Дрогобицький державний педагогічний університет

імені Івана Франка

АННА КАРПИН, ДМИТРО КАРПИН

Комп’ютерні мережі: тексти лекцій

Навчальний посібник

Дрогобич, 2025

УДК 004.7(075.8)

К26

Рекомендовано вченою радою
Дрогобицького державного педагогічного університету імені
Івана Франка
(протокол № 7 від 26.06.2025 року)

Рецензенти:

О. Сікора – кандидат технічних наук, доцент, доцент кафедри фізики та інформаційних систем Дрогобицького державного педагогічного університету імені Івана Франка.

М. Лучкевич – кандидат фізико-математичних наук, доцент, доцент кафедри інформаційних систем та мереж Національного університету "Львівська політехніка".

Відповідальний за випуск: **Гольський В.Б.** – доцент, завідувач кафедри фізики та інформаційних систем Дрогобицького державного педагогічного університету імені Івана Франка.

Анна Карпин, Дмитро Карпин

Комп'ютерні мережі : навчальний посібник : тексти лекцій. Дрогобич : Дробицький державний педагогічний університет ім. І. Франка, 2025. 157 с.

Навчальний посібник містить основні теми лекцій з дисципліни "Комп'ютерні мережі". Він охоплює основи побудови, функціонування та управління комп'ютерними мережами, включаючи моделі OSI та TCP/IP, принципи маршрутизації, протоколи передачі даних і засоби безпеки. Окрема увага приділяється мережевому обладнанню, адмініструванню та діагностиці мереж. Посібник слугує базою для розуміння сучасних технологій Інтернету та корпоративних мереж.

Бібліографія 25 назв.

ЗМІСТ

ВСТУП

Сучасний світ неможливо уявити без комп’ютерних мереж, які забезпечують глобальну комунікацію, обмін інформацією та інтеграцію цифрових ресурсів. Вони стали невід'ємною частиною повсякденного життя, сприяючи розвитку науки, бізнесу, освіти та соціальних зв'язків. Завдяки комп'ютерним мережам, відбувається швидкий доступ до знань, миттєвий обмін даними та ефективна взаємодія між пристроями, незалежно від географічного положення.

Вивчення комп'ютерних мереж є ключовим елементом підготовки фахівців у галузі інформаційних технологій, оскільки вони виступають основою для функціонування як локальних, так і глобальних інформаційних систем. Глибоке розуміння мережевих технологій дає змогу забезпечувати безперебійну роботу цифрової інфраструктури, оптимізувати процеси передачі даних, а також розробляти і впроваджувати нові рішення для підвищення продуктивності та безпеки систем.

Пропонований посібник «Комп'ютерні мережі» спрямований на формування системного розуміння принципів побудови та функціонування комп’ютерних мереж. У рамках лекційного матеріалу розглянуто фундаментальні аспекти мережевих технологій, зокрема:

- Основні поняття та характеристики комп’ютерних мереж: визначення, класифікація, ключові властивості та сфери застосування;
- Архітектура комп’ютерних мереж: моделі OSI та TCP/IP, рівневий підхід до організації мережевої взаємодії, особливості кожного рівня;
- Топології та компоненти комп’ютерних мереж: види топологій, активне та пасивне обладнання, їхнє призначення та роль у мережі;
- Канали і лінії зв’язку. Кабельні системи: середовища передавання даних, типи кабелів, їхні характеристики та критерії вибору;
- Адресація в мережах: IP-адреси, маски підмереж, протоколи маршрутизації, концепція динамічної та статичної адресації;

- Бездротові мережі. Глобальні мережі (WAN): стандарти бездротового зв’язку, технології мобільних мереж, принципи організації та особливості глобальних мереж;
- Огляд категорій атак на комп’ютерні мережі: типи атак, вразливості, методи захисту та засоби виявлення загроз;
- Інтеграція технологій і сучасні виклики: тренди розвитку мережевих технологій, кібербезпека, впровадження хмарних обчислень та Інтернету речей (IoT).

Матеріали посібника структуровані відповідно до логіки вивчення дисципліни, що сприяє поступовому засвоєнню теоретичних знань і набуттю практичних навичок. Викладений матеріал супроводжується ілюстраціями, схемами, реальними кейсами та контрольними запитаннями для самоперевірки, що забезпечує глибше розуміння складних концепцій і сприяє формуванню аналітичного мислення.

Видання буде корисним для студентів природничих, технічних напрямів підготовки, які прагнуть опанувати сучасні підходи до побудови комп’ютерних мереж та підвищити свій професійний рівень у сфері інформаційних технологій.

Текст лекцій до дисципліни “Комп'ютерні мережі ”забезпечує такі компетентності як:

загальні компетентності:

- здатність застосовувати знання в практичних ситуаціях;
- навички використання інформаційних і комунікаційних технологій;
- здатність до абстрактного мислення, аналізу та синтезу;
- здатність вчитися і оволодівати сучасними знаннями;
- здатність до пошуку, оброблення та аналізу інформації з різних джерел;
- здатність працювати в команді;
- здатність діяти соціально відповідально та свідомо;
- здатність приймати обґрунтовані рішення;

фахові компетентності:

- здатність нести відповідальність за прийняття рішень у непередбачуваних умовах. − здатність використовувати у професійній діяльності основні положення, методи, принципи фундаментальних та прикладних наук.
- здатність використовувати сучасні інформаційні технології та спеціалізоване програмне забезпечення та інтегрувати їх в освітнє середовище.

програмні результати навчання:

- володіти інформацією чинних нормативно-правових документів, законодавства, галузевих стандартів професійної діяльності в установах та організаціях галузі освіти. − доносити зрозуміло і недвозначно професійні знання, обґрунтування і висновки до фахівців і широкого загалу державною та іноземною мовами.
- аналізувати та оцінювати ризики, проблеми у професійній діяльності й обирати ефективні шляхи їх вирішення.
- самостійно планувати й організовувати власну професійну діяльність і діяльність здобувачів освіти.
- відшуковувати, обробляти, аналізувати та оцінювати інформацію, що стосується професійної діяльності, користуватися спеціалізованим програмним забезпеченням та сучасними засобами зберігання та обробки інформації.
- − емпатійно взаємодіяти, відповідати за прийняття рішень в межах своєї компетенції, дотримуватися стандартів професійної етики.

Тексти лекцій з дисципліни «Комп'ютерні мережі» укладені згідно із робочою програмою навчальної дисципліни «Комп'ютерні мережі» (затверджена науково-методичною радою Дрогобицького державного педагогічного університету імені Івана Франка, протокол № 2 від 24 лютого 2025 року).

Також у посібнику є питання для самоконтролю. Картинки-схеми створені за допомогою штучного інтелекту.

Лекція 1: Основні поняття та характеристика мереж

Комп’ютерні мережі стали фундаментом сучасного цифрового світу. Вони забезпечують взаємодію між пристроями, створюючи інфраструктуру для обміну даними, яка охоплює як локальні системи, так і глобальні. Уявіть собі: лише кілька десятиліть тому комп’ютери існували як ізольовані пристрої, які працювали автономно. Сьогодні ж світ став настільки пов’язаним, що важко уявити повсякденне життя без мережевих технологій.

Поняття комп’ютерних мереж охоплює широкий спектр технологій, які дають можливість передавати дані від одного пристрою до іншого. Це може бути проста домашня мережа, яка дає змогу переглядати відео на телевізорі через Wi-Fi, або ж складна глобальна мережа, яка об’єднує тисячі серверів і пристроїв для забезпечення роботи величезних корпорацій. Завдяки таким мережам світ стає більш інтегрованим, доступним і продуктивним.

Основною метою комп’ютерних мереж є обмін інформацією. Це може бути передача файлів, доступ до вебсайтів, надсилання електронних листів, здійснення відеодзвінків, управління хмарними сервісами тощо. Принципи роботи мережі базуються на використанні фізичних чи бездротових каналів зв’язку та протоколів, які встановлюють правила для передачі даних. Ці протоколи діють як мова спілкування між пристроями, забезпечуючи надійність, швидкість та безпеку обміну інформацією.

Комп’ютерні мережі можуть бути класифіковані за масштабом і призначенням. Наприклад, локальні мережі (LAN) використовуються для з’єднання пристроїв у межах однієї будівлі, тоді як глобальні мережі (WAN) охоплюють величезні географічні території. Крім того, мережі можуть відрізнятися за технологіями передачі даних, такими як оптоволоконні канали, супутниковий зв’язок або бездротові з’єднання.

Рис 1.1 Основні аспекти комп'ютерних мереж

Окрім технічної складової, комп'ютерні мережі мають величезний вплив на наше повсякденне життя. Наприклад, вони забезпечують можливість спілкування через месенджери та соціальні мережі, доступ до величезних баз знань через Інтернет, онлайн-освіту та дистанційну роботу. В бізнесі мережі дають можливість організаціям з різних куточків світу співпрацювати в режимі реального часу, оптимізувати логістичні процеси та автоматизувати операції.

Важливо також розуміти, що розвиток мережевих технологій не стоїть на місці. Сучасні тренди, такі як Інтернет речей (IoT), 5G-зв'язок та хмарні обчислення, вже сьогодні змінюють спосіб нашої взаємодії з технологіями. IoT дає змогу поєднувати різні пристрої в єдину екосистему, створюючи "розумні" будинки, міста та навіть індустрії. Хмарні обчислення забезпечують доступ до обчислювальних потужностей та даних з будь-якої точки світу, значно знижуючи витрати на інфраструктуру.

Розуміння основ комп’ютерних мереж є критично важливим для сучасного фахівця. Знання цієї теми відкриває доступ до широкого спектру можливостей у галузі IT, телекомунікацій, освіти та багатьох інших сфер.

Рис 1.2 Схема використання IoT у розумному будинку

Історія комп’ютерних мереж починається з ідеї створення системи, яка дозволила б комп’ютерам обмінюватися даними на відстані. У 1960-х роках, коли комп’ютери були величезними машинами, що займали кімнати, концепція зв’язку між ними здавалася революційною. Ця ідея стала можливою завдяки проєкту ARPANET, який започаткувало Агентство перспективних дослідницьких проєктів США (ARPA).

ARPANET вважається предком сучасного Інтернету. Ця мережа дозволила кільком комп’ютерам обмінюватися даними за допомогою комутації пакетів, що стало проривом у технології передачі інформації. У 1969 році до ARPANET були підключені чотири вузли, розташовані в університетах США. Це був перший реальний приклад мережевої взаємодії між комп’ютерами.

У 1970-х роках з’явилися нові протоколи, такі як TCP/IP, які стали основою сучасних мереж. Ці протоколи були розроблені для стандартизації передачі даних, що дозволило мережам різних типів взаємодіяти між собою. Важливим етапом стало введення доменних імен (DNS), що спростило доступ до ресурсів.

Розвиток локальних мереж (LAN) у 1980-х роках привів до появи технологій, таких як Ethernet. Ця технологія стала стандартом для побудови

офісних і домашніх мереж. Ethernet дозволив об’єднувати пристрої за допомогою кабельних з’єднань, забезпечуючи швидкість і надійність передачі даних.

1990-ті роки ознаменувалися стрімким розвитком глобальної мережі – Інтернету. Впровадження веббраузерів, таких як Mosaic, дозволило користувачам взаємодіяти з вебсторінками, відкриваючи доступ до величезних обсягів інформації. Це був час, коли Інтернет почав активно проникати у бізнес, освіту і побут.

Сучасні мережі базуються на досягненнях попередніх десятиліть. Технології стали більш доступними, швидкими та безпечними. Зараз ми користуємося бездротовими з’єднаннями, хмарними сервісами, і навіть мобільними мережами п’ятого покоління (5G), які забезпечують миттєвий доступ до інформації.

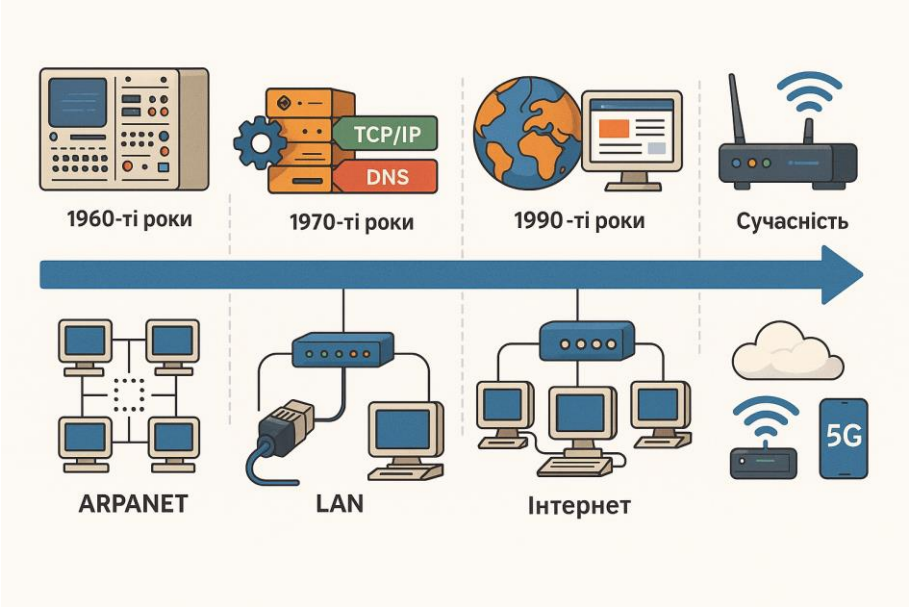


Рис 1.3 Схема часової шкали розвитку комп’ютерних мереж

Розуміння історії розвитку мереж дає змогу краще усвідомити принципи їх функціонування. Від перших експериментів із комутацією пакетів до сучасних технологій Інтернету речей (IoT), мережі продовжують розвиватися, відкриваючи нові можливості для науки, бізнесу і нашого повсякденного життя.

Комп’ютерні мережі базуються на кількох ключових поняттях, які визначають їхню структуру та принципи роботи. Ці поняття допомагають

зрозуміти, як взаємодіють пристрої у мережі та як забезпечується ефективна передача даних.

Одним із основних понять є **вузол** (node). У мережі вузлом називають будь-який пристрій, який підключений до мережі й може надсилати або отримувати дані. Це може бути комп’ютер, сервер, смартфон, маршрутизатор або навіть датчик у системі Інтернету речей. Вузли можуть взаємодіяти один з одним напряму або через проміжні пристрої, такі як комутатори або маршрутизатори.

Ще одним важливим поняттям є **сегмент мережі**. Сегмент – це частина мережі, в межах якої пристрої можуть взаємодіяти напряму, без використання маршрутизаторів. Наприклад, у локальній мережі сегмент може об’єднувати кілька комп’ютерів і принтерів, підключених до одного комутатора.

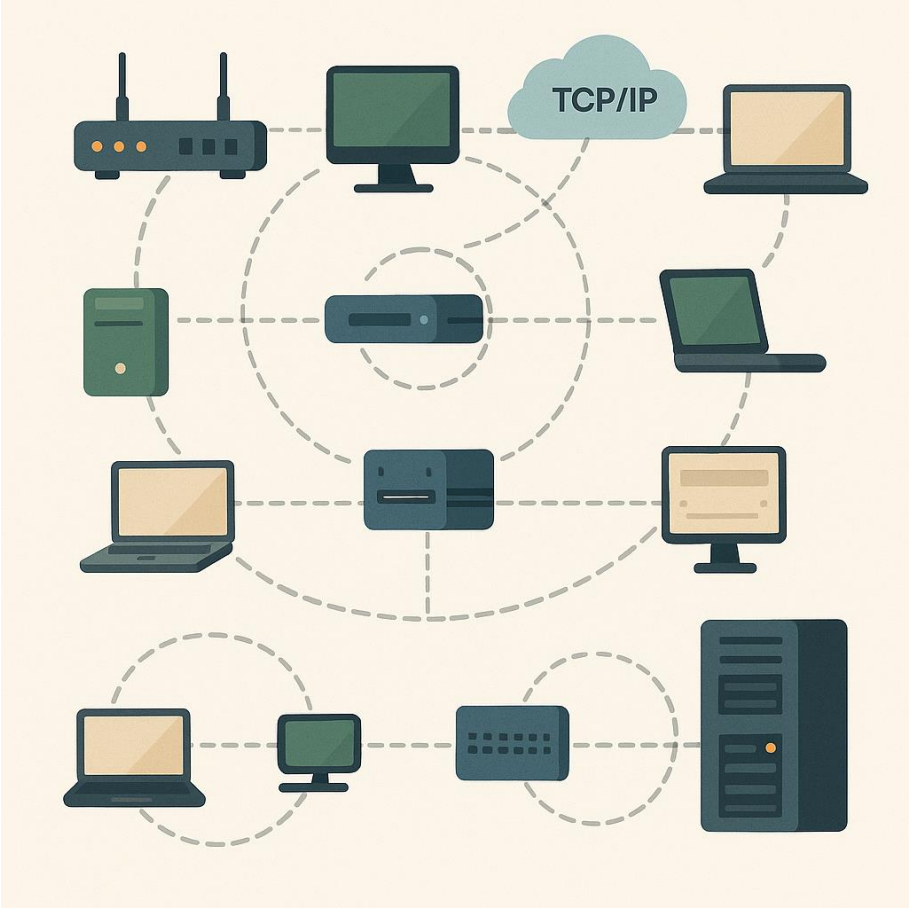


Рис 1.4 Вузли та сегменти мережі

Ключову роль у функціонуванні мереж відіграють **протоколи**. Протокол – це набір правил, які визначають, як дані передаються між вузлами. Протоколи забезпечують стандартизацію обміну інформацією, що дає змогу пристроям

різних виробників взаємодіяти один з одним. Найбільш відомими є протоколи сімейства TCP/IP, які використовуються в Інтернеті. Вони визначають, як дані діляться на пакети, передаються через мережу і збираються назад у вихідний формат.

Щоб зрозуміти структуру мережі, важливо ознайомитися з поняттям **мережевої архітектури**. Архітектура описує логічну і фізичну організацію мережі. Вона включає рівні моделі OSI або TCP/IP, які визначають, як різні компоненти мережі взаємодіють на різних етапах передачі даних. Наприклад, рівень фізичної передачі відповідає за кабелі й сигнали, тоді як прикладний рівень забезпечує роботу програм, які використовують мережу.

Крім того, варто розглянути поняття **адресації**. У мережі кожен пристрій має унікальну адресу, яка дає змогу ідентифікувати його серед інших вузлів. Адресація може бути фізичною (MAC-адреса) або логічною (IP-адреса). Логічна адреса використовується для маршрутизації даних у глобальних мережах, таких як Інтернет.

Ці ключові поняття формують основу розуміння роботи комп'ютерних мереж. Вони дають можливість не лише побудувати ефективну мережу, а й забезпечити її надійність, безпеку та масштабованість.

Комп'ютерні мережі класифікуються за різними ознаками, які відображають їх масштаби, технології та способи взаємодії. Розуміння цієї класифікації є важливим для вибору оптимальної мережевої архітектури для конкретних завдань.

а) за масштабом

Масштаб є одним із найпоширеніших критеріїв класифікації. Основні типи мереж за цим критерієм:

- **Локальні мережі (LAN)**: мережі, які охоплюють обмежену географічну територію, наприклад, офіс, будинок або школу. Вони зазвичай використовують високошвидкісні з'єднання і забезпечують швидкий обмін даними між пристроями.

- **Глобальні мережі (WAN)**: мережі, які охоплюють великі географічні території, такі як міста, країни чи навіть континенти. Прикладом глобальної мережі є Інтернет.
- **Регіональні мережі (MAN)**: проміжний варіант між LAN і WAN, що охоплює територію міста або великого кампусу.
- **Бездротові локальні мережі (WLAN)**: вони використовують бездротову технологію передачі даних, наприклад, Wi-Fi.

б) за технологіями передачі даних

Мережі також класифікуються за типом середовища передачі даних:

- **Кабельні мережі**: дані передаються через фізичні кабелі, такі як виті пари, коаксіальні кабелі або оптоволоконні лінії.
- **Бездротові мережі**: використовують радіохвилі, інфрачервоне випромінювання або супутниковий зв'язок.

в) за топологією

Топологія визначає фізичну або логічну структуру мережі:

- **Шина**: всі пристрої підключені до одного кабелю. Простий і економічний варіант, але з обмеженням пропускної здатності.
- **Зірка**: всі пристрої підключені до центрального вузла. Зручна для обслуговування і модернізації.
- **Кільце**: дані передаються по колу. Має недолік у випадку розриву лінії.
- **Сітка**: кожен вузол з'єднаний з іншими, що забезпечує високу надійність.

г) за призначенням

Мережі можуть бути:

- **Корпоративними**: використовуються компаніями для внутрішніх комунікацій і доступу до ресурсів.
- **Домашніми**: призначені для використання в межах однієї домівки.
- **Гібридними**: поєднують особливості корпоративних і публічних мереж.

д) Інші критерії

ПОРІВНЯЛЬНА ТАБЛИЦЯ ТИПІВ МЕРЕЖ

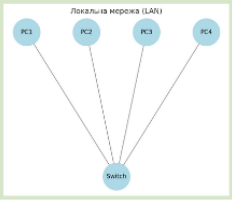
Тип мережі	Опис	Приклади	Схема
Локальна мережа (LAN)	Об'єднує комп'ютери на обмеженій території (офіс, будівля, кампус). Висока швидкість передавання даних	Корпоративні мережі, комп'ютерні класи, домашні мережі	
Міська мережа (MAN)	Поєднує локальні мережі в межах міста чи регіону. Високошвидкісний зв'язок	Міські мережі провайдерів, університетські мережі	
Глобальна мережа (WAN)	З'єднує комп'ютери та мережі на великій відстані через Інтернет або спеціалізовані канали зв'язку	Інтернет, корпоративні мережі великих компаній	
Бездротова мережа (WLAN)	Використовує радіосигнали для з'єднання пристроїв без фізичних кабелів.	Wi-Fi, Bluetooth, мобільні мережі 4G/5G	
Персональна мережа (PAN)	Використовується для з'єднання пристроїв на близькій відстані.	Bluetooth-мережі, підключення смарт-годинників до смартфонів	
Кластерна мережа (Cluster Network)	Об'єднує сервери для паралельних обчислень та розподілених задач	Суперкомп'ютери, серверні ферми	

Рис 1.5 Порівняльна таблиця основних типів мереж із прикладами та схемами

Мережі також можна класифікувати за типом трафіку (передача файлів, мультимедіа), рівнем безпеки (захищені чи публічні), а також за типом взаємодії (однорангові чи клієнт-серверні).

Класифікація комп'ютерних мереж допомагає вибрати оптимальні рішення для конкретних потреб, зважаючи на масштаб, ресурси та технічні вимоги.

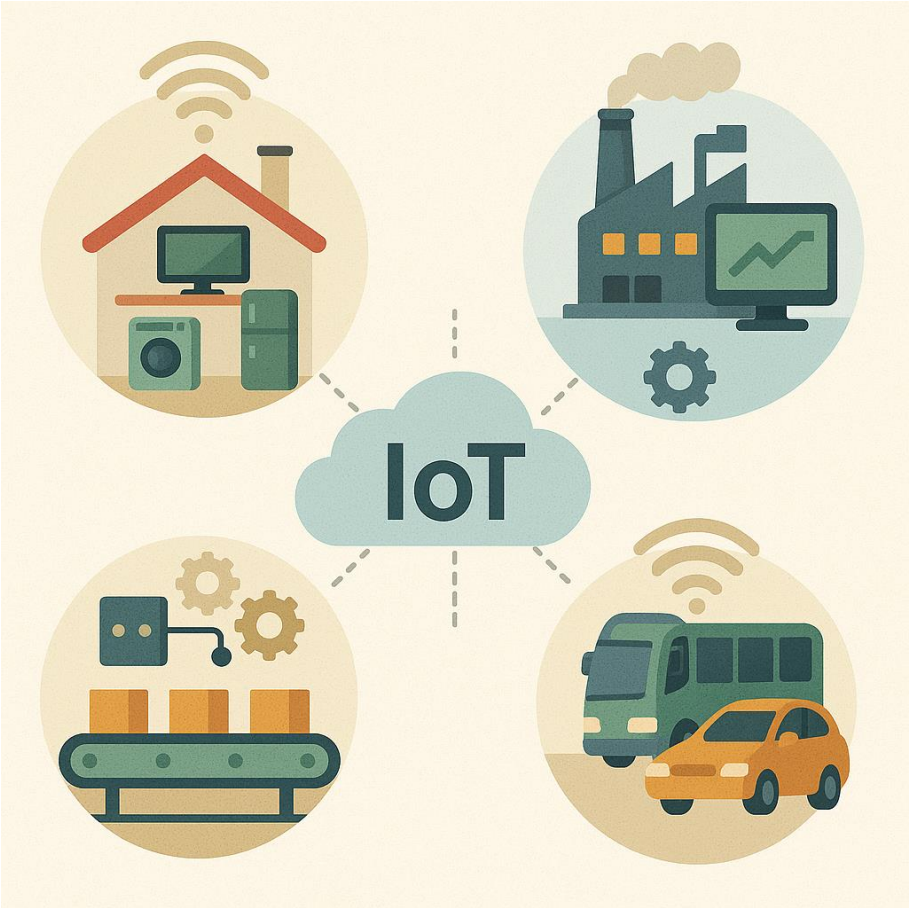


Рис 1.6 Схема використання IoT у різних сферах

Комп’ютерні мережі перебувають у постійному розвитку, адаптуючись до нових викликів і потреб сучасного суспільства. Однією з найважливіших тенденцій є зростання популярності Інтернету речей (IoT), який дає змогу взаємодіяти величезній кількості пристроїв між собою. Від "розумних" будинків до автономних автомобілів, IoT забезпечує нові способи використання технологій у повсякденному житті. Наприклад, "розумний" термостат може автоматично регулювати температуру в будинку, базуючись на прогнозі погоди та вашій присутності, що не лише підвищує комфорт, але й сприяє зниженню енергоспоживання. Ще одним значним проривом є поява мобільних мереж п’ятого покоління (5G), які забезпечують неймовірну швидкість передачі даних і мінімальні затримки. Завдяки 5G можливо реалізувати такі складні проєкти, як дистанційні операції в медицині, а також створення повноцінної віртуальної та доповненої реальності. 5G дає змогу не лише обслуговувати більше пристроїв, але й забезпечувати стабільний зв’язок навіть у густонаселених районах.

Хмарні обчислення стали ще однією ключовою тенденцією. Вони дають можливість компаніям та індивідуальним користувачам зберігати величезні обсяги даних і обробляти їх без необхідності в інвестуванні в дороге обладнання. Наприклад, використання хмарних сервісів Google Drive чи Microsoft Azure дає змогу отримувати доступ до файлів із будь-якої точки світу, забезпечуючи високу мобільність і ефективність. Крім того, хмарні платформи часто інтегруються з штучним інтелектом, дозволяючи автоматизувати багато процесів, таких як аналіз даних або створення прогнозів.

Ще одним напрямом розвитку є підвищення рівня безпеки в мережах. У зв'язку зі збільшенням кількості кіберзагроз сучасні мережі все частіше використовують передові методи захисту, такі як шифрування даних, багатофакторна аутентифікація та технології виявлення вторгнень. Наприклад, у багатьох системах для входу в обліковий запис тепер потрібно не лише пароль, але й підтвердження через мобільний додаток або біометричні дані. Це значно ускладнює доступ до конфіденційної інформації для зловмисників.

Сучасні тенденції у розвитку мереж продовжують змінювати наше сприйняття технологій. Вони роблять життя зручнішим, підвищують продуктивність бізнесу та відкривають нові можливості для науки і техніки. Однак ці тенденції також вимагають від нас постійного вдосконалення знань, щоб залишатися на передовій у світі технологій.

Комп'ютерні мережі оточують нас усюди, навіть якщо ми цього не помічаємо. Вони відіграють ключову роль у нашому повсякденному житті, забезпечуючи зв'язок, доступ до інформації та автоматизацію різних процесів. Один із найпростіших і водночас найпоширеніших прикладів використання мереж – це домашня Wi-Fi мережа. Завдяки Wi-Fi ми можемо підключатися до Інтернету з різних пристроїв: смартфонів, ноутбуків, телевізорів. Така мережа дає змогу переглядати відео, спілкуватися в соціальних мережах, робити покупки онлайн та працювати віддалено.

Корпоративні мережі є ще одним прикладом використання технологій. Вони забезпечують ефективну роботу компаній, дозволяючи співробітникам

обмінюватися даними, працювати над спільними проєктами та мати доступ до централізованих ресурсів, таких як сервери чи бази даних. Наприклад, у банківській сфері мережі дають можливість здійснювати транзакції в реальному часі, а також забезпечувати безпеку клієнтських даних. У великих корпораціях часто використовуються VPN (віртуальні приватні мережі), які забезпечують захищений доступ до корпоративних систем для віддалених працівників.

Глобальні мережі, такі як Інтернет, дають можливість об’єднувати мільйони пристроїв по всьому світу. Вони забезпечують доступ до інформації, яка зберігається на віддалених серверах, наприклад, у вигляді вебсайтів, онлайн-сервісів або хмарних сховищ. Наприклад, студент може виконувати дослідження для своєї курсової роботи, користуючись ресурсами бібліотек, розташованих у різних країнах, або брати участь в онлайн-курсах, які викладають найкращі університети світу.

Інтернет речей (IoT) розширює можливості використання мереж, дозволяючи об’єднувати в одну систему не лише комп’ютери, а й різноманітні пристрої: датчики, побутову техніку, автомобілі. Наприклад, у "розумному" будинку термостат автоматично регулює температуру залежно від часу доби, а холодильник може повідомляти про закінчення продуктів. У сфері промисловості IoT дає змогу контролювати виробничі процеси в режимі реального часу, знижуючи витрати і підвищуючи ефективність. У транспорті мережі дають можливість оптимізувати маршрути, забезпечувати безпеку дорожнього руху та розвивати автономний транспорт.

Приклади використання мереж демонструють, наскільки важливою є їхня роль у сучасному суспільстві. Від домашнього комфорту до складних технологічних рішень – мережі стали невід’ємною частиною нашого життя, дозволяючи нам бути продуктивнішими, ефективнішими та більш з’єднаними зі світом.

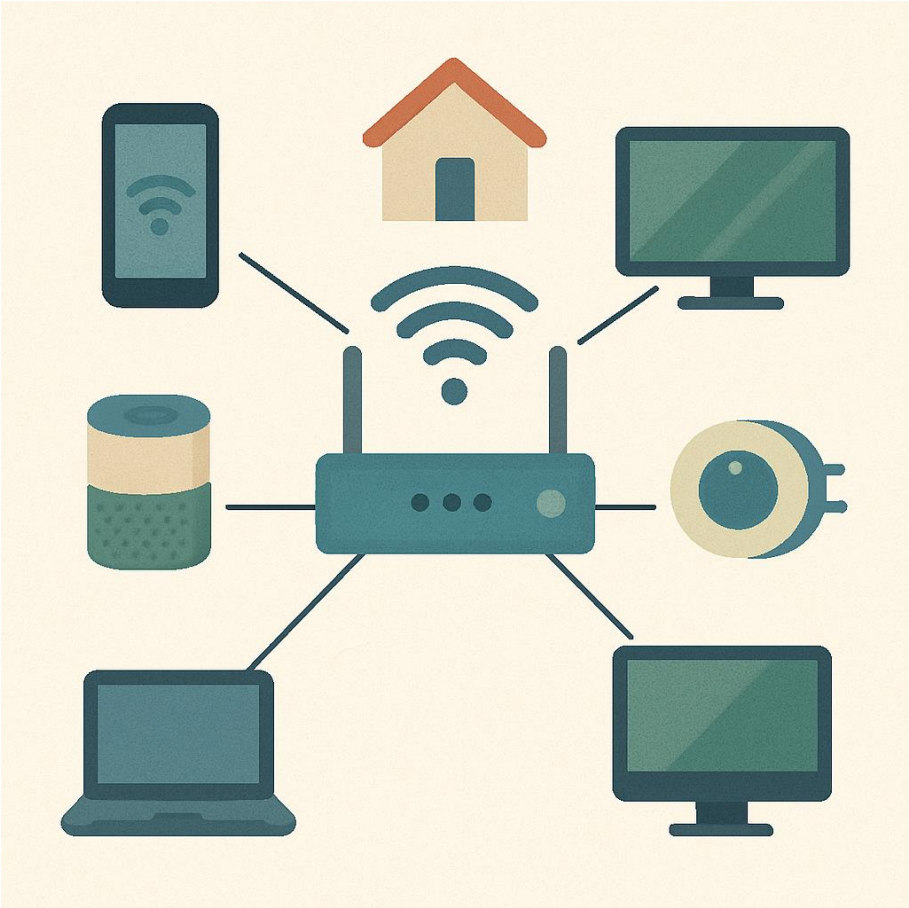


Рис 1.7 Приклад схеми домашньої мережі, яка об’єднує смартфони, ноутбуки, телевізори і "розумні" пристрої

Комп’ютерні мережі є одним із найважливіших досягнень людства, які забезпечують фундамент для функціонування сучасного світу. Вони дають можливість людям і пристроям взаємодіяти незалежно від їхнього місця розташування, відкриваючи нові горизонти для навчання, роботи і розваг. Від локальних мереж у межах будинку чи офісу до глобальних систем, які об’єднують мільйони користувачів, мережі демонструють свою універсальність і значущість.

Сучасні мережі базуються на принципах, які були розроблені протягом десятиліть. Починаючи з ARPANET і Ethernet, ці технології поступово еволюціонували, інтегруючи нові протоколи, моделі і способи передачі даних. Протоколи TCP/IP, які лежать в основі Інтернету, стали стандартом, завдяки якому пристрої з усього світу можуть обмінюватися інформацією. Ця еволюція

продовжується і зараз, адже нові виклики, такі як кібербезпека, Інтернет речей та мобільні технології 5G, потребують інноваційних рішень.

Рис 1.8 Узагальнююча схема із взаємодією локальних, глобальних мереж та Інтернету речей

Роль мереж не обмежується лише забезпеченням зв’язку. Вони стають платформою для розвитку нових технологій, таких як штучний інтелект, хмарні обчислення та автоматизація. Уявіть, як у найближчому майбутньому завдяки мережам автономні автомобілі зможуть обмінюватися інформацією в режимі реального часу, щоб уникати аварій, або як "розумні" міста оптимізуватимуть свої ресурси, забезпечуючи комфортне життя для мешканців.

Комп’ютерні мережі також вимагають нашої уваги до питань безпеки. Зі збільшенням кількості пристроїв і користувачів, що підключаються до мереж, зростають і ризики несанкціонованого доступу, витоку даних чи кібератак. Саме тому знання основ мережевих технологій є не лише корисним, але й необхідним для будь-якого спеціаліста в сучасному світі.

Мережі – це не просто технологія, це спосіб пов’язати людей, ідеї та можливості.

Лекція 2. Архітектура комп’ютерних мереж

Архітектура комп’ютерних мереж – це основа, яка визначає, як побудовані мережі, як вони функціонують і як взаємодіють їхні компоненти. Без добре продуманої архітектури жодна мережа не може забезпечити надійний і безперебійний зв’язок між пристроями. Вона слугує структурним планом, завдяки якому різні елементи мережі – від комп’ютерів і серверів до комутаторів і маршрутизаторів – працюють разом як єдина система.

