



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
УКРАЇНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ЗАЛІЗНИЧНОГО ТРАНСПОРТУ

С. Є. Бантюков, І. Г. Бізюк, О. В. Казанко

Серія Комп'ютерні науки
МЕРЕЖЕВІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Навчальний посібник

Частина 1

Харків 2024

УДК 004.9(075)

Б 22

*Рекомендовано вченою радою Українського державного університету
залізничного транспорту як навчальний посібник
(витяг з протоколу № 4 від 21 червня 2023 р.)*

Рецензенти:

професори А. Л. Єрохін (ХНУРЕ, Харків),
І. В. Левикін (ХНУРЕ, Харків),
О. Г. Панченко (Onapsis Inc., Берлін, Німеччина),

Б 22 Бантюков С. Є., Бізюк І. Г., Казанко О. В. Серія Комп'ютерні науки: Мережеві інформаційні технології: Навч. посібник. – Харків: УкрДУЗТ, 2024. – Ч. 1. – 120 с., рис. 32, табл. 2.

ISBN

Навчальний посібник містить загальну інформацію про історію та основні тенденції розвитку сучасних мережевих технологій і безпекові аспекти роботи в мережі.

Навчальний посібник призначений для здобувачів вищої освіти, які вивчають дисципліни «Комп'ютерна техніка і організація обчислювальних робіт», «Комп'ютерна техніка та технології», «Алгоритмізація і програмування», «Обчислювальна техніка та програмування», «Комп'ютерна техніка та програмування», «Інформаційні системи і технології», «Інформатика», усіх факультетів і форм навчання.

УДК 004.9(075)

ISBN

© Бантюков С. Є., Бізюк І. Г., Казанко О. В., 2024.
© Український державний університет
залізничного транспорту, 2024.

ЗМІСТ

ВСТУП	4
РОЗДІЛ 1. ЕВОЛЮЦІЯ КОМП'ЮТЕРНИХ МЕРЕЖ	5
1.1. Тенденції розвитку комп'ютерних мереж	7
1.2. Комп'ютерні та телекомунікаційні мережі	22
1.2.1. Глобальні мережі	25
1.2.2. Локальні мережі	28
1.2.3. Наближення локальних і глобальних мереж	31
1.3. Розвиток комп'ютерної техніки на основі малогабаритних і суперкомп'ютерів	33
1.3.1. Створення малогабаритних персональних комп'ютерів	33
1.3.2. Створення потужних суперкомп'ютерів	43
1.4. Покоління архітектури в парадигмі програмування	47
1.4.1. Векторно-конвеєрні комп'ютери. Історія виникнення	53
1.4.2. Векторно-паралельні комп'ютери	54
1.4.3. Масивно-паралельні комп'ютери з розподіленою пам'яттю	54
1.4.4. Паралельні комп'ютери з загальною пам'яттю	55
1.5. Класифікація обчислювальних систем	63
1.6. Принципи нейронної обробки інформації	70
РОЗДІЛ 2. ЗАГАЛЬНІ ПРИНЦИПИ ПОБУДОВИ МЕРЕЖ.	
ІНФОРМАЦІЙНА БЕЗПЕКА	74
2.1. Найпростіша мережа з двох комп'ютерів	74
2.1.1. Спільне використання ресурсів	74
2.1.2. Мережеві інтерфейси	76
2.2. Мережеве програмне забезпечення	79
2.2.1. Мережеві служби та сервіси	79
2.2.2. Мережева операційна система	83
2.2.3. Мережеві додатки	87
2.3. Інформаційна безпека	88
2.3.1. Основні поняття інформаційної безпеки	88
2.3.2. Правове та законодавче регулювання в Україні	95
2.3.3. Загрози безпеці інформації в мережах	98
2.3.4. Несанкціонований доступ до інформації	103
Контрольні запитання	111
БІБЛІОГРАФІЧНИЙ СПИСОК	112
ДОДАТОК 1	115

ВСТУП

Комп'ютерні мережі відіграють важливу роль у сучасному світі, об'єднуючи мільйони пристроїв і людей у всьому світовому співтоваристві. Мережі є фундаментальною основою для обміну інформацією в різних сферах нашого життя.

Сьогодні цей напрям комп'ютерних наук найбільш динамічно розвивається, відкриваються нові технології, і старі речі набувають нового сенсу. У зв'язку з цим на новий рівень виходить і захист інформації в мережі. Тому в першій частині навчального посібника подано огляд комп'ютерних мереж від їхньої історії, основних концепцій і протоколів до передових технологій і тенденцій, що визначають мережеву індустрію сьогодні і безпекові питання, пов'язані з роботою в мережі.

У першому розділі основну увагу приділено як історії розвитку комп'ютерних мереж, так і останнім тенденціям у галузі мережевих технологій. У другому розділі посібника висвітлено питання безпеки мереж і методи захисту від загроз, пов'язаних із мережевими атаками, вірусами та несанкціонованим доступом до даних.

Мета навчального посібника полягає в отриманні здобувачами знань з історії та перспектив розвитку комп'ютерних мереж і питань безпеки. Висвітлено застосування мереж у різних сферах, таких як бізнес, освіта, охорона здоров'я, розваги і багато інших, а також перспективні напрями їхнього розвитку, включаючи Інтернет речей (IoT), мережі наступного покоління та новітні технології мережевого зв'язку.

Посібник призначений як для початківців, так і для тих, хто має певний досвід роботи з комп'ютерними мережами. Сподіваємося, що він допоможе всім, хто бажає розширити знання в галузі комп'ютерних мереж і підвищити власні компетенції в цьому напрямі.

Розділ 1. ЕВОЛЮЦІЯ КОМП'ЮТЕРНИХ МЕРЕЖ

Комп'ютерні мережі мають широкий *спектр застосувань* і використовуються в різних сферах діяльності людини. Розглянемо деякі з них.

Бізнес та організації. Комп'ютерні мережі дають змогу організаціям обмінюватися даними, ресурсами та інформацією всередині компанії та з зовнішніми партнерами. Вони забезпечують доступ до загальних баз даних, електронної пошти, спільної роботи над проєктами, відеоконференцій та інших бізнес-додатків.

Інтернет. Світова мережа комп'ютерів (Інтернет) є найбільшою комп'ютерною мережею, що зв'язує мільйони комп'ютерів і пристроїв по всьому світу. Вона забезпечує доступ до інформації, електронної пошти, веб-сайтів, соціальних мереж, онлайн-торгівлі, потокового відео та багато іншого.

Освіта та дослідження. Комп'ютерні мережі відіграють важливу роль в освітніх закладах і наукових дослідженнях. Вони забезпечують доступ до електронних бібліотек, онлайн-курсів, віддаленого навчання, колаборативної¹ роботи над проєктами, спільної наукової роботи та обміну інформацією між науковцями та дослідницькими групами всього людства.

Домашні мережі. У домашніх умовах комп'ютерні мережі використовуються для забезпечення доступу до Інтернету, обміну файлами та сумісного використання зовнішніх пристроїв (наприклад принтерами, модемами тощо) у домашній мережі, потокового медіаконтенту, розумного будинку та інших програм.

Охорона здоров'я. У медичній сфері комп'ютерні мережі використовуються для обміну медичною інформацією, електронною

¹ Із французької *collaboration* — це **співробітництво**, що зараз досить популярне. Слова *co-author*, *co-founder*, *co-owner* означають створення певного продукту в тандемі з партнером.

медичною документацією, телемедицини, обліку пацієнтських записів, систем управління лікарнями та іншими медичними програмами.

Телекомунікації. Комп'ютерні мережі у сфері телекомунікацій забезпечують передавання голосового зв'язку, відеоконференцій, мобільного зв'язку, Інтернету, телебачення та інших послуг.

Виробництво та промисловість. Комп'ютерні мережі використовуються у промислових підприємствах для моніторингу та управління виробничими процесами, автоматизації виробництва, збирання, зберігання та аналізу даних, контролю якості та управління інфраструктурою.

Безпека. Комп'ютерні мережі відіграють важливу роль у забезпеченні безпеки в різних сферах, включаючи захист від вторгнень, моніторинг активності мережі, контроль доступу, шифрування даних і виявлення потенційних загроз.

Це лише деякі сфери застосування комп'ютерних мереж, і їхнє значення продовжує зростати з розвитком технологій і впровадженням нових інновацій.

Виділимо деякі *передумови, що призвели до створення комп'ютерних мереж.*

Потреба в обміні ресурсами. Комп'ютерні мережі створено для обміну ресурсами між комп'ютерами. Ресурси можуть включати спільні файли, папки, принтери, бази даних, додатки та інші ресурси, до яких потрібен доступ із різних комп'ютерів.

Необхідність спільної роботи. Мережі забезпечують можливість спільної роботи над проектами та завданнями. Користувачі можуть обмінюватися інформацією, спільно редагувати документи, спілкуватися та координувати дії в режимі реального часу.

