

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ**

**Харківський національний університет внутрішніх справ**

**Факультет № 4**

**Кафедра інформаційної безпеки**

**ТЕКСТ ЛЕКЦІЇ**

**з дисципліни “ Комп’ютерні мережі та засоби телекомунікації ”  
на тему:**

**Інтегрована технологія**

**Галузь знань - 1701 - „Інформаційна безпека”**

**Напрямок підготовки - 6.170102 - „Системи технічного захисту  
інформації “**

**Ступінь вищої освіти - бакалавр**

**м. Харків  
2016 рік**

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ**

**Харківський національний університет внутрішніх справ**

**Факультет №4**

**Кафедра інформаційних технологій**

**ТЕКСТ ЛЕКЦІЇ**

з навчальної дисципліни «Комп'ютерні мережі»

вибірковий компонент освітньої програми  
першого бакалаврського рівня вищої освіти

**за темою Internet/Intranet технології**

**Спеціальність – 125 «Кібербезпека»(безпека інформаційних та  
комунікаційних систем )**

**м. Харків**

**2019**

## ПЕРЕДМОВА

### ЗАТВЕРДЖЕНО

Науково-методичною радою ХНУВС  
Протокол від \_\_\_\_\_ № \_\_\_\_\_  
(дата, місяць, рік )

### СХВАЛЕНО

Вченою радою факультету № 4  
Протокол від \_\_\_\_\_ № \_\_\_\_\_  
(дата, місяць, рік )

### ПОГОДЖЕНО

Секцією Науково-методичної ради  
ХНУВС з технічних дисциплін  
Протокол від \_\_\_\_\_ № \_\_\_\_\_  
(дата, місяць, рік )

Розглянуто на засіданні кафедри інформаційних технологій факультету № 4  
(*протокол від 15.01.2019р. №4*)

### Розробники:

1. професор кафедри інформаційних технологій факультету № 4 доктор технічних наук, професор Можаяєв О.О.
2. доцент кафедри інформаційних технологій факультету № 4 кандидат технічних наук, професор Можаяєв М.О.

### Рецензенти:

1. **Зацеркляний М.М.**, доктор технічних наук, професор;
2. **Серков О.А.**, доктор технічних наук, професор завідувач кафедрою системи інформації Національного технічного університету «Харківський політехнічний інститут»

## Лекція 4. Internet/Intranet технології

### План лекції

1. Інтернет
2. Стек протоколів TCP/IP
3. Адресація в мережах TCP/IP
4. Система доменних імен DNS

### Література

1. Антонов В. М. Сучасні комп'ютерні мережі / Валерій Миколайович Антонов. - К. : МК-Прес, 2005. - 480 с.
2. Валецька Т. М. Комп'ютерні мережі. Апаратні засоби: навч. посіб. для студ. вищ. навч. закл. / Тетяна Михайлівна Валецька. - К. : Центр навчальної літератури, 2004. - 208 с.
3. Жуков І. А. Комп'ютерні мережі та технології: навч. посіб. для студ. вищих навч. закл. / Жуков І. А., Гуменюк В. О., Альтман І. Є.. - К. : НАУ, 2004. - 276 с. - (Комп'ютерні технології).
4. Компьютеры, сети, Интернет: Энциклопедия: Наиболее полн. и подроб. рук. / Ю. Новиков, Д. Новиков, А. Черепанов, В. Чуркин; Под общ. ред. Ю. Новикова. - 2. изд. - М. [и др.]: Питер, 2003 (СПб.: ГПП Печ. Двор им. А.М. Горького). - 831 с.: ил.; 24 см.
5. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебное пособие для студентов вузов, обучающихся по направлению "Информатика и вычислительная техника" и по специальностям "Вычислительные машины, комплексы, системы и сети", "Автоматизированные машины, комплексы, системы и сети", "Программное обеспечение вычислительной техники и автоматизированных систем" / В. Олифер, Н. Олифер. - 4-е изд. - Москва [и др.]: Питер, 2010. - 943 с.: ил.; 24 см. - (Учебник для вузов).
6. Олифер В. Г. Новые технологии и оборудование IP-сетей / Виктор Олифер, Наталья Олифер. - СПб. и др.: BHV, 2000. - 512 с.: ил., табл.; 24 см. - (Мастер) (Современные сетевые технологии).
7. Таненбаум Э. Компьютерные сети / Э. Таненбаум ; [пер. с англ. В. Шрага]. - 4-е изд. - М. [и др.]: Питер, 2005. - 991 с.: ил., табл.; 24 см. - (Классика computer science).
8. Ретана А. Принципы проектирования корпоративных IP-сетей: Основополагающие принципы построения масштабируемых IP-сетей: Экзамен на получение квалификации сертифиц. специалиста по межсетевому обмену CISCO / Альваро Ретана, Дон Слайс, Расс Уайт; [Пер. с англ. и ред. А.В. Журавлева]. - М. [и др.]: Вильямс, 2002. - 367 с.: ил.; 24 см. - (Сертифицированный специалист по межсетевому обмену CISCO).
9. Руководство по технологиям объединенных сетей: [настол. справ. специалиста по сетевым технологиям] / Cisco Systems, Inc. ; [пер. с англ. и ред. А.Н. Крикуна]. - 4-е изд. - М. [и др.]: Вильямс, 2005 (СПб.: ГПП Печ. Двор). - 1033 с.: ил., табл.; 24 см.