Ідея створення архітектури мереж виникла з необхідності стандартизації. У перші десятиліття розвитку комп’ютерних мереж кожен виробник створював свої унікальні технології, які не були сумісними між собою. Наприклад, обладнання від однієї компанії могло не працювати з рішеннями іншої, що ускладнювало створення великих і масштабованих мереж. Ця проблема сприяла розробці стандартизованих підходів, таких як модель OSI, яка стала фундаментом для багатьох сучасних мережевих рішень.

Архітектура мереж визначає рівні, які відповідають за різні аспекти передачі даних. Це може включати фізичний рівень, на якому здійснюється передача сигналів по кабелях чи радіоканалах, і прикладний рівень, який відповідає за взаємодію користувача з додатками. Розподіл на рівні дає змогу спростити проєктування, обслуговування і модернізацію мереж. Наприклад, якщо потрібно замінити одну частину мережі, це можна зробити без впливу на інші рівні.

Сучасна архітектура мереж відображає складність і різноманітність технологій. Вона не обмежується лише кабельними чи бездротовими з’єднаннями. Інновації, такі як хмарні обчислення, віртуалізація та мережеві функції як послуга (NFaaS), змінюють спосіб побудови і використання мереж. Наприклад, хмарні сервіси дають можливість користувачам отримувати доступ до даних і програм незалежно від їхнього фізичного розташування, а віртуалізація мережевих функцій дає змогу значно знизити витрати на обладнання.

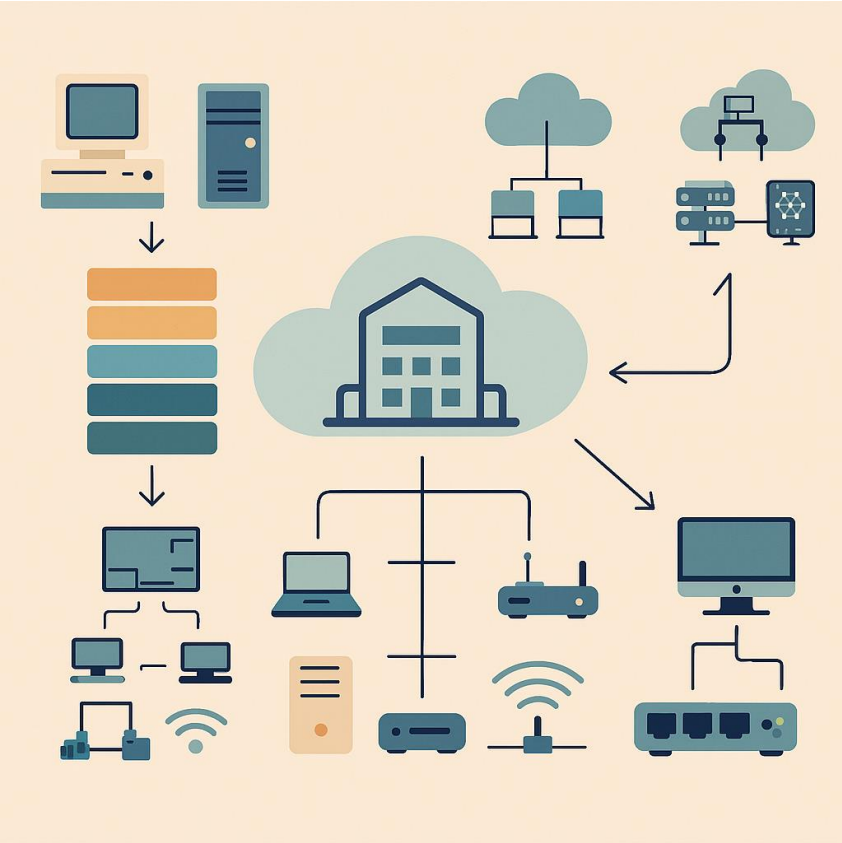


Рис 2.1 Архітектура комп'ютерної мережі: взаємодія рівнів, пристроїв і сучасних технологій у єдиній інфраструктурі

Архітектура мереж також відіграє ключову роль у забезпеченні безпеки. Сучасні мережі піддаються численним загрозам, від хакерських атак до шкідливих програм. Добре спроєктована архітектура дає змогу створити багаторівневу систему захисту, яка ускладнює доступ для зловмисників. Наприклад, інтеграція шифрування даних на транспортному рівні чи використання брандмауерів на прикладному рівні значно підвищує безпеку.

Розуміння архітектури мереж є надзвичайно важливим для професіоналів у галузі інформаційних технологій. Воно не лише забезпечує базу для створення ефективних і масштабованих систем, але й дає змогу інтегрувати нові технології, такі як IoT, 5G і штучний інтелект. Наприклад, у майбутньому завдяки передовій архітектурі можливе створення повністю автономних транспортних систем, які будуть взаємодіяти через глобальні мережі.

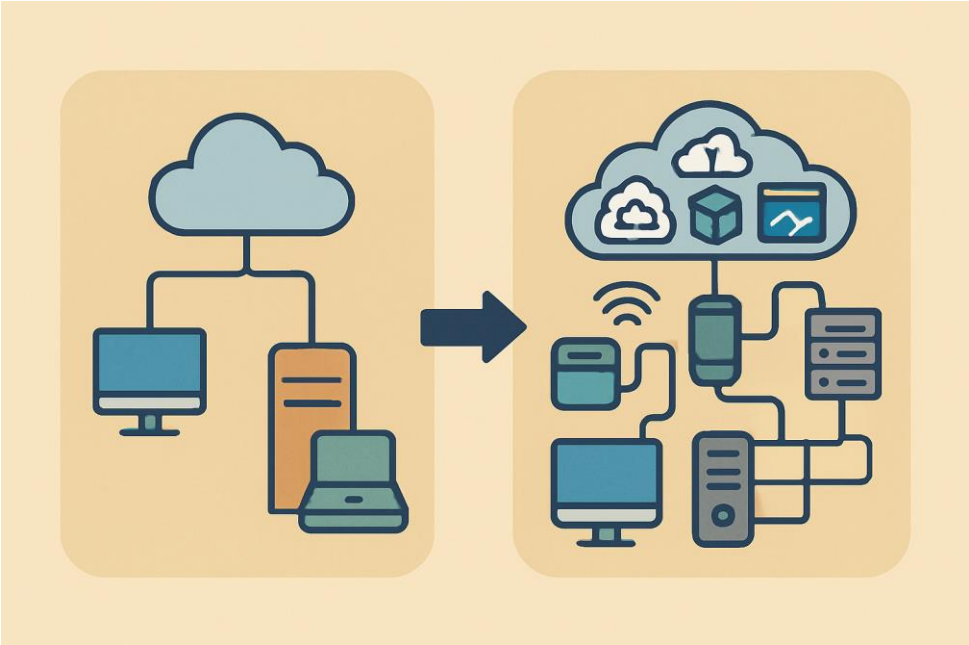


Рис 2.2 Схема порівняння традиційної архітектури мереж із сучасними підходами

Модель OSI (Open Systems Interconnection) є однією з найвідоміших концепцій у галузі комп'ютерних мереж. Вона була розроблена у 1984 році Міжнародною організацією зі стандартизації (ISO) як теоретична основа для опису взаємодії між компонентами мережі. Модель OSI слугує стандартом, який дає змогу забезпечити сумісність пристроїв і програмного забезпечення, навіть якщо вони створені різними виробниками. Її головною метою є стандартизація мережевих процесів і спрощення їхнього розуміння.

Модель OSI складається з семи рівнів, кожен із яких відповідає за певний аспект передачі даних. Цей поділ дає змогу чітко розмежувати функції різних компонентів мережі, а також забезпечує гнучкість у її побудові. Наприклад, якщо в мережі виникають проблеми, модель OSI допомагає визначити, на якому рівні ці проблеми з'явилися, що значно спрощує їх вирішення.

Фізичний рівень є найнижчим у моделі OSI. Він відповідає за фізичне з'єднання між пристроями, включаючи кабелі, конектори та сигнали. На цьому рівні визначаються характеристики середовища передачі, такі як тип кабелю (мідний чи оптоволоконний), частота сигналів і швидкість передачі даних. Фізичний рівень є основою, на якій будується вся мережа, адже без нього неможливий обмін даними.

Канальний рівень займається організацією передачі даних через фізичне середовище. Він забезпечує розбиття даних на кадри, контроль за їхньою доставкою та виявлення помилок. Канальний рівень також відповідає за використання MAC-адрес, які ідентифікують пристрої у локальній мережі. Завдяки цьому рівню пристрої можуть взаємодіяти навіть у складних умовах, таких як високий рівень перешкод.

Мережевий рівень забезпечує маршрутизацію даних між різними мережами. Він відповідає за вибір найкращого маршруту для передачі пакетів і використовує IP-адреси для ідентифікації пристроїв у глобальній мережі. Наприклад, коли ви надсилаєте електронний лист, мережевий рівень визначає шлях, яким пакети з вашого комп'ютера потрапляють до серверів одержувача.

Транспортний рівень відповідає за надійність передачі даних. Він гарантує, що всі пакети будуть доставлені у правильному порядку і без втрат. Одним із найвідоміших протоколів цього рівня є TCP (Transmission Control Protocol), який використовується для забезпечення надійної доставки даних у багатьох сучасних мережах.

Сеансовий рівень займається управлінням сеансами зв'язку між пристроями. Він встановлює, підтримує та завершує з'єднання, забезпечуючи синхронізацію між пристроями. Наприклад, у випадку відеоконференції сеансовий рівень дає змогу підтримувати стабільний зв'язок між учасниками.

Рівень представлення відповідає за перетворення даних між форматами, які використовуються різними програмами. Він забезпечує шифрування, стиснення і перекодування даних, що робить їх доступними для користувача. Наприклад, цей рівень відповідає за конвертацію зображення у формат, який може бути відображений на вашому екрані.

Прикладний рівень є найвищим у моделі OSI. Він надає інтерфейс для взаємодії користувача з мережею. Всі додатки, які використовують мережеві ресурси, працюють саме на цьому рівні. Прикладом є веббраузери, електронна пошта, FTP-клієнти.

Рис 2.3 Схема моделі OSI з описом функцій кожного рівня

Модель OSI не використовується у реальних мережах як практична архітектура, але її концепція дає змогу зрозуміти принципи роботи мереж і впорядкувати взаємодію між різними компонентами. Вона стала основою для багатьох інших моделей, включаючи TCP/IP.

Модель TCP/IP (Transmission Control Protocol/Internet Protocol) є основою сучасного Інтернету та багатьох мережевих технологій. Вона була розроблена у 1970-х роках для мережі ARPANET і з часом стала стандартом для взаємодії пристроїв у глобальних мережах. На відміну від моделі OSI, TCP/IP базується на практичному підході, що зробило її широко застосовуваною у реальних мережах.

Модель TCP/IP складається з чотирьох рівнів, кожен із яких виконує певні функції у передачі даних. Вона є менш деталізованою, ніж модель OSI, але більш ефективною у практичному використанні. Ці рівні забезпечують взаємодію між

пристроями, починаючи від фізичного з’єднання і закінчуючи обміном даними між додатками.

Перший рівень моделі TCP/IP – це рівень доступу до мережі. Він відповідає за фізичне підключення пристроїв, включаючи кабелі, маршрутизатори, комутатори та інші компоненти. Цей рівень також займається кодуванням і декодуванням сигналів, які передаються через мережу. Наприклад, у Wi-Fi мережах цей рівень відповідає за зв’язок між вашим ноутбуком і маршрутизатором.

Мережевий рівень TCP/IP забезпечує маршрутизацію даних між вузлами у глобальній мережі. Найважливішим протоколом цього рівня є IP (Internet Protocol), який відповідає за адресацію пристроїв та передавання даних у вигляді пакетів. Наприклад, коли ви відкриваєте вебсайт, IP-протокол визначає, куди мають бути доставлені ваші запити і як повернути відповіді.

Транспортний рівень моделі TCP/IP відповідає за забезпечення надійності передачі даних. Основними протоколами цього рівня є TCP (Transmission Control Protocol) і UDP (User Datagram Protocol). TCP використовується для передачі даних, які потребують високої надійності, наприклад, під час завантаження файлів або відправлення електронних листів. UDP, зі свого боку, застосовується у випадках, коли швидкість важливіша за надійність, наприклад, у потоковому відео чи онлайн-іграх.

Прикладний рівень є найвищим у моделі TCP/IP. Він забезпечує взаємодію користувача з мережею через програми та сервіси. Протоколи цього рівня включають HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol) та багато інших. Наприклад, коли ви вводите адресу вебсайту у браузері, HTTP-протокол застосовується для завантаження сторінки.

Головною перевагою моделі TCP/IP є її гнучкість і практичність. Вона дає змогу інтегрувати різні технології та адаптуватися до нових потреб. Завдяки цьому модель стала основою для побудови сучасного Інтернету та більшості

корпоративних мереж. Водночас її недоліком є недостатня деталізація, що інколи ускладнює діагностику проблем у складних системах.

Модель TCP/IP не лише спрощує побудову мереж, але й забезпечує їхню масштабованість. Вона підтримує різні типи підключень, від невеликих локальних мереж до глобальних систем із мільярдами пристроїв. Саме тому вона залишається незамінною у світі інформаційних технологій.

Моделі OSI та TCP/IP є двома найважливішими концепціями у світі комп'ютерних мереж. Хоча обидві моделі служать схожій меті – опису процесу передачі даних у мережах, вони мають суттєві відмінності у структурі, деталізації та практичному застосуванні. Їхнє порівняння допомагає зрозуміти, які аспекти кожної моделі є більш підходящими для різних завдань.

Модель OSI має сім рівнів, кожен із яких чітко визначає свої функції. Це дає змогу детально описати всі етапи передачі даних, починаючи від фізичного сигналу і закінчуючи взаємодією з користувачем. Така деталізація є її перевагою, адже дає змогу глибше аналізувати процеси в мережах. Проте на практиці модель OSI рідко використовується як основа для побудови мереж, оскільки вона є більш теоретичною.

Модель TCP/IP, на відміну від OSI, складається лише з чотирьох рівнів. Ця модель розроблена з урахуванням реальних потреб і використовується як основа для більшості сучасних мереж, включаючи Інтернет. Вона є менш деталізованою, але більш практичною, оскільки всі її рівні відповідають за конкретні завдання, які часто зустрічаються у реальних мережах.

Головна відмінність між моделями полягає у підході до взаємодії між рівнями. У моделі OSI кожен рівень чітко визначає свої функції і не залежить від інших. Це робить модель зручною для навчання і аналізу. У моделі TCP/IP рівні тісно інтегровані один з одним, що дає змогу забезпечити більшу гнучкість і ефективність у реальних мережах.

Ще однією важливою відмінністю є походження моделей. OSI була розроблена міжнародною організацією ISO як універсальний стандарт, тоді як TCP/IP створювалася для конкретного завдання – забезпечення роботи мережі

ARPANET. Це пояснює, чому TCP/IP має більш прикладний характер і є основою для сучасного Інтернету.

Обидві моделі мають свої сильні сторони. OSI краще підходить для розуміння концепцій і структури мереж, а TCP/IP є ефективнішою для побудови реальних систем. Наприклад, OSI використовується в освітніх цілях для пояснення, як різні протоколи працюють разом, тоді як TCP/IP активно використовується у корпоративних і глобальних мережах.

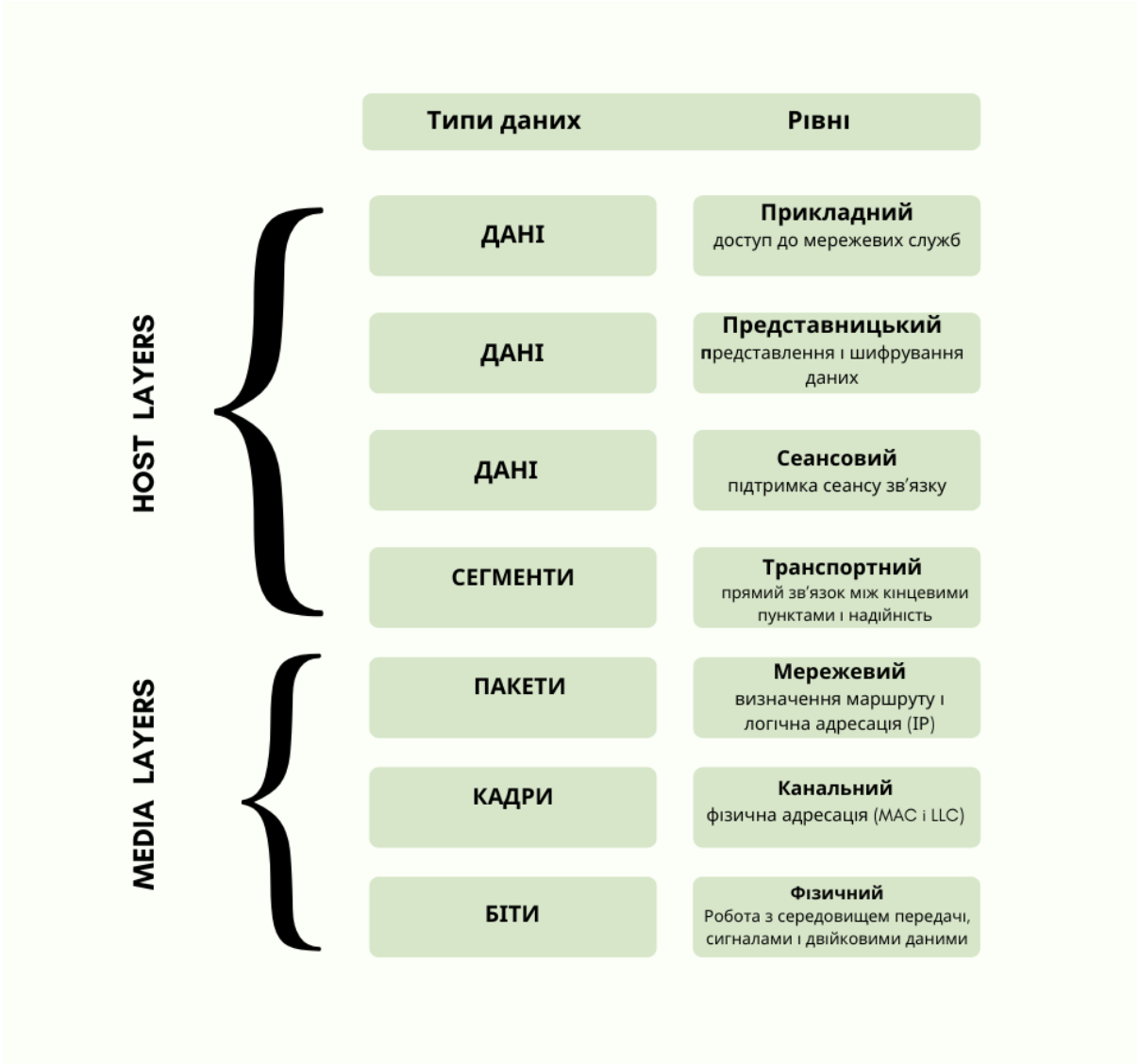


Рис 2.4 Схема порівняння моделей OSI та TCP/IP із основними характеристиками рівнів

Хоча обидві моделі мають суттєві відмінності, вони доповнюють одна одну. OSI забезпечує структурований підхід до вивчення мережевих технологій, а TCP/IP пропонує практичні рішення для реальних завдань. Завдяки їхньому

поєднанню спеціалісти можуть не лише розуміти принципи роботи мереж, але й ефективно застосовувати ці знання на практиці.

Протоколи є основою функціонування комп'ютерних мереж. Вони визначають правила, за якими пристрої обмінюються даними, забезпечують ефективність, надійність і безпеку цього процесу. Протокол можна порівняти з мовою, якою спілкуються пристрої у мережі. Завдяки протоколам різні пристрої та програми, навіть створені різними виробниками, можуть взаємодіяти.

Один із найважливіших протоколів – це IP (Internet Protocol), який використовується для передачі даних у мережах TCP/IP. Він відповідає за маршрутизацію пакетів даних від джерела до одержувача. IP працює за принципом адресації, тобто кожен пристрій у мережі має унікальну IP-адресу, яка ідентифікує його серед інших. Наприклад, коли ви відкриваєте вебсайт, ваш запит надсилається на IP-адресу сервера, який відповідає за цей ресурс.

Ще одним важливим протоколом є TCP (Transmission Control Protocol), який забезпечує надійну доставку даних. TCP гарантує, що всі пакети будуть доставлені у правильному порядку, навіть якщо вони надходять по різних маршрутах. Це особливо важливо для таких додатків, як електронна пошта або завантаження файлів, де втрата частини даних може зробити їх непридатними.

UDP (User Datagram Protocol) є альтернативою TCP і використовується у випадках, коли швидкість передачі важливіша за надійність. Наприклад, у потоковому відео або голосових дзвінках через Інтернет невеликі втрати даних не критичні, але затримки можуть суттєво вплинути на якість.

DNS (Domain Name System) – це протокол, який дає змогу перетворювати доменні імена на IP-адреси. Наприклад, коли ви вводите у браузері "www.example.com", DNS знаходить відповідну IP-адресу сервера, який обслуговує цей сайт. Це дає змогу користувачам не запам'ятовувати складні числові адреси, що значно спрощує роботу з Інтернетом.

DHCP (Dynamic Host Configuration Protocol) автоматично призначає IP-адреси пристроям у мережі. Наприклад, коли ви підключаєтеся до Wi-Fi, DHCP-

сервер надає вашому пристрою IP-адресу, маску підмережі та інші налаштування, необхідні для роботи у мережі.

ARP (Address Resolution Protocol) працює на рівні локальних мереж і перетворює IP-адреси на MAC-адреси, що дає змогу пристроям знаходити один одного у фізичному сегменті мережі. Це особливо важливо для взаємодії у межах однієї підмережі.

Протоколи забезпечують гнучкість і масштабованість мереж, дозволяючи адаптувати їх до різних завдань і умов. Розуміння принципів роботи протоколів є ключовим для проєктування, адміністрування та оптимізації комп'ютерних мереж. У сучасному світі зростаюча складність мережевих систем вимагає від спеціалістів глибоких знань про протоколи і їхню взаємодію.

Інтеграція рівнів архітектури є ключовим принципом, який забезпечує ефективну роботу комп'ютерних мереж. Кожен рівень, визначений у моделях OSI чи TCP/IP, виконує специфічні функції, проте всі вони тісно взаємодіють один з одним, утворюючи єдину систему. Саме завдяки цій взаємодії дані можуть передаватися від користувача до користувача, незалежно від складності мережевої інфраструктури.

Передача даних у мережі починається на прикладному рівні, де користувач взаємодіє з додатками. Наприклад, коли ви надсилаєте електронний лист, додаток для електронної пошти створює повідомлення. На цьому рівні визначаються формат і зміст даних, які потрібно передати.

Далі дані проходять через транспортний рівень, який відповідає за розбиття їх на пакети. Наприклад, якщо ви передаєте великий файл, транспортний рівень розділяє його на частини, які можуть бути відправлені окремо. На цьому етапі також додається інформація про порядок збирання пакетів, щоб їх можна було коректно об'єднати на боці одержувача.

На мережевому рівні визначається маршрут, яким пакети будуть передані до одержувача. Кожен пакет отримує IP-адресу, яка використовується для його доставки. Наприклад, якщо ви відправляєте дані з одного континенту на інший,

мережевий рівень визначить оптимальний шлях через різні маршрутизатори і мережеві вузли.

Канальний рівень відповідає за доставку пакетів у межах локальної мережі. Він забезпечує передачу даних через фізичне середовище, наприклад, кабель чи Wi-Fi. На цьому етапі використовуються MAC-адреси, які дають можливість знайти конкретний пристрій у межах мережі.

Фізичний рівень є останньою ланкою, через яку дані передаються у вигляді електричних сигналів, оптичних імпульсів або радіохвиль. Наприклад, у випадку з оптоволоконними мережами інформація передається у вигляді світлових сигналів, які кодують дані.

Після того як дані досягають одержувача, вони проходять той самий шлях у зворотному напрямку. Кожен рівень на боці отримувача виконує свої функції, розшифровуючи інформацію, додаючи необхідні дані чи об’єднуючи пакети. Наприклад, транспортний рівень збирає всі частини файлу у вихідний формат, а прикладний рівень відображає його у додатку користувача.

Інтеграція рівнів забезпечує прозорість і універсальність мереж. Користувачам не потрібно знати, як працюють всі ці механізми, адже вони автоматизовані і приховані від очей. Водночас фахівці, які займаються проєктуванням чи адмініструванням мереж, повинні розуміти принципи цієї взаємодії, щоб забезпечити надійність і продуктивність систем.

Архітектура "Термінал – головний комп'ютер" (Mainframe-Terminal)

Ця модель була однією з перших у комп'ютерних мережах і досі залишається актуальною у сферах, де важливі централізоване зберігання даних і висока обчислювальна потужність. Головний комп'ютер (мейнфрейм) виконує всі обчислення, а термінали лише передають запити і відображають результати.

Особливості роботи. Термінали не мають власної обчислювальної потужності, тому вони повністю залежать від центрального вузла. Доступ до ресурсів здійснюється лише через головний комп'ютер, що спрощує управління.

Перевагами цієї архітектури є:

- Централізоване управління, що спрощує адміністрування та технічну підтримку.
- Високий рівень безпеки завдяки зберіганню даних в одному місці з обмеженим доступом.
- Мінімальні вимоги до обладнання на стороні користувача (прості термінали).

Звісно, є і недоліки:

- Висока залежність від головного комп'ютера: відмова мейнфрейма паралізує всю систему.
- Обмежена масштабованість, оскільки продуктивність мережі обмежується можливостями центрального комп'ютера.

Прикладами таких архітектур є банківські системи, державні установи, великі корпорації з високими вимогами до обробки даних.

Одноранговa архітектура (Peer-to-Peer)

Peer-to-Peer (P2P) – це децентралізована модель, у якій кожен комп'ютер у мережі може бути як клієнтом, так і сервером. Пристрої безпосередньо обмінюються даними, без необхідності центрального сервера.

Особливості роботи. Кожен комп'ютер самостійно керує своїми ресурсами і може надавати їх іншим пристроям. Це забезпечує простоту налаштування, але ускладнює адміністрування великих мереж.

Перевагами цієї архітектури є:

- Простота налаштування – не потрібен окремий сервер.
- Гнучкість у спільному доступі до файлів та принтерів.
- Відсутність єдиної точки відмови (якщо один комп'ютер вимкнеться, інші продовжать працювати).

Звісно, є і недоліки:

- Низький рівень безпеки – дані розподілені між пристроями.
- Погана масштабованість – продуктивність падає зі збільшенням кількості пристроїв.

Прикладами таких архітектур є домашні мережі, невеликі офіси, платформи для обміну файлами (наприклад, торренти).

Архітектура "Клієнт – сервер" (Client-Server)

Ця модель є найпопулярнішою у сучасних мережах завдяки високій ефективності. Сервери обробляють запити клієнтів і надають доступ до ресурсів, додатків або інформації.

Особливості роботи. Клієнти надсилають запити на сервер, який обробляє їх і надсилає відповідь. Це забезпечує централізований контроль, але робить сервер критично важливим вузлом.

Перевагами цієї архітектури є:

- Висока продуктивність і швидкість обробки запитів.
- Централізоване управління безпекою, резервним копіюванням та оновленнями.
- Легка масштабованість: можна додавати більше серверів для збільшення потужності.

Звісно, є і недоліки:

- Необхідність витрат на серверне обладнання.
- Сервер – єдина точка відмови, хоча це можна вирішити кластеризацією або резервуванням.

Прикладами таких архітектур є вебсайти, хмарні платформи, корпоративні системи управління (CRM, ERP).

Сучасні комп’ютерні мережі стикаються з численними викликами, які вимагають постійної адаптації архітектури до нових умов і потреб. Зі зростанням

обсягів даних, кількості пристроїв і складності систем, вимоги до архітектури мереж постійно змінюються. Ці виклики охоплюють як технічні, так і організаційні аспекти.

Один із ключових викликів – це бездротові технології. Зі зростанням популярності Wi-Fi, мобільних мереж 5G і пристроїв Інтернету речей (IoT), архітектура мереж повинна забезпечувати стабільний і безперервний зв'язок у бездротовому середовищі. Наприклад, 5G пропонує високу швидкість передачі даних і мінімальні затримки, але потребує великої кількості базових станцій та нових підходів до маршрутизації і управління ресурсами.

Хмарні обчислення стали ще одним викликом для традиційної архітектури. У хмарних мережах дані та програми розташовані на віддалених серверах, що вимагає ефективної передачі інформації між користувачем і центром обробки даних. Наприклад, служби, такі як Google Drive чи Dropbox, повинні забезпечувати швидкий доступ до файлів навіть при великому навантаженні на систему.

Кібербезпека залишається одним із найбільших викликів. Зі зростанням кількості атак, таких як DDoS, фішинг та шкідливі програми, архітектура мереж повинна бути оснащена багаторівневими механізмами захисту. Це включає використання брандмауерів, шифрування, систем виявлення вторгнень та багатофакторної аутентифікації. Наприклад, у корпоративних мережах активно використовуються VPN для захищеного доступу до внутрішніх ресурсів.

Ще один виклик пов'язаний із масштабованістю мереж. Зі збільшенням кількості пристроїв, підключених до мережі, архітектура повинна забезпечувати її розширення без втрати продуктивності. Це особливо актуально для Інтернету речей, де мільярди пристроїв потребують одночасного підключення і управління. Технології, такі як IPv6, були розроблені саме для розв'язання цієї проблеми, забезпечуючи практично необмежений простір адресації.

Окрім технічних аспектів, важливим викликом є управління складними мережами. Великі організації часто використовують програмно-визначені мережі (SDN), які дають можливість централізовано управляти конфігурацією і

ресурсами мережі. Це значно підвищує гнучкість і зменшує витрати на обслуговування.

Сучасні виклики вимагають постійного розвитку мережевих технологій і впровадження інновацій. Архітектура мереж повинна бути адаптивною, щоб відповідати зростаючим потребам бізнесу, науки і суспільства. Знання цих викликів дає змогу фахівцям ефективніше працювати з мережами і проєктувати системи, які витримують навантаження сучасного світу.

Архітектура комп'ютерних мереж є критично важливим аспектом, який визначає спосіб функціонування мережевих систем, забезпечує їхню надійність, ефективність та безпеку. Розуміння основ архітектури дає змогу не лише будувати нові мережі, а й удосконалювати існуючі, адаптуючи їх до сучасних викликів.

Моделі OSI та TCP/IP стали основою для розробки мережевих технологій. OSI слугує теоретичним каркасом, який допомагає зрозуміти і пояснити складні процеси передачі даних у мережах. TCP/IP, зі свого боку, забезпечує практичні рішення, які лежать в основі роботи сучасного Інтернету. Їхнє поєднання створює комплексний підхід до аналізу та управління мережами.

Протоколи відіграють ключову роль у функціонуванні мереж. Вони забезпечують обмін інформацією, організовують передачу даних, маршрутизацію, шифрування та багато іншого. Без них будь-яка мережа була б хаотичною системою, у якій пристрої не змогли б ефективно взаємодіяти. Протоколи, такі як IP, TCP, UDP, DNS та інші, є основою для реалізації різноманітних функцій, необхідних для повсякденної роботи з мережами.

Сучасні виклики вимагають постійної адаптації архітектури до нових технологій і умов. Розвиток бездротових технологій, хмарних обчислень, Інтернету речей та 5G значно змінюють підходи до побудови мереж. Окрім того, щораз більша складність систем і загроза кіберзлочинності вимагають впровадження нових рішень для забезпечення безпеки та масштабованості.

Підсумовуючи, можна сказати, що розуміння архітектури мереж є основою для створення ефективних, безпечних і масштабованих систем. Це знання

необхідне для роботи у сфері інформаційних технологій, де мережі відіграють одну з центральних ролей.

Лекція 3. Топології та компоненти комп'ютерних мереж

Топологія та компоненти комп'ютерних мереж є основою, яка визначає функціонування будь-якої мережевої системи. Топологія задає фізичну або логічну структуру, що описує, як пристрої у мережі взаємодіють, тоді як компоненти забезпечують технічну реалізацію цієї взаємодії. Без належного вибору топології та компонентів неможливо створити ефективну, стабільну й безпечну мережу.

Поняття топології включає кілька аспектів, серед яких фізичне розташування пристроїв і канали зв'язку між ними, а також логічний спосіб обміну даними. Наприклад, у домашній мережі фізична топологія може виглядати як один маршрутизатор, до якого підключені смартфони, ноутбуки й телевізори, тоді як логічна топологія описує, як ці пристрої взаємодіють, передаючи дані через маршрутизатор. Вибір топології впливає на ключові параметри мережі, такі як швидкість передачі даних, стійкість до збоїв і можливість масштабування.

Не менш важливими є компоненти мережі, які виконують специфічні функції у її роботі. Від мережевих адаптерів, які забезпечують підключення пристроїв до мережі, до серверів, які зберігають і обробляють дані, кожен компонент відіграє важливу роль. Наприклад, комутатори забезпечують передачу даних між пристроями у локальній мережі, тоді як маршрутизатори відповідають за з'єднання різних мереж і вибір оптимального маршруту для передачі даних.

У сучасному світі, де обсяги даних постійно зростають, а кількість підключених пристроїв досягає мільярдів, грамотне проєктування топології та вибір компонентів стають дедалі складнішими завданнями. Мережі повинні не лише підтримувати високий рівень продуктивності, але й залишатися адаптивними до нових технологій, таких як хмарні обчислення, Інтернет речей (IoT) чи мобільні мережі 5G. Наприклад, у великих корпораціях мережі

проєктуються так, щоб витримувати надзвичайно високі навантаження і забезпечувати безперебійну роботу навіть у разі виходу з ладу одного з компонентів.