Централізоване управління. Комп'ютерні мережі дають змогу централізовано управляти ресурсами та налаштуваннями.

Адміністратори мережі можуть контролювати доступ, встановлювати політику безпеки, оновлювати програмне забезпечення та виконувати інші адміністративні завдання.

Поліпшення продуктивності. Мережі дають змогу поліпшити продуктивність і ефективність роботи комп'ютерів. Ресурси та завдання можна розподілити між кількома комп'ютерами, щоб прискорити обробку даних і поліпшити реагування системи.

Потреба в обміні інформацією. Комп'ютерні мережі полегшують обмін інформацією між різними системами та програмами. Вони дають змогу передавати дані по мережі, виконувати віддалене управління та доступ до віддалених ресурсів.

Зниження витрат. Створення мережі дає змогу знизити витрати на обладнання та програмне забезпечення. Ресурси можна спільно використовувати між кількома комп'ютерами, що економить ресурси та знижує витрати на придбання нового обладнання.

Робота в групах дистанційно-глобального зв'язку. Комп'ютерні мережі забезпечують глобальний зв'язок між комп'ютерами по всьому світу. Інтернет є прикладом глобальної комп'ютерної мережі, що пов'язує мільйони комп'ютерів і пристроїв.

Усі ці передумови призвели до розвитку та розповсюдження комп'ютерних мереж, що відіграють важливу роль у сучасному інформаційному суспільстві.

1.1. Тенденції розвитку комп'ютерних мереж

З комп'ютерними мережами пов'язано багато тенденцій розвитку, що значно впливають на сучасні мережеві технології. Усе частіше ці тенденції перетинаються, доповнюють і стимулюють одна одну до розвитку. Розглянемо деякі з них.

Зростання швидкості передавання даних. З появою більш широкопasmових мереж і нових технологій передавання даних, таких як оптоволоконні кабелі, Wi-Fi стандарти високої пропускної спроможності (наприклад Wi-Fi 6 і Wi-Fi 6E), а також 5G мобільний зв'язок, швидкість передавання даних у мережах значно збільшилася. Це дає змогу швидше передавати великі обсяги інформації та підтримувати вимоги високошвидкісного інтернету, стримінгу відео високої роздільної здатності, віртуальної реальності та інших передових технологій.

Історія розвитку мобільного зв'язку налічує кілька десятиліть і пройшла через кілька ключових етапів. Ось коротка характеристика основних етапів розвитку мобільного зв'язку.

1G (перше покоління) – 1980-ті роки. Перше покоління мобільного зв'язку переважно використовувало аналогові системи передавання голосу. Найвідоміша стандартна система 1G – AMPS (англ. Advanced Mobile Phone System), що надавала основні можливості мобільного зв'язку, хоча якість зв'язку була обмежена.

2G (друге покоління) – кінець 1980-1990-ті роки. Друге покоління привнесло введення цифрових систем передавання даних. Стандарти 2G, такі як GSM (Global System for Mobile Communications), дали змогу поліпшити якість зв'язку та впровадити додаткові функції, включаючи SMS (Short Message Service) і підтримку даних на рівні GPRS (General Packet Radio Service).

3G (третє покоління) – початок 2000-х років. Третє покоління внесло суттєві зміни до мобільного зв'язку, надаючи значно вищі швидкості передавання даних. Стандарти 3G, такі як UMTS (Universal Mobile Telecommunications System) і CDMA2000 (Code Division Multiple Access 2000), дали змогу користувачам здійснювати відеодзвінки, використовувати мобільний інтернет, відправляти мультимедійні повідомлення тощо. 3G-інтернет – це набір послуг, особливістю яких є швидкісний мобільний

доступ до послуг мережі Інтернет і технологія радіозв'язку, що створює канал передавання даних. Мережі 3G працюють на частотах дециметрового діапазону близько 2 ГГц, швидкість передавання даних від 1 до 3 Мбіт/с. 3G включає п'ять стандартів сімейства IMT-2000 (UMTS/WCDMA, CDMA2000/IMT-MC, TD-CDMA/TD-SCDMA (власний стандарт Китаю), DECT і UWC-136). В Україні 3G з'явився у 2015 році, що на сім-вісім років пізніше, ніж у європейських країнах.

4G (четверте покоління) – середина 2000-х років. Четверте покоління мобільного зв'язку (LTE – Long-Term Evolution) запропонувало ще більшу пропускну здатність і поліпшену продуктивність. Стандарт 4G забезпечив високошвидкісний доступ до Інтернету, стримінг відео високої роздільної здатності, онлайн-ігри та інші передові сервіси. 4G дає змогу здійснювати передавання даних зі швидкістю вище 100 Мбіт/с – високомобільним і 1 Гбіт/с – абонентам з низькою мобільністю. Основна відмінність мереж четвертого покоління від попередніх полягає в тому, що технологія 4G заснована повністю на протоколах пакетного передавання даних, у той час як 3G поєднує як пакетну комутацію, так і комутацію каналів. Для передавання в 4G передбачені технології VoLTE. Кабінетом Міністрів України було ухвалено рішення щодо гармонізації спектра для систем мобільного зв'язку четвертого покоління в діапазоні 1800 МГц. Слід зазначити, що 4G не тільки швидше, а й дорожче, тому його спочатку встановлюють у великих містах. На сьогодні 170 країн, у тому числі майже всі держави Європи, впровадили 4G-технології.

5G (п'яте покоління) – з 2010-х років. П'яте покоління мобільного зв'язку пропонує ще більшу швидкість передавання даних, меншу затримку та підвищену ємність мережі. 5G дає змогу підтримувати ширший спектр послуг, таких як автономні автомобілі, IoT (інтернет речей), доповнена та віртуальна реальність, розумні міста та інше. Зараз нема стандартів розгортання мереж 5G [27].

6G (шосте покоління) – з 2018 року. Китайські вчені почали розробляти новий стандарт мобільного зв'язку шостого покоління. Одним із ключових завдань розроблення та розвитку нового покоління зв'язку є «загальна машинізація», коли більшість робочих людських завдань делегується машині. Поки що ці розробки ведуться паралельно з технологіями 5G. Швидкість передавання даних буде 10-11 Гбіт/с і затримка 1-10 мс аналогічні поколінню 5G.

Разом із мобільним зв'язком 6G *продовжується і поява нових технологій*, таких як розширений спектр (mmWave). *Технологія mmWave (millimeter Wave)* – це бездротова технологія передавання даних, що використовує високочастотні радіохвилі в діапазоні міліметрових хвиль (зазвичай від 30 до 300 ГГц). Цей діапазон частот знаходиться вище за традиційні діапазони, що використовуються в бездротових мережах, таких як 2.4 ГГц і 5 ГГц.

Основні характеристики технології mmWave:

- висока пропускна здатність. Технологія mmWave має дуже широку смугу пропускання, що дає змогу досягати дуже високих швидкостей передавання даних. Вона може забезпечувати швидкості кілька десятків гігабіт на секунду, що робить її придатною для передавання великих обсягів даних, наприклад при використанні високоякісного відео, віртуальної реальності (VR) і хмарних сервісів [12];

- короткий радіус дії. Через особливості високочастотних хвиль технологія mmWave має відносно низьку дальність передавання та проникнення крізь стіни і перешкоди. Сигнали mmWave легко поглинаються атмосферою і погано проникають через перепони, тому вона потребує більш щільного встановлення антен і точок доступу для забезпечення належного покриття;

- спрямована комунікація. Використання високочастотних хвиль дає змогу створювати вузьконаправлені промені сигналу, що сприяє більш

точній комунікації між пристроями, а отже, збільшити пропускну здатність і поліпшити якість зв'язку;

– використання в мережах 5G. Технологія mmWave є однією з ключових складових стандарту 5G. У мережах 5G вона застосовується для забезпечення високошвидкісного широкосмугового передавання даних на короткі відстані. Можливості mmWave в 5G дають змогу створювати більш щільні та швидкі мережі в містах і на заходах, де потрібна висока пропускну здатність.

У цілому технологія mmWave є потужним інструментом для забезпечення високошвидкісного бездротового зв'язку в обмежених географічних зонах, де потрібна висока щільність пристроїв і велика пропускну здатність.

Розширення використання хмарних обчислень. Хмарні обчислення стають усе популярнішими, і мережі відіграють ключову роль у їхньому розвитку. Більшість організацій вважають за краще зберігати дані та запускати програми у хмарній інфраструктурі, що потребує високошвидкісного та надійного мережевого підключення. Більш розподілена та гнучка архітектура мереж розробляється для підтримки хмарних обчислень, включаючи використання віртуалізації та програмно-визначуваних мереж (SDN).