### 1. Інтернет

Інтернет - це найбільша у світі мережа, що не має єдиного центру управління, але працює за єдиними правилами і надає своїм користувачам єдиний набір послуг. Інтернет можна розглядати як "мережу мереж", кожна з яких управляється незалежним оператором - постачальником послуг інтернет (ISP, Internet Service Provider).

З точки зору користувачів, інтернет є набором інформаційних ресурсів, розосереджених по різних мережах, включаючи ISP-сети, корпоративні мережі, мережі і окремі комп'ютери домашніх користувачів. Кожен окремий комп'ютер в даній мережі називається хостом (від англ. host).

Сьогоднішній інтернет зобов'язаний своїй появі об'єднаній мережі ARPANET, яка починалася як скромний експеримент у новій тоді технології комутації пакетів (табл. 4.1). Мережа ARPANET була розгорнута в 1969 р. і складалася спочатку з чотирьох вузлів з комутацією пакетів, використовуваних для взаємодії невеликої кількості хостів і терміналів. Перші лінії зв'язка, що сполучали вузли, працювали на швидкості всього 50 Кбіт/с. Мережа ARPANET фінансувалася управлінням перспективного планування науково-дослідних робіт ARPA (Advanced Research Projects Agency) міністерства оборони США і призначалася для вивчення технології і протоколів комутації пакетів, які могли б використовуватися для кооперативних розподілених обчислень.

Таблиця 14.1 Хронологія розвитку інтернет (з 1966 по 2000 р.)

Рік	Подія
1966	Експеримент з комутацією пакетів управління ARPA
1969	Перші працездатні вузли мережі ARPANET
1972	Винахід розподіленої електронної пошти
1973	Перші комп'ютери, підключені до мережі ARPANET за межами США
1975	Мережа ARPANET передана у ведення управління зв'язку міністерства оборони США
1980	Починаються експерименти з TCP/IP
1981	Кожні 20 днів до мережі додається новий хост
1983	Завершений перехід на TCP/IP
1986	Створена магістраль NSFnet
1990	Мережа ARPANET припинила існування
1991	Поява Gopher
1991	Винахід Усесвітньої павутини. Випущена система PGP. Поява Mosaic
1995	Приватизація магістралі інтернет
1996	Побудована магістраль OC-3 (155 Мбіт/с)
1998	Кількість зареєстрованих доменних імен перевищило 2 млн
2000	Кількість індексованих Web-сторінок перевищила 1 млрд

У 2000 р. нараховувалося близько 327 млн користувачів, з них тільки в США чисельність перевищувала 100 млн чоловік.

У 2004 р. інтернет нараховував 700 млн користувачів, і найближчим часом їхня кількість зросте до 1 млрд. Кількість сайтів, що складало в 1993 р. 26 тис., сьогодні перевищує 5 млн.

На рис. 14.1 наведено графік, що показує динаміку зростання кількості хостів (формально зареєстрованих - верхня крива, активно діючих - нижня крива).