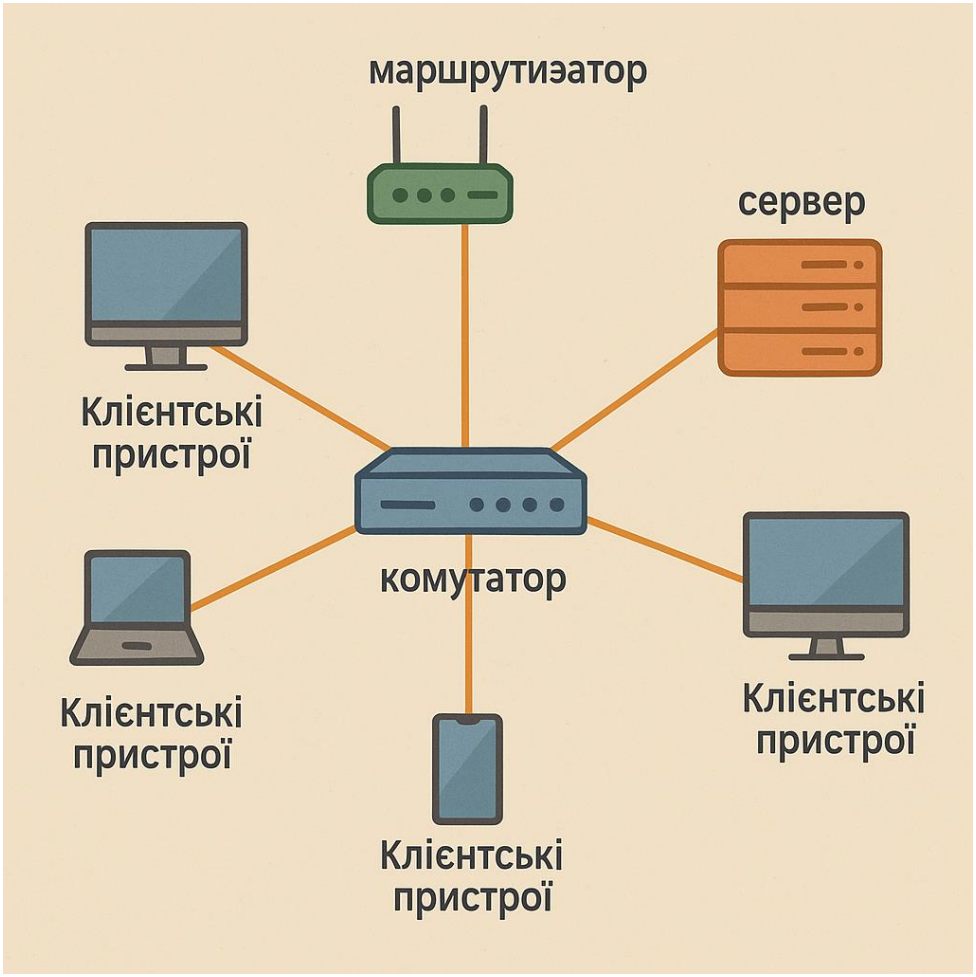


Рис 3.1 Схема топології "зірка"

Топологія мережі – це ключовий аспект її побудови, що визначає спосіб з’єднання пристроїв і організацію передачі даних між ними. Вибір топології впливає на швидкість, надійність, вартість і можливість масштабування мережі. У сучасних мережах використовуються різні типи топологій, кожна з яких має свої переваги і недоліки.

Одна з найпростіших топологій – **шина**. У цій конфігурації всі пристрої підключаються до одного загального кабелю, який слугує спільним середовищем для передачі даних. Шина є економним варіантом для невеликих мереж, оскільки вимагає мінімальної кількості кабелів. Проте ця топологія має значні недоліки: у

разі розриву кабелю вся мережа перестає працювати, а одночасна передача даних кількома пристроями може спричинити колізії.

Топологія **зірка** є однією з найпоширеніших у сучасних локальних мережах. У ній всі пристрої підключаються до центрального вузла, такого як комутатор або маршрутизатор. Це забезпечує високу швидкість передачі даних і легкість у діагностиці проблем, адже несправність одного пристрою не впливає на роботу всієї мережі. Однак центральний вузол стає критичною точкою відмови: якщо він виходить з ладу, мережа перестає функціонувати.

Кільце – це топологія, у якій кожен пристрій з'єднаний із двома сусідніми, утворюючи замкнутий контур. Дані передаються по колу в одному напрямку, що дає змогу уникнути колізій. Проте головним недоліком є те, що вихід з ладу одного пристрою або з'єднання може зупинити роботу всієї мережі. Для усунення цієї проблеми використовуються подвоєні кільця або механізми резервування.

Сітка є найбільш надійною топологією, оскільки кожен вузол з'єднаний з кількома іншими. Це забезпечує надмірність, адже у разі виходу з ладу одного з'єднання дані можуть передаватися альтернативним шляхом. Сітка часто використовується у великих корпоративних або державних мережах, де критично важлива безперебійність роботи. Проте така топологія є дорогою і складною у налаштуванні.

Окрім основних, існують змішані топології, які поєднують елементи різних конфігурацій. Наприклад, у великих організаціях часто використовують поєднання зірки і сітки, де окремі відділи підключені до центрального вузла, а між підрозділами забезпечується резервування.

Рис 3.2 Порівняльна таблиця основних топологій із їх перевагами та недоліками

Кожен тип топології має свої сфери застосування. Наприклад, шина може використовуватися у невеликих офісах чи домашніх мережах, зірка – у сучасних офісах або навчальних закладах, а сітка – у великих дата-центрах чи урядових установах. Розуміння цих топологій допомагає вибрати оптимальну структуру для конкретних завдань.

Комп’ютерна мережа складається з різноманітних компонентів, кожен із яких виконує специфічну роль у забезпеченні її функціонування. Ці компоненти працюють разом, створюючи інфраструктуру для передачі даних, управління

трафіком і забезпечення безпеки. Вибір правильних компонентів є ключовим для досягнення оптимальної продуктивності мережі.

Мережеві адаптери є базовим компонентом, який дає змогу пристроям підключатися до мережі. Вони можуть бути дротовими або бездротовими, залежно від типу мережі. Наприклад, ноутбук із вбудованим Wi-Fi адаптером може підключатися до бездротової мережі, тоді як настільний комп'ютер часто потребує Ethernet-адаптера для підключення через кабель. Сучасні адаптери підтримують високі швидкості передачі даних, а також забезпечують оптимізацію трафіку.

Комутатори є центральними пристроями у багатьох локальних мережах (LAN). Вони забезпечують передачу даних між пристроями, що підключені до мережі. Комутатори працюють на канальному рівні і використовують MAC-адреси для спрямування даних до правильного пристрою. Існують два основні типи комутаторів: **керовані** та **некеровані**. Керовані комутатори дозволяють адміністратору гнучко налаштовувати параметри мережі, тоді як некеровані працюють за принципом "підключай і працюй", не вимагаючи додаткових налаштувань. Маршрутизатори відповідають за з'єднання різних мереж і маршрутизацію трафіку між ними. Вони працюють на мережевому рівні і використовують IP-адреси для визначення найкращого маршруту передачі даних. Наприклад, домашній маршрутизатор з'єднує вашу локальну мережу з Інтернетом, забезпечуючи при цьому базовий захист, такий як брандмауер або NAT. У великих мережах маршрутизатори використовуються для складної маршрутизації між різними підмережами.

Сервери є основними вузлами у багатьох мережах. Вони забезпечують зберігання, обробку і розповсюдження даних. Наприклад, файлові сервери дають можливість користувачам отримувати доступ до спільних документів, вебсервери обслуговують вебсторінки, а поштові сервери керують електронною кореспонденцією. Сервери можуть бути фізичними або віртуальними, залежно від потреб і масштабу мережі.

Клієнтські пристрої – це кінцеві точки мережі, які взаємодіють із її ресурсами. Це можуть бути комп’ютери, смартфони, принтери або навіть пристрої Інтернету речей, такі як "розумні" датчики чи камери спостереження. Клієнтські пристрої отримують доступ до мережі через адаптери, комутатори та маршрутизатори, використовуючи різні протоколи для обміну даними.

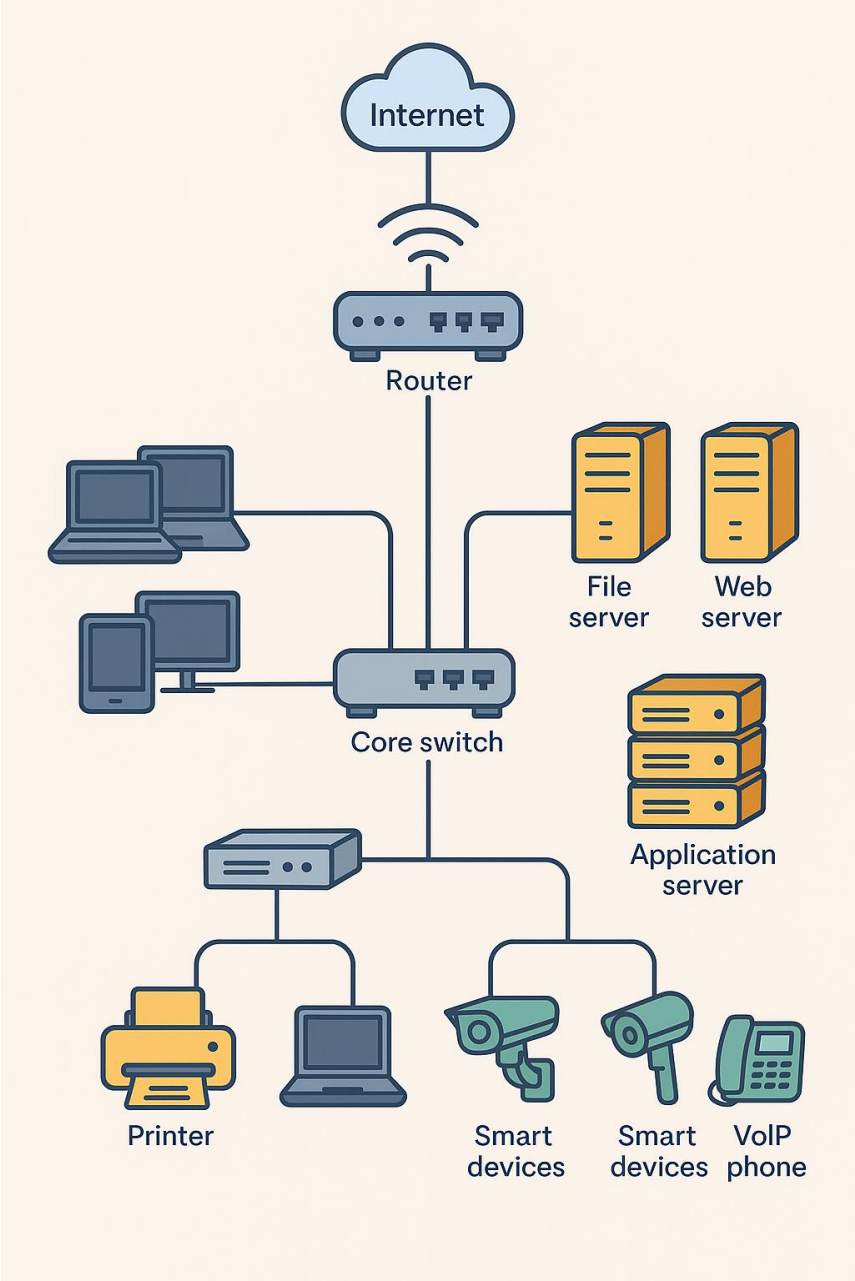


Рис 3.3 Схема мережі, яка включає маршрутизатор, комутатори, сервери, клієнтські пристрої та їх взаємодію

Вибір і конфігурація компонентів мережі залежить від її масштабу та призначення. Наприклад, у домашніх умовах достатньо маршрутизатора з інтегрованим комутатором, тоді як у великих організаціях використовуються

десятки спеціалізованих пристроїв. Кожен компонент має свої технічні характеристики, які важливо враховувати для досягнення необхідного рівня продуктивності і безпеки.

Вибір правильної топології та компонентів є критичним етапом у проєктуванні мережі. Ці рішення впливають на продуктивність, масштабованість, стійкість до збоїв та вартість створення і обслуговування мережі. Різні сценарії використання вимагають різних підходів, і розуміння основних критеріїв вибору допомагає знайти оптимальне рішення.

При виборі топології одним із головних критеріїв є масштаб мережі. Для невеликих локальних мереж, таких як домашні або офісні, часто обирають топологію "зірка", яка забезпечує високу швидкість передачі даних і легкість у налаштуванні. Наприклад, маршрутизатор, підключений до комп’ютерів і принтерів, є класичним прикладом такої топології. Для більших організацій, які потребують надійності та масштабованості, може використовуватися змішана топологія, що поєднує "зірку" і "сітку". Це дає змогу знизити ризик відмови окремих елементів і забезпечити резервні маршрути передачі даних.

Ще одним важливим аспектом є призначення мережі. Наприклад, у закладі освіти топологія може бути спроєктована так, щоб забезпечити легкий доступ студентів до освітніх ресурсів, тоді як у комерційній організації мережа повинна підтримувати ефективну роботу бізнес-процесів. У першому випадку більший акцент робиться на доступності та швидкості передачі даних, тоді як у другому – на безпеці і резервуванні.

Щодо вибору компонентів, вирішальним фактором є їхні технічні характеристики. Наприклад, у локальних мережах невеликих офісів часто використовуються некеровані комутатори, які не потребують складного налаштування. Для великих організацій керовані комутатори є кращим вибором, оскільки вони дають можливість налаштовувати пріоритети трафіку, балансувати навантаження і забезпечувати високий рівень безпеки.

Маршрутизатори також обираються залежно від масштабів і потреб мережі. У домашніх умовах зазвичай використовуються універсальні пристрої, які

об’єднують функції маршрутизатора, комутатора і точки доступу Wi-Fi. У корпоративних мережах використовуються високопродуктивні маршрутизатори, здатні обробляти великі обсяги трафіку і забезпечувати резервування каналів зв’язку.

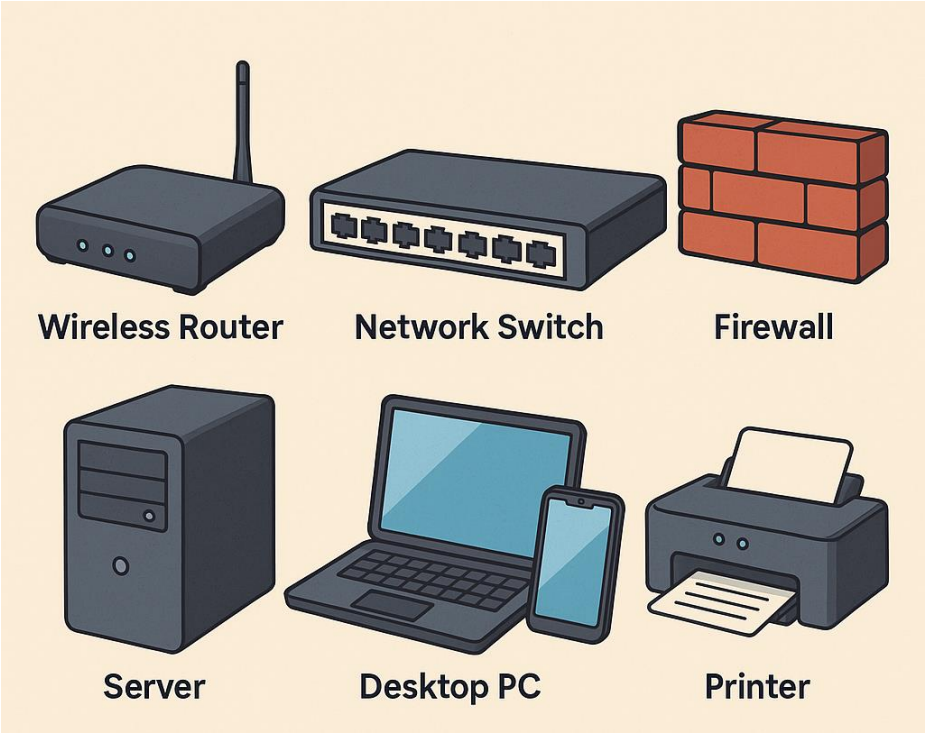


Рис 3.4 Приклад вибору компонентів для малої офісної мережі

Резервування і стійкість до відмов також є важливими критеріями. У критичних системах, таких як фінансові установи чи лікарні, використовуються дубльовані комутатори, сервери і навіть канали зв’язку, щоб забезпечити безперебійну роботу мережі навіть у разі відмови обладнання. Це значно підвищує надійність системи, хоча й збільшує витрати.

Вибір топології та компонентів – це складний процес, який вимагає врахування багатьох факторів. Проте правильні рішення на етапі проєктування забезпечують не лише ефективність і безпеку мережі, але й значну економію ресурсів у майбутньому.

Розподіл навантаження є важливим аспектом побудови ефективних комп’ютерних мереж, особливо коли мова йде про системи з великим обсягом трафіку чи високими вимогами до доступності. Цей процес полягає у рівномірному розподілі трафіку між вузлами мережі або серверами, що дає змогу

уникнути перевантажень, мінімізувати затримки і підвищити продуктивність системи.

Одним із основних методів розподілу навантаження є використання балансувальників навантаження. Балансувальники працюють на рівні мережі або додатків, перенаправляючи трафік на ті сервери чи вузли, які мають найменше навантаження в конкретний момент часу. Наприклад, у вебхостингу балансувальники навантаження дають можливість обробляти тисячі запитів користувачів, рівномірно розподіляючи їх між кількома вебсерверами. Це забезпечує високу швидкість завантаження сторінок навіть під час пікових навантажень.

Іншим важливим аспектом є вертикальне і горизонтальне масштабування мережевих ресурсів. Вертикальне масштабування передбачає збільшення потужності окремих вузлів, наприклад, додавання оперативної пам’яті або потужніших процесорів на серверах. Горизонтальне масштабування, навпаки, полягає у збільшенні кількості вузлів, які обслуговують трафік. Наприклад, додавання нових серверів у кластер дає змогу підвищити загальну продуктивність мережі.

Однією з сучасних практик є використання хмарних технологій для розподілу навантаження. Хмарні платформи, такі як Amazon Web Services (AWS) або Google Cloud, дають можливість динамічно збільшувати або зменшувати кількість ресурсів залежно від поточних потреб. Це дає змогу не лише підвищити ефективність, але й оптимізувати витрати, оскільки ви платите лише за використані ресурси.

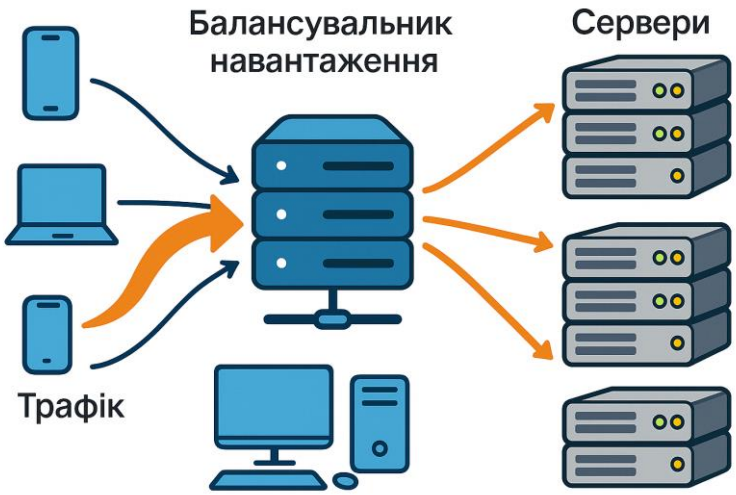


Рис 3.5 Схема роботи балансувальника навантаження, який перенаправляє трафік між декількома серверами

Методи розподілу навантаження також застосовуються до мережевого обладнання. Наприклад, у маршрутизаторах із підтримкою протоколу Equal-Cost Multi-Path (ECMP) трафік розподіляється між кількома маршрутами з однаковою вартістю. Це дає змогу збільшити пропускну здатність мережі і забезпечити надійність у разі відмови одного з маршрутів.

Розподіл навантаження також відіграє важливу роль у забезпеченні відмовостійкості. Наприклад, у критичних системах, таких як електронна комерція або онлайн-банкінг, використання кластерів серверів із балансувальниками дає змогу забезпечити безперебійну роботу навіть у разі виходу з ладу одного або декількох вузлів.

Ефективний розподіл навантаження забезпечує стабільну роботу мережі та підвищує якість обслуговування користувачів. Це є невід'ємною частиною сучасного проєктування мережевих систем, особливо у масштабних або критично важливих інфраструктурах.

Сучасні тенденції у розвитку мережевих технологій значно впливають на вибір компонентів та топологій, які використовуються у побудові інфраструктури. Зростання обсягів даних, збільшення кількості підключених пристроїв та потреба у високій продуктивності сприяють впровадженню нових підходів і рішень у цій галузі.

Одним із найважливіших трендів є впровадження програмно-визначених мереж (SDN). SDN дають можливість розділити управління мережею і її фізичну інфраструктуру. Це забезпечує централізоване управління трафіком, підвищує гнучкість і спрощує масштабування. Наприклад, у великих дата-центрах SDN використовуються для оптимізації потоків даних, забезпечення автоматизації управління та швидкого впровадження нових сервісів.

Інший важливий тренд – це інтеграція віртуалізації у топології мереж. Завдяки віртуалізації можна створювати логічні мережі, які функціонують поверх фізичних, що забезпечує економію ресурсів і підвищення продуктивності. Наприклад, у хмарних середовищах віртуалізовані мережі дають можливість користувачам динамічно налаштовувати ресурси відповідно до своїх потреб, незалежно від фізичної інфраструктури.

Топології мереж також адаптуються до нових викликів. Наприклад, у мережах Інтернету речей (IoT) активно використовуються децентралізовані топології, які забезпечують низькі затримки і високу надійність. У розумних містах чи промислових мережах децентралізація дає змогу обробляти дані безпосередньо на рівні пристроїв, зменшуючи залежність від центральних серверів.

Ще одним трендом є використання високопродуктивних компонентів, таких як комутатори і маршрутизатори, здатні працювати зі швидкостями 100 Гбіт/с і вище. Такі компоненти необхідні для сучасних дата-центрів, що обслуговують глобальні сервіси, такі як стрімінгові платформи чи соціальні мережі. Наприклад, у мережах Amazon або Google використання надшвидких комутаторів дає змогу обробляти мільярди запитів у режимі реального часу.

Зростає популярність гібридних рішень, які поєднують хмарні і локальні інфраструктури. Такі рішення дають можливість організаціям зберігати чутливі дані на власних серверах, використовуючи при цьому хмарні ресурси для масштабування і обробки даних. Це особливо важливо для банківської сфери, охорони здоров’я та інших галузей, де безпека даних є критично важливою.

Сучасні тренди у компонентах і топологіях відкривають нові можливості для побудови ефективних, гнучких і безпечних мереж. Вони дають можливість розв’язувати складні завдання сучасного світу, зокрема забезпечувати стабільну роботу критично важливих сервісів, обробку величезних обсягів даних і інтеграцію інноваційних технологій.

Топології та компоненти комп’ютерних мереж є фундаментальними елементами, які визначають їхню продуктивність, надійність і масштабованість. Розуміння різних типів топологій дає змогу проєктувати мережі, що відповідають конкретним потребам користувачів чи організацій. Від простої шини до складної сітки, кожна топологія має свої переваги та недоліки, які важливо враховувати при виборі.

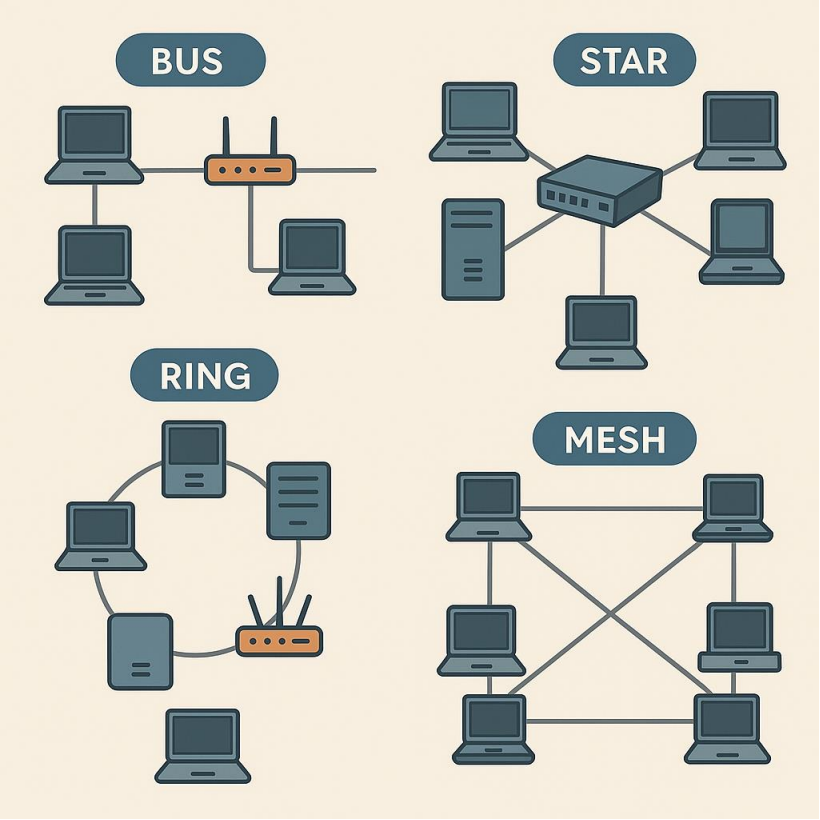


Рис 3.6 Схема з основних топологій

Компоненти мережі, такі як маршрутизатори, комутатори, сервери та клієнтські пристрої, працюють разом, забезпечуючи передачу даних, обробку інформації та доступ до ресурсів. Кожен компонент виконує свої функції, які доповнюють один одного, створюючи ефективну інфраструктуру. Наприклад,

маршрутизатори відповідають за маршрутизацію даних між мережами, тоді як сервери забезпечують зберігання і обробку інформації.

Сучасні тенденції, такі як програмно-визначені мережі (SDN), віртуалізація та інтеграція IoT, змінюють традиційні підходи до побудови мереж. Вони дають можливість підвищити гнучкість, автоматизувати управління та адаптувати мережі до нових викликів. Наприклад, у розумних містах чи великих дата-центрах використання сучасних технологій забезпечує стабільність і продуктивність навіть у найскладніших умовах.

Лекція 4. Канали і лінії зв’язку. Кабельні системи

Канали зв’язку є основою будь-якої комп’ютерної мережі, оскільки вони забезпечують фізичне середовище для передачі даних між пристроями. Від правильного вибору типу ліній зв’язку залежить стабільність мережевих підключень, швидкість передачі інформації та загальна продуктивність інформаційної системи. Вплив на якість з’єднання мають різні фактори, серед яких фізичні характеристики середовища передачі, перешкодостійкість, затримки у передачі пакетів та методи кодування сигналу.

Розвиток мережевих технологій спричинив суттєву еволюцію каналів зв’язку. Якщо раніше для комунікаційних потреб використовувалися телефонні лінії, що передавали дані зі швидкістю 56 Кбіт/с, то сучасні оптоволоконні магістралі забезпечують швидкість у десятки терабіт за секунду. Завдяки цьому мережі стали значно надійнішими та продуктивнішими, що дозволило реалізувати такі технології, як хмарні обчислення, передача відео у форматі 4K та 8K, онлайн-ігри у реальному часі та високошвидкісний мобільний Інтернет.

Однією з ключових відмінностей між сучасними каналами зв’язку є спосіб їхньої реалізації. Існують дротові і бездротові канали, кожен із яких має свої переваги та недоліки. Дротові лінії, такі як вита пара або оптоволокно, забезпечують стабільне та швидке з’єднання, проте потребують фізичного прокладання кабелів. Бездротові канали, навпаки, не потребують кабелів, але можуть страждати від перешкод і меншої пропускної здатності.

У сучасних комп’ютерних мережах часто використовується комбінований підхід, що включає як дротові, так і бездротові рішення. Наприклад, у великих дата-центрах та корпоративних мережах використовується оптоволоконне з’єднання для магістральних каналів, тоді як користувачі підключаються до мережі через Wi-Fi. Така стратегія дає змогу досягти оптимального балансу між продуктивністю, гнучкістю та витратами.

З огляду на сучасні тенденції розвитку інформаційних технологій, канали зв’язку продовжують удосконалюватися. Впровадження 5G, розвиток квантових

комунікацій, поліпшення методів захисту від кібератак – усе це сприяє створенню більш надійних та ефективних мереж.

Канал зв’язку – це середовище, через яке передається інформація між відправником і отримувачем у мережі. Він може бути як фізичним (дротові або бездротові середовища передачі), так і віртуальним (логічні канали, створені у межах мережі). Основне завдання каналів зв’язку – забезпечення ефективної, швидкої та надійної передачі даних між вузлами мережі.

У комп’ютерних мережах використовуються різні типи каналів зв’язку, кожен з яких має свої особливості, які визначають їхню ефективність у різних середовищах. Наприклад, у локальних мережах (LAN) найчастіше використовуються дротові з’єднання, такі як Ethernet на основі витої пари або оптоволокна. У мобільних мережах (WAN) основний акцент робиться на бездротових технологіях, таких як 4G, 5G та супутниковий зв’язок.

Канали зв’язку класифікуються за кількома критеріями. Один із основних – це тип середовища передачі:

- Дротові канали – використовують фізичні кабелі для передачі даних. До них належать мідні кабелі (вита пара, коаксіальний кабель) та волоконно-оптичні лінії.
- Бездротові канали – використовують електромагнітні хвилі для передавання сигналу. До них належать Wi-Fi, мобільний зв’язок (4G/5G), супутниковий зв’язок, радіорелейні системи.

Ще один критерій класифікації – метод доступу до каналу:

- дуплексні канали – забезпечують одночасну двосторонню передачу даних (наприклад, телефонні лінії та Ethernet);
- напівдуплексні канали – допускають передавання даних лише в одному напрямку за раз (наприклад, рації, де передача та прийом сигналу відбуваються по черзі);
- симплексні канали – передають інформацію лише в одному напрямку без можливості зворотного зв’язку (наприклад, телевізійне мовлення).

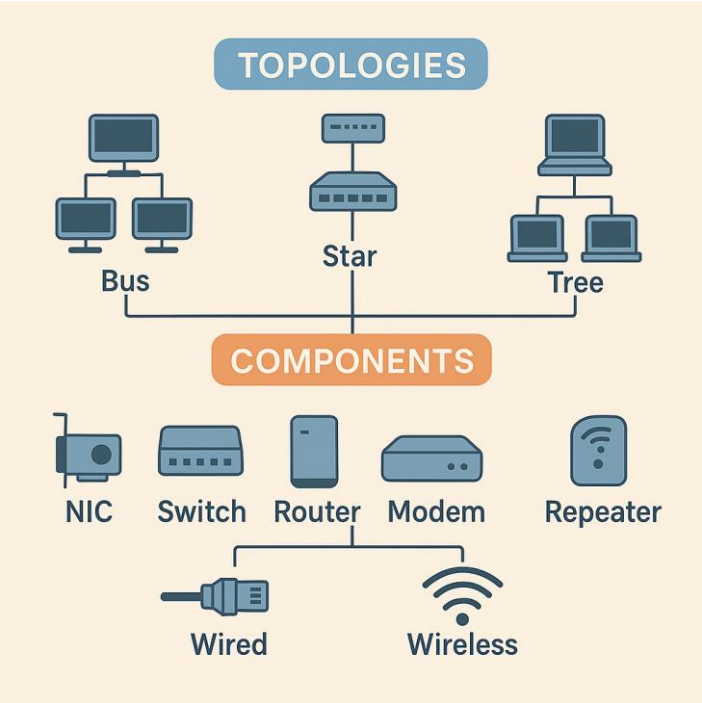


Рис 4.1 Схема класифікації каналів зв'язку за типами середовища та методом доступу

Ще один важливий аспект – стандартизація каналів зв'язку. Для забезпечення сумісності між пристроями та стабільної роботи мережі використовуються міжнародні стандарти, такі як:

- Ethernet (IEEE 802.3) – стандарт для дротових локальних мереж.
- Wi-Fi (IEEE 802.11) – стандарт для бездротових мереж.
- 5G NR (New Radio) – новий стандарт мобільного зв'язку, що забезпечує високу швидкість і низьку затримку.

Окрім фізичних та технологічних параметрів, важливу роль відіграє якість каналу зв'язку, яка визначається такими характеристиками, як пропускна здатність, затримка, рівень шумів та втрата пакетів. Наприклад, у реальному часі (відеоконференції, онлайн-ігри) низькі затримки та стабільний сигнал є важливішими за максимальну швидкість передачі.

Знання основних понять про канали зв'язку дає змогу розуміти, як вони працюють та як їх можна ефективно використовувати в мережах різного типу. Це є основою для подальшого аналізу дротових та бездротових технологій, їхньої ефективності та сфер застосування.

Дротові канали

Дротові канали зв’язку є найбільш стабільним і продуктивним способом передавання даних у мережах. Вони забезпечують високу швидкість, низький рівень перешкод і надійність з'єднання. Завдяки цим характеристикам дротові канали використовуються у локальних мережах (LAN), магістральних лініях зв’язку та центрах обробки даних.

Одним із найпоширеніших типів дротових з’єднань є вита пара. Це кабель, що складається з двох або більше мідних провідників, скручених між собою. Основною причиною такого скручування є зниження рівня електромагнітних перешкод, що покращує якість сигналу.

Існує кілька категорій витої пари, кожна з яких підтримує певний рівень продуктивності:

- CAT5 – забезпечує швидкість до 100 Мбіт/с і використовується у застарілих мережах.
- CAT5e – поліпшена версія, яка підтримує швидкість до 1 Гбіт/с, що робить її стандартом для сучасних офісних і домашніх мереж.
- CAT6 – може працювати на швидкостях до 10 Гбіт/с на відстанях до 55 м, що забезпечує високу продуктивність.
- CAT7 і CAT8 – найновіші версії, які дають можливість передавати дані на швидкостях до 40 Гбіт/с, проте мають значну вартість і складність монтажу.

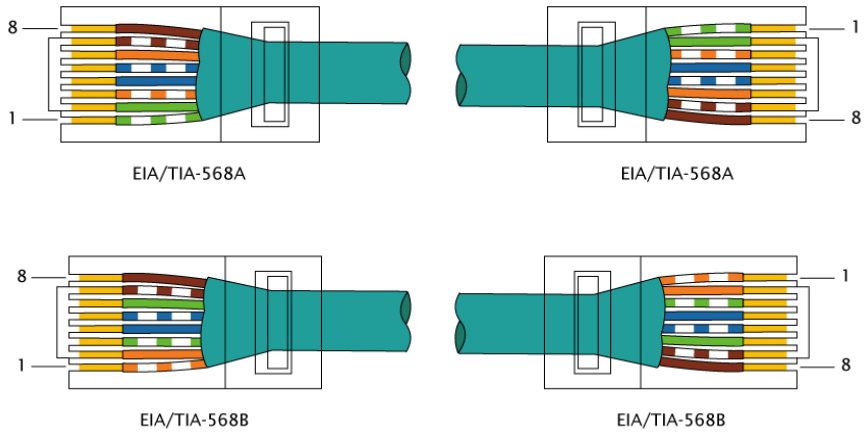


Рис 4.2 Схема розведення витої пари

Ще одним популярним типом дротового з’єднання є **коаксіальний кабель**. Він складається із зовнішньої оболонки. Коаксіальний кабель забезпечує кращий захист від центрального мідного провідника, ізоляційного шару, екрануючого шару та електромагнітних завад порівняно з витою парою, що дає змогу використовувати його для передачі сигналів на більші відстані.

Коаксіальні кабелі традиційно застосовувалися у локальних мережах (наприклад, у мережах типу Ethernet 10BASE2), проте нині вони частіше використовуються у телебаченні, кабельному Інтернеті та системах відеоспостереження.

Переваги коаксіального кабелю:

- висока стійкість до зовнішніх перешкод;
- можливість передачі сигналу на великі відстані без значного затухання;
- використання у мережах із високою щільністю трафіку.

Рис 4.3 Схема розведення витої пари

Одним із найсучасніших та найефективніших дротових каналів зв’язку є **оптоволоконні кабелі**. Вони використовують світлові імпульси для передавання даних, що забезпечує надзвичайно високу швидкість передачі та мінімальні втрати сигналу. Волоконно-оптичні лінії є основою для магістральних мереж, що з’єднують великі міста та країни.

Основні типи оптоволоконних кабелів:

- *Багатомодові (Multimode)* – використовуються для передачі даних на короткі відстані (до 2 км). Вони мають більший діаметр серцевини, що дає змогу одночасно передавати кілька сигналів.

- *Одномодові (Singlemode)* – забезпечують передачу даних на дуже великі відстані (до сотень кілометрів) із мінімальними затуханнями. Використовуються у великих дата-центрах та міжміських магістралях.