Хмарні технології (Cloud Computing) являють собою модель надання комп'ютерних ресурсів, таких як обчислювальна потужність, зберігання даних і програми через інтернет. Замість того щоб підтримувати та обслуговувати власну інфраструктуру, користувачі можуть орендувати ці ресурси у хмарного провайдера за необхідності [29].

Основні характеристики хмарних технологій включають:

– ондеманд самообслуговування. Користувачі можуть отримувати доступ до необхідних ресурсів (наприклад віртуальних машин, сховища

даних) без необхідності прямої взаємодії з хмарним провайдером. Вони можуть самостійно масштабувати ресурси залежно від потреб;

– універсальний доступ до мережі. Ресурси у хмарному середовищі доступні через інтернет. Користувачі можуть отримувати доступ до них з будь-якого пристрою і будь-якої точки світу, маючи підключення до Інтернету;

– розподіл ресурсів [14]. Хмарні провайдери надають ресурси, такі як сервери, мережеві пристрої та сховище даних, що можуть бути масштабовані та розподілені серед багатьох клієнтів. Це дає змогу ефективного використання ресурсів і гнучкості в адаптації до потреб клієнтів. *Сервер* як комп'ютер – це комп'ютер у локальній чи глобальній мережі, що надає користувачам свої обчислювальні і дискові ресурси, а також доступ до встановлених сервісів; найчастіше працює цілодобово чи при роботі групи його користувачів. Комп'ютер або програма, встановлена на цьому комп'ютері, здатні автоматично розподіляти інформацію чи файли під управлінням мережевої ОС або у відповідь на запити, надіслані в режимі онлайн користувачами, і в такий спосіб надавати послуги іншим комп'ютерам мережі (клієнтам);

– вимірювання та оплата використання. Замість фіксованих витрат на інфраструктуру хмарні технології пропонують модель оплати за використання ресурсів. Користувачі платять лише за ресурси, які вони фактично використовують, і можуть масштабувати витрати відповідно до потреб;

– гнучкість і масштабованість. Хмарні технології пропонують гнучкість у використанні та масштабуванні ресурсів залежно від потреб. Користувачі можуть легко збільшувати або зменшувати обчислювальну потужність, зберігати дані та інші ресурси відповідно до вимог, що змінюються.

Хмарні технології надають організаціям та користувачам потужні обчислювальні ресурси [29].

Розвиток хмарних технологій має досить тривалу історію. Ось короткий огляд основних етапів історії розвитку хмарних технологій.

Наприкінці 1990-х років компанії почали надавати віртуальні приватні сервери (Virtual Private Servers, VPS), що давали змогу користувачам орендувати віртуальний простір на сервері. Це було першим кроком надання обчислювальних ресурсів через інтернет.

На початку 2000-х років з'явилася концепція «утилітарних обчислень» (Utility Computing), що пропонує можливість платити тільки за використані ресурси подібно до комунальних послуг. Це стало основою поняття «хмарних обчислень».

У 2006 році компанія Amazon запустила свою першу хмарну платформу Amazon Web Services (AWS), що надає інфраструктуру як послугу (Infrastructure as a Service, IaaS). AWS запропонував широкий набір послуг, таких як віртуальні машини, сховище даних і мережеві можливості, які користувачі могли використовувати на вимогу.

У 2008 році компанія Google надала Google App Engine – платформу для розроблення та розгортання вебзастосунків у хмарному середовищі. Це призвело до появи концепції «платформи як послуги» (Platform as a Service, PaaS), що пропонує середовище користувача для розроблення та виконання додатків.

Протягом 2010-х років хмарні технології стали все популярнішими, і безліч компаній запропонували свої хмарні платформи та послуги. Microsoft Azure, IBM Cloud та інші великі гравці увійшли на цей ринок, пропонуючи широкий спектр хмарних послуг, таких як обчислювальні ресурси, сховище даних, аналітику та машинне навчання.

На сьогодні хмарні технології продовжують розвиватися та інновувати. Зростає попит на гібридні хмари, що поєднують публічні та приватні хмари, а також на спеціалізовані хмарні послуги, такі як блокчейн-хмари та роботизовані процеси автоматизації (Robotic Process Automation, RPA).

Хмарні технології значно змінили спосіб надання та використання інформаційних технологій, забезпечуючи гнучкість, масштабованість і доступність ресурсів для організацій і користувачів по всьому світу.

Інтернет речей (IoT). IoT являє собою мережу фізичних об'єктів (пристроїв), що взаємодіють між собою та з зовнішнім середовищем із використанням мережевих технологій. Ось деякі аспекти розвитку IoT:

– розширення кількості підключених пристроїв. Кількість пристроїв IoT продовжує зростати. Від побутових пристроїв, таких як розумні будинки, телевізори, колонки та пристрої, до промислових систем моніторингу та управління, медичного обладнання, транспортних систем і міської інфраструктури все більше пристроїв стають підключеними до інтернету і обмінюються даними між собою;

– розвиток мережевих технологій. Для забезпечення зв'язку та обміну даними між пристроями IoT потрібні різні мережеві технології. Класичні технології, такі як Wi-Fi, Bluetooth та Ethernet, усе ще широко використовуються, але розвиваються і нові технології, такі як Narrowband IoT (NB-IoT), Low-Power Wide-Area Networks (LPWAN), 5G тощо. Ці технології забезпечують ширше охоплення, менше енергоспоживання та більш надійний зв'язок для різних типів пристроїв IoT;

– обробка даних і аналітика. Величезні обсяги даних, що збираються від пристроїв IoT, потребують потужних систем обробки даних і аналітики. Хмарні платформи та системи аналітики даних використовуються для збирання, зберігання та аналізу даних IoT. Аналітика даних дає змогу виявляти тенденції, прогнозувати події, оптимізувати процеси та приймати поінформовані рішення на основі даних, зібраних від пристроїв IoT;

– безпека та конфіденційність. Зі збільшенням кількості підключених пристроїв IoT виникають нові питання безпеки та конфіденційності даних. Захист від кібератак, шифрування даних, автентифікація пристроїв і механізми управління доступом стають важливими аспектами розвитку IoT;

– інтеграція зі штучним інтелектом (ШІ) та автоматизація. ШІ та машинне навчання стають більш важливими для обробки і аналізу даних IoT, а також автоматизації та управління пристроями. Розумні системи, засновані на ШІ, можуть приймати рішення і виконувати дії на основі даних, зібраних від пристроїв IoT, що сприяє підвищенню ефективності та автоматизації процесів.

Розвиток Інтернету речей пропонує величезний потенціал для перетворення різних галузей і поліпшення нашого життя, призводить до збільшення кількості підключених пристроїв, що обмінюються даними через мережі. Пристрої IoT можуть включати датчики, смарт-пристрої, медичне обладнання, системи безпеки та багато іншого. Це потребує розвитку більш масштабованих і безпечних мереж, здатних обробляти величезний обсяг даних і забезпечувати надійне з'єднання для багатьох пристроїв. Проте з ним також пов'язані проблеми з приватністю, безпекою та управлінням даних.

Поліпшення безпеки мереж. Зі збільшенням кількості загроз у мережі, таких як кібератаки та віруси, безпека стає все більш важливим аспектом розвитку комп'ютерних мереж. Розвиваються нові методи захисту даних і мережевих пристроїв, включаючи шифрування, міжмережеві екрани, системи виявлення вторгнень та інші технології. Більш докладно це питання розглянемо у другому розділі посібника.

Поширення останнім часом програмно-визначених мереж. Програмно-визначені мережі (*Software-Defined Networking, SDN*) – архітектурний підхід до побудови та управління мережами, що відокремлює управління мережевими пристроями від передавання даних. Він заснований на ідеї централізованого контролера, що приймає рішення про маршрутизацію та управління трафіком, а потім передає відповідні інструкції на мережеві комутатори та маршрутизатори.

Ось основні характеристики SDN:

– централізоване управління. У SDN-архітектурі управління мережею здійснюється за допомогою централізованого контролера. Це дає змогу мережевим адміністраторам легко управляти і налаштовувати мережу, приймати рішення про маршрутизацію та управління трафіком з однієї точки управління;

– поділ управління та передавання даних. SDN відокремлює управління мережею від передавання даних. Контролер приймає рішення про трафік і налаштовує мережеві комутатори, тоді як само передавання даних здійснюється на мережевих пристроях;

– гнучкість і масштабованість. SDN дає змогу легко змінювати і адаптувати мережу до потреб, що змінюються. Адміністратори можуть програмно налаштовувати правила маршрутизації, управління трафіком і політики без необхідності налаштування кожного мережевого пристрою окремо. Завдяки цьому SDN має високу гнучкість і масштабованість;

– спрощення управління мережею. SDN знижує складність управління мережею та підвищує автоматизацію. Адміністратори можуть використовувати програмні інтерфейси та контролери для управління всією мережею, встановлювати та змінювати правила та політики, контролювати пропускну здатність і маршрутизацію, а також виявляти атаки і запобігати їм;

– підтримка інновацій. SDN забезпечує гнучку платформу для розроблення та впровадження нових мережевих сервісів і програм. Шляхом програмного управління та контролю мережі SDN дає змогу інтегрувати мережу з іншими системами та додатками, що сприяє інноваціям і створенню нових можливостей.