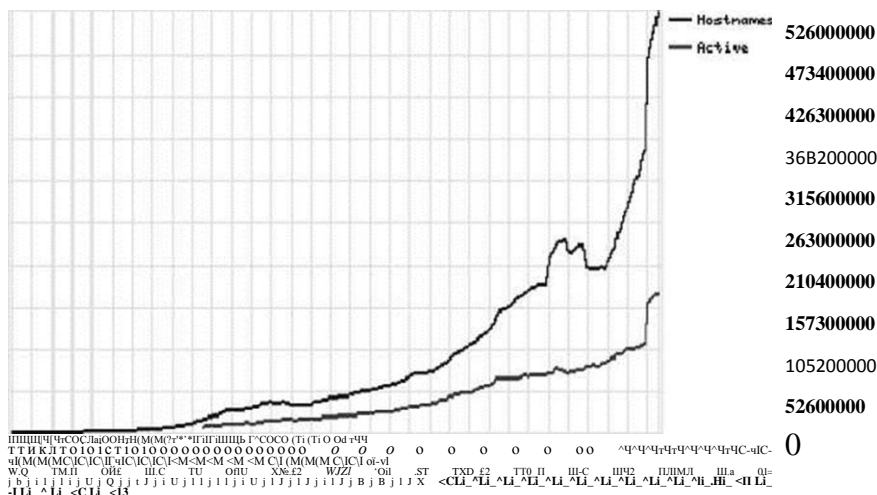


Рис. 14.1. Динаміка зростання кількості хостів в інтернет [[www.netcraft.com](http://www.netcraft.com)]

Централізоване управління в такій глобальній мережі неможливе, оскільки, по-перше, дана мережа є транснаціональною і, по-друге, через історичні передумови її формування.

Проте в інтернеті можуть виявлятися опосередковані форми централізації у формі єдиної технічної політики, погодженому наборі технічних стандартів, призначенні імен і адрес комп'ютерів і мереж, що входять в інтернет. Тобто інтернет є децентралізованою мережею і має переваги та недоліки.

Переваги: легкість нарощування інтернет шляхом укладення договору між двома ISP.

Недоліки:

- складність модернізації технологій і послуг інтернет, оскільки потрібні погоджені зусилля всіх постачальників послуг;
- невисока надійність інтернет-послуг;
- відповідальність за працездатність окремих сегментів цієї мережі покладається на постачальників інтернет-послуг.

Типи постачальників інтернет-послуг:

- просто постачальник інтернет-послуг виконує транспортну функцію для кінцевих користувачів - передачу їх трафіку в мережі інших постачальників послуг інтернет;
- постачальник інтернет-контента має власні інформаційно-довідкові ресурси, надаючи їх вміст у вигляді Web-сайтів;
- постачальник послуг хостингу надає свої приміщення, канали зв'язку і сервери для розміщення зовнішнього контенту;
- постачальник послуг з доставки контенту займається лише доставкою контенту в багаточисельні точки доступу з метою підвищення швидкості доступу користувачів до інформації;
- постачальник послуг з підтримки додатків надає клієнтам доступ до крупних універсальних програмних продуктів;
- постачальник білінгових послуг забезпечує оплату рахунків по інтернет.

Отже, інтернет є дуже складною мережею і, відповідно, таким же складним є завдання організації взаємодії між пристроями мережі. Для вирішення таких завдань використовується декомпозиція, тобто розбиття складного завдання на декілька простіших завдань-модулів. Однією з концепцій, що реалізують декомпозицію, є багаторівневий підхід. Такий підхід дає можливість проводити розробку, тестування і модифікацію кожного окремого рівня незалежно від інших рівнів. Ієрархічна декомпозиція дозволяє, переміщаючись у напрямі від нижчих до вищих рівнів,

переходити до простішого представлення вирішуваного завдання.

Специфіка багаторівневого представлення мережної взаємодії полягає в тому, що в процесі обміну повідомленнями беру участь, як мінімум, дві сторони, для яких необхідно забезпечити погоджену роботу двох ієрархій апаратно-програмних засобів. Кожен з рівнів повинен підтримувати інтерфейс з рівнями власної ієрархії засобів, що вище, і пролягають нижче, і інтерфейс із засобами взаємодії іншої сторони на тому ж рівні ієрархії. Даний тип інтерфейсу називається протоколом.