Основні переваги оптоволоконних кабелів:

- висока пропускна здатність (до 100 Тбіт/с у лабораторних тестах);
- відсутність електромагнітних перешкод;
- можливість передавання сигналу на великі відстані без значних втрат.

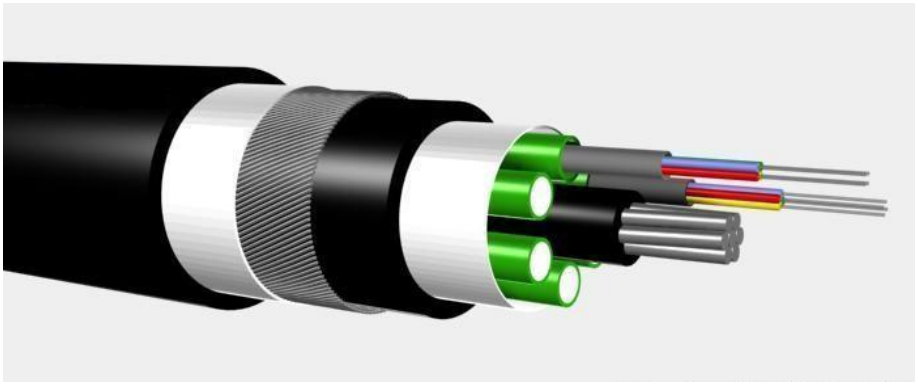


Рис 4.4 Схема оптоволоконного кабелю

Оптоволоконні технології поступово замінюють мідні кабелі у багатьох сферах, особливо у магістральних мережах. Завдяки своїм характеристикам вони є основним засобом побудови високошвидкісного інтернету та центрів обробки даних.

Порівняння дротових каналів зв’язку.

Для того, щоб краще розуміти, який тип дротового з’єднання підходить для різних умов, розглянемо їхні основні характеристики у таблиці:

Тип кабелю	***Швидкість передачі***	***Відстань передачі***	***Вартість***	***Стійкість до перешкод***
Вита пара	До 10 Гбіт/с	До 100 м	Низька	Середня
Коаксіальний	До 1 Гбіт/с	До 500 м	Середня	Висока
Оптоволоконний	До 100 Тбіт/с	До 100 км	Висока	Дуже висока

Таблиця 4.1 Порівняння витої пари, коаксіального кабелю та оптоволокна

Вибір дротового каналу зв’язку залежить від вимог до швидкості, відстані та рівня перешкод. Вита пара є ідеальним варіантом для локальних мереж, коаксіальний кабель залишається корисним для телекомунікаційних і відеосистем, тоді як оптоволоконні технології стають стандартом для високошвидкісних магістральних з’єднань.

Бездротові канали зв’язку забезпечують передачу даних без використання фізичних дротових з’єднань. Вони є ключовим елементом сучасної цифрової інфраструктури, дозволяючи пристроям взаємодіяти без обмежень, пов’язаних із прокладанням кабелів. Завдяки технологічному розвитку бездротові мережі можуть забезпечувати швидку, стабільну та безпечну передачу даних на значні відстані.

Радіохвильові технології

Передача даних у бездротових мережах здійснюється за допомогою електромагнітних хвиль. Вони передають сигнал у різних частотних діапазонах, що визначає дальність і швидкість зв’язку. Радіохвильові технології поділяються на кілька категорій:

- *Низькочастотні системи* (до 1 ГГц) – забезпечують великий радіус дії, але мають низьку швидкість передачі.
- *Середньочастотні системи* (1-6 ГГц) – використовуються у Wi-Fi та мобільному зв’язку.
- *Високочастотні системи* (понад 6 ГГц) – забезпечують дуже високу швидкість, але потребують лінії прямої видимості.

Wi-Fi є найпоширенішою бездротовою технологією, що використовується у локальних мережах. Вона базується на стандартах **IEEE 802.11** і дає змогу передавати дані на швидкостях до кількох гігабіт за секунду. Останні покоління Wi-Fi, такі як **Wi-Fi 6 (802.11ax)** та **Wi-Fi 7**, пропонують вищу продуктивність, поліпшену енергоефективність та знижену затримку.

Основні переваги Wi-Fi:

- Відсутність потреби у прокладанні кабелів.

- Гнучкість і можливість підключення великої кількості пристроїв.
- Достатньо висока швидкість для більшості застосувань.

Недоліки Wi-Fi:

- Залежність від якості сигналу та відстані до точки доступу.
- Вразливість до перешкод від інших бездротових пристроїв.
- Безпекові ризики, пов’язані з можливістю несанкціонованого доступу.

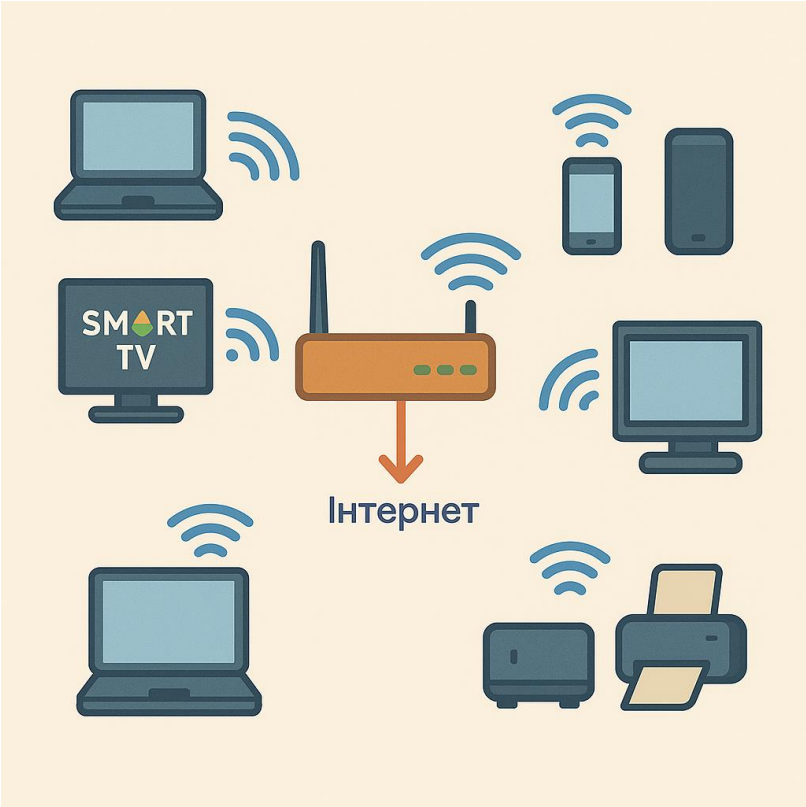


Рис 4.5 Схема роботи Wi-Fi мережі з точкою доступу та підключеними пристроями

Мобільні технології (4G, 5G)

Мобільний зв’язок забезпечує підключення до мережі незалежно від місця перебування користувача. Сучасні технології мобільного Інтернету включають **4G LTE** та **5G**, які дають можливість передавати дані на високих швидкостях.

- **4G LTE** забезпечує середню швидкість передачі даних у діапазоні 50-100 Мбіт/с, що дає змогу комфортно переглядати відео, користуватися інтернетом та здійснювати відеодзвінки.
- **5G** є найсучаснішою мобільною технологією, яка дає змогу передавати дані на швидкостях до **10 Гбіт/с**. Вона забезпечує низьку затримку та підтримує

велику кількість одночасних підключень, що є критично важливим для розвитку **Інтернету речей (IoT)**.

Основні переваги мобільних технологій:

- Висока швидкість передачі даних.
- Широке покриття, що дає змогу отримати доступ до Інтернету практично у будь-якій точці світу.
- Підтримка мобільних пристроїв без необхідності фіксованого підключення.

Супутниковий зв’язок

Супутникові технології використовуються для забезпечення зв’язку у віддалених регіонах, де немає можливості прокласти дротові або наземні бездротові мережі. Сучасні супутникові системи, такі як **Starlink**, забезпечують високу швидкість підключення та низькі затримки.

Переваги супутникового зв’язку:

- Доступність у будь-якому регіоні світу.
- Висока стійкість до фізичних пошкоджень інфраструктури.
- Незалежність від наземної інфраструктури.

Недоліки супутникового зв’язку:

- Висока вартість обладнання та абонентського обслуговування.
- Затримки сигналу через велику відстань між супутниками та користувачами.
- Вплив погодних умов на якість з’єднання.

Рис 4.6 Схема роботи супутникової мережі із передачею даних через супутник

Технологія	***Швидкість передачі***	***Радіус дії***	***Стійкість до перешкод***	***Сфера застосування***
Wi-Fi	До 9,6 Гбіт/с	До 100 м	Середня	Домашні та офісні мережі
4G LTE	До 100 Мбіт/с	До 10 км	Висока	Мобільний інтернет
5G	До 10 Гбіт/с	До 1 км	Висока	IoT, автономний транспорт
Супутниковий зв'язок	До 1 Гбіт/с	Глобальне покриття	Низька	Віддалені регіони

Таблиця 4.2 Порівняння бездротових технологій

Бездротові канали зв'язку відіграють ключову роль у забезпеченні гнучкості мережевих рішень. Вони дають можливість підключати пристрої без потреби у фізичних кабелях, що значно спрощує розгортання та масштабування мереж. Проте для забезпечення високої якості зв'язку важливо правильно підбирати бездротові технології залежно від потреб користувачів і умов експлуатації.

При виборі каналу зв'язку для мережевої інфраструктури важливо враховувати його ключові характеристики. Від цих параметрів залежить продуктивність мережі, стабільність передачі даних, рівень завадостійкості та можливість масштабування.

Пропускна здатність – це максимальна кількість даних, яка може бути передана через канал за одиницю часу. Вона вимірюється у бітах за секунду

(bps), кілобітах (Кбіт/с), мегабітах (Мбіт/с) або гігабітах (Гбіт/с). Висока пропускна здатність є критично важливою для сучасних застосувань, таких як потокове відео, хмарні сервіси та передача великих обсягів даних.

Наприклад:

- Вита пара (CAT5e) підтримує швидкості до 1 Гбіт/с.
- Оптоволоконні канали можуть передавати дані на швидкостях до 100 Тбіт/с.
- Wi-Fi 6 забезпечує пропускну здатність до 9,6 Гбіт/с.
- 5G може підтримувати передачу даних на швидкості до 10 Гбіт/с.

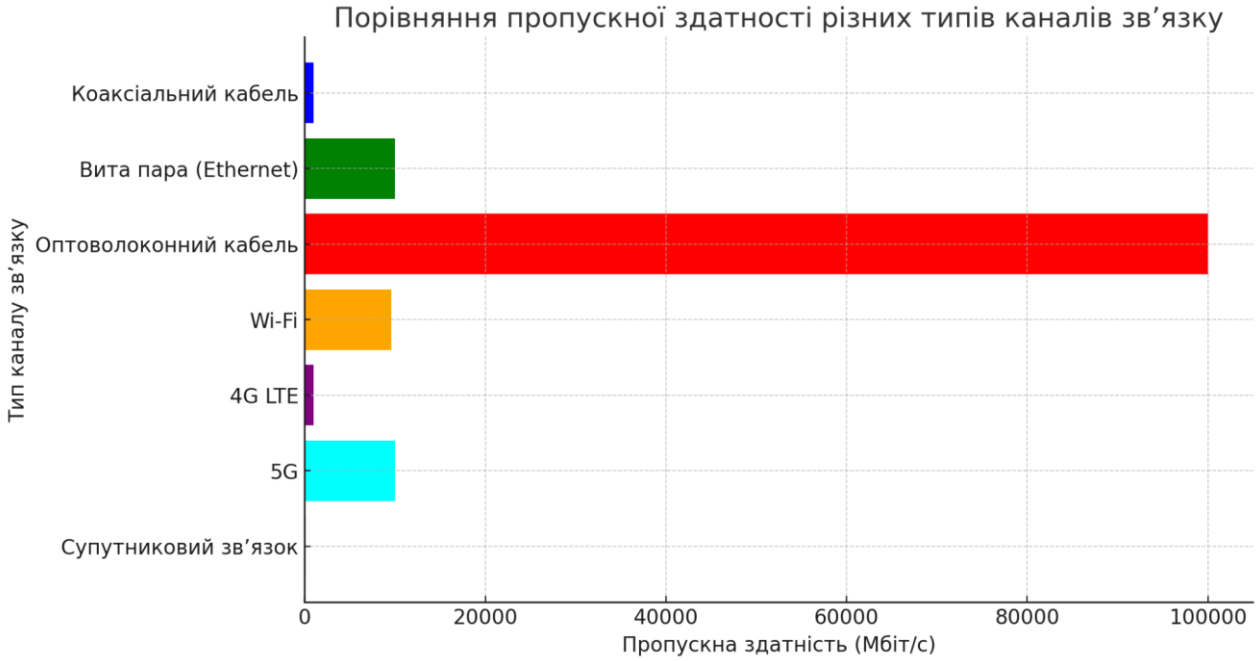


Рис 4.7 Графік порівняння пропускної здатності різних типів каналів зв'язку

Затримка (latency) – це час, необхідний для того, щоб пакет даних дійшов від відправника до одержувача. Вона вимірюється у мілісекундах (мс) і має велике значення для реального часу зв'язку, такого як відеоконференції, онлайн-ігри та хмарні обчислення.

Фактори, що впливають на затримку:

- *Тип середовища передачі* – оптоволоконні канали мають мінімальну затримку, тоді як супутникові з'єднання можуть мати значні затримки через велику відстань до супутника.

- *Кількість проміжних пристроїв* – що більше маршрутизаторів та комутаторів проходить пакет, то більша затримка.
- *Перевантаженість мережі* – високий рівень трафіку може спричинити додаткові затримки через обробку черг.

Перешкодостійкість визначає здатність каналу передавати дані без втрат, незважаючи на зовнішні завади. Електромагнітні перешкоди можуть спричиняти втрати пакетів, що впливає на стабільність з'єднання. Найбільш стійкими до перешкод є **оптоволоконні кабелі**, оскільки вони передають дані світлом і не піддаються електромагнітному впливу.

Методи зниження перешкод:

- *Екрановані кабелі (STP)* – вита пара з додатковим екрануванням, що зменшує вплив електромагнітних завад.
- *Використання волоконно-оптичних ліній* – забезпечує максимальний рівень захисту від перешкод.
- *Сучасні алгоритми корекції помилок* – використовуються у бездротових мережах для виправлення втрат даних.

Надійність – це здатність каналу підтримувати стабільний зв'язок без втрат та аварій. Основні фактори, що впливають на надійність:

- **Тип кабелю** – оптоволокно є найбільш надійним варіантом, тоді як вита пара може зазнавати фізичних пошкоджень.
- **Рівень резервування** – використання дубльованих каналів забезпечує безперебійність зв'язку у разі виходу з ладу одного з них.
- **Системи моніторингу мережі** – дають можливість виявляти несправності ще до їхнього критичного впливу на роботу системи.

Надійні канали зв'язку забезпечують безперебійну роботу мереж у критичних сферах, таких як медицина, фінанси, промисловість та державні структури.

Втрати пакетів виникають, коли пакети даних не досягають місця призначення через завади, перевантаження або технічні несправності. Високий

рівень втрат може призводити до погіршення якості відео, аудіо та інших критичних сервісів.

Методи компенсації втрат:

- **Протокол TCP** – автоматично повторює передачу втрачених пакетів.
- **Протокол UDP з механізмом FEC (Forward Error Correction)** – передає додаткові дані, що дають можливість відновити втрачений пакет без повторного запиту.
- **Оптимізація маршрутизації** – вибір альтернативних маршрутів у разі виявлення проблем із певним сегментом мережі.

Характеристика	***Вита пара (CAT6)***	***Коаксіальний кабель***	***Оптоволокно***	***WI-FI 6***	***5G***
Швидкість	До 10 Гбіт/с	До 1 Гбіт/с	До 100 Тбіт/с	До 9,6 Гбіт/с	До 10 Гбіт/с
Дальність передачі	До 100 м	До 500 м	До 100 км	До 100 м	До 10 км
Перешкодо-стійкість	Середня	Висока	Дуже висока	Середня	Висока
Надійність	Висока	Висока	Дуже висока	Середня	Висока
Втрата пакетів	Середня	Низька	Дуже низька	Висока при перевантаженні	Залежить від покриття

Таблиця 4.2 Порівняльна таблиця характеристик різних каналів зв'язку

Правильний вибір характеристик каналу зв'язку дає змогу забезпечити оптимальну продуктивність мережі, мінімізувати втрати даних і гарантувати стабільне з'єднання. Розуміння цих параметрів є важливим при проєктуванні мереж різного рівня складності – від домашніх з'єднань до великих корпоративних і магістральних мереж.

Структуровані кабельні системи (СКС)

Структуровані кабельні системи (СКС) є основою сучасних корпоративних мереж, оскільки забезпечують надійне й ефективне середовище для передачі

даних між пристроями. Вони складаються із різних типів кабелів, комутаційного обладнання та з'єднувачів, що формують єдину інтегровану інфраструктуру для передавання даних, голосу та відео.

СКС включає кілька ключових елементів:

- **Горизонтальна підсистема** – охоплює кабелі, які з'єднують робочі місця з комутаційними вузлами. Як правило, використовуються мідні кабелі категорії CAT6 або CAT6a.
- **Магістральна підсистема** – забезпечує з'єднання між комутаційними шафами, серверними приміщеннями та будівлями. Зазвичай використовуються волоконно-оптичні кабелі.
- **Розподільчі шафи та комутаційне обладнання** – включають комутатори, маршрутизатори, патч-панелі та сервери.
- **Розетки та конектори** – точка підключення користувачів до мережі через Ethernet-кабелі.
- **Патч-корди** – короткі з'єднувальні кабелі, що використовуються для гнучкого перепідключення обладнання.

СКС розробляється з урахуванням міжнародних стандартів, таких як **TIA/EIA-568, ISO/IEC 11801**, які визначають параметри кабелів, методи з'єднання та загальні вимоги до інфраструктури.

Основні принципи проєктування:

- **Скалабельність** – можливість розширення мережі без суттєвих змін у кабельній інфраструктурі.
- **Надійність** – використання якісних матеріалів та правильний монтаж для мінімізації впливу електромагнітних завад.
- **Гнучкість** – підтримка різних типів з'єднань (Ethernet, телефонія, відеоспостереження) через універсальну кабельну систему.
- **Легкість адміністрування** – маркування кабелів та ведення документації для швидкого обслуговування мережі.

Структуровані кабельні системи мають низку переваг:

- *Зменшення простоїв* – завдяки чіткій організації кабельного господарства адміністратор може швидко локалізувати проблеми.
- *Оптимізація витрат* – уніфікована система зменшує витрати на обслуговування та модернізацію.
- *Підвищена безпека* – правильний вибір кабелів та їхнє екранування знижують ризик витоків даних та електромагнітних перешкод.

Сучасні тенденції у СКС включають впровадження **інтелектуальних систем моніторингу**, які відстежують стан кабельної інфраструктури в реальному часі. Наприклад, системи автоматичного контролю можуть сигналізувати про пошкодження кабелів або перевантаження мережевих портів, що дає змогу оперативно усувати несправності.

Структуровані кабельні системи є основою для побудови ефективних, надійних і масштабованих мереж. Вони використовуються у великих підприємствах, дата-центрах, освітніх установах і урядових організаціях для забезпечення безперебійного з’єднання та високої продуктивності мережевої інфраструктури.

Сучасні канали зв'язку

Сучасні канали зв’язку постійно еволюціонують, забезпечуючи все вищі швидкості, надійність та безпеку передачі даних. Із розвитком цифрових технологій виникають нові виклики, які потребують інноваційних рішень у сфері мережевих комунікацій. У цьому розділі ми розглянемо найбільш актуальні тренди та перспективи розвитку каналів зв’язку.

Технологія **5G** відкриває нові можливості для бездротових мереж, забезпечуючи швидкості до 10 Гбіт/с, мінімальні затримки та високу щільність підключень.

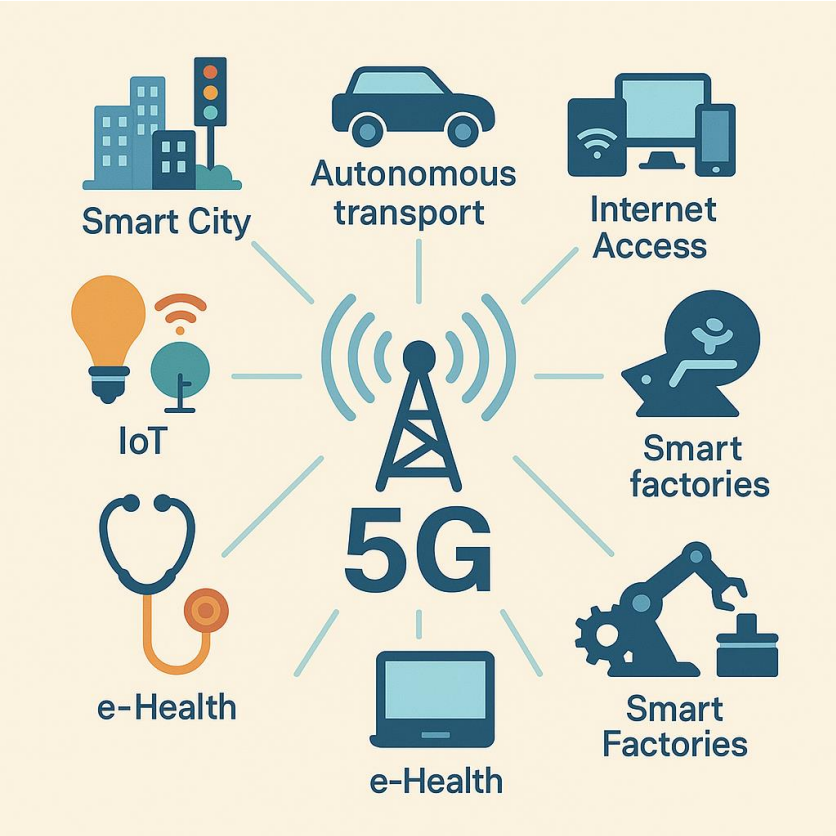


Рис 4.8 Схема мережі 5G з різними сценаріями використання

Основні переваги 5G:

- **Низька затримка (<1 мс)** – дає змогу використовувати 5G для дистанційного керування роботами, автономного транспорту та критично важливих сервісів.
- **Висока пропускна здатність** – підтримує одночасне підключення тисяч пристроїв на одному квадратному кілометрі.
- **Можливість розгортання приватних 5G-мереж** – компанії можуть створювати власні бездротові інфраструктури для промислових застосувань.

Квантові мережі є однією з найбільш інноваційних технологій, що забезпечують **абсолютно захищену передачу даних** за допомогою квантової криптографії.

Основні принципи:

- Використання **квантової суперпозиції** для передачі інформації.
- Неможливість перехоплення сигналу без його руйнування.
- Висока стійкість до атак хакерів.

Квантові комунікації вже тестуються у державних і фінансових організаціях, і в майбутньому можуть стати стандартом для забезпечення найвищого рівня безпеки в мережах.

Розвиток волоконно-оптичних ліній триває, дозволяючи досягати **швидкостей понад 100 Тбіт/с**.

Основні вдосконалення:

- *Технологія спектрального ущільнення каналів (WDM)* – дає змогу передавати кілька потоків даних через одне волокно.
- *Гібридні оптичні та електронні системи* – підвищують ефективність передачі на великі відстані.
- *Нові матеріали для оптичних волокон* – знижують втрати сигналу та дають можливість передавати дані на тисячі кілометрів без підсилювачів.

Очікується, що **Wi-Fi 7** запропонує ще вищі швидкості, кращу продуктивність у багатокористувацькому середовищі та знижену затримку.

Головні особливості:

- Пропускна здатність **до 30 Гбіт/с**.
- Удосконалені алгоритми управління трафіком.
- Вища стійкість до перешкод.

Щодо **6G**, що очікується після 2030 року, ця технологія зможе забезпечити швидкості передачі **до 1 Тбіт/с**, що уможливить реалізувати повноцінну доповнену реальність (AR), Інтернет-нейроінтерфейсів та інтеграцію штучного інтелекту у всі аспекти мережевої комунікації.

Усе більше мережевих технологій впроваджують **штучний інтелект (AI) та машинне навчання** для:

- Моніторингу стану каналів зв’язку та прогнозування відмов.
- Динамічного балансування навантаження.
- Автоматичного виявлення атак та загроз.

Такі рішення дають можливість значно підвищити ефективність управління мережею та зменшити ризики збоїв.

Сучасні підприємства все частіше використовують **гібридні мережі**, що поєднують фізичну інфраструктуру з хмарними сервісами.

Це дає змогу:

- Гнучко масштабувати ресурси.
- Оптимізувати витрати на обладнання.
- Забезпечити резервне копіювання та катастрофостійкість.

Рішення **Network-as-a-Service (NaaS)** дає змогу компаніям орендувати мережеву інфраструктуру, а не будувати власні дата-центри.

Із розвитком мереж збільшується загроза кібератак.

Основні виклики:

- Використання **VPN та шифрування** для захисту каналів зв'язку.
- Впровадження **багатофакторної аутентифікації (MFA)**.
- Застосування **Zero Trust Architecture** – підхід, що передбачає перевірку кожного підключення незалежно від його розташування.

Сучасні технології зв'язку спрямовані на досягнення балансу між продуктивністю, надійністю та безпекою, що є ключовим фактором для майбутніх цифрових інфраструктур.

Канали та лінії зв'язку є фундаментальною частиною будь-якої комп'ютерної мережі, оскільки саме вони забезпечують фізичну або бездротову передачу даних між пристроями. Від правильного вибору каналу залежить продуктивність, стабільність, безпека та масштабованість мережі.

Дротові канали, такі як **вита пара, коаксіальний кабель та оптоволокно**, продовжують залишатися основою для локальних і магістральних мереж. Вони забезпечують високу пропускну здатність, низькі затримки та мінімальний рівень втрат даних. Оптоволоконні лінії зв'язку є найбільш перспективними, оскільки вони підтримують швидкості передачі даних у терабітному діапазоні,

що робить їх ідеальним вибором для магістралей зв'язку та центрів обробки даних.

Бездротові технології, такі як **Wi-Fi, 4G, 5G і супутниковий зв'язок**, дають можливість забезпечувати доступ до мережі без необхідності прокладання фізичних кабелів. Вони є ключовими для мобільного зв'язку, розумних міст, віддалених регіонів та IoT-рішень. Нові покоління Wi-Fi 7 та 6G обіцяють ще вищу швидкість і ефективність, що дозволить інтегрувати бездротові технології у більшість сучасних інфраструктур.

Окреме значення має концепція **структурованих кабельних систем (СКС)**, які дають можливість організовувати ефективну, масштабовану та керовану інфраструктуру у великих організаціях. Дотримання стандартів (TIA/EIA-568, ISO/IEC 11801) забезпечує стабільність і сумісність обладнання.

Сучасні тенденції у сфері каналів зв'язку включають:

- *Швидкий розвиток 5G* та його використання у критично важливих галузях, таких як медицина, транспорт і промисловість.
- *Вдосконалення оптоволоконних ліній* з використанням спектрального ущільнення (WDM) та нових матеріалів, що зменшують загасання сигналу.
- *Квантові комунікації* як майбутнє безпечного зв'язку, що захищає від кібератак.
- *Гібридні мережі* та поєднання фізичних каналів із хмарними сервісами (Network-as-a-Service, NaaS).
- *Використання штучного інтелекту для управління мережами,* оптимізації трафіку та прогнозування збоїв.

Знання про канали зв'язку є критично важливими для спеціалістів у сфері інформаційних технологій. Вибір відповідної технології дає змогу досягти балансу між продуктивністю, вартістю та безпекою. Майбутнє мереж зв'язку полягає у впровадженні новітніх рішень, таких як квантова криптографія, автономні 5G-мережі та інтелектуальні системи керування трафіком.

Лекція 5. Адресація в мережах

Адресація є одним із найважливіших аспектів комп'ютерних мереж, оскільки вона дає змогу пристроям взаємодіяти між собою та знаходити один одного в локальних і глобальних мережах. Без правильної адресації передача даних була б хаотичною, і пакети не могли б досягати своїх цілей.

IP-адреса (Internet Protocol Address) – це унікальний ідентифікатор, що використовується для ідентифікації пристрою у мережі. Вона виконує ту саму функцію, що й поштові адреси у фізичному світі: допомагає правильно спрямувати трафік до призначеного одержувача. У комп'ютерних мережах IP-адреси дають можливість маршрутизаторам визначати, куди треба пересилати пакети.

Кожен пристрій у мережі, підключений до Інтернету або локальної мережі, має власну IP-адресу, яка може бути **статичною** (закріпленою за пристроєм) або **динамічною** (призначається автоматично сервером DHCP).

Залежно від стандарту, що використовується, існує два основних типи IP-адрес:

- **IPv4** – використовується в більшості сучасних мереж, має 32-бітну структуру, що дає змогу створити близько 4,3 мільярда унікальних адрес. Формат IPv4 виглядає як чотири числа, розділені крапками, наприклад: `192.168.1.1`.
- **IPv6** – новіший стандарт, який використовує 128-бітні адреси, що дає змогу створювати майже необмежену кількість унікальних ідентифікаторів. Формат IPv6 складається із восьми груп шістнадцяткових чисел, наприклад: `2001:db8::ff00:42:8329`.

IP-адреси можуть бути призначені статично або динамічно.

- **Статична IP-адреса** закріплюється за пристроєм вручну і не змінюється з часом. Використовується для серверів, маршрутизаторів та інших критично важливих пристроїв.

- **Динамічна IP-адреса** призначається автоматично за допомогою сервера DHCP і може змінюватися кожного разу при підключенні пристрою до мережі. Використовується у великих корпоративних мережах та серед користувачів Інтернету.

Параметр	***IPv4***	***IPv6***
Довжина адреси	32 біти	128 біт
Формат запису	Чотири десяткові октети, розділені крапками	Вісім груп шістнадцяткових чисел, розділених двокрапками
Приклад адреси	192.168.1.1	2001:0db8:85a3:0000:0000:8a2e:0370:7334
Кількість доступних адрес	Близько 4.3 мільярда адрес	340 ундециль йонів адрес
Метод конфігурації	DHCP, статична конфігурація	Автоконфігурація, DHCPv6
Підтримка безпеки	Немає вбудованої безпеки (IPsec опціонально)	Вбудована підтримка IPsec
Підтримка QoS	Обмежена підтримка	Оптимізована підтримка
Основне використання	Локальні та глобальні мережі	Інтернет речей (IoT), сучасні мережі

Таблиця 5.1 Порівняльна таблиця IPv4 та IPv6 із прикладами адрес

Усі IP-адреси поділяються на **публічні** та **приватні**:

- **Публічні IP-адреси** використовуються для ідентифікації пристроїв в Інтернеті. Вони унікальні у всьому світі і надаються провайдерами.
- **Приватні IP-адреси** застосовуються всередині локальних мереж і не виходять за їхні межі. Вони мають визначені діапазони, наприклад:
    - 192.168.0.0 – 192.168.255.255
    - 10.0.0.0 – 10.255.255.255
    - 172.16.0.0 – 172.31.255.255

Оскільки кількість публічних IPv4-адрес обмежена, у більшості локальних мереж використовується технологія NAT (Network Address Translation), яка дає

змогу багатьом пристроям у локальній мережі використовувати одну публічну IP-адресу для виходу в Інтернет.

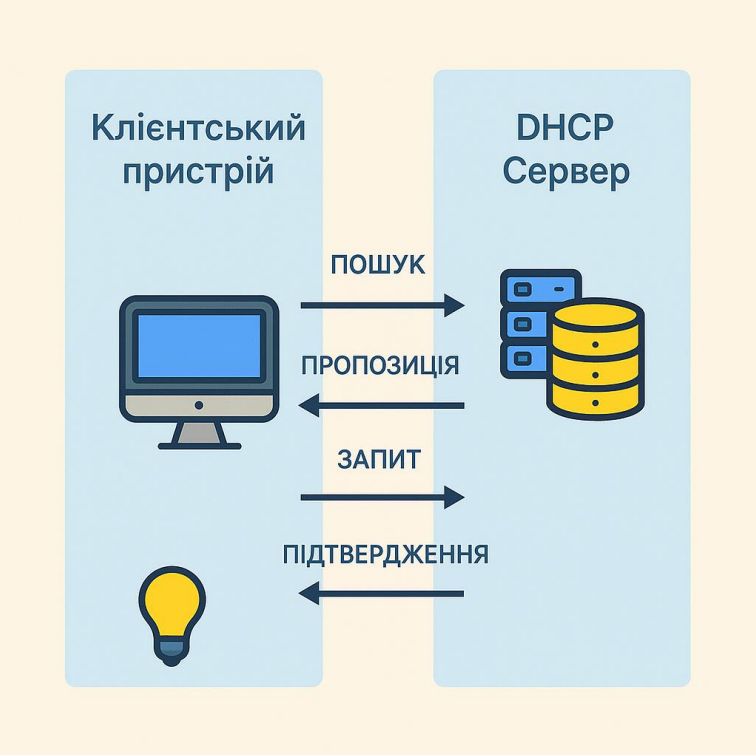


Рис 5.1 Схема роботи DHCP-сервера для динамічної адресації

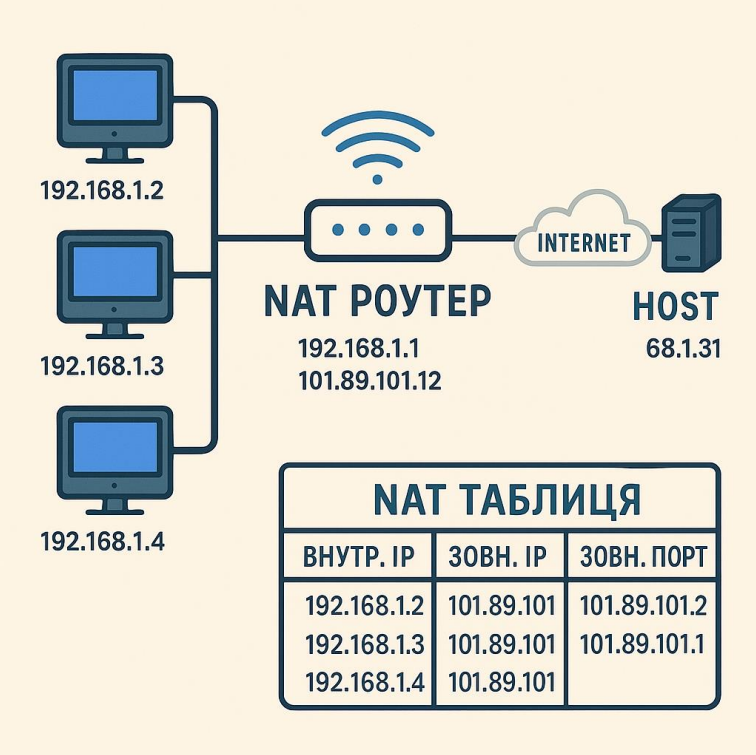


Рис 5.2 Схема NAT

Адресація є ключовим елементом комп’ютерних мереж, забезпечуючи унікальну ідентифікацію пристроїв та ефективну маршрутизацію трафіку. Використання IPv4 залишається стандартом, проте через обмежену кількість доступних адрес триває поступовий перехід на IPv6. Динамічна адресація та використання NAT дають можливість раціонально використовувати наявний адресний простір та спрощують управління мережами.

