

Міністерство освіти і науки України  
Департамент науки і освіти  
Харківської обласної державної адміністрації  
Комунальний заклад  
«Харківська гуманітарно-педагогічна академія»  
Харківської обласної ради

# КОМП'ЮТЕРНІ МЕРЕЖІ, ІНТЕРНЕТ-ТЕХНОЛОГІЇ

Курс лекцій



Харків  
2022

**К 63**

**Укладачі:**

**Русскін В. М.**, кандидат технічних наук, доцент, завідувач кафедри інформатики Комунального закладу «Харківська гуманітарно-педагогічна академія» Харківської обласної ради;

**Хміль Н. А.**, доктор педагогічних наук, доцент, професор кафедри інформатики Комунального закладу «Харківська гуманітарно-педагогічна академія» Харківської обласної ради.

**Рецензенти:**

**Кисельова О. Б.**, кандидат педагогічних наук, доцент, доцент кафедри інформатики Комунального закладу «Харківська гуманітарно-педагогічна академія» Харківської обласної ради;

**Стадник О. М.**, кандидат фізико-математичних наук, старший науковий співробітник, доцент кафедри медіаінженерії та інформаційних радіоелектронних систем Харківського національного університету радіоелектроніки.

**К 63 Комп'ютерні мережі, інтернет-технології** : курс лекцій для здобувачів першого бакалаврського рівня вищої освіти зі спеціальності 014.09 Середня освіта (Інформатика) / укладачі Русскін В. М., Хміль Н. А. Комунальний заклад «Харківська гуманітарно-педагогічна академія» Харківської обласної ради. Харків, 2021. 120 с.

Курс лекцій розроблено та структуровано відповідно до розділів робочої програми освітнього компонента «Комп'ютерні мережі, інтернет-технології». У матеріалі лекцій розглянуто апаратні та логічні принципи побудови мереж, функції протоколів, сучасні технології локальних і глобальних мереж; уміщено відомості про мережу Internet і сервіси, які надаються користувачеві; описано принципи створення особистих Web-сторінок.

У виданні міститься необхідний теоретичний матеріал для організації практичних і самостійних робіт здобувачів вищої освіти. Кожна тема представлена стислим і систематизованим викладом основних теоретичних положень, містить перелік запитань, що є обов'язковими для вивчення і підсумкового контролю знань.

Навчальне видання рекомендоване здобувачам вищої освіти першого (бакалаврського) рівня освітньо-професійної програми Середня освіта (Інформатика).

*Рекомендовано до друку науково-методичною радою Комунального закладу «Харківська гуманітарно-педагогічна академія» Харківської обласної ради (протокол №4 від 31.03.2022 р.).*

УДК 378.016:004.771(075)

© ХГПА, 2022

Русскін В. М., Хміль Н. А., 2022

## ЗМІСТ

<b>ПЕРЕДМОВА</b>	5
<b>ЛЕКЦІЯ 1. Тема. Історія розвитку та класифікація комп'ютерних мереж</b>	7
1.1. Історичні аспекти розвитку комп'ютерних мереж	7
1.2. Поняття комп'ютерної мережі	10
1.3. Класифікація комп'ютерних мереж	11
1.4. Однорангові мережі	15
1.5. Мережі з виділеним сервером (мережі типу «клієнт-сервер»)	17
1.6. Взаємодія комп'ютерів у мережі	18
1.7. Стандартизація у комп'ютерних мережах	19
1.8. Структура моделі OSI	22
Запитання для перевірки знань	26
<b>ЛЕКЦІЯ 2. Тема. Топології, методи доступу та архітектурні принципи побудови комп'ютерних мереж</b>	27
2.1. Базові мережеві топології	27
2.2. Інші можливі мережеві топології	33
2.3. Доступ до середовища передавання	35
2.4. Вибір комп'ютерної мережі	36
2.5. Вибір мережевої архітектури	37
Запитання для перевірки знань	51
<b>ЛЕКЦІЯ 3. Тема. Стеки протоколів і методи маршрутизації</b>	52
3.1. Вибір стека протоколів	52
3.2. Основи IP-Адресації	61
3.3. Основи IP-маршрутизації	67
3.4. Призначення IP-адрес та перевірка працездатності TCP/IP	74
Запитання для перевірки знань	77
<b>ЛЕКЦІЯ 4. Тема. Світова інформаційна мережа Інтернет</b>	78
4.1. Історія розвитку мережі Internet	78
4.2. Загальна характеристика мережі Internet	82
4.2.1. Визначення Internet	82
4.3. Адресація в Internet і доменна система імен	83
4.4. Світові електронні служби мережі Internet	84
4.4.1. Загальна характеристика й класифікація електронних служб мережі Internet	84
4.4.2. Поняття прикладного сервера в мережі Internet	85
4.4.3. Прикладні сервери мережі Internet	86
4.5. Базові технології й служби мережі Internet	87
Запитання для перевірки знань	93

<b>ЛЕКЦІЯ 5. Тема. Основи програмування для Web</b>	95
5.1. Web-документи і web-сторінки	95
5.2. Структура web-документів	96
5.3. Основні теги мови HTML	96
5.4. МІМЕ-типи документів	108
5.5. Програмне забезпечення для створення web-документів	110
Запитання для перевірки знань	115
<b>РЕКОМЕНДОВАНА ЛІТЕРАТУРА</b>	117
<b>ПІСЛЯМОВА</b>	119

## ПЕРЕДМОВА

Сьогодні можна із упевненістю сказати, що комп'ютерні мережі стали невід'ємною складовою нашого життя, а галузь їхнього застосування охоплює майже всі сфери діяльності сучасної людини. У цьому контексті заклади вищої освіти, окрема й педагогічні, повинні забезпечити випереджальну підготовку студентів щодо проектування, розробки, конфігурування та обслуговування комп'ютерних мереж. Зазначимо, що такі знання та вміння вчителів інформатики у галузі комп'ютерних телекомунікацій необхідно розглядати як елемент їх професійної майстерності. Тому вивчення основ комп'ютерних мереж та Інтернет-технологій є важливим напрямом професійної підготовки здобувачів вищої освіти освітньо-професійної програми «Середня освіта (Інформатика)» першого бакалаврського рівня.

Освітній компонент «Комп'ютерні мережі, інтернет-технології» є нормативним і входить до циклу освітніх компонентів професійної підготовки навчального плану підготовки бакалаврів, які навчаються за спеціальністю 014.09 Середня освіта (Інформатика).

Запропонований курс лекцій має на меті формування компетенцій, необхідних для вирішення різних практичних завдань у професійній діяльності, пов'язаної з організацією та налаштуванням комп'ютерних мереж. Для його підготовки пропрацьований великий обсяг інформації, розташованої на інформаційно-пошукових серверах Інтернет, також використовувалася література, приведена у списку рекомендованих джерел.

Навчальне видання містить п'ять лекцій. Перша лекція присвячується історичним аспектам розвитку комп'ютерних мереж, основним поняттям термінології. Також розглянуто класифікацію комп'ютерних мереж, питання стандартизації у комп'ютерних мережах, пояснюється структура моделі OSI.

У другій лекції пояснюються існуючі топології комп'ютерних мереж, методи доступу до середовища передавання даних, звертається увага на вибір мережевої архітектури.

У третій лекції дається поняття стек протоколів і приведені найбільш популярні стеки протоколів, описані основи IP-адресації, IP-маршрутизації та перевірка працездатності TCP/IP.

Лекція чотири присвячена історії розвитку мережі Інтернет, її загальним характеристикам. Описано світові служби, базові технології та основні загрози під час роботи в мережі Інтернет.

П'ята лекція присвячена основам програмування для Web. Звертається увага на поняття Web-документа і web-сторінки; розглянуто структуру web-документів та основні теги мови HTML; схарактеризовано програмне забезпечення для створення web-документів.

Усі лекції мають загальну структуру: мета, план, найбільш важливі теоретичні відомості, запитання для самоконтролю. Крім того, курс лекцій містить рекомендовану літературу до освітнього компоненту.

## **ЛЕКЦІЯ 1.**

### **Тема. Історія розвитку та класифікація комп'ютерних мереж**

**Мета:** Ознайомити здобувачів вищої освіти з історією створення, основними поняттями, класифікацією та стандартизацією комп'ютерних мереж.

#### **ПЛАН**

1. Історичні аспекти розвитку комп'ютерних мереж.
2. Поняття комп'ютерної мережі.
3. Класифікація комп'ютерних мереж.
4. Однорангові мережі.
5. Мережі з виділеним сервером (мережі типу «клієнт-сервер»).
6. Взаємодія комп'ютерів у мережі.
7. Стандартизація у комп'ютерних мережах.
8. Структура моделі OSI.

### **1.1. Історичні аспекти розвитку комп'ютерних мереж**

Безпосередньою основою комп'ютерних мереж (КМ) були телефонні й телеграфні мережі, створені у XIX ст. У 50-х роках XX ст. унаслідок розвитку мікроелектроніки з'явилися потужні електронно-обчислювальні машини (ЕОМ). Для використання їх обчислювальних потужностей виникла необхідність з'єднати їх з кількома віддаленими терміналами. Таким чином з'явилися системи з розподілом часу роботи центрального процесора, в яких кожному терміналу по чергово виділявся квант часу. Мережа такої структури наведена на рис.1.1.

Особливостями таких систем було неефективне використання дуже дорогих каналів зв'язку між центральним процесором і терміналами. Згодом були розроблені спеціальні пристрої – мультиплексори і концентратори, що дозволяли збирати трафік від розташованих поруч терміналів і передавати його одним спільним каналом зв'язку до центрального процесора.

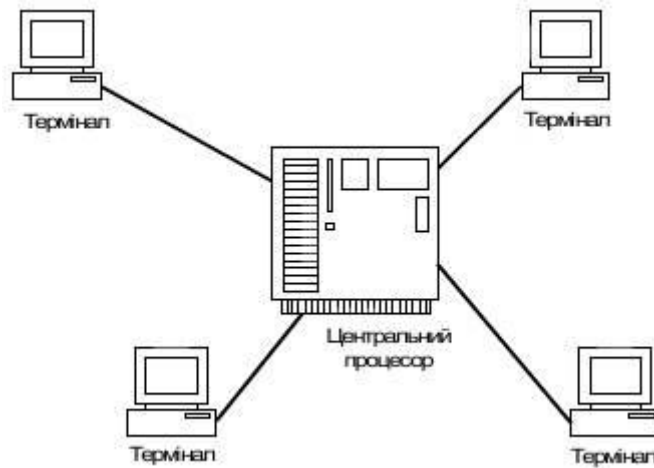


Рис. 1.1. Схема комп'ютерної мережі з терміналами

Обов'язковим елементом такої системи був фронтальний процесор, на який покладались функції організації зв'язку. Схема такої мережі наведена на рис.1.2.

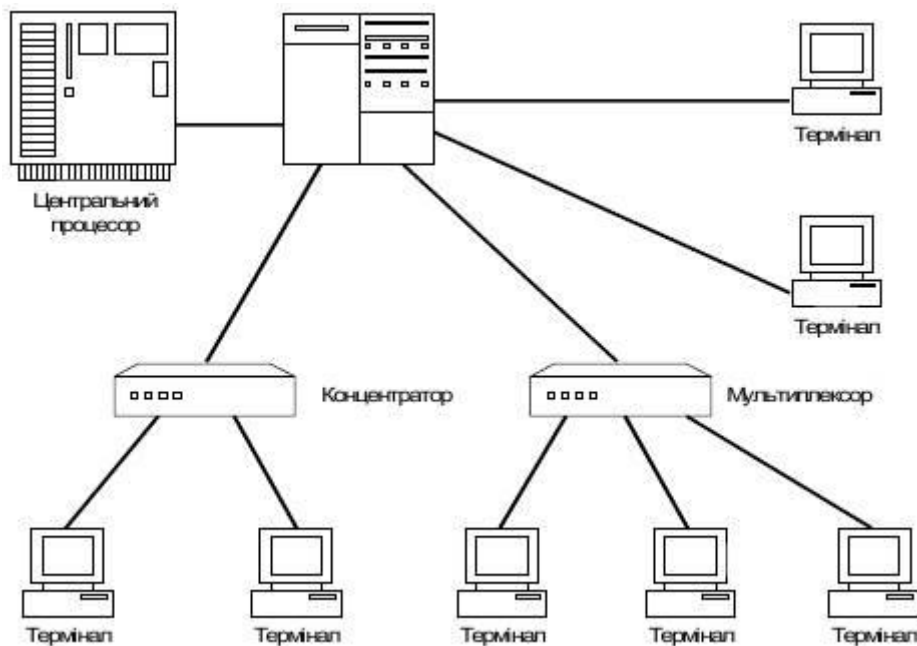


Рис. 1.2. Комп'ютерна мережа з фронтальним процесором, концентратором і мультиплексором

Сучасні комп'ютерні мережі будують з використанням багатфункціональних пристроїв – концентраторів, що одночасно виконують також функції маршрутизації та коригування сигналів. У таких мережах може бути багато центральних процесорів і терміналів чи робочих станцій. Структура сучасних глобальних мереж наведена на рис.1.3.



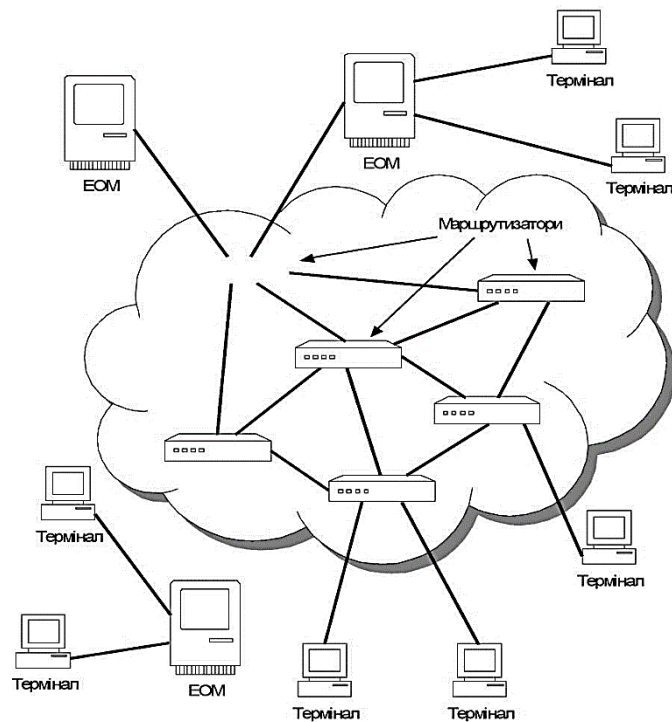


Рис. 1.3. Структура сучасних глобальних мереж

Усі ці рішення стосувались комп'ютерних мереж, які охоплювали території великих підприємств та установ, а також території держав.

Із розвитком персональних комп'ютерів постало питання про створення локальних комп'ютерних мереж у межах невеликих організацій, ділянок підприємств та офісів. Розвиток мікропроцесорної техніки й здешевлення персональних комп'ютерів дозволило розвинути технології локальних комп'ютерних мереж, в яких зараз за результатами спостережень концентрується до 80% інформаційних потоків.

Загалом із розвитком персональних комп'ютерів з'явилась можливість наблизити територіально місце обробки даних до місця їх виникнення, й, таким чином, підвищити ефективність роботи інформаційних систем.

Отже, технічною передумовою появи комп'ютерних мереж став розвиток комп'ютерної техніки й технологій зв'язку.

Натомість економічною передумовою появи комп'ютерних мереж стала постановка таких завдань, вирішення яких давало значно більший прибуток, ніж становили витрати на створення комп'ютерних мереж.

До таких завдань відносились зокрема завдання в галузі оборони, освоєння космосу, наукових досліджень у метеорології, матеріалознавстві, фундаментальній фізиці й хімії тощо.

## 1.2. Поняття про комп'ютерну мережу

З терміном «мережа» ми зустрічаємося дуже часто: мережа магазинів, мережа водопостачання в місті, телефонна мережа тощо.

**Мережа** – це сукупність взаємопов'язаних об'єктів, що мають однакове призначення та спільні властивості. До будь-якої мережі може входити різна кількість об'єктів – від двох до великої кількості.

Комп'ютери також можуть бути об'єднані в мережу. Але щоб вони були об'єднані між собою, потрібні додаткові пристрої та спеціальне програмне забезпечення (див. рис. 1.4).



**Мережа (Network)** – група комп'ютерів і/або інших пристроїв, з'єднаних між собою будь-яким способом для обміну даними й спільного використання ресурсів (пристроїв).



**Ресурси** – програми, файли даних, а також принтери й інші периферійні пристрої в мережі, що спільно використовуються.

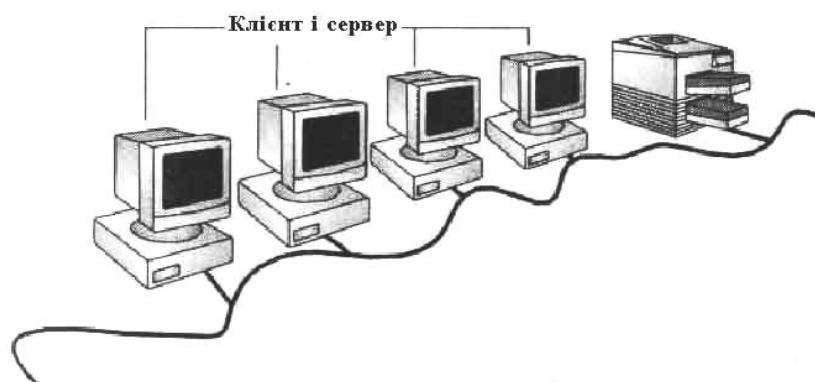


Рис. 1.4. Найпростіша мережа (кілька комп'ютерів і загальний принтер)

Комп'ютери об'єднують між собою для того, щоб:

- отримати доступ до об'єктів файлової системи комп'ютерів мережі;

- перемістити дані з одного комп'ютера на інший комп'ютер у мережі;
- отримати доступ до мережевого пристрою, наприклад, принтера, з можливістю друкування на ньому власних документів.

### **Основні характеристики комп'ютерної мережі**

Основними характеристиками комп'ютерної мережі є:

- мережева топологія – відображає просторове розташування мережевих вузлів та каналів зв'язку, яким визначається здатність мережевих компонентів приймати і передавати дані;
- мережеві протоколи – виражають формальний опис формату повідомлень і правил, за якими здійснюється обмін даними між вузлами мережі;
- мережеві інтерфейси – апаратні технічні засоби з'єднання функціональних вузлів;
- мережеві технічні засоби – пристрої, що забезпечують з'єднання абонентських систем в комп'ютерну мережу;
- мережеве програмне забезпечення – програмне забезпечення, що призначене для управління роботою комп'ютерної мережі і забезпечення інтерфейсу користувача.

### **1.3. Класифікація комп'ютерних мереж**

Комп'ютерні мережі класифікують за різними ознаками, зокрема (див. рис. 1.5).

Найпоширенішою є класифікація комп'ютерних мереж за територіальною ознакою. Відповідно з нею розрізняють такі мережі:

Локальні мережі (LAN) – невелика група комп'ютерів, з'єднаних один з одним і розташованих зазвичай в межах однієї будівлі або організації. У загальному випадку локальні мережі є комунікаційними системами, що належать одній організації. Ці мережі з просторовою протяжністю 1-2 км, в

яких використовуються високоякісні лінії зв'язку зі швидкостями передачі даних ~100 Мбіт/с. У локальних мережах дороговартісними є пристрої обробки інформації (комп'ютери), а не комунікаційні пристрої. Ефективність локальних мереж визначається ефективністю використання прикладного програмного забезпечення.

Локальна мережа дозволяє абоненту (користувачу) не помічати з'єднання, тобто забезпечує прозоре з'єднання. За своєю суттю, комп'ютери, зв'язані локальною мережею об'єднуються в один віртуальний комп'ютер, ресурси якого можуть бути доступні всім користувачам.

Головна відмінність LAN від будь-якої іншої – висока швидкість пересилання інформації (зараз зустрічається 1000 Мбіт/с), а також вірогідність інформації, що передається, визначається кількістю помилок на один знак.



Рис. 1.5. Класифікація комп'ютерних мереж

Міські (регіональні) мережі (MAN) – мережі, що з'єднують безліч локальних мереж у межах одного району, міста або регіону. Вони є менш поширеним типом. Середні за протяжністю мережі, що призначені для обслуговування великого міста (мегаполісу). Залежно від конкретної реалізації ці мережі можуть створюватись і функціонувати на основі локальних чи

глобальних мереж. Відстань між вузлами мережі становить 10-1000 км. Ці мережі використовують цифрові магістральні лінії зв'язку (оптоволоконні) зі швидкостями передачі даних від 45 Мбіт/с. Ці мережі були розроблені спочатку для передавання даних, але зараз вони підтримують і такі послуги, як відеоконференції і інтегральне передавання голосу і тексту.

Глобальні мережі (WAN) – мережа, що об'єднує комп'ютери різних міст, регіонів і держав. Територіально розподілені на великих площах мережі, що використовують вже існуючі лінії зв'язку з невисокою якістю передачі даних (телефонні і телеграфні зі швидкостями передачі даних порядку десятків Кбіт/с), або нові, спеціально прокладені лінії зв'язку та потребують складного комунікаційного обладнання для прийому-передачі даних. Із-за низьких швидкостей таких ліній зв'язку в глобальних мережах (десятки кілобіт в секунду) набір послуг, що надаються, зазвичай обмежується передаванням файлів, переважно не в оперативному, а у фоновому режимі. Завдяки використанню супутникових каналів зв'язку, комп'ютери з'єднуються на відстані 15 тис. км один від одного.

Основним фізичним середовищем для передавання даних у глобальних мережах є звичайні телефонні лінії з низькою швидкістю передавання, коаксіальні оптоволоконні кабелі, вита (скручена) пара, мікрохвильовий, інфрачервоний або радіоканал; (1 – 3 Кбіт/с) та великим рівнем перешкод. Відповідно, швидкість передавання даних у цих мережах не перевищує можливостей ліній зв'язку і є значно нижчою від швидкості обробки даних у комп'ютері.

У глобальних мережах найдорожчий елемент – обладнання та лінії зв'язку, які визначають ефективність та швидкість функціонування таких мереж. Швидкість обробки даних у комп'ютері тут практично несуттєва.

Істотною відмінністю локальних і глобальних мереж, крім площі, на якій розміщено комп'ютери, є використання різних форм подання даних під час їх передавання. У локальних мережах дані передаються так, як вони зберігаються й опрацьовуються в комп'ютері. Для роботи в глобальній мережі потрібен певний

пристрій, що буде здійснювати перетворення даних на вході й на виході комп'ютера.

Основними відмінностями між LAN і WAN є:

- протяжність;
- якість ліній зв'язку;
- швидкість передачі даних;
- складність обладнання та методів передачі і обробки даних.

Сучасною тенденцією є зближення LAN і WAN за рахунок:

- покращення якості передачі даних (за рахунок використання оптоволоконних ліній зв'язку);
- виникнення MAN;
- зростання захищеності інформації;
- виникнення intranet-технологій;
- можливість інтерактивної роботи навіть в WAN.

Об'єднання глобальних, регіональних і локальних обчислювальних мереж дозволяє створювати багаторівневі ієрархії, які надають потужні засоби для обробки величезних масивів даних і доступ до практично необмежених інформаційних ресурсів.

Останнім часом у зв'язку з розвитком мережевих технологій та розширенням сфери їх застосування в окрему групу стали виокремлюватися й корпоративні комп'ютерні мережі.

Корпоративні комп'ютерні мережі – це об'єднання кількох локальних комп'ютерних мереж однієї організації чи підприємства у єдину мережу за допомогою ліній зв'язку глобальних комп'ютерних мереж.

Локальні обчислювальні мережі можуть входити як компоненти до складу регіональної мережі; регіональні мережі – об'єднуватися у складі глобальної мережі; нарешті, глобальні мережі можуть утворювати ще більші структури. Найбільшим об'єднанням комп'ютерних мереж в масштабах планети Земля на сьогодні є «мережа мереж» – Інтернет.

Цікавим прикладом зв'язку локальних і глобальних мереж є віртуальна приватна мережа (Virtual Private Network, VPN). Так називається мережа організації, що створюється в результаті об'єднання двох або декількох територіально розділених локальних мереж за допомогою загальнодоступних каналів глобальних мереж, наприклад, через Інтернет (див. рис. 1.6).

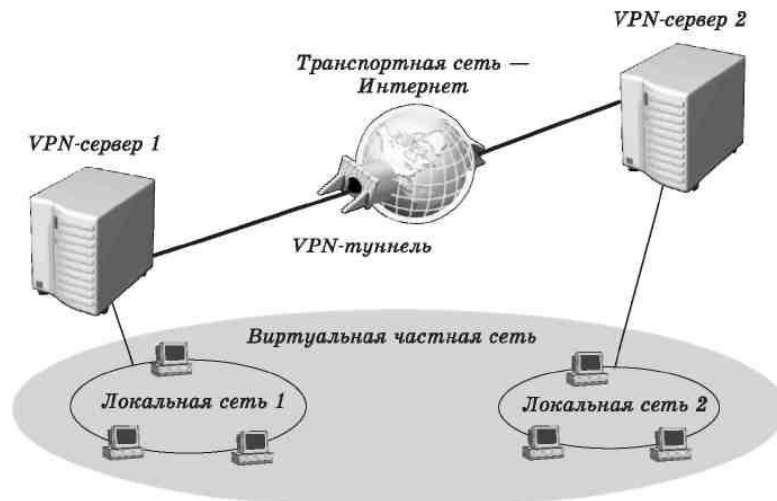


Рис. 1.6. Віртуальна приватна мережа – кілька локальних мереж підприємства, об'єднаних через Інтернет

За типом середовища передавання мережі діляться на проводові (дротові) й бездротові.

За швидкістю передавання інформації комп'ютерні мережі можна розділити на низько-, середньо- та високошвидкісні.

Із погляду розподілу ролей між комп'ютерами мережі бувають однорангові й клієнт-серверні.

Розглянемо детальніше однорангові й клієнт-серверні мережі.

#### 1.4. Однорангові мережі

В одноранговій мережі (див. рис. 1.7) всі комп'ютери рівноправні. Кожен із них може бути як сервером, тобто надавати файли й апаратні ресурси (накопичувачі, принтери тощо) іншим комп'ютерам, так і клієнтом, який користується ресурсами інших комп'ютерів. Наприклад, якщо на комп'ютері встановлений принтер, то з його допомогою зможуть роздруковувати свої

документи інші користувачі мережі, а ви, разом із тим, зможете працювати з Інтернетом, підключеним через сусідній комп'ютер.

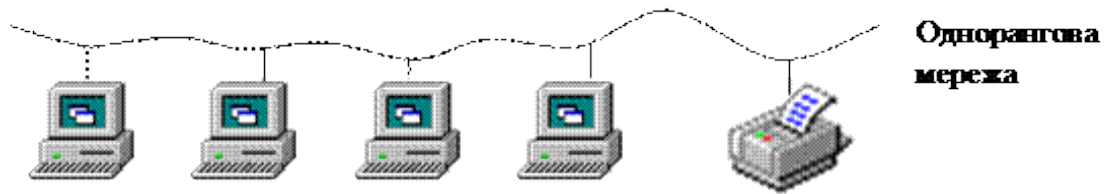


Рис. 1.7. Приклад однорангової мережі



**Адміністратор мережі** – людина, яка володіє всіма повноваженнями для управління комп'ютерами, користувачами й ресурсами в мережі.



**Адміністрування мережі** – рішення цілого комплексу завдань щодо управління роботою комп'ютерів, мережевого обладнання й користувачів, захисту даних, забезпечення доступу до ресурсів, установки й модернізації системного й прикладного програмного забезпечення.

### Переваги й недоліки однорангових мереж

Однорангові мережі мають як свої переваги, так і недоліки (див. табл. 1.1).

Таблиця 1.1.

### Переваги та недоліки однорангових мереж

<i>Переваги</i>	<i>Недоліки</i>
<ul style="list-style-type: none"> <li>– легкість під час установлення й налаштування;</li> <li>– незалежність окремих комп'ютерів та їхніх ресурсів один від одного;</li> <li>– можливість для користувача контролювати ресурси власного комп'ютера;</li> <li>– порівняно низька вартість розгортання й підтримки;</li> <li>– відсутність необхідності в додатковому програмному забезпеченні (крім операційної системи);</li> <li>– відсутність необхідності в постійній присутності адміністратора мережі;</li> </ul>	<ul style="list-style-type: none"> <li>– необхідність пам'ятати стільки паролів, скільки є розділених ресурсів (для мереж на основі Windows або імен і паролів для входу);</li> <li>– необхідність робити резервне копіювання окремо на кожному комп'ютері, щоб захистити всі дані, що спільно використовуються;</li> <li>– відсутність можливості централізованого керування мережею й доступом до даних;</li> <li>– низька загальна захищеність мережі й даних</li> </ul>



Кількість комп'ютерів у однорангових мережах звичайно не перевищує 10, їх називають робочою групою. Типовими прикладами таких груп є домашні мережі або мережі невеликих офісів.

### 1.5. Мережі з виділеним сервером (мережі типу «клієнт-сервер»)

Як правило, мережі створюються в установах або великих організаціях. У таких мережах (див. рис. 1.8) виділяються один або кілька комп'ютерів, які називаються серверами, їх завдання полягає у швидкій й ефективній обробці великої кількості запитів інших комп'ютерів – клієнтів. При цьому клієнтські запити бувають самими різними, починаючи з найпростішої перевірки імені й пароля користувача при вході в систему й закінчуючи складними пошуковими запитами до баз даних.

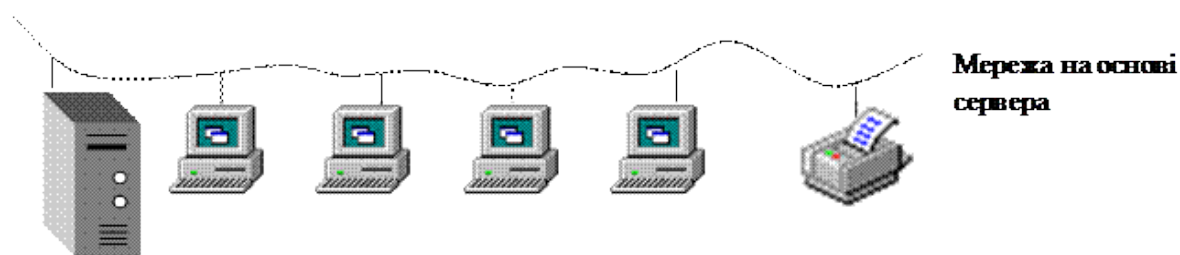


Рис. 1.8. Приклад мережі з виділеним сервером



**Сервер** – спеціально виділений високопродуктивний комп'ютер, оснащений відповідним програмним забезпеченням, що централізовано керує роботою мережі й/або, надає іншим комп'ютерам мережі свої ресурси (файли даних, накопичувачі, принтер тощо).



**Клієнтський комп'ютер (клієнт, робоча станція)** – комп'ютер певного користувача мережі, що одержує доступ до ресурсів сервера (серверів).

Серверами є потужні й надійні комп'ютери. Сервери часто оснащують спеціалізованим обладнанням, наприклад, сховищами даних великого обсягу (жорсткими дисками й так званими «рейд-масивами» на їхній основі), високошвидкісними мережевими адаптерами тощо. Такі комп'ютери працюють

постійно, цілодобово, надають користувачам свої ресурси й забезпечують доступ до своїх служб.



**Служби (services)** – програми, що працюють на серверах і виконують будь-які дії на запит клієнта.

Клієнт-серверні мережі мають як свої переваги, так і недоліки (див. табл. 1.2).

*Таблиця 1.2.*

### **Переваги й недоліки клієнт-серверних мереж**

<b>Переваги</b>	<b>Недоліки</b>
<ul style="list-style-type: none"> <li>– використання потужного серверного встаткування забезпечує швидкий доступ до ресурсів і ефективну обробку запитів клієнтів: один сервер може обслуговувати тисячі користувачів;</li> <li>– централізація даних і ресурсів дозволяє налагодити чітке керування інформацією й користувацькими даними;</li> <li>– розміщення даних на сервері суттєво спрощує процедури резервного копіювання;</li> <li>– підвищується загальна захищеність мережі й безпечність.</li> </ul>	<ul style="list-style-type: none"> <li>– несправність сервера може зробити всю мережу практично неприцездатною, а ресурси – недоступними;</li> <li>– складність розгортання й підтримки вимагає наявності кваліфікованого персоналу, що збільшує загальну вартість супроводу мережі;</li> <li>– вартість супроводу мережі також збільшується через потребу у додатковому устаткуванні й спеціалізованому програмному забезпеченні;</li> <li>– потрібна постійна присутність на робочому місці адміністратора(ів)</li> </ul>

### **1.6. Взаємодія комп'ютерів у мережі**

Розглянемо взаємодію комп'ютерів у мережі. Для взаємодії комп'ютерів у мережі, спочатку потрібно з'єднати між собою всіх учасників мережі – сервери, стаціонарні робочі станції користувачів, ноутбуки, принтери, мережеві сховища даних тощо. Для цих цілей застосовуються мережеві кабелі різних типів, телефонні або супутникові канали, бездротові рішення (WLAN, Wi-Fi, Wi-max). При використанні кабелів потрібні спеціальні конектори, закріплені на їхніх кінцях. Потім кабель одним кінцем вставляється в мережевий адаптер –

спеціальну плату («карту розширення»), установлену в комп'ютер і, що дозволяє підключити його до мережі, а іншим – у будь-який пристрій зв'язку (концентратор, міст, комутатор, маршрутизатор, шлюз тощо). У більшості сучасних комп'ютерів мережевий адаптер є вбудованим (відповідний роз'єм є безпосередньо на материнській платі). Якщо ж використовується бездротовий мережевий адаптер, то взаємодія з мережею відбувається за рахунок передачі радіосигналів між адаптером і точкою доступу, з'єднаної з локальною мережею.

Однак з'єднати комп'ютери один із одним недостатньо – потрібно ще й «навчити їх розмовляти» один з одним. Для цього потрібні мережеві операційні системи, що підтримують той самий набір протоколів, або мов, за допомогою яких комп'ютери «спілкуються» по мережі. І тільки після цього, відкривши мережевий додаток, можна буде, наприклад, поспілкуватися будь з ким і будь де.

## **1.7. Стандартизація у комп'ютерних мережах**

Створення, розвиток і поширення використання комп'ютерних мереж були б неможливими без використання однакових правил передачі та обробки даних – стандартів.

Основними організаціями, які розробляють та сприяють впровадженню стандартів в галузі комп'ютерних мереж є:

1. Міжнародний телекомунікаційний союз (МТС) (ITU – International Telecommunication Union). Стандарти МТС поділяються на серії. Стандарти кожної серії присвячені одній тематиці і позначаються великою літерою латинського алфавіту. Після літери ставиться крапка і номер стандарту. Так, наприклад, літерою V позначаються стандарти щодо передавання даних телефонними каналами, літерою X – стандарти щодо мереж передавання даних, літерою Q – стандарти щодо телефонної комутації та сигналізації.

2. Технічний комітет 97 – комітет міжнародної організації зі стандартизації (ISO – International Standard Organization). Технічний комітет

розробляє стандарти щодо опрацювання інформації за допомогою комп'ютера. Стандарти цієї організації позначаються чотиризначним числом і суфіксом ISO. Так, наприклад, стандарт, який стосується протокольного стеку TCP/IP має позначення 7498 ISO.

3. Комісія з питань діяльності Internet (IAB – Internet Activities Board) – розробляє стандарти щодо діяльності Internet.

Дотримання стандартів, які розроблені цими організаціями, є обов'язковим під час проектування, створення та експлуатації будь-яких комп'ютерних мереж.

До недавнього часу в практиці організації комп'ютерного зв'язку широко використовувалась модель взаємодії відкритих систем. Відкрита система (Open system) – система, яка побудована і функціонує з дотриманням вимог міжнародних стандартів.

Структура середовища зв'язку відкритих систем визначається стандартом 7498 ISO. Середовище в цілому має складний набір функцій. Під час його створення використовують ієрархічний підхід, який ґрунтується на наступних засадах:

- оскільки функція передавання у середовищі дуже складна, то її розділяють за рівнями;
- на кожному рівні виконується конкретний скінчений набір завдань;
- на межі між рівнями обмін даними повинен бути мінімальним;
- рівні повинні описуватись так, щоб зміни на одному з них не викликали необхідності внесення змін на інших рівнях.

Розглянемо принципи взаємодії комп'ютерів у мережі більш детально.

Щоб спілкуватися, люди найчастіше використовують усну мову. Однак таке безпосереднє спілкування можливо, тільки якщо співрозмовники знаходяться поруч один із одним. Але якщо уявити, що треба передати дані товаришеві, який живе в іншому місті, а тим більше – в іншій країні, то у такій ситуації не обійтись без виконання певних дій: потрібно написати текст на аркуші паперу, підписати його, вкласти в конверт, указати на ньому адреси

відправника й одержувача, наклеїти марку й віддати листоноші (або кинути в поштову скриньку). Подальша доля цього листа залежить уже не від вас, а від поштової служби. Будь-яким способом – потягом, кораблем, літаком або якимось іншим способом, але лист доходить до країни й міста, де живе ваш друг, потім доставляється до його поштового відділення й, нарешті, попадає до її поштової скриньки. Тільки тоді ваш адресат одержує можливість відкрити конверт і прочитати ваше повідомлення. Зазначимо, якщо будь-яка зі стадій доставки не спрацює, наприклад, через відсутність листоноші або розходжень у правилах запису адреси у різних країнах, то інформація до вашого друга так і не дійде.

Точно так само працюють і комп'ютери при «спілкуванні» в мережі. Способів безпосереднього спілкування в них немає – «розмовляти» один з одним комп'ютери поки ще не навчилися. Тому, щоб «спілкуватися», їм доводиться вдаватися до цілого ряду послідовно виконуваних процедур, які називаються мережевими протоколами. Щоб протоколи працювали надійно й злагоджено, кожна операція в них чітко регламентується. А щоб програми й обладнання різних виробників могли взаємодіяти одна з одною, протоколи повинні відповідати певним промисловим стандартам.



**Протокол** – це набір правил і процедур, що регулюють порядок взаємодії комп'ютерів у мережі.

За довгі роки існування комп'ютерних мереж було створене безліч різних протоколів – як відкритих (опублікованих для безкоштовного застосування), так і закритих (розроблених комерційними компаніями й потребують ліцензування для їхнього використання). Проте всі ці протоколи прийнято співвідносити з так званою еталонною моделлю взаємодії відкритих систем (Open Systems Interconnection Reference Model), або просто моделлю OSI. Її опис був опубліковано в 1984 р. Міжнародною організацією зі стандартизації (International Standards Organization, ISO), тому для неї часто використовується інша назва – модель ISO/OSI. Ця модель являє собою набір специфікацій, що

описують мережі з неоднорідними пристроями, вимоги до них, а також способи їхньої взаємодії.

## 1.8. Структура моделі OSI

Модель OSI має вертикальну структуру, у якій усі мережеві функції розподілені між сімома рівнями (див. рис. 1.9). Кожному такому рівню відповідають певні операції, обладнання та протоколи.

Реальна взаємодія рівнів, тобто передача інформації всередині одного комп'ютера, можлива тільки по вертикалі й тільки з сусідніми рівнями (вищими і нижчими).

Логічна взаємодія (відповідно до правил того чи іншого протоколу) здійснюється по горизонталі – з аналогічним рівнем іншого комп'ютера на протилежному кінці лінії зв'язку. Кожний вищий рівень користується послугами рівня, розташованого нижче, знаючи, у якому виді та яким способом (тобто через який інтерфейс) потрібно передати йому дані.

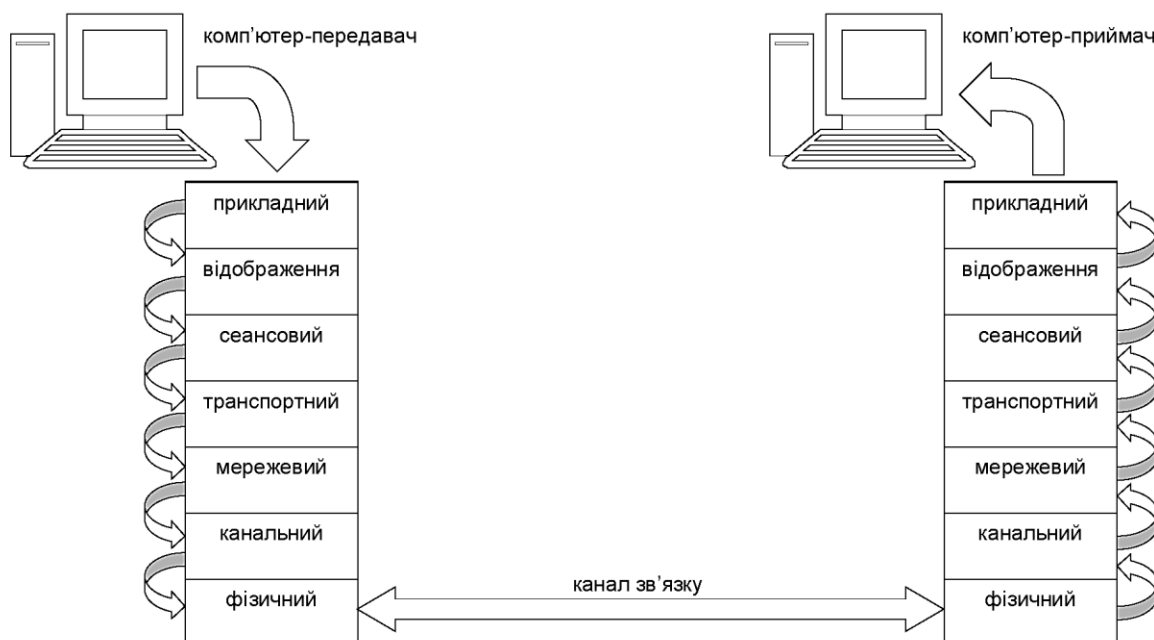


Рис. 1.9. Взаємозв'язки між рівнями моделі OSI

Завдання більш низького рівня – прийняти дані, додати свою інформацію (наприклад, форматуєчу або адресну, яка необхідна для правильної взаємодії з

аналогічним рівнем на іншому комп'ютері) і передати дані далі. Тільки дійшовши до самого нижчого, фізичного рівня мережевої моделі, інформація попадає в середовище передачі й досягає комп'ютера-одержувача. У ньому вона проходить крізь усі шари у зворотному порядку, поки не досягне того ж рівня, з якого була надіслана комп'ютером-відправником.

Як бачимо, усе це дуже схоже на наш приклад з роботою пошти – програми «спілкуються» по мережі приблизно так само, як ви зі своїм другом поштою. Ваш аркуш паперу з текстом передається з верхнього рівня вниз, проходячи безліч необхідних стадій. При цьому він «обростає» службовою інформацією (конверт певного виду, адреса на конверті, поштовий індекс) і зазнає певної обробки (листоноша у відділенні забирає лист, на конверт наклеюють марки, ставлять штемпелі, а після сортування лист попадає в контейнер для перевезення пошти в інше місто). Так ваша інформація доходить до самого нижнього рівня – поштового транспорту, яким вона перевозиться в пункт призначення. Там відбувається зворотний процес: відкривається контейнер, лист витягають, зчитується адреса, після чого листоноша доставляє лист вашому другові. А потім ваш друг одержує інформацію в первісному виді – коли витягає аркуш із конверта, перевіряє підпис і читає текст.

Таким чином, ви з вашим другом логічно маєте прямий зв'язок, і деталі доставки вас мало турбують. Листоноші також мають прямий зв'язок: листоноша в чужім місті одержить у точності те, що ви передали своєму листоноші – конверт із листом і адресною інформацією. Листонош при цьому не хвилюють проблеми, наприклад, залізничників, які в дійсності й здійснювали перевезення поштової кореспонденції.

Розглянемо рівні моделі OSI і визначимо мережеві послуги, які вони надають суміжним рівням.

## **Рівні моделі OSI**

**Рівень 0** – не визначений у загальній схемі (на рис. 1.10), але досить важливий для розуміння. Тут представлені посередники, за якими власне і

відбувається передача сигналів: кабелі різних типів, радіо-, інфрачервоні сигнали та ін. На цьому рівні нічого не описується, рівень 0 надає фізичному рівню 1 тільки середовище передавання.

**Рівень 1 – Фізичний (Physical).** Тут здійснюється передавання неструктурованого потоку бітів, отриманих від вищого канального рівня 2, по фізичному середовищу, наприклад, у вигляді електричних або світлових сигналів. Фізичний рівень відповідає за підтримку зв'язку (link) і детально описує електричні, оптичні, механічні й функціональні інтерфейси із середовищем передавання: напруги, частоти, довжини хвиль, типи конекторів, число й функціональність контактів, схеми кодування сигналів тощо.

**Рівень 2 – Канальний (Data Link).** Забезпечує безпомилкове передавання даних, отриманих від вищого мережевого рівня 3, через фізичний рівень 1, який сам по собі не гарантує відсутності помилок й може спотворювати дані. Інформація на цьому рівні поміщається в кадри (frames), де на початку (заголовку кадру) містяться адреси одержувача й відправника, а також керуюча інформація, а наприкінці – контрольна сума, що дозволяє виявити помилки, що виникають при передаванні.



Можна припустити, що контрольна сума (CRC) як засіб контролю правильності передавання даних з'явилася одночасно з першими ЕОМ. Але виявляється, що ідея «контрольної суми» була вперше винайдена тими хто переписував Біблію, стурбованими великою кількістю розбіжностей в текстах переписаної вручну Біблії (ще до винаходу друкарства): адже при кожному такому копіюванні писарі не тільки повторювали всі помилки свого оригіналу, але й додавали нові. З цієї проблеми було знайдено наступний вихід. На спеціальній нараді вищих духовних чинів був обраний і затверджений канонічний варіант Біблії. У ньому були підраховані кількості слів і букв в кожному розділі. Переписувач, закінчивши свою роботу, повинен був підрахувати цю кількість у зробленій копії і порівняти з оригінальними.

При отриманні даних на канальному рівні визначаються початок і кінець кадру в потоці бітів, сам кадр витягується з потоку й перевіряється на наявність помилок. Ушкоджені при передачі кадри, а також кадри, для яких не отримане підтвердження про прийом, пересилаються заново



(ретранслюються). Нарешті, на каналному рівні забезпечується керування доступом до середовища передавання.

Канальний рівень досить складний, тому відповідно зі стандартами IEEE (Institute of Electrical and Electronics Engineers), введеними в дію в лютому 1980 р. у рамках «Проекту 802» (Project 802), його часто розбивають на два підрівня: управління доступом до середовища (Media Access Control, MAC) і управління логічним зв'язком (Logical Link Control, LLC).



**Рівень MAC** забезпечує спільний доступ мережевих адаптерів до фізичного рівня, визначення границь кадрів, розпізнавання адрес призначення кадрів (ці адреси часто називають фізичними, або MAC-адресами).

Рівень LLC, що діє над рівнем MAC, відповідає за встановлення каналу зв'язку й за безпомилкове пересилання й прийом повідомлень із даними.

**Рівень 3 – Мережевий (Network).** Відповідає за забезпечення зв'язку між будь-якими вузлами в мережі. Цей рівень здійснює проведення повідомлень по мережі, яка може складатися з безлічі окремих мереж, з'єднаних безліччю ліній зв'язку. Така доставка вимагає маршрутизації, тобто визначення шляху доставки повідомлення, а також вирішення завдань управління потоками даних і обробки помилок передачі.

**Рівень 4 – Транспортний (Transport).** Гарантує доставку інформації від одного комп'ютера іншому. На цьому рівні комп'ютера-відправника великі блоки даних розбиваються на більш дрібні *пакети*, які доставляються комп'ютеру-одержувачеві в потрібній послідовності, без втрат і дублювання. На транспортному рівні комп'ютера-одержувача пакети знову збираються у вихідні блоки даних. Таким чином, транспортний рівень завершує процес передавання даних, приховуючи від більш високих рівнів усі деталі й проблеми, пов'язані з доставкою інформації *будь-якого обсягу* між будь-якими вузлами у всій мережі.

**Рівень 5 – Сеансовий (Session).** Дозволяє двом *мережевим додаткам* на різних комп'ютерах установлювати, підтримувати й завершувати з'єднання, яке називається *мережевим сеансом*. Цей рівень також відповідає за відновлення аварійно перерваних сеансів зв'язку. Крім того, на п'ятому рівні виконується перетворення зручних для людей імен комп'ютерів у мережеві адреси (*розпізнавання імен*), а також реалізуються функції *захисту сеансу*.

**Рівень 6 – Представницький, або Рівень подання даних (Presentation).** Визначає формати інформації, яка передається між комп'ютерами. Тут вирішуються такі завдання, як *перекодування* (переклад інформації у вид, зрозумілий для всіх комп'ютерів, що беруть участь в обміні), *стиснення* і *розпакування* даних, *шифрування* й *дешифрування*, підтримка мережевих файлових систем тощо.

**Рівень 7 – Прикладний (Application), або Рівень Додатків.** Забезпечує інтерфейс взаємодії програм, що працюють на комп'ютерах у мережі. Саме за допомогою цих програм користувач одержує доступ до таких мережевих послуг, як обмін файлами, передача електронної пошти, віддалений термінальний доступ тощо.



До появи моделі OSI вже існували й показали високу ефективність інші **набори (стеки) протоколів**, наприклад **стек TCP/IP**. Тому побудований у повній відповідності з описаною вище моделлю **набір протоколів OSI** так і не одержав широкого поширення. Більшість сучасних мережевих архітектур і наборів протоколів відповідають цій моделі лише до певної міри. Незважаючи на це, сама модель ISO/OSI досі широко використовується для опису взаємодії в мережевих середовищах.

### Запитання для перевірки знань

1. Що таке комп'ютерна мережа?
2. Які типи мереж ви знаєте?
3. Назвіть переваги комп'ютерних мереж?
4. Що таке тимчасова мережа? Які її переваги та недоліки?
5. Що таке мережа «клієнт-сервер»? Які її переваги та недоліки?

6. Що таке «адміністрування мережі»?
7. Опишіть яким чином комп'ютери взаємодіють один з одним у мережі?
8. Що розуміється під терміном «мережевий протокол»?
9. Які мережеві функції здійснюються в моделі OSI?
10. Який рівень, відповідно до моделі OSI, відповідає за вибір маршруту передачі даних?
11. На якому рівні моделі OSI взаємодіють програми, що забезпечують передачу повідомлень електронної пошти?

## **ЛЕКЦІЯ 2.**

### **Тема. Топології, методи доступу та архітектурні принципи побудови комп'ютерних мереж**

**Мета:** Ознайомити здобувачів вищої освіти з топологіями комп'ютерних мереж, методами доступу до середовища передавання даних і основними мережевими архітектурами.

### **ПЛАН**

1. Базові мережеві топології.
2. Інші можливі мережеві топології.
3. Доступ до середовища передавання.
4. Вибір комп'ютерної мережі.
5. Вибір мережевої архітектури.

#### **2.1. Базові мережеві топології**

При організації комп'ютерної мережі важливим є вибір топології, тобто компонування мережевих пристроїв і кабельної інфраструктури. Потрібно вибрати таку топологію, яка б забезпечила надійну й ефективну роботу мережі, зручне керування потоками мережевих даних.

Важливо розрізняти такі поняття, як фізична та логічна топологія.

Фізична топологія – спосіб розміщення комп'ютерів, мережевого устаткування та їхнє з'єднання за допомогою кабельної інфраструктури.

Логічна топологія – це структура взаємодії комп'ютерів і характеру поширення сигналів по мережі.

Існує три базові топології, на основі яких будується більшість мереж. Розглянемо їх більш детально.

Топологія «Шина» (Bus). Загальна шина це тип мережевої топології, в якій робочі станції розташовані уздовж однієї ділянки кабелю, що називається сегментом. У цій топології всі комп'ютери з'єднуються між собою одним кабелем. Топологія Загальна шина (див. рис. 2.1) припускає використання одного кабелю, до якого підключаються усі комп'ютери мережі.

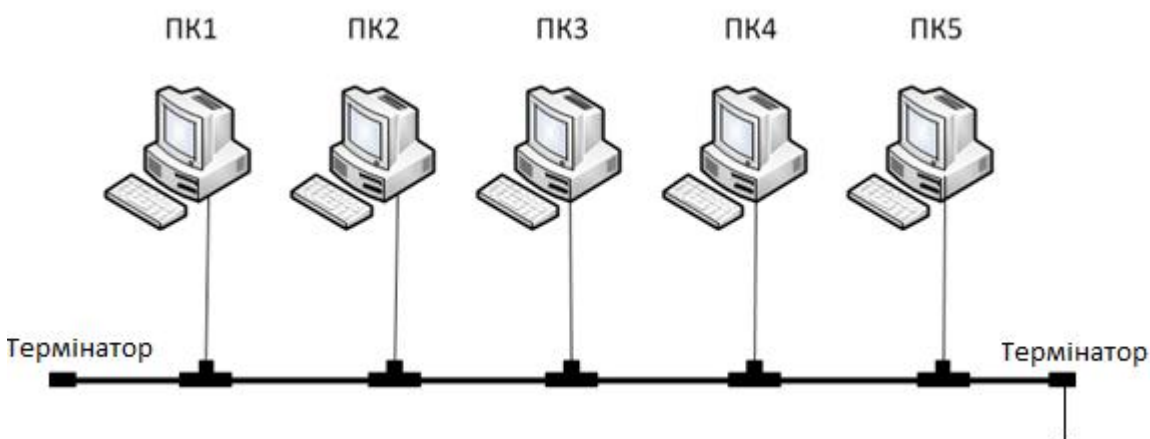


Рис. 2.1. Мережа з топологією «шина»

У разі топології Загальна шина кабель використовується усіма станціями по черзі. Вживаються спеціальні заходи для того, щоб при роботі із загальним кабелем комп'ютери не заважали один одному передавати і приймати дані. Усі повідомлення, що посилаються окремими комп'ютерами, приймаються і прослуховуються усіма іншими комп'ютерами, підключеними до мережі. Робоча станція відбирає адресовані їй повідомлення, користуючись адресною інформацією. Надійність тут вище, оскільки вихід з ладу окремих комп'ютерів не порушить працездатність мережі в цілому. Пошук несправності в мережі ускладнений. Крім того, оскільки використовується тільки один кабель, у разі

обриву порушується робота усієї мережі. Шинна топологія – це найбільш проста і найбільш поширена топологія мережі.

Шинна топологія – це найбільш проста і найбільш поширена топологія мережі., однак вона має низку істотних недоліків.

### **Недоліки мереж типу «шина»**

1. Такі мережі важко розширювати (збільшувати кількість комп'ютерів у мережі й кількість сегментів – окремих відрізків кабелю, що їх з'єднують).

2. Оскільки шина використовується спільно, у кожний момент часу передавання даних може здійснювати тільки один із комп'ютерів. Якщо передавання одночасно починають два або більше комп'ютерів, виникає спотворення сигналу (зіткнення, або колізія), що призводить до пошкодження всіх кадрів. Тоді комп'ютери змушені призупинити передачу, а потім по черзі ретранслювати дані. Вплив зіткнень тим помітніший, чим вищий обсяг переданої по мережі інформації і чим більше комп'ютерів підключено до шини. Обидва ці фактори, природно, знижують як максимально можливу, так і загальну продуктивність мережі, сповільнюючи її роботу.

3. «Шина» є пасивною топологією – комп'ютери тільки «слухають» кабель і не можуть відновлювати затухаючі при передаванні по мережі сигнали. Щоб подовжити мережу, потрібно використовувати повторювачі (репітери), що посилюють сигнал перед його передаванням до наступного сегменту.

4. Надійність мережі з топологією «шина» невисока. Коли електричний сигнал досягає кінця кабелю, він (якщо не вжити спеціальні заходи) відбивається, порушуючи роботу всього сегмента мережі. Щоб запобігти такому відображенню сигналів, на кінцях кабелю встановлюються спеціальні резистори (термінатори), що поглинають сигнали. Якщо ж у будь-якому місці кабелю виникає обрив – наприклад, при порушенні цілісності кабелю або просто при від'єднанні конектора, – то виникають два незатермінованих сегменти, на кінцях яких сигнали починають відбиватися, і вся мережа перестає працювати.

Проблеми, характерні для топології «шина», призвели до того, що ці мережі, популярні ще десять років тому, зараз уже практично не використовуються.

Топологія «Кільце» (Ring). У цій топології кожен із комп'ютерів з'єднується із двома іншими так, щоб від одного він одержував інформацію, а другому – передавав її (див. рис. 2.2). Останній комп'ютер підключається до першого, і кільце замикається. Кожен ПК працює як повторитель, ретранслюючи повідомлення до наступному ПК, тобто дані, передаються від одного комп'ютера до іншого як би по естафеті. Якщо комп'ютер отримує дані, призначені для іншого комп'ютера, він передає їх далі по кільцю, в іншому випадку вони далі не передаються. Дуже просто робиться запит на усі станції одночасно. Основна проблема при кільцевій топології полягає в тому, що кожна робоча станція повинна брати активну участь в пересилці інформації, і у разі виходу з ладу хоч би однієї з них, уся мережа паралізується. Підключення нової робочої станції вимагає короткострокового виключення мережі, оскільки під час установки кільце має бути розімкнене. Топологія Кільце має добре передбачуваний час відгуку, визначуваний числом робочих станцій

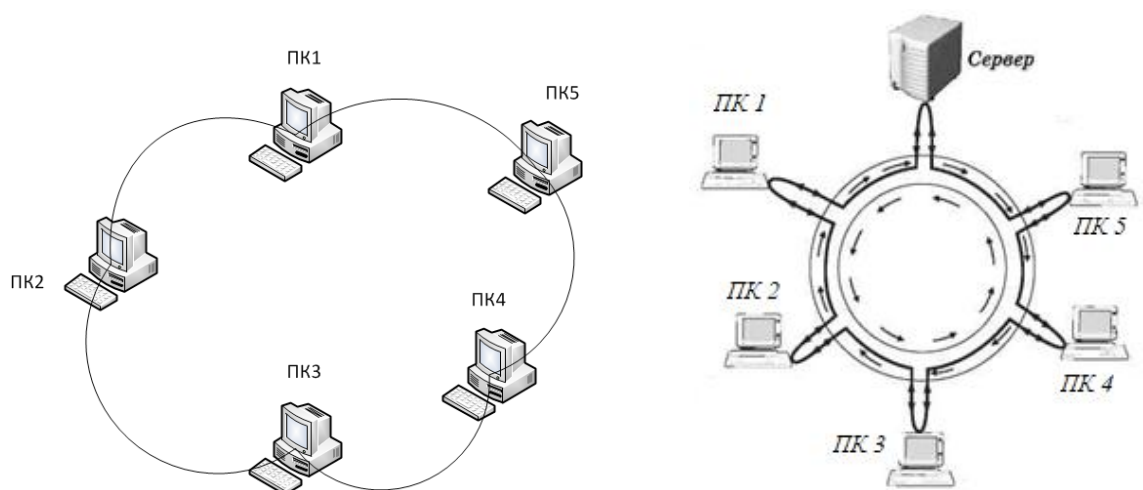


Рис. 2.2. Мережа з топологією «кільце»

Мережа з топологією «кільце» має свої переваги та недоліки (див. табл. 2.1).

### Переваги й недоліки мереж з топологією «кільце»

Переваги	Недоліки
<ul style="list-style-type: none"> <li>– не потрібні <i>термінатори</i>, оскільки у кабелів немає вільних кінців;</li> <li>– кожний з комп'ютерів виступає в ролі <i>повторювача</i>, посилюючи сигнал, що дозволяє будувати мережі великої довжини;</li> <li>– через відсутність <i>зіткнень</i> топологія має високу стійкість до перевантажень, забезпечуючи ефективну роботу з більшими потоками переданої по мережі інформації</li> </ul>	<ul style="list-style-type: none"> <li>– сигнал в «кільці» повинен пройти послідовно (і тільки в одному напрямку) через усі комп'ютери, кожний з яких перевіряє, чи не йому адресована інформація, тому час передачі може бути достатньо великим;</li> <li>– підключення до мережі нового комп'ютера часто вимагає її зупинки, що порушує роботу всіх інших комп'ютерів;</li> <li>– вихід з ладу хоча б одного з комп'ютерів або пристроїв порушує роботу всієї мережі;</li> <li>– обрив або коротке замикання в кожному з кабелів кільця робить роботу всієї мережі неможливою;</li> <li>– щоб уникнути зупинки роботи мережі при відмові комп'ютерів або обриві кабелю, звичайно прокладають два кільця, що суттєво здорожує мережу</li> </ul>

Чиста кільцева топологія використовується рідко. Замість цього кільцева топологія грає транспортну роль в схемі методу доступу. Кільце описує логічний маршрут, а пакет передається від однієї станції до іншої, здійснюючи у результаті повний круг. У мережах Token Ring кабельна гілка з центрального концентратора називається MAU (Multiple Access Unit). MAU має внутрішнє кільце, що сполучає усі підключені до нього станції, і використовується як альтернативний шлях, коли обірваний або від'єднаний кабель однієї робочої станції. Коли кабель робочої станції приєднаний до MAU, він просто утворює розширення кільця: сигнали поступають до робочої станції, а потім повертаються назад у внутрішнє кільце.

Сьогодні більш поширеною топологією є варіант – «зірка-шина» (Star Bus), або «пасивна зірка» (див. рис. 2.3). Тут периферійні комп'ютери підключаються не до центрального комп'ютера, а до пасивного концентратора, або хабу (hub). Останній, на відміну від центрального комп'ютера, ніяк не відповідає за керування обміном даними, а виконує ті ж функції, що й повторювач, тобто відновлює сигнали, які надходять, та пересилає їх усім іншим комп'ютерам і пристроям, підключеним до нього. Саме тому ця топологія, хоча фізично й виглядає як «зірка», логічно є топологією «шина» (що й відображено в її назві).

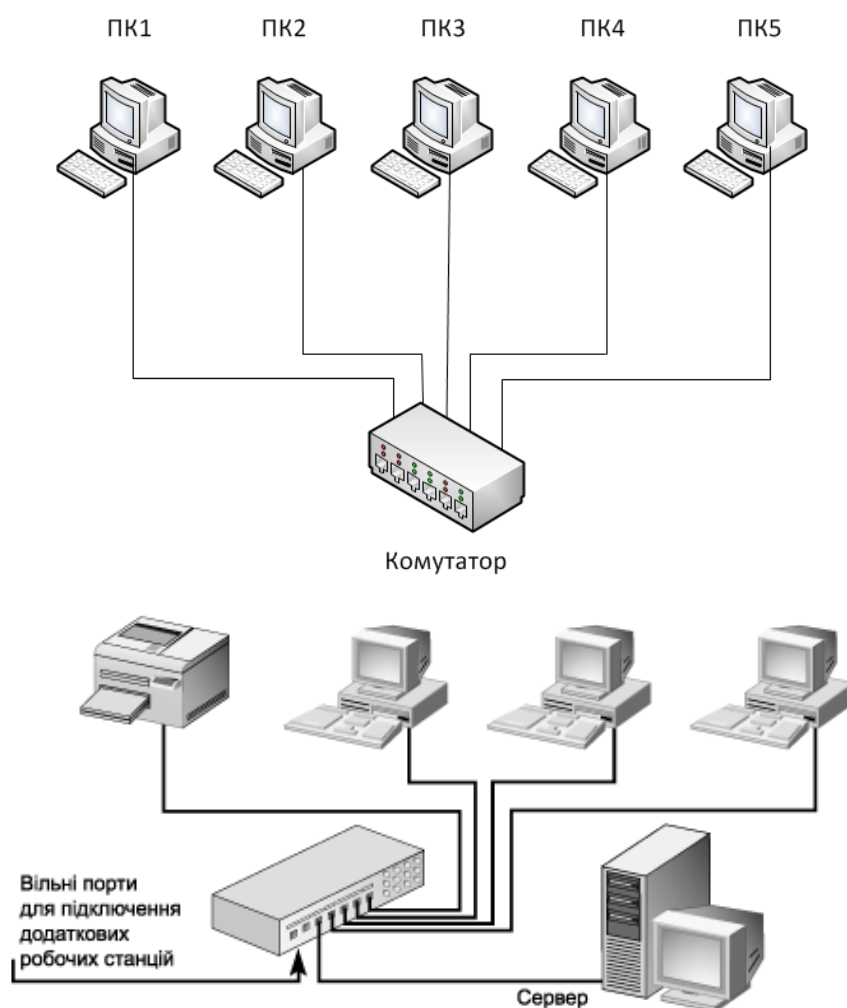


Рис. 2.3. Мережа з топологією «зірка-шина»

Незважаючи на більшу витрату кабелю, характерну для мереж типу «зірка», ця топологія має суттєві переваги перед іншими, що й обумовило її найширше застосування в сучасних мережах.



## **Переваги мереж типу «зірка-шина»**

1. *Надійність* – підключення до центрального концентратора й відключення комп'ютерів від нього ніяк не відбивається на роботі іншої мережі; обриви кабелю впливають тільки на одиничні комп'ютери; термінатори не потрібні.

2. *Легкість при обслуговуванні й усуненні проблем* – усі комп'ютери й мережеві пристрої підключаються до центрального з'єднувального пристрою, що істотно спрощує обслуговування й ремонт мережі.

3. *Захищеність* – концентрація точок підключення в одному місці дозволяє легко обмежити доступ до важливих об'єктів мережі.

Відзначимо, що при використанні замість концентраторів більш «інтелектуальних» мережевих пристроїв (*мостів, комутаторів і маршрутизаторів*) виходить «проміжний» тип топології між активною й пасивною зіркою. У цьому випадку пристрій зв'язку не тільки ретранслює сигнали, що надходять, але й проводить управління їх обміном.

## **2.2. Інші можливі мережеві топології**

Реальні комп'ютерні мережі постійно розширюються й модернізуються. Тому майже завжди така мережа є гібридною, тобто її топологія представляє собою комбінацію декількох базових топологій. Легко уявити собі гібридні топології, що є комбінацією «зірки» і «шини» або «кільця» і «зірки».

Однак особливо слід виділити топологію «дерево» (*tree*), яку можна розглядати як об'єднання декількох «зірок» (див. рис. 2.4). Саме ця топологія сьогодні є найбільш популярною при побудові локальних мереж.

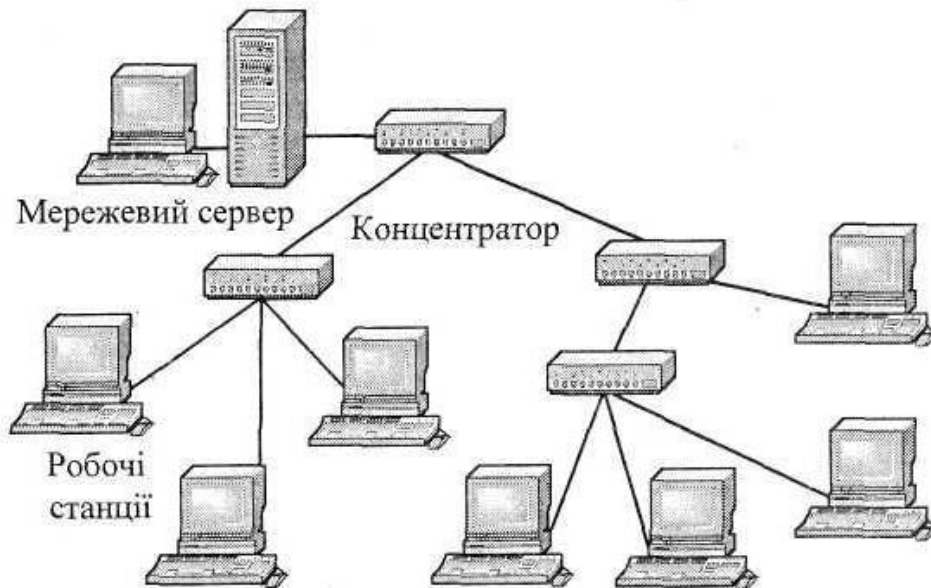


Рис. 2.4. Древоподібна топологія мережі

Сітчаста, або сіткова топологія (mesh). У цій топології всі або багато комп'ютерів та інші пристрої з'єднані один із одним безпосередньо (див. рис. 2.5). Така топологія надійна – при обриві будь-якого каналу передавання даних не припиняється, оскільки можливі декілька маршрутів доставки інформації. Сіткові топології (найчастіше не повні, а часткові) використовуються там, де потрібно забезпечити максимальну відмовостійкість мережі, наприклад, при об'єднанні кількох ділянок мережі великого підприємства або при підключенні до Інтернету (див. рис. 2.5.)

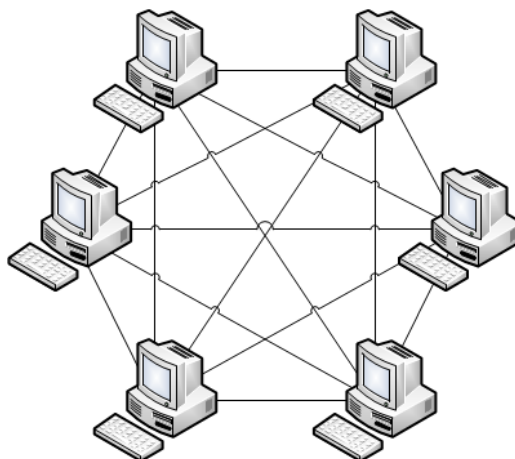


Рис. 2.5. Сітчаста топологія

## 2.3. Доступ до середовища передавання

З мережевою топологією тісно пов'язане поняття способу доступу до середовища передавання.



**Спосіб доступу до середовища передавання** – це набір правил, що визначають, як саме комп'ютери повинні відправляти й приймати дані по мережі.

Основними такими способами є:

- множинний доступ із контролем несучої й виявленням зіткнень;
- множинний доступ із контролем несучої й запобіганням зіткнень;
- передачею маркера.

При множинному доступі з контролем несучої й виявленням зіткнень (Carrier Sense Multiple Access with Collision Detection, CSMA/CD) усі комп'ютери (множинний доступ) «слухають» кабель (контроль несучої), щоб визначити, передаються по ньому дані чи ні. Якщо кабель вільний, будь-який комп'ютер може почати передавання; тоді всі інші комп'ютери повинні чекати, поки кабель не звільниться. Якщо комп'ютери почали передавання одночасно й виникло зіткнення, усі вони припиняють передавання (виявлення зіткнень), кожен – на різні проміжки часу, після чого ретранслюють дані.

Серйозним недоліком цього способу доступу є те, що при великій кількості комп'ютерів і високому навантаженню на мережу число зіткнень зростає, а пропускна здатність падає, іноді дуже суттєво.

Однак цей метод дуже простий у технічній реалізації, тому саме він використовується в найбільш популярній сьогодні технології Ethernet. А щоб зменшити кількість зіткнень, у сучасних мережах застосовуються такі пристрої, як мости, комутатори й маршрутизатори.

Метод множинного доступу з контролем несучої й запобіганням зіткнень (Carrier Sense Multiple Access with Collision Avoidance, CSMA/CA) відрізняється від попереднього тим, що перед передаванням даних комп'ютер посилає в мережу спеціальний невеликий пакет, повідомляючи іншим комп'ютерам про свій намір почати трансляцію. Так інші комп'ютери

«дізнаються» про підготовку передавання, що дозволяє уникнути зіткнень. Звичайно, ці повідомлення збільшують загальне навантаження на мережу й знижують її пропускну спроможність (через що метод CSMA/CA працює повільніше, чим CSMA/CD), однак вони, безумовно, необхідні для роботи, наприклад, бездротових мереж.

У мережах із передачею маркера (Token Passing) від одного комп'ютера до іншого по колу постійно курсує невеликий блок даних, що називається маркером. Якщо у комп'ютера, який одержав маркер, немає інформації для передавання, він просто пересилає його наступному комп'ютеру. Якщо ж така інформація є, комп'ютер «захоплює» маркер, доповнює його даними й відсилає все це наступному комп'ютеру по колу. Такий інформаційний пакет передається від комп'ютера до комп'ютера, поки не досягне станції призначення. Оскільки в момент передавання даних маркер у мережі відсутній, інші комп'ютери вже не можуть нічого передавати. Тому в мережах із передачею маркера неможливі ні зіткнення, ні тимчасові затримки, що робить їх досить привабливими для використання в системах автоматизації роботи підприємств.

## **2.4. Вибір комп'ютерної мережі**

Розглянувши мережеві топології та методи доступу, які найбільш часто використовуються сьогодні, обговоримо й інші чинники, що визначають вибір потрібного типу мережі. При цьому слід урахувати:

- уже наявну кабельну систему та обладнання – є чи у вас дома, навчальному закладі, офісі мережі, яку потрібно просто розширити, або у вас є тільки окремі комп'ютери;
- фізичне місце розташування – важливо враховувати, як розташовані комп'ютери й де ви збираєтеся розмістити мережеве обладнання. Об'єднати комп'ютери в одній кімнаті досить просто, проте якщо ваші комп'ютери розташовуються на різних поверхах будинку або навіть в декількох будівлях, найкращу конфігурацію мережі та її топологію слід ретельно продумати;

– розміри мережі, що планується – якщо у вас є лише кілька комп'ютерів, структура мережі буде досить простою; якщо ж комп'ютерів сотні або тисячі, то, швидше за все, доведеться зупинити свій вибір на складній гібридній топології;

– обсяг і тип інформації для спільного використання – ці параметри повинні обов'язково враховуватися при виборі типу мережі: якщо між комп'ютерами передаються великі файли – музичні, відео- або графічні, то вам буде потрібна високошвидкісна мережа, що дозволяє швидко й без затримок передавати такі обсяги інформації.



Переважна більшість сучасних мереж використовують топологію «зірка» або гібридну топологію, що представляє собою об'єднання декількох «зірок» (наприклад, топологію типу «дерево»), і метод доступу до середовища передачі CSMA/CD (множинний доступ з контролем несучої й виявленням зіткнень).

## 2.5. Вибір мережевої архітектури

Розглянемо основні мережеві архітектури, їх переваги й недоліки.



**Мережева архітектура** – набір стандартів, топологій і протоколів низького рівня, необхідних для створення працездатної мережі.

За багато років розвитку мережевих технологій було розроблено досить багато різних архітектур. Деякі з них уже вийшли з ужитку, тоді як інші, такі як *Ethernet*, не тільки активно використовуються донині, а й постійно вдосконалюються.

Розглянемо деякі з них.

### Token Ring

Token Ring (маркерне кільце) – архітектура мереж з кільцевою логічною топологією і детермінованим методом доступу із передачею маркера. Вона була розроблена компанією IBM в 70-х рр. XX ст. Стандарт визначений документом IEEE802.5. Token Ring має наступні характеристики:

- фізична топологія – «зірка»;

- логічна топологія – «кільце»;
- метод доступу – передача маркера;
- швидкість передавання даних – 4 або 16 Мбіт/с;
- максимальний розмір кадра – до 16 Кбайт;
- середовище передавання – кручена пара (використовується 2 пари);
- максимальна довжина сегмента:
  - UTP – 150 м (для 4 Мбіт/с) або 60 м (для 16 Мбіт/с),
  - STP – 300 м (для 4 Мбіт/с) або 100 м (для 16 Мбіт/с);
- максимальна довжина сегмента з репітерами:
  - UTP – 365 м,
  - STP – 730 м;
- максимальна кількість комп'ютерів на сегмент – 72 або 260 (залежно від типу кабелю).

Для об'єднання комп'ютерів у мережах Token Ring використовуються концентратори MSAU (Multistation Access Unit), неекранована або екранована кручена пара (можливо й застосування оптоволокна); у якості роз'ємів використовуються спеціалізовані з'єднувачі фірми IBM або стандартні конектори RJ-45.

Основні переваги архітектури Token Ring:

- велика дальність передавання даних (при використанні повторювачів MSAU можна передавати дані на відстань до 730 м);
- легко розрахувати максимальну затримку при передаванні інформації між будь-якими двома обладнаннями – адже в якості методу доступу до середовища використовується передача маркера;
- використання Token Ring у системах реального часу (свідомо обмежений час очікування обслуговування вузла, обумовлене детермінованим методом доступу і можливістю управління пріоритетом);
- легко з'єднуються з мережами на великих машинах (IBM Mainframe).

Недоліки архітектури Token Ring:

- досить висока вартість;
- низька сумісність устаткування (наприклад, у 16-мегабітних мережах Token Ring не можна використовувати 4-мегабітне обладнання);
- досить мала швидкість передавання даних.

## **ARCnet**

ARCnet (Attached Resource Computing Network – комп'ютерна мережа з'єднаних ресурсів) була розроблена корпорацією Datapoint в 1977 р. Стандартом вона так і не стала, але в цілому відповідає специфікації IEEE 802.4. Ця проста, гнучка й недорога архітектура для невеликих мереж (до 256 комп'ютерів) характеризується наступними параметрами:

- фізична топологія – «шина» або «зірка»;
- логічна топологія – «шина»;
- метод доступу – передача маркера;
- швидкість передачі даних — 2,5 або 20 (в Arcnet Plus) Мбіт/з;
- максимальний розмір кадра — 516 байт (в Arcnet Plus – близько 4 Кбайт);
- середовище передачі – кручена пара або коаксіальний кабель;
- максимальна довжина сегмента:
  - для крученої пари – 244 м (для будь-якої топології),
  - для коаксіального кабелю – 305 або 610 м (для топології «шина» або «зірка», відповідно).

Для з'єднання комп'ютерів використовуються концентратори. Основний тип кабелю – коаксіальний типу RG-62; підтримується також кручена пара й оптоволокло. Для коаксіального кабелю використовуються BNC-Конектори, для крученої пари – конектори RJ-45.

Перевага архітектури ARCnet – велика дальність передавання інформації при невисокій вартості встаткування.

Недоліки:

- важко знайти мережеві адаптери Arcnet.
- відсутність драйверів до мережевих адаптерів Arcnet у сучасних

операційних системах.

## **AppleTalk**

AppleTalk – стек протоколів, розроблених компанією Apple в 1983 р. і вбудована в комп'ютери Macintosh (остання версія – AppleTalk Phase 2). Архітектура AppleTalk містить у собі цілий набір протоколів, відповідних до моделі OSI. На рівні мережевої архітектури використовується протокол LocalTalk, що має наступні характеристики:

- топологія – «шина» або «дерево»;
- метод доступу – CSMA/CA;
- швидкість передавання даних – 230,4 Кбіт/с;
- середовище передавання – екранована кручена пара;
- максимальна довжина мережі – 300 м;
- максимальна кількість комп'ютерів – 32.

Дуже низька пропускна здатність вбудованої архітектури LocalTalk привела до того, що багато виробників стали пропонувати адаптери розширення, що дозволяли AppleTalk працювати з мережними середовищами більшої пропускної здатності – EtherTalk, TokenTalk і FddiTalk. У локальних мережах, побудованих на базі IBM-сумісних комп'ютерів, мережеве середовище AppleTalk практично не зустрічається.

## **100VG-AnyLAN**

Архітектура 100VG-AnyLAN була розроблена в 90-х рр. XX ст. компаніями AT&T і Hewlett-Packard для об'єднання мереж Ethernet і Token Ring (звідси слово «Any» у назві) і наступної міграції до єдиної швидкісної мережі. У 1995 р. ця архітектура одержала статус стандарту IEEE 802.12. Вона має наступні параметри:

- топологія – «зірка»;
- метод доступу – по пріоритету запиту;
- швидкість передавання даних – 100 Мбіт/с;



- середовище передавання – кручена пара категорії 3, 4 або 5 (використовуються всі 4 пари);
- максимальна довжина сегмента (для встаткування HP) – 225 м.

Відповідно зі специфікацією, концентратор 100VG-AnyLAN можна налаштувати на підтримку як кадрів Ethernet, так і кадрів Token Ring. Особливістю мереж 100VG-AnyLAN є використання у них методу доступу за пріоритетом запиту (Demand Priority), при якому концентратори управляють доступом до кабелю, опитуючи кожний вузол у мережі й виявляють запити на передачу. При одночасних запитах перевага віддається вузлу, що має більший пріоритет. Це дозволяє без затримок передавати в мережі 100VG-ANYLan мультимедійні дані (аудіо- і відеофайли).

Через складність і високу вартості встаткування архітектура 100VG-AnyLAN не одержала широкого поширення. У цей час вона практично не застосовується.

### Архітектури для домашніх мереж: Home PNA

У 1996 р. цілий ряд компаній об'єдналися для створення стандарту, що дозволяє будувати домашні мережі на основі звичайної телефонної проводки. Результатом їх роботи стала поява в 1998 р. архітектури Home PNA 1.0 (Home Phoneline Networking Alliance), а потім – архітектур Home PNA 2.0 і Home PNA 3.0. Їхні короткі характеристики наведені в табл 2.1.

*Таблиця 2.1*

#### Порівняння стандартів Home PNA

Версія Home PNA	Топологія	Швидкість передавання даних, Мбіт/з	Дальність передавання по телефонному кабелю, м	Максимальна кількість комп'ютерів у сегменті
1.0	«зірка» або «шина»	1	150	25
2.0	«шина»	10	350	32
3.0	«зірка» або «шина»	128	300	50

У всіх зазначених стандартах використовується самий популярний на сьогодні метод доступу до середовища – CSMA/CD; у якості середовища передавання, природно, рекомендується використання телефонного кабелю; у якості роз'ємів використовуються телефонні конектори RJ-11. Однак пристрої Home PNA можуть працювати і з крученою парою, і з коаксіальним кабелем, причому дальність передавання інформації при цьому суттєво зростає. Варто зазначити, що використання топології «зірка» і комутаторів в Home PNA версій 1.0 і 3.0 дозволяє об'єднувати сегменти, тоді загальна кількість пристроїв в об'єднаній мережі Home PNA може бути набагато більшою, ніж зазначено в табл. 2.1.

Незважаючи на уявну привабливість перспективи використання телефонних ліній для створення домашніх мереж, слід урахувати, що телефонна проводка в нашій країні багато в чому не відповідає стандартам розвинених країн як по якості, так і по охопленню (по наявності вже встановлених розеток у всіх кімнатах). Крім того, ціни на адаптери й обладнання для мереж Home PNA високі. Тому домашні мережі, побудовані на основі цієї технології майже не поширені. Проте архітектуру Home PNA (особливо її останню версію) цілком можна розглядати в якості альтернативи як для бездротових мереж (в офісних будинках і житлових будинках), так і для модемних з'єднань (при підключенні до Інтернету).

### **Домашні мережі на базі електропроводки**

Ще більш специфічними є спроби використання як середовища передачі звичайної електропроводки. Ця технологія з'явилася зовсім недавно й отримала назву Home PLC (Power Line Communication), або просто «HomePlug».

Спроби низки великих компаній, що об'єдналися під егідою некомерційної організації Homeplug Powerline Alliance, просувати цей стандарт як спосіб створення домашніх мереж, у тому числі з підключенням до Інтернету, поки особливим успіхом не увінчалися. Однак мережеве обладнання HomePlug уже є в продажі. Більшість із такого обладнання на практиці є

конвертерами (перетворювачами), що забезпечують підключення до мережі HomePlug адаптерів таких популярних мережевих технологій, як Ethernet або Wi-Fi (про них буде розказано далі). Існують і зовсім «екзотичні» пристрої, що наприклад дозволяють передавати по електропроводці аудіоінформацію між комп'ютером і музичним центром.

Параметри мереж Homeplug:

- топологія – «шина»;
- метод доступу – CSMA/CD;
- швидкість передавання даних – до 85 Мбіт/с;
- середовище передавання – електрична проводка;
- дальність зв'язку – до 200 м;
- рекомендована кількість обладнання в мережі – не більш 15.

Недоліки мереж Home PLC – незахищеність від перехоплення, що вимагає обов'язкового застосування технологій шифрування, і більша чутливість до електричних перешкод, які досить різко знижують швидкість передачі на більших відстанях. До того ж обладнання Homeplug поки ще досить дороге. Проте стандарт Home PLC є перспективним для використання в будинках, де мережна й телефонна проводка відсутня, а також для забезпечення зв'язку з керованими домашніми побутовими приладами. Тепер привернемо увагу до вивчення найбільш популярних технологій, що використовуються в сучасних локальних мережах.

## **Ethernet**

Архітектура Ethernet фактично поєднує цілий набір стандартів, що мають як загальні риси, так і відмінності. Спочатку вона була створена фірмою Херох у середині 70-х рр. і тоді представляла собою систему передачі зі швидкістю 2,93 Мбіт/с. Після доопрацювання за участю компаній Intel і DEC архітектура Ethernet послужила основою прийнятого в 1985 р. стандарту IEEE 802.3, що визначив для неї наступні параметри:

- топологія – «шина»;

- метод доступу – CSMA/CD;
- швидкість передачі – 10 Мбіт/з;
- середовище передачі – коаксіальний кабель;
- застосування термінаторів – обов’язково;
- максимальна довжина сегмента мережі – до 500 м;
- максимальна довжина мережі – до 2,5 км;
- максимальна кількість комп’ютерів у сегменті – 100;
- максимальна кількість комп’ютерів у мережі – 1024.

У початковій версії Ethernet передбачалося застосування коаксіального кабелю двох видів – «товстого» і «тонкого» (стандарти 10Base-5 і 10Base-2, відповідно). Однак на початку 90-х рр. також з’явилися специфікації для побудови мереж Ethernet з використанням крученому пари (10Base-T) і оптоволокна (10Base-fl). Пізніше, у 1995 р., був опублікований стандарт архітектури Fast Ethernet (IEEE 802.3u), що забезпечує передавання на швидкостях до 100 Мбіт/з, у 1998 р. – стандарт Gigabit Ethernet (IEEE 802.3z і 802.3ab), а в 2002 р. – стандарт 10 Gigabit Ethernet (IEEE 802.3ae).

Порівняння різних стандартів Ethernet наведено в табл. 2.2.

Таблиця 2.2

### Характеристики різних стандартів Ethernet

Реалізація	Швидкість передавання даних, Мбіт/с	Топологія	Середовище передавання	Максимальна довжина кабелю, м
<i>Ethernet</i>				
10Base-5	10	«шина»	товстий коаксіальний кабель	500
10Base-2	10	«шина»	тонкий коаксіальний кабель	185; реально – до 300
10Base-T	10	«зірка»	кручена пара	100

Реалізація	Швидкість передавання даних, Мбіт/с	Топологія	Середовище передавання	Максимальна довжина кабелю, м
10Base-fl	10	«зірка»	оптоволокно	500 (станція-концентратор); 2000 (між концентраторами)
<i>Fast Ethernet</i>				
100Base-tx	100	«зірка»	кручена пара категорії 5 (використо-вується дві пари)	100
100Base-T4	100	«зірка»	кручена пара категорії 3, 4 або 5 (використову-ється чотири пари)	100
100Base-fx	100	«зірка»	багатомодове або одномодове оптоволокно	2000 (багатомодовий); 15000 (одномодовий); реально – до 40 км
<i>Gigabit Ethernet</i>				
1000Base-T	1000	«зірка»	кручена пара категорії 5 або вище	100
1000Base-cx	1000	«зірка»	спеціальний кабель типу STP	25
1000Base-sx	1000	«зірка»	оптоволокно	220-550 (багатомодовий), залежно від типу
1000Base-lx	1000	«зірка»	оптоволокно	550 (багатомодовий); 5000 (одномодовий); реально – до 80 км
<i>10 Gigabit Ethernet</i>				
10Gbase-x (x – набір стандартів)	10000	«зірка»	оптоволокно	300-40000 (залежно від типу кабелю й довжини хвилі лазера)

Основний недолік мереж Ethernet пов'язаний з використанням у них методу доступу до середовища CSMA/CD (нагадаємо: це скорочення розшифровується як «множинний доступ із контролем несучої й виявленням

зіткнень»). При збільшенні кількості комп'ютерів зростає число зіткнень, що знижує пропускну здатність мережі й збільшує час доставки кадрів. Тому рекомендованим навантаженням для мереж Ethernet вважається рівень в 30-40 % від загальної смуги пропускання. Відразу зауважимо, що в сучасних мережах цей недолік досить легко усувається шляхом заміни концентраторів *мостами* й *комутаторами*, що вміють «ізолювати» передачу даних між двома комп'ютерами в мережі від інших (про ці обладнання буде розповідь у наступній главі).

А ось переваг у архітектурі Ethernet досить багато. Перш за все, сама ця технологія досить проста в реалізації. Відповідно, Ethernet-пристрої (мережеві адаптери, концентратори, комутатори тощо) виявляються значно дешевші аналогічних обладнань інших мережних архітектур. В Ethernet можна використовувати практично будь-які види кабелю, а застосування оптоволокна дозволяє об'єднувати ділянки мереж, розташовані далеко друг від друга. Нарешті, сумісність різних варіантів Ethernet дуже висока, що дозволяє не лише нарощувати потужності мережі з використанням існуючої кабельної інфраструктури, а й легко розширювати мережу, підключаючи до неї нові, більш швидкісні сегменти. Тому сьогодні архітектура Ethernet переважає в локальних мережах і витісняє інші технології в регіональних і глобальних мережах.

## **Бездротові мережі**

Перейдемо тепер до бездротових мережевих рішень, з яких у локальних мережах зараз найбільше часто застосовуються технології Wi-Fi та Bluetooth.

Wi-Fi (скорочення від «Wireless Fidelity», «бездротова точність») – популярна у світі технологія й швидко розбудовується в Україні, що забезпечує бездротове підключення мобільних користувачів до локальної мережі й Інтернету (див. рис. 2.6).

Під іменем «Wi-Fi» насправді ховається кілька стандартів, розроблених для бездротових мереж на основі випущеної ще в 1997 р. специфікації IEEE 802.11 (див. табл. 2.3).



Рис. 2.6. Підключення користувачів до локальної мережі й Інтернету за допомогою технології Wi-Fi

Важливо відзначити, що в стандарті 802.11 передбачається використання тільки напівдуплексних приємопередавачі, які не можуть одночасно передавати та приймати інформацію. Через це в бездротових мережах 802.11 станція в принципі не може виявити зіткнення під час передачі (оскільки в цей час не має можливості ухвалювати дані). Тому в якості методу доступу до середовища у всіх стандартах використовується метод CSMA/CA (із запобіганням колізій), що дозволяє уникати зіткнень. Це призводить до додаткових складнощів при взаємодії й, як наслідок, до істотно менших швидкостей передачі даних, ніж, наприклад, у технології Ethernet.

## Wireless USB – альтернатива Bluetooth



Технологія Wireless USB заснована на використанні нового стандарту ультраширокопasmового бездротовому зв'язку – UWB і забезпечує супершвидкісну (до 480 Мбіт/з, а в перспективі – і до 1 Гбіт/с) передачу даних на короткі відстані (до 10 м). Вона дозволяє реалізувати бездротове підключення периферійних пристроїв, аналогічне USB 2.0.

Перший серійний зразок адаптер Wireless USB був представлений на Форумі Intel для розробників (IDF-2005).

Основним недоліком мереж Wi-Fi на сьогодні є досить мала дальність передачі даних, що не перевищує для більшості обладнань 150 м (максимум 300 м) на відкритому просторі або всього декількох десятків метрів – у приміщенні.

Таблиця 2.3

### Найбільш важливі стандарти IEEE 802.11x

Стандарт	Середовище передавання	Швидкість передавання, Мбіт/с	Примітка
802.11	радіосигнал із частотою близько 2,4 ГГц або ІК-Сигнал	1 або 2	Базовий стандарт, що визначає взаємодію на фізичному й каналному рівнях моделі OSI
802.11a	радіосигнал із частотою близько 5 ГГц	до 54	Несумісний на фізичному рівні зі стандартами 802.11b і g; в Україні не використовується
802.11b	радіосигнал із частотою 2,4-2,483 ГГц	до 11	Має відносно низьку швидкість та захищеність (захист шифруванням за технологією WEP – Wireless Equivalent Privacy). Забезпечує трохи більшу, порівняно з іншими стандартами, дальність передавання даних
802.11g	радіосигнал із частотою 2,4-2,483 ГГц	до 54	Забезпечує зворотну сумісність зі стандартом 802.11b, але характеризується більшою швидкістю й захищеністю (крім WEP, підтримується стандарт захисту WPA – Wi-Fi Protected Access)



Вирішенням зазначеної проблеми може стати архітектура WiMAX (Worldwide Interoperability for Microwave Access), що розроблюється в межах робочої групи IEEE 802.16. Реалізація цієї технології, також використовує радіосигнали в якості середовища передачі, дозволить надати користувачам швидкісний бездротовий доступ на відстанях до декількох десятків кілометрів (див. рис. 2.7).

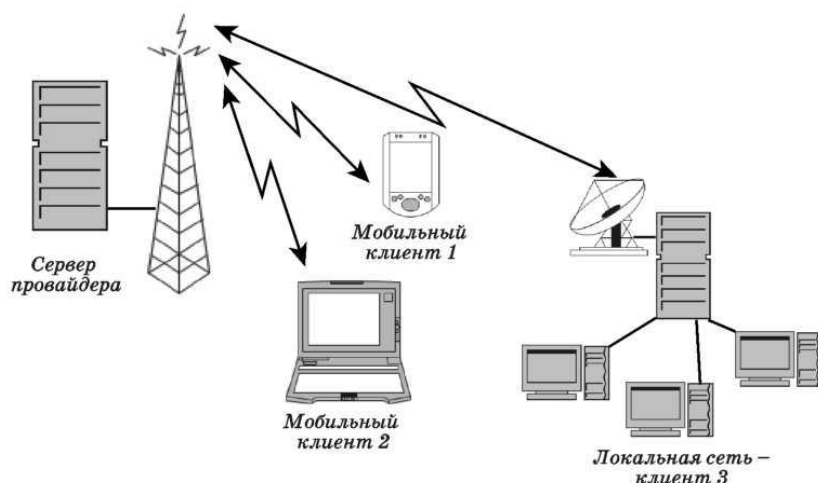


Рис. 2.7. Приклад використання архітектури WiMAX

Нарешті, варто згадати ще про одну з популярних сьогодні бездротових архітектур – про технологію Bluetooth (стандарт IEEE 802.15.1), а також про зовсім нову технологію Zigbee.

Як і в Wi-Fi, в Bluetooth використовується радіосигнал із частотою 2,4 ГГц, однак ці стандарти між собою несумісні. Bluetooth характеризується досить низьким енергоспоживанням, що дозволяє з успіхом застосовувати цю технологію в переносних пристроях – ноутбуках, КПК і мобільних телефонах (див. рис. 2.8). До того ж Bluetooth практично не вимагає налаштування – цей стандарт дозволяє пристроям установлювати взаємодію при мінімальній участі користувача. З іншого боку, в Bluetooth досить низькі показники за дальністю передачі й пропускною здатністю – не більш 10 метрів і 400-700 Кбіт/з, – що різко обмежує можливості використання цієї технології в локальних мережах.

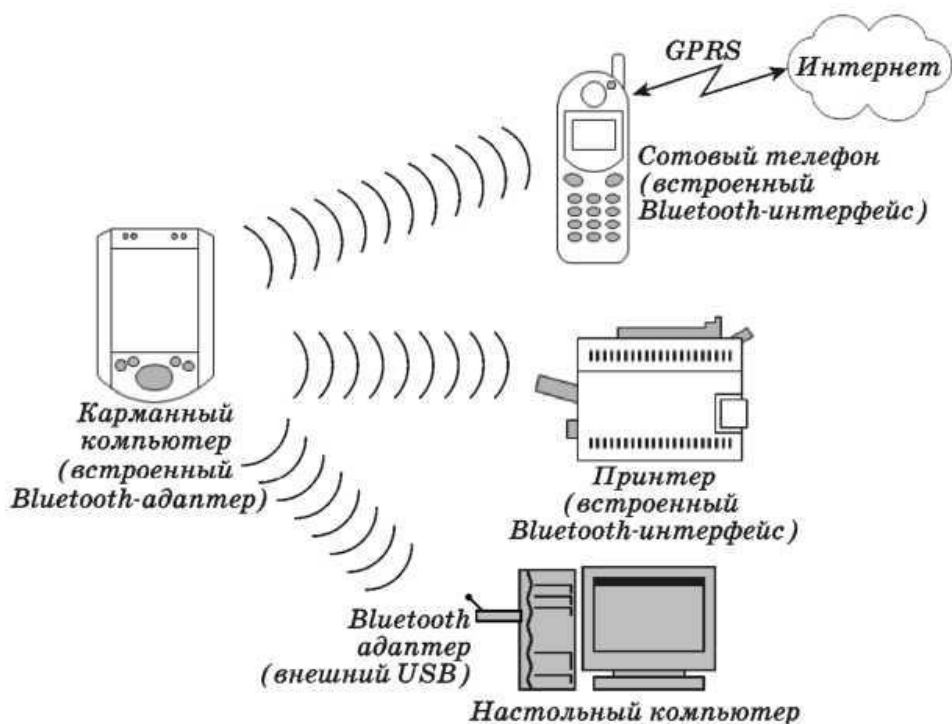


Рис. 2.8. Приклад підключення переносних пристроїв за допомогою архітектури Bluetooth

У технології Zigbee, що з'явився недавно завдяки зусиллям декількох великих комунікаційних компаній (стандарт 802.15.4), показники ще «скромніше» – її специфікація передбачає захищену передачу даних у радіусі 10-75 метрів і з максимальною швидкістю до 250 Кбіт/с. Здавалося б, навіщо вона потрібна, якщо швидкості передачі в ній ще нижче, ніж для Bluetooth. Проте «родзинкою» пристроїв Zigbee є їхнє наднизьке споживання енергії й здатність переходити в «сплячий режим», коли передача даних не потрібна. Тому основною сферою використання Zigbee-пристроїв стануть не локальні мережі, а системи моніторингу й контролю апаратури, у тому числі мережевого обладнання.

Основною технологією, яка використовується сьогодні в провідних мережах, є Ethernet. Важливо лише визначити конкретний стандарт або набір стандартів, які використовуються в мережі, і закупити потрібне обладнання. При цьому рекомендації досить прості: намагайтеся вибрати найбільш швидкісне й надійне обладнання, що задовольняє вас за ціною. Бажане, щоб це

обладнання було максимально функціональним і керованим, проте ці критерії більш значущі для мережевих адміністраторів великих корпоративних мереж.

Для підключення бездротових клієнтів слід зупинитися на технології Wi-Fi, причому вибирати потрібно пристрої, що підтримують останній стандарт 802.11g – тільки в ньому забезпечується достатня швидкість передачі даних і, найголовніше, їх надійний захист.

### **Запитання для перевірки знань**

1. Поясніть у чому полягає відмінність між фізичними і логічними зв'язками?
2. Перелічіть базові мережеві типології.
3. Назвіть переваги та недоліки конфігурації «зірка»? У яких локальних мережах вона застосовується?
4. Назвіть переваги та недоліки топології «кільце»? У яких локальних мережах вона застосовується?
5. Назвіть переваги та недоліки конфігурації «шина»? У яких локальних мережах вона застосовується?
6. Які гібридні топології вам відомі?
7. Які фактори необхідно враховувати при плануванні мережі?
8. Які ви знаєте мережеві архітектури? Які їх переваги та недоліки?
9. Чому архітектура Ethernet сьогодні набула найбільшого поширення?
10. Які ви знаєте різновиди архітектури Ethernet? Чим вони відрізняються?
11. Які ви знаєте бездротові мережні технології?
12. Які мережеві технології, на ваш погляд, краще всього використовувати:
  - при створенні локальної мережі у великому офісі?
  - при розгортанні домашньої мережі у міській квартирі (з телефоном)?
  - при розгортанні домашньої мережі в сільській хаті (телефон відсутній)?

- при об'єднанні в мережу мобільних комп'ютерів на території торгового центру або складу?
- при організації систем збору даних в польових умовах на території селища у сільській місцевості?

## **ЛЕКЦІЯ 3.**

### **Тема. Стеки протоколів і методи маршрутизації**

**Мета:** Ознайомити здобувачів вищої освіти з поняттям стек протоколів, з існуючими стеками, а також з найпоширенішим стеком TCP/IP, адресацією в мережі Інтернет і методами маршрутизації.

#### **План**

1. Вибір стека протоколів.
2. Основи IP-адресації.
3. Основи IP-маршрутизації.
4. Призначення IP-адрес і перевірка працездатності TCP/IP.

### **3.1. Вибір стека протоколів**

На цій лекції ми дізнаємося про деякі найбільш часто застосовувані в мережах стеки протоколів, в тому числі найпоширеніший на сьогодні набір протоколів – стек TCP/IP.

#### **NetBEUI**

Невеликий за обсягами необхідного програмного забезпечення протокол, який реалізує підтримку мережевого, транспортного та сеансового рівнів моделі OSI. Найбільш простий в налаштуванні (фактично його не вимагає), працює ефективно і швидко у невеликих і середніх за розмірами мережах (до 200 комп'ютерів). Серйозними, за сучасними мірками, недоліками протоколу NetBEUI є обмеження при роботі в мережах з великою кількістю комп'ютерів і, найголовніше, відсутність підтримки маршрутизації – можливості мережевої адресації та функції пересилання пакетів між мережами в ньому просто не

реалізовані. Відповідно, його не можна використовувати у великих мережах, об'єднаних маршрутизаторами, та при роботі з Інтернетом. Протокол NetBEUI поставлявся у складі всіх операційних систем Windows аж до Windows 2000, однак в останніх версіях його підтримка припинена.

Абревіатура NetBEUI розшифровується як «NetBIOS Extended User Interface» – «поліпшена версія протоколу NetBIOS».

### **IPX/SPX і Nwlink**

Стек протоколів IPX/SPX був розроблений фірмою Novell на початку 80-х рр. XX ст. для своєї мережевої операційної системи NetWare. Основа стека – це протоколи IPX (Internetwork Packet eXchange) та SPX (Sequenced Packet eXchange), що реалізують функції мережевого та транспортного рівнів моделі OSI відповідно. Як і NetBEUI, протокол IPX/SPX є невеликим (його програмну підтримку легко вмістити на звичайній дискеті 1,44 Мб разом з DOS) і швидким, що було особливо важливо в епоху першого покоління ІВМ-сумісних комп'ютерів з малим об'ємом оперативної пам'яті (640 Кбайт). Крім того, в стеці IPX/SPX підтримується маршрутизація. Обидва ці фактори, поряд з надійністю серверів на базі операційної системи Novell Netware тих років, сприяли широкому розповсюдженню стека IPX/SPX у локальних мережах у 80-і та 90-і рр. XX ст. До недоліків цього стека протоколів слід віднести інтенсивне використання широкомовних повідомлень, серйозно навантажують мережу, особливо при роботі з повільними глобальним каналам. Ця обставина, а також те, що стек IPX/SPX належить фірмі Novell та для його реалізації іншим виробникам мережевих операційних систем доводилося купувати ліцензію, привели у підсумку до витіснення IPX/SPX загальнодоступним стеком TCP/IP. Важливу роль тут зіграло і те, що все більше організацій в 90-і рр. XX ст. стали підключатися до Інтернету, в якому використовувався саме стек TCP/IP, а підтримувати в мережі два стека протоколів – зайвий «головний біль» для мережевих адміністраторів.

NWLink – реалізація стека IPX/SPX компанією Microsoft, що поставляється в усіх версіях Windows.

## **TCP/IP**

Історія розвитку стеку TCP/IP (як і історія Інтернету) почалася ще в кінці 60-х рр. XX століття з проекту ARPANet – мережі Агентства перспективних дослідницьких проєктів (Advanced Research Project Agency Network) Міністерства оборони США. Оскільки для військових за часів «холодної війни» була особливо важлива можливість передавання даних навіть в умовах атомних бомбардувань, ARPANet замислювалася як високонадійна мережа, яка об'єднує військові, державні та наукові установи. Отримана в результаті мережа і розроблений дещо пізніше (в 70-х рр. XX століття) стек протоколів TCP/IP виявилися настільки вдалим, що навіть після припинення фінансування проєкту ARPANet Міністерством оборони продовжували жити і успішно розвиватися, створивши основи сучасного Інтернету.

Основні переваги стеку TCP/IP перед іншими (наприклад, перед стеком IPX/SPX) – більш зручна система мережевої адресації, можливість фрагментації пакетів і дуже невелика кількість ширококомовних повідомлень. Ці переваги виявилися вирішальними не тільки при побудові глобальних мереж, що об'єднують мережі з різнорідними архітектурами, але й при створенні великих корпоративних мереж. У результаті сьогодні стек TCP/IP практично витіснив всі інші – він використовується і в невеликих домашніх мережах, і в глобальній мережі Інтернет.

Оскільки стек TCP/IP є загальнодоступним, його стандарти (а також просто інформаційні матеріали) публікуються в Інтернеті у вигляді спеціальних документів під назвою «RFC» («Request for Comments», «запит коментарів») з послідовно зростаючим номером. Як приклад, специфікація протоколу IP опублікована в RFC 791, а протоколу HTTP версії 1.1 – в RFC 2616. Перший документ RFC був представлений ще у квітні 1969 р., а зараз поточні номери RFC перевалили за 4 тисячі.

Стек TCP/IP, на відміну від семирівневої моделі OSI, прийнято описувати в рамках чотирьох рівнів (див. рис. 3.1).

## Потік даних

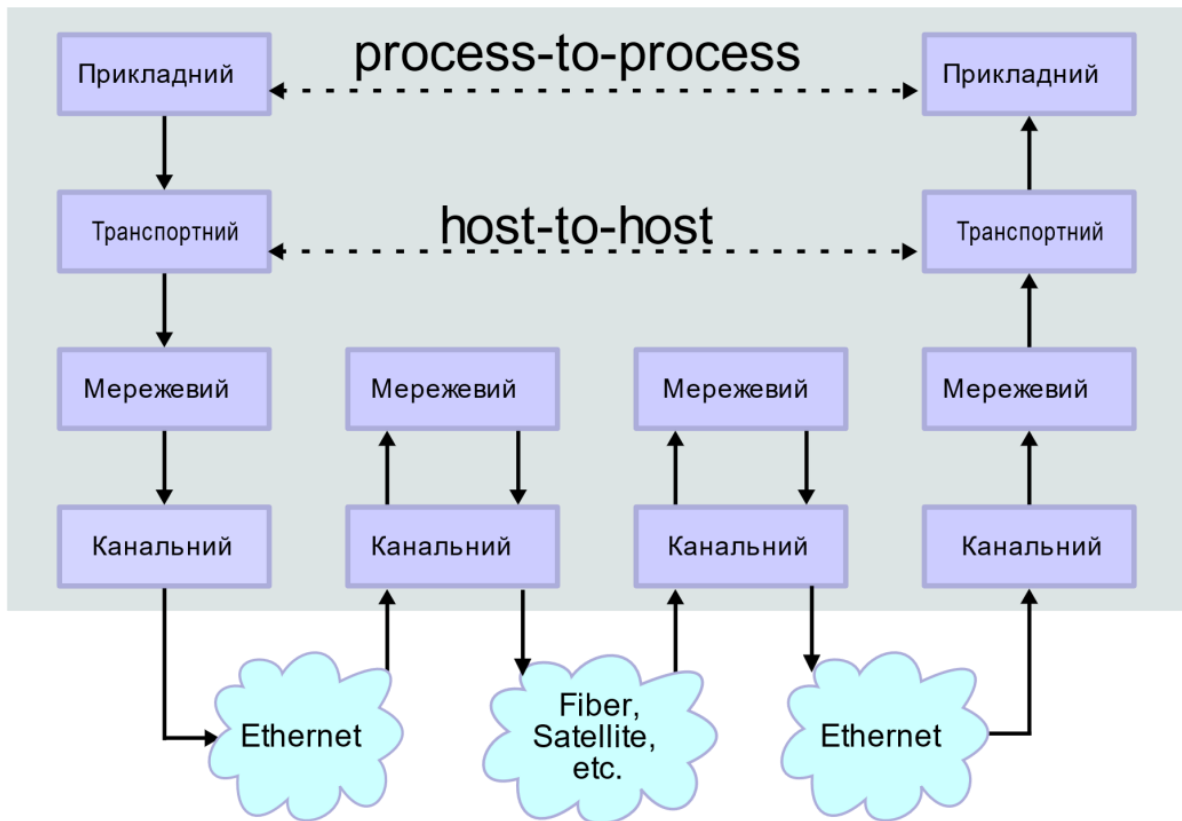


Рис. 3.1. Структура стеку TCP/IP

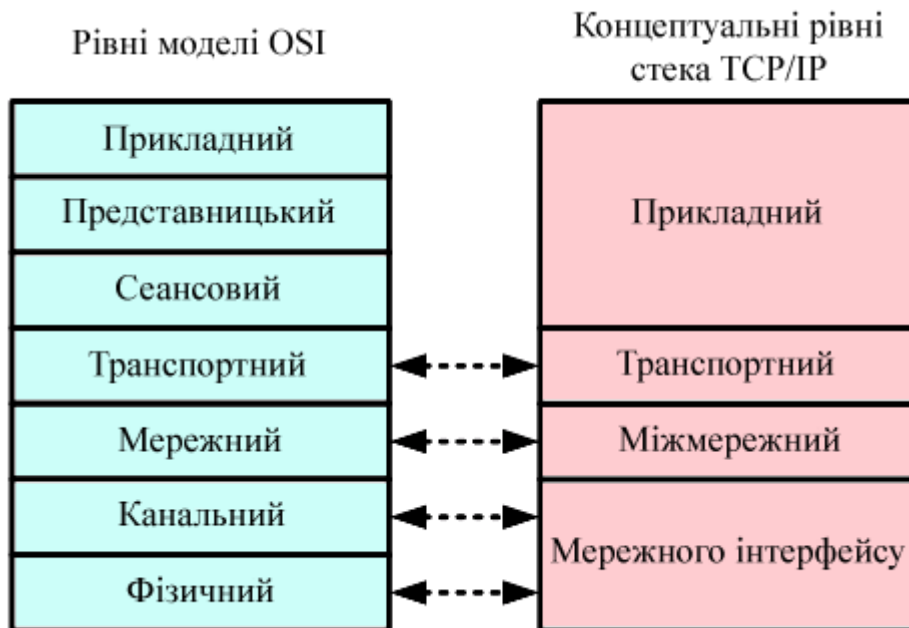


Рис. 3.2. Порівняння Моделі OSI та стеку TCP/IP

## Характеристика рівнів і протоколів стека TCP/IP

На фізичному рівні TCP/IP підтримує роботу з основними технологіями локальних мереж – Ethernet, Token Ring, Wi-Fi, Bluetooth та ін.

На мережевому рівні розташовуються декілька протоколів:

- протокол ARP (Address Resolution Protocol) є ланкою, що пов'язує мережевий рівень із фізичним. Він відповідає за перетворення мережевих IP-адрес в апаратні MAC-адреси;



За допомогою команди **ARP-A** можна перевірити IP-адреси комп'ютерів вашої мережі, що були останнім часом перетворені у відповідні їм MAC-адреси

- протокол RARP (Reverse Address Resolution Protocol) – здійснює зворотне перетворення MAC-адрес в IP-адреси (в операційних системах Windows підтримка протоколу RARP не передбачена);

- протокол ICMP (Internet Control Message Protocol) – використовується для передавання повідомлень про помилки, діагностики доступності мережевого вузла й маршруту доставки пакетів (саме його використовують такі популярні утиліти, як *PING* і *TRACERT*);

- протокол IGMP (Internet Group Management Protocol) – використовується для управління групами комп'ютерів, наприклад, при передаванні в мережах потокового відео й звуку, коли для зниження навантаження на мережу пакет посилає за спеціальним адресом відразу декільком комп'ютерам (багатоадресне розсилання);


- протокол IP (Internet Protocol) – один з найважливіших у стеці TCP/IP. Як випливає з його назви («IP» переводиться як «міжмережевий протокол»), він відповідає за доставку IP-дейтаграм (так правильно називаються пакети на рівні протоколу IP), забезпечуючи передачу пакета з однієї мережі в іншу. Про те, як це відбувається детально розглянемо далі.

На транспортному рівні працюють два протоколи:



– протокол TCP (Transmission Control Protocol, протокол управління передачею) – основний протокол транспортного рівня. Забезпечує установку з'єднання між відправником і одержувачем, розбиття великого блоку інформації (наприклад, файлу) на невеликі TCP-пакети і їхню гарантовану доставку одержувачу (у потрібному порядку й без помилок). Відповідно, протокол TCP використовується в тих додатках, де важливо забезпечити цілісність при передаванні даних;

– протокол UDP (User Datagram Protocol), на відміну від TCP, не встановлює з'єднання перед передачею інформації й не забезпечує надійної доставки даних, працюючи при цьому швидше, чим TCP. Його використовують там, де забезпечення доставки інформації не дуже важливо в порівнянні зі швидкістю передавання (контроль над цілісністю даних у цьому випадку покладається на, що використовує протокол UDP додаток).

 Щоб краще уявити собі роботу протоколів TCP і UDP, повернемося до нашої аналогії з поштою. Нехай нам треба переслати у видавництво цілий роман, а в конверт дозволяється вкладати не більше декількох сторінок тексту. Щоб у такій ситуації нічого не втратити під час пересилання й не переплутати при прийомі рукопису до друку, спочатку добре б домовитися з видавництвом про системи позначення саме для вашого роману (адже є й інші автори!) і про нумерацію повідомлень. Для цього потрібно надіслати листа, що сповіщає видавництво про наш намір переслати роман, у якому вказати вихідний номер вашого наступного повідомлення. Видавництво підтвердить одержання вашого повідомлення й у відповідному листі повідомить вам свої вихідні й вхідні номери, а ви підтвердите одержання цих номерів. Таким чином, обидві сторони узгодять номери повідомлень, які вони пізніше будуть очікувати один від одного, що й означає встановлення зв'язку. Далі вам залишається тільки розділити роман на невеликі частини й посилати кожна в окремому листі, а видавництву – підтверджувати одержання цих частин. Помилки роботи пошти (якщо якийсь повідомлення не дійде до видавництва

через втрату або ушкодження листа або прийде позачергово) легко визначити за вхідними і вихідними номерами, щоб вжити відповідних заходів – заново переслати загублену частину або зібрати сторінки роману в потрібному порядку.

Приблизно так само працює й протокол TCP:

- зупиняє з'єднання між комп'ютерами за певними портами;
- на комп'ютері-відправнику розбиває інформацію на пакети, нумерує їх і за допомогою протоколу IP передає одержувачу;
- на комп'ютері-одержувачі перевіряє, чи всі пакети отримані, а якщо пакет пропущений або ушкоджений, запитує у відправника повторне пересилання;
- після одержання всіх пакетів закриває з'єднання, збирає пакети в потрібному порядку й передає отримані дані додатку більш високого рівня.

Протокол UDP у цій аналогії можна зрівняти з розсиланням рекламних повідомлень. Ніякого встановлення зв'язку й підтвердження отримання кореспонденції тут немає – листи з рекламною інформацією просто кидають у вашу поштову скриньку. При цьому ні відправника, ні одержувача надійність доставки інформації або її цілісність не дуже турбують.

Очевидно, поштові відправлення в обох цих прикладах є аналогами IP-пакетів, а листоноші виконують функції протоколу IP.



**Порт в TCP або UDP** – це логічний канал з певним номером (від 0 до 65536), що забезпечує поточне взаємодію між відправником і одержувачем

Порти дозволяють комп'ютеру з однією IP-адресою паралельно обмінюватися даними з безліччю інших комп'ютерів. Деякі номери портів (так звані «добре відомі», або «well-known», порти з номерами від 0 до 1024) прив'язані до певних служб і додатків, що дозволяє клієнтам легко звертатися до потрібних їх мережевих сервісів.

Нарешті, найбагатшим за набором протоколів є прикладний рівень стеку TCP/IP. Нижче в табл. 3.1 наведені найпопулярніші протоколи, а також зарезервовані для них порти. Помітимо, що, хоча для протоколів звичайно резервуються однакові номери портів і для TCP, і для UDP, у таблиці наведені порти для найбільш часто застосовуваного протоколу транспортного рівня (TCP або UDP).

Незважаючи на існування великої кількості наборів протоколів, основним сьогодні є загальнодоступний стек TCP/IP. Він використовується практично повсюдно, починаючи з невеликих домашніх мереж і закінчуючи найбільшою мережею – Інтернетом.

Таблиця 3.1

### Протоколи прикладного рівня стека TCP/IP

Протокол	Призначення	Номер порту
NTP (Network Time Protocol)	Протокол мережевого часу, використовується для синхронізації системних годин комп'ютерів у мережах	123 (UDP)
DNS (Domain Name System, або Service)	Служба доменних імен, використовується для перетворення (дозволу) зрозумілих людям імен комп'ютерів (наприклад, імен типу <a href="http://www.microsoft.com">www.microsoft.com</a> ) в IP-адреси	53 (TCP і UDP)
NetBIOS name service і WINS (Windows Internet Naming Service)	Служба імен NetBIOS і служба міжмережєвих імен Windows, використовуються для перетворення NetBIOS-імен комп'ютерів (наприклад, імен типу SERVER) в IP-адреси	137 і 138 (UDP)
NetBIOS session service	Служба сеансів NetBIOS, використовується для встановлення сеансів між комп'ютерами	139 (TCP)
LDAP (Lightweight Directory Access Protocol)	Простий протокол доступу до каталогу, використовується для роботи з різними мережевими каталогами (наприклад, зі службою Active Directory у доменах на основі Windows Server 2003)	389 (TCP)
RPC (Remote Procedure Call)	Виклик віддаленої процедури, використовується для роботи з багатьма мережевими службами в мережах Майкрософт	135 (TCP)
Telnet	Протокол для забезпечення термінального доступу до віддалених комп'ютерів	23 (TCP)

Протокол	Призначення	Номер порту
FTP (File Transfer Protocol)	Протокол передавання файлів, один з «найстаріших» протоколів Інтернету; використовується для ефективного й надійного передавання файлів між клієнтом і сервером FTP	20 і 21 (TCP)
TFTP (Trivial File Transfer Protocol)	Спрощений варіант FTP, не має таких функцій, як перевірка користувача при вході, перегляд каталогів і файлів сервера; використовується тільки для запису й читання файлів	69 (UDP)
Gopher	Протокол Gopher («ховрашок»), використовується для доступу до текстових інформаційних ресурсів на вилученому сервері	70 (TCP)
HTTP (HyperText Transfer Protocol)	Протокол передачі гіпертексту, самий популярний сьогодні протокол, що використовується у Всесвітній павутині (World Wide Web); описує, яким способом потрібно представляти дані (текстові, аудіо-, відео- та ін.) на веб-серверах, як до них звертатися за допомогою веб-браузера (наприклад, програми Internet Explorer) і як передавати ці дані	80 (TCP)
NNTP (Network News Transfer Protocol)	Протокол передавання мережевих новин, використовується для обміну повідомленнями в системах телеконференцій	119 (TCP)
SMTP (Simple Mail Transfer Protocol)	Простий протокол передавання пошти, використовується поштовими серверами для обміну електронними повідомленнями (на етапі відправлення поштового повідомлення його автором)	25 (TCP)
POP3 (Post Office Protocol)	«Протокол поштової відділення», досить простий протокол, що використовується поштовим клієнтом (наприклад, програмою Outlook Express) для підключення до своєї поштової скриньки на сервері й зчитування повідомлень (на етапі доставки поштового повідомлення адресатові)	110 (TCP)
IMAP4 (Internet Message Access Protocol)	Протокол доступу до електронних повідомлень – більш функціональний, ніж POP3, клієнтський протокол для доступу до поштового сервера	143 (TCP)
SSL (Secure Sockets Layer)	Протокол, що забезпечує узгодження алгоритмів і обмін ключами шифрування. Використовується для захисту даних при їхньому пересиланні по мережах	25 (SMTP) 995 (POP3S) 993 (IMAPS) 443 (HTTPS) (TCP)



Щоб подивитися, які порти на вашому комп'ютері використовуються або очікують підключення, досить виконати команду **NETSTAT – AN**.

На фізичному рівні стек TCP/IP підтримує роботу з усіма основними мережевими технологіями локальних і глобальних мереж, на мережевому – забезпечує логічну систему адресації й ефективної міжмережевої маршрутизації, на транспортному рівні – протоколи як гарантованої, так і швидкої доставки даних, а на рівні додатків – цілу гаму різноманітних протоколів.

Тому ми рекомендуємо використовувати в мережі саме стек TCP/IP.

### 3.2. Основи IP-адресації

Стек не запрацює, поки в комп'ютерній мережі не буде правильним чином налаштована IP-адресація й маршрутизація.

Тому, зосередимо увагу на тому, що таке IP-адреса й маска підмережі, з'ясуємо, як обидва цих параметра використовуються для визначення локальних або віддалених IP-мереж, і на конкретних прикладах ознайомимося з тим, як комп'ютери й маршрутизатори доставляють IP-пакети з однієї мережі в іншу.

Першим обов'язковим параметром у властивостях протоколу TCP/IP будь-якого комп'ютера є його IP-адреса.



**IP-адреса** – це унікальна 32-розрядна послідовність двійкових цифр, за допомогою якої комп'ютер *однозначно ідентифікується* в IP-мережі. (Нагадаємо, що на каналному рівні в ролі таких же унікальних адрес комп'ютерів виступають MAC-адреси мережевих адаптерів, неможливість збігу яких контролюється на стадії виробництва).

Основну увагу зосередимо на версія 4 протоколу IP, або IPv4. Однак уже створена наступна версія протоколу – IP версії 6 (IPv6), у якій IP-адреса представляється у вигляді 128-бітної послідовності двійкових цифр. Ця версія

протоколу IP поки ще не одержала широкого розповсюдження, хоча й підтримується багатьма сучасними маршрутизаторами й операційними системами (наприклад, Windows або Windows Server).



**IPv6** Багато країни, що активно розвиваються в технічному відношенні (Китай, Японія, Корея та ін.) починають відчувати дефіцит IP-адрес, що ідентифікують не тільки комп'ютери, але й інші пристрої з функціями доступу до Інтернет. Ухвалений зараз 32-бітовий стандарт забезпечує кількість IP-адрес, який становить майже 4,3 млрд., але їхня більшість закріплена за США (близько 70%), Канадою і європейськими країнами, а от, наприклад, КНР одержала їх усього 22 млн.

Нова, 128-розрядна версія протоколу IP v.6 дозволить збільшити кількість IP-адрес до величезної величини –  $3,4 \times 10^{38}$ .

Для зручності роботи з IP-адресами 32-розрядну послідовність зазвичай розділяють на 4 частини по 8 бітів (на октети), кожний октет переводять у десяткове число й при записі поділяють ці числа крапками. У такому вигляді (це подання називається «десяткові числа із крапками» (з англійської «dotted–decimal notation») IP-адреси займають значно менше місця й набагато легше запам'ятовуються (див. табл. 3.2).

Таблиця 3.2

### Різні уявлення IP-адреси

IP адреса у 32 розрядному коді	11000000 10101000 0000101 11001000				
IP адреса, яка розбита на октети	<table border="1" style="display: inline-table; vertical-align: middle;"> <tr> <td style="text-align: center;">11000000</td> <td style="text-align: center;">10101000</td> <td style="text-align: center;">0000101</td> <td style="text-align: center;">11001000</td> </tr> </table>	11000000	10101000	0000101	11001000
11000000	10101000	0000101	11001000		
Октети у десятковому представленні	<table border="1" style="display: inline-table; vertical-align: middle;"> <tr> <td style="text-align: center;">192</td> <td style="text-align: center;">168</td> <td style="text-align: center;">5</td> <td style="text-align: center;">200</td> </tr> </table>	192	168	5	200
192	168	5	200		
IP адреса у вигляді у десяткових чисел, розділених крапками	192.168.5.200				

Щоб швидко рахувати в пам'яті, корисно запам'ятати наступну таблицю. У ній наведені десяткові значення ступенів числа 2 з показником, рівним

порядковому номеру біта в октеті (нагадаємо – нумерація бітів виробляється справа наліво і починається з нуля):

Порядковий номер біта в октеті	7	6	5	4	3	2	1	0
2 у ступені, відповідної до номера біта	128	64	32	16	8	4	2	1

Запам'ятавши таку таблицю, нескладно в пам'яті перетворювати октети в десяткові числа й назад.

Десяткове число легко обчислюється як сума цифр, відповідних ненульовим бітам в октеті, наприклад:

$$10101101 \rightarrow 128 \cdot 1 + 64 \cdot 0 + 32 \cdot 1 + 16 \cdot 0 + 8 \cdot 1 + 4 \cdot 1 + 2 \cdot 0 + 1 \cdot 1 = 173.$$

Дещо складніше перевести десяткове число у двійкове, але при деякому тренуванні це також не представить проблем. Наприклад:

$$201 \rightarrow 128 \cdot 1 + 64 \cdot 1 + 32 \cdot 0 + 16 \cdot 0 + 8 \cdot 1 + 4 \cdot 0 + 2 \cdot 0 + 1 \cdot 1 = 11001001.$$

Однак однієї лише IP-адреси комп'ютеру для роботи в мережі TCP/IP недостатньо. Іншим обов'язковим параметром, без якого протокол TCP/IP працювати не буде, є маска під мережі.



**Маска підмережі** – це 32-розрядне число, що складається з одиниць, які йдуть спочатку, а потім – нулів, наприклад (у десятковому поданні).

**255.255.255.0 або 255.255.240.0.**

Маска підмережі грає винятково важливу роль в IP-адресації й маршрутизації. Щоб зрозуміти значення цього параметра, згадаємо, що мережа ARPANet будувалася як набір з'єднаних один з одним гетерогенних мереж. Для правильної взаємодії в такій складній мережі кожен учасник повинен уміти визначати, які IP-адреси належать його локальній мережі, а які – віддаленим мережам.

Тут і використовується маска підмережі, за допомогою якої проводиться поділ будь-якої IP-адреси на дві частини: ідентифікатор мережі (Net ID) і

ідентифікатор вузла (Host ID). Такий поділ робиться дуже просто: там, де в масці підмережі стоять одиниці, знаходиться ідентифікатор мережі, а де стоять нулі – ідентифікатор вузла.

Наприклад, в IP-адресі 192.168.5.200 при використанні маски підмережі 255.255.255.0 ідентифікатором мережі буде число 192.168.5.0, а ідентифікатором вузла – число 200. Варто нам поміняти маску підмережі, скажімо, на число 255.255.0.0, як і ідентифікатор вузла, і ідентифікатор мережі зміняться на 192.168.0.0 і 5.200, відповідно, і від цього, як ми далі побачимо, інакше буде поводитися комп'ютер при посиланні IP-пакетів.

### **Правила призначення IP-адрес мереж і вузлів**

Тепер, коли ми знаємо, що таке IP-адреса, маска підмережі, ідентифікатори мережі й вузла, корисно запам'ятати правила, які слід застосовувати при призначенні цих параметрів:

- 1) ідентифікатор мережі не може містити тільки двійкові нулі або тільки одиниці. Наприклад, адреса 0.0.0.0 не може бути ідентифікатором мережі;
- 2) ідентифікатор вузла також не може містити тільки двійкові нулі або лише одиниці – такі адреси зарезервовані для спеціальних цілей:
  - усі нулі в ідентифікаторі вузла означають, що ця адреса є адресою мережі. Наприклад, 192.168.5.0 є правильною адресою мережі при використанні маски 255.255.255.0 і її не можна використовувати для адресації комп'ютерів;
  - усі одиниці в ідентифікаторі вузла означають, що ця адреса є адресою ширококомовлення для даної мережі. Наприклад, 192.168.5.255 є адресою ширококомовлення в мережі 192.168.5.0 при використанні маски 255.255.255.0 і її не можна використовувати для адресації комп'ютерів;
- 3) ідентифікатор вузла в межах однієї й тієї ж підмережі повинен бути унікальним;



4) діапазон адрес від 127.0.0.1 до 127.255.255.254 не можна використовувати в якості IP-адрес комп'ютерів. Уся мережа 127.0.0.0 за маскою 255.0.0.0 зарезервована під так званий «адресу заглушки» (loopback), що використовується в IP для звернення комп'ютера до самого себе.

Це легко перевірити: досить на будь-якому комп'ютері зі встановленим протоколом TCP/IP виконати команду

PING 127.12.34.56

і, якщо протокол TCP/IP працює, ви побачите, як ваш комп'ютер буде відповідати на власні запити.

### Класова й безкласова IP-адресація

Первісна система IP-адресації в Інтернеті виглядала наступним чином. Увесь простір можливих IP-адрес (а це більш чотирьох мільярдів, точніше 4 294 967 296 адрес) було розбито на п'ять класів, причому приналежність IP-адреси до певного класу визначалася за кількома бітами першого октету (див. табл. 3.3). Зауважимо, що для адресації мереж і вузлів використовувалися тільки класи А, В і С. Крім того, для цих мереж були визначені фіксовані маски підмережі за замовчуванням, які становлять, відповідно, 255.0.0.0, 255.255.0.0 і 255.255.255.0, які не тільки жорстко визначали діапазон можливих IP-адрес вузлів у таких мережах, але й механізм маршрутизації.

*Таблиця 3.3*

**Класи адрес у первісній схемі IP-адресації**

Клас	Перші біти в октеті	Можливі значення першого октету	Можливе число мереж	Можливе число вузлів у мережі
А	0	1–126	126	16777214
В	10	128–191	16384	65534
С	110	192–223	2097152	254
Д	1110	224–239	Використовується для багатоадресного розсилання (multicast)	
Е	1111	240–254	Зарезервований як експериментальний	

Розподілом IP-Адрес у світі займається приватна некомерційна корпорація під назвою ICANN (Internet Corporation for Assigned Names and Numbers), а точніше організація, що працює під її патронажем, IANA (Internet Assigned Numbers Authority).

Щоб розрахувати максимально можливу кількість вузлів у будь-якій IP-мережі, досить знати, скільки бітів міститься в ідентифікаторі вузла, або, інакше, скільки нулів є в масці підмережі. Це число використовується як показник ступеня двійки, а потім з результату віднімається дві зарезервовані адреси (мережі й широкомовлення). Аналогічним чином легко обчислити й можливу кількість мереж класів А, В або С, якщо врахувати, що перші біти в октеті вже зарезервовані, а в класі А не можна використовувати IP-адреси 0.0.0.0 і 127.0.0.0 для адресації мережі.

Для одержання потрібного діапазону IP-адрес організаціям пропонувалося заповнити реєстраційну форму, у якій слід було вказати поточне число комп'ютерів і плановане зростання комп'ютерного парку протягом двох років.

Спочатку ця схема добре працювала, оскільки кількість мереж була невеликою. Однак із розвитком Інтернету такий підхід до розподілу IP-адрес став викликати проблеми, особливо гострі для мереж класу В. Дійсно, організаціям, у яких кількість комп'ютерів не перевищувало декількох сотень (скажімо, 500), доводилося реєструвати для себе цілу мережу класу В. Тому кількість доступних мереж класу В стало на очах «танути», але при цьому величезні діапазони IP-адрес (у нашому прикладі – більш 65000) пропадали даремно.

Щоб вирішити проблему, була розроблена безкласова схема IP-адресації (Classless Interdomain Routing, CIDR), у якій не тільки відсутня прив'язка IP-адреси до класу мережі й маски підмережі за замовчуванням, але й допускається застосування так званих масок підмережі зі змінною довжиною (Variable Length Subnet Mask, VLSM). Наприклад, якщо при виділенні мережі для вищевказаної організації з 500 комп'ютерами замість фіксованої маски 255.255.0.0 використовувати маску 255.255.254.0, то отриманого діапазону з

512 можливих IP-адрес буде цілком достатньо. Решту 65 тисяч адрес можна зарезервувати на майбутнє або роздати іншим бажаючим підключитися до Інтернету.

Цей підхід дозволив ефективніше виділяти організаціям потрібні їм діапазони IP-адрес, і проблема з нестачею IP-мереж і адрес стала менш гострою.

### **IP-адреси для локальних мереж**

Усі використовувані в Інтернеті адреси, про як ми вже говорили, повинні реєструватися в IANA, що гарантує їхню унікальність у масштабі всієї планети. Такі адреси називають реальними, або публічними (public) IP-адресами.

Для локальних мереж, не підключених до Інтернету, реєстрація IP-адрес, природно, не потрібна, тому тут можна використовувати будь-які можливі адреси. Однак, щоб не допускати можливих конфліктів при подальшому підключенні такої мережі до Інтернету, RFC 1918 рекомендує застосовувати в локальних мережах тільки наступні діапазони так званих приватних (private) IP-адрес (в Інтернеті ці адреси не існують і використовувати їх там немає можливості):

- 10.0.0.0 – 10.255.255.255;
- 172.16.0.0 – 172.31.255.255;
- 192.168.0.0 – 192.168.255.255.

### **3.3. Основи IP-маршрутизації**

Як уже говорилося, щоб правильно взаємодіяти з іншими комп'ютерами й мережами, кожен комп'ютер визначає, які IP-адреси належать його локальній мережі, а які – віддаленим мережам. Якщо з'ясується, що IP-адреса комп'ютера призначення належить локальній мережі, пакет посилається безпосередньо комп'ютеру призначення, якщо ж це адреса віддаленої мережі, то пакет надсилається за адресою основного шлюзу.

Головним параметром маршрутизації є IP-адреса. У відповідності з протоколом IP вузли поділяються на маршрутизатори (routers) та хости або вузли (hosts).



**Хост** – це спільний термін, який описує програмно-апаратний комплекс, який містить ресурси (апаратні, програмні та інформаційні) і надає до них доступ.

Хости не розсилають таблиць маршрутизації, хоча й можуть мати програмне забезпечення для їх створення та для маршрутизації.

### **Алгоритм вибору маршруту**

Алгоритм вибору маршруту:

1. З пакету зчитується IP-адреса.
2. В IP-адресі виділяється адреса мережі призначення.
3. Якщо адреса мережі призначення відповідає даній локальній мережі, то пакет надсилається безпосередньо адресату.
4. Якщо вказана адреса є в таблиці маршрутизації, то пакет надсилається за відповідним маршрутом.
5. Якщо описаний маршрут за замовчуванням, то пакет надсилається за адресою за замовчуванням.
6. Якщо ні один із варіантів неможливий, то видається повідомлення про помилку маршрутизації.

Розглянемо цей процес докладніше. Візьмемо комп'ютер з наступними параметрами протоколу IP:

- IP-адреса – 192.168.5.200;
- маска підмережі – 255.255.255.0;
- основний шлюз – 192.168.5.1.

При запуску протоколу IP на комп'ютері виконується операція логічного «І – кон'юнкція» між його власною IP-адресою й маскою підмережі, у результаті якої всі біти IP-адреси, відповідні нульовим бітам маски підмережі, також стають нульовими:

- IP-адреса в 32-розрядному виді –

11000000 10101000 00000101 11001000;

- маска підмережі –

11111111 11111111 11111111 00000000;

- ідентифікатор мережі –

11000000 10101000 00000101 00000000.

Ця проста операція дозволяє комп'ютеру визначити ідентифікатор власної мережі (у нашому прикладі – 192.168.5.0).

Тепер припустимо, що комп'ютеру треба відправити IP-пакет за адресою 192.168.5.15. Щоб вирішити, як це потрібно зробити, комп'ютер виконує операцію логічного «І» з IP-адресою комп'ютера призначення й власної маскою підмережі. Легко зрозуміти, що отриманий у результаті ідентифікатор мережі призначення буде збігатися з ідентифікатором власної мережі комп'ютера-відправника. Так наш комп'ютер визначить, що комп'ютер призначення знаходиться в одній з ним мережі, і виконає наступні операції:

- за допомогою протоколу ARP буде визначено фізичну MAC-адресу, відповідну IP-адресі комп'ютера призначення;
- за допомогою протоколів канального й фізичного рівня з цієї MAC-адреси буде послана потрібна інформація.

Тепер подивимося, що зміниться, якщо пакет треба відправити за адресою 192.168.10.20. Комп'ютер виконає аналогічну процедуру визначення ідентифікатора мережі призначення. У результаті буде отримано адресу 192.168.10.0, що не збігається з ідентифікатором мережі комп'ютера-відправника. Так буде встановлено, що комп'ютер призначення знаходиться у віддаленій мережі, і алгоритм дій комп'ютера-відправника зміниться:

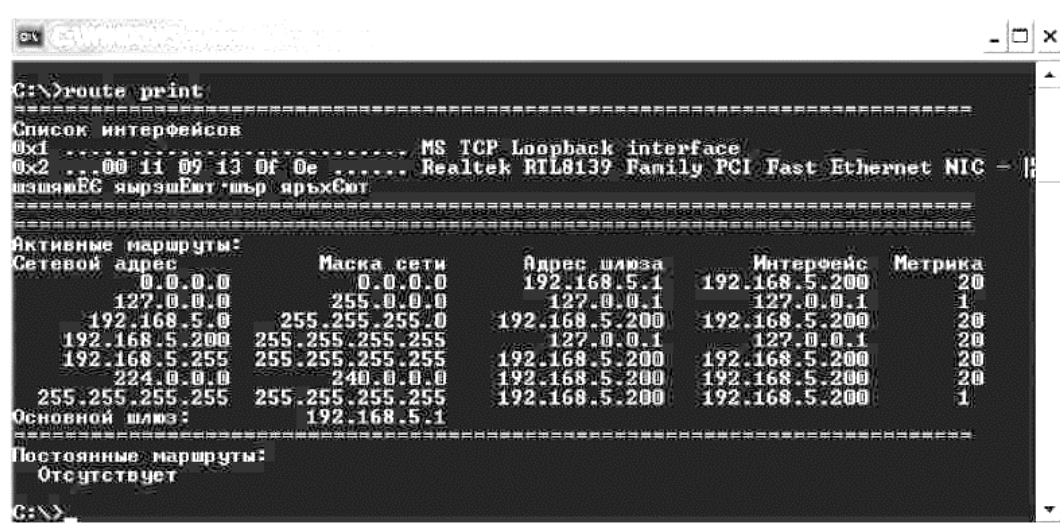
- буде визначена MAC-адреса не комп'ютера призначення, а маршрутизатора;
- за допомогою протоколів канального й фізичного рівня з цієї MAC-адреси на маршрутизатор буде послано потрібну інформацію.

Незважаючи на те, що IP-пакет у цьому випадку не доставляється безпосередньо за призначенням, протокол IP на комп'ютері-відправника вважає

своє завдання виконаним (згадаєте, що й ми при відправленні листа лише кидаємо його до поштової скриньки). Подальша доля IP-пакета залежить від правильного налаштування маршрутизаторів, що поєднують мережі 192.168.5.0 та 192.168.10.0.

До речі, у даному прикладі легко продемонструвати, наскільки важливе правильне налаштування маски підмережі в параметрах IP-адресації. Нехай ми помилково вказали для комп'ютера 192.168.5.200 маску підмережі, яка становить 255.255.0.0. У цьому випадку при спробі послати пакет за адресою 192.168.10.20 наш комп'ютер порахує, що комп'ютер призначення перебуває в його власній мережі (адже ідентифікатори мереж при такій масці збігаються!), і намагатиметься відправити пакет самостійно. У результаті цей пакет не потрапить у маршрутизатор і не буде доставлений за призначенням.

Щоб зрозуміти, як працюють маршрутизатори, давайте спочатку проаналізуємо таблицю маршрутів, яку вибудовує при завантаженні протоколу IP звичайний комп'ютер, наприклад, з операційною системою Windows (див. рис. 3.3). Для цього виберіть у меню Пуск пункт Виконати, уведіть у запропонованому полі команду `cmd` і клацніть мишею на кнопці ОК, а потім уведіть у рядку запрошення у вікні, що з'явилося, DOS-додатка команду `route print` і натисніть клавішу `Enter`.



```
C:\>route print
=====
Список интерфейсов
0x1 ..... MS TCP Loopback interface
0x2 .. 00 11 09 13 0f 0e ..... Realtek RTL8139 Family PCI Fast Ethernet NIC -
изъямЕС яврэмЕот шър ярхСот
=====
Активные маршруты:
Сетевой адрес      Маска сети      Адрес шлюза      Интерфейс      Метрика
-----
0.0.0.0            0.0.0.0        192.168.5.1      192.168.5.200  20
127.0.0.0          255.0.0.0      127.0.0.1        127.0.0.1      1
192.168.5.0        255.255.255.0  192.168.5.200    192.168.5.200  20
192.168.5.200     255.255.255.255  127.0.0.1        127.0.0.1      20
192.168.5.255     255.255.255.255  192.168.5.200    192.168.5.200  20
224.0.0.0          240.0.0.0      192.168.5.200    192.168.5.200  20
255.255.255.255   255.255.255.255  192.168.5.200    192.168.5.200  1
Основной шлюз:      192.168.5.1
=====
Постоянные маршруты:
Отсутствует
C:\>
```

Рис. 3.3. Таблица маршрутів в ОС Windows

Як неважко побачити, у таблиці визначено кілька маршрутів з різними параметрами. Читати кожен такий запис у таблиці маршрутизації потрібно таким чином:

*Щоб доставити пакет у мережу з адресою з поля Мережева адреса й маскою з поля Маска мережі, потрібно з інтерфейсу з IP-адресою з поля Інтерфейс надіслати пакет за IP-адресою з поля Адреса шлюзу, а «вартість» такої доставки буде дорівнює числу з поля Метрика.*

Відзначимо, що параметри Мережева адреса й Маска мережі разом задають діапазон усіх дозволених у даній мережі IP-адрес. Наприклад, 127.0.0.0 і 255.0.0.0, як ми вже говорили, означають будь-який IP-адреса від 127.0.0.1 до 127.255.255.254. Згадаємо також, що IP-адреса 127.0.0.1 називається «адресою заглушки» – надіслані за цією адресою пакети повинні оброблятися самим комп'ютером. Крім того, маска 255.255.255.255 означає мережу з одного IP-адреси, а комбінацію 0.0.0.0 – будь-яку невизначену адресу або маску підмережі.

Тоді перший рядок у таблиці маршрутизації означає точно те, що робить комп'ютер при необхідності надіслати пакет у віддалену, тобто невідому йому з таблиці маршрутизації, мережа – зі свого інтерфейсу пакет посилається на IP-адресу маршрутизатору.

Другий рядок таблиці змушує комп'ютер посилати самому собі (і відповідати на них) усі пакети, відправлені за будь-якою IP-адресою з діапазону 127.0.0.1 – 127.255.255.254.

У третьому рядку визначено, як посилати пакети комп'ютерам локальної мережі (за адресами з діапазону 192.168.5.1 – 192.168.5.254). Тут чітко видно, що робити це повинен сам комп'ютер – адресою шлюзу є його власний IP-адреса 192.168.5.200.

Аналогічно (п'ятий, шостий та сьомий рядок таблиці) потрібно чинити й у випадку, коли пакети надсилаються за адресою розсилки підмережі

(192.168.5.255), за адресами багатоадресної розсилки (224.0.0.0) або за адресою локальної широкомовної розсилки (255.255.255.255).

Четвертий рядок означає, що пакети, послані за IP-адресою 192.168.5.200 (зверніть увагу на маску!), повинні оброблятися самим комп'ютером.

Дещо складніше буде виглядати таблиця маршрутизації комп'ютера із двома мережевими адаптерами, який ми будемо використовувати в якості маршрутизатора для об'єднання двох сегментів невеликої мережі (див. рис. 3.4).

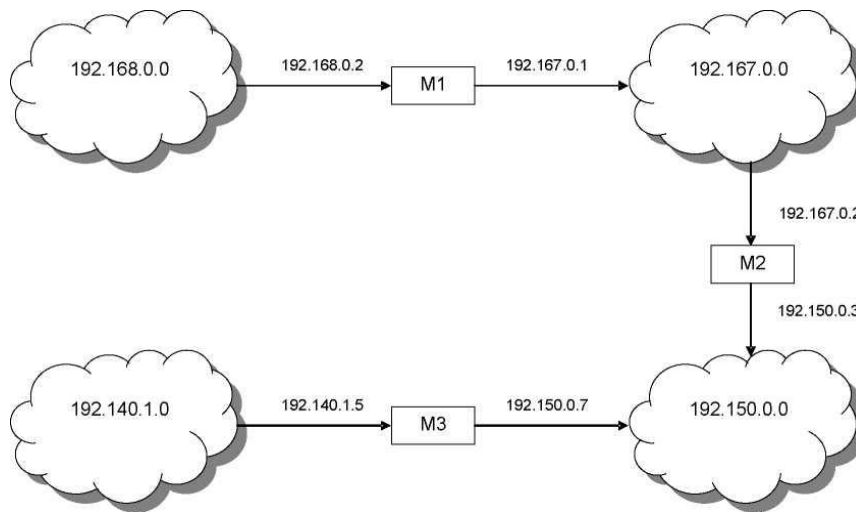


Рис. 3.4. Об'єднання мережі за допомогою маршрутизаторів M1, M2, M3

На цій схемі зображено чотири мережі-адресати, три маршрутизатори і IP-адреси мереж та кожного маршрутизатора зі сторони кожної мережі.

Для цієї мережі таблиця маршрутизації матиме наступний вигляд (див. табл. 3.4):

Таблиця 3.4

**Таблиця маршрутизації для маршрутизатора M2**

Мережа-адресат	Маршрут
192.167.0.0	пряме передавання
192.150.0.0	пряме передавання
192.168.0.0	через адресу 192.167.0.1
192.140.1.0	через адресу 192.150.0.7



У цій таблиці з'явилося кілька додаткових рядків, що позначають маршрути в обидві мережі – 192.167.0.0 і 192.150.0.0. Зауважимо, що всі такі маршрути будуть побудовані комп'ютером автоматично.

Щоб після цього налагодити обмін IP-пакетами між мережами, потрібно виконати наступні дії:

- включити маршрутизацію на комп'ютері  $R_1$  – це можна зробити, наприклад, налаштувавши службу маршрутизації й віддаленого доступу, що входить до складу операційної системи Windows Server 2003;
- на всіх комп'ютерах у мережі  $N_1$  параметр Основний шлюз потрібно встановити рівним IP-адресі інтерфейсу маршрутизатора, підключеного до цієї мережі, тобто рівним 192.168.5.1, а на комп'ютерах у мережі  $N_2$  – рівним 192.168.10.1.

Таким чином, маршрутизатор – це програмно-апаратний пристрій з декількома мережевими інтерфейсами, на якому працює служба маршрутизації.

У великих мережах, що містять велику кількість з'єднаних одна з одною підмереж, вручну прописувати маршрути доставки пакетів на всіх маршрутизаторах досить важко. До того ж такі маршрути є статичними, отже, при кожній зміні конфігурації мережі потрібно буде виконувати велику роботу з перебудови системи IP-маршрутизації.

Щоб уникнути цього, достатньо налаштувати маршрутизатори так, щоб вони обмінювалися один з одним інформацією про маршрути. Для цього в локальних мережах використовують такі протоколи, як RIP (Routing Information Protocol) і OSPF (Open Shortest Path First). Протокол RIP простіше в налаштуванні, чому OSPF, однак для обміну інформацією в ньому застосовуються ширококомвні повідомлення, що помітно навантажують мережа. Тому RIP зазвичай використовують у відносно невеликих мережах. Протокол OSPF працює ефективніше, але складніше налаштовується, тому його використання рекомендується для великих корпоративних мереж.

### 3.4. Призначення IP-адрес та перевірка працездатності TCP/IP

Ми вже бачили, наскільки важливою для взаємодії комп'ютерів у мережі TCP/IP є правильне налаштування протоколу IP. Тому важливо обговорити, якими способами можна налаштовувати параметри IP на комп'ютерах і як швидко перевірити працездатність усієї системи IP-адресації й маршрутизації.

Найпростіший спосіб налаштування параметрів протоколу IP – призначити їх вручну. Перевагою такого методу є те, що адміністратори мережі повністю контролюють усі IP-адреси комп'ютерів у ній, що може бути важливо з погляду захисту даних або взаємодії з Інтернетом. Однак у цього способу багато недоліків. По-перше, легко помилитися й увести неправильні параметри маски або шлюзу або, призначити повторювану у мережі IP-адресу. По-друге, при змінах параметрів IP-адресації в мережі (наприклад, при зміні IP-адреси маршрутизатора) доведеться переналаштовувати всі комп'ютери. При такому способі налаштування практично неможливо працювати у великих корпоративних мережах із мобільними пристроями типу ноутбуків або КПК, які часто переміщуються з одного сегмента мережі в іншій.

Тому в організаціях частіше застосовують спеціальні сервери, що підтримують протокол динамічної конфігурації вузлів (Dynamic Host Configuration Protocol, DHCP), завдання яких полягає в обслуговуванні запитів клієнтів на отримання IP-адреси й іншої інформації, необхідної для правильної роботи в мережі. Саме тому комп'ютери з операційними системами Windows за замовчуванням налаштовані на автоматичне одержання IP-адреси.

Якщо сервер DHCP недоступний (відсутній або не працює), то починаючи з версії Windows 98 комп'ютери самостійно призначають собі IP-адресу. При цьому використовується механізм автоматичної особистої IP-адресації (Automatic Private IP Addressing, APIPA), для якого корпорацією Microsoft в IANA був зареєстрований діапазон адрес 169.254.0.0 – 169.254.255.255.

Нарешті, обговоримо, які кроки потрібно зробити для перевірки параметрів і працездатності протоколу IP.

### **1. Виконайте команду IPCONFIG /ALL.**

Якщо у виданій на екран інформації не міститься жодних параметрів, отже, у вас немає активних інтерфейсів.

Якщо у виданій інформації є діагностичне повідомлення «Мережа відключена», отже, у вас проблеми з фізичним рівнем – перевірте підключення конектора в роз'ємі мережевого адаптера й/або працездатність комутатора.

Якщо ваші параметри IP-адреси й маски підмережі рівні 0.0.0.0, отже, ви використовуєте статичну IP-адресу, що конфліктує з іншим вузлом у мережі.

Якщо ваша IP-адреса знаходиться в діапазоні 169.254.x.x, то DHCP-Сервер недоступний і працювати ви зможете тільки з тими комп'ютерами в мережі, які також самостійно призначили собі адресу.

У нормальній ситуації при отриманні IP-адреси від DHCP-сервера або правильного ручного налаштування ви повинні побачити у виданій на екран інформації такі параметри, як IP-адреса комп'ютера, маска підмережі, основний шлюз, DNS-сервер і DHCP-сервер (а також, можливо, інші параметри).

### **2. Виконайте команду PING 127.0.0.1.**

Якщо відповідь не отримана, це свідчить про неправильне налаштування стека протоколів TCP/IP; доведеться перевстановити відповідну програмну підтримку.

Якщо відповідь отримана, отже, стек протоколів TCP/IP працює правильно.

### **3. Виконайте команду PING w.x.y.z, де w.x.y.z – IP-адреса сусіднього комп'ютера.**

Так перевіряється працездатність локальної мережі.

### **4. Виконайте команду PING w.x.y.z, де w.x.y.z – IP-адреса основного шлюзу.**

Так перевіряється доступність і працездатність маршрутизатора.

### **5. Виконайте команду PING w.x.y.z, де w.x.y.z – IP-адреса будь-**

## якого вилученого комп'ютера.

Так перевіряється працездатність усієї системи маршрутизації вашої корпоративної мережі або з'єднання з Інтернетом.

6. У багатьох сучасних мережах пакети протоколу ICMP, за допомогою яких утиліта PING трестує взаємодію, забороняються за вимогою служб безпеки. ОС Windows XP SP2 із включеним фаєрволом також блокує ICMP-пакети. Тому, якщо утиліта PING не показує відповідей, не поспішайте шукати причину «збою» на своєму комп'ютері, а спочатку з'ясуєте в адміністратора мережі (або в налаштуваннях своєї ОС Windows XP), чи дозволено у вашій мережі використання ICMP.

На закінчення приведемо набір коротких правил, які допоможуть вам не помилитися при налаштуванні IP-адресації й маршрутизації в мережах TCP/IP:

- 1) щоб взаємодіяти в мережі TCP/IP, усі комп'ютери повинні мати IP-адреси;
- 2) комп'ютери, що знаходяться в одному фізичному сегменті мережі (з'єднані концентраторами або комутаторами), повинні належати одній IP-мережі, але мати унікальні IP-адреси;
- 3) для визначення ідентифікаторів локальної мережі або віддалених мереж використовується маска підмережі;
- 4) щоб взаємодіяти з віддаленими мережами, комп'ютерам потрібен адреса основного шлюзу, яка повинна співпадати з адресою маршрутизатора, що з'єднує вашу мережу з іншими;
- 5) маршрутизатори – це комп'ютери з декількома мережевими інтерфейсами, що вміють передавати IP-пакети з однієї мережі в іншу у відповідності зі своїми таблицями маршрутизації;
- 6) маршрутизатор завжди має маршрути до всіх мереж, підключених до нього безпосередньо; маршрути в інші мережі потрібно налаштовувати;
- 7) таблиці маршрутизації можна налаштовувати вручну або застосовувати динамічні протоколи обміну інформацією про маршрутизацію.

## Запитання для перевірки знань

1. Що таке набір (стек) протоколів? У чому суть терміну «стек»?
2. Які набори протоколів ви знаєте? Чим вони різняться?
3. Який стек протоколів сьогодні найбільш популярний? Чому?
4. Які рівні моделі OSI підтримуються в стеку протоколів TCP / IP?
5. У чому подібність і відмінність між протоколами TCP і UDP? Коли який з цих протоколів рекомендується використовувати?
6. Перерахуйте відомі вам протоколи прикладного рівня в стеку TCP / IP. Для чого призначений кожен з них?
7. Що таке «порт» у TCP / IP? Для чого потрібні порти?
8. Який з транспортних протоколів стека TCP / IP ви б використовували:
  - a. для пересилання по мережі Інтернет архівних файлів?
  - b. для реалізації IP-телефонії (передаванні голосових повідомлень в реальному часі) між користувачами двох мобільних комп'ютерів (КПК), з'єднаних по бездротовому каналу Wi-Fi?
9. Які параметри і налаштування обов'язкові для забезпечення роботи стека протоколів TCP / IP
10. Що таке IP-адреса? Яка його структура? Які можливі способи представлення IP-адрес?
11. Чим відрізняються версії 4 і 6 протоколу IP? Які переваги забезпечить версія 6 протоколу IP? Чому виникла необхідність у переході на версію 6 протоколу IP?
12. Що таке маска підмережі? Для чого вона потрібна?
13. У чому полягає зміст поділу IP-адреси на ідентифікатори мережі і вузла? Для чого це потрібно?
14. Які IP-адреси і маски є допустимими, а які – ні? Чому?
15. У чому полягає відмінність між класовою і безкласовою IP-адресацією? Які їх переваги та недоліки?
16. Що таке класи IP-адрес? За якими правилами вони визначаються?
17. Як призначити IP-адреси в локальній мережі (без виходу в Інтернет)?

18. Які основні принципи маршрутизації пакетів у локальних і віддалених мережах?
19. Що таке таблиця маршрутів (таблиця маршрутизації)? Поясніть зміст кожної з її колонок.
20. Як «прописати» в таблиці маршрутизації відсутній в ній новий маршрут?
21. Що таке динамічна конфігурація вузлів? Для чого вона потрібна?

## **ЛЕКЦІЯ 4.**

### **Тема. Світова інформаційна мережа Інтернет**

**Мета:** Ознайомити здобувачів вищої освіти з історією розвитку, загальною характеристикою, а також із світовими службами, базовими технологіями та основними загрозами під час роботи в мережі Інтернет

#### **План**

1. Історія розвитку мережі Internet
2. Загальна характеристика мережі Internet
3. Адресація в Internet і доменна система імен
4. Світові електронні служби мережі Internet
5. Загальна характеристика й класифікація електронних служб мережі Internet
6. Базові технології й служби мережі Internet
7. Інформаційна мережа WWW (World Wide Web)
8. Основні загрози під час роботи в мережі Internet

Вплив глобальної мережі Internet на сучасне суспільство важко переоцінити, оскільки він настільки багатогранний і динамічний, що зачіпає практично всі сфери життя суспільства.

З одного боку, Internet – це відсутність будь-яких меж, що дозволяє всім користувачам, що мають доступ до мережі, обмінюватися інформацією в планетарному масштабі. У цьому зв'язку поява й розвиток Internet істотно

змінити характер інформаційного обміну як і в окремих країнах, так і в масштабі всієї планети.

З іншого боку, Internet – це об'єднання чималої кількості обчислювальних машин, які є технічною основою мережі.

І нарешті, Internet – це великий, постійно доступний інформаційний простір, що поєднує значну кількість накопиченої людством інформації.

Постійне збільшення інформаційних ресурсів мережі, інтеграція різних видів інформації (дані, графіка, звук, відео) є однією з головних рушійних сил розвитку апаратних і програмних засобів обчислювальних мереж. Раніше вже відзначався історичний поворот у розвитку операційних систем сімейства Windows, що полягає в тому, що всі операційні системи, що випускаються, цієї компанії є по суті мережевими. Це пов'язане з потребами користувачів в ефективній роботі в мережі Internet. Операційна система Windows, що з'явилась пізніше тільки лише підтвердила цю тенденцію. Аналогічні тенденції й у сфері розвитку апаратних засобів, де зусилля розробників в основному націлені на створення апаратних засобів, що забезпечують користувачу повсюдний і постійний доступ до глобальної мережі.

Унікальність Internet полягає в тому, що ця мережа одночасно є й засобом загальносвітового мовлення, і механізмом поширення інформації, і середовищем для співробітництва й спілкування людей за допомогою обчислювальних машин, що охоплює увесь світ, а останнім часом Internet є й сферою бізнесу.

#### **4.1. Історія розвитку мережі Internet**

Перший і найголовніший аспект історичного розвитку мережі Internet – це технологічна еволюція, яка почалася з ранніх досліджень з пакетної комутації й мережі ARPANET. Технологічна еволюція мережі на сьогоднішній день не закінчена, оскільки на сучасному етапі необхідно розв'язати низку завдань, пов'язаних з масштабуванням мережі, підвищенням її ефективності й функціональності й, що не менш важливе – безпеки.

Другий історичний аспект розвитку мережі Internet пов'язаний з розвитком технологій експлуатації й керування територіально розподіленої (глобальної) інфраструктури.

Не менш цікава й історія створення зовсім нового соціального явища – Internet-співтовариства, що поєднує безліч користувачів і організацій, що спільно працюють добровільно над створенням і розвитком технології Internet.

Ідея пакетної комутації була другим фундаментальним кроком на шляху до Internet, тому що першим кроком можна вважати саму ідею створення глобальної мережі.

Перший етап розвитку Internet завершився в 1969 р. створенням мережі ARPANET. На цьому етапі були закладені фундаментальні положення побудови майбутньої глобальної мережі, що, однак, не зменшує важливості наступних етапів розвитку мережі. В 1969 р. до сучасного вигляду Internet було ще далеко, та й самі творці першої глобальної мережі не припускали такого результату.

Наступний етап розвитку глобальних мереж характеризується збільшенням нових технологій і розширенням мережі, оскільки починаючи з 1970 р. кількість комп'ютерів, підключених до ARPANET, швидко збільшувалось. Разом із тим проводились роботи зі створення повнофункціонального протоколу міжкомп'ютерної взаємодії й іншого мережевого програмного забезпечення.

Для майбутнього мережі у 1972 р. відбулися два важливі події. По-перше, на початку року Рей Томлінсон (BBN) доробив створену роком раніше програму E-mail (електронна пошта) для її використання в мережі ARPANET, де вона швидко набула популярності. З того часу більш ніж на 10 років електронна пошта стала найбільшим (провідним) мережевим додатком. По-друге, у цьому ж році була прийнята специфікація протоколу Telnet (RFC 318).

Черговий найважливіший крок, що визначив вигляд сучасної глобальної обчислювальної мережі, припав на цей же, 1972 р., коли Боб Кан уперше



висловив ідею «відкритої мережевої архітектури», реалізація якої переросла в проект «Internetting». Так з'явилося саме поняття «Internet».

Відкрита мережева архітектура передбачає, що окремі мережі можуть проектуватися й розроблятися незалежно зі своїми унікальними інтерфейсами, що надаються користувачам та іншим постачальникам мережевих послуг. Під час проектування кожної мережі можуть бути прийняті до уваги специфіка оточення й особливі вимоги користувачів. У загальному випадку відкрита архітектура не накладає жодних обмежень на типи поєднаних мереж або їх територіальний масштаб.

Широке поширення в 1980-ті роки локальних мереж, персональних комп'ютерів і робочих станцій дало поштовх бурхливому росту Internet.

Перехід від невеликої кількості мереж із помірною кількістю вузлів з поділом часу (початкова модель ARPANET) до багатьох мереж призвів до вироблення низки нових концепцій та внесення змін до базових технологій. Зокрема, були визначено 3 класи мереж (А, В і С), що враховують різні масштаби конфігурацій.

У 1982 р. DCA, що управляє мережею з 1975 р., і DARPA встановили як основу побудови мережі протоколи IP і TCP.

По-справжньому день народження Internet багато фахівців вважають 1 січня 1983 р. Саме в цей день відбувся перехід ARPANET із протоколу NCP на TCP/IP. Це був перехід у стилі «Дня X», що потребує одночасних змін на всіх комп'ютерах. Перехід ретельно планувався всіма зацікавленими сторонами протягом кількох попередніх років, що дозволило уникнути серйозних проблем.

Визнання Міністерством оборони США стека протоколів TCP/IP у якості військового стандарту (в 1980 р.) зумовило поділ Internet на військову й цивільну складові, оскільки до 1983 р. ARPANET використовували більшість військових дослідних, розробляючих та експлуатуючих організацій. Перехід ARPANET з NCP на TCP/IP дозволив розділити цю мережу на MILNET, що

обслуговувала оперативні потреби, і ARPANET, що використовувався в дослідницьких цілях.

Перше січня 1983 р. можна вважати початком нового, третього історичного етапу розвитку глобальної мережі.

Спочатку при невеликій кількості комп'ютерів використовувалася єдина таблиця відповідності імен і адрес. Перехід до великої кількості незалежно адміністрованих мереж зробив ідею єдиної таблиці непридатною. В 1984 р. було запроваджено систему доменних імен (Domain Name System, DNS). Система DNS дозволила створити масштабований розподілений механізм для відображення ієрархічних імен комп'ютерів (наприклад, history.com в 194.222.13.44) в Internet-адреси. На той час мережа включала вже 1000 вузлів.

Зростання Internet стимулювало розвиток програмного забезпечення, особливо його мережевої частини. Управління DARPA підтримало дослідження Університету Берклі (Каліфорнія) щодо модифікації операційної системи Unix, у тому числі й реалізації в ядрі операційної системи стеку протоколів TCP/IP.

Упровадження мережевих протоколів TCP/IP у доступну користувачам операційну систему стало одним із ключових кроків щодо подальшого успішного та повсюдного поширення Internet.

## **4.2. Загальна характеристика мережі Internet**

### **4.2.1. Визначення Internet**

24 жовтня 1995 р. Федеральна мережева рада (FNC) схвалила резолюцію, що визначає термін «Internet». Це визначення розроблялося за участю фахівців в галузі мереж і в галузі права на інтелектуальну власність. У цій резолюції наводиться наступне комплексне визначення мережі Internet, яке можна розглядати як офіційне:

**Internet** – це глобальна інформаційна система, яка:

- 1) логічно взаємопов'язана простором глобальних унікальних адрес, заснованих на Internet-протоколі (IP) або на подальших розширеннях або наступниках IP;

2) здатна підтримувати комунікації з використанням стека протоколів TCP/IP або його подальших розширень/наступників та/або інших IP-сумісних протоколів;

3) забезпечує, використовує або робить доступною на громадській або приватній основі високорівневі сервіси, надбудовані над комунікаційною й іншою пов'язаною з нею інфраструктурою.

Очевидно, з одного боку, за всіма ознаками, що наводяться у визначенні, основою глобальної мережі Internet є сімейство протоколів TCP/IP.

З іншого боку, це визначення не накладає жодних обмежень на високорівневий сервіс, що надається мережею, і жодних обмежень на комунікаційну інфраструктуру, крім сумісності зі стеком протоколів TCP/IP.

У зв'язку з цим кожна з мереж, що складає Internet, може бути реалізована на різних принципах. Це можуть бути такі мережі, як Ethernet, Token Ring, ATM, ISDN, X.25, FDDI, Arcnet та інших.

Крім цього, окремі вузли, що підключаються до Internet, можуть використовувати різне обладнання й різні способи підключення (виділені лінії, модемне з'єднання по лініях, що комутируються), а також різні мережеві програмні засоби, проте обов'язковою умовою є підтримка стека протоколів TCP/IP.

### **4.3. Адресація в Internet і доменна система імен**

#### **Поняття домена й доменного імені**

Однією з головних проблем побудови глобальної мережі Internet є проблема адресації. З одного боку, постійне розширення мережі Internet призвело до дефіциту унікальних адрес для вузлів, що щойно підключаються. З іншого боку, система адресації в такій мережі має бути універсальною й зручною для користувача. Остання обставина особлива була важливою з початком застосування ресурсів мережі не тільки фахівцями, але й непідготовленими користувачами, що не володіють тонкощами адресації в мережі. Вирішальним аргументом для переходу до альтернативних способів адресації в мережі, зручним

для роботи користувачів, була незручність запам'ятовування 32-бітового коду, що ідентифікує окремий вузол. Ця незручність виявилася відразу ж, коли мережа використовувалася вузьким колом фахівців. Тому з'явилися альтернативні форми запису 32-бітового IP-адреса – десяткова (195.224.11.77) і шістнадцяткова (0xffffffbo) дот-нотації. Остання форма запису особливо була зручної для програмістів, які часто застосовують шістнадцятковий алфавіт для запису коду програми.

Згодом з появою в мережі різних сервісів (електронна пошта й інші служби), а також зі збільшенням кількості вузлів і така форма запису виявилася незручної, оскільки досить складно запам'ятати декілька цифрових адрес, навіть у десятковій доті-нотації. Це обумовило появу в мережі ARPANET принципово нового способу адресації, що полягає в присвоєнні вузлам мережі доменного імені. У цьому випадку правильніше говорити про новий спосіб іменування вузлів мережі, оскільки доменне ім'я не є логічною адресою, наприклад, як IP-адреса, або фізичною адресою, як, наприклад, 6-байтова адреса мережевого інтерфейсу. Доменне ім'я – це зручна для користувача форма ідентифікації вузла обчислювальної мережі (сервіс).

**Домен** – це логічне угруповання комп'ютерів, об'єднаних спільною базою даних користувачів і комп'ютерів, політикою безпеки та управління. Наприклад, домен «ua» поєднує вузли на території України, а домен «**sport**» – вузли, що відносяться до спортивних організацій або містять інформацію про спорт та ін.

**Доменне ім'я** – це унікальний алфавітно-цифровий ідентифікатор вузла (складається із символів ASCII-коду – літер від A до Z1 латинського алфавіту й цифр від 0 до 9, також допускається дефіс «-»).

## **4.4. Світові електронні служби мережі Internet**

### **4.4.1. Загальна характеристика й класифікація електронних служб мережі Internet**

До цього часу Internet розглядався з погляду пристрою як глобальна обчислювальна мережа. Раніше були розглянуті моделі мережевої взаємодії,

фізичні основи обчислювальних мереж і принципи створення глобальних обчислювальних мереж, принципи адресації й іменування вузлів обчислювальної мережі та ін.

Однак це лише одна сторона Internet, набагато більш цікавою й привабливою для більшості користувачів мережі є її інша сторона – інформаційна, тобто Internet як глобальна інформаційна мережа.

Із цього погляду Internet є величезним, постійно доступним масивом інформаційних ресурсів, територіально розподіленим у масштабі всієї планети. Крім цього, Internet – це набір безлічі різних прикладних сервісів і служб, що обслуговують запити користувачів. Internet постійно розвивається. З кожним роком з'являються нові мережеві служби й сервіси, а разом з ними постійно збільшується інформаційний простір мережі Internet.

Сучасне мережеве програмне забезпечення надає користувачеві численні засоби навігації по інформаційному просторі Internet.

#### **4.4.2. Поняття прикладного сервера в мережі Internet**

В основу всіх прикладних процесів Internet покладено принцип клієнт-серверної архітектури мережевих програмних засобів.

Відповідно до цього принципу джерелом усіх мережевих послуг і сервісів в Internet є відповідні сервери (наприклад, Web-сервер, ftp-сервер та ін.) спеціальні програми, що отримують по мережі запити користувачів (клієнтів) та обробляють їх, а при необхідності повертають результати виконання запитів. Зазвичай кожен сервер підтримує або забезпечує один вид мережевих послуг. Це з тим, що функції серверів реалізуються різними прикладними протоколами (наприклад, для згаданих раніше як приклад типів серверів – це протокол передачі гіпертексту – http і протокол передачі файлів – ftp тощо).

Програмний сервер, що забезпечує прикладний сервіс, може працювати на будь-якому вузлі, підключеному до мережі. Оскільки під сервером у цьому випадку розуміється програма, очевидно, що на одній обчислювальній машині, що є вузлом обчислювальної мережі, можуть функціонувати кілька серверів.

У цьому полягає відмінність у визначенні поняття сервер обчислювальної мережі й сервер у мережі Internet. У першому випадку йдеться про окремий вузол обчислювальної мережі, що виконує функції керуючого вузла або вузла, що надає свої ресурси в загальне користування, а в другому випадку йдеться про програму (набір програм), що забезпечує певний мережевий сервіс.

Таким чином, можна зробити наступний висновок: будь-який вузол обчислювальної мережі Internet, що надає свої ресурси в загальне користування та обробляє запити користувачів, є фізичним сервером мережі Internet. Поряд із цим один фізичний сервер може бути основою одного й більше прикладних серверів мережі Internet, а фізичний сервер окремої локальної мережі (наприклад, вузол, що надає свої ресурси користувача тільки цієї локальної мережі), підключеної до мережі Internet, не обов'язково є сервером Internet.

Слід особливо підкреслити автоматичний характер роботи серверів Internet, які функціонують цілодобово, що забезпечує постійний доступ до мережевих сервісів.

#### **4.4.3. Прикладні сервери мережі Internet**

Найбільш популярними й розповсюдженими в мережі Internet є наступні види серверів:

- сервер новин,
- файловий сервер,
- FTP-сервер,
- сервер доступу,
- Фах-Сервер,
- сервер баз даних,
- сервер статистики.

## **Сервіс мережевих служб Internet**

Крім розглянутих найпоширеніших прикладних серверів, мережевий сервіс Internet забезпечується безліччю мережевих служб, в основі функціонування яких також клієнт-серверна архітектура.

Найбільш поширеними службами Internet є:

- служба IRC;
- служба ICQ;
- Gopher;
- WAIS;
- Archie і VERONICA;
- E-mail;
- WWW;
- USENET.

## **4.5. Базові технології й служби мережі Internet**

### **4.5.1. Всесвітня мережа WWW (World Wide Web)**

Коли наша мережа побудована, захищена, підключена до Інтернету і налаштована для роботи з іменами вузлів, нам залишається тільки дізнатися, які служби надає нам Інтернет і які програми потрібно використовувати для роботи з цими службами.

Почнемо з Всесвітньої павутини, або WWW (World Wide Web) – це найпопулярніший сьогодні сервіс Інтернету, єдиний інформаційний простір, що утворюється із сотень мільйонів взаємозалежних електронних документів, що зберігаються на Web-Серверах. Інформація у WWW подається у вигляді веб-сторінок, які можуть містити звичайний текст, або ж гіпертекст, а також практично будь-які інші дані, в тому числі графіку, музичні або відео-ролики. Крім того, на веб-сторінках можуть розміщуватися посилання на інші веб-сторінки, які зберігаються на тому ж самому або на будь-якому іншому сервері в Інтернеті.

Веб-сторінки розміщуються на веб-серверах у вигляді пов'язаних один з одним наборів, які називаються сайтами. Сайти можуть належати будь-якій конкретній особі або організації і підтримуються розробниками (веб-майстрами).

Зауважимо, що WWW є тільки однією з багатьох служб, які працюють в Інтернеті, однак саме через неї до Інтернету підключається переважна більшість користувачів (багато з них навіть вважають, що поняття «WWW» та «Інтернет» збігаються).

При зверненні до веб-сайту завжди відкривається його *головна сторінка*, іноді вона називається *домашньою (home page)*. Для зручності роботи на головній сторінці часто розміщують колонку змісту, карту сайту, або навігаційну панель, які дозволяють відвідувачам сайту швидко знайти необхідну інформацію.

### **Історія розвитку WWW**

Історія WWW розпочалася в березні 1989 р., коли Тім Бернерс-Лі, англійський інженер-програміст, який працював у Європейській лабораторії фізики елементарних часток у Женеві (CERN), запропонував керівництву CERN проект «Гіпертекст». Його суть полягала в об'єднанні всієї безлічі інформаційних ресурсів CERN, яка складалася з бази даних звітів, комп'ютерної документації, списків поштових адрес, інформаційної реферативної системи, наборів даних результатів експериментів та ін., у єдиний гіпертекстовий простір, який дозволяв легко переходити з одного документа до іншого.

До 1992 р. ідея Тіма Бернерса-Лі втілилася в технологію World Wide Web, що стала однією з базових технологій мережі Internet.

Після того як цей вид сервісу був оприлюднено. Незважаючи на те, що WWW був розроблений з метою застосування співробітниками CERN, його популярність стала рости надзвичайно швидко.

У 1993 р. Марко Андрессен та Ерик Байна з Національного центру програм для суперкомп'ютерів (National Center for Supercomputing Applications, NCSA) створили програму NCSA Mosaic – графічний браузер для відображення



гіпертекстових документів. Із цього часу популярність WWW почала набирати обертів (за перші 5 років існування технології WWW кількість Web-серверів, що складають Web-простір, досягла приблизно 1500. За наступні 5 років кількість Web-серверів перевищило 7 млн.).

Слід зазначити, що сам проєкт NCSA Mosaic забезпечив розвиток технології World Wide Web, суттєво збагативши компоненти системи. Розробники Mosaic запровадили в стандарти WWW велику кількість нововведень.

Згодом було створено безліч прикладних програм, що використовувалися у якості WWW-клієнтів, тобто, забезпечують доступ до WWW-серверів і демонстрації гіпертекстових документів на екрані.

### **Основні загрози під час роботи в мережі**

Під загрозою розуміють будь-які обставини та події, що виникають у зовнішньому середовищі, які у відповідних умовах можуть викликати появу небезпечної події.



**Інформаційна загроза** – це потенційна можливість певним чином порушити інформаційну безпеку.

Загрози, що чекають користувачів при підключенні комп'ютера до мережі, досить багато. Наведемо основні з них:

- «зламування» комп'ютера – здійснюється з метою захоплення контролю над операційною системою й одержання доступу до даних);
- пошкодження системи – організується, щоб пошкодити працездатність (викликати відмову в обслуговуванні – «Denial of Service») будь-яких сервісів або комп'ютера (частіше сервера) цілком, а іноді – навіть усієї мережевої інфраструктури організації;
- викрадання даних через неправильно встановлених прав доступу, при передаванні даних або «зламуванні» системи – призводить до отримання доступу до інформації, що захищається, частіше – конфіденційної;
- знищення даних – мета пошкодити або навіть паралізувати роботу систем, комп'ютерів, серверів або всієї організації.

Атаки на комп'ютери або сервери, віруси, «хробаки», шпигунські й «троянські» програми – усе це шкідливе програмне забезпечення розробляється для того, щоб здійснити схарактеризовані вище загрози.



Типова «троянська» програма зазвичай «маскується» під будь-яку корисну утиліту (або може бути захована в будь-якій програмі), а якщо користувач через незнання запустить її на виконання, така програма починає контролювати комп'ютер, надаючи доступ автору «троянської програми» доступ до даних (так званий «backdoor» – «чорний хід»), викрадаючи й пересилаючи йому паролі, що набираються із клавіатури і таке ін.

**Основні правила безпеки під час роботи в мережі.** Сформулюємо основні з них:

- відключайте комп'ютер, коли ви ним не користуєтеся;
- вчасно оновляйте операційну систему. У будь-якій ОС періодично виявляються так звані «уразливості», що знижують захищеність вашого комп'ютера. Наявність уразливостей потрібно уважно відслідковувати, щоб вчасно вживати заходів для їхнього усунення.

Для ОС Windows корпорацією Microsoft створено спеціальний веб-вузол Windows Update, звернувшись до якого (наприклад, за допомогою програми WUPDMGR.EXE або команди Windows Update в меню Пуск), неважко переглянути й завантажити список оновлень, рекомендованих для вашого комп'ютера;

- використовуйте обмежений набір перевірених додатків, не встановлюйте самі й не дозволяйте іншим встановлювати на ваш комп'ютер програми, узяті з неперевірених джерел (особливо з Інтернету). Якщо додаток більше не потрібно, видаліть його;
- без необхідності не надавайте ресурси свого комп'ютера в загальний доступ. Якщо ж це було потрібно, обов'язково налаштуйте мінімально необхідний рівень доступу до ресурсу тільки для зареєстрованих облікових записів;

- установіть (або включіть) на комп'ютері персональний міжмережевий екран (брандмауер). Якщо мова йде про корпоративні мережі, встановіть брандмауери як на маршрутизаторах, що з'єднують вашу локальну мережу з Інтернетом, так і на всіх комп'ютерах мережі;

- обов'язково встановіть на комп'ютер спеціалізоване антивірусне й «антишпигунське» програмне забезпечення. Налаштуйте його на автоматичне одержання оновлень як мінімум один раз на тиждень (краще – щодня або навіть кілька разів на день);

- навіть якщо ви єдиний власник комп'ютера, для звичайної роботи застосовуйте користувацький обліковий запис: у цьому випадку ушкодження системи, наприклад, при зараженні вірусом, буде менше, чим якби ви працювали із правами адміністратора. Для всіх облікових записів, особливо адміністративних, установіть й запам'ятаєте складні паролі.

Складним вважається пароль, що містить випадкову комбінацію літер, цифр і спеціальних символів, наприклад, jxglrg\$N. Зрозуміло, пароль не повинен збігатися з іменем вашого облікового запису. В операційних системах Windows складний пароль можна згенерувати автоматично, використовуючи команду NET USER із ключем /RANDOM, наприклад:

NET USER Ім'я\_Користувача /RANDOM


Пароль у вигляді випадкової послідовності символів нелегко запам'ятати, тому часто використовують наступну техніку – пароль набирається в англійській розкладці російськими літерами. Наприклад, слово «Пароль» тоді буде виглядати як «Gfhjkm». Однак цей спосіб слід застосовувати з обережністю – зломники давно мають цілі словники подібним чином перетворених слів, так що бажано вставляти в такі паролі спеціальні символи й цифри.

Паролі для доступу в різні системи повинні бути різними. Неприпустимо використовувати той самий пароль для адміністрування вашого комп'ютера й для входу, наприклад, на ігровий веб-сайт;


- при роботі з електронною поштою ніколи відразу не відкривайте

вкладення, особливо отримані від невідомих відправників. Збережіть вкладення на диску, перевірте його антивірусною програмою й тільки потім відкрийте. Якщо є така можливість, увімкніть у вашій поштовій програмі захист від потенційно небезпечного вмісту й відключіть підтримку HTML;

- при роботі з веб-сайтами дотримуйте запобіжного заходів: намагайтеся уникати реєстрації, не передавайте нікому персональні відомості про себе й уважно працюйте з Інтернет-магазинами й іншими службами, де застосовуються онлайнві способи оплати за допомогою кредитних карт або систем типу Webmoney, Яндекс-гроші тощо. Під час проведення оплати переконаєтеся, що з'єднання захищене шифруванням за допомогою технології Secure Sockets Layer (SSL) – у цьому випадку адресний рядок обов'язково повинна починатися з «https://»;

 **«Фішинг» («риболовля»)** – так називається поширений сьогодні вид шахрайства в Інтернеті. Зловмисники створюють сайти, зовні схожі на сайти Інтернет-магазинів, банків тощо, а потім «заманюють» на них відвідувачів (наприклад, за допомогою рекламних банерів) і пропонують «підтвердити свої персональні дані». Іноді зловмисники з тією ж метою розсилають електронні листи нібито від імені адміністрації поштового сервера з проханням «підтвердити пароль доступу до поштової скриньки».

- перераховані вище заходи лише підвищують загальну захищеність системи й даних, але не дають ніякої гарантії від їхнього пошкодження або навіть повної втрати. Тому обов'язково слід створювати резервні копії системи й даних на з'ємному жорсткому диску або на DVD-RW – це дозволить легко відновити їх у випадку втрати. При цьому одну копію варто зберігати не вдома, наприклад, у сейфі;

 Під час резервного копіювання корисно використовувати утиліти для створення «образів» жорсткого диска (такі, як Norton Ghost). Резервну копію можна зняти з «системного» жорсткого диска після правильної установки на нього всіх необхідних

програм і антивірусної перевірки й зберігати її на іншому жорсткому диску (мережевому або з'ємному), щоб у випадку ушкодження системи швидко відновити її працездатність.

- виключно важливу роль відіграє навчання всіх користувачів основам безпечної роботи в мережах – як у домашніх, так і в корпоративних, – адже порушення правил одним користувачем ставить під загрозу всю систему захисту.

Отже, для роботи в мережі потрібні мережеві операційні системи, які прийнято поділяти на клієнтські й серверні. Клієнтські ОС відрізняються невеликим набором служб, але містять у собі спектр мережевих додатків. Серверні системи бувають різних типів і призначені для обслуговування тих або інших запитів мережевих клієнтів.

Для організації роботи в мережах Microsoft застосовуються дві моделі: робочі групи, які використовуються при невеликій кількості комп'ютерів, і домени, що дозволяють легко об'єднувати велику кількість користувачів, робочих станцій і серверів.

Усі мережеві ОС та дані, що зберігаються на комп'ютерах дані повинні бути надійно захищені, причому бажано, щоб система безпеки, що використовується була багаторівневою.

### **Запитання для перевірки знань**

1. Що таке DNS? Як вона працює?
2. Як структура запису доменного імені (кілька «слів», записаних через символ «крапки») пов'язана з деревовидною структурою служби DNS? (Поясніть на прикладі у вигляді умовної схеми.)
3. У чому полягає основна перевага DNS?
4. Чому поява нових доменних імен верхнього рівня завжди викликає помітний ажіотаж у всьому світі?
5. Як ви вважаєте, які переваги і недоліки могла б дати можливість реєстрації доменних імен не тільки англійською, а й національною мовою?

6. Що таке «Всесвітня Павутина»? Яка історія її появи? Які основні компоненти потрібні були для її реалізації?
7. Що означає термін «розподілена» у визначенні WWW як «розподіленої інформаційної системи»? Які переваги та недоліки пов'язані з цією властивістю WWW?
8. У чому полягає ідея гіпертекстового представлення інформації? Які її переваги?
9. Що таке веб-сторінка? Веб сайт? Веб-сервер? Як взаємопов'язані ці поняття?
10. Якою може бути типова структура веб-сайту? У чому полягають переваги та недоліки кожного з трьох видів структури веб-сайту? В яких випадках має сенс застосовувати ту чи іншу структуру?
11. Яке призначення веб-порталів і пошукових систем? (Наведіть приклади.)
12. Що таке браузер? Яке його призначення? Як ви вважаєте, чому саме Internet Explorer є найбільш популярним браузером, хоча при бажанні можна встановити практично будь-який браузер з декількох інших їх «сімейств»?
13. Які основні загрози під час роботи в мережі? Які, на вашу думку, основні причини (мотиви), що спонукають зловмисників здійснювати подібні дії?
14. Які основні правила (заходи) безпеки під час роботи в мережі?
15. Які додаткові заходи безпеки, на вашу думку, необхідні під час роботи в мережі (зокрема, в Інтернет) неповнолітніх? Як би ви організували роботу з Інтернетом для своєї дитини на своєму домашньому комп'ютері? В шкільному комп'ютерному класі?

## ЛЕКЦІЯ 5.

### Тема. Основи програмування для Web

Мета: ознайомити здобувачів вищої освіти з основними технологіями, які використовуються у Web. Навчити створювати простіші Web-сторінки та Web-сайти.

#### ПЛАН

1. Web-документи і web-сторінки.
2. Структура web-документів.
3. Основні теги мови HTML.
4. MIME-типи документів.
5. Програмне забезпечення для створення web-документів.

#### 5.1. Web-документи і web-сторінки

Web-документ – це текстовий документ в якому міститься опис web-сторінки для інтерпретування його програмою браузером спеціальною мовою HTML (Hyper Text Markup Language – мова гіпертекстової розмітки текстів).

На відміну від текстових документів, що містять змістовний текст і мають розширення *.txt*, файли web-документів мають розширення *.htm* або *.html*.

Web-документ містить інструкції для браузера. Результатом інтерпретації web-документа є web-сторінка. Web-сторінка, що відтворює web-документ у різних браузерах може мати різний вигляд.

Це зумовлено передусім відсутністю загальновизнаних стандартів і жорсткою конкуренцією виробників програмних продуктів. Наступною важливою причиною різного інтерпретування одного й того ж web-документа може бути різне налаштування системи і браузера на комп'ютері користувача. Проектуючи web-документ, слід враховувати по-можливості ці обставини.

До web-документа висувається ще низка вимог, пов'язаних з Internet як джерелом інформації. Передусім це стосується такої характеристики документу, як розмір файлу. Чим він менший, тим швидше сторінка завантажується в браузері, і тим більше шансів, що документ побачать багато

користувачів. Вважається, що документ повинен завантажуватись в браузері протягом 1-2 с. Про привабливість і зручність опублікованих в Internet web-документів повинен піклуватися їх автор.

## 5.2. Структура web-документів

Структура будь-якого HTML-документа однакова, а саме:

<code>&lt;HTML&gt;</code>	– відкриваючий тег документу
<code>&lt;head&gt;</code>	– відкриваючий тег заголовка документа
-----	– службова інформація про документ
<code>&lt;/head&gt;</code>	– закриваючий тег заголовка
<code>&lt;body&gt;</code>	– відкриваючий тег тіла документа
-----	– інформація про вміст документа
<code>&lt;/body&gt;</code>	– закриваючий тег тіла документа
<code>&lt;HTML&gt;</code>	– закриваючий тег документа

HTML-документ можна уявляти у вигляді контейнера, обмеженого тегами `<HTML>` та `</HTML>` (парний дескриптор, який не має атрибутів). Усередині цього основного контейнера знаходяться ще два контейнери чи секції. Перший контейнер, обмежений дескрипторами `<head>` та `</head>` – секція заголовку документу. У ньому розміщуються службові дані, які характеризують документ та окремі його особливості. Другий контейнер, обмежений дескрипторами `<body>` та `</body>` – тіло документу, де і міститься те, що згодом виводитиметься у вікні браузера.

## 5.3. Основні теги мови HTML

Мова HTML залишається основною мовою для створення web-документів. Вона не є повноцінною мовою програмування, та й процес створення web-документів дійсно більше нагадує процес його опису, ніж його програмування.

Під час класичного програмування мовами високого рівня процес відбувається за схемою наведеною на рисунку 5.1.



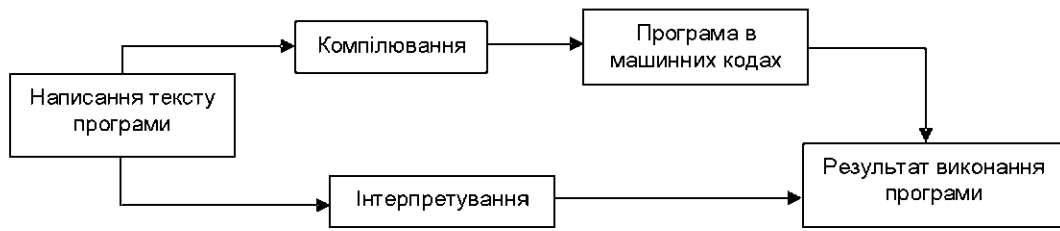


Рис.5.1. Загальна схема програмування мовами високого рівня

Написаний текст програми передається для обробки або за допомогою компілятора, або за допомогою інтерпретатора. У першому випадку отримуємо скомпільовану програму в машинних кодах (файл `.exe` або `.com`), у результаті виконання якого отримуємо результати роботи програми. У другому випадку текст програми відразу інтерпретується і виконується, в результаті чого маємо результати виконання програми.

В обох випадках результат виконання всіх операцій та процедур є передбачуваним, а будь-яка помилка, не передбачена програмою, спричинює зупинку її виконання та появу повідомлення про помилку.

У випадку роботи з web-документом його інтерпретатором може бути лише програма-браузер. Саме тут бачимо результати програмування – web-сторінку. Різні браузери можуть інтерпретувати один і той же код по-різному. Крім цього, помилки у програмі не призводять до зупинки, а лише до спотворення результатів її виконання. З огляду на ці обставини, результат інтерпретування Web-документа не є (і не може бути) однозначний, що ускладнює процес їх створення, якщо підходити до ідеології їх програмування з критеріями класичного програмування.

Якщо можна так висловитись, то програмування для Web значно «демократичніше» від класичного та орієнтоване на кінцевого користувача, тобто на потенційного адресата таких документів. Лише від користувача залежить, чи буде сторінка взагалі переглянута, в якому режимі її переглядатимуть і чи захочеться користувачеві переналаштувати свій комп'ютер, щоб побачити web-сторінку у найкращому вигляді.

Інструкціями в мові HTML є спеціальні конструкції – дескриптори чи теги, які мають наступний загальний формат:

`<ім'я [атрибути]>`

Відповідно зі специфікацією мови опису web-документів HTML, дескриптори можна писати як великими, так і малими буквами. Код web-документів можна писати підряд, без примусового виділення дескрипторів та їх атрибутів окремими рядками. Інтерпретація документа браузером від цього не залежить. Але для зручності автора і користувачів варто виокремлювати дескриптори великими літерами і візуально структурувати документ на секції, опис окремих абзаців, ілюстрацій, таблиць, опис інших об'єктів так, як це буде показано далі на прикладі.

Дескриптори керують способом відображення частин документа у вікні браузера. Дескриптори бувають парні і непарні. Парний дескриптор завжди має відкриваючий і закриваючий тег. Закриваючий тег має ту ж назву, що й відкриваючий. Закриваючий тег відрізняється від відкриваючого двома ознаками:

- закриваючий тег завжди починається з дробової риски, наприклад `</font>`;
- у закриваючому тегу не використовують ніяких атрибутів.

Непарні дескриптори не мають закриваючих тегів.

У заголовку документа (між тегами `<head>` та `</head>`) розміщуються щонайменше два дескриптори, а саме:

- `<title>Назва</title>` – парний дескриптор, в якому вказується назва Web-сторінки, яка буде з'являтися у верхньому рядку вікна програми-браузера (синій рядок вгорі активного вікна);
- `<meta [атрибути]>` – непарний дескриптор, атрибутами якого задається інформація про документ та його основні параметри: MIME, кодова таблиця, мова документу тощо.

Подальший розгляд питань, пов'язаних зі створенням Web-документів, буде супроводжуватись посиланнями на фрагменти коду документу intro.html, вигляд якого у вікні браузера Microsoft Edge наведено на рис.5.2.

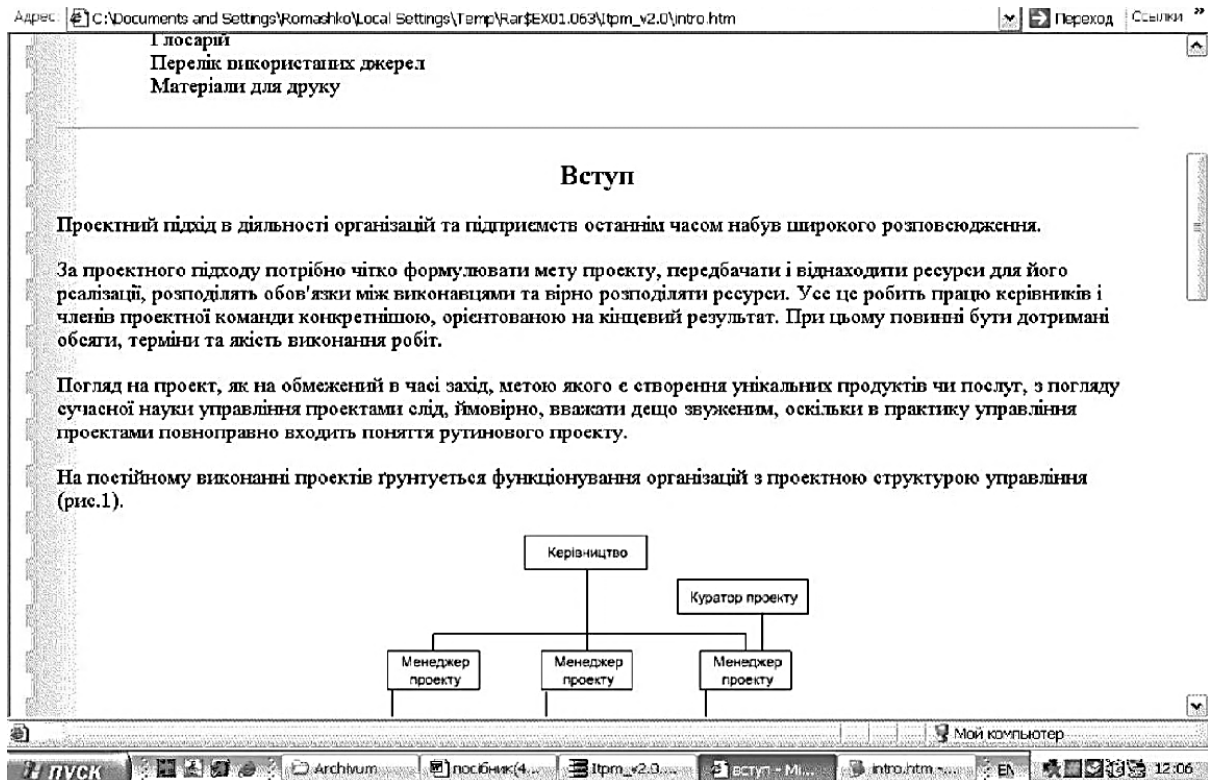


Рис.5.2. Вигляд документу intro.htm у вікні браузера Microsoft Edge

Фрагмент HTML-кода цього документа (частина, яку видно на рис. 5.2) наведено нижче.

```
<html>
  <head>
    <title>Вступ</title>
    <meta http-equiv="Content-Type" content="text/html;
charset=windows-1251">
    <link rel="stylesheet" href="itpm_v2.css" type="text/css">
  </head>
  <body bgcolor="#FFFFFF" text="#000000"
background="Images/backgr.jpg" leftmargin="4 0">
    <blockquote>
      <p>Глосарій<br>
```

Перелік використаних джерел<br>Матеріали для друку</p>

</blockquote> <hr>

<h2 align="center"> <a name="intro\_2"></a>Вступ</h2>

<p> <font size="4">Проектний підхід в діяльності організацій та підприємств останнім часом набув широкого розповсюдження.

</font></p>

<p><font size="4">За проектного підходу потрібно чітко формулювати мету проекту, передбачати і віднаходити ресурси для його реалізації, розподілять обов'язки між виконавцями та вірно розподіляти ресурси. Усе це робить працю керівників і членів проектної команди конкретнішою, орієнтованою на кінцевий результат. При цьому повинні бути дотримані обсяги, терміни та якість виконання робіт.

</font></p>

<p><font size="4">Погляд на проект, як на обмежений в часі захід, метою якого є створення унікальних продуктів чи послуг, з погляду сучасної науки управління проектами слід, ймовірно, вважати дещо звуженим, оскільки в практику управління проектами повноправно входить поняття рутинного проекту. </font></p>

<p><font size="4">На постійному виконанні проектів ґрунтується функціонування організацій з проектною структурою управління.

</font></p>

<p align="center"><font size="4"></font></p>

<p align="center"><font size="4">Рис. 1. Проектна структура управління </font></p>

.....

</body>

</html>

Як видно, в кодах документа, а саме в його заголовку:

<head>

```
<title>Вступ</title>
```

```
<meta http-equiv="Content-Type" content="text/html;  
charset=windows-1251">
```

```
<link rel="stylesheet" href="itpm_v2.css" type="text/css"> </head>
```

вказано, що назва сторінки – «Вступ» (дескриптор `<title>вступ</title>`); зміст документу є HTML-код web-сторінки, а в документі використовується кодова сторінка windows-1251 (дескриптор `<meta http-equiv="Content-Type" content="text/html; charset=windows-1251">`); під час інтерпретації документа в браузері слід враховувати правила оформлення елементів сторінки, викладені у файлі `itpm_v2.css`, який містить каскадну таблицю стилів (дескриптор `<link rel="stylesheet" href="itpm_v2.css" type="text/css">`). Дескриптором

```
<body bgcolor="#FFFFFF" text="#000000"  
background="Images/backgr.jpg" leftmargin="4 0">
```

починається тіло документа. У цьому дескрипторі вказано, що колір тла сторінки – `#FFFFFF` (білий), колір тексту на сторінці – `#000000` (чорний), тло тексту утворене малюнком `backgr.jpg`, який знаходиться в папці `Images/`, а ліве поле тексту на сторінці має розмір 40 пк (пікселів). Атрибути в дескрипторі `<body>` дійсні для усього документа за винятком тих фрагментів, параметри яких вказуються додатково безпосередньо біля них. Увесь текст на сторінці сформатований окремими абзацами, що вказується за допомогою дескриптора `<p>`, `</p>`, наприклад:

```
<p><font size="4"> За проектного підходу потрібно чітко формулювати мету проекту, передбачати і віднаходити ресурси для його реалізації, розподілять обов'язки між виконавцями та вірно розподіляти ресурси. Усе це робить працю керівників і членів проектної команди конкретнішою, орієнтованою на кінцевий результат. При цьому повинні бути дотримані обсяги, терміни та якість виконання робіт </font> </p>.
```

Кожний абзац починається з нового рядка, а попередній абзац відділяється від попереднього пустим рядком. Якщо потрібно почати наступний текст не з нового абзацу, а просто з нового рядка (без проміжків між

рядками), то використовують непарний дескриптор `<br>`, як це видно у наступному фрагменті:

```
<p>Глосарій<br>
```

```
Перелік використаних джерел<br>Матеріали для друку</p>
```

У дескрипторі `<p>...</p>` міститься дескриптор `<font>...</font>`, який дозволяє явно вказувати атрибути тексту, з врахуванням яких текст буде відображатись на екрані.

Дескриптор `<font>` може мати наступні атрибути:

- **face** – шрифт; звичайно використовують три типи шрифтів: із засічками – Times New Roman, прямий – Arial та пропорційний – Courier New. Назву шрифту слід писати в лапках;
- **size=розмір**; розмір шрифту можна вказувати в абсолютних (пікселі), умовних (позначення HTML) чи відносних (приріст) одиницях. Так, наприклад, атрибут `size="4"` вказує на те, що шрифт має умовний розмір 4. Всього в HTML використовується сім умовних розмірів шрифтів: від 1 до 7. Розмір 1 – найменший, розмір 7 – найбільший. Їх відображення у вікні браузера залежить від налаштувань браузера. Атрибут `size="12"` означав би, що шрифт повинен мати розмір 12 пікселів, а атрибут `size="+2"` вказує на те, що розмір шрифту на дві умовних одиниці більший, ніж розмір шрифту, прийнятий для документу за замовчуванням, або вказаний у дескрипторі `<body>`;
- **align=спосіб\_вирівнювання\_тексту**; таких способів є чотири:
  - `left` – вліво, `right` – вправо, `center` – на центр, `justified` – на ширину сторінки;
- **color=колір\_шрифту**; колір в документах HTML можна задавати двома способами: текстовим позначенням кольору (наприклад: `black`, `red`, `green`, `yellow`, `blue`, `magenta`, `cyan`, `white`) та шістнадцятковим позначенням кольору в системі RGB (Red-Green-Blue) у наступному форматі (див. рис.5.3):

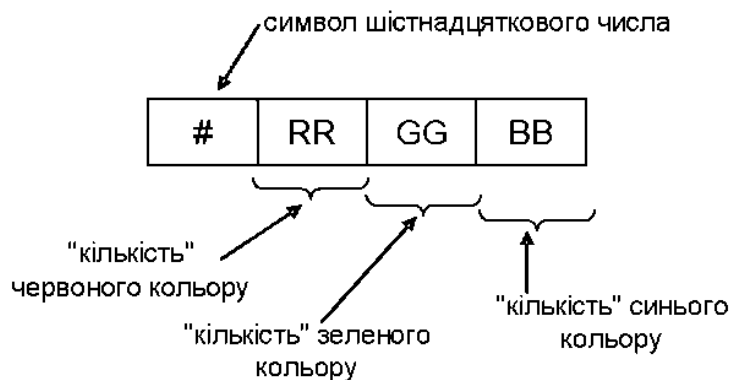


Рис. 5.3. Формат позначення кольору

У шістнадцятковій системі числення числа в кожному розряді позначаються цифрами від 0 до 9 і літерами латинського алфавіту від А до F. Найменше додатне двоцифрове шістнадцяткове число дорівнює #00 (00 у десятковій системі), а найбільше – #FF (255 у десятковій системі). Таким чином, для позначення білого кольору, який є результатом накладання усіх трьох кольорів максимальної яскравості у рівній «кількості» слід указати максимальну «кількість» для всіх трьох складових позначення кольору, тобто #FFFFFF. Для позначення чорного кольору, який утворюється внаслідок відсутності всіх складових, слід вказати мінімальну «кількість» всіх складових, тобто #000000. З подібних міркувань максимально яскравий червоний колір позначається як #FF0000, максимально яскравий зелений – як #00FF00 і максимально яскравий синій – як #0000FF. Усі інші кольори є комбінаціями трьох основних кольорів у різних пропорціях. Очевидно, що використання однакової «кількості» всіх кольорів меншої, ніж максимальна яскравості (наприклад #888888) означатиме сірий колір (у цьому випадку приблизно 50%).

Приклад використання дескрипторів <p>...</p>, <font>...</font> та <br> наведено у наступному фрагменті:

```
<h2 align="center"><a name="intro_2"></a>Вступ</h2>
```

```
<p><font size="4"> Проєктний підхід в діяльності організацій та підприємств останнім часом набув широкого розповсюдження </font></p>.
```

Продовжуючи розмову про форматування тексту, зазначимо, що стиль шрифту позначається дескрипторами стилів, а саме:

<B>Абзац, слово, символ</B> – **напівжирний шрифт**;

<I>Абзац, слово, символ</I> – *нахилений шрифт (курсив)*;

<U>Абзац, слово, символ</U> – підкреслений шрифт;

<S>Абзац, слово, символ</S> – ~~перекреслений шрифт~~.

Як і в інших подібних випадках, можливе комбінування цих дескрипторів, наприклад: шрифт, який знаходиться між дескрипторами <B><S>...</S></B> буде напівжирним перекресленим, а між дескрипторами <U><I>...</I></U> – нахиленим підкресленим.

Для форматування і виділення окремих елементів тексту призначені також наступні стандартні дескриптори HTML:

- від <h1>Текст</h1> до <h7>Текст</h7> – заголовки в тексті розміром від 1 до 7. З їх допомогою можна організувати семирівневу ієрархію заголовків у тексті;
- <big>Текст</big> – текст відображається більшого розміру, ніж решта тексту;
- <small>Текст</small> – текст відображається меншого розміру, ніж решта тексту;
- <sub>Текст</sub> – текст відображається як нижній індекс;
- <sup>Текст</sup> – <sup>текст</sup> відображається як верхній індекс;
- <code>Текст</code> – текст відображається як код або формула (найчастіше – шрифтом Courier);
- <tt>Текст</tt> – текст відображається моноширинним шрифтом;
- <kbd>Текст</kbd> – **текст** виводиться напівжирним моноширинним шрифтом;
- <var>Текст</var> – відображення змінних у формулі чи *тексті* (зазвичай – курсив);
- <cite>Текст</cite> – *текст* відображається як цитата (зазвичай Текст дрібніший курсив);



- `<address>Текст</address>` – *текст* відображається як адреса (зазвичай – курсив).

Переліченими вище дескрипторами не вичерпуються всі можливості форматування тексту. Як правило, потрібний вигляд сторінки досягається шляхом комбінованого використання різних дескрипторів та їх атрибутів. Докладне ознайомлення з ефектом використання різних дескрипторів та атрибутів (і не лише для форматування тексту) можливе лише в процесі практичного конструювання Web-документа, перевірки способів інтерпретування HTML-коду в різних браузера за умови різних налаштувань браузера та пошук власних методів і підходів до конструювання Web-документів.

Наступний об'єкт, який часто розміщується у Web-документах, – це різні малюнки. Для їх розміщення в документ використовують непарний дескриптор `<img>` з атрибутами.

Приклад використання цього атрибуту наведено у наступному фрагменті:

```
<p align="center"><font size="4"></font></p>
```

У дескрипторі `<img>` обов'язково повинен бути атрибут `src="повне_ім'я_файла"` із зазначенням адреси, за якою знаходиться малюнок, який розміщується у Web-документі. Так у наведеному фрагменті зображення вставляється з файлу `0_1.gif`, який знаходиться в папці `Images/`. Крім цього в атрибутах дескриптора можуть вказуватись наступні параметри:

- `width=ширина` – ширина малюнка в пікселях або відсотках від ширини сторінки;
- `height=висота` – висота малюнка в пікселях;
- `hspace="розмір"` – відстань по горизонталі до оточуючого тексту в пікселях;
- `vspace="розмір"` – відстань по вертикалі до оточуючого тексту в пікселях;
- `border="товщина"` – товщина видимої рамки зображення в пікселях, або

відсутність рамки (`border="0"`);

- `align="вирівнювання"` – вирівнювання малюнка на сторінці.

Дуже важливим елементом на Web-сторінці є гіперпосилання, яким може бути довільний об'єкт на ній (текст, символ, малюнок тощо).

Дескриптор гіперпосилання має наступний формат:

```
<A href="URL_об'єкту[#закладка]>Текст</A>
```

У відкриваючому тегові `<A>` атрибутом `href=` задається адреса (URL) тієї сторінки (або того місця на сторінці, якщо вказана назва закладки на ній `#закладка`), яку треба завантажити в браузер, коли гіперпосилання активується. На сторінці текстове гіперпосилання за замовчуванням – виділяється синім кольором і підкреслюванням. Якщо встановити курсор на гіперпосилання і один раз клацнути лівою кнопкою миші, то сторінка, URL якої вказаний у гіперпосилання, буде завантажена в браузер.

Якщо як гіперпосилання використовується малюнок, то відповідний фрагмент HTML-коду може мати наступний вигляд:

```
<p><a href="intro.htm"></a></p>
```

Тут гіперпосилання на документ `intro.htm` зроблене з малюнка `Images/02.gif`, який розміщений в документі дескриптором ``; малюнок має розміри 70x109 пікселів і не має рамки.

Наступним об'єктом, що використовується у Web-документах є таблиці.

Таблиця описується складною щонайменше трирівневою ієрархічною конструкцією з дескрипторів `<TABLE>...</TABLE>`, `<TR>...</TR>` та `<TD>...</TD>`. Перша пара тегів описує таблицю в цілому, друга – рядок таблиці, а третя – комірки таблиці. Проілюструємо сказане на прикладі.

Припустимо, в документі потрібно розмістити таку таблицю:

1	2	3
4	5	6

Фрагмент HTML-коду з описом цієї таблиці матиме вигляд:

```
<TABLE border="1">  
  <TR>  
    <TD>1</TD>  
    <TD>2</TD>  
    <TD>3</TD>  
  </TR>  
  <TR>  
    <TD>4</TD>  
    <TD>5</TD>  
    <TD>6</TD>  
  </TR>  
</TABLE>
```

} Опис комірок першого  
рядка таблиці

} Опис комірок другого  
рядка таблиці

У дескрипторах опису таблиці в цілому та елементів таблиці (рядків, комірок) можна вказувати атрибути, які задають параметри шрифту, кольорового оформлення, параметри абзаців тощо для цих елементів, або для всієї таблиці.

Таблиці використовують не лише як окремі об'єкти на сторінці, але й як спосіб впорядкування площі сторінки загалом. Так, наприклад, використовуючи таблицю, можна поділити сторінку на декілька незалежних із погляду оформлення й форматування полів. Приклад такого розподілу наведено на рис.5.4.

Поле меню 1	реклама, рухома стрічка	Поле меню 2
	Заголовок сторінки	
	Суть сторінки	
	меню 3	
	банери, реклама	

Рис. 5.4. Приклад розподілу сторінки на поля за допомогою таблиці

Рамки таблиці в цьому випадку повинні бути невидимі, тобто, дескриптор таблиці міститиме атрибут "border" і матиме вигляд

```
<TABLE border=0>
```

Викладеним вище не обмежуються всі можливості мови HTML, яка і далі розвивається й удосконалюється.

#### 5.4. MIME-типи документів

У заголовку web-документа є поле Content-Type, в якому вказується тип документів, які можуть правильно (коректно) інтерпретуватись клієнтом та передаватись сервером.

Специфікація MIME (Multipurpose Internet Mail Extension – багатоцільове поштове розширення Internet) початково була розроблена для забезпечення можливості передавання файлів різних форматів засобами електронної пошти. Згодом цю специфікацію почали активно використовувати для обміну будь-якими даними в мережах, і зараз вона стала невід’ємною частиною правил роботи в Internet.

До появи MIME з комп’ютера на комп’ютер передавали виключно текстову інформацію. Для передавання зображень чи інших двійкових файлів використовували протокол FTP.

Відповідно зі специфікацією MIME для опису формату даних використовується тип і підтип. Тип позначає, до якого класу відноситься

формат вмісту запиту або відповіді. Підтип уточнює цю інформацію. Тип і підтип відділяють один від одного дробовою рискою:

тип/підтип

Приклади позначення поширених типів форматів файлів наведені в табл.5.1.

Таблиця 5.1

### Приклади позначення поширених типів форматів файлів

MIME-типи <sup>1</sup>		
Тип/підтип	Розширення файлів	Опис
application/pdf	.pdf	Документ, призначений для обробки програмою Acrobat Reader
application/msexcel	.xls	Документ у форматі Microsoft Excel
application/postscript	.ps, .eps	Документ у форматі PostScript
application/x-tex	.tex	Документ у форматі TeX
application/msword	.doc	Документ у форматі Microsoft Word
application/rtf	.rtf	Документ у форматі RTF; обробляється програмою Microsoft Word
image/gif	.gif	Зображення у форматі GIF (векторна графіка)
image/jpeg	.jpg, .jpeg, .jpe	Зображення у форматі JPEG (растрова графіка)
image/tiff	.tiff, tif	Зображення у форматі TIF (растрова графіка)
image/x-xbitmap	.xbm	Зображення у форматі XBitmap (растрова графіка)
text/plain	.txt	ASCII-текст
text/html	.html, .htm	Документ у форматі HTML
audio/midi	.midi, .mid	Аудіо файл у форматі MIDI

<sup>1</sup> **MIME тип** – код, який визначає формат файлу або тип контенту, що передається мережею Інтернет. Складається з двох частин. Коди визначає та офіційно оприлюднює тільки IANA (IANA (Адміністрація адресного простору Інтернет) – американська організація, що керує просторами IP-адрес, доменів верхнього рівня, а також реєструє типи даних MIME і параметри інших протоколів Інтернету. MIME типи спочатку були визначені електронної пошти та вкладень. З часом, MIME типи почали використовувати в інших протоколах, таких як HTTP, та в форматах документів, таких як HTML, XML тощо, у RFC 2045 у листопаді 1996 року, як частина MIME специфікації, для визначення типу вмісту повідомлень

Тип/підтип	Розширення файлів	Опис
audio/x-wav	.wav	Аудіо файл у форматі WAV
message/rfc822		Поштове повідомлення
message/news		Повідомлення з групи новин
video/mpeg	.mpeg, .mpg, .mpe	Відеофрагмент у форматі MPEG
video/avi	.avi	Відеофрагмент у форматі AVI

### 5.5. Програмне забезпечення для створення web-документів

Розробка веб-сторінок може здійснюватися з використанням різних засобів:

- текстових редакторів, у середовищі яких користувач може вводити текст і теги. Для цього можна використовувати текстові редактори Блокнот, Edit Plus, Homesite, HTML Pad та ін. Готову сторінку потрібно зберегти та надати розширення імені файлу htm або html. Створення веб-сторінки такими засобами передбачає обов'язкове знання мови розмітки гіпертекстів, наприклад HTML. Усю роботу з добору тегів розробник виконує власноруч. Розробка сторінки здійснюється повільно, але завдяки невеликому розміру файлу, у якому вона зберігається, така сторінка швидко завантажується та відкривається у вікні браузера;

- прикладних програм загального призначення, наприклад з пакета Microsoft Office, які можуть зберігати файли у форматі HTML. Як ви вже знаєте, документи, створені в програмах Word, PowerPoint, Publisher та інших, можна зберігати, вибравши тип файлу Веб-сторінка (\*.htm, \*.html). При цьому створюються веб-сторінки, у яких застосування тегів для розмітки відбувається автоматично. Розробнику не потрібно знати мову розмітки гіпертексту. Але файли, у яких зберігаються такі сторінки, мають набагато більший обсяг, ніж файли, створені в текстових редакторах. Причиною є велика

кількість тегів, які описують структуру і форматування документа та дублюються під час застосування до кожного окремого елемента сторінки;

- спеціалізованих веб-редакторів – програм, що призначені для розробки веб-сайтів. Популярними веб-редакторами є Adobe Dreamweaver, Microsoft FrontPage, SharePoint Designer, WYSIWYG Web Builder, KompoZer та ін. Ці програми мають додаткові засоби для створення статичних і динамічних веб-сторінок, при цьому не вимагають від розробника знання мови HTML. Такі програми називають WYSIWYG-редакторами (англ. **What You See Is What You Get** – що ви бачите, то ви й отримуєте), створена їхніми засобами веб-сторінка виглядатиме так, як вона сконструйована в редакторі. HTML-код сторінки більш коректний, ніж під час використання, наприклад програм пакета Microsoft Office, але теж надлишковий;

- систем управління веб-контентом WCMS (англ. **Web Content Management System** – система управління веб-контентом), які надають користувачам зручні інструменти для керування текстовим і графічним наповненням веб-сайтів, додавання та видалення статей з інформаційними матеріалами, створення системи навігації веб-сайтів та ін. Популярними WCMS є системи Joomla, Wordpress, Drupal, MediaWiki, Mambo, NUKE та ін. Системи управління вмістом веб-сайтів пропонують набори шаблонів оформлення веб-сторінок і модулів, що роблять сайт динамічним: форумів, чатів, стрічок новин, каталогів файлів, контролю статистики тощо.

Названі засоби створення веб-сайтів можна встановити на локальному комп'ютері. Створені в їх середовищі веб-сторінки після завершення процесу розробки потрібно опублікувати в Інтернеті. У той самий час існують WCMS, які одночасно з послугами з розробки веб-сайтів надають послуги безкоштовного хостингу. Такими є системи uCoz, Google Sites, Prom.ua, Ua7.biz та ін. У цих системах створення веб-сайту здійснюється в режимі онлайн відразу на сервері хостингу.

Найпростіші web-сторінки можна конструювати «вручну», пишучи код у довільному текстовому редакторі як, наприклад, NotePad у Windows.

Написаний таким чином код потрібно зберегти у файлі з розширенням .htm або .html.

Складніші web-сторінки, або їх набори створюються за допомогою спеціально розроблених Web-редакторів.

Створення web-документів шляхом написання його коду у текстовому редакторі має ту велику перевагу, що дає чистий, компактний код, розмір якого є мінімально можливий для документу. Розміру документу – це той критерій, за яким визначається час завантаження сторінки в браузер. Час завантаження сторінки в браузер об'єктивно впливає на відвідуваність сторінки із-за зручності її перегляду навіть у мережах з низькими технічними показниками (як, наприклад, вузькою смугою пропускання та малою швидкістю передавання). Як відомо, у глобальних мережах швидкість передавання залежить в основному від технічних характеристик каналів зв'язку – ліній та лінійного обладнання.

Однак «ручне» створення складної за змістом і оформленням інтерактивної web-сторінки за умови використання в ній багатьох різних об'єктів (таблиці, малюнки, армовані об'єкти, відеофрагменти, форми, інші активні об'єкти) справа складна як для непрофесіонала, та і для професійного Web-дизайнера.

Тому в багатьох випадках кінцеві користувачі використовують під час конструювання web-документів спеціальні редактори, які дозволяють в значній мірі спростити роботу, автоматизуючи процес написання коду сторінки маючи її вигляд. Конструювання web-сторінки в такому редакторі відбувається практично в режимі її перегляду, коли її елементи мають майже такий вигляд, який вони мали б у браузері. Коди документа генеруються редактором автоматично. За необхідності коди можна відредагувати вручну, в режимі редагування кодів.

Одним з найпоширеніших програмних продуктів такого призначення є web-редактор Dreamweaver, розроблений фірмою Macromedia. Крім нього у комплекті програмних продуктів є також редактор анімованої графіки Flash,



редактор векторної графіки FreeHand і редактор растрової графіки Firework. Цей комплект дозволяє створювати дуже складні і насичені інтерактивні web-сторінки з мінімальними затратами сил і часу на виконання рутинних процедур.

Одна з останніх версій цього комплекту програмних продуктів має позначення MX, хоча складові цього комплекту мають різні версії.

На рис. 5.5 наведено вигляд вікна редактора Dreamweaver (русифікована версія) із документом, що в ньому редагується.

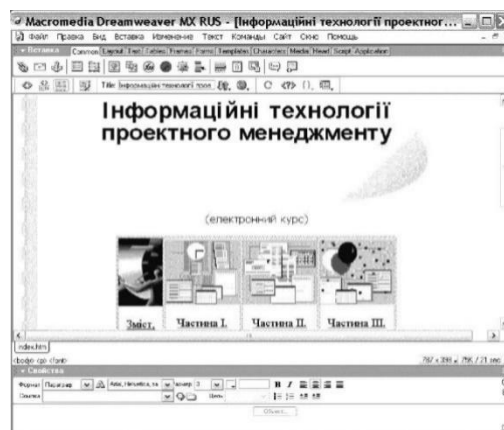


Рис. 5.5. Вікно редактор Dreamweaver у режимі дизайну web-сторінки

На рис. 5.6 наведено вигляд вікна того ж редактора в режимі редагування кодів документа.

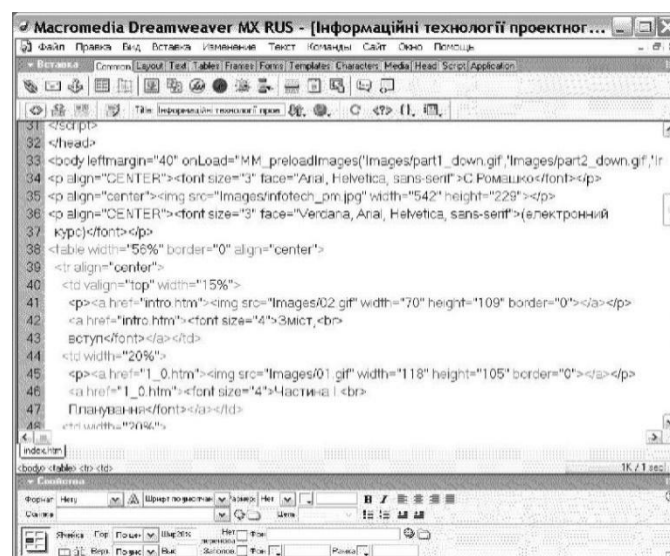


Рис. 5.6. Вікно редактор Dreamweaver в режимі редагування кодів

Зручний, знайомий кожному користувачеві Windows, інтерфейс, додаткові панелі інструментів і властивостей об'єктів, розвинена система контекстної допомоги (щоправда, англійською), роблять його надзвичайно простим у використанні й зручним інструментом для конструювання складних Web-документів.

Для створення Web-документів можна використовувати текстові заготовки у форматах .doc та .rtf, імпортуючи їх безпосередньо у документ, що створюється.

Редагований документ можна переглядати у двох різних браузерах.

Редактор дозволяє відносно просто розробляти власні *web-сайти* – набори взаємопов'язаних Web-документів, присвячених одній темі, тобто реалізовувати web-проекти.

Звідси ж, із редактора, можна без зайвих зусиль опублікувати свій твір в Internet.

Ще одним Web-редактором, доступним кожному кінцевому користувачу, який володіє навичками роботи з продуктами з пакету MS Office, є редактор Front Page.

У комплекті MS Office поставляється повна версія цього продукту – Front Page, а в комплекті Windows – спрощена його версія Front Page Express.

Можливості цього редактора такі ж, як і у Dreamweaver, але Front Page претензійно орієнтований на інтегрування з усіма іншими продуктами пакету MS Office та браузером Internet Explorer, що інколи заважає розробці документів, призначених для однакового інтерпретування будь-яким браузером.

Зазначимо, що кожний з продуктів пакету MS Office дозволяє зберегти редагований документ у форматі HTML, створивши таким чином web-документ взагалі без жодних додаткових зусиль. Тут, однак, слід мати на увазі наступне.

У кожному з перелічених спеціальних редакторів, або в програмах пакету MS Office можна створити однакові за своїм виглядом Web-документи, але вони сильно відрізнятимуться один від одного розміром кодів. Найменший і

найчистіший код ми отримали б за допомогою Dreamweaver, дещо більший і з багатьма зайвими тегами – за допомогою Front Page. Найбільший і найнелогічніший із-за багатьох повторень і невиправданих уточнень код отримується, наприклад, за допомогою MS Word. Код, отриманий з редактора Word, у 2-3 рази за обсягом перевищуватиме код такого ж документу, отриманого за допомогою редактора Dreamweaver. За інших рівних обставин такий документ у 2-3 рази довше завантажуватиметься в браузері, а редагувати його коди вручну – вкрай складно.

Цим і зумовлена порада використовувати для конструювання складних і великих Web-документів переважно спеціалізовані редактори.

### **Запитання для перевірки знань**

1. Що таке гіперпосилання?
2. Що таке гіпертекст?
3. Що таке web-документ?
4. Для чого призначена програма-браузер?
5. Що таке web-вузол (web-сайт)?
6. Яка структура простого web-документа?
7. Для чого призначена мова HTML?
8. Що таке тег? Назвіть теги які ви знаєте.
9. Які параметри може мати тег BODY?
10. Який тег позначає початок нового абзацу?
11. Які теги позначають напівжирне, курсивне і підкреслене накреслення шрифту?
12. Які теги призначені для вирівнювання елементів на сторінці?
13. Яке призначення тега FONT?
14. Яких значень можуть набувати параметри тега FONT?
15. Які є типи списків?
16. Як створити маркований список?
17. Як створити нумерований список?

18. Як створити список означень?
19. Яке призначення тега TABLE?
20. Які параметри може мати тег TABLE?
21. Які теги формують у таблиці рядки, комірки-заголовки і звичайні комірки?
22. Як у таблиці об'єднати декілька комірок в одну?
23. Який параметр використовують для вирівнювання елементів? Яка особливість пари тегів <PRE>...</PRE>?
24. Як вставити графічне зображення у web-сторінку?
25. Як вставити відеофільм у web-сторінку?
26. Які параметри може мати тег IMG?
27. За допомогою якого тега вставляють гіперпосилання?
28. Яке призначення параметрів LINK, VLINK, ALINK?
29. Як деяке графічне зображення зробити гіперпосиланням? Які є види покликань у межах одної web-сторінки?
30. Як створити динамічний ефект рухомого тексту?
31. Які ви знаєте параметри рухомого тексту?

## СПИСОК ВИКОРИСТАНОЇ ТА РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Азарова А. О., Лисак Н. В. Комп'ютерні мережі та телекомунікації : навч. посіб. Вінниця : ВНТУ, 2012. 293 с. URL: <https://press.vntu.edu.ua/index.php/vntu/catalog/download/208/379/413-1?inline=1> (дата звернення: 15.11.2021).
2. Безкоровайний В., Русскін В. Багатокритеріальна Оптимізація топологічних структур корпоративних комп'ютерних мереж. *Інформаційні системи та технології* : матеріали статей 9-ї Міжнар. наук.-техн. конф., 17-20 листоп. 2020 р. Харків : ХНУРЕ, 2020. С. 23-24.
3. Безкоровайний В. В., Русскін В. М. Оптимізація корпоративних комп'ютерних мереж на етапі реінжинірингу. *Інформаційні технології та комп'ютерне моделювання* : матеріали Міжнар. наук.-практ. конф., 5-10 лип. 2021 р. Івано-Франківськ. С.134-136.
4. Буров Є. Комп'ютерні мережі. Львів: БаК, 1999. 468 с. URL: <http://194.44.152.155/elib/local/sk629495.pdf> (дата звернення: 04.12.2021).
5. Волосюк Ю. В. Комп'ютерні мережі : курс лекцій. Миколаїв : МНАУ, 2019. 203 с. URL: [https://dspace.mnau.edu.ua/jspui/bitstream/123456789/6377/1/Kompiuterni\\_merezhi\\_kurs\\_lektsii.pdf](https://dspace.mnau.edu.ua/jspui/bitstream/123456789/6377/1/Kompiuterni_merezhi_kurs_lektsii.pdf).
6. Городецька О. С., Гикавий В. А., Онищук О. В. Комп'ютерні мережі : навчальний посібник. Вінниця : ВНТУ, 2017. 129 с. URL: [http://pdf.lib.vntu.edu.ua/books/IRVC/2021/Gorodetska\\_2017\\_129.pdf](http://pdf.lib.vntu.edu.ua/books/IRVC/2021/Gorodetska_2017_129.pdf) (дата звернення: 04.12.2021).
7. Загальні положення теорії комп'ютерних мереж. URL: <http://flame.nm.ru/d2.htm> (дата звернення: 15.11.2021).
8. Комп'ютерні мережі : навч. посіб. / Азаров О. Д., Захарченко С. М., Кадук О. В. та ін. Вінниця : ВНТУ, 2013. 371 с.
9. Комп'ютерні мережі : навч. посіб. / Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Львів : «Магнолія 2006», 2013. 256 с. URL: [http://elartu.tntu.edu.ua/bitstream/123456789/16930/5/Mykytyshyn\\_A\\_G\\_Mytnyk\\_M\\_M\\_Kompiuterni\\_merezhi\\_Knyga\\_1.pdf](http://elartu.tntu.edu.ua/bitstream/123456789/16930/5/Mykytyshyn_A_G_Mytnyk_M_M_Kompiuterni_merezhi_Knyga_1.pdf) (дата звернення: 04.12.2021).

10. Комп'ютерні мережі. URL: [http://comp-net.at.ua/index/topologija\\_komp\\_3\\_9\\_juternikh\\_merezh/0-6](http://comp-net.at.ua/index/topologija_komp_3_9_juternikh_merezh/0-6) (дата звернення: 04.12.2021).
11. Комп'ютерні мережі. URL: <https://sites.google.com/site/kmposibnyk/home> (дата звернення: 04.12.2021).
12. Комп'ютерні мережі: навч. посібник / А. І. Блозва, Ю. В. Матус, В. В. Смолій, Б. С. Гусєв, Д. Ю. Касаткін, Т. Ю. Осипова, Я. А. Савицька. Київ : Компрінт, 2017. 821 с. URL: [https://nubip.edu.ua/sites/default/files/u34/posibnik\\_-\\_kompyuterni\\_merezhi.pdf](https://nubip.edu.ua/sites/default/files/u34/posibnik_-_kompyuterni_merezhi.pdf) (дата звернення: 04.12.2021).
13. Комп'ютерні мережі. Конспект лекцій / укл.: Зав'ялець Ю. А. Чернівці, 2015. 183 с.
14. Коротка історія розвитку Інтернету. URL: [http://b-ko.com/book\\_16\\_glava\\_7\\_Kоротка\\_історія\\_.html](http://b-ko.com/book_16_glava_7_Kоротка_історія_.html) (дата звернення: 15.11.2021).
15. Ромашко С.М. Конспект лекцій з дисципліни «Комп'ютерні мережі і телекомунікації». Львів: ЛРІДУ НАДУ, 2006. 61 с. URL: <http://www.lim.lviv.ua/files/konspectlec/romashko/KMT.pdf> (дата звернення: 04.12.2021).
16. Тарнавський Ю. А., Кузьменко І. М. Організація комп'ютерних мереж : підручник: для студ. спеціальності 121 «Інженерія програмного забезпечення» та 122 «Комп'ютерні науки» / КПІ ім. Ігоря Сікорського ; Електронні текстові дані (1 файл: 45,7 Мбайт). Київ: КПІ ім. Ігоря Сікорського, 2018. 259 с. URL: [https://ela.kpi.ua/bitstream/123456789/25156/1/Tarnavsky\\_Kuzmenko\\_Org\\_Komp\\_merej.pdf](https://ela.kpi.ua/bitstream/123456789/25156/1/Tarnavsky_Kuzmenko_Org_Komp_merej.pdf) (дата звернення: 04.12.2021).
17. Технології WEB-програмування : курс лекцій / уклад. Русскін В. М.: Комунал. заклад «Харків. гуманіт.-пед. академія» Харків. обл. ради. Харків, 2019. 130 с.

## **ПІСЛЯМОВА**

Представлені у виданні теоретичні відомості можуть бути застосовані на практиці під час виконання лабораторних, практичних і самостійних робіт, а також під час проходження педагогічної практики.

*Навчальне видання*

Укладачі:  
**РУССКІН Володимир Михайлович**  
**ХМІЛЬ Наталія Анатоліївна**

## **КОМП'ЮТЕРНІ МЕРЕЖІ, ІНТЕРНЕТ-ТЕХНОЛОГІЇ**

Курс лекцій для здобувачів освітнього рівня «бакалавр»  
зі спеціальності 014.09 Середня освіта (Інформатика)

За достовірність викладеного матеріалу відповідають укладачі

Друкується в авторській редакції