SDN пропонує новий підхід до побудови та управління мережами, маючи переваги гнучкості, керованості та масштабованості, спрощує впровадження нових сервісів і підвищує ефективність роботи. Він має широке застосування в центрах обробки даних, корпоративних провайдерських мережах і хмарних середовищах.

Мережа зберігання даних (Storage Area Network, SAN) – це спеціалізована архітектура, призначена для централізованого управління зберіганням та обміном даними між серверами та сховищами даних.

У SAN використовується високошвидкісна мережа зазвичай на основі фіброоптичного кабелю для з'єднання серверів із сховищами даних, такими як дискові масиви (disk arrays) або пристрої зберігання на основі флеш-пам'яті (flash storage). Мережа SAN надає високу пропускну здатність, низьку затримку та можливість масштабування, що дає змогу ефективно управляти сховищем даних і забезпечувати високу доступність.

Переваги SAN включають:

- централізоване управління. SAN дає змогу централізовано управляти сховищем даних, що спрощує процеси резервного копіювання, відновлення та масштабування;

- висока продуктивність. SAN забезпечує високу пропускну здатність і низьку затримку, що дає змогу серверам швидко отримувати доступ до даних;

- висока доступність. SAN дає змогу створювати стійкі до відмови конфігурації, включаючи резервне дублювання даних і механізми відновлення після збоїв;

- масштабованість. SAN дає змогу легко додавати додаткові сховища даних і розширювати ємність сховища без переривання роботи системи;

- зручність управління. SAN забезпечує єдиний інтерфейс для управління сховищем даних, що спрощує його адміністрування та конфігурування.

SAN широко використовується в підприємствах і центрах обробки даних, де потрібна висока продуктивність, надійність і масштабованість сховища даних. Він забезпечує ефективне використання зберігання ресурсів і гнучкість у розгортанні додатків та обробці даних [12].

Ось кілька прикладів топологій і протоколів, що використовуються в SAN:

1. Фіброоптична SAN (Fibre Channel SAN) – один із найпоширеніших прикладів SAN. Він використовує спеціальні комутатори Fibre Channel та оптичні кабелі для передавання даних між серверами і сховищем даних. Фіброоптична SAN забезпечує високу швидкість передавання даних і низьку затримку, що робить її ідеальною для критично важливих програм.

Розглянемо декілька прикладів застосування мережі Fibre Channel SAN.

Сховище даних. У корпоративному середовищі Fibre Channel SAN може використовуватися для підключення до централізованого сховища даних. Це дає змогу кільком серверам звертатися до спільного сховища з високою швидкістю і надійністю. SAN також забезпечує можливість розширення сховища, даючи змогу додавати нові пристрої зберігання за необхідності.

Бекап і відновлення. Мережа Fibre Channel SAN часто використовується для забезпечення швидкого та надійного бекапу та відновлення даних. Вона дає змогу резервувати і відновлювати великі обсяги даних із високою швидкістю і мінімальним навантаженням на продуктивність серверів.

Кластеризація. У високонавантажених середовищах, таких як сервери баз даних або вебпрограми, Fibre Channel SAN може використовуватися для створення кластерів серверів. Кластеризація дає змогу розподілити навантаження між кількома серверами та забезпечити відмовостійкість. SAN забезпечує високу пропускну здатність і низьку затримку, що важливо для забезпечення швидкого доступу до даних у кластері.

Віртуалізація. Мережа Fibre Channel SAN також широко використовується у віртуалізованих середовищах. Вона забезпечує зберігання віртуальних машин на загальному сховищі даних і дає змогу

гнучко переміщувати і масштабувати віртуальні ресурси між фізичними серверами.

Big Data. Мережа використовується задля забезпечення швидкого доступу до даних, що дає змогу ефективно виконувати обчислення та аналізувати великі обсяги інформації.

2. iSCSI (Internet Small Computer System Interface) SAN є протоколом, що дає змогу використовувати мережу TCP/IP для передавання блокових даних між серверами та сховищем даних. iSCSI SAN може використовувати наявну мережеву інфраструктуру, таку як Ethernet, що робить його доступнішим з точки зору вартості.

Мережі iSCSI SAN включають такі базові компоненти:

Ініціатори iSCSI – сервери або вузли, що ініціюють з'єднання iSCSI зі сховищем даних. Вони зазвичай налаштовані за допомогою спеціального програмного забезпечення, яке дає змогу серверам бачити віддалені блокові пристрої, підключені через iSCSI.

Цільові пристрої iSCSI – сховища даних, що надають блокові пристрої для серверів за допомогою протоколу iSCSI. Цільові пристрої можуть бути фізичними серверами, спеціалізованими сховищами чи віртуальними машинами.

iSCSI-мережа – IP-мережа, якою передаються iSCSI-пакети. Це може бути локальна мережа (LAN) або виділена мережа, створена спеціально для передавання iSCSI-трафіка. Зазвичай рекомендується використовувати виділену мережу для iSCSI-трафіка, щоб уникнути конкуренції з іншими мережевими програмами.

Мережеві комутатори використовуються для з'єднання та маршрутизації iSCSI-трафіка всередині iSCSI SAN. Вони забезпечують високу пропускну здатність і низьку затримку для забезпечення ефективного передавання даних.

Для управління та моніторингу iSCSI SAN використовуються спеціальні програмні інструменти. Вони дають змогу адміністраторам налаштовувати і контролювати з'єднання iSCSI, моніторити продуктивність мережі та сховища даних, а також виявляти та усувати можливі проблеми.

Реалізація iSCSI SAN може змінюватися залежно від конкретних вимог та інфраструктури організації.

3. FCoE SAN (Fibre Channel over Ethernet) – протокол, що поєднує переваги Fibre Channel та Ethernet, даючи змогу передавати фрейми Fibre Channel через мережу Ethernet. FCoE SAN використовує спеціальні комутатори, Converged Network Switches, для об'єднання мережі даних і сховища даних.

Приклади простої мережі FCoE SAN:

Комутатор FCoE – використовується комутатор, що підтримує FCoE, для об'єднання мереж Fibre Channel та Ethernet.

Сервери – підключаються до комутатора FCoE через конвертери FCoE або мережеві адаптери, що підтримують протокол FCoE.

Сховище даних – таке, як система зберігання даних на основі Fibre Channel, підключається до комутатора FCoE.

Мережа Ethernet – комутатор FCoE підключається до наявної Ethernet-інфраструктури, що може використовуватися для обміну даними з серверами або іншими пристроями Ethernet.

Зверніть увагу, що фактична конфігурація мережі FCoE SAN може змінюватися залежно від вимог і архітектури мережі кожної організації.

4. NVMe over Fabrics (NVMe-oF) – це протокол, що дає змогу передавати дані з використанням протоколу NVMe (Non-Volatile Memory Express) через мережу, таку як Ethernet чи InfiniBand. NVMe-oF SAN дає можливість використання протоколу NVMe для передавання між хостом і віддаленим сховищем через мережу, забезпечує низьку затримку та високу пропускну здатність, що особливо важливо для роботи з високопродуктивними твердотілими накопичувачами (SSD).

Ось кілька прикладів мереж, що використовують технологію NVMe-oF.

У підприємстві може бути налаштований кластер сховища, що складається з кількох вузлів сховища, пов'язаних мережею NVMe-oF. Хости можуть звертатися до кластера сховища через NVMe-oF для швидкого доступу до даних.

Центр обробки даних (ЦОД) може розгорнути мережу NVMe-oF для зв'язку між серверами і сховищем. Саме це дає змогу серверам обмінюватися даними зі сховищем із високою швидкістю і низькою затримкою.

Гіпермасштабовані системи NVMe-oF можуть використовуватися для зв'язку між вузлами в гіпермасштабованих системах, таких як системи розподіленої бази даних або хмарні обчислення. Це забезпечує високу пропускну здатність і низьку латентність² при передаванні даних між вузлами.

Віддалений доступ до даних – NVMe-oF дає змогу організаціям забезпе-чити віддалений доступ до даних, що зберігаються на віддалених серверах. Це особливо корисно для надання віддаленого доступу до даних у режимі реального часу, таких як відеостримінг або обробка великих обсягів даних.

Віртуалізація сховища. Мережа NVMe-oF може бути використана для віртуалізації сховища, даючи змогу кільком хостам віртуалізувати доступ до спільного сховища за допомогою протоколу NVMe-oF.