Поділ мережі на підмережі, або **маскування підмереж (subnetting)**, є важливим методом оптимізації використання IP-адресного простору та підвищення ефективності роботи комп’ютерних мереж. Завдяки subnetting можна логічно розділити одну велику мережу на менші сегменти, що дає змогу підвищити продуктивність, зменшити кількість широкомовних повідомлень (broadcasts) та покращити безпеку.

Поділ мережі на підмережі використовується для:

- Зменшення навантаження на мережу за рахунок скорочення широкомовного трафіку.
- Оптимізації використання IP-адрес та усунення їх неефективного розподілу.
- Підвищення безпеки через розмежування трафіку між сегментами.
- Кращої організації мережевої інфраструктури у великих компаніях та дата-центрах.

Наприклад, якщо у компанії є окремі підрозділи (бухгалтерія, технічний відділ, відділ продажів), кожен із них може працювати у власній підмережі, що допомагає ізолювати трафік та уникнути перевантаження.

IP-адреса складається з двох частин:

- **Ідентифікатор мережі** – визначає, до якої мережі належить IP-адреса.
- **Ідентифікатор хоста** – визначає конкретний пристрій у мережі.

Маска підмережі вказує, яка частина IP-адреси відповідає за ідентифікатор мережі, а яка – за пристрої в ній.

Наприклад:

- **192.168.1.0/24** – означає, що перші 24 біти адреси відведені для ідентифікації мережі, а решта 8 біт – для ідентифікації пристроїв.

Основні класи масок підмереж:

- **/8 (255.0.0.0)** – великі мережі з понад 16 мільйонами адрес.
- **/16 (255.255.0.0)** – середні мережі (до 65 536 пристроїв).
- **/24 (255.255.255.0)** – малі мережі (до 256 пристроїв).

Розглянемо приклад:

Якщо маємо IP-мережу `192.168.1.0/24`, у якій потрібно створити дві підмережі, можна використати маску `/25`, що розділить мережу на два рівні сегменти:

- **192.168.1.0/25** (пристрої з 192.168.1.1 до 192.168.1.127)
- **192.168.1.128/25** (пристрої з 192.168.1.129 до 192.168.1.254)

Така операція дає змогу ефективно використовувати адресний простір, запобігаючи його марнуванню.

На відміну від IPv4, у **IPv6** маскування підмереж спрощене завдяки величезному адресному простору. IPv6 використовує фіксовану маску **/64** для кожної підмережі, що значно спрощує керування адресами. Наприклад, якщо IPv4 потребує складних розрахунків для розбиття мереж, IPv6 автоматично виділяє підмережі в межах глобальних префіксів.

Маскування підмереж є ефективним механізмом управління IP-адресним простором. Використання subnetting дає змогу оптимізувати продуктивність мережі, удосконалити її безпеку та зробити адміністрування більш зручним. IPv6 суттєво спрощує цей процес, автоматизуючи створення підмереж та усуваючи багато проблем, пов’язаних з обмеженістю адресного простору в IPv4.

В умовах обмеженої кількості IPv4-адрес та необхідності підключення великої кількості пристроїв до Інтернету активно використовується технологія **Network Address Translation (NAT)**. Вона дає змогу пристроям у локальних мережах використовувати приватні IP-адреси та одночасно взаємодіяти із

зовнішніми ресурсами через одну або кілька публічних IP-адрес. NAT є важливим інструментом для підвищення безпеки й ефективного використання адресного простору.

NAT працює шляхом **перетворення приватних IP-адрес на публічні** при виході в Інтернет. Це означає, що внутрішні пристрої, які використовують приватні IP-адреси, можуть спільно використовувати одну публічну адресу для зв'язку із зовнішнім світом.

Основні види NAT:

- **Static NAT (SNAT)** – дає змогу зіставити одну приватну IP-адресу з однією публічною. Використовується для серверів, які мають бути доступні з Інтернету.
- **Dynamic NAT (DNAT)** – призначає публічну IP-адресу з певного пулу адрес для пристроїв у локальній мережі.
- **Port Address Translation (PAT)** – варіант NAT, який дає змогу багатьом пристроям локальної мережі використовувати одну публічну IP-адресу, але різні порти для передачі даних.

Для ефективного використання IPv4-адресного простору були виділені **приватні діапазони IP-адрес**, які використовуються у внутрішніх мережах і не маршрутизуються в Інтернеті. Всі пристрої, що мають приватні IP-адреси, повинні використовувати NAT для виходу у глобальну мережу.

Типові діапазони приватних IP-адрес:

- **10.0.0.0 – 10.255.255.255** (великі корпоративні мережі)
- **172.16.0.0 – 172.31.255.255** (середні мережі)
- **192.168.0.0 – 192.168.255.255** (домашні та малі офісні мережі)

Публічні IP-адреси, на відміну від приватних, призначаються глобальними реєстраторами (IANA, RIR) і є унікальними в межах Інтернету.

Оскільки діапазон IPv4-адрес обмежений, NAT допомагає:

- Забезпечити доступ до Інтернету для десятків і сотень пристроїв через одну публічну IP-адресу.
- Підвищити безпеку мережі, оскільки приватні IP-адреси не видно у глобальному Інтернеті.
- Оптимізувати використання адресного простору.

Приклад використання PAT (NAT Overload):

Якщо у локальній мережі є 100 пристроїв із приватними адресами `192.168.1.0/24`, вони можуть виходити в Інтернет через одну публічну IP-адресу, використовуючи різні порти TCP/UDP.

Попри всі переваги, NAT має свої недоліки:

- Деякі протоколи (наприклад, SIP для VoIP) можуть не працювати коректно через зміни IP-адрес у заголовках пакетів.
- Використання NAT додає певну затримку при обробці трафіку.
- NAT не потрібен в IPv6, оскільки цей протокол забезпечує достатню кількість унікальних адрес.

Перехід на IPv6 поступово зменшує потребу у NAT, оскільки новий стандарт дає змогу кожному пристрою отримати унікальну публічну IP-адресу.

NAT є важливим компонентом сучасних мереж, оскільки дає змогу економити IPv4-адреси та підвищує рівень безпеки. Проте його використання додає певні складності у конфігурації мережевих сервісів. IPv6 усуває потребу у NAT, пропонуючи більш ефективне управління адресами та безпосередню маршрутизацію трафіку.

У великих і динамічних мережах призначення IP-адрес вручну для кожного пристрою може бути складним і неефективним. Для автоматизації цього процесу використовується **DHCP (Dynamic Host Configuration Protocol)** – протокол, який дає змогу динамічно розподіляти IP-адреси та інші мережеві параметри між клієнтами в локальній мережі.

DHCP працює за клієнт-серверною моделлю:

- **DHCP-сервер** – це пристрій (маршрутизатор, сервер або спеціалізований мережевий пристрій), який надає клієнтам IP-адреси та інші налаштування.
- **DHCP-клієнт** – будь-який пристрій у мережі (комп'ютер, смартфон, принтер), який звертається до DHCP-сервера для отримання конфігурації.

Процес отримання IP-адреси DHCP-клієнтом відбувається у кілька етапів:

1. **DHCPDISCOVER** – клієнт відправляє широкомовний запит, шукаючи DHCP-сервер у мережі.
2. **DHCPOFFER** – сервер відповідає, пропонуючи IP-адресу зі свого пулу.
3. **DHCPREQUEST** – клієнт приймає пропозицію і запитує підтвердження адреси.
4. **DHCPACK** – сервер підтверджує адресу та надсилає всі необхідні параметри (шлюз, DNS-сервер, маску підмережі).

Адміністратор може налаштувати DHCP-сервер для автоматичного керування IP-адресами у локальній мережі. При конфігурації сервера задаються:

- **Діапазон IP-адрес (DHCP pool)** – набір доступних адрес для видачі клієнтам.
- **Термін оренди (lease time)** – час, на який видається IP-адреса (після закінчення терміну адреса може бути змінена).
- **DNS-сервер** – адреси серверів, які використовуватимуть клієнти для перетворення доменних імен на IP-адреси.
- **Шлюз (default gateway)** – IP-адреса маршрутизатора, через який клієнти виходять в Інтернет.

У великих компаніях можуть використовуватися **DHCP-ретранслятори (DHCP relay)**, які дають можливість клієнтам отримувати IP-адреси навіть якщо DHCP-сервер розташований в іншій підмережі. Це особливо корисно для централізованого управління мережею та зменшення широкомовного трафіку.

Також у великих мережах можна використовувати **резервування IP-адрес (DHCP reservation)**, що дає змогу видавати певним пристроям статичні IP-адреси на основі їх MAC-адреси.

Переваги DHCP:

- *Автоматизація* – немає потреби вручну призначати IP-адреси.
- *Гнучкість* – клієнти можуть отримувати різні параметри конфігурації залежно від мережі.
- *Оптимізація використання IP-адрес* – сервер видає адреси лише тим пристроям, які їх потребують.

Недоліки DHCP:

- *Залежність від DHCP-сервера* – якщо сервер виходить з ладу, клієнти не зможуть отримати адреси.
- *Можливість атак (DHCP spoofing)* – зловмисник може створити підроблений DHCP-сервер для видачі некоректних налаштувань.

DHCP значно спрощує адміністрування мережі, забезпечуючи автоматичний розподіл IP-адрес і зменшуючи кількість конфліктів у мережі. У великих корпоративних мережах використання DHCP-релєїв та резервування адрес дає змогу підтримувати гнучку та надійну інфраструктуру.

Канали зв'язку та IP-адресація є двома взаємопов'язаними компонентами комп'ютерних мереж. Вибір каналу зв'язку безпосередньо впливає на спосіб адресації пристроїв та управління трафіком у мережі. Наприклад, у дротових Ethernet-мережах IP-адресація використовується разом із MAC-адресами, тоді як у бездротових та мобільних мережах адресація може змінюватися через переміщення пристрою між різними точками доступу.

Як вибір каналу впливає на схему адресації?

- **Дротові мережі (Ethernet, оптоволоконні лінії)** зазвичай використовують статичну або DHCP-адресацію. Оскільки фізична топологія таких мереж залишається стабільною, IP-адреси рідко змінюються.
- **Бездротові мережі (Wi-Fi, 4G, 5G)** частіше працюють із динамічними IP-адресами, які змінюються залежно від місцезнаходження пристрою та доступності мережі.

- **VPN та тунелювання** – у корпоративних та віддалених мережах IP-адреси можуть бути віртуальними (тунельними), що дає змогу забезпечити безпечне з'єднання між користувачем та компанією, незалежно від його фізичного розташування.

Проблеми адресації у бездротових і мобільних мережах

У мобільних мережах 4G/5G та Wi-Fi існують виклики, пов'язані з динамічною зміною IP-адрес. Основні проблеми:

- **Зміна IP-адрес при переміщенні пристрою** – коли користувач переміщується між Wi-Fi-точками або стільниковими базовими станціями, йому може бути призначена нова IP-адреса.
- **Перевантаження мережі** – у великих міських районах мобільні мережі можуть призначати тимчасові IP-адреси для оптимізації ресурсів.
- **Реалізація Mobile IP** – механізм, який дає змогу зберігати стабільну IP-адресу навіть при зміні точки підключення.

Динамічні зміни адреси у мобільних користувачів (Mobile IP)

Протокол **Mobile IP** дає змогу пристрою зберігати постійну IP-адресу навіть під час переходу між різними мережами. Це особливо важливо для:

- **Роумінгу в мобільних мережах** – користувач зберігає доступ до Інтернету, не перериваючи з'єднання.
- **VoIP-зв'язку** – при дзвінках через IP-телефонію під час руху.
- **Стрімінгового відео** – коли пристрій переходить між мережами Wi-Fi і LTE без втрати підключення.

Mobile IP працює за принципом «домашнього агента» та «віддаленого агента», які дають можливість спрямовувати пакети до пристрою незалежно від його реального місцезнаходження.

Канали зв'язку та адресація є взаємопов'язаними складовими комп'ютерних мереж. У дротових інфраструктурах використовуються переважно статичні або DHCP-адреси, тоді як у мобільних та бездротових мережах динамічна зміна IP – стандартна практика. Технології Mobile IP та VPN допомагають підтримувати

безперервність з’єднання, навіть якщо користувач переміщується між різними мережами.

Із розвитком комп’ютерних мереж змінюються і підходи до використання каналів зв’язку та адресації. Новітні технології спрямовані на підвищення продуктивності, розширення можливостей управління трафіком та забезпечення безпеки даних. Сучасні виклики, такі як зростання кількості підключених пристроїв (IoT), вичерпання IPv4-адрес та необхідність масштабованості, стимулюють впровадження нових рішень. Штучний інтелект (AI) та машинне навчання (ML) все частіше використовуються для управління IP-адресацією та аналізу мережевого трафіку. Інтернет речей (IoT) створює нові виклики для систем адресації, адже кількість підключених пристроїв стрімко зростає. IPv6 надає кожному IoT-пристрою унікальну адресу, що дає змогу уникнути складних схем NAT. Квантові мережі та квантова криптографія стануть основою безпечної передачі даних у майбутньому. Квантова адресація уможливить створення абсолютно захищених каналів зв’язку, які неможливо зламати традиційними методами.

Канали зв’язку та адресація є основними компонентами комп’ютерних мереж, що визначають їхню продуктивність, ефективність і надійність. Без належної адресації пакети даних не могли б досягати своїх одержувачів, а без якісних каналів зв’язку передача інформації була б нестабільною або надто повільною.

Адресація та канали зв’язку – взаємопов’язані елементи мережевої інфраструктури і їхнє правильне налаштування є ключем до ефективної та безпечної передачі даних. Вибір між дротовими та бездротовими каналами, використання NAT чи IPv6, автоматизоване керування IP-адресами – всі ці аспекти впливають на стабільність роботи мереж.

Сучасні технології продовжують розвиватися, і спеціалісти з мережевого адміністрування мають бути готовими до переходу на нові стандарти, оптимізації наявних мереж та впровадження нових рішень, які допоможуть ефективно керувати адресацією та підтримувати надійні канали зв’язку.

Лекція 6: Бездротові мережі. Глобальні мережі (WAN)

Бездротові мережі стали невід'ємною частиною сучасного світу, забезпечуючи комунікацію між пристроями без використання фізичних з'єднань. Вони використовуються в мобільному зв'язку, домашніх і корпоративних локальних мережах, промислових системах, Інтернеті речей та багатьох інших сферах. Популярність бездротових технологій пояснюється їхньою мобільністю, гнучкістю та можливістю швидкого розгортання навіть у складних умовах.

Однією з головних переваг бездротових мереж є їхня здатність забезпечувати з'єднання там, де прокладання кабелів є неможливим або економічно недоцільним. Наприклад, мобільні мережі дають можливість користувачам отримувати доступ до Інтернету з будь-якого місця, Wi-Fi забезпечує швидкий і зручний доступ до мережі в будинках, офісах та публічних місцях, а супутникові системи надають зв'язок у віддалених регіонах.

Рис 6.1 Загальна схема бездротових мереж – Wi-Fi, мобільні, супутникові мережі.

Однак, незважаючи на всі переваги, бездротові мережі мають і певні недоліки. Вони більш чутливі до перешкод і можуть зазнавати впливу погодних

умов, будівельних матеріалів та інших джерел завад. Крім того, питання безпеки стає ще більш актуальним, оскільки бездротові сигнали можуть бути перехоплені або підроблені.

Сучасні бездротові технології постійно вдосконалюються, забезпечуючи вищу швидкість передачі даних, кращу захищеність та зниження затримок. У цій лекції ми розглянемо основні принципи роботи бездротових мереж, їхні види, технічні характеристики, а також сучасні тенденції та перспективи розвитку цієї технології.

Основи бездротового зв’язку

Бездротовий зв’язок базується на використанні електромагнітних хвиль для передавання інформації між пристроями. На відміну від дротових мереж, де сигнал передається через фізичне середовище (мідний або оптоволоконний кабель), у бездротових технологіях дані передаються через повітря, що робить їх більш гнучкими та мобільними.

Передача даних у бездротових мережах відбувається за допомогою радіохвиль, які коливаються на різних частотах. Кожен стандарт бездротового зв’язку використовує певний частотний діапазон, що визначає радіус дії, швидкість передачі даних та стійкість до перешкод. Наприклад, Wi-Fi працює у **2,4 ГГц і 5 ГГц діапазонах**, а мобільні мережі 4G та 5G використовують значно ширший спектр частот, що дає змогу їм передавати дані на великі відстані.

Бездротові мережі зазвичай використовують схему точка-точка або точка-багатоточка. У першому випадку передача відбувається безпосередньо між двома пристроями, наприклад, у Bluetooth-з’єднаннях. У другому випадку один передавач може спілкуватися з багатьма приймачами, як це відбувається у Wi-Fi-мережах або мобільних базових станціях.

Рис 6.2 Схема роботи бездротової мережі точка-точка та точка-багатоточка

При оцінці якості бездротового зв’язку важливо враховувати кілька ключових характеристик:

- **Частотний діапазон** – визначає, у яких межах працює сигнал. Наприклад, Wi-Fi використовує **2,4 ГГц** (дальність вища, швидкість нижча) та **5 ГГц** (дальність нижча, швидкість вища).
- **Ширина каналу** – впливає на максимальну швидкість передачі даних. Що ширший канал (наприклад, 160 МГц у Wi-Fi 6), то більшу швидкість можна досягти.
- **Швидкість передачі** – визначає, скільки даних може бути передано за секунду. Наприклад, 4G LTE підтримує швидкості до **1 Гбіт/с**, а 5G може досягати **10 Гбіт/с**.
- **Затримка (latency)** – час, необхідний для передачі пакета даних від відправника до отримувача. Для Wi-Fi він зазвичай складає **10-30 мс**, для 4G **50-100 мс**, а для 5G **<1 мс**.
- **Стійкість до перешкод** – визначає, наскільки сигнал стійкий до впливу інших електромагнітних джерел, будівель та інших об’єктів.

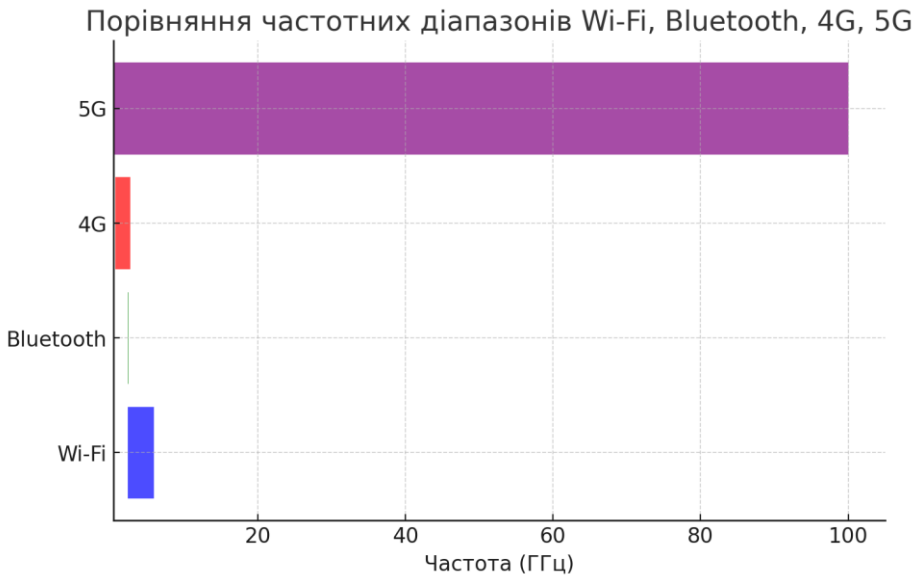


Рис 6.3 Графік, що порівнює частотні діапазони Wi-Fi, Bluetooth, 4G, 5G.

Оскільки радіохвилі використовуються для передачі інформації, необхідно застосовувати **модуляцію**, яка дає змогу закодувати цифрові дані у вигляді змін радіосигналу.

Основні типи модуляції у бездротових мережах:

- **AM (Amplitude Modulation)** – змінює амплітуду хвилі залежно від даних.
- **ЧМ (Frequency Modulation, FM)** – змінює частоту сигналу.
- **ФМ (Phase Modulation, PM)** – змінює фазу хвилі.

У Wi-Fi та мобільних мережах використовуються складніші методи модуляції, наприклад:

- **QPSK (Quadrature Phase Shift Keying)** – дає змогу передавати два біти на кожну фазову зміну.
- **QAM (Quadrature Amplitude Modulation)** – комбінує фазову та амплітудну модуляцію для підвищення швидкості передачі.

Бездротовий зв’язок є складною технологією, яка поєднує фізичні, математичні та інженерні принципи для забезпечення ефективної передачі даних. Його якість залежить від частотного діапазону, ширини каналу, рівня перешкод та методів модуляції. Завдяки розвитку технологій, бездротові мережі стають дедалі швидшими й ефективнішими, забезпечуючи глобальне підключення для мільярдів пристроїв.

Типи бездротових мереж

Бездротові мережі охоплюють широкий спектр технологій, що забезпечують зв’язок між пристроями на різних відстанях – від персональних гаджетів до глобальних комунікаційних систем. Вони класифікуються за радіусом дії, швидкістю передачі даних і використанням у різних сферах.

Персональні бездротові мережі забезпечують передачу даних на коротких відстанях, зазвичай у межах кількох метрів. Вони використовуються для зв’язку між мобільними пристроями, розумними гаджетами, сенсорами та периферійними пристроями.

Основні технології WPAN:

- *Bluetooth* – працює у діапазоні 2,4 ГГц, забезпечує швидкість до 3 Мбіт/с (Bluetooth 4.0) та до 50 Мбіт/с (Bluetooth 5.0), використовується у гарнітурах, клавіатурах, навушниках та інших мобільних пристроях.
- *ZigBee* – розрахований на малопотужні пристрої з низькою швидкістю передачі (до 250 Кбіт/с), використовується у системах розумного будинку, промислових мережах та IoT-пристроях.
- *NFC (Near Field Communication)* – технологія, що працює на дуже коротких відстанях (до 10 см) та використовується для безконтактних платежів і передачі даних.

Найпоширенішим типом WLAN є **Wi-Fi**, який забезпечує зв’язок у межах будівлі чи невеликої території.

Стандарти Wi-Fi (IEEE 802.11):

- **802.11a/b/g** – перші стандарти Wi-Fi, що працювали у діапазонах 2,4 ГГц та 5 ГГц.
- **802.11n (Wi-Fi 4)** – підтримує швидкості до 600 Мбіт/с.
- **802.11ac (Wi-Fi 5)** – використовує ширші канали, забезпечуючи швидкість до 6,9 Гбіт/с.
- **802.11ax (Wi-Fi 6, 6E)** – підтримує більшу кількість одночасних підключень, мінімізує затримки та підвищує ефективність роботи.

Wi-Fi використовується в домашніх, корпоративних та публічних мережах, забезпечуючи підключення смартфонів, ноутбуків, розумних пристроїв та IoT-систем.

Регіональні бездротові мережі (WMAN, Wireless Metropolitan Area Network)

WMAN забезпечують бездротовий доступ до Інтернету на рівні міста або великих підприємств. Основні технології:

- **WiMAX (802.16)** – забезпечує швидкісний доступ до Інтернету на відстанях до 50 км, використовується у віддалених районах без дротової інфраструктури.
- **Приватні 5G-мережі** – дають можливість компаніям розгортати власну мобільну інфраструктуру для підключення персоналу та IoT-пристроїв.

Глобальні бездротові мережі (WWAN, Wireless Wide Area Network)

WWAN охоплюють великі території та забезпечують мобільний доступ до мережі. До цієї категорії належать мобільні мережі 3G, 4G LTE та 5G.

- **3G** – перше покоління мобільного Інтернету, підтримувало швидкості до 42 Мбіт/с (HSPA+).
- **4G LTE** – забезпечує високі швидкості (до 1 Гбіт/с) та низьку затримку.
- **5G** – нове покоління мобільного зв’язку, що дає змогу передавати дані на швидкостях до 10 Гбіт/с з мінімальними затримками.

Мобільні мережі використовуються у смартфонах, мобільних модемах, автомобільних системах зв’язку та розумних містах.

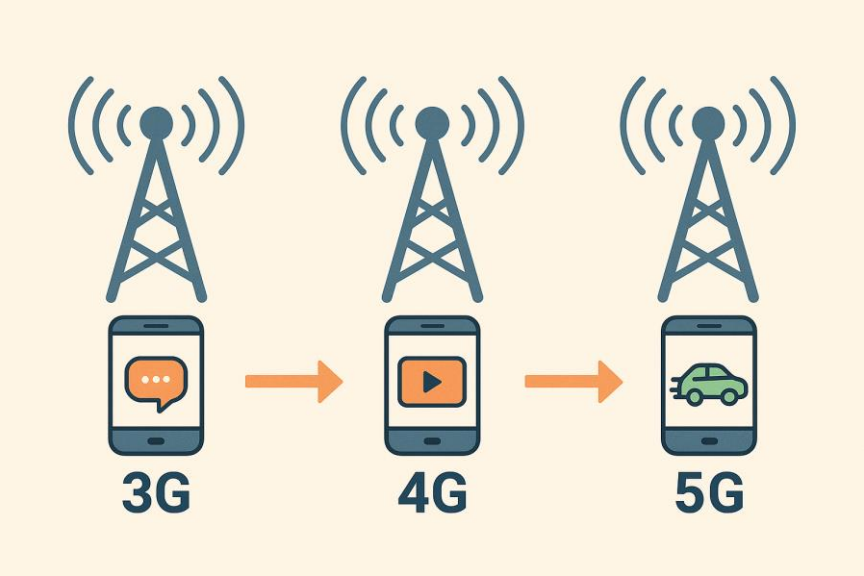


Рис 6.4 Схема еволюції мобільних мереж – 3G, 4G, 5G

Супутникові бездротові мережі

Супутниковий зв'язок використовується у віддалених регіонах, де немає можливості підключення до наземних мереж. Останніми роками технології, такі як **Starlink**, забезпечують високу швидкість підключення та низькі затримки.

- **Геостаціонарні супутники** – розташовані на висоті 35 786 км, мають значні затримки у передачі сигналу.
- **Низькоорбітальні супутники (LEO)** – розміщені на висоті 500–2000 км, забезпечують швидке з'єднання без значних затримок.

Технології Wi-Fi

Wi-Fi є однією з найпоширеніших бездротових технологій, що забезпечує високошвидкісний доступ до мережі без необхідності використання фізичних кабелів. Вона використовується у домашніх, корпоративних і громадських мережах, забезпечуючи зручний спосіб підключення пристроїв до Інтернету.

Wi-Fi-мережі будуються за двома основними архітектурами:

- **Інфраструктурна мережа** – пристрої підключаються до точки доступу (AP, Access Point), яка, і собі, підключена до дротової мережі та забезпечує зв'язок із Інтернетом.

- **Ad-hoc (перехресна)** – пристрої з’єднуються безпосередньо один з одним без використання точки доступу (наприклад, для обміну файлами між ноутбуками або смартфонами).

Основні компоненти Wi-Fi-мережі:

- *Точка доступу (Access Point, AP)* – роздає бездротовий сигнал та забезпечує зв’язок пристроїв з мережею.
- *Клієнтські пристрої (Stations, STA)* – ноутбуки, смартфони, планшети та IoT-пристрої, що підключаються до мережі.
- *Контролери Wi-Fi* – використовуються у великих корпоративних мережах для централізованого управління точками доступу.

Wi-Fi базується на стандартах **IEEE 802.11**, які визначають частотний діапазон, швидкість передачі даних та інші параметри.

Основні стандарти Wi-Fi:

- **802.11b (2,4 ГГц, до 11 Мбіт/с)** – один із перших стандартів, що використовувався у 2000-х роках.
- **802.11g (2,4 ГГц, до 54 Мбіт/с)** – підвищена швидкість, сумісність із 802.11b.
- **802.11n (Wi-Fi 4, 2,4/5 ГГц, до 600 Мбіт/с)** – підтримка MIMO (багатоантенна передача).
- **802.11ac (Wi-Fi 5, 5 ГГц, до 6,9 Гбіт/с)** – підвищена ефективність у багатокористувацькому середовищі.
- **802.11ax (Wi-Fi 6, 2,4/5 ГГц, до 9,6 Гбіт/с)** – зменшення затримки, підтримка OFDMA для одночасного передавання даних багатьом пристроям.

Бездротові мережі мають підвищений рівень вразливості, оскільки їхні сигнали можуть бути перехоплені або зламані. Для забезпечення безпеки використовуються різні методи шифрування та автентифікації.

Основні протоколи захисту Wi-Fi:

- **WEP (Wired Equivalent Privacy)** – застарілий стандарт із низьким рівнем безпеки.

- **WPA (Wi-Fi Protected Access)** – удосконалена версія з використанням динамічних ключів.
- **WPA2** – стандартний метод шифрування (AES), що використовується у більшості сучасних мереж.
- **WPA3** – новий стандарт, що посилює захист від атак та забезпечує додаткові механізми безпеки.

Основні загрози для Wi-Fi:

- **Evil Twin Attack** – створення підробленої точки доступу для викрадення даних користувачів.
- **Man-in-the-Middle (MITM)** – перехоплення трафіку між клієнтом і точкою доступу.
- **Атаки на WPS (Wi-Fi Protected Setup)** – використання вразливостей для отримання доступу до захищених мереж.

Щоб забезпечити стабільну та продуктивну роботу Wi-Fi, необхідно правильно налаштувати параметри мережі:

1. **Вибір оптимального каналу**

- У діапазоні 2,4 ГГц доступні 14 каналів, але лише 3 (1, 6, 11) не перетинаються.
- У 5 ГГц більше каналів, що дає змогу мінімізувати завади.

2. **Регулювання потужності сигналу**

- Висока потужність може спричинити перекриття зон покриття та створювати перешкоди.

3. **Налаштування QoS (Quality of Service)**

- Пріоритезація важливих типів трафіку (відеоконференції, VoIP).

4. **Розподіл навантаження між точками доступу**

- У корпоративних мережах використовуються кілька точок доступу з технологією **Roaming** (перехід між точками без втрати з'єднання).

Wi-Fi є невід'ємною частиною сучасних бездротових технологій, що забезпечують швидкий і зручний доступ до мережі. Використання новітніх стандартів (Wi-Fi 6, 6E) дає змогу досягти вищих швидкостей та зменшити затримки. Водночас важливо правильно налаштовувати параметри мережі та забезпечувати її безпеку, щоб уникнути атак та збоїв у роботі.

Мобільні бездротові мережі

Мобільні бездротові мережі забезпечують зв'язок між пристроями незалежно від їхнього розташування, дозволяючи користувачам отримувати доступ до Інтернету навіть у русі. Вони використовуються для телефонного зв'язку, передачі даних, навігаційних сервісів і підключення Інтернету речей (IoT).

Мобільні мережі складаються з кількох основних компонентів:

- *Мобільні пристрої (UE, User Equipment)* – смартфони, планшети, модеми та інші пристрої, що підключаються до мережі.
- *Базові станції (eNodeB, gNodeB)* – приймають та передають сигнали між мобільними пристроями та ядром мережі.
- *Ядро мережі (Core Network)* – включає сервери, що керують підключенням користувачів, маршрутизацією трафіку та безпекою.
- *Інтернет-шлюзи* – забезпечують вихід мобільних пристроїв у глобальну мережу.

Мобільні технології розвивалися від простих аналогових систем до високошвидкісних цифрових мереж, що підтримують відеозв'язок, потокове відео та хмарні сервіси.

- *3G (UMTS, HSPA+)* – забезпечив перший мобільний Інтернет зі швидкістю до 42 Мбіт/с.

- *4G LTE* – суттєво підвищив швидкість (до 1 Гбіт/с) та зменшив затримки, що дозволило передавати HD-відео та забезпечувати високу якість голосового зв'язку через VoLTE.
- *5G* – найновіший стандарт, що забезпечує швидкість до 10 Гбіт/с, мінімальну затримку (<1 мс) та підтримку мільярдів пристроїв у рамках IoT.

5G дає змогу впроваджувати **приватні мобільні мережі**, що використовуються у промисловості, медицині та на підприємствах:

- Розумні заводи – автономні роботи з підключенням до хмарних платформ.
- Медичні технології – дистанційна хірургія, моніторинг пацієнтів у реальному часі.
- Автономний транспорт – самокеровані автомобілі, зв'язок між транспортними засобами (V2X).

Мобільні мережі стали основою сучасної бездротової комунікації, дозволяючи користувачам залишатися на зв'язку в будь-якому місці. Технології 4G та 5G забезпечують високу швидкість і низькі затримки, що відкриває нові можливості для промисловості, транспорту та IoT. Перехід до 5G дає змогу значно підвищити продуктивність мобільних мереж та інтегрувати нові цифрові сервіси.

Інтернет речей (IoT) та бездротові технології

Інтернет речей (**IoT, Internet of Things**) є однією з найперспективніших галузей розвитку бездротових технологій. IoT об'єднує мільярди пристроїв, що взаємодіють між собою з хмарними платформами для збору, аналізу та автоматизації даних у реальному часі. Бездротові мережі є критично важливим компонентом IoT, оскільки дають можливість підключати сенсори, розумні пристрої та промислове обладнання без потреби у дротовому підключенні.

IoT-пристрої передають дані через бездротові технології, такі як Wi-Fi, мобільні мережі (4G, 5G), LoRaWAN, ZigBee, Bluetooth та супутниковий зв'язок.

Вибір конкретної технології залежить від потреб у швидкості передачі, дальності зв’язку та енергоефективності.

Основні сценарії використання IoT:

- **Розумні міста** – моніторинг трафіку, екологічний контроль, автоматизоване вуличне освітлення.
- **Розумні будинки** – дистанційне керування пристроями (освітлення, безпека, клімат-контроль).
- **Промислові IoT (IIoT)** – автоматизація виробничих процесів, контроль обладнання, підключені сенсори для моніторингу стану систем.
- **Сільське господарство** – контроль вологості ґрунту, прогнозування погоди, автоматизовані системи зрошення.

Для підключення IoT-пристроїв використовуються спеціалізовані бездротові технології, що забезпечують низьке енергоспоживання та передачу даних на великих відстанях.

Основні бездротові технології IoT:

- *Wi-Fi* – підходить для IoT-пристроїв із високими вимогами до швидкості, таких як камери відеоспостереження.
- *Bluetooth Low Energy (BLE)* – використовується для підключення пристроїв-носіїв (фітнес-трекери, смарт-годинники).
- *LoRaWAN (Long Range Wide Area Network)* – дає змогу передавати дані на відстань до 15 км із мінімальним енергоспоживанням.
- *Sigfox* – використовується для передачі невеликих обсягів даних на великих територіях.
- *NB-IoT (Narrowband IoT)* – мобільна технологія для роботи IoT-пристроїв у мережах операторів стільникового зв’язку.

Розширення IoT-мереж піднімає питання **безпеки**, адже велика кількість підключених пристроїв створює потенційні вразливості для атак. Основні загрози:

- **DDoS-атаки через IoT-ботнети** – зловмисники можуть використати IoT-пристрої для масових атак (наприклад, ботнет Mirai).

- **Перехоплення даних** – незашифровані бездротові передачі можуть бути вразливими для хакерів.
- **Зловмисне втручання у розумні пристрої** – несанкціонований доступ до пристроїв розумного будинку або промислових систем.

Основні способи захисту IoT-мереж:

- **Використання шифрування трафіку** (TLS, AES-256).
- **Сегментація мережі** – створення окремих підмереж для IoT-пристроїв.
- **Регулярне оновлення прошивки IoT-пристроїв** для закриття вразливостей.

IoT та бездротові технології суттєво змінюють спосіб взаємодії пристроїв і керування інфраструктурою. Вибір відповідної технології бездротового зв'язку залежить від вимог до дальності дії, швидкості передачі даних та енергоспоживання. Безпека IoT-мереж стає ключовим викликом, що потребує комплексного підходу до захисту даних та підключених пристроїв.

Бездротові сенсорні мережі (WSN)

Бездротові сенсорні мережі (**WSN, Wireless Sensor Networks**) – це спеціалізовані мережі, що складаються з бездротових сенсорів, які збирають, обробляють та передають дані в режимі реального часу. Вони використовуються для моніторингу навколишнього середовища, промислових систем, розумних міст і військових застосувань.

Основна функція WSN – це автоматичний збір інформації про навколишнє середовище та передача даних у центральну систему для аналізу. Сенсорні мережі дають можливість ефективно моніторити природні процеси, технологічні системи та фізичні об'єкти без потреби у фізичному втручанні.

Основні сфери застосування WSN:

- **Екологічний моніторинг** – вимірювання рівня забруднення повітря, вологості ґрунту, температури.
- **Розумні міста** – контроль енергоспоживання, автоматизоване освітлення, моніторинг трафіку.

- **Промислові мережі** – моніторинг стану обладнання, контроль за рівнем рідин і газів у резервуарах.
- **Сільське господарство** – контроль зрошення, моніторинг стану врожаю та погодних умов.
- **Охорона здоров'я** – дистанційний контроль стану пацієнтів у медичних закладах.

Бездротові сенсорні мережі відкривають нові можливості для автоматизації та моніторингу у багатьох сферах. Вони дають можливість ефективно збирати та аналізувати дані без необхідності втручання людини. Використання оптимізованих топологій та технологій енергозбереження забезпечує довговічність роботи сенсорних пристроїв та стійкість мережі до відмов.

Сучасні тренди та перспективи розвитку бездротових технологій

Бездротові технології розвиваються надзвичайно швидкими темпами, забезпечуючи вищу швидкість передачі даних, покращену безпеку та знижену затримку. Впровадження нових стандартів, таких як **Wi-Fi 7, 6G, інтеграція AI в управління мережею та розвиток супутникових мереж**, значно розширює можливості бездротового зв'язку.

Технологія **6G**, яка очікується після 2030 року, обіцяє ще більш значне поліпшення зв'язку:

- *Швидкості понад 1 Тбіт/с* – у сотні разів швидше, ніж 5G.
- *Голографічний зв'язок та VR/AR* – передача тривимірних потокових даних у реальному часі.
- *Терагерцові частоти (THz band)* – підвищена ефективність передачі даних, хоча поки що є виклики у впровадженні.

Завдяки проєктам **Starlink, OneWeb, Amazon Kuiper** супутниковий Інтернет стає все більш доступним і швидким.

- **Низькоорбітальні супутники (LEO)** забезпечують мінімальні затримки та високу швидкість передачі даних.

- **Інтеграція супутникового Інтернету з мобільними мережами** уможливить отримати глобальне покриття без сліпих зон.

Сучасні бездротові технології швидко розвиваються, наближаючи нас до нового рівня швидкості передачі даних, гнучкості та безпеки. Використання AI, перехід на Wi-Fi 7 та підготовка до 6G зроблять бездротовий зв'язок ще надійнішим і масштабованим. Супутникові мережі допоможуть покрити навіть найвіддаленіші куточки світу, що відкриє нові можливості для комунікації.

Бездротові мережі є одним із ключових технологічних досягнень, що змінили спосіб комунікації між пристроями та людьми. Вони забезпечують зручний та гнучкий зв'язок без необхідності використання фізичних кабелів, що робить їх ідеальними для мобільного Інтернету, розумних міст, промислових систем та IoT-рішень.

Бездротові технології продовжують вдосконалюватися, забезпечуючи швидший, надійніший та безпечніший зв'язок. Впровадження 5G та IoT змінює спосіб взаємодії між пристроями, дозволяючи створювати автономні системи, розумні міста та нові цифрові сервіси. Попри виклики, розвиток бездротових мереж відкриває нові можливості для бізнесу, науки та повсякденного життя.

Глобальні мережі (WAN)

Глобальні мережі (**WAN, Wide Area Networks**) відіграють ключову роль у забезпеченні зв'язку між віддаленими об'єктами та забезпеченні доступу до ресурсів Інтернету. Вони охоплюють великі географічні території, об'єднуючи локальні мережі (LAN) та регіональні мережі (MAN) у єдину інфраструктуру. WAN використовується для корпоративних мереж, міжурядових організацій, телекомунікаційних компаній і користувачів, що підключаються до Інтернету через провайдерів.

Основна відмінність WAN від локальних мереж полягає у використанні **глобальних магістралей зв'язку, що надаються телекомунікаційними компаніями або державними інфраструктурними організаціями**. На відміну

від LAN, де адміністратор має повний контроль над усіма пристроями та з’єднаннями, WAN покладається на послуги сторонніх провайдерів.

Ключові переваги WAN:

- Дає змогу організаціям об'єднувати офіси в різних містах і країнах.
- Забезпечує доступ до хмарних сервісів та корпоративних VPN.
- Використовується для глобального доступу до ресурсів Інтернету.

Основні виклики WAN:

- Затримки та втрати пакетів через великі відстані між вузлами.
- Залежність від інфраструктури провайдерів, що може впливати на якість з’єднання.
- Необхідність ефективного керування трафіком, особливо у випадку великого навантаження.

Зі зростанням попиту на високу швидкість передачі даних та надійність з'єднань WAN продовжують розвиватися, інтегруючи нові технології, такі як **SD-WAN, 5G та супутниковий Інтернет**.

Глобальні мережі (**WAN**) базуються на складній архітектурі, що поєднує різні технології передачі даних та інфраструктуру провайдерів зв’язку. WAN може охоплювати як приватні корпоративні мережі, так і публічний Інтернет, забезпечуючи віддалений доступ до ресурсів і підтримку великої кількості користувачів.

WAN складається з кількох ключових елементів:

- *Кінцеві вузли (End Nodes)* – пристрої користувачів, сервери, маршрутизатори, що підключаються до мережі.
- *Мережеві маршрутизатори (WAN Routers)* – забезпечують передачу даних між локальними мережами та глобальними каналами.
- *Комутовані мережі та канали зв’язку* – включають дротові (оптоволокно, кабельні з’єднання) та бездротові (мобільний зв’язок, супутниковий Інтернет) канали.

- *Провайдерська інфраструктура* – магістральні мережі великих телекомунікаційних компаній, які забезпечують міжконтинентальні з'єднання.

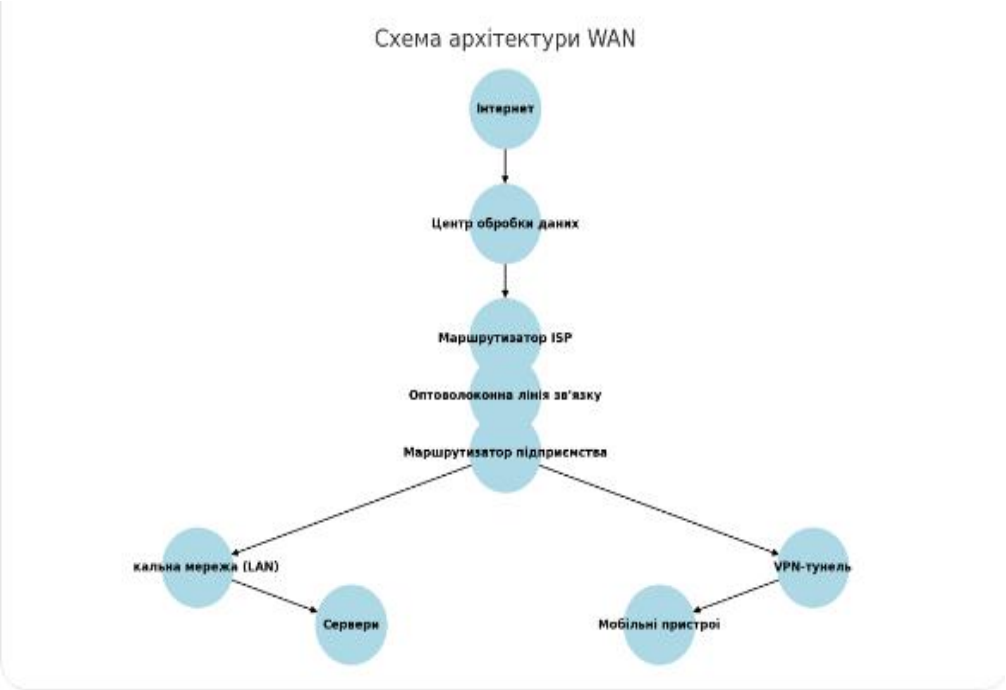


Рис 6.5 Архітектура WAN із зазначенням ключових компонентів.

Існує кілька способів організації підключень у глобальних мережах:

- *Точка-точка (Point-to-Point)* – використовується для з'єднання двох вузлів безпосередньо через виділений канал.
- *Комутовані мережі (Switched Networks)* – використовують інфраструктуру провайдера для динамічного маршрутизації трафіку через кілька вузлів.
- *MPLS (Multiprotocol Label Switching)* – сучасна технологія для швидкої маршрутизації пакетів даних через попередньо визначені канали.

Більшість WAN-з'єднань використовує **послуги телекомунікаційних компаній**:

- *Інтернет-провайдери (ISP)* – надають доступ до Інтернету через кабельні, оптоволоконні та мобільні мережі.
- *Провайдери MPLS* – пропонують приватні канали з високим рівнем безпеки для корпоративних клієнтів.

- *Супутникові оператори* – забезпечують підключення у віддалених регіонах.

Архітектура WAN складається з кінцевих пристроїв, маршрутизаторів, комутованих мереж та провайдерської інфраструктури. Використання різних типів з'єднань дає змогу організаціям адаптувати WAN під власні потреби – від традиційних точка-точка каналів до складних MPLS-мереж.

Глобальні мережі (**WAN**) використовують різні типи з'єднань для забезпечення зв'язку між віддаленими пристроями та мережами. Вибір технології залежить від таких факторів, як **швидкість передачі даних, доступність інфраструктури, вартість та рівень безпеки**.

Комутовані з'єднання є найстарішою формою підключення до WAN і використовують телефонні лінії для передачі даних.

- *Dial-up (аналогове з'єднання)* – низькошвидкісне підключення через телефонну мережу з використанням модему. Максимальна швидкість – до **56 Кбіт/с**.
- *ISDN (Integrated Services Digital Network)* – цифровий варіант телефонного підключення, що забезпечує швидкість до **128 Кбіт/с**.

Переваги: доступність, простота налаштування. **Недоліки**: низька швидкість, високі затримки, витіснені сучаснішими технологіями.

Виділені лінії – це **постійне фізичне з'єднання** між двома мережами або вузлами.

- *Leased Line (орендована лінія)* – забезпечує фіксовану смугу пропускання між точками.
- *T1/E1* – стандартизовані цифрові канали (T1 – **1,5 Мбіт/с**, E1 – **2,048 Мбіт/с**).
- *DSL (Digital Subscriber Line)* – технологія, що використовує телефонні лінії для передачі даних (швидкість до **100 Мбіт/с**).
- *Metro Ethernet* – використання Ethernet-технології у WAN для високошвидкісного з'єднання між офісами у межах міста.

Переваги: висока швидкість, надійність.

Недоліки: висока вартість, обмеження за відстанню.

Розвиток WAN призвів до появи більш ефективних технологій передачі даних, а саме:

- *MPLS (Multiprotocol Label Switching)* – забезпечує маршрутизацію на основі міток, що підвищує продуктивність.
- *ATM (Asynchronous Transfer Mode)* – використовує фіксовані пакети для передачі даних, забезпечуючи низькі затримки.
- *Frame Relay* – застаріла технологія пакетної комутації для організації приватних WAN-каналів.
- *SD-WAN (Software-Defined WAN)* – програмно-визначена технологія, що автоматизує управління WAN-з'єднаннями та оптимізує використання доступних каналів.

Переваги SD-WAN: адаптивність, зниження витрат, централізоване управління.

Недоліки SD-WAN: потреба у високошвидкісному з'єднанні та складніша конфігурація.

У віддалених регіонах або при відсутності наземної інфраструктури використовуються **супутникові та бездротові технології**:

- *Супутниковий Інтернет* – використовує геостаціонарні та низькоорбітальні супутники (Starlink, OneWeb).
- *5G WAN* – мобільні мережі нового покоління, що можуть використовуватися для резервного підключення.
- *Мікрохвильові радіорелейні лінії* – точка-точка з'єднання для організації WAN без фізичних кабелів.

Переваги: глобальне покриття, відсутність залежності від кабельної інфраструктури.

Недоліки: затримки в супутникових каналах, залежність від погодних умов.

WAN-з'єднання можуть бути організовані за допомогою різних технологій, від традиційних комутованих ліній до сучасних SD-WAN та супутникового

Інтернету. Вибір рішення залежить від **потреб у швидкості, доступності каналів, вартості та рівня безпеки**.

Глобальні мережі (**WAN**) використовують різні **протоколи та технології маршрутизації**, які забезпечують ефективну передачу даних на великі відстані. Основні протоколи WAN визначають спосіб встановлення з'єднання, організацію маршрутизації та механізми безпеки.

На канальному рівні OSI у WAN використовуються наступні протоколи:

- *PPP (Point-to-Point Protocol)* – один із найстаріших WAN-протоколів, що забезпечує аутентифікацію, шифрування та стиснення даних.
- *HDLC (High-Level Data Link Control)* – протокол, який використовується для з'єднань "точка-точка" у середовищі Cisco та інших маршрутизаторів.
- *Frame Relay* – комутаційна технологія, що використовувалася у приватних WAN-мережах для передачі даних у вигляді кадрів.

Переваги: ефективність, сумісність з різними мережевими пристроями.

Недоліки: обмежена масштабованість у порівнянні з сучасними WAN-рішеннями.

Для забезпечення маршрутизації трафіку між віддаленими мережами у WAN використовуються спеціалізовані протоколи:

- *BGP (Border Gateway Protocol)* – основний протокол маршрутизації в Інтернеті, що використовується між автономними системами (ISP, великі корпорації).
- *OSPF (Open Shortest Path First)* – динамічний протокол маршрутизації, який швидко адаптується до змін у топології мережі.
- *EIGRP (Enhanced Interior Gateway Routing Protocol)* – пропрієтарний протокол Cisco, що забезпечує ефективну маршрутизацію у великих корпоративних мережах.

Переваги: гнучкість у маршрутизації, підтримка великих мереж.

Недоліки: складність налаштування та необхідність професійного адміністрування.

Безпека трафіку у WAN забезпечується **тунелюванням**, що дає змогу передавати дані через публічні мережі у захищеному вигляді.

Основні технології тунелювання:

- *GRE (Generic Routing Encapsulation)* – інкапсуляція пакетів для передачі через WAN, що дає змогу з'єднувати віддалені LAN.
- *IPsec VPN (Internet Protocol Security)* – забезпечує шифрування та автентифікацію даних, що передаються через Інтернет.

Переваги: безпечний доступ до віддалених ресурсів.

Недоліки: додаткові затримки через процеси шифрування.

WAN використовує **різноманітні протоколи маршрутизації та передачі даних**, що забезпечують ефективну взаємодію між віддаленими вузлами. Важливими аспектами є **тунелювання трафіку та безпека переданих даних**, що реалізується через VPN, GRE та IPsec.

Глобальні мережі (**WAN**) відіграють вирішальну роль у забезпеченні доступу до Інтернету, підключенні корпоративних структур до хмарних сервісів та підтримці комунікацій між віддаленими офісами. Основним викликом при використанні WAN є баланс між **швидкістю, безпекою та стабільністю підключення**.

Доступ до Інтернету через WAN може бути організований різними способами:

- *Через провайдера Інтернету (ISP, Internet Service Provider)* – підключення через оптоволоконні, DSL або мобільні мережі.
- *Використання приватних каналів (MPLS, Metro Ethernet)* – корпоративні організації часто використовують окремі канали для підключення до дата-центрів.
- *Хмарні підключення* – компанії можуть використовувати **AWS Direct Connect, Azure ExpressRoute** для прямого доступу до хмарних сервісів.

Переваги: висока швидкість та безперебійність підключення.

Недоліки: залежність від інфраструктури провайдерів та потреба у додатковому захисті.

У сучасних WAN широко використовуються хмарні сервіси, які дають можливість компаніям зменшити витрати на власну інфраструктуру:

- *AWS Direct Connect* – створює безпечний і швидкий канал між корпоративною мережею та Amazon Web Services.
- *Azure ExpressRoute* – забезпечує захищене з'єднання з сервісами Microsoft Azure.
- *Google Cloud Interconnect* – дає змогу напряму підключатися до Google Cloud.

Переваги: стабільність з'єднання, низькі затримки, підвищена безпека.

Недоліки: висока вартість, потреба у спеціалізованому адмініструванні.

Оскільки глобальні мережі часто передають конфіденційні дані через відкриті канали, необхідно використовувати засоби захисту:

- *VPN (Virtual Private Network)* – шифрує трафік та забезпечує безпечний доступ до корпоративних ресурсів.
- *Брандмауери (Firewalls)* – контролюють вхідні та вихідні з'єднання, запобігаючи атакам.
- *IDS/IPS (Intrusion Detection/Prevention Systems)* – аналізують трафік на предмет підозрілої активності та блокують потенційні загрози.

Переваги: підвищена конфіденційність, запобігання атакам.

Недоліки: додаткові витрати на адміністрування та шифрування.

WAN забезпечує **доступ до Інтернету, інтеграцію з хмарними сервісами та передачу конфіденційних даних між корпоративними мережами**. Використання VPN, брандмауерів та хмарних рішень дає змогу підвищити безпеку та продуктивність WAN-з'єднань.

Оскільки **WAN-з'єднання охоплюють великі відстані**, важливим аспектом є **управління продуктивністю**, яке дає змогу **мінімізувати затримки, оптимізувати використання каналів зв'язку та покращити якість сервісів**. Оптимізація WAN сприяє підвищенню ефективності роботи корпоративних мереж і зменшенню витрат на інфраструктуру.

QoS (Quality of Service) – це набір технологій, що дає змогу **пріоритизувати мережевий трафік** для покращення продуктивності критичних сервісів.

Методи QoS у WAN:

- *Пріоритетний трафік* – важливі служби (VoIP, відеоконференції) отримують вищий пріоритет перед некритичними (завантаження файлів, потокове відео).
- *Обмеження смуги пропускання (Bandwidth Control)* – контроль використання каналів для рівномірного розподілу ресурсів.
- *Traffic Shaping* – згладжування трафіку задля уникнення перевантаження каналів.

Переваги: підвищення якості сервісів, зниження затримок.

Недоліки: потреба у точному налаштуванні та моніторингу.

Для підвищення надійності WAN використовують **балансування навантаження (Load Balancing)** та **резервування з'єднань (Failover Mechanisms)**.

- *Load Balancing* – розподіляє трафік між кількома каналами для запобігання перевантаженню.
- *Failover Mechanisms* – автоматичне перемикання на резервний канал при відмові основного.
- *Механізм BGP Multihoming* – підключення до кількох Інтернет-провайдерів для підвищення надійності.

Переваги: безперервність роботи мережі, зниження ризику відмов.

Недоліки: складність налаштування та необхідність підтримки кількох підключень.

SD-WAN (Software-Defined WAN) – це програмно-керована технологія, яка дає змогу автоматично **керувати маршрутами трафіку, обираючи найефективніші канали**.

Основні переваги SD-WAN:

- *Динамічний вибір маршруту* – оптимізує використання доступних каналів у режимі реального часу.

- *Зниження витрат* – дає змогу комбінувати дорогі MPLS-з’єднання з дешевшими Інтернет-каналами.
- *Підвищена безпека* – інтеграція з VPN, шифрування трафіку та контроль доступу.

Переваги: адаптивність, зниження витрат на WAN-з’єднання.

Недоліки: складність впровадження та потреба у централізованому керуванні.

Оптимізація WAN дає змогу **мінімізувати затримки, покращити стабільність з’єднання та зменшити витрати**. Використання **QoS, балансування навантаження та SD-WAN** робить WAN-з’єднання більш ефективними та надійними.

З розвитком технологій **WAN-інфраструктура** зазнає суттєвих змін. Традиційні підходи до управління глобальними мережами поступово замінюються на **програмно-визначені рішення (SD-WAN), інтеграцію 5G та супутникові технології**. Це дає змогу забезпечити **гнучкість, швидкість і надійність підключень** для підприємств та кінцевих користувачів.

- SD-WAN поступово замінює традиційні WAN-рішення, уможливлюючи динамічне керування маршрутами трафіку.

Основні тенденції SD-WAN:

- *Інтеграція з хмарними сервісами* – безпечне з'єднання між WAN та хмарними платформами (AWS, Google Cloud, Azure).
- *Автоматизація та штучний інтелект* – використання AI для розумного керування мережею.
- *Гнучкість у використанні різних каналів* – комбінування MPLS, LTE, 5G для підвищення продуктивності.

Переваги: автоматизація, гнучкість, зниження витрат.

Недоліки: потреба у централізованому керуванні та підтримці.

Мобільні мережі **5G** відіграють важливу роль у розвитку WAN, забезпечуючи **високошвидкісні з’єднання** для корпоративних мереж та IoT-пристроїв.

- *Швидкість до 10 Гбіт/с* –дає змогу використовувати 5G як основний або резервний WAN-канал.
- *Зниження затримок (<1 мс)* –критично важливо для промислових та фінансових сервісів.
- *Гнучкість у розгортанні* – можливість використання приватних 5G-мереж для підприємств.

Переваги: мобільність, швидкість, надійність.

Недоліки: обмежена зона покриття, залежність від операторів.

Також штучний інтелект активно впроваджується у WAN для:

- *Передбачення збоїв та оптимізації маршрутизації.*
- *Автоматичного перерозподілу навантаження.*
- *Захисту мереж від DDoS-атак та кіберзагроз.*

Переваги: мінімізація простоїв, підвищена безпека.

Недоліки: складність впровадження.

Останнім часом **супутниковий Інтернет** активно розвивається завдяки проєктам:

- *Starlink (SpaceX)* – низькоорбітальні супутники з низькою затримкою.
- *OneWeb, Amazon Kuiper* – конкуруючі рішення для глобального покриття.

Переваги супутникового Інтернету у WAN:

- *Доступ до Інтернету у віддалених регіонах.*
- *Мінімізація залежності від наземної інфраструктури.*
- *Резервування підключень для критично важливих систем.*

Переваги: глобальне покриття, незалежність від наземних провайдерів.

Недоліки: висока вартість обладнання, чутливість до погодних умов.

Сучасні WAN зазнають значних змін завдяки **впровадженню SD-WAN, 5G, штучного інтелекту та супутникових рішень**. Це дає змогу забезпечити **більш стабільне, безпечне та ефективне підключення** у всьому світі.

Глобальні мережі (**WAN**) є основою сучасної IT-інфраструктури, забезпечуючи **зв'язок між віддаленими вузлами, доступ до хмарних сервісів та безперебійний обмін даними**. WAN використовується у корпоративних

мережах, державних структурах, Інтернет-провайдерах та навіть у космічних комунікаціях.

Основні висновки щодо WAN:

- WAN відрізняється від LAN та MAN тим, що охоплює **великі території** та використовує інфраструктуру телекомунікаційних провайдерів.
- Основні типи з'єднань – від комутованих ліній до сучасних SD-WAN та 5G-рішень.
- Маршрутизація в WAN – здійснюється за допомогою **BGP, OSPF, MPLS, VPN**.
- Оптимізація продуктивності – забезпечується через **QoS, балансування навантаження та SD-WAN**.
- Нові технології – 5G, AI-автоматизація, супутниковий Інтернет (Starlink, OneWeb) змінюють традиційні WAN-мережі.

Основними перевагами WAN є:

- *Масштабованість* – підтримка великих територіальних мереж.
- *Гнучкість підключень* – використання різних технологій (кабельні, бездротові, супутникові).
- *Розширена безпека* – впровадження **VPN, шифрування, Zero Trust Architecture**.
- *Оптимізація через SD-WAN* – зменшення витрат на інфраструктуру та автоматизація управління трафіком.

Виклики та перспективи розвитку WAN:

- *Висока вартість приватних каналів* – MPLS та орендовані лінії коштують дорого.
- *Перевантаження мережі* – зростаючий трафік (хмарні сервіси, відео, IoT) створює нові виклики.
- *Залежність від провайдерів* – якість підключення часто залежить від ISP.
- *Безпекові ризики* – кібератаки, перехоплення трафіку, DDoS.

Перспективи WAN:

- Перехід на повністю програмно-визначені WAN (SD-WAN).

- Інтеграція 5G для корпоративних WAN-мереж.
- Розвиток супутникового Інтернету для резервування підключень.
- Застосування AI для моніторингу та оптимізації WAN.

Рис 6.6 Прогноз розвитку WAN на найближчі 10 років

Глобальні мережі WAN забезпечують стабільне з'єднання між континентами, підтримку хмарних сервісів та надійний доступ до корпоративних ресурсів. Розвиток SD-WAN, 5G та супутникових технологій змінює традиційні підходи до побудови WAN, роблячи їх більш гнучкими, ефективними та безпечними.

У найближчі роки автоматизація та штучний інтелект значно поліпшать управління WAN, а нові технології зв'язку допоможуть розв'язатипроблеми перевантаження та кібербезпеки.

Лекція 7: Огляд категорій атак на комп’ютерні мережі

Мережева безпека є одним із найважливіших аспектів сучасної цифрової інфраструктури, оскільки від неї залежить захист конфіденційної інформації, безперебійність роботи систем та стійкість до атак. Кожен пристрій, підключений до мережі, потенційно є ціллю для зловмисників, а рівень складності атак та методів їхнього виконання постійно зростає. У сучасному світі компанії, державні установи та навіть окремі користувачі стикаються з різноманітними загрозами: від крадіжки особистих даних до атак на критичну інфраструктуру, які можуть спричинити серйозні наслідки, включаючи фінансові втрати, зупинку виробництва та компрометацію державних систем.

Ключовим викликом є те, що мережева безпека не є статичним поняттям – це динамічна сфера, що потребує постійного оновлення стратегій захисту, впровадження нових технологій та адаптації до змін у тактиках атак. Традиційні методи захисту, такі як брандмауери, антивірусні програми та шифрування, вже не завжди ефективні у боротьбі з новітніми загрозами, які використовують штучний інтелект, соціальну інженерію та складні атаки на рівні протоколів зв’язку. Однією з найважливіших складових мережевої безпеки є **підхід багаторівневого захисту**, коли різні методи оборони працюють разом, створюючи єдину систему безпеки, що здатна адаптуватися до загроз у режимі реального часу.

Основні загрози мережевої безпеки поділяються на кілька категорій. Це **атакуючі дії на рівні мережі**, коли зловмисники намагаються перехопити трафік, отримати несанкціонований доступ або викликати відмову в обслуговуванні. Також є **загрози на рівні користувачів**, які часто стають найслабшою ланкою у системі безпеки через використання слабких паролів, фішингових атак або програм-шпигунів. Додатковим фактором ризику є **незахищені бездротові мережі**, які можуть бути легко атаковані за допомогою підроблених точок доступу або методів злому слабкого шифрування.

Із зростанням хмарних технологій та розвитку концепції **Інтернету речей (IoT)** ситуація ще більше ускладнюється. Кількість пристроїв, що підключаються до Інтернету, збільшується в геометричній прогресії, а їхня захищеність часто залишається під питанням. Багато IoT-пристроїв мають обмежені обчислювальні потужності, що ускладнює впровадження стандартних засобів безпеки, таких як шифрування або багатофакторна автентифікація. Це створює величезну кількість потенційних точок входу для атак, і будь-який скомпрометований пристрій може стати джерелом загрози для всієї мережі.

Окрім технологічних аспектів, значну роль у забезпеченні безпеки відіграє **людський фактор**. Користувачі можуть ненавмисно стати жертвами атак через **фішингові повідомлення, використання незахищених паролів або нехтування політиками безпеки**. Саме тому навчання користувачів, регулярні тренінги з кібербезпеки та впровадження **принципу найменших привілеїв** у доступі до систем є критично важливими для забезпечення захисту корпоративних мереж.

Сучасні підходи до мережевої безпеки включають не лише захист окремих елементів інфраструктури, а й комплексний моніторинг усього середовища, автоматичне виявлення загроз, використання машинного навчання для аналізу поведінки користувачів та алгоритмів виявлення аномалій. Такі методи дають можливість оперативно реагувати на спроби атак, мінімізувати ризики та впроваджувати проактивні заходи, спрямовані на запобігання загрозам.

Загалом, мережева безпека є важливим компонентом функціонування будь-якої організації або цифрової екосистеми. Вона базується на **поєднанні апаратних засобів, програмних рішень, політик доступу, навчання персоналу та активного моніторингу**. Комплексний підхід до безпеки дає змогу не лише запобігати атакам, а й забезпечувати **цілісність, доступність та конфіденційність даних**, що є основними принципами інформаційної безпеки.

Усі ці аспекти мають величезне значення для корпоративних та державних організацій, оскільки кіберзлочинці використовують все складніші методи атак. В останні роки спостерігається збільшення кількості атак на ланцюги поставок

(Supply Chain Attacks), спрямованих на компрометацію ПЗ, яке використовується тисячами компаній по всьому світу. Наприклад, атака на SolarWinds у 2020 році призвела до витоку конфіденційної інформації з десятків урядових установ США та інших країн.

Окрему увагу слід приділити **протидії загрозам, пов'язаним із соціальною інженерією**. Сучасні атаки більше не обмежуються технічними експлойтами – зловмисники все частіше маніпулюють користувачами, змушуючи їх самостійно відкривати доступ до систем. **Фішингові листи, телефонні дзвінки від "служби підтримки" та підроблені веб-сайти** є основними інструментами соціальної інженерії. Це підтверджує необхідність не тільки технічного захисту, а й підвищення обізнаності користувачів про загрози.

Рис 7.1 Загальна схема мережевої безпеки, що включає шифрування, брандмауери, системи виявлення вторгнень та політики доступу

Окрім цього, кіберзлочинці активно використовують **ботнети**, які можуть складатися з мільйонів заражених пристроїв. Ці мережі використовуються для

масованих DDoS-атак, розсилки спаму, крадіжки облікових даних та зламу корпоративних систем. У 2021 році одна з найпотужніших DDoS-атак на сервіс Microsoft Azure досягла пікової потужності **2,4 Тбіт/с**, що свідчить про те, що загрози з боку ботнетів продовжують зростати.

Зважаючи на все це, мережева безпека повинна бути глобальним пріоритетом, а компанії мають впроваджувати проактивні методи захисту, автоматизацію моніторингу, використання штучного інтелекту та новітніх криптографічних алгоритмів.

Мережеві атаки стають дедалі складнішими, а їхні наслідки – серйознішими. Зловмисники можуть перехоплювати дані, змінювати мережеві пакети, здійснювати атаки на сервери та навіть повністю виводити мережі з ладу. Захист від таких загроз потребує комплексного підходу, що включає як апаратні, так і програмні рішення, а також відповідні політики безпеки.

Одна з найпоширеніших загроз – це **атаки типу "людина посередині" (MITM – Man-in-the-Middle)**, коли зловмисник перехоплює та змінює дані, що передаються між клієнтом і сервером.

MITM-атака може здійснюватися через підроблені точки доступу Wi-Fi, маніпуляції з ARP-кешем або DNS-запитами. Наприклад, користувач підключається до безкоштовного Wi-Fi у кафе, а зловмисник, створивши точку з такою ж назвою, перехоплює всі його запити, включаючи логіни та паролі.

DDoS (Distributed Denial of Service) – це атака на мережу, що спрямована на перевантаження сервера великою кількістю запитів, через що він стає недоступним для легітимних користувачів.

DDoS-атаки можуть бути реалізовані через ботнети – мережі заражених комп’ютерів, які під управлінням хакера починають одночасно надсилати запити до цілі. Великі компанії та державні установи часто стають жертвами таких атак, що призводить до зупинки онлайн-сервісів та фінансових збитків.

Віруси, трояни та інше зловмисне ПЗ можуть проникати в мережі через шкідливі вкладення в електронних листах, завантаження файлів з ненадійних джерел або через заражені веб-сайти.

- **Трояни** надають зловмисникам віддалений доступ до зараженого комп’ютера.
- **Руткіти** приховують свою присутність у системі та дають можливість зловмисникам маніпулювати мережею без відома адміністратора.
- **Шпигунські програми** можуть викрадати конфіденційну інформацію (паролі, дані кредитних карток).

У 2020-2022 роках атаки програм-вимагачів стали масовими, зачіпаючи як бізнес, так і державні установи. Випадок з Colonial Pipeline у США показав, наскільки критичними можуть бути наслідки таких атак: через компрометацію системи управління постачанням палива довелося повністю зупинити роботу одного з найбільших паливних операторів.

Бездротові мережі особливо вразливі до атак, оскільки сигнал передається через повітря та може бути перехоплений.

Основні загрози Wi-Fi:

- *Атака Evil Twin* – створення зловмисником підробленої точки доступу, що має ідентичну назву з легітимною, для перехоплення даних користувачів.
- *Перехоплення трафіку (Packet Sniffing)* – прослуховування переданих пакетів за допомогою програм, таких як Wireshark.
- *Злом шифрування WPA/WPA2* – використання атак на слабкі паролі або вразливості WPS для отримання доступу до мережі.

Останнім часом атакуючі методи стають все більш витонченими, і зловмисники використовують комбінації різних підходів для досягнення своїх цілей. Однією з таких загроз є **атаки на ланцюги постачання (Supply Chain Attacks)**. Вони націлені на **компрометацію постачальників програмного забезпечення або апаратних рішень** для подальшого проникнення у корпоративні мережі. Відомий випадок атаки на SolarWinds у 2020 році продемонстрував, що зловмисники можуть впроваджувати шкідливий код у оновлення програмного забезпечення, яке розповсюджується серед тисяч клієнтів.

Крім технічних загроз, **велика частина атак ґрунтується на маніпулюванні користувачами**. Фішинг залишається **найпоширенішим способом компрометації облікових записів**, оскільки жертви самі вводять свої дані на підроблених сайтах. Зловмисники використовують підроблені електронні листи, повідомлення у месенджерах та соціальних мережах, маскуючи їх під комунікації від банків, роботодавців або сервісних компаній.

Захист від таких атак включає **навчання співробітників та користувачів**, використання **багатофакторної автентифікації**, автоматизованих систем моніторингу загроз та **розширеного аналізу поведінки користувачів** для виявлення підозрілих дій.

Загалом, загрози для комп'ютерних мереж еволюціонують разом із розвитком технологій. Для їхнього ефективного виявлення та запобігання компанії повинні застосовувати комплексний підхід до безпеки, що включає автоматизовані інструменти виявлення атак, AI-аналіз трафіку, мережеве зонування та багаторівневий контроль доступу.

Розробка ефективних політик безпеки є критично важливим елементом управління мережею, оскільки саме вони визначають правила доступу, контроль трафіку, способи автентифікації та заходи реагування на інциденти. Без чітких політик безпеки навіть найдосконаліші технічні рішення можуть виявитися неефективними, адже саме людський фактор та помилки в адмініструванні часто стають основними причинами витоків інформації або компрометації мереж. Політики безпеки мають бути гнучкими, адаптивними та відповідати реальним загрозам, які постійно змінюються у зв'язку з розвитком нових технологій та методів атак. Організації повинні впроваджувати комплексні моделі захисту, що поєднують різні рівні контролю та запобіжні заходи для мінімізації ризиків. Важливим аспектом є документування всіх правил та інструкцій, а також постійний аудит їхньої відповідності сучасним стандартам та законодавчим вимогам.

Одним із фундаментальних принципів побудови ефективної системи безпеки є **принцип найменших привілеїв**, який передбачає, що кожен

користувач чи пристрій отримує доступ лише до тих ресурсів, які необхідні для виконання їхніх функцій. Це дає змогу значно зменшити ризики, пов’язані з несанкціонованим доступом та помилковими діями працівників. Також важливо розмежовувати рівні доступу за категоріями користувачів, що дає змогу обмежувати можливість критичних змін у мережевих налаштуваннях лише для адміністративного персоналу. Впровадження **багатофакторної автентифікації (MFA)** є ще одним важливим кроком у підвищенні безпеки, оскільки зменшує ймовірність компрометації облікових записів у випадку витоку паролів.

Загалом, ефективна політика безпеки повинна передбачати декілька рівнів контролю. Наприклад, використання білого списку додатків (Application Whitelisting) дає змогу запускати у системі лише перевірені програми, що значно знижує ризик запуску шкідливого ПЗ. Контроль доступу за часом і місцем входу (Geo-IP фільтрація, обмеження доступу у неробочий час) допомагає виявляти та блокувати підозрілі спроби підключення. Впровадження автоматизованих систем виявлення загроз (IDS/IPS) дає змогу не лише реєструвати підозрілу активність у мережі, але й автоматично блокувати небезпечні дії, що суттєво знижує ризик атак.

Останніми роками у корпоративному секторі все більше впроваджується модель **Zero Trust**, яка базується на принципі «ніколи не довіряй, завжди перевіряй». Це означає, що кожен користувач, пристрій або додаток повинен проходити перевірку незалежно від того, знаходиться він у внутрішній мережі компанії чи підключається ззовні. У традиційних підходах до безпеки зазвичай вважалося, що пристрої та користувачі всередині корпоративної мережі є довіреними, проте практика показала, що така модель є вразливою до атак. Впровадження Zero Trust передбачає, що всі підключення постійно перевіряються, незалежно від того, з якої мережі вони здійснюються. Ключові елементи цієї моделі включають **багаторівневу автентифікацію, поведінковий аналіз трафіку, мікросегментацію мережі та постійний моніторинг активності**.

Розподіл мережі на **сегменти та ізольовані зони** є важливим елементом безпеки, оскільки дає змогу обмежити масштаб потенційної атаки. Наприклад, виділення **демілітаризованої зони (DMZ)** для сервісів, які повинні бути доступні з Інтернету (вебсервери, поштові сервери, VPN-шлюзи), дає змогу ізолювати їх від критично важливих внутрішніх ресурсів. Корпоративні мережі можуть використовувати **віртуальні локальні мережі (VLAN)** для ізоляції трафіку між різними відділами компанії, що запобігає несанкціонованому доступу. Впровадження політики сегментованого доступу значно знижує ризик розповсюдження атак у разі компрометації одного з сегментів.

Контроль безпеки також повинен включати **постійний аудит, тестування на проникнення та аналіз вразливостей**. Регулярне сканування мережевої інфраструктури на предмет слабких місць дає змогу своєчасно виявляти ризики та виправляти їх до того, як вони будуть використані зловмисниками. Важливим елементом безпеки є **навчання персоналу**, оскільки навіть найдосконаліші засоби захисту можуть виявитися неефективними, якщо співробітники компанії нехтують правилами безпеки, використовують слабкі паролі або потрапляють на фішингові атаки.

Проблема сучасної мережевої безпеки полягає в тому, що зловмисники постійно знаходять нові методи обходу традиційних засобів захисту. Наприклад, **атаки на довірені сервіси (Living off the Land attacks)** використовують легітимні мережеві протоколи та програми для проникнення в систему, що робить їх важчими для виявлення. Використання штучного інтелекту для аналізу поведінки користувачів допомагає виявляти **аномальну активність**, наприклад, підозрілі запити на доступ до конфіденційної інформації або підключення з незвичних локацій.

Ще одним важливим аспектом є **захист даних під час їхньої передачі та зберігання**. Політики безпеки повинні передбачати **автоматичне шифрування файлів та мережевого трафіку**. Наприклад, використання **SSL/TLS для зашифрованих з'єднань, IPsec для VPN-тунелів та шифрування дисків за допомогою BitLocker** значно підвищує рівень захисту. Важливою є також

політика резервного копіювання, оскільки у разі атак програм-вимагачів компанії зможуть швидко відновити свої дані без необхідності виплачувати викуп.

Загалом, ефективна модель безпеки повинна бути гнучкою, багаторівневою та адаптивною до сучасних загроз. Вона повинна включати комбінацію мережевих політик, технічних засобів захисту, поведінкової аналітики, сегментування трафіку, автоматичного шифрування та постійного моніторингу активності. Тільки комплексний підхід до безпеки дає змогу організаціям мінімізувати ризики та протистояти сучасним загрозам.

Захист даних у мережах неможливий без шифрування та автентифікації, оскільки ці технології забезпечують конфіденційність, цілісність і справжність переданої інформації. У світі, де інформація є ключовим ресурсом, загроза її перехоплення та компрометації є серйозним викликом. Зловмисники використовують методи перехоплення трафіку, атаки на протоколи безпеки та підробку автентифікації для отримання несанкціонованого доступу. Без належного шифрування будь-яка передача даних через Інтернет або корпоративну мережу стає потенційно вразливою до атак, які можуть спричинити витік конфіденційної інформації, фінансові втрати або навіть компрометацію державних чи військових мереж.

Шифрування дає змогу перетворювати відкритий текст у зашифрований формат, який може бути розшифрований лише за наявності спеціального ключа. Найпоширенішими методами шифрування є **симетричне та асиметричне шифрування**. Симетричне шифрування передбачає використання одного ключа як для шифрування, так і для дешифрування даних. Одним із найвідоміших алгоритмів симетричного шифрування є **AES (Advanced Encryption Standard)**, який широко використовується у VPN, WPA3 та інших технологіях захисту. Його головною перевагою є висока швидкість роботи, що робить його ідеальним для потокового шифрування великих обсягів даних. Проте проблема симетричного шифрування полягає у безпечному обміні ключами: якщо ключ буде перехоплений, усі дані можна дешифрувати.

Асиметричне шифрування використовує два різні ключі – відкритий та закритий. Відкритий ключ використовується для шифрування даних, тоді як закритий – для їхнього дешифрування. Найвідоміші алгоритми цього типу – RSA (Rivest-Shamir-Adleman) та ECC (Elliptic Curve Cryptography). Вони використовуються у цифрових підписах, SSL/TLS-захисті вебсайтів, захищених каналах зв'язку. Головною перевагою асиметричного шифрування є те, що ключі не потрібно передавати між сторонами, що мінімізує ризик їхнього перехоплення. Недоліком є висока обчислювальна складність, яка потребує більше ресурсів у порівнянні з симетричним шифруванням.

SSL/TLS – це протоколи безпеки, що використовують **асиметричне шифрування** для забезпечення захищеного передавання даних між клієнтами та серверами. Вони є основою безпечного веб-трафіку через HTTPS, захищають банківські операції, онлайн-автентифікацію та корпоративні системи. Використання **SSL-сертифікатів** гарантує, що дані передаються у зашифрованому вигляді, унеможливлюючи їхнє перехоплення зловмисниками. Однак атаки типу **"людина посередині" (MITM)** можуть обходити SSL-захист у випадку компрометації сертифікатів або довірених центрів сертифікації.

Автентифікація є ще одним важливим компонентом безпеки, оскільки вона дає змогу визначити, чи є користувач або пристрій дійсно тим, за кого він себе видає. Традиційно автентифікація базується на введенні **паролю**, однак цей метод є одним із найуразливіших. Користувачі часто використовують **слабкі паролі**, які легко зламати, або повторно застосовують один і той самий пароль для кількох облікових записів, що збільшує ризик компрометації. Одним із найбільш ефективних методів захисту є використання **багатофакторної автентифікації (2FA, MFA)**, яка включає додаткові рівні перевірки: код із SMS або додатка-аутентифікатора, біометричні дані або фізичний USB-ключ.

Рис 7.2 Схема двофакторної автентифікації – пароль + SMS-код

Біометрична автентифікація, така як **розпізнавання відбитків пальців, сканування сітківки ока або розпізнавання обличчя**, набуває дедалі більшої популярності завдяки зручності використання та високому рівню безпеки. Вона широко застосовується у мобільних пристроях, банківських системах та корпоративних мережах для підтвердження особи. Недоліком є можливість **спуфінгу біометричних даних**, коли зловмисники можуть використати підроблені відбитки пальців або фотографії для обходу захисту.

Ще одним ефективним підходом є використання **апаратних токенів** (наприклад, YubiKey), які забезпечують криптографічну автентифікацію та зменшують ризик зламу паролів. Такі ключі дають можливість безпечно проходити автентифікацію без необхідності введення паролів, що значно знижує ймовірність атак на соціальну інженерію.

Захист даних також включає шифрування інформації, що зберігається на жорстких дисках, серверних сховищах та у хмарних середовищах. Наприклад, технології **BitLocker, VeraCrypt та Apple FileVault** дають можливість автоматично шифрувати жорсткі диски, унеможливлюючи доступ до даних у разі фізичного викрадення пристрою. У корпоративних середовищах широко використовується **зашифрований обмін файлами через PGP (Pretty Good**

Privacy), який гарантує конфіденційність електронної пошти та переданих документів.

Шифрування та автентифікація є двома ключовими компонентами безпеки, які необхідні для захисту мережевої інфраструктури. Вони дають можливість уникати витоків даних, компрометації облікових записів та атак на перехоплення трафіку. Сучасні загрози, включаючи квантові атаки, можуть суттєво змінити методи шифрування в майбутньому, тому ведеться активна розробка постквантової криптографії, яка зможе витримати атаки квантових комп'ютерів.

Загалом, майбутнє безпеки мереж залежить від поєднання сучасних методів шифрування, багатофакторної автентифікації, штучного інтелекту для аналізу загроз та автоматизації процесів захисту. Використання цих технологій дає змогу гарантувати конфіденційність, цілісність та доступність інформації у глобальній мережі.

Мережевий захист базується на використанні багаторівневих механізмів контролю трафіку та ідентифікації потенційних загроз. Одними з найважливіших інструментів, які відіграють ключову роль у забезпеченні безпеки, є **брандмауери (firewalls) та системи виявлення та запобігання вторгненням (IDS/IPS)**. Вони дають можливість блокувати несанкціонований доступ до мережі, фільтрувати небажаний трафік та виявляти підозрілу активність, яка може свідчити про наявність атаки.

Брандмауери є першою лінією оборони, яка контролює всі вхідні та вихідні з'єднання. Вони працюють за принципом аналізу та фільтрації трафіку, дозволяючи або блокуючи певні запити відповідно до заздалегідь визначених правил. Існує два основних типи брандмауерів: апаратні та програмні. Апаратні брандмауери встановлюються на мережевих шлюзах і забезпечують централізований контроль трафіку між зовнішнім Інтернетом і внутрішньою мережею. Вони часто використовуються у великих корпоративних мережах для захисту серверів та критичних ресурсів. Програмні брандмауери працюють на рівні окремих пристроїв та забезпечують індивідуальний контроль трафіку на

рівні операційної системи. Наприклад, Windows Firewall та iptables у Linux є прикладами програмних брандмауерів.

Крім класичних механізмів фільтрації, сучасні брандмауери використовують глибокий аналіз пакетів (DPI – Deep Packet Inspection), що дає змогу детально перевіряти вміст трафіку, а не лише заголовки пакетів. Це дає змогу виявляти складніші загрози, такі як командно-контрольний трафік ботнетів, спроби експлуатації вразливостей та аномалії у мережевій поведінці. Наприклад, якщо система виявляє підозрілу активність, таку як масова передача даних у невідомі місця, брандмауер може автоматично блокувати таке з'єднання або перенаправити його для подальшого аналізу.

Брандмауери можуть працювати за різними принципами фільтрації. Фільтрація за адресами та портами (ACL – Access Control Lists) дає змогу задавати конкретні IP-адреси та порти, які дозволені або заборонені для використання. Це класичний підхід, який забезпечує базовий рівень безпеки, але є малоефективним проти складних атак. Більш прогресивний метод – станова фільтрація (Stateful Packet Inspection, SPI), яка аналізує контекст з'єднання та дає змогу або блокує трафік залежно від того, чи є він частиною раніше встановленої сесії.

Одним із важливих аспектів забезпечення безпеки є системи виявлення та запобігання вторгненням (IDS/IPS). Вони працюють разом із брандмауерами, але мають більш активну роль у боротьбі з кіберзагрозами. IDS (Intrusion Detection System) відповідає за виявлення підозрілої активності, але не втручається у процес обробки трафіку. Вона просто повідомляє адміністратора про можливі загрози, і той приймає рішення про подальші дії. IPS (Intrusion Prevention System), навпаки, має можливість не лише виявляти, але й автоматично блокувати шкідливий трафік у режимі реального часу.

IDS та IPS можуть працювати за двома основними методами аналізу: сигнатурним та поведінковим. Сигнатурний аналіз базується на використанні відомих шаблонів атак, які порівнюються із вхідним трафіком. Це дає змогу ефективно виявляти відомі загрози, але є малоефективним проти нових, раніше

невідомих атак. Поведінковий аналіз використовує штучний інтелект та машинне навчання, щоб виявляти аномальні дії у мережі, які можуть свідчити про атаку.

Ще одним важливим елементом безпеки є використання VPN (Virtual Private Network), що забезпечує захист даних під час передавання через відкриті мережі. VPN використовує технології шифрування для створення захищених тунелів, через які передаються дані між клієнтами та серверами. Це критично важливо для віддаленого доступу співробітників до корпоративних ресурсів, оскільки зменшує ризик перехоплення трафіку у публічних Wi-Fi мережах.

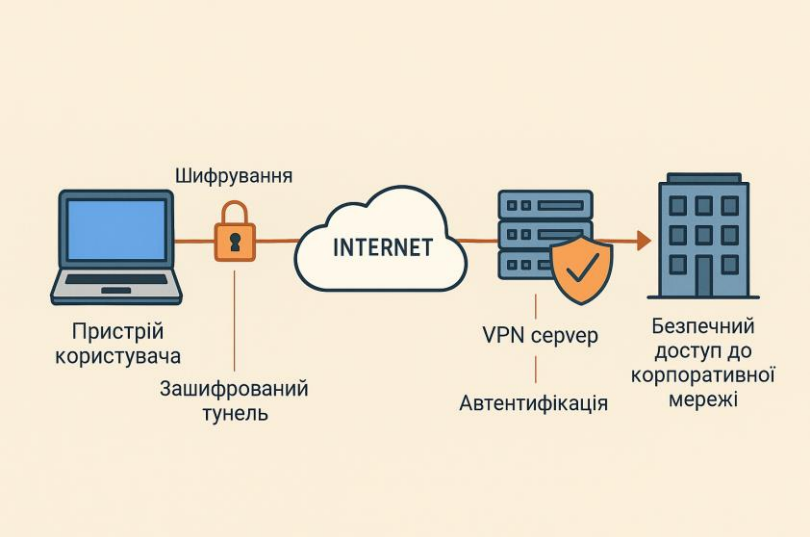


Рис 7.3 Схема роботи VPN (Virtual Private Network)

VPN може працювати на основі різних протоколів, кожен із яких має свої переваги та недоліки. PPTP (Point-to-Point Tunneling Protocol) є одним із найстаріших, але вважається недостатньо безпечним. L2TP/IPsec (Layer 2 Tunneling Protocol) забезпечує кращий рівень шифрування, але має підвищені вимоги до продуктивності. OpenVPN є одним із найбільш безпечних рішень, яке широко використовується завдяки гнучкості налаштувань та відкритому вихідному коду.

Сучасні VPN-рішення також використовують WireGuard, який забезпечує високий рівень продуктивності та захисту. Його перевагою є спрощена

архітектура у порівнянні з OpenVPN та IPsec, що робить його ідеальним для використання у мобільних пристроях та хмарних сервісах.

В умовах зростання загроз та активного використання мобільних та хмарних середовищ, брандмауери, IDS/IPS та VPN стали обов'язковими елементами безпеки для захисту сучасних мереж. Їхнє впровадження дає змогу не лише запобігати атакам, а й вчасно реагувати на підозрілу активність, зменшуючи потенційні ризики.

Сьогодні організації також використовують Zero Trust Network Access (ZTNA) замість традиційних VPN-рішень. ZTNA працює за принципом мінімальної довіри, перевіряючи кожне підключення та застосовуючи політики обмеженого доступу. Це дає змогу значно покращити безпеку віддалених підключень та знизити ризик компрометації мережі.

Усі ці технології разом створюють потужну багаторівневу систему захисту, яка допомагає виявляти, блокувати та мінімізувати загрози. Ефективне поєднання брандмауерів, IDS/IPS, VPN та сучасних Zero Trust-рішень забезпечує надійний захист організаційних мереж та конфіденційних даних.

Бездротові мережі є важливим компонентом сучасної IT-інфраструктури, адже вони забезпечують мобільність та зручність у підключенні користувачів до Інтернету та корпоративних ресурсів. Проте саме ця мобільність і відкритість робить Wi-Fi та інші бездротові технології надзвичайно вразливими до атак. Без належного захисту зловмисники можуть отримати доступ до переданих даних, викрасти конфіденційну інформацію або навіть повністю перехопити контроль над мережею. Тому питання безпеки бездротових технологій є критично важливим для будь-якої організації, що використовує Wi-Fi, мобільні з'єднання або IoT-інфраструктуру.

Однією з найпоширеніших проблем у бездротових мережах є незахищені точки доступу (AP, Access Points). Дуже часто користувачі підключаються до Wi-Fi у громадських місцях – у кафе, аеропортах, готелях, торгових центрах – не підозрюючи, що ці точки можуть бути підробленими або неправильно налаштованими. Атака типу Evil Twin передбачає створення зловмисником

підробленої точки доступу з ідентичним іменем (SSID), яка обманює користувачів і змушує їх підключатися до небезпечної мережі. У такій ситуації весь трафік користувача проходить через контрольовану хакером точку, що дає змогу перехоплювати паролі, банківські дані та інші чутливі відомості.

Ще однією серйозною проблемою є відсутність належного шифрування у бездротових мережах. Старі стандарти, такі як WEP (Wired Equivalent Privacy), більше не вважаються безпечними, оскільки можуть бути зламані за лічені хвилини навіть малодосвідченими хакерами. Більш сучасні стандарти WPA (Wi-Fi Protected Access) значно підвищили рівень захисту, але і вони мають вразливості. WPA2, який довгий час був стандартом для бездротової безпеки, у 2017 році отримав серйозну уразливість KRACK (Key Reinstallation Attack), що дозволяла перехоплювати дані, навіть якщо вони передавалися через захищене з'єднання.

Сучасним стандартом захисту є WPA3, який виправляє слабкі місця попередніх протоколів та вводить нові механізми захисту, такі як індивідуальне шифрування для кожного пристрою та захист від атак методом перебору паролів. Проте його впровадження йде повільно через необхідність оновлення обладнання, тому багато мереж все ще працюють на WPA2. Для підвищення безпеки у таких мережах рекомендується використовувати Enterprise-режим WPA2, який передбачає централізовану автентифікацію через сервер RADIUS.

Одним із найсерйозніших методів атаки на бездротові мережі є перехоплення трафіку (Packet Sniffing). Використовуючи спеціалізовані програми, такі як Wireshark або Aircrack-ng, зловмисники можуть відстежувати весь переданий трафік у незашифрованих мережах. Якщо користувачі передають конфіденційну інформацію у відкритому вигляді (наприклад, через HTTP), хакери можуть легко перехопити паролі, логіни та фінансові дані. Навіть якщо мережа використовує захист, її можна атакувати за допомогою відключення користувачів (Deauthentication Attack) – це метод, який примушує пристрої повторно підключатися до мережі, відкриваючи можливість атак на процес встановлення ключів шифрування.

Щоб захиститися від таких атак, користувачам слід дотримуватися декількох ключових принципів:

- *Використовувати VPN* для шифрування трафіку у громадських мережах.
- *Перевіряти SSID точки доступу перед підключенням.*
- *Не передавати важливі дані через незахищені сайти (HTTP).*
- *Відключати автоматичне підключення до відкритих Wi-Fi-мереж.*

Окрім загроз, пов'язаних із Wi-Fi, є ще одна велика категорія атак, що стосується **бездротових IoT-пристроїв**. Багато таких пристроїв, наприклад, розумні камери, датчики або системи управління будинком, мають слабкі механізми захисту, оскільки виробники часто не приділяють достатньої уваги безпеці. Внаслідок цього багато IoT-пристроїв мають **відкриті порти**, **заводські паролі** або навіть **працюють без шифрування трафіку**.

Одним із найвідоміших прикладів атак на IoT є **ботнет Mirai**, який у 2016 році заразив сотні тисяч незахищених пристроїв, використовуючи стандартні заводські паролі. Після зараження ці пристрої були використані для масових DDoS-атак, які призвели до глобальних збоїв в Інтернеті. З цієї причини рекомендується використовувати **сильні унікальні паролі, обмежувати віддалений доступ до IoT-пристроїв та оновлювати їхнє програмне забезпечення**.

Ще одним ефективним способом захисту бездротових мереж є **розділення трафіку на сегменти**. Наприклад, у корпоративних мережах можна виділити **окрему гостьову мережу**, яка не має доступу до основних ресурсів компанії. Це дає змогу мінімізувати ризик компрометації внутрішньої мережі у разі атаки на гостьовий сегмент. Також варто використовувати **MAC-фільтрацію**, яка дає змогу підключати до мережі лише перевірені пристрої, хоча цей метод не є надійним через можливість підміни MAC-адрес.

Сучасні підходи до захисту бездротових мереж включають **автоматизовані рішення**, такі як **системи виявлення атак на Wi-Fi (Wireless IDS/IPS)**, які аналізують поведінку пристроїв у бездротовій мережі та можуть автоматично

блокувати підозрілі з'єднання. Це особливо важливо у великих компаніях, де адміністратор фізично не може контролювати всі підключення.

Захист бездротових мереж вимагає комплексного підходу: **використання сучасних протоколів шифрування, впровадження VPN, обмеження доступу до IoT-пристроїв та моніторинг підозрілої активності**. Це дає змогу мінімізувати ризики атак та гарантувати безпечну роботу бездротової інфраструктури.

Ефективний захист комп’ютерних мереж неможливий без постійного **аудиту та моніторингу**, які дають можливість своєчасно виявляти загрози, аналізувати потенційні вразливості та запобігати атакам ще до їх реалізації. У сучасних організаціях інформаційна безпека вже давно не обмежується лише налаштуванням брандмауерів та VPN – зловмисники використовують складні методи обходу захисту, тому компаніям доводиться впроваджувати проактивні засоби аналізу трафіку, перевірки вразливостей та тестування на проникнення (penetration testing).

Основна мета аудиту мережевої безпеки полягає у перевірці відповідності інфраструктури компанії сучасним стандартам безпеки, ідентифікації слабких місць та оцінці ефективності існуючих заходів захисту. У рамках аудиту можуть перевірятися налаштування доступу, політики безпеки, конфігурація брандмауерів, рівень шифрування трафіку, рівень захищеності кінцевих пристроїв та стан резервного копіювання даних.

Одним із ключових методів моніторингу безпеки є **логування та аналіз подій у мережі**. Усі сервіси, сервери та мережеві пристрої генерують **журнали подій (лог-файли)**, які містять інформацію про підключення користувачів, доступ до файлів, спроби автентифікації, помилки системи та інші події. Ці дані є надзвичайно важливими для виявлення аномальної активності та можливих атак. Наприклад, якщо в логах з’являються спроби входу з підозрілих IP-адрес або великий потік помилкових спроб авторизації, це може свідчити про атаку перебором паролів (Brute Force).

Сучасні організації використовують SIEM-системи (Security Information and Event Management) для автоматизованого аналізу логів та виявлення загроз. SIEM об’єднує інформацію з брандмауерів, антивірусних програм, серверів, баз даних та хмарних сервісів, аналізує її в режимі реального часу та генерує сповіщення про можливі інциденти. Це дає змогу значно прискорити виявлення атак та автоматизувати реагування на них.

Ще одним важливим компонентом безпеки є перевірка вразливостей (Vulnerability Scanning). Системи пошуку вразливостей регулярно аналізують мережеві пристрої, сервери та додатки на предмет відкритих портів, небезпечних налаштувань або застарілого програмного забезпечення. Найпоширенішими інструментами для автоматизованого сканування є Nessus, OpenVAS, Qualys. Вони дають можливість знаходити відомі уразливості, які можуть бути використані хакерами для злому систем.

Однак автоматичне сканування вразливостей не завжди дає змогу виявити складні загрози, такі як логічні помилки в програмному забезпеченні або неправильно налаштовані механізми автентифікації. Саме тому компанії проводять тестування на проникнення (Penetration Testing), у ході якого експерти з безпеки імітують атаки з боку хакерів, щоб перевірити реальний рівень захисту мережі.

Пентестинг може бути **білим, сірим або чорним**:

- *Білий (White Box Penetration Testing)* – тестери отримують повну інформацію про систему, включаючи схеми мережі, налаштування серверів та паролі адміністратора. Це дає змогу максимально точно оцінити слабкі місця.
- *Сірий (Gray Box Testing)* – фахівці мають лише частковий доступ до системи, що наближує тестування до реальних умов, коли хакер має певні обмеження, але може використовувати викрадені облікові записи.
- *Чорний (Black Box Testing)* – тестування виконується без жодної інформації про систему, фахівці намагаються отримати доступ так само, як справжній зловмисник.

В останні роки **етичне хакерство (Ethical Hacking)** стало одним із головних інструментів підвищення рівня безпеки організацій. Багато компаній запрошують **білих хакерів**, які мають легальний доступ до систем та перевіряють їх на вразливості. Такий підхід дає змогу виявити потенційні загрози ще до того, як ними скористаються справжні злочинці.

Окрім технічних методів моніторингу та тестування, важливим аспектом є перевірка політик безпеки та відповідності стандартам (Compliance Auditing). Багато галузей мають обов'язкові вимоги щодо безпеки, такі як ISO 27001, GDPR, NIST, HIPAA, і організації повинні доводити, що їхня IT-інфраструктура відповідає цим нормам.

Останнім важливим компонентом є моніторинг поведінки користувачів (UBA – User Behavior Analytics). Багато атак відбуваються через компрометацію облікових записів, тому аналіз дій користувачів дає змогу виявити підозрілу активність. Наприклад, якщо працівник ніколи не підключався до корпоративної мережі з-за кордону, але раптово система реєструє вхід з іншої країни – це може свідчити про викрадення облікових даних.

Комплексний підхід до аудиту та моніторингу безпеки передбачає:

- Автоматизоване логування та аналіз трафіку.
- Використання SIEM-систем для виявлення загроз.
- Періодичне сканування на вразливості та тестування на проникнення.
- Перевірку відповідності безпековим стандартам.
- Моніторинг активності користувачів та поведінковий аналіз.

Усе це дає змогу не лише виявляти загрози в режимі реального часу, а й запобігати атакам на ранніх стадіях, що є ключовим фактором ефективного захисту сучасних мережевих інфраструктур.

З розвитком інформаційних технологій змінюються не лише методи атак, але й підходи до захисту. Сучасні тенденції у сфері кібербезпеки орієнтовані на автоматизацію процесів, використання штучного інтелекту, біометричну автентифікацію та новітні криптографічні алгоритми. Захист мереж більше не є

статичною системою – тепер це динамічна екосистема, яка навчається, аналізує поведінку користувачів, адаптується до загроз та реагує у реальному часі.

Однією з найважливіших тенденцій є використання штучного інтелекту (AI) у кібербезпеці. Традиційні системи безпеки, такі як антивірусні програми, IDS/IPS та SIEM, уже не можуть впоратися з величезною кількістю загроз, що постійно змінюються. Сучасні атаки використовують методи обходу традиційних сигнатурних систем, а отже, виявлення лише на основі бази відомих загроз більше не є ефективним. AI може аналізувати великі обсяги даних, виявляти аномалії у поведінці користувачів, прогнозувати атаки та автоматично реагувати на загрози. Наприклад, якщо алгоритм помічає аномальну активність, таку як різке збільшення вихідного трафіку з робочої станції, це може свідчити про витік даних або активність програми-вимагача (Ransomware). AI може автоматично блокувати підозріле з'єднання та сповістити адміністратора.

Ще одним трендом є біометрична автентифікація, яка поступово витісняє традиційні паролі. Паролі є найслабшою ланкою безпеки, оскільки користувачі часто використовують легкі для запам’ятовування комбінації, повторно застосовують одні й ті самі паролі або зберігають їх у незахищених файлах. Біометрична автентифікація дає змогу замінити паролі на сканування відбитків пальців, розпізнавання обличчя, аналіз голосу або навіть унікальні особливості друкування на клавіатурі.

Популярність набирає Zero Trust Architecture (ZTA) – концепція, яка передбачає, що жодному пристрою або користувачеві не можна довіряти за замовчуванням. У традиційних корпоративних мережах передбачалося, що всі пристрої, підключені до внутрішньої мережі, є безпечними. Однак сучасні атаки, такі як фішинг, викрадення облікових даних та атаки на віддалені VPN-з’єднання, показали, що навіть всередині мережі можуть знаходитися зловмисники. У рамках Zero Trust кожен запит на доступ до ресурсів вимагає верифікації користувача, пристрою та рівня довіри.

Ще одним проривним напрямком є квантова криптографія, яка дає змогу створювати абсолютно безпечні канали зв’язку. Класичні алгоритми

шифрування, такі як RSA, ECC та AES, можуть стати уразливими через розвиток квантових комп'ютерів, які здатні розшифровувати навіть найскладніші криптографічні ключі у рази швидше, ніж традиційні суперкомп'ютери. Для захисту даних розробляються квантові алгоритми шифрування (Quantum Key Distribution, QKD), які базуються на фізичних принципах квантової механіки та не можуть бути перехоплені без зміни самого сигналу.

Ще одним важливим напрямком розвитку є автоматизація реагування на інциденти (SOAR – Security Orchestration, Automation, and Response). Якщо раніше реагування на загрози потребувало залучення IT-спеціалістів, то тепер цей процес можна автоматизувати, що дає змогу зменшити час реакції на загрози з годин або днів до секунд. Наприклад, якщо SIEM-система виявляє спробу несанкціонованого входу, то SOAR може автоматично блокувати обліковий запис, відключити підозрілий пристрій від мережі та надіслати адміністратору детальний звіт.

Розвиток хмарних технологій також змінює підхід до безпеки. Багато компаній переходять на мультихмарні середовища (Multi-Cloud), що поєднують Amazon Web Services (AWS), Microsoft Azure, Google Cloud, що дає змогу зменшити залежність від одного провайдера, але створює нові виклики щодо безпеки та управління доступом. Використання шифрування, розподілених політик доступу та багатофакторної автентифікації (MFA) є критично важливими для зменшення ризиків у хмарних середовищах.

Одним із найбільших викликів у сфері кібербезпеки є використання атак на основі штучного інтелекту. Зловмисники вже розробляють AI-боти, які можуть автоматично знаходити вразливості, генерувати фішингові повідомлення, обходити традиційні засоби захисту та навіть маскувати шкідливий код. Це означає, що компаніям доведеться використовувати AI для захисту від AI-атак, що призведе до справжньої «гонки озброєнь» у сфері кібербезпеки.

Підсумовуючи, сучасна безпека мереж переходить від статичних моделей до динамічних та самонавчальних систем, що можуть автоматично адаптуватися

до загроз. Компанії, які використовують AI-аналіз, біометрію, Zero Trust, квантове шифрування та автоматизацію реагування на інциденти, отримують значну перевагу у сфері захисту даних. Однак разом із розвитком технологій збільшуються і виклики, тому майбутнє безпеки буде визначатися здатністю компаній впроваджувати інновації швидше, ніж їх можуть використовувати кіберзлочинці.

Сучасний світ цифрових технологій потребує не лише гнучких і швидкодіючих систем зв'язку, але й ефективних механізмів захисту мережевої інфраструктури. Кібербезпека перетворилася на одну з головних сфер протистояння між бізнесом, державними установами та кіберзлочинцями. З кожним днем зростає кількість атак, спрямованих на крадіжку даних, порушення безперервності бізнес-процесів та злом критично важливих систем. Атаки стають складнішими, їх важче виявити, а методи захисту потребують постійного оновлення та адаптації.

Сьогоднішні загрози мережевої безпеки включають не лише класичні методи атак, такі як DDoS, перехоплення трафіку, фішингові кампанії чи експлуатація вразливостей у ПЗ, а й інтелектуальні атаки, керовані штучним інтелектом. Використання AI у злочинній діяльності дає змогу зловмисникам автоматизувати пошук слабких місць у мережах, обходити традиційні засоби захисту та навіть проводити соціальні атаки, такі як deepfake-маніпуляції для отримання конфіденційних даних.

Сучасна кібербезпека не може бути побудована лише на окремих інструментах захисту. Використання брандмауерів, VPN, систем IDS/IPS, шифрування та антивірусних програм є необхідним, але цього більше не достатньо. Новітні підходи базуються на комплексному багаторівневому захисті, аналізі поведінки користувачів, динамічному виявленні загроз та автоматизації реагування на інциденти. Особливу роль відіграє Zero Trust Architecture, що передбачає відсутність довіри до будь-яких пристроїв або користувачів за замовчуванням.

Основні заходи для захисту мереж

- *Шифрування даних (AES, RSA, TLS)* – захист інформації від перехоплення.
- *Брандмауери та IDS/IPS* – виявлення та запобігання вторгненням.
- *Двофакторна автентифікація (2FA)* – захист користувацьких акаунтів.
- *Сканування на вразливості та тестування безпеки* – виявлення слабких місць у мережі.
- *Зонування мережі та контроль доступу* – ізоляція критично важливих ресурсів.

Виклики та перспективи розвитку безпеки

- *Зростання кількості атак* – кіберзлочинці використовують складні багатовекторні атаки.
- *Перехід до квантової криптографії* – класичні алгоритми можуть стати вразливими.
- *Безпека IoT* – величезна кількість підключених пристроїв створює нові загрози.
- *Адаптація до Zero Trust* – традиційні моделі безпеки більше не ефективні.

Рис 7.4 Графік зростання кіберзагроз та витрат на безпеку.

Захист мережі – це не одноразовий процес, а постійний цикл оновлення та вдосконалення. Поєднання технологічних рішень, моніторингу та політик безпеки дає змогу мінімізувати ризики атак та забезпечити стабільну роботу систем.

Сучасні організації переходять до автоматизованих, самонавчальних систем кібербезпеки, що допомагають виявляти загрози в реальному часі. У найближчому майбутньому штучний інтелект, квантова криптографія та Zero Trust стануть основними стандартами безпеки.

Технології кібербезпеки постійно розвиваються, і ключові тенденції на найближчі роки включають:

- *Перехід до квантової криптографії* – забезпечення захисту від атак квантових комп'ютерів.
- *Розвиток біометричної автентифікації* – заміна паролів на біометричні дані та фізичні токени.
- *AI-аналіз загроз* – штучний інтелект, що передбачає атаки на основі аналізу великих обсягів даних.
- *Захист мультихмарних середовищ* – нові механізми безпеки для роботи з AWS, Azure, Google Cloud.
- *Глибока інтеграція Zero Trust* – повний перехід на безперервний моніторинг та перевірку кожного підключення.

З розвитком цифрового світу кіберзагрози будуть тільки ускладнюватися. Успішні компанії та державні установи мають розглядати мережеву безпеку як стратегічний напрямок, що вимагає постійного оновлення засобів захисту, навчання персоналу та адаптації до нових загроз. Головна мета – не лише захищати дані та ресурси, а й створювати екосистему безпеки, яка здатна працювати у режимі реального часу та запобігати атакам ще до їх реалізації.

У сучасних умовах головною перевагою є гнучкість, автоматизація та інтелектуальна аналітика, що дає змогу реагувати на атаки ще до того, як вони завдадуть шкоди. Впровадження інноваційних методів безпеки, інтеграція AI у

аналіз загроз та новітні алгоритми шифрування – це ключ до стійкості та стабільності будь-якої цифрової інфраструктури.

Кібербезпека у XXI столітті – це не просто набір технологій, а динамічний процес, що вимагає постійного оновлення, гнучкості та адаптації до нових загроз. Виживання та успіх організацій залежить від того, наскільки швидко вони можуть інтегрувати сучасні методи захисту, реагувати на кіберінциденти та передбачати майбутні атаки.

Лекції 8: Інтеграція технологій і сучасні виклики

Інтеграція різних мережевих технологій стає ключовим аспектом розвитку сучасної IT-інфраструктури. Сьогодні організації та постачальники послуг стикаються з викликами, пов’язаними з поєднанням традиційних локальних мереж, мобільних технологій, хмарних рішень та Інтернету речей (IoT). Усе це вимагає високого рівня адаптивності, ефективного управління ресурсами та забезпечення безпеки в розподілених середовищах.

Сучасні мережі об'єднують дротові та бездротові інфраструктури, підтримують мобільні підключення та інтегруються з хмарними сервісами. Розвиток **програмно-визначених мереж (SDN), хмарних обчислень, 5G та штучного інтелекту** змінює підхід до управління IT-інфраструктурою. Глобалізація процесів та зростання цифрової трансформації також впливають на методи взаємодії між компаніями, користувачами та пристроями.

Важливим фактором інтеграції є підтримка високої продуктивності, доступності та кібербезпеки. Оскільки кількість підключених пристроїв стрімко зростає, адміністрування таких середовищ стає все складнішим. Додатково ускладнюється захист даних, оскільки різні платформи та технології можуть мати вразливості, які стають точками входу для атак.

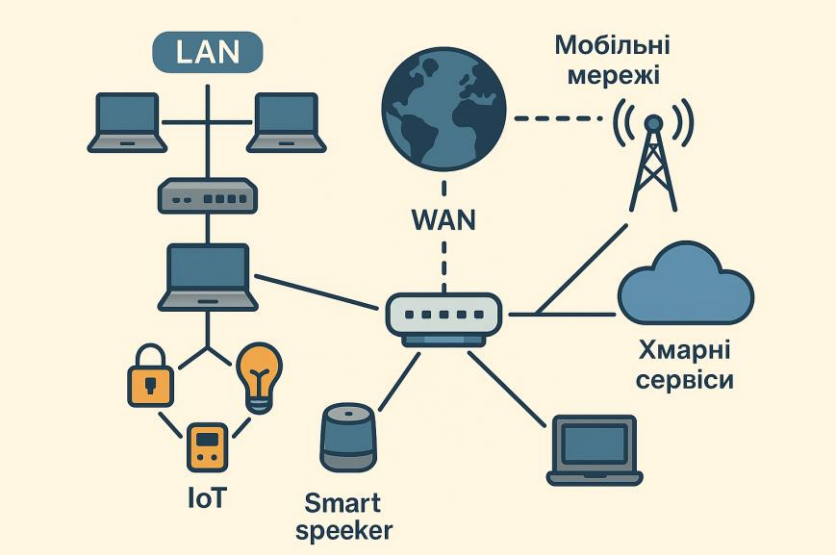


Рис 8.1 Схема інтеграції сучасних мережевих технологій, що включає LAN, WAN, мобільні мережі, IoT та хмарні сервіси

Розвиток технологій також створює нові виклики – обробка великих обсягів даних, підтримка стабільності мережі, боротьба з кіберзагрозами та розширення можливостей для масштабованості. Використання автоматизованих систем управління, штучного інтелекту та блокчейн-рішень дає змогу значно підвищити ефективність взаємодії між різними компонентами мережі.

Сучасна мережева інфраструктура більше не обмежується лише дротовими або бездротовими рішеннями. Різні типи мереж – **LAN, WAN, мобільні мережі (4G, 5G), IoT-інфраструктури та хмарні сервіси** – працюють у взаємодії, забезпечуючи безперервний зв'язок та ефективну передачу даних. Це явище отримало назву **конвергенції мереж**. Його головна мета – інтеграція різних технологій, що дає змогу забезпечити **гнучкість, продуктивність та адаптивність** мережевої інфраструктури.

Дротові мережі, такі як **Ethernet**, традиційно використовуються в локальних інфраструктурах, оскільки вони забезпечують **високу швидкість, низькі затримки та надійність** з'єднання. Проте для мобільних та динамічних середовищ більш зручними є **бездротові та мобільні мережі**. Wi-Fi забезпечує локальну бездротову доступність, а **5G та LTE** стають основними технологіями для підключення пристроїв у віддалених регіонах та промислових об'єктах.

Інтеграція мобільних мереж із Wi-Fi дає змогу реалізувати безперервне перемикання між з'єднаннями. Наприклад, сучасні смартфони можуть автоматично перемикатися між **Wi-Fi та 5G-з'єднанням**, забезпечуючи безперебійний Інтернет-доступ без втрати якості зв'язку. Це особливо важливо для **автономних транспортних систем, хмарних додатків та індустрії потокового відео**.

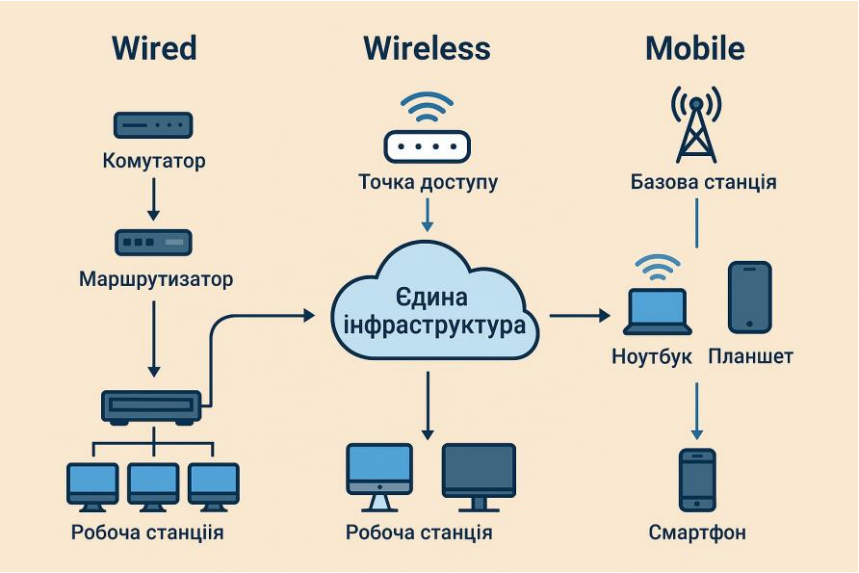


Рис 8.2 Схема інтеграції дротових, бездротових і мобільних мереж у єдину інфраструктуру

Один із важливих аспектів конвергенції – **віртуалізація мережевих функцій (NFV) та програмно-визначені мережі (SDN)**. NFV дає змогу розгортати мережеві сервіси без фізичного обладнання, що значно спрощує керування мережею. SDN, зі свого боку, надає централізований контроль над маршрутизацією трафіку, що підвищує продуктивність та знижує операційні витрати.

Також конвергенція мереж відіграє ключову роль в **індустрії IoT**. Оскільки мільярди пристроїв потребують ефективного підключення, поєднання **Wi-Fi, 5G, LPWAN (Low Power Wide Area Network) та супутникового зв'язку** дає змогу досягти високої масштабованості та мінімізувати затримки передачі даних.

Конвергенція мереж дає змогу об'єднувати дротові, бездротові та мобільні рішення для створення адаптивної інфраструктури. Вона покращує гнучкість, продуктивність та масштабованість мереж, що критично важливо для інноваційних галузей, таких як розумні міста, автономний транспорт та Інтернет речей.

Із розвитком і взаємопроникненням різних мережевих технологій питання кібербезпеки набувають ще більшої актуальності. Інтеграція локальних,

глобальних, мобільних та хмарних мереж створює нові вразливості, що можуть бути використані зловмисниками для атак на критично важливу інфраструктуру.

Основні виклики безпеки в інтегрованих мережах включають захист конфіденційних даних, управління доступом, виявлення загроз та запобігання атакам. Велика кількість взаємопов'язаних технологій означає, що одна вразливість у слабкій ланці може призвести до компрометації всієї інфраструктури.

Зростання популярності хмарних сервісів та гібридних мереж дає змогу компаніям покращувати продуктивність, однак водночас створює нові ризики:

- *Незахищені API та недостатня ізоляція ресурсів* – атаки на хмарні сервіси часто пов'язані з неправильною конфігурацією або використанням застарілих API.
- *Розподілена мережа без єдиного захисту* – гібридні інфраструктури складаються з локальних серверів, віртуальних машин та хмарних платформ, що ускладнює управління безпекою.
- *Атаки на хмарне середовище (Cloud Hijacking)* – зловмисники можуть отримати контроль над акаунтами адміністраторів хмарної платформи та завдати значних збитків.

Інтернет речей (IoT) – одна з найбільш вразливих технологій, оскільки більшість пристроїв мають слабкі механізми захисту, відкриті порти та незашифрований трафік. Основні виклики:

- *Масштаб атак на IoT* – хакери можуть використовувати великі ботнети (наприклад, Mirai) для атак на сервіси.
- *Відсутність оновлень* – багато IoT-пристроїв працюють на застарілих прошивках, що містять відомі вразливості.
- *Перехоплення трафіку* – відкриті IoT-пристрої можуть використовувати незахищені протоколи, такі як HTTP, що дає змогу легко викрадати передані дані.

Оскільки класичні моделі безпеки, що базуються на периметральному захисті, більше не є ефективними, компанії переходять до **Zero Trust**

Architecture (ZTA), яка передбачає, що жодному підключенню не можна довіряти за замовчуванням.

Основні принципи Zero Trust:

- *Мінімізація довіри* – кожен пристрій та користувач проходить автентифікацію перед доступом до ресурсів.
- *Контроль доступу на основі поведінкового аналізу* – навіть після автентифікації система може блокувати підозрілу активність.
- *Сегментація мережі* – ізоляція ресурсів для запобігання розповсюдженню атак.
- *Багатофакторна автентифікація (MFA)* – перевірка особи за кількома факторами перед наданням доступу.

Зростання обчислювальних потужностей, розвиток технологій зберігання та потреба у масштабованих рішеннях сприяли стрімкому поширенню хмарних технологій. Сучасні компанії все частіше інтегрують локальні мережі з хмарною інфраструктурою, що дає змогу ефективно розподіляти ресурси, зменшувати витрати на обслуговування серверів та забезпечувати безперервний доступ до корпоративних даних.

Хмарні технології можуть використовуватися для зберігання даних, обробки великих масивів інформації, резервного копіювання, управління мережею та організації безпечного віддаленого доступу. Такі рішення як AWS, Microsoft Azure, Google Cloud надають платформу для організації хмарних сервісів, що дає змогу компаніям значно знизити навантаження на локальну IT-інфраструктуру.

Хмарні рішення дають можливість компаніям зберігати та обробляти дані без необхідності розгортання фізичних серверів. Основні моделі хмарних сервісів:

- *IaaS (Infrastructure as a Service)* – оренда віртуальних серверів, сховищ та мережевої інфраструктури (наприклад, AWS EC2, Google Compute Engine).
- *PaaS (Platform as a Service)* – готові середовища для розробки та запуску додатків (наприклад, Azure App Services, Google App Engine).

- *SaaS (Software as a Service)* – використання програмного забезпечення без локального розгортання (наприклад, Google Workspace, Microsoft 365).

Багато компаній використовують **гібридні рішення**, поєднуючи локальні сервери та хмарні сервіси для підвищення ефективності мережевої інфраструктури. Основні підходи до інтеграції:

- *Hybrid Cloud* – комбінація локальних серверів і хмарних обчислень.
- *Multi-Cloud* – використання кількох хмарних провайдерів одночасно (AWS + Azure + Google Cloud).
- *Приватні хмари* – організація власної хмарної інфраструктури для підвищеної безпеки та контролю.

Переваги та виклики гібридних хмарних рішень

- *Гнучкість та масштабованість* – компанії можуть адаптувати ресурси до своїх потреб.
- *Зниження витрат* – немає необхідності купувати й обслуговувати фізичні сервери.
- *Відмовостійкість* – хмарні платформи підтримують резервне копіювання та балансування навантаження.

Безпека – ризик витоку даних через ненадійне шифрування або уразливості API.

Залежність від провайдера – при зміні провайдера може виникнути складність у міграції сервісів.

Регулювання та відповідність – збереження чутливих даних у хмарі може суперечити законодавчим нормам.

Інтеграція хмарних сервісів у мережеву інфраструктуру забезпечує гнучкість, продуктивність і масштабованість мережевих рішень. Використання гібридних та мультихмарних підходів дає змогу компаніям зменшити витрати, покращити безпеку та підвищити відмовостійкість систем.

Інтернет речей (IoT, Internet of Things) – це технологія, що об'єднує мільярди пристроїв у єдину мережу, дозволяючи їм збирати, обробляти та обмінюватися даними без участі людини. Сучасні IoT-рішення використовуються у розумних

містах, промислових системах, транспорті, медицині, сільському господарстві та багатьох інших сферах.

Із ростом кількості IoT-пристроїв виникає потреба у ефективній мережевій інфраструктурі, яка здатна підтримувати підключення мільйонів об'єктів одночасно. Це створює нові виклики для пропускної здатності мереж, безпеки, масштабованості та обробки даних.

IoT-мережі часто працюють із великими обсягами даних та вимагають низької затримки для забезпечення ефективної взаємодії між пристроями. Основні виклики:

- *Перевантаження мережі* – мільярди сенсорів і пристроїв створюють постійний трафік, що може спричинити затримки та втрати пакетів.
- *Обмеження обчислювальних потужностей* – багато IoT-пристроїв мають **низьку продуктивність** та працюють на обмежених ресурсах.
- *Високі вимоги до енергоспоживання* – для автономних пристроїв важливо мінімізувати споживання енергії.

Штучний інтелект та машинне навчання дають можливість автоматизувати управління IoT-мережами, підвищуючи їхню продуктивність та безпеку.

- *AI-оптимізація трафіку* – динамічне балансування навантаження між IoT-пристроями.
- *Передбачення збоїв та несправностей* – алгоритми аналізують дані та прогнозують відмови обладнання.
- *Самонавчальні системи кібербезпеки* – AI може виявляти аномалії та запобігати атакам на IoT.

Безпека IoT є одним із найважливіших викликів, оскільки велика кількість підключених пристроїв створює нові точки входу для хакерських атак.

- *Шифрування трафіку* – використання TLS, AES-256 для захисту даних.
- *Ідентифікація пристроїв* – автентифікація через сертифікати та біометричні механізми.
- *Моніторинг активності* – SIEM-системи аналізують підозрілу активність у мережі.

IoT-мережі змінюють підхід до роботи з даними та мережею. Їхній стрімкий розвиток створює виклики для масштабованості, безпеки та продуктивності, однак використання AI, хмарних сервісів та вдосконалених алгоритмів управління дає змогу оптимізувати роботу таких мереж.

Штучний інтелект (AI) та машинне навчання (ML) відіграють ключову роль у автоматизації управління мережами, підвищуючи ефективність адміністрування, безпеку та продуктивність. Зі зростанням складності мережевих інфраструктур, інтеграція AI дає змогу зменшити залежність від ручного управління та поліпшити моніторинг, виявлення загроз та оптимізацію трафіку.

AI-технології дають можливість прогнозувати мережеві збої, автоматично реагувати на інциденти та забезпечувати динамічну маршрутизацію трафіку у залежності від завантаження мережі. Використання штучного інтелекту у SD-WAN, IoT, кібербезпеці та хмарних сервісах значно покращує адаптивність та стабільність мереж.

Однією з головних переваг AI у мережевих технологіях є автоматизоване виявлення загроз.

- *Системи аналізу поведінки трафіку (UBA, User Behavior Analytics)* – AI виявляє аномальні дії у мережі, такі як раптове збільшення трафіку або підозрілі підключення.
- *Автоматизовані рішення SIEM (Security Information and Event Management)* – AI аналізує журнали безпеки у режимі реального часу та попереджає про потенційні атаки.
- *AI-оптимізація маршрутизації* – розумні алгоритми автоматично вибирають найшвидший маршрут для передачі даних, мінімізуючи затримки.

AI дає змогу зменшити потребу у ручному налаштуванні мережі та підвищує її ефективність завдяки:

- *Автоматичному виявленню перевантажень* – система моніторить трафік і змінює пріоритети QoS (Quality of Service) у реальному часі.

- *Прогнозуванню несправностей* – алгоритми AI аналізують історію роботи мережі та передбачають можливі збої, дозволяючи запобігати інцидентам.
- *Адаптивному розподілу навантаження* – динамічне балансування трафіку між доступними каналами для забезпечення найкращої продуктивності.

AI суттєво покращує ефективність *SD-WAN (Software-Defined WAN),* дозволяючи компаніям:

- *Автоматично визначати найкращі маршрути для трафіку*.
- *Пріоритизувати критичні сервіси* (наприклад, відеоконференції, корпоративні додатки).
- *Оптимізувати використання ресурсів провайдерів,* комбінуючи MPLS, 5G та VPN.

Це дає змогу мінімізувати затримки та зменшити витрати на мережеву інфраструктуру.

Штучний інтелект змінює підхід до управління мережами, дозволяючи автоматизувати процеси моніторингу, аналізу трафіку, оптимізації продуктивності та підвищення безпеки. AI-алгоритми поліпшують роботу SD-WAN, IoT та кібербезпеки, роблячи сучасні мережі більш адаптивними та безперервними.

Інтеграція хмарних технологій, IoT, мобільних мереж і SD-WAN створює нові виклики для кібербезпеки, оскільки розширюється кількість точок входу для атак. Сучасні мережі більше не обмежуються фізичними межами офісів або центрів обробки даних – вони включають віддалених користувачів, підключені пристрої та хмарні сервіси, що підвищує рівень ризиків.

Кіберзлочинці використовують автоматизовані атаки, штучний інтелект і складніші методи обходу захисних механізмів. Основні виклики для безпеки сучасних мереж включають захист критичних інфраструктур, протидію DDoS-атакам, забезпечення безпеки IoT та використання нових криптографічних методів.

Критичні інфраструктури (енергетика, транспорт, фінанси, медицина) стають головною ціллю для кібератак, оскільки їхня компрометація може мати катастрофічні наслідки. Основні типи атак:

- *Ransomware-атаки* – шифрування файлів з вимогою викупу (наприклад, атака на Colonial Pipeline у США).
- *DDoS-атаки* – масовані атаки на сервери, що блокують доступ до онлайн-сервісів.
- *Supply Chain Attacks* – атаки на постачальників програмного забезпечення для проникнення у корпоративні мережі.

Сучасні методи шифрування можуть стати вразливими у майбутньому через розвиток **квантових комп'ютерів**, які здатні швидко зламувати класичні криптографічні алгоритми (RSA, ECC).

- *Квантова криптографія (QKD – Quantum Key Distribution)* – дає змогу створювати абсолютно захищені канали зв'язку.
- *Алгоритми постквантової криптографії* – розробка нових методів шифрування, стійких до атак квантових комп'ютерів.

Гібридні та мультихмарні середовища потребують особливих підходів до безпеки через:

- *Ризик витоку даних* – через ненадійні API або неправильні налаштування хмарних сервісів.
- *Складність моніторингу загроз* – розподілені системи можуть ускладнювати виявлення атак.
- *Взаємодію між приватними та публічними хмарами* – необхідність шифрування та контролю доступу.

Захист сучасних мереж потребує комплексного підходу, який включає AI-моніторинг загроз, квантову криптографію, нові методи автентифікації та хмарні технології. Безперервний розвиток технологій змушує компанії адаптувати свої стратегії кібербезпеки та впроваджувати автоматизовані системи захисту.

Сучасні мережі швидко розвиваються, адаптуючись до зростаючих обсягів даних, нових технологічних стандартів та кібербезпекових викликів. У

найближчі роки ключові зміни торкнуться мобільного зв'язку (6G), супутникового Інтернету, блокчейн-мереж та інтеграції AI для автоматизації процесів керування мережею.

Технологія **6G**, очікувана після 2030 року, обіцяє значні покращення у сфері зв'язку:

- *Передача даних на швидкостях понад 1 Тбіт/с* – це в 100 разів більше, ніж можливості 5G.
- *Терагерцовий діапазон (THz Band)* – використання нових частот для мінімізації перевантаження мереж.
- *Інтеграція AI у мережу* – автоматизоване управління, прогнозування збоїв та балансування навантаження.

Переваги: мінімальна затримка, підтримка IoT нового покоління, повна автономія мереж.

Недоліки: потреба у новій фізичній інфраструктурі та високі витрати на впровадження.

Супутниковий Інтернет розширює можливості підключення там, де наземні мережі не можуть забезпечити покриття. Основні проєкти:

- *Starlink (SpaceX)* – глобальний доступ через низькоорбітальні супутники.
- *OneWeb, Amazon Kuiper* – альтернативні рішення для швидкісного Інтернету.
- *Інтеграція супутникового та 5G-зв'язку* – для безперебійного покриття віддалених регіонів.

Переваги: глобальне покриття, альтернатива наземним мережам.

Недоліки: висока вартість обладнання, можливі затримки в передачі даних.

Блокчейн може використовуватися для:

- *Безпечного зберігання логів мережевого трафіку* – унеможливлює підробку даних.
- *Автоматизованого управління доступом* – заміна традиційних паролів на блокчейн-ідентифікацію.
- *Децентралізованого DNS* – захист від атак на доменні системи.

Переваги: прозорість, неможливість фальсифікації даних.

Недоліки: обмежена масштабованість, високі обчислювальні витрати.

Майбутнє мережевих технологій пов'язане з 6G, супутниковими системами, блокчейном і автоматизованими AI-рішеннями. Це дозволить мінімізувати затримки, підвищити швидкість передачі даних та покращити безпеку.

Сучасні мережеві технології розвиваються надзвичайно швидко, інтегруючи хмарні обчислення, мобільні мережі, IoT, штучний інтелект та квантову криптографію. Ця інтеграція відкриває нові можливості для автоматизації, гнучкості та масштабованості, але водночас створює нові виклики у сфері кібербезпеки, управління трафіком та надійності з'єднань.

Основні висновки щодо інтеграції мережевих технологій

- *Об'єднання дротових, бездротових та мобільних мереж* дає змогу створювати безперервні, адаптивні інфраструктури.
- *Хмарні технології стали ключовим компонентом сучасних мереж,* забезпечуючи гнучкість, відмовостійкість та розподіл обчислювальних потужностей.
- *Інтернет речей (IoT)* змінює підхід до побудови мереж, створюючи нові виклики для масштабованості та безпеки.
- *Штучний інтелект дає змогу автоматизувати управління мережами*, забезпечуючи оптимізацію продуктивності та захист від атак.
- *Кібербезпека у розподілених системах* стає все складнішою, вимагаючи впровадження Zero Trust, квантової криптографії та блокчейн-захисту.
- ***Перспективи 6G, супутникового Інтернету та блокчейну*** формують основу майбутніх технологій передачі даних.

Основні переваги інтеграції мережевих технологій

- *Підвищена масштабованість та гнучкість* – мережі легко адаптуються до змін навантаження.
- *Автоматизація та AI-контроль* – мінімізує потребу у ручному адмініструванні.

- *Зниження витрат через хмарні обчислення та SD-WAN.*
- *Посилена безпека завдяки новим методам ідентифікації та шифрування.*

Виклики інтеграції технологій

- Висока **с**кладність управління розподіленими мережами.
- Зростаюча кількість атак на IoT та хмарні сервіси.
- Виклики квантової криптографії та необхідність адаптації до постквантової безпеки.

Майбутнє мережевих технологій – це інтелектуальні, автоматизовані, безпечні та глобальні системи зв'язку, які поєднують IoT, 5G/6G, AI, хмарні обчислення та квантову криптографію. Організації повинні адаптувати свої мережі до нових реалій, використовуючи динамічні, гнучкі рішення, що забезпечують продуктивність та безпеку.

Питання для самоконтролю

1. Що таке комп'ютерна мережа?
2. Які існують типи комп'ютерних мереж за охопленням?
3. Що таке локальна мережа (LAN)?
4. Що таке глобальна мережа (WAN)?
5. У чому різниця між MAN та WAN?
6. Що таке топологія мережі?
7. Які основні види топологій мереж?
8. У чому переваги топології "зірка"?
9. Які недоліки має шинна топологія?
10. Чому топологія "кільце" рідко використовується?
11. Що таке модель OSI?
12. Які рівні включає модель OSI?
13. За що відповідає фізичний рівень OSI?
14. Які основні функції канального рівня?
15. Що таке MAC-адреса і де вона використовується?
16. Які функції виконує мережевий рівень?
17. Що таке IP-адреса?
18. Які відмінності між IPv4 та IPv6?
19. Що таке підмережа?
20. Як визначається маска підмережі?
21. Яка функція транспортного рівня?
22. У чому різниця між TCP та UDP?
23. Що таке сесійний рівень?
24. Що відбувається на рівні представлення?
25. Яка роль прикладного рівня?
26. Чим модель TCP/IP відрізняється від OSI?
27. Які рівні включає модель TCP/IP?
28. Що таке порти у TCP/IP?
29. Які порти використовуються для HTTP та HTTPS?
30. Що таке NAT і для чого він потрібен?
31. Які основні види мережевих кабелів?
32. Що таке кручена пара (UTP, STP)?
33. У чому різниця між одномодовим і багатомодовим оптичним кабелем?
34. Які основні характеристики коаксіального кабелю?
35. Що таке частотний діапазон у бездротових мережах?
36. Які частоти використовуються у Wi-Fi?

37. Що таке дуплексний режим передачі?
38. Що таке термінатор у коаксіальних мережах?
39. Які основні засоби передачі даних у мережах?
40. Чим відрізняються аналоговий і цифровий сигнали?
41. Що таке Ethernet?
42. Які основні стандарти Ethernet?
43. Що таке MAC-адреса?
44. Яка структура MAC-адреси?
45. Що таке колізії в Ethernet?
46. Як працює метод доступу CSMA/CD?
47. Що таке VLAN?
48. Як VLAN допомагає у сегментації мережі?
49. Яка різниця між комутатором і концентратором?
50. Що таке фрейм Ethernet?
51. Як працює маршрутизація в IP-мережах?
52. Які існують типи маршрутизації?
53. Що таке статична маршрутизація?
54. Як працює динамічна маршрутизація?
55. Які основні протоколи маршрутизації?
56. Що таке ARP?
57. Як працює ARP-запит?
58. Що таке DHCP?
59. Яка роль ICMP у мережах?
60. Що таке VPN і для чого він використовується?
61. Які функції має TCP?
62. Як працює механізм трьохетапного встановлення з'єднання у TCP?
63. Що таке вікно TCP?
64. Як працює контроль потоку у TCP?
65. Які особливості UDP?
66. У яких випадках UDP кращий за TCP?
67. Що таке номер порту?
68. Які порти є зарезервованими?
69. Як працює механізм повторної передачі в TCP?
70. Що таке MTU та як він впливає на передачу даних?
71. Які функції виконує DNS?
72. Як працює DNS-запит?
73. Що таке HTTP?
74. Яка різниця між HTTP і HTTPS?
75. Що таке FTP?

76. Які основні команди FTP?
77. Що таке SSH і для чого він використовується?
78. Як працює POP3?
79. У чому різниця між POP3 і IMAP?
80. Що таке SNMP?
81. Що таке Wi-Fi?
82. Які основні стандарти Wi-Fi?
83. Що таке точка доступу?
84. Як працює WPA2?
85. Що таке Bluetooth?
86. Які відмінності між 4G і 5G?
87. Як працює мобільний роумінг?
88. Що таке SSID?
89. Як захистити бездротову мережу?
90. Що таке Mesh Wi-Fi?
91. Що таке міжмережевий екран?
92. Як працює брандмауер?
93. Що таке DDoS-атака?
94. Які методи захисту від DDoS?
95. Що таке фішинг?
96. Як працює VPN?
97. Що таке двофакторна аутентифікація?
98. Що таке IDS/IPS?
99. Як працює цифровий сертифікат?
100. Що таке Zero Trust Security?
101. Що таке внутрішньомережеві та зовнішньомережеві протоколи маршрутизації?
102. Як поділяються IP-адреси за класами?
103. Що таке приватні IP-адреси?
104. Які існують зарезервовані IP-адреси?
105. Як розрахувати кількість хостів у підмережі?
106. Як працює розподілена адресація?
107. Що таке адреса призначення broadcast?
108. Як працює IPv6?
109. Чим відрізняється Fast Ethernet від Gigabit Ethernet?
110. Що таке Trunk порт?
111. Що таке оптоволоконний Інтернет?
112. Що таке WEP, WPA, WPA2 і WPA3?
113. Чому WEP вважається небезпечним?

114. Що таке Wi-Fi Mesh-мережі?
115. Що таке хмарні обчислення?
116. Як працюють мережі IoT?
117. Як працює 5G у контексті IoT?
118. Що таке Smart Home?
119. Які перспективи розвитку комп’ютерних мереж у майбутньому?

Бібліографічний список

Основні джерела:

1. Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Комп’ютерні мережі : кн. 1. Тернопіль : ТНТУ, 2020. 256 с.
2. Городецька О. С., Гикавий В. А., Онищук О. В. Комп’ютерні мережі. Вінниця : ВНТУ, 2021. 129 с.
3. Жураковський Б. Ю., Зенів І. О. Комп’ютерні мережі. Ч. 2. Київ : КПІ ім. Ігоря Сікорського, 2020. 372 с.
4. Задерейко О. В., Логінова Н. І., Толокнов А. А. Комп’ютерні мережі. Одеса : ОНУА, 2022. 249 с.
5. Таненбаум Е., Ветерс Е. Комп’ютерні мережі. 6-те вид., переробл. Київ : Діалектика, 2022. 960 с.
6. Курган М. М. Основи побудови комп’ютерних мереж : підручник. Львів : ЛНУ ім. Івана Франка, 2021. 312 с.
7. Мельник Ю. М. Комп’ютерні мережі та захист інформації. Харків : ХНУРЕ, 2023. 288 с.
8. Баранов В. О. Кабельні системи та канали зв’язку : навч. посіб. Київ : КНЕУ, 2020. 240 с.
9. Бойко А. А. Бездротові мережі: основи та технології. Київ : НаУКМА, 2023. 198 с.
10. Пархоменко О. О. Локальні комп’ютерні мережі: сучасний стан і тенденції розвитку. Київ : НТУУ КПІ, 2022. 284 с.

Допоміжні джерела:

11. Левченко М. С. Протоколи комп’ютерних мереж: TCP/IP, UDP, HTTP. Дніпро : ДНУ, 2021. 172 с.
12. Семенюк Т. О. Бездротові технології передачі даних. Вінниця : ВНТУ, 2020. 158 с.
13. Шевченко П. Г. Системи та мережі передачі даних. Харків : ХНУРЕ, 2022. 215 с.
14. Новак Р. В. Основи інформаційної безпеки в мережах. Київ : КНУ ім. Тараса Шевченка, 2023. 190 с.
15. Савчук В. А. Адміністрування комп’ютерних мереж : практикум. Тернопіль : ТНТУ, 2020. 175 с.
16. Кононенко О. М. Wi-Fi та WiMAX: технології доступу до Інтернету. Київ : НАУ, 2021. 148 с.

17. Тимошенко А. П. Технології Ethernet і оптичних мереж. Київ : КНУБА, 2022. 210 с.
18. Глушко О. І. Системи супутникового зв’язку : основи побудови. Київ : ІТ-Університет, 2023. 192 с.
19. Стасюк В. Л. Захищені комп’ютерні мережі : основи побудови. Львів : ЛНУ ім. Івана Франка, 2021. 234 с.
20. Прохоренко Ю. М. Інфраструктура мереж підприємств: принципи та проєктування. Одеса : ОНПУ, 2022. 220 с.

Електронні джерела

21. Kurose J. F., Ross K. W. Computer Networking: A Top-Down Approach [Електронний ресурс]. 8th ed. Pearson, 2021. 864 p. Режим доступу: https://www.pearson.com/en-us/subject-catalog/p/computer-networking-a-top-down-approach/P200000007481 (дата звернення: 05.05.2025).
22. Cisco Networking Academy. Networking Essentials v2.0 [Електронний ресурс]. 2022. Режим доступу: https://www.netacad.com/courses/networking/networking-essentials (дата звернення: 05.05.2025).
23. IEEE Standards Association. IEEE 802.11-2020 - Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications [Електронний ресурс]. 2020. Режим доступу: https://standards.ieee.org/standard/802_11-2020.html (дата звернення: 05.05.2025).
24. Wi-Fi Alliance. Wi-Fi CERTIFIED™ 6 Release 2: Technical Overview [Електронний ресурс]. 2022. Режим доступу: https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-6-release-2 (дата звернення: 05.05.2025).
25. ITU-T Recommendations. G.9960 : Unified high-speed wire-line based home networking transceivers – System architecture and physical layer specification [Електронний ресурс]. 2021. Режим доступу: https://www.itu.int/rec/T-REC-G.9960-202106-I/en (дата звернення: 05.05.2025).

Предметний покажчик

Електронне навчально-методичне видання

Анна Карпин, Дмитро Карпин

КОМП'ЮТЕРНІ МЕРЕЖІ: ТЕКСТИ ЛЕКЦІЙ

Дрогобицький державний педагогічний університет імені Івана Франка

Редактор
Ірина Невмержицька
Технічний редактор
Ірина Артимко

Здано до набору 04.07.2025 р. Формат 60x90/16. Гарнітура Times. Ум. друк. арк. 9,75. Зам. 58.

Дрогобицький державний педагогічний університет імені Івана Франка. (Свідоцтво про внесення суб'єкта видавничої справи до державного реєстру видавців, виготівників та розповсюджувачів видавничої продукції ДК № 5140 від 01.07.2016 р.). 82100, Дрогобич, вул. Івана Франка, 24, к. 203