Ієрархічно організований набір протоколів, достатній для організації взаємодії вузлів у мережі, називається стеком протоколів.

На початку 1980-х рр. міжнародні організації зі стандартизації ISO (International Organization for Standardization), ITU (International Telecommunications Union) та інші розробили стандартну модель взаємодії відкритих систем OSI (Open System Interconnection). Призначення даної моделі полягає в узагальненому представленні засобів мережної взаємодії. Її також можна розглядати як універсальну мову мережних фахівців (довідкової моделі).

Оскільки мережа - це з'єднання різнорідного устаткування, актуальною є проблема сумісності, що у свою чергу, вимагає узгодження всіма виробниками загальноприйнятих стандартів. Відкритою є система, побудована відповідно до відкритих специфікацій.

Специфікація є формалізованим описом апаратних (програмних) компонентів, способів їх функціонування, взаємодії з іншими компонентами, умов експлуатації, особливих характеристик. Під відкритими специфікаціями розуміються опубліковані, загальнодоступні специфікації, відповідні стандартам і прийняті в результаті досягнення згоди після обговорення всіма зацікавленими сторонами. Використання відкритих специфікацій при розробці систем дозволяє третім сторонам розробляти для цих систем апаратно-програмні засоби розширення і модифікації, а також створювати програмно-апаратні комплекси з продуктів різних виробників.

Якщо дві мережі побудовано з дотриманням принципів відкритості, це дає такі переваги:

- можливість побудови мережі з апаратних і програмних засобів різних виробників, що дотримуються стандарту;
- безболісна заміна окремих компонентів мережі іншими, досконалішими;
- легкість сполучення однієї мережі з іншою.

У рамках моделі OSI засобу взаємодії діляться на сім рівнів: прикладний, вистави, сеансовий, транспортний, мережний, каналний і фізичний. У розпорядження програмістів надається прикладний програмний інтерфейс, що дозволяє поводитися із запитами до самого верхнього рівня, а саме - рівню додатків.

Мережа інтернет будувалася в повній відповідності з принципами відкритих систем. У розробці стандартів цієї мережі брали участь тисячі фахівців-користувачів мережі з вузів, наукових організацій і компаній. Результат роботи зі стандартизації втілюється в документах RFC.

RFC (англ. Request for Comments) - документ із серії пронумерованих інформаційних документів інтернет, що містять технічні специфікації і стандарти, широко вживані в Усесвітній мережі. У даний час первинною публікацією документів RFC займається IETF під егідою відкритої організації суспільство інтернет (ISOC). Правами на RFC володіє саме суспільство інтернет. Формат RFC з'явився в 1969 р. при обговоренні проекту ARPANET. Перші RFC поширювалися в друкарському вигляді на папері у вигляді звичайних листів, але вже з грудня 1969 р., коли запрацювали перші сегменти ARPANET, документи почали поширюватися в електронному вигляді. У табл. 4.2 наведено деякі з найбільш відомих документів RFC.

Таблиця 14.2  
Приклади популярних RFC-документів

Номер RFC	Тема
RFC 768	UDP
RFC 791	IP
RFC 793	TCP
RFC 822	Формат електронної пошти, замінений RFC 2822
RFC 959	FTP
RFC 1034	DNS - концепція
RFC 1035	DNS - впровадження
RFC 1591	Структура доменних імен
RFC 1738	URL
RFC 1939	Протокол POP версії 3 (POP3)
RFC 2026	Процес стандартизації в інтернет
RFC 2045	MIME
RFC 2231	Кодування символів
RFC 2616	HTTP
RFC 2822	Формат електронної пошти
RFC 3501	IMAP версії 4 видання 1 (IMAP4rev1)

Основним організаційним підрозділом, що координує роботу зі стандартизації інтернет, є ISOC (Internet Society), об'єднуючі понад 100 тис. учасників, які займаються різними аспектами розвитку даної мережі. ISOC займається роботою IAB (Internet Architecture Board), що включає дві групи:

- IRTF (Internet Research Task Force);
- координує довгострокові дослідницькі проекти, що відносяться до TCP/IP;
- IETF (Internet Engineering Task Force);
- інженерна група, що визначає специфікації для подальших стандартів інтернет.