Технологія NVMe-oF забезпечує високу продуктивність, низьку затримку та можливість масштабування, роблячи її привабливим рішенням для різних сценаріїв зберігання та передавання даних.

Ми розглянули лише деякі приклади технологій, що використовуються в мережі зберігання даних (SAN), – залежно від вимог і

² Латентність (від лат. *Latentis*) — прихований, невидимий: властивість об'єктів або процесів перебувати у прихованому стані, не виявляючи себе; затримка між стимулом і реакцією.

бюджету організації можна вибрати відповідну топологію та протокол реалізації SAN; тенденції розвитку комп'ютерних мереж – розвиток технологій і потреби користувачів продовжують вносити зміни та інновації в галузь комп'ютерних мереж.

1.2. Комп'ютерні та телекомунікаційні мережі

Комп'ютерні мережі з'явилися порівняно недавно, наприкінці 1960-х років. Комп'ютерні мережі успадкували багато корисних властивостей від інших, більш старих і розповсюджених, телекомунікаційних мереж, а саме телефонних. У той же час комп'ютерні мережі привнесли в телекомунікації щось зовсім нове – вони зробили загальнодоступними невичерпні обсяги інформації, що створені цивілізацією за кілька тисячоліть свого існування і продовжують поповнюватися зі зростаючою швидкістю в наші дні.

Результатом впливу комп'ютерних мереж на інші типи телекомунікаційних мереж став процес їхньої *конвергенції* (лат. Convergo – зближаю) – процес зближення, сходження, взаємопроникнення, на відміну від *дивергенції* (розбіжності).

Цей процес почався досить давно, однією з перших ознак зближення було передавання телефонними мережами голосу в цифровій формі. Комп'ютерні мережі також активно йдуть назустріч телекомунікаційним мережам, розробляючи нові сервіси, які раніше були прерогативою телефонних, радіо- й телевізійних мереж – сервіси IP-телефонії, радіо- і відеовіщання, ряд інших.

Комп'ютерні мережі, що називаються також *мережами передавання даних*, є логічним результатом еволюції двох найважливіших науково-технічних галузей сучасної цивілізації – комп'ютерних і телекомунікаційних технологій.

З одного боку, мережі являють собою окремий випадок розподілених обчислювальних систем, у яких група комп'ютерів узгоджено вирішує набір

взаємозалежних завдань, обмінюючись даними в автоматичному режимі. З іншого боку, комп'ютерні мережі можуть розглядатися як засіб передавання інформації на більші відстані, для чого в них застосовуються методи кодування та мультиплексування даних, що одержали розвиток у різних телекомунікаційних системах.

Перші комп'ютери 1950-х років – громіздкі й дорогі – призначалися для невеликої кількості користувачів. Часто ці комп'ютери займали цілі будинки. Такі комп'ютери не були призначені для інтерактивної роботи користувача, а застосовувалися в режимі пакетної обробки (рис. 1.1).

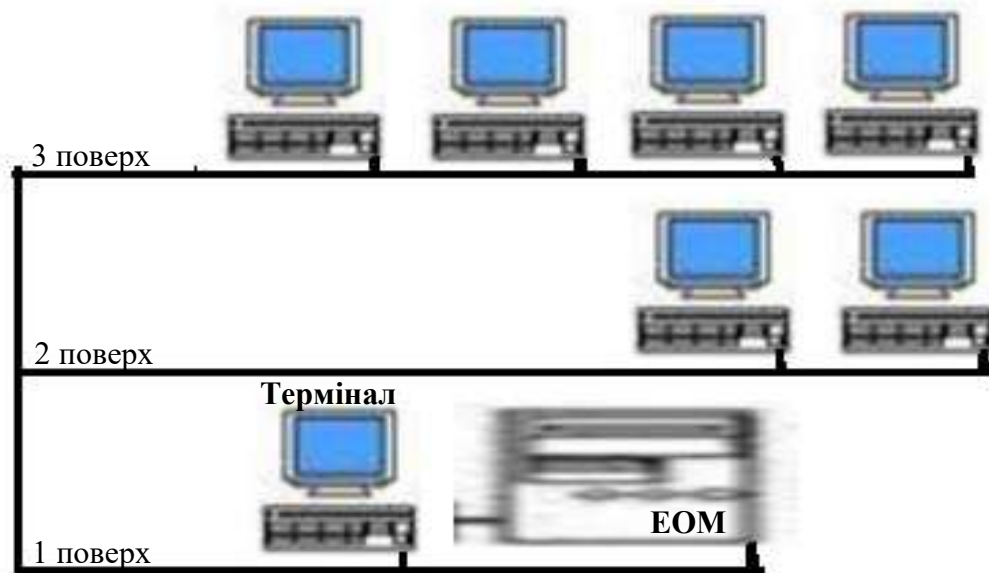


Рис. 1.1. Багатотермінальна система,
прототип обчислювальної мережі

Системи пакетної обробки [14] зазвичай будувалися на базі ЕОМ – потужного і надійного комп'ютера універсального призначення. Користувачі підготовляли перфокарти, що містять дані і команди програм, і передавали їх в обчислювальний центр. Оператори вводили ці карти в комп'ютер, а роздруковані результати користувачі одержували тільки наступного дня. Для користувачів *інтерактивний режим роботи*, при якому можна з терміналу оперативно управляти процесом обробки своїх

даних, був би зручнішим. Але інтересами користувачів на перших етапах розвитку обчислювальних систем переважно нехтували. На першому місці була ефективність роботи найдорожчого пристрою обчислювальної машини – процесора, а не ефективність роботи фахівців, які його використовують.

Зі здешевленням процесорів на початку 1960-х років з'явилися нові способи організації обчислювального процесу, що дали змогу врахувати інтереси користувачів. Почали розвиватися інтерактивні *багатотермінальні системи розподілу часу*.

У таких системах кожен користувач одержував власний термінал, за допомогою якого він міг вести діалог з комп'ютером. Кількість працівників, які одночасно працювали з комп'ютером, визначалася його *потужністю*: час реакції обчислювальної системи мав бути досить малим, щоб користувачу була не дуже помітна паралельна робота з комп'ютером інших користувачів.

Термінали, вийшовши за межі обчислювального центру, розосередилися по всьому підприємству. І хоча обчислювальна потужність залишалася повністю централізованою, деякі функції, такі як введення й виведення даних, стали розподіленими. Подібні багатотермінальні централізовані системи зовні вже були дуже схожі на локальні обчислювальні мережі.

Дійсно, рядовий користувач роботу за терміналом ЕОМ сприймав приблизно так само, як зараз він сприймає роботу за підключеним до мережі персональним комп'ютером. Користувач міг одержати доступ до загальних файлів і периферійних пристроїв, при цьому в нього підтримувалася повна ілюзія одноособового володіння комп'ютером, тому що він міг запустити потрібну йому програму в будь-який момент і майже відразу одержати результат.

Багатотермінальні системи, що працюють у режимі розподілу часу, стали першим кроком на шляху створення локальних обчислювальних

мереж. Але потреба підприємств у створенні локальних мереж у цей час ще не дозріла – в одному будинку просто не було що поєднувати в мережу, оскільки через високу вартість обчислювальної техніки підприємства не мали змоги придбати декілька комп'ютерів.

1.2.1. Глобальні мережі

Потреба в з'єднанні комп'ютерів, що перебувають на великій відстані один від одного, до цього часу вже цілком назріла. Почалося все з вирішення більш простого завдання – доступу до комп'ютера з терміналів, віддалених від нього на багато сотень, а то й тисяч кілометрів. Термінали з'єднувалися з комп'ютерами через телефонні мережі за допомогою модемів. Такі мережі давали змогу численним користувачам одержувати віддалений доступ до розподілених ресурсів декількох потужних суперкомп'ютерів. Потім з'явилися системи, у яких разом із віддаленими з'єднаннями типу термінал-комп'ютер були реалізовані й віддалені зв'язки типу комп'ютер-комп'ютер.

Комп'ютери отримали можливість обмінюватися даними в автоматичному режимі, що і є базовою ознакою будь-якої обчислювальної мережі. *На основі подібного механізму в перших мережах були реалізовані служби обміну файлами, синхронізації баз даних, електронної пошти й інші мережеві служби, що стали тепер традиційними.*

Отже, хронологічно першими з'явилися **глобальні обчислювальні мережі** (Wide Area Network, WAN), що поєднують територіально розосереджені комп'ютери, які, можливо, перебувають у різних містах і країнах.

Саме при побудові глобальних мереж були вперше запропоновані і відпрацьовані багато основних ідей, що лежать в основі сучасних обчислювальних мереж: *багаторівнева побудова комунікаційних протоколів, концепції комутації та маршрутизації пакетів.*

Глобальні комп'ютерні мережі дуже багато чого успадкували від інших, набагато старіших і розповсюджених глобальних мереж – телефонних. Головне технологічне нововведення, що привнесли перші глобальні комп'ютерні мережі, становило відмову від принципу комутації каналів, що протягом багатьох десятиріч років успішно використовувався в телефонних мережах.

Виділений на весь час сеансу зв'язку складений телефонний канал, що передає інформацію з постійною швидкістю, не міг ефективно використовуватися пульсуючим трафіком комп'ютерних даних, у якого періоди інтенсивного обміну чергуються з тривалими паузами.

Натурні експерименти та математичне моделювання показали, що пульсуючий і значною мірою не чутливий до затримок комп'ютерний трафік набагато ефективніше передається мережами, які працюють за принципом комутації пакетів, коли дані поділяються на невеликі порції – пакети, що самостійно переміщуються по мережі завдяки наявності адреси кінцевого вузла в заголовку пакета.

Оскільки прокладання високоякісних ліній зв'язку на великі відстані дуже дороге, то в перших глобальних мережах часто використовувалися наявні канали зв'язку, призначені зовсім для іншого. Наприклад, протягом багатьох років глобальні мережі будувалися на основі телефонних каналів тональної частоти, здатних у кожний момент часу передавати тільки одну розмову в аналоговій формі. Оскільки швидкість передавання дискретних комп'ютерних даних по таких каналах була дуже низькою (десятки кілобітів за секунду), набір послуг у глобальних мережах такого типу звичайно обмежувався передаванням файлів (переважно у фоновому режимі) і електронною поштою.

Окрім низької швидкості, такі канали мають і інший недолік – вони дуже спотворюють передавання сигналу. Тому протоколи глобальних мереж, побудованих із використанням каналів зв'язку низької якості, відрізняються

складними процедурами контролю та відновлення даних. Типовим прикладом таких мереж є мережі X.25, розроблені ще на початку 1970-х років, коли низькошвидкісні аналогові канали, орендовані в телефонних компаній, були переважним типом каналів, що з'єднують комп'ютери і комутатори глобальної обчислювальної мережі.

У 1969 році міністерство оборони США ініціювало роботи з об'єднання в єдину мережу суперкомп'ютерів оборонних і науково-дослідних центрів. Ця мережа одержала назву ARPANET і стала відправною точкою для створення першої і найвідомішої нині глобальної мережі – Інтернет.

Мережа ARPANET поєднувала комп'ютери різних типів, що працювали *під управлінням різних операційних систем (ОС)* з додатковими модулями, що реалізують комунікаційні протоколи, загальні для всіх комп'ютерів мережі. ОС цих комп'ютерів можна вважати першими *мережевими операційними системами*.

Мережеві операційні системи, на відміну від багатотермінальних операційних систем, давали змогу не тільки розосередити користувачів, але й організувати розподілені зберігання та обробку даних між декількома комп'ютерами, пов'язаними електричними зв'язками. Будь-яка мережева операційна система, з одного боку, виконує всі функції локальної операційної системи, а з іншого боку, має деякі додаткові засоби, що дають змогу їй взаємодіяти через мережу з операційними системами інших комп'ютерів. *Програмні модулі, що реалізують мережеві функції, з'являлися в операційних системах поступово, з розвитком мережевих технологій, апаратної бази комп'ютерів і виникнення нових завдань, що потребують мережевої обробки.*

1.2.2. Локальні мережі

Важлива подія, що вплинула на еволюцію комп'ютерних мереж, відбулася на початку 1970-х років. У результаті технологічного прориву в галузі виробництва комп'ютерних компонентів з'явилися *великі інтегральні схеми (ВІС)*. Їхня порівняно невисока вартість і гарні функціональні можливості призвели до створення мінікомп'ютерів, що стали реальними конкурентами електронної обчислювальної машини. Навіть невеликі підрозділи організації одержали можливість мати власні комп'ютери. Мінікомп'ютери вирішували завдання управління технологічним устаткуванням, складом та інші завдання рівня відділу організації. Отже, з'явилася концепція розподілу комп'ютерних ресурсів по всій організації. Необхідно враховувати той факт, що різні відділи в одній організації могли знаходитися в різних частинах міста, області або навіть країни.

Однак при цьому всі комп'ютери однієї організації, як і раніше, продовжували працювати автономно (рис. 1.2).

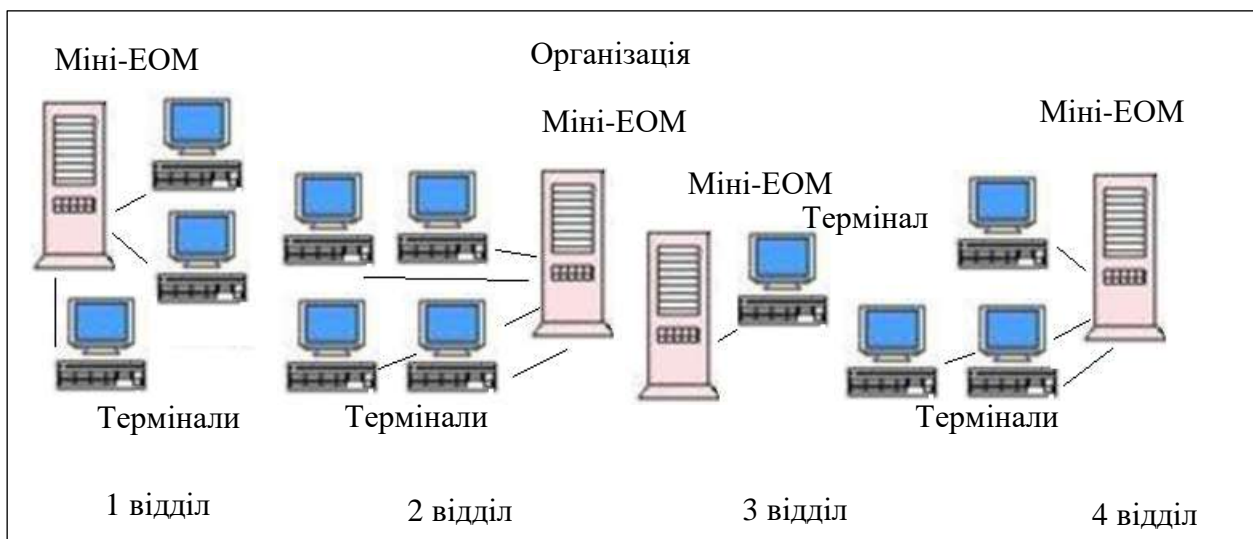


Рис. 1.2. Автономне використання деякої кількості мінікомп'ютерів на одному підприємстві

Час минав, і потреби користувачів обчислювальної техніки росли. Їх уже не задовольняла ізольована робота на власному комп'ютері, а хотілося в автоматичному режимі обмінюватися комп'ютерними даними з користувачами інших підрозділів. Відповіддю на цю потребу стала поява перших локальних обчислювальних мереж.

Локальні обчислювальні мережі (Local Area Network, LAN) – це об'єднання комп'ютерів, зосереджених на невеликій території, звичайно в радіусі не більше 1-2 км, хоча в окремих випадках локальна мережа може мати і більші розміри, наприклад декілька десятків кілометрів. У загальному випадку локальна мережа являє собою комунікаційну систему, що належить одній організації.

Спочатку для з'єднання комп'ютерів один з одним використовувалися нестандартні мережеві технології.

Мережева технологія – це погоджений набір програмних і апаратних засобів (наприклад драйверів, мережевих адаптерів, кабелів і роз'ємів), а також механізмів передавання даних по лініях зв'язку, достатній для побудови обчислювальної мережі.

Різні пристрої сполучення, що використовують власні способи подання даних на лініях зв'язку, свої типи кабелів і т. п., могли з'єднувати тільки ті конкретні моделі комп'ютерів, для яких були розроблені, наприклад мінікомп'ютери PDP-11 (рис. 1.3, а) з мейнфреймом³ IBM 360 (рис. 1.3, б) або мінікомп'ютери HP з мікрокомп'ютерами LSI-11.

PDP-11 16-розрядна машина компанії Digital 1970 року випуску. Серія PDP-11 вироблялася аж до 1990 року, останні версії були MicroPDP-11/94 і -11/93 (табл. 1.1).

³ Мейнфрейм (англ. mainframe) – велика універсальна високопродуктивна практично безвідмовна електронна обчислювальна машина (часто це сервер) з великими ресурсами введення/виведення, значним обсягом оперативної та зовнішньої пам'яті.

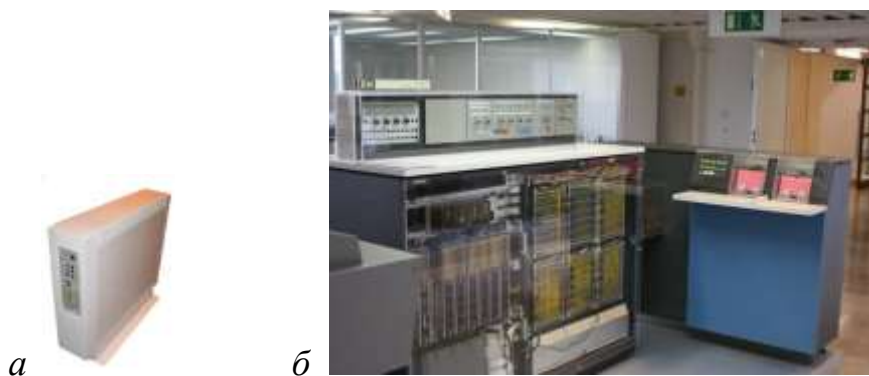


Рис. 1.3. Мінікомп'ютери: *a* – Digital Micro PDP-11/53(1987);
б – IBM System/360 Model 20

Таблиця 1.1

Інші системи Micro компанії Digital

Система Micro	Дата випуску
Digital PDP-11/03-L	1970
Digital Micro PDP-11/23	1970
Digital PDP-8/E	1971
Digital Hi Note CT475	1994
DECpc 425SE Laptop	1994
DEC Prototype Set Top Box	1996

У середині 1980-х років положення справ у локальних мережах кардинально змінилося. Затвердилися **стандартні мережеві технології** об'єднання комп'ютерів у мережу – *Ethernet, Arcnet, Token Ring, Token Bus*, трохи пізніше – *FDDI*.

Потужним стимулом для їхньої появи послужили **персональні комп'ютери**. Ці масові продукти стали ідеальними елементами побудови мереж: з одного боку, вони були досить потужними, щоб забезпечувати роботу мережевого програмного забезпечення, а з іншого боку, явно мали потребу в об'єднанні своєї обчислювальної потужності для вирішення складних завдань, а також розподілу дорогих периферійних пристроїв і дискових масивів. Тому персональні комп'ютери стали переважати в

локальних мережах, причому не тільки як клієнтські комп'ютери, але і центри зберігання і обробки даних, тобто мережевих серверів, потіснивши з цих звичних ролей мінікомп'ютери та мейнфрейми.

Усі стандартні технології локальних мереж спиралися на той самий принцип комутації, що був з успіхом випробуваний і довів свої переваги при передаванні трафіка даних у глобальних комп'ютерних мережах, – *принцип комутації пакетів*.

Стандартні мережеві технології перетворили процес побудови локальної мережі з вирішення нетривіальної технічної проблеми в рутинну роботу. Для створення мережі досить було придбати стандартний кабель, мережеві адаптери відповідного стандарту, наприклад Ethernet, вставити адаптери в комп'ютери, приєднати їх до кабелю стандартними роз'ємами та встановити на комп'ютери одну з популярних мережевих операційних систем, наприклад Novell NetWare.

1.2.3. Наближення локальних і глобальних мереж

Наприкінці 1980-х років відмінності між локальними і глобальними мережами проявлялися досить чітко.

Довжина і якість ліній зв'язку. Локальні комп'ютерні мережі відрізняються від глобальних мереж невеликими відстанями між вузлами мережі. Це в принципі уможливорює використання в локальних мережах більш якісних ліній зв'язку.

Складність методів передавання даних. В умовах низької надійності фізичних каналів у глобальних мережах потрібні більше складні, ніж у локальних мережах, методи передавання даних і відповідне устаткування.

Швидкість обміну даними в локальних мережах (10, 16 і 100 Мбіт/с) у той час була істотно вище, ніж у глобальних (від 2,4 кбіт/с до 2 Мбіт/с).

Різноманітність послуг. Високі швидкості обміну даними дали змогу надавати в локальних мережах широкий спектр послуг – це насамперед різні

механізми використання файлів, що зберігаються на дисках інших комп'ютерів мережі, спільне використання пристроїв друкування, модемів, факсів, доступ до єдиної бази даних, електронна пошта та ін. У той же час глобальні мережі в основному обмежувалися поштовими і файловими послугами в їхньому найпростішому (не найзручнішому для користувача) вигляді.

Поступово розходження між локальними і глобальними мережевими технологіями стали зникати. Ізольовані раніше локальні мережі почали поєднувати, при цьому як сполучне середовище використовувалися глобальні мережі. Починаючи з 1990-х років комп'ютерні глобальні мережі, що працюють на основі швидкісних цифрових каналів, істотно розширили спектр послуг і наздогнали локальні мережі. Стало можливим створення служб, робота яких пов'язана з доставкою користувачеві більших обсягів інформації в реальному часі: зображень, відеофільмів, голосу – загалом усього того, що одержало назву *мультимедійної інформації*. *Найбільш яскравий приклад – гіпертекстова інформаційна служба World Wide Web, що стала основним постачальником інформації в Інтернеті.*

Її інтерактивні можливості перевершили можливості багатьох аналогічних служб локальних мереж, так що розробникам локальних мереж довелося просто запозичити цю службу у глобальних мереж. Процес перенесення технологій із глобальної мережі Інтернет у локальні набув такого масового характеру, що з'явився навіть спеціальний термін – *intranet-технології* (intra — внутрішній).

Ще однією ознакою зближення локальних і глобальних мереж є поява мереж, що займають проміжне положення між локальними і глобальними мережами.

Міські мережі, мережі мегаполісів – регіональні обчислювальні мережі (Metropolitan Area Network, MAN) – призначені для обслуговування території великого міста (регіона). Ці мережі використовують цифрові лінії

зв'язку, часто оптоволоконні, зі швидкостями на магістралі від 155 Мбіт/с і вище. Вони забезпечують економічне по'єднання локальних мереж між собою, а також вихід у глобальні мережі.

З'явився новий термін – *інфокомунікаційна мережа*, що прямо розуміє дві складові сучасної мережі (інформаційної) – комп'ютерної і телекомунікаційної.

1.3. Розвиток комп'ютерної техніки на основі малогабаритних і суперкомп'ютерів

Наприкінці ХХ століття розвиток комп'ютерної техніки відбувався за двома основними напрямками: створення *малогабаритних персональних комп'ютерів* і створення *потужних суперкомп'ютерів*.

1.3.1. Створення малогабаритних персональних комп'ютерів

Персональний комп'ютер – це настільна або переносна електронно-обчислювальна машина, що відповідає вимогам загальнодоступності і універсальності застосування.

Малогабаритні комп'ютери також відомі як *мінікомп'ютери* або *мікрокомп'ютери*, є компактними пристроями з невеликим розміром і низьким енергоспоживанням. Вони призначені для виконання простих завдань, таких як доступ до Інтернету, виконання офісних завдань, мультимедійне відтворення, та інших програм із низьким обчислювальним навантаженням. Ось кілька прикладів малогабаритних комп'ютерів:

1. Raspberry Pi є одним із найпопулярніших мінікомп'ютерів. Він є одноплатним комп'ютером розміром із кредитну картку. Raspberry Pi працює на базі ARM-процесора та має моделі з різними характеристиками та можливостями. Він широко використовується для багатьох проєктів, включаючи розумний будинок, медіацентри, ретроігрові консолі та ін.

Наприклад, мінікомп'ютер Raspberry Pi 4 B 4GB RasPad 3 Bundle вартістю на сьогодні близько 300 євро має роздільну здатність зображення – 1280 x 800 пікселів; Bluetooth; розмір екрана 10,1 дюйма; 4 ядра; дротове підключення HDMIUSBEthernetAudio; тактову частоту 1,5 ГГц; сенсорний емнісний екран; W-Lan, важить 0,60 кг (рис. 1.4).



Рис. 1.4. Мінікомп'ютер Raspberry Pi 4 B 4GB RasPad 3 Bundle

2. Intel NUC (Next Unit of Computing) – це компактний комп'ютер, розроблений Intel. Він є мініатюрною системою, що містить процесор, оперативну пам'ять, накопичувач та інші компоненти в одному корпусі. Intel NUC підтримує операційні системи Windows і Linux і може використовуватися як домашній медіацентр, мінісервер або настільний комп'ютер. Наприклад, мінікомп'ютер Intel NUC 13 Extreme Kit – NUC13RNGi7, Desktop, PC Barebone, Intel Z690, LGA 1700, DDR-SDRAM, PCI Express, Serial ATA III вартістю на сьогодні близько 1600 євро має технологію віртуалізації Intel® Directed-I/O (VT-d), налаштовану на найкраще забезпечення підтримки віртуальних програм для IA-32 (VT-x) і системи з процесором Itanium® (VT-i), покращує цю функцію для нового обладнання die I/O-Gerätevirtualisierung. Intel VT-d kann Benutzern helfen, die Sicherheit und Zuverlässigkeit von Systemen sowie die Leistung von I/O-Geräten in virtualisierten Umgebungen zu verbessern (рис. 1.5).



Рис. 1.5. Мінікомп'ютер Intel NUC 13 Extreme Kit - NUC13RNGi7

Міні РС. Існує безліч різних виробників, які пропонують мінікомп'ютери під маркою Mini PC. Ці пристрої зазвичай мають невеликий форм-фактор⁴ і можуть бути оснащені різними процесорами, оперативною пам'яттю і накопичувачами. Вони можуть бути використані як комп'ютер для офісних завдань, мультимедійного центру або навіть ігрової консолі.

Chromebox – це мінікомп'ютер, який працює на операційній системі Chrome OS від Google. Він призначений для використання вебдодатків і хмарних сервісів. Chromebox може бути використаний як комп'ютер для виконання простих завдань, таких як інтернет-серфінг, електронна пошта та офісні програми. Наприклад, мінікомп'ютер 90MS0252-M00970 ASUS Chromebox 4 G5007UN Mini-PC Core i5 10210U / 1.6 GHz вартістю на сьогодні близько 1000 євро має RAM 8 GB-SSD 128 GB-UHD Graphics-GigE-WLAN: Bluetooth 5.0-802.11a/b/g/n/ac/ax-Chrome OS-Монітор: keiner-Gun Metal (рис. 1.6).



Рис. 1.6. 90MS0252-M00970 ASUS Chromebox 4 G5007UN
Mini-PC Core i5 10210U / 1.6 GHz

⁴ Форм-фактор – типорозмір материнської плати. Це означає, що в певний корпус можна вставити лише певне устаткування.

Це лише деякі приклади малогабаритних комп'ютерів, і ринок пропонує різноманітні варіанти з різними характеристиками та можливостями, щоб задовольнити потреби користувачів.

Базовою апаратною конфігурацією персонального комп'ютера називають мінімальний комплект апаратних засобів, достатній для початку роботи з комп'ютером, який можна гнучко змінювати відповідно до вимог користувача. Базовою конфігурацією персонального комп'ютера є наявність таких пристроїв: системний блок, монітор, клавіатура, миша. Додатково можуть підключатися інші пристрої: вентилятори охолодження, вебкамера, блок живлення, звукові колонки, принтер, сканер та ін.

Пристрої, що знаходяться всередині системного блока, називають *внутрішніми*, а пристрої, що підключаються до нього зовні, – *зовнішніми* (рис. 1.7).



Рис. 1.7. Структурна схема сучасного персонального комп'ютера базової конфігурації, побудованого за принципом фон Неймана

Внутрішні пристрої

Системний блок являє собою основний вузол, усередині якого встановлені найбільш важливі компоненти персонального комп'ютера. Системний блок захищає внутрішні компоненти від зовнішнього впливу і механічних пошкоджень, підтримує необхідний температурний режим усередині, екранує створюване внутрішніми компонентами електромагнітне випромінювання. Є основою для подальшого удосконалення системи.

До складу системного блока обов'язково входять п'ять пристроїв (рис. 1.8): материнська плата, процесор (CPU), оперативна пам'ять, пам'ять на жорсткому диску (HDD), відеокарта.



Рис. 1.8. Основні внутрішні пристрої системного блока:

1 – блок живлення; 2 – материнська плата; 3 – кулер; 4 – слоти для оперативної пам'яті; 5 – відеокарта; 6 – HDD; 7 – CD-DVD привод

Материнська плата персонального комп'ютера – один з найважливіших модулів комп'ютера, що входять до складу системного блока. Материнська плата (motherboard), або системна плата (system board), – центральна комплексна плата, що забезпечує електронний і логічний зв'язок між усіма пристроями, що входять до складу персонального комп'ютера (рис. 1.9).

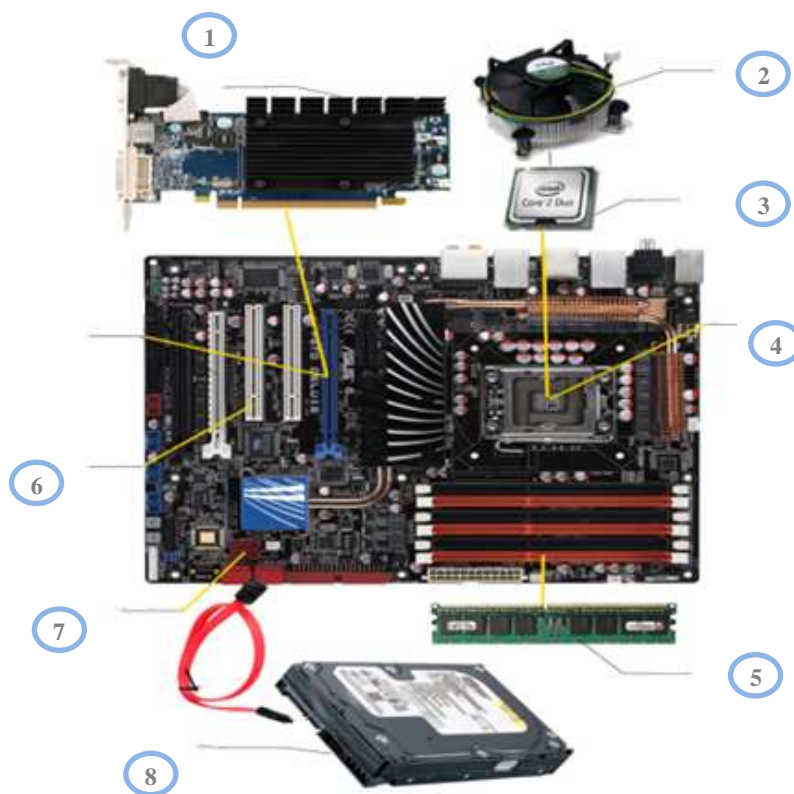


Рис. 1.9. Персональний комп'ютер у розрізі: 1 – відеокарта; 2 – кулер;
 3 – центральний процесор; 4 – роз'єм для процесора Socket;
 5 – модуль ОЗП; 6 – роз'єм PCI; 7 – роз'єм SATA; 8 – жорсткий диск

На материнській платі розташовуються основні елементи комп'ютера:

- *процесор* (CPU – Central Processing Unit – центральний обчислювальний пристрій, центральний процесор) – встановлюється в спеціальний роз'єм типу сокет, що дає змогу замінити процесор без спеціального інструменту (рис. 1.10, 1.11);

- *чипсет* (chipset) або набір чипів (мікросхем) – управляє взаємодією процесора з іншими пристроями. Чипсет повністю визначає всі потенційні можливості материнської плати: використовуваний процесор, тип і обсяг пам'яті, допустимі периферійні пристрої;

- *системна* шина (system bus) – електричні з'єднання, за допомогою яких пристрої комп'ютера обмінюються сигналами один з одним. Усі зовнішні пристрої підключаються до шини безпосередньо через відповідні

уніфіковані роз'єми (слоти) або специфічні адаптери (контролери). Швидкість (пропускна здатність) системної шини впливає на швидкість роботи комп'ютера;



Рис. 1.10. Материнська плата



Рис. 1.11. Роз'єм для установлення центрального процесора (сокет, socket)

– мікросхема постійної пам'яті (ROM – Read Only Memory – пам'ять тільки для читання) – містить набір основних параметрів комп'ютера, необхідних для спільної роботи всіх його пристроїв, і базову систему введення/виведення (Basic Input Output System – BIOS). Вміст постійної пам'яті підтримується живленням від спеціальної батарейки;

– оперативна пам'ять (RAM – Random Access Memory – пам'ять з довільним доступом) – реалізується у вигляді модулів з мікросхемами динамічної пам'яті, які вставляються в спеціальні роз'єми на материнській платі (слоти на рис. 1.12);



Рис. 1.12. Роз'єми (слоти) для установлення модулів оперативної пам'яті

– *кеш-пам'ять* (cache) – дуже швидка (надоперативна) пам'ять, що містить інформацію, необхідну процесору в першу чергу;

– *додаткові мікросхеми* (additional chips) – виконують специфічні функції, наприклад вбудований у материнську плату звуковий чип.

Крім того, материнська плата містить спеціальні роз'єми (слоти) для підключення різних додаткових пристроїв, наприклад відеокарти, звукової, мережевої карти. Стандартизовані інтерфейси материнської плати (порти) служать для підключення периферійного обладнання – принтери, сканери, зовнішні пристрої, що запам'ятовують, тощо (рис. 1.13).



Рис. 1.13. Порти введення/виведення

Для збільшення продуктивності системи використовуються локальні шини (local bus), що зв'язують процесор безпосередньо з контролерами периферійних пристроїв і тим самим збільшують загальну швидкодію персонального комп'ютера.

Для відведення тепла, що виділяється при роботі процесора, застосовується кулер – система охолодження процесора, що являє собою систему з тепловідводного радіