і атестовано комплекси ТЗІ та інформаційні системи з впровадженою КСЗІ з підтвердженою відповідністю.

Спеціальний дозвіл на провадження діяльності, пов'язаної з державною таємницею.

Окреме приміщення, в якому розміщується начальницький склад та працівники, а також апаратура підрозділу ТЗІ і забезпечується обмежений доступ сторонніх осіб.

Начальницький склад та працівники підрозділу ТЗІ повинні знати методики та порядок виконання робіт з ТЗІ відповідно до вимог нормативних документів та уміти застосовувати наявну апаратуру і обладнання.

10.11 Створення та впровадження комплексних систем захисту інформації

Етапи побудови КСЗІ визначають в рівній кількості для всіх і кожного окремо напрямків (з врахуванням всіх основ). Виділяють наступні етапи побудови КСЗІ:

– визначення інформаційних ресурсів (ІР), які підлягають захисту;

– виявлення всієї можливої кількості загроз безпеки ІР, які підлягають захисту;

– проведення оцінки чутливості і ризиків для ІР, які підлягають захисту, при виявленні великої кількості загроз;

– розробка проекту (плану) системи захисту інформації, знижаючого за вибраним критерієм ризику для ІР, які підлягають захисту, при виявленні великої кількості загроз.

– реалізація проекту (плану) захисту інформації;

– визначення якості реалізації системи захисту;

– здійснення контролю функціонування і управління системою захисту.

Аналіз стану і уточнення вимог до СЗІ об'єднує складові блоків основи, напрямки, етапи за принципом один з одним.

10.12 Створення та впровадження комплексів технічного захисту інформації

Захист інформації з обмеженим доступом при автономному використанні на ОІД пристроїв обробки інформації здійснюється шляхом створення комплексу ТЗІ, який складається із сукупності:

– організаційних заходів захисту від несанкціонованих дій з інформацією (для захисту конфіденційної інформації, що є власністю держави або вимога щодо захисту якої встановлена законом);

– організаційних заходів захисту від несанкціонованих дій з інформацією та технічних засобів захисту інформації від витоку технічними каналами за наявності можливості створення таких каналів (для захисту інформації,що становить державну таємницю).

За результатами спеціального дослідження приймається рішення про необхідність встановлення активних та/або пасивних засобів захисту. Після цього проводиться оцінка захищеності ІзОД від витоку технічними каналами на об'єкті ЕОТ (атестація комплексу ТЗІ).

Організаційні заходи захисту від несанкціонованих дій з інформацією при автономному використанні пристроїв обробки інформації:

– встановлення порядку користування пристрій обробки інформації, що використовується автономно (пристрій автономного використання) – ПАВ;

– встановлення порядку використання зовнішніх пристроїв пам'яті в ПАВ;

– визначення та встановлення обов'язків осіб, що користуються ПАВ та здійснюють контроль за користуванням ПАВ;

– встановлення порядку фізичного захисту ОІД, де функціонує ПАВ;

– визначення та встановлення змісту і порядку контролю за користуванням ПАВ.

10.13 Кіберзахист та організація протидії кіберзагрозам

Комунікаційні системи, які використовуються у ДСНС, відносяться до критичної інформаційної інфраструктури і є об'єктами кіберзахисту.

Об'єктами кіберзахисту в ДСНС є інформаційні системи та інформаційно-комунікаційні мережі, поштові та загальносистемні сервери.

Суб'єктами, які безпосередньо здійснюють у межах компетенції заходи із забезпечення кібербезпеки в ДСНС, є фахівці кібербезпеки, технічного захисту інформації, користувачі та інші.

Структурні підрозділи (фахівці) установи, які відповідають у межах компетенції за забезпечення кібербезпеки на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління:

– здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;

– здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз;

– розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту;

– забезпечують проведення контролю виконання заходів та функціонування засобів інформаційної безпеки;

– здійснюють адміністрування телекомунікаційних мереж, поштових та загальних серверів;

– надають дозвіл, контролюють та підтримують функціонування системи контролю та управління доступу до внутрішньої мережі, мережі Інтернет тощо;

– беруть участь у заходах щодо створення, впровадження та забезпечення функціонування системи управління інформаційною безпекою;

– забезпечують інформування про кіберінциденти керівництва установи, ДСНС та взаємодіють із іншими органами відповідно до чинного законодавства.

Закон України «Про основні засади забезпечення кібербезпеки України» не поширюється на діяльність, пов'язану із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення».

10.14 Організація заходів протидії кіберзагрозам

З метою забезпечення надійного функціонування засобів кіберзахисту в установі щороку проводиться визначення ризиків кібербезпеки, оцінка надійності засобів кіберзахисту, коригування поточного профілю кібербезпеки. Ці заходи виконуються фахівцями установи, у разі потреби до їх виконання можуть бути залучені сторонні фахівці чи організації в сфері кіберзахисту.

За рекомендаціями Державної служби спеціального зв'язку та захисту інформації України з метою запобігання кіберінцидентам і сприяння підвищенню рівня кіберзахисту електронних ресурсів та систем необхідно:

Провести аудит запроваджених заходів захисту та рівня інформаційної безпеки систем у цілому.

Провести роз'яснювальну роботу з працівниками, які користуються службовою електронною поштою, щодо правил та вимог безпеки, особливо в частині, що стосується вхідних листів (повідомлень).

Заборонити відкриття вкладень у підозрілих повідомленнях (листах від адресатів, щодо авторства яких виникають сумніви та зобов'язати користувачів службової електронної пошти негайно повідомляти про такі листи адміністратора безпеки.

Зобов'язати користувачів службової електронної пошти провести її ревізію на предмет виявлення листів, що мають вкладення «MoF critical IT needs_eng.xls», «Додаток №2.xls», заборонивши їх відкриття, та невідкладно повідомляти про наявність таких листів адміністратора безпеки.

Заборонити використання приватної електронної пошти для цілей службової діяльності.

Заборонити використання точок публічного доступу до Інтернет для входу до службової електронної пошти.

Адміністраторам безпеки рекомендовано звести до мінімуму мережеву активність усіх пристроїв систем управління з Інтернет, ужити заходів до дотримання вимог із сегментування, не допускати циркуляції технологічної інформації поза межами адміністративного сегмента мережі.

Для організації віддаленого доступу використовувати лише безпечні методи (наприклад, такі технологічні рішення, як VPN).

Для унеможливлення проведення атак типу Man-in-the-Middle з використанням техніки ARP-spoofing ужити заходів з налаштування статичних значень ARP-таблиць АРМ і серверного обладнання. Для цього здійснити прив'язку MAC-адрес АРМ до конкретного інтерфейсу комутатора, цим самим заборонивши підключення сторонніх пристроїв.

Передбачити моніторинг та фіксацію (журналювання) подій, які мають відношення до інформаційної безпеки (доступ до баз даних, адміністративний доступ до обладнання тощо).

Запровадити політику, що потребує використання лише надійних паролів.

Провести рекомендоване виробником оновлення програмного забезпечення, щоб запобігти вже виявленим уразливостям.

Контролювати створення аккаунтів на рівні адміністраторів системи.

Здійснити зміну авторизаційних даних до критично важливих вузлів системи, попередньо перевіривши їх на наявність процесів, які можуть скомпрометувати дані.

Проводити постійний аналіз вхідного/вихідного Інтернет-трафіку.

Проводити аналіз лог-файлів мережевого та серверного обладнання на наявність у них відомостей про аномальну активність (доступ до системи із систем, які перебувають поза адміністративним сегментом мережі; наявність нелегітимних авторизаційних даних).

Здійснювати перевірку ПЕОМ адміністраторів мережі та критично важливих вузлів системи на наявність підозрілих процесів і програм (наприклад: системних служб, що запускаються не зі стандартного розташування; програм, що не мають цифрового підпису виробника, тощо).

Дотримуватися організації заходів протидії кіберзагрозами у відповідності до рекомендацій Національного стандарту України ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT) Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки.

10.15 Система управління інформаційною безпекою

В Україні та в усьому світі щороку вчиняються десятки тисяч злочинів з використанням інформаційно-комунікаційних технологій, програмних, програмно-апаратних засобів, інших технічних і технологічних засобів та

обладнання. Україна, як і всі країни світу, щодня зіштовхується з викликами у сфері кібербезпеки.

Відповідно до українського законодавства, кібербезпека – це захищеність життєво важливих інтересів людини й громадянина, суспільства та держави у процесі використання кіберпростору, яка забезпечує сталий розвиток інформаційного суспільства і цифрового комунікативного середовища, своєчасне виявлення, запобігання та нейтралізацію реальних і потенційних загроз національній безпеці України у кіберпросторі (ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII).

Забезпечення безпеки критичної інфраструктури (Critical Infrastrurture Protection, CIP) представляє собою концепцію готовності протистояти серйозним загрозам роботи важливих об’єктів інфраструктури та об’єктів підвищеної загрози в умовах розповсюдження інформаційних технологій.

До об’єктів кібербезпеки та кіберзахисту віднесено:

– комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси;

– об’єкти критичної інформаційної інфраструктури (перелік затверджується КМ України);

– комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

Рисунок 5 – Місце кібербезпеки згідно ISO 27032

Найбільш уразливими об’єктами забезпечення інформаційної безпеки України в умовах надзвичайних ситуацій є система прийняття рішень з оперативних дій (реакцій), пов’язаних із розвитком таких ситуацій і ходом ліквідації їхніх наслідків, а також система збору й обробки інформації про можливе виникнення надзвичайних ситуацій.

Особливе значення для нормального функціонування зазначених об’єктів має забезпечення безпеки інформаційної інфраструктури країни при аваріях, катастрофах і стихійних лихах. Приховування, затримка надходження, перекручування та руйнування оперативної інформації, несанкціонований доступ до неї окремих осіб чи груп осіб можуть призвести як до людських жертв, так і до виникнення різних утруднень при ліквідації наслідків надзвичайної ситуації.

Основою функціонування систем інформаційної підтримки прийняття колективних рішень (за міжнародною термінологією – brain storm – мозковий штурм) є застосування інтерактивної обчислювальної мережі та відповідних методів аналізу, що використовуються для отримання інформації та опрацювання різних аспектів і шляхів вирішення поставленої проблеми.

Широке використання ПОЕМ і розробка різного плану інформаційних систем підвищують ефективність прийняття групових рішень, алгоритмічні та програмні засоби яких є елементами моделювання деревовидних структур рішень аналізу ризику, прогнозування, містять засоби зв’язку та системи управління даними із загальним і індивідуальним доступом, стандартні засоби аналізу даних і управління інформацією.

Особливе значення для нормального функціонування зазначених об’єктів має забезпечення безпеки інформаційної інфраструктури при аваріях, катастрофах і стихійних лихах.

До специфічних для даних умов напрямів забезпечення інформаційної безпеки належать:

– розробка ефективної системи моніторингу об’єктів підвищеної небезпеки, порушення функціонування яких може призвести до виникнення надзвичайних ситуацій, і прогнозування надзвичайних ситуацій;

– підвищення надійності систем обробки та передачі інформації, розробка спеціальних заходів із захисту інформаційних систем, які забезпечують керування екологічно небезпечними об’єктами й економічно важливими виробництвами.

Отже, важливо дотримуватися організаційно-технічних принципів, порядку здійснення заходів із технічного захисту інформації, порядку контролю в цій сфері, характеристик загроз для інформації, норм та вимог з технічного захисту інформації, порядку атестації та експертизи комплексних систем захисту інформації та комплексів технічного захисту інформації, що визначаються нормативно-правовими актами, прийнятими в установленому порядку відповідними органами.

До об’єктів ТЗІ належить інформація, вимога щодо захисту якої встановлена законом. До об’єктів захисту в телекомунікаційних системах та

інформаційних технологіях відноситься програмне забезпечення, що призначене для обробки цієї інформації.

Організаційно-технічні принципи, порядок здійснення заходів щодо ТЗІ, порядок контролю у цій сфері, характеристики загроз для інформації, норми та вимоги з ТЗІ визначаються нормативно-правовими актами з питань ТЗІ.

В якості конкретних об'єктів захисту виступають нерозрізнені носії інформації, а об'єднана загальними задачами упорядкована їх сукупність. Тоді в цілому під об'єктом захисту розуміється інформаційна система (ІС), яка реалізує автоматизований збір, обробку і маніпулювання даними, що включає: технічні засоби, програмне забезпечення, відповідний персонал і допоміжні засоби.

Систему захисту інформації (СЗІ) для конкретних об'єктів (інформаційних систем) можна представити у вигляді:

– основ побудови системи захисту інформації;

– направлень по захисту інформації;

– етапів побудови СЗІ.

Основою побудови системи захисту інформації є:

1) Законодавча, нормативно-правова, наукова і методична база забезпечення захисту інформації.

2) Структура і задачі органів (підрозділів), що забезпечують безпеку інформаційних технологій.

3) Організаційно-технічні і режимні заходи і методи захисту інформації.

4) Програмно-технічні способи і засоби, що використовуються для захисту інформації.

Напрямки захисту інформації формуються виходячи із конкретних особливостей інформаційної системи як об'єкту захисту. Виходячи з типової структури ІС і історично складених висновків робіт по захисту інформацією, можна виділити наступні напрямки:

1) Захист об'єктів інформаційних систем.

2) Захист процесів, процедур і програм обробки інформації.

3) Захист каналів зв'язку.

4) Пригнічення побічних електромагнітних наведень.

5) Управління системою захисту.

Етапи побудови СЗІ необхідно пройти в рівній кількості для всіх і кожного окремо напрямків(з врахуванням всіх основ).

У загальному випадку можна виділити наступні етапи побудови СЗІ:

– визначення інформаційних ресурсів (ІР), які підлягають захисту;

– виявлення всієї кількості загроз безпеки ІР, які підлягають захисту;

– проведення оцінки чутливості і ризиків для ІР, які підлягають захисту, при виявленні великої кількості загроз;

– розробка проекту (плану) системи захисту інформації, знижаючого за вибраним критерієм ризику для ІР, які підлягають захисту, при виявленні великої кількості загроз.

– реалізація проекту (плану) захисту інформації;

– визначення якості реалізації системи захисту;

– здійснення контролю функціонування і управління системою захисту.

Проходження етапів необхідно в тій чи іншій мірі здійснювати безперервно і по замкнутому циклу, з проведенням відповідного аналізу стану СЗІ та уточнюючою вимогою до неї після кожного кроку (рис. 79).

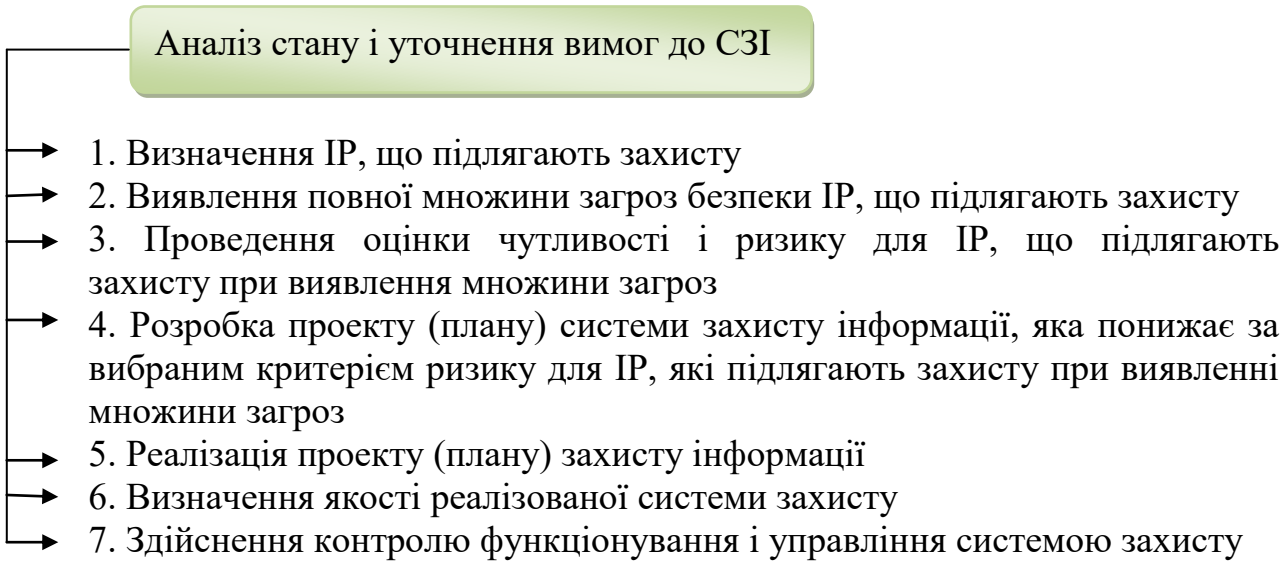


Рисунок 79 – Аналіз стану і уточнення вимог до СЗІ

Для описання логічних зв’язків і більш повного представлення процесу захисту інформації для кожної ІС пропонується формувати так звану матрицю знань інформаційної безпеки (ІБ). Матриця знань ІБ логічно об’єднує складові блоків основи, напрямки, етапи за принципом один з одним. Використовуючи міжнародний стандарт ISO/IEC 15408 «Загальні критерії оцінки безпеки інформаційних технологій», можна показати (рис. 80) динаміку побудови системи захисту інформації й процеси, що відбуваються при цьому.

Тут:

– контрзаходи – комплекс засобів захисту;

– загрози події, які потенційно можуть порушити одне із властивостей інформації, що захищають;

– порушник – людина, діяльність якого може привести до реалізації загроз, тобто він є джерелом;

– уразливості – властивості носіїв інформації, які можуть сприяти реалізації загроз безпеки інформації;

– ризик – величина, що характеризує можливість зазнати шкоди через порушення режиму інформаційної безпеки;

– керуванням ризиками – процес ідентифікації й зменшення ризиків, які можуть впливати на інформаційну систему.

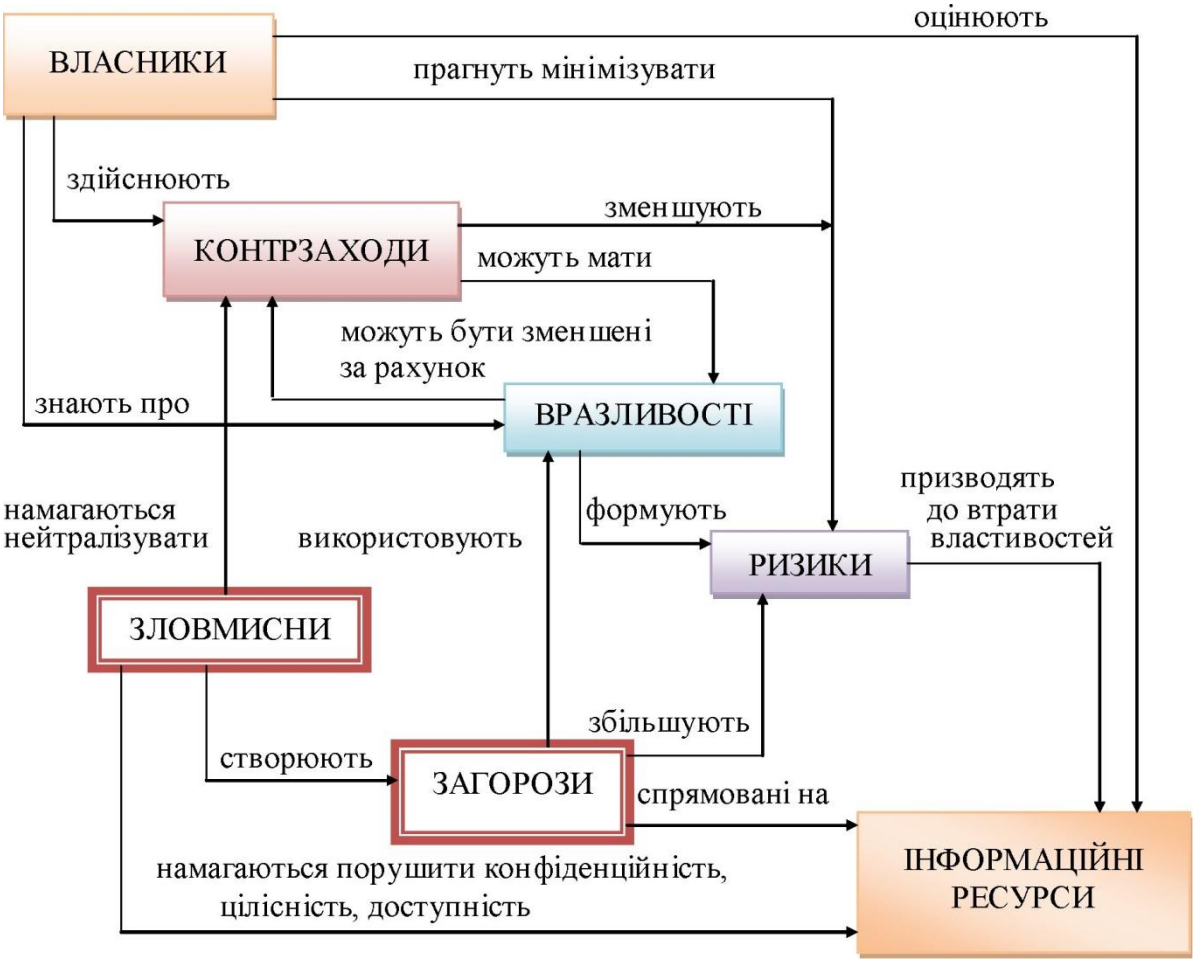


Рисунок 80 – Динаміка побудови системи захисту інформації

По виду реалізації загрози діляться на дві групи:

– фізичний вплив зовнішніх сил на джерела інформації, в результаті якого можливі її зміни, знищення, викрадення і блокування;

– несанкціоноване поширення носія з захищеною інформацією від її джерела до зловмисника, який призводить до викрадення інформації.

Кожний конкретний об’єкт є індивідуальним набором параметрів та інформаційних додаткових даних. Ступінь впливу параметрів один на одного досить різний і визначає швидкість наростання аварійного процесу. Кожний параметр в інформаційній базі має:

– своє критичне значення, вище якого він переходить в передаварійну область;

– свій поріг аварійності.

Слід зазначити, що всі параметри інформаційної бази взаємозалежні, впливаючи один на одного тою чи іншою мірою. Найбільш уразливим об’єктами забезпечення інформаційної безпеки є системи збору і обробки інформації про можливе виникнення надзвичайних ситуацій і прийняття рішень щодо оперативних дій, пов’язаних із розвитком таких ситуацій і ходом ліквідації їх наслідків.

10.16 Автоматизована система оповіщення

Автоматизована система оповіщення – сукупність алгоритмів дій, процесів (заходів), технологій, а також організаційно і технічно поєднаних програмних і технічних засобів електронних комунікацій, засобів обробки та передачі (відображення) інформації, що забезпечують своєчасне доведення сигналів та інформації з питань цивільного захисту до органів виконавчої влади, органів місцевого самоврядування, органів управління і сил цивільного захисту, підприємств, установ, організацій та населення в разі загрози виникнення або під час виникнення надзвичайних ситуацій.

Інформування населення у сфері цивільного захисту – доведення органами управління цивільного захисту через засоби масової інформації, теле-радіомережі відомостей про надзвичайні ситуації, що прогнозуються або виникли, з визначенням їх класифікації, меж поширення і наслідків, про способи та методи захисту від них, а також про свою діяльність з питань цивільного захисту, в тому числі з урахуванням особливостей оповіщення осіб з фізичними, психічними, інтелектуальними та сенсорними порушеннями.

Основними призначенням служби зв'язку ДСНС відповідно до галузевого спрямування діяльності є організація та забезпечення надійним зв'язком органів управління та сил Оперативно-рятувальної служби цивільного захисту в умовах загрози виникнення і виникнення НС (НП), здійснення контролю за організацією та виконанням заходів щодо підтримання у готовності автоматизованих систем централізованого оповіщення про загрозу або виникнення НС (НП) для оповіщення центральних та місцевих органів виконавчої влади, органів управління та сил цивільного захисту в мирний час та в особливий період.

Основними завданнями служби є:

– у режимі повсякденного функціонування – організація та здійснення заходів щодо контролю готовності автоматизованих систем централізованого оповіщення про загрозу або виникнення НС (НП);

– у режимі підвищеної готовності – здійснення заходів щодо контролю підтримання в готовності автоматизованих систем централізованого оповіщення про загрозу або виникнення НС (НП) для забезпечення оповіщення центральних та місцевих органів виконавчої влади, органів управління та сил цивільного захисту, а також координація діяльності із забезпечення інформування населення про загрозу виникнення НС (НП) та дії в умовах такої ситуації;

– у режимі НС (НП) – здійснення заходів щодо контролю підтримання в готовності автоматизованих систем централізованого оповіщення про загрозу або виникнення НС (НП) для забезпечення оповіщення центральних та місцевих органів виконавчої влади, органів управління та сил цивільного захисту, а також координація діяльності із забезпечення інформування населення про загрозу виникнення НС (НП) та дії в умовах такої ситуації;

приведення в готовність спеціалізованої служби, залучення в разі потреби додаткових сил і засобів.

За рівнями системи оповіщення згідно до Кодексу Цивільного Захисту України у Розділі IV «Захист населення і територій від надзвичайних ситуацій» (ст.30) поділяються на загальнодержавну автоматизовану систему централізованого оповіщення, територіальні автоматизовані системи централізованого оповіщення, місцеві автоматизовані системи централізованого оповіщення, а також спеціальні, локальні та об'єктові системи оповіщення, систем циркулярного виклику.

Ці системи забезпечують оповіщення і подальше інформування:

– чергових служб міністерств та інших центральних органів виконавчої влади по службових телефонах;

– чергових служб місцевих органів виконавчої влади;

– чергових аварійно-рятувальних служб.

Спеціальні системи оповіщення створюються і функціонують:

– на атомних електростанціях;

– на гідротехнічних спорудах Дніпровського та Дністровського каскадів та в зонах їх можливого катастрофічного затоплення;

– на магістральних продуктопроводах.

Спеціальні системи оповіщення передбачають взаємодію з відповідними територіальними та місцевими автоматизованими системами централізованого оповіщення. Електронні комунікаційні послуги для потреб автоматизованих систем централізованого оповіщення надаються операторами електронних комунікацій на договірних засадах.

Між об’єктами, де функціонують спеціальні, локальні та об’єктові системи оповіщення, та оперативно-черговою (черговою) службою місцевих органів виконавчої влади (органів місцевого самоврядування) керівником об'єкта організовується безпосередній телефонний зв’язок.

Готовність систем оповіщення забезпечено шляхом:

– організація цілодовового чергування відповідних служб;

– налагодження телефонного зв’язку чергових служб потенційно небезпечних підприємств, зона ураження яких може поширюватися на заселені території або території інших підприємств, установ, організацій з оперативно-черговою службою пункту управління облдержадміністрації, чергових служб органів МВС в містах та районах області;

– завчасна підготовка персоналу чергових служб до дій у надзвичайних ситуаціях;

– впровадження автоматизованих систем оповіщення з використанням сучасних технологій;

– проведення якісного експлуатаційно-технічного обслуговування апаратури оповіщення та інших технічних засобів зв'язку та оповіщення.

Забороняється зняття та відключення телекомунікаційних мереж, абонентських ліній, через які здійснюється запуск електросирен, демонтувати вуличні гучномовці без погодження з відповідними органами Департаменту.

Порядок дій оперативно-чергових (чергових, диспетчерських) служб центральних та місцевих органів виконавчої влади, а також центрів управління мережами операторів електронних комунікацій, провайдерів програмної послуги, телерадіоорганізацій, засобів масової інформації незалежно від форми власності, які долучаються до оповіщення та інформування населення, під час передачі сигналів оповіщення та інформування населення визначається законодавством, зокрема положеннями про системи оповіщення, планами у сфері цивільного захисту.

Одним із головних способів оповіщення населення про небезпеку та шляхи рятування від дії їх вражаючих чинників є передача повідомлень по всіх мережах зв'язку, радіомовлення, через зовнішні гучномовці, а також через місцеві радіомовні і телевізійні станції в разі їх наявності.

Система оповіщення на всіх рівнях Єдиної Державної Системи запобігання і реагування на НС техногенного та природного характеру – це організаційно-технічне об'єднання (організаційно-технічну систему) оперативних чергових служб органів управління ЦЗ, спеціальної апаратури управління і засобів оповіщення, а також каналів (ліній зв'язку), які забезпечують передачу команд управління і мовної інформації при НС. Системи централізованого оповіщення (СЦО) регіонального рівня є основною ланкою системи оповіщення в Україні.

Завданням СЦО регіонального рівня є оповіщення посадових осіб і сил місцевого і об'єктового рівнів та їх посадових осіб, а також населення, яке проживає на території, на яку поширюється дія СЦО цього рівня.

Інформація, яка доводиться до органів управління і посадових осіб, має оперативний характер, а до населення доводиться інформація про характер і масштаби загрози та про дії людей в умовах НС. СЦО регіонального рівня мають забезпечувати як циркулярне, так і вибіркове включення СЦО місцевого і об'єктового рівня, а також оповіщення населення, яке проживає на території, яку охоплює система оповіщення цього рівня. Управління СЦО місцевого рівня може здійснюватися безпосередньо від оперативної чергової служби у місті або через чергового зміни вузла зв'язку міста.

Використання цих систем в комплексі з існуючими мережами операторів мобільного зв'язку, які покривають практично всю територію України, зробить можливим розгортання мережі з глобальним оповіщенням практично 100 % населення і дозволить виконати наступні завдання:

– побудувати мережу оповіщення населення і спеціальних структур;

– організувати мережу оповіщення з мінімальними інфраструктурними витратами;

– утворити простір поширення сигналів оповіщення незалежно від конкретного оператора та/або телекомунікаційної мережі;

– здійснювати вибіркове оповіщення за територіальним розташуванням зони потенційної надзвичайної ситуації;

– персоналізувати повідомлення для різних органів, таких як ДСНС, МВС та ін.;

– здійснювати оповіщення зі встановленням пріоритетів за важливістю і формувати інструкції групам для їх негайного виконання;

– проводити контроль і управління ситуацією щодо оповіщення; оперативно використовувати і спрямовувати необхідні ресурси для локалізації аварій, катастроф або будь-яких інших подій.

При розробці нових систем оповіщення населення про виникнення надзвичайних ситуацій необхідно передбачати автоматизовані системи досліджень (наземних, авіаційних, радарних, супутникових), систем збору та передачі даних із застосуванням сучасних засобів зв'язку, автоматичної обробки даних спостережень і видачі актуальної інформації, сучасне доведення інформації до населення впровадженням сучасних інноваційних технологій.

Для управління суб'єктами забезпечення цивільного захисту у разі загрози виникнення або виникнення надзвичайних ситуацій використовуються ресурси електронних комунікаційних мереж загального користування, державної системи урядового зв'язку та Національної системи конфіденційного зв'язку.

Оператори електронних комунікацій в умовах надзвичайних ситуацій надають послуги у порядку, передбаченому Законом України «Про електронні комунікації».

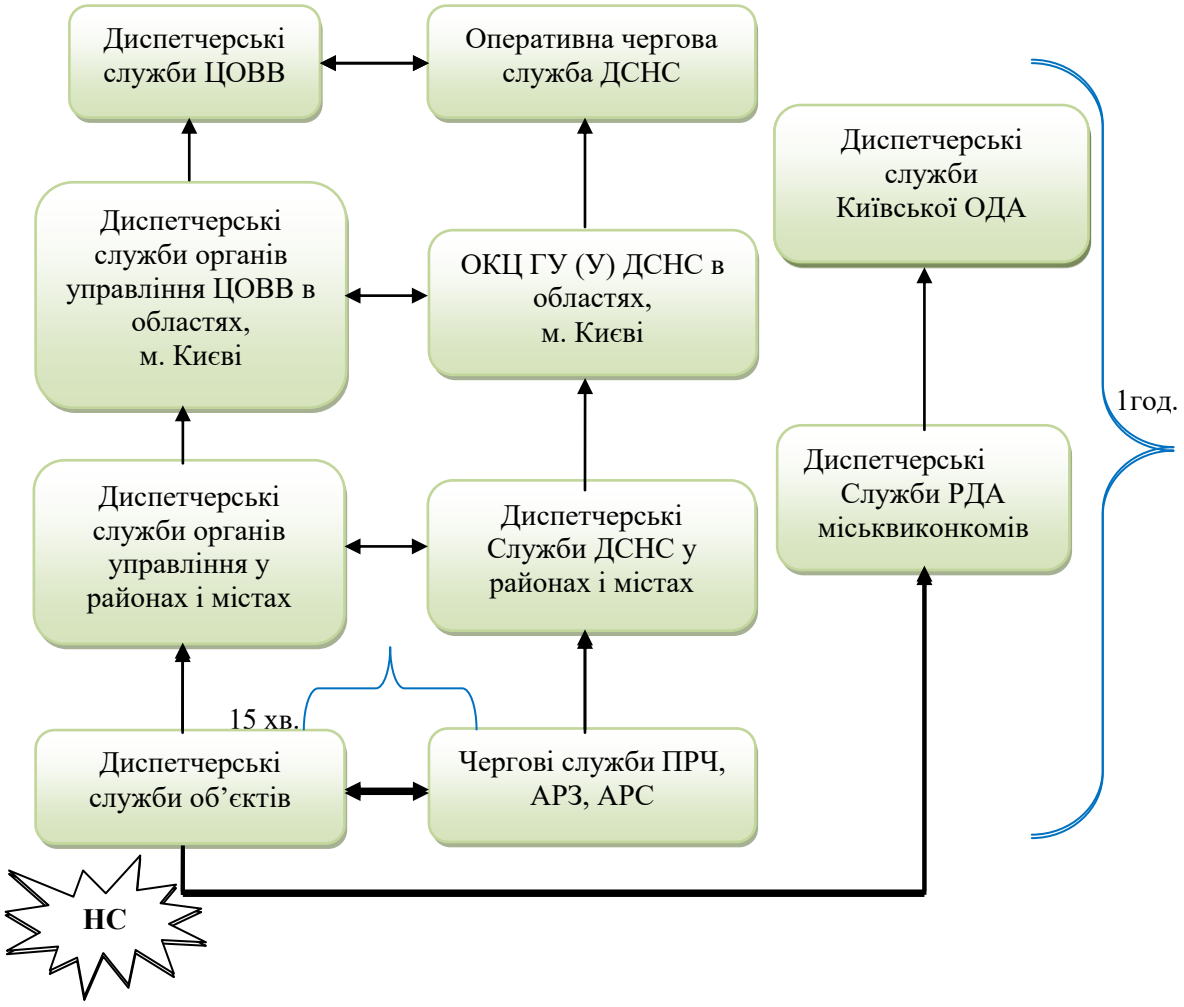


Рисунок 81 – Схема проходження інформації від об'єкта де виникла НС

10.17 Автоматизовані системи раннього виявлення загрози виникнення надзвичайних ситуацій та оповіщення населення (СРВНСО) (ДБН В.2.5-76:2014)

Автоматизована система класу «людино-машина», у якій суміщено автоматичні процеси виявлення загрози виникнення НС, спостереження та оброблення інформації щодо поточного стану об'єктів та будівель, інженерних споруд, мереж, що розташовані на територіях з ризиком прояву небезпечних природних явищ і процесів, оперативне надання користувачам фактичної та прогнозованої інформації, а також оповіщення (за необхідності) працівників та керівників об'єкта, відповідальних за стан техногенної безпеки, посадових осіб органів виконавчої влади та місцевого самоврядування і населення при безпосередній участі людини-оператора.

СРВНСО повинна виконувати такі функції:

– безперервно отримувати дані від джерел первинної інформації;

– контролювати в реальному вимірі часу відповідність поточних (граничних) значень параметрів проектним режимам технологічного процесу

– об'єкта та (або) унормованим значенням параметрів джерел НС природного характеру;

– інформувати працівників, відповідальних за функціонування технологічного обладнання, щодо виявлених фактів досягнення докритичних та критичних значень параметрів, які контролюють;

– інформувати посадових осіб, які відповідають за стан техногенної безпеки об'єкта, про факти досягнення критичних значень параметрами, які контролюють.

СРВНСО отримує від оператора СРВНСО підтвердження прийняття сигналів про досягнення параметрами, які контролюються, докритичних та критичних значень, а також сигналів про спрацьовування ручних оповіщувачів. За відсутності підтвердження СРВНСО автоматично виконує інформування відповідальних посадових осіб по підприємству.

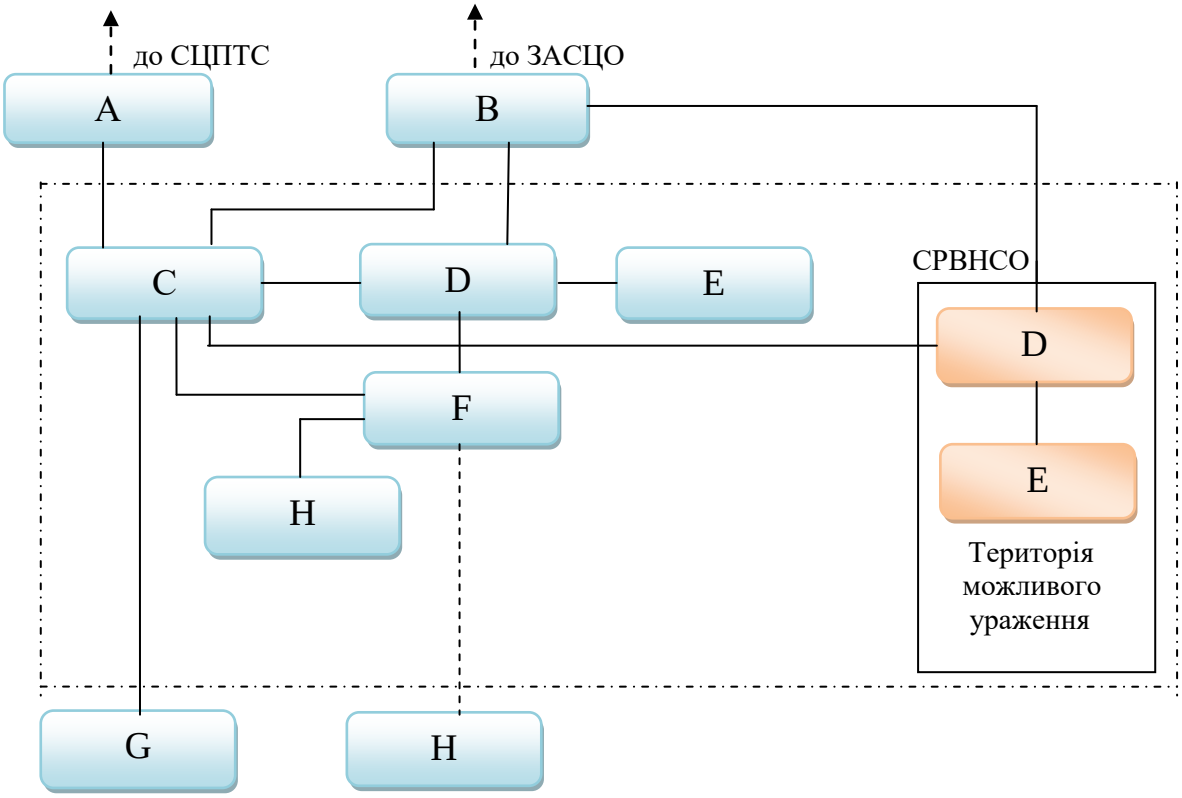
СРВНСО автоматично формує та за командою оператора СРВНСО передає до ПЦС тривожне сповіщення щодо виявлення загрози або виникнення НС разом із ідентифікатором електронної картки аварії, з можливістю отримання від ПЦС сигналу підтвердження його прийняття.

СРВНСО та суміжні системи повинні програмно і апаратно суміщатись із ієрархічними структурами вищого рівня та між собою.

Інформаційна підтримка дій повинна здійснюється шляхом автоматизованого визначення та візуалізації певного сценарію розвитку НС. Сукупність усіх можливих сценаріїв розвитку НС зберігається у базі даних АРМ оператора СРВНСО у вигляді електронних карток аварії, які містять інформацію з оперативної частини планів локалізації і ліквідації аварії.

У разі відсутності підтвердження з боку ПЦС факту отримання тривожного сповіщення СРВНСО здійснює автоматичне телефонне з'єднання з оперативно-диспетчерською службою відповідного аварійно-рятувального підрозділу, на який відповідно до плану локалізації і ліквідації аварії покладено

оперативне реагування на НС, з подальшою передачею тривожного мовного повідомлення, що містить ідентифікатор електронної картки аварії.



СЦПТС	Система централізованого пожежного та техногенного спостереження
ЗАСЦО	Загальнодержавна автоматизована система централізованого оповіщення
A – ПЦС	Пульт централізованого спостереження
B – ТАСЦО	Територіальна автоматизована система централізованого оповіщення
C – ПК	Пульт керування СРВНСО
D – ПО	Пристрій оповіщення
E – КТЗІО	Кінцеві технічні засоби інформування та оповіщення
F – КП	Комунікаційний пристрій
H	Джерела первинної інформації
G	Суміжні системи забезпечення безпеки

Рисунок 82 – Структурна схема СРВНСО

Для оповіщення населення, яке проживає в зоні ураження за межами об’єкта, допускається використовувати ТАСЦО за її наявності на відповідній території та технічної можливості.

Джерелом первинної інформації для СРВНСО є існуючі на підприємстві технологічні датчики і сигналізатори промислової автоматики, що входять до складу систем протиаварійного захисту та автоматизованих систем керування технологічними процесами.

Комунікаційні пристрої забезпечують виконання таких функцій:

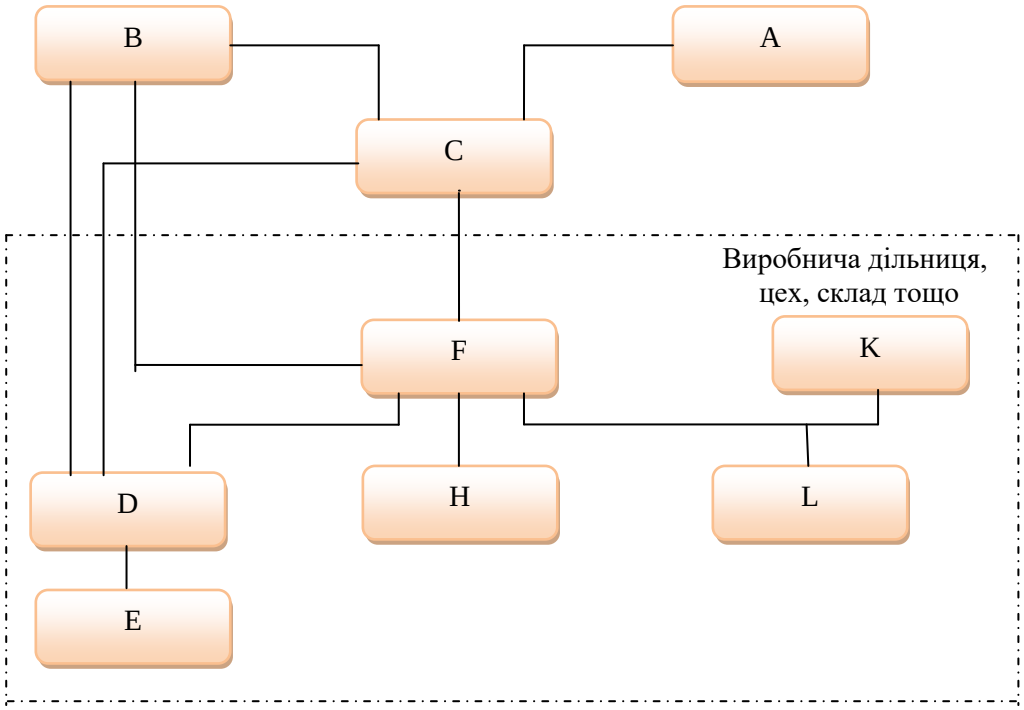
– самодіагностування працездатності;

– отримання даних від ДПІ щодо поточного стану джерел техногенної та (або) природної небезпеки, обробку отриманої інформації;

– інформування респондентів щодо результатів оброблення інформації;

– прийняття та виконання команд, що надходять від пульту керування СРВНСО;

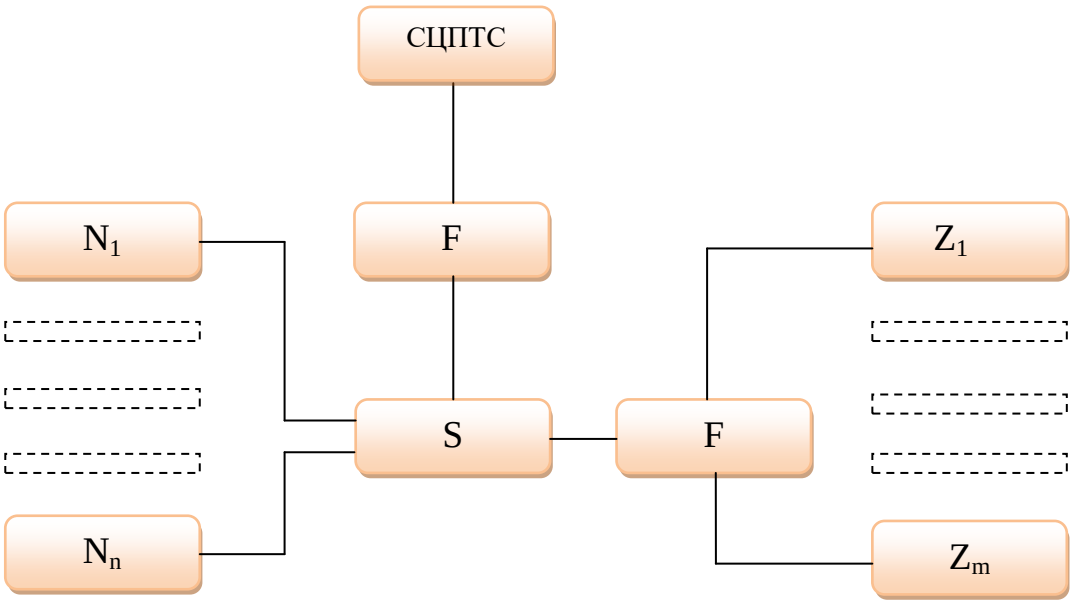
– формування архівного журналу.



СЦПТС	Система централізованого пожежного та техногенного спостереження
ЗАСЦО	Загальнодержавна автоматизована система централізованого оповіщення
A – ПЦС	Пульт централізованого спостереження
B – ТАСЦО	Територіальна автоматизована система централізованого оповіщення
C – ПК	Пульт керування
D – ПО	Пристрій оповіщення
E – КТЗІО	Кінцеві технічні засоби інформування та оповіщення
F – КП	Комунікаційний пристрій
H – ДПІ	Джерела первинної інформації
K – ПДП	Пристрій дистанційного пуску

L – УЛНСРС	Установки локалізації/ліквідації НС на ранній стадії

Рисунок 83 – Структурна схема установок локалізації/ліквідації НС на ранній стадії



СЦПТС	Система централізованого пожежного та техногенного спостереження
F	Комунікаційний пристрій
N – АРМ	Автоматизоване робоче місце оператора ПЦС
Z – СРВНСО	Автоматизовані системи раннього виявлення загрози виникнення надзвичайних ситуацій та оповіщення населення
S	Сервер

Рисунок 84 – Пульт централізованого спостереження за СРВНСО

Канали зв'язку між СРВНСО, їх складовими та суміжними системами організовують з урахуванням забезпечення їх функціонування протягом часу, необхідного для виявлення НС, інформування та оповіщення, вжиття невідкладних заходів щодо ліквідування НС та їх наслідків, перш за все - евакуація людей із зони НС.

10.17 Забезпечення функціонування апаратури і технічних засобів автоматизованих систем централізованого оповіщення та зв'язку, контроль за їх станом

Експлуатаційно-технічне обслуговування апаратури і технічних засобів оповіщення та технічних засобів електронних комунікацій – комплекс

організаційно-технічних заходів щодо технічного обслуговування, поточного ремонту, планування експлуатації, а також здійснення контролю за забезпеченням надійного функціонування апаратури і технічних засобів оповіщення та технічних засобів електронних комунікацій.

Технічне обслуговування автоматизованих систем оповіщення здійснюється підготовленим технічним персоналом органу виконавчої влади (органу місцевого самоврядування), підприємства (установи, організації), на які покладено створення автоматизованої системи оповіщення або на договірних засадах суб'єктами господарювання, що надають послуги у сфері електронних комунікацій (інформаційних технологій) відповідно до законодавства.

Контрольні перевірки готовності автоматизованих систем оповіщення здійснюються оперативно-черговими (черговими, диспетчерськими) службами пунктів управління всіх рівнів шляхом передачі контрольних сигналів управління та отримання підтвердження їх виконання в автоматичному (автоматизованому) режимі з періодичністю не менше одного разу на добу.

У разі виявлення несправностей апаратури і технічних засобів оповіщення та технічних засобів електронних комунікацій загальнодержавної (територіальної або місцевої) автоматизованої системи централізованого оповіщення органом виконавчої влади (органом місцевого самоврядування), що здійснює управління системою, та суб'єктом господарювання, що здійснює технічне обслуговування зазначеної апаратури і технічних засобів, негайно вживаються заходи до усунення несправностей.

У разі виникнення аварійних ситуацій або помилок у роботі програмно-технічного комплексу автоматизованої системи централізованого оповіщення інструменти контролю зберігають повний набір інформації, необхідної користувачеві і розробникові для ідентифікації проблеми (знімки екранів, коди помилки (збою), поточний стан пам'яті та файлової системи програмних засобів).

10.18 Функціональна структура Системи 112

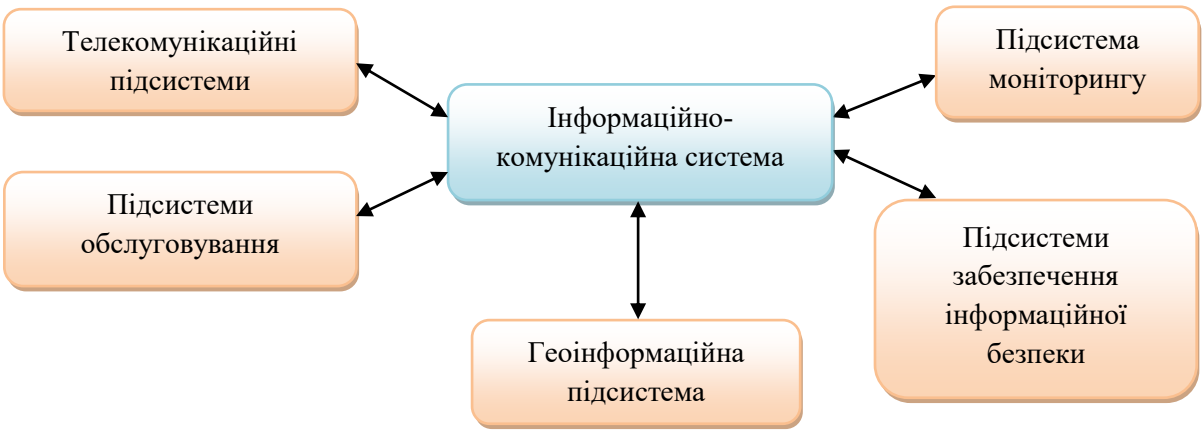


Рисунок 51 – Функціональна структура Системи 112

Система 112 включає утворенні у складі територіальних органів спеціально уповноваженого центрального органу виконавчої влади з питань цивільного захисту центри екстреної допомоги населенню за єдиним телефонним номером 112 (ЦЕДН-112), оперативно-диспетчерські служби, підрозділи екстреної допомоги населенню, які з використанням телекомунікаційних мереж, програмних, технічних та інших засобів надають екстрену допомогу населенню та отримання від операторів телекомунікацій інформації про номер телефону, з якого здійснюється екстрений виклик, а також місцезнаходження абонента мережі рухомого (мобільного) зв'язку або адресу встановлення телефону (таксофону) фіксованого зв'язку.

Телекомунікаційні підсистеми здійснюють приймання та оброблення екстрених викликів від користувачів фіксованого та мобільного зв'язку у вигляді голосових, SMS, MMS повідомлень, а також забезпечує взаємодію між оперативно диспетчерськими службами підрозділів екстреної допомоги населенню.

Інформаційно-комунікаційні підсистеми забезпечують зберігання і актуалізацію баз даних, обробку інформації про отримані виклики а також інформаційно-аналітичну підтримку прийняття рішень по екстреному реагуванню на прийняті виклики та планування заходів реагування;

*Підсистеми консультативного обслугов*ування населення призначені для надання інформаційно-довідкової допомоги особам з питань безпеки життєдіяльності, в тому числі через мережу Інтернет, соціальні мережі, форуми та інше.

Геоінформаційна підсистема, призначена для відображення на основі електронних карт природно-географічних, соціально-демографічних, економічних та інших характеристик територій, місцезнаходження особи, яка звернулася за номером «112», і/або абонентського пристрою, з якого здійснено виклик (повідомлення про подію), місце події, а також місцезнаходження транспортних засобів підрозділів екстреної допомоги, залучених до реагування на подію;

Підсистема моніторингу забезпечує прийому та обробки інформації і сигналів, що надходить від датчиків, встановлених на контрольованих стаціонарних та рухомих об'єктах, у тому числі від автомобільних терміналів системи екстреного реагування при аваріях та терміналів GPS/ГЛОНАСС, встановлених на транспортних засобах чергових підрозділів, залучених до реагування на подію і транспортних засобах, що перевозять небезпечні вантажі;

Підсистеми забезпечення інформаційної безпеки призначені для захисту інформації та засобів її обробки в Системі-112.[23] У разі виникнення аварійних

[23] Фахівцями Полтавського підприємства – ТОВ «Полтаварадіоком» розроблено комплексну систему оперативного управління всіма службами взаємодії всередині громади (за принципом 112, або 911), яка за допомогою застосування сучасних систем комунікацій та комплексному підходу до вирішення проблеми дозволяє здійснювати покладені на неї функції. Така система на сьогодні вже більше року експлуатується в м. Полтаві та дозволяє оперативно управляти діяльністю різних служб в радіусі ~ 50 км. навколо Полтави. Поряд з цим розроблена та готується до впровадження подібна система для однієї з об'єднаних територіальних громад Полтавської області. Інтегрувавши таку розробку в систему оперативного управління службами територіальної

ситуацій або помилок у роботі програмно-технічного комплексу автоматизованої системи централізованого оповіщення інструменти контролю зберігають повний набір інформації, необхідної користувачеві і розробникові для ідентифікації проблеми (знімки екранів, коди помилки (збою), поточний стан пам’яті та файлової системи програмних засобів).

Висновки

1. Сучасні інформаційні технології визначаються як безперервні процеси обробки, зберігання, передачі і відображення інформації, які спрямовані на ефективне використання інформаційних ресурсів, засобів обчислювальної техніки й передачі даних при управлінні системами різного класу і призначення.

2. Характерною рисою мереж для спеціальних споживачів є те, що з одного боку вони традиційно є найбільш консервативним об’єктом в галузі зв’язку, а з іншого боку – вони повинні бути засновані на новітніх досягненнях цієї галузі, щоб забезпечувати високу якість обслуговування.

3. За результатами аналізу тенденцій розвитку і світового досвіду побудови систем оповіщення та новітніх інформаційно-телекомунікаційних технологій зроблено висновок про необхідність модернізації автоматизованих системи централізованого оповіщення про загрозу або виникнення надзвичайних ситуацій сучасними інноваційними технологіями.

4. Аналіз ризиків інформаційної безпеки, що становлять собою усвідомлену небезпеку (загрозу), настання в будь-якій системі негативної події з окресленими у часі та просторі наслідками або існування чи можливість виникнення ситуації при якій формуються передумови протидії реалізації задач і функції підрозділу ДСНС і забезпеченню й безпеки є актуальною. Забезпечення безпеки може бути досягнуте двома способами: по-перше, вжиттям всіх практично можливих заходів, по-друге, зниженням ризиків до прийнятного рівня.

громади на базі єдиної диспетчерської ЦГБ можливо швидко отримати гнучку та оперативну систему управління сучасного, європейського рівня.