Розробкою стандартів для Web-мережі, починаючи з 1994 р., займається Консорціум W3C (World Wide Web Consortium), заснований і до цих пір очолюваний Тімом Бернерсом-Лі.

Консорціум W3C - організація, яка розробляє і впроваджує технологічні стандарти для інтернет і WWW. Місія W3C формулюється таким чином: "Повністю розкрити потенціал Усесвітньої павутини шляхом створення протоколів і принципів, що гарантують довгостроковий розвиток мережі". Дві інші найважливіші завдання Консорціуму - забезпечити повну "інтернаціоналізацію Мережі" і зробити її доступною для людей з обмеженими можливостями.

W3C розробляє для WWW єдині принципи і стандарти - "Рекомендації", які потім упроваджуються розробниками програм і устаткування. Завдяки Рекомендаціям досягається сумісність між програмними продуктами і устаткуванням різних компаній, що робить мережу WWW досконалішою, універсальною і зручною у використанні.

Усі Рекомендації W3C відкриті, тобто, не захищені патентами і можуть упроваджуватися будь-якою людиною без яких-небудь фінансових відрахувань Консорціуму.

Для зручності користувачів Консорціумом створено спеціальні програми-валідатори (від англ. Online Validation Service), які доступні по мережі і можуть за декілька секунд перевірити документи на відповідність популярним Рекомендаціям W3C. Консорціумом також створено багато інших утиліт для полегшення роботи Web-майстрів і програмістів. Більшість утиліт - це програми з відкритим вихідним кодом, всі вони безкоштовні. Останнім часом, покоряючись світовим тенденціям, Консорціум, у цілому, значно більше уваги приділяє проектам з відкритим вихідним кодом.

Перш ніж перейти до опису структури, принципів роботи і основних протоколів



мережі, розглянемо основний стек протоколів мережі інтернет - стек TCP/IP.

## **2. Стек протоколів TCP/IP**

Ці протоколи спочатку орієнтовані на глобальні мережі, в яких якість сполучних каналів неідеальна. Він дозволяє створювати глобальні мережі, комп'ютери в яких сполучені один з одним самими різними способами - від високошвидкісних оптоволоконних кабелів і супутникових каналів до комутованих телефонних ліній. TCP/IP відповідає моделі OSI досить умовно і містить чотири рівні. Прикладний рівень стека відповідає трьом верхнім рівням моделі OSI: прикладному, рівню управління і сеансовому.

У мережі дані завжди передаються блоками відносно невеликого розміру. Кожен блок має префіксну частину (заголовок), що описує вміст блоку, і суфіксну, що містить, наприклад, інформацію для контролю цілісності переданого блоку даних.

Назва стека протоколів TCP/IP складається з назв двох різних протоколів. Протокол IP (Internet Protocol) є протоколом нижнього (мережного) рівня і відповідає за передачу пакетів даних у мережі. Він належить до так званих протоколів дейтаграм і працює без підтверджень. Останнє означає, що при його використанні доставка пакетів даних не гарантується і не підтверджується. Не гарантується також і те, що пакети досягнуть пункту призначення в тій послідовності, в якій вони були відправлені.

До протоколів мережного рівня відноситься також протокол міжмережних повідомлень ICMP (Internet Control Message Protocol), що управляють, призначений для передачі маршрутизатором джерелу інформації про помилки при передачі пакету.

Вочевидь, набагато зручніше передавати дані каналом, який працює коректно, доставляючи всі пакети по черзі. Тому поверх протоколу IP працює протокол передачі даних більш високого рівня - TCP (Transmission Control Protocol). Посилаючи і приймаючи пакети через протокол IP, протокол TCP гарантує доставку всіх переданих пакетів даних у правильній послідовності.

Слід зазначити, що при використанні протоколу IP забезпечується швидша передача даних, оскільки не витрачається час на підтвердження прийому кожного пакету. Є й інші переваги. Одна з них полягає в тому, що він дозволяє розсилати пакети даних у широкомовному режимі, при якому вони досягають всіх комп'ютерів фізичної мережі. Що ж до протоколу TCP, то для передачі даних з його допомогою необхідно створити канал зв'язку між комп'ютерами. Він і створюється з використанням протоколу IP.

Для ідентифікації мережних інтерфейсів використовуються три типи адрес:

- апаратні адреси (або MAC-адреса);
- мережні адреси (IP-адреса);
- символні (доменні) імена.

У рамках IP протоколу для створення глобальної системи адресації, не залежної від способів адресації вузлів в окремих мережах, використовується пара ідентифікаторів, що складається з номера мережі і номера вузла. При цьому IP-адрес ідентифікує не окремий комп'ютер або маршрутизатор, а одне мережне з'єднання у складі мережі, в яку він входить; тобто кінцевий вузол може входити в декілька IP-мереж.

## **3. Адресація в мережах TCP/IP**

Для ідентифікації мережних інтерфейсів використовується три типи адрес: локальні (апаратні) адреси; мережні адреси (IP-адреси); символні (доменні) імена. Щоб технологія TCP/IP могла вирішувати завдання об'єднання мереж, їй необхідна власна глобальна система адресації, що дозволяє універсальним і однозначним способом ідентифікувати будь-який інтерфейс мережі. Очевидним рішенням є нумерація всіх підмереж складовою мережі, а потім нумерація мережних інтерфейсів у межах кожної з цих підмереж. Пара, що складається з номера мережі і номери вузла, відповідає поставленим умовам і може слугувати як мережна адреса, або IP-адреса.

Найпоширенішою формою подання IP-адреси є запис у вигляді чотирьох чисел, що

представляють значення кожного байта в десятковій формі і розділених крапками, наприклад: 128.10.2.30.

У деяких випадках виявляється корисним уявлення IP-адреси в двійковому форматі: 10000000 00001010 00000010 00011110.

Запис адреси не передбачає спеціального розмежувального знака між номером мережі і номером вузла. Разом з тим при передачі пакета по мережі часто виникає необхідність автоматичними засобами поділяти адресу на ці дві частини. Наприклад, маршрутизація, як правило, здійснюється на підставі номера мережі, тому кожен маршрутизатор, отримавши пакет, повинен прочитати з відповідного заголовка адресу призначення і виділити з нього номер мережі. Для цих цілей слугують два підходи:

- перший - заснований на використанні класів адрес. Уводиться п'ять класів адрес: А, В, С, D, Е. Три з них - А, В, С - слугують для адресації мереж. А два інших D і Е - мають спеціальне призначення. Для кожного класу мережних адрес визначено власне становище границі між номером мережі і номером вузла;

- другий - у даний час найбільш поширений, заснований на використанні маски, яка дозволяє максимально гнучко встановлювати межу між номером мережі і номером вузла. Маска - це число, яке використовується в парі з IP-адресою, причому двійковий запис маски містить безперервну послідовність одиниць у тих розрядах, які повинні в IP-адресі інтерпретуватися як номер мережі.

Для першого підходу в мережі класу А адреса визначається першим октетом IP-адреса (зліва направо). Значення першого октету, що знаходиться в межах 1 - 126, зарезервовано для гігантських транснаціональних корпорацій. У світі може існувати лише 126 мереж класу А, кожна з яких може містити майже 17 млн комп'ютерів.

Клас В використовує два перші октету в якості мережі, а значення першого октету може бути в межах 128 - 191. У мережі класу В може бути близько 65 тис. комп'ютерів, такі мережі мають найбільші університети та інші великі організації.

У класі С під адресу мережі відводиться вже три перших октети, а значення першого октету - в межах 192 - 223. Це найбільш поширені мережі, їх кількість може перевищувати 2 млн, а кількість комп'ютерів у кожній мережі - до 254.

Протокол TCP/IP спроектований так, що вся мережа може бути розбита на підмережі. Хости в одній підмережі спілкуються один з одним безпосередньо. Якщо треба передати пакети з однієї підмережі в іншу, то вони передаються через маршрутизатори (маршрутизаторами можуть бути ті ж комп'ютери або спеціальні пристрої). Комп'ютеру, що передає пакт, треба знати, як передавати дані - напряму або через маршрутизатор. Для цього йому задається крім IP-адреси отримувача ще й маска підмережі. За допомогою маски підмережі комп'ютер легко обчислює знаходження адресата і визначає, чи знаходиться він в одній з ним підмережі, якщо так - посилає пакет безпосередньо, якщо ні - посилає його на маршрутизатор, який передає його в іншу підмережу.

*Маска підмережі* - це шаблон, за допомогою якого IP-адресу поділяють на дві частини: адреса мережі та номер комп'ютера в цій мережі.

Маски підмережі є основою методу безкласової маршрутизації. У цьому підході маску підмережі записують разом з IP-адресою у форматі "IP-адрес/кількість одиничних біт в масці". Число після слеша означає кількість одиничних розрядів у масці підмережі.

Розглянемо приклад запису діапазону IP-адрес у вигляді 10.96.0.0/11. У цьому випадку маска підмережі буде мати двійковий вид 11111111 11100000 00000000 00000000, або те ж саме в десятковому вигляді: 255.224.0.0. 11 розрядів IP-адреси відводяться під адресу мережі, а решта  $32 - 11 = 21$  розряд повної адреси (11111111 11100000 00000000 00000000) - під локальну адресу в цій мережі. Разом 10.96.0.0/11 означає діапазон адрес від 10.96.0.0 до 10.127.255.255.

Маска призначається за такою схемою 28-n (для мереж класу С), де n - кількість комп'ютерів в підмережі + 2, округлене до найближчого більшого ступеня двійки (ця формула справедлива для  $n < 254$ , для  $n > 254$  буде інша формула).

Приклад: в якійсь мережі класу С є 30 комп'ютерів, маска для такої мережі обчислюється таким чином:

$28 - 32 = 224$  (0E0h)  $\Leftrightarrow$  255.255.255.224

*Порядок призначень IP-адресів.* За визначенням, схема IP-адресації повинна забезпечити унікальність нумерації мереж, а також вузлів у межах кожної з мереж. Коли справа стосується мережі, що є частиною інтернету, унікальність нумерації в межах всієї величезної мережі може бути забезпеченою тільки зусиллями спеціально створених для цього центральних органів. Головним органом реєстрації глобальних адрес в інтернеті з 1998 р. є неурядова організація ICANN (Internet Corporation for Assigned Names and Numbers). Ця організація координує роботу регіональних відділів, діяльність яких охоплює великі географічні площі: ARIN (Америка), RIPE (Європа), ARNIC (Азія і Тихоокеанський регіон). Регіональні відділи виділяють блоки адрес мереж великим постачальникам послуг, а ті, у свою чергу, розподіляють їх між своїми клієнтами, серед яких можуть бути і більш дрібні постачальники.

У невеликій же автономній IP-мережі умова унікальності номерів мережі може бути виконана силами мережевого адміністратора. У цьому випадку в розпорядженні адміністратора є всеадресний простір. Однак при такому підході виключена можливість у майбутньому підключення до інтернету, оскільки довільно вибрані адреси даної мережі можуть збігатися з централізовано призначеними адресами інтернету. Для того щоб уникнути колізій, пов'язаних з такого роду збігами, у стандартах інтернету визначено декілька діапазонів так званих приватних адрес, рекомендованих для автономного використання:

- у класі А - мережа 10.0.0.0;
- у класі В - діапазон з 16 номерів мереж (172.16.0.0.-172.31.0.0.);
- у класі С - діапазон з 255 мереж (192.168.0.0.-192.168.255.0.).

Ці адреси, виключені з безлічі, централізовано розподіляються, складають величезний адресний простір, достатній для нумерації вузлів автономних мереж практично будь-яких розмірів.

#### **4. Система доменних імен DNS**

Попри те, що апаратне і програмне забезпечення в рамках TCP/IP мереж для ідентифікації вузлів використовує IP-адреса, користувачі віддають перевагу символьним іменам (доменні імена).

Спочатку в локальних мережах з невеликої кількості комп'ютерів застосовувалися прості імена, що складаються з послідовності символів без розділення їх на окремі частини, наприклад MYCOMP. Для встановлення відповідності між символьними іменами і числовими адресами використовувалися широкомовні запити. Проте для великих територіально розподілених мереж, що працюють на основі протоколу TCP/IP, такий спосіб виявився неефективним. Тому для встановлення відповідності між доменним ім'ям і IP-адресом використовується спеціальна система доменних імен (DNS, Domain Name System), яка заснована на створюваних адміністраторами мережі таблиць відповідності.

У мережах TCP/IP використовується доменна система імен, що має ієрархічну (у вигляді дерева) структуру. Дана структура імен нагадує ієрархію імен, використовувану в багатьох файлових системах. Запис доменного імені починається з наймолодшою складовою, потім після крапки слідує наступна за старшинством символьна частина імені і так далі. Послідовність закінчується кореневим ім'ям, наприклад: company.yandex.ru.

Побудована таким чином система імен дозволяє розділяти адміністративну відповідальність по підтримці унікальності імен у межах свого рівня ієрархії між різними людьми або організаціями.

Сукупність імен, в яких декілька старших складових частин збігаються, утворюють домен імен.

Кореневий домен управляється центральними органами інтернету: IANA і Internic.

Домени верхнього рівня призначаються для кожної країни, а також для різних типів

організацій. Імена цих доменів повинні слідувати міжнародному стандарту ISO 3166. Для позначення країн використовуються двобуквені аббревіатури, наприклад ua-(Україна) ru-(Російська Федерація), it-Італія), fr-(Франція).

Для різних типів організацій використовуються трибуквенні аббревіатури:

- net - мережеві організації;
- org - некомерційні організації;
- com - комерційні організації;
- edu - освітні організації;
- gov - урядові організації.

Адміністрування кожного домена покладається на окрему організацію, яка делегує адміністрування піддоменів іншим організаціям.

Для здобуття доменного імені необхідно реєструватися у відповідній організації, якою організація INTERNIC делегувала свої повноваження по розподілу доменних імен.

У TCP/IP мережах відповідність між доменними іменами і IP-адресами може встановлюватися як локальними засобами, так і централізованими службами. Первинна відповідність задавалася за допомогою створюваного вручну на хості файлу hosts.txt, що складається з рядків, що містять пару виду “доменне ім’я - IP-адрес”. Проте з активним зростанням інтернету таке рішення виявилось немасштабованим.

Альтернативне рішення - централізована служба DNS, що використовує розподілену базу відображень “доменне ім’я - IP-адрес”. Сервер домена зберігає лише імена, які закінчуються на наступному нижче по дереву рівні. Це дозволяє розподіляти більш рівномірно навантаження по дозволу імен між всіма DNS-серверами. Кожен DNS-сервер окрім таблиці відображення імен містить посилання на DNS-сервера своїх піддоменів.

Існують дві схеми дозволу DNS-імен.

Нерекурсивна процедура:

- DNS-клієнт звертається до кореневого DNS-серверу з вказівкою повного доменного імені;
- DNS-сервер відповідає клієнтові, вказуючи адресу наступного DNS-сервера, обслуговуючого домен верхнього рівня, заданий в наступній старшій частині імені;
- DNS-клієнт робить запит наступного DNS-сервера, який посилає його до DNS-серверу потрібного піддомена і так далі, поки не буде знайдений DNS-сервер, в якому зберігається відповідність запитаного імені IP-адресу. Сервер дає остаточну відповідь клієнтові.

Рекурсивна процедура:

- DNS-клієнт запрошує локальний DNS-сервер, обслуговуючий піддомен, якому належить клієнт;
- далі якщо локальний DNS-сервер знає відповідь, він повертає його клієнтові;
- якщо локальний сервер не знає відповідь, то він виконує ітеративні запити до кореневого сервера. Після здобуття відповіді сервер передає його клієнтові.

Таким чином, при рекурсивній процедурі клієнт фактично передоручає роботу своєму серверу. Для прискорення пошуку IP-адресів DNS-сервери широко застосовують кешування (на якийсь час від години до декількох днів) відповідей, що проходять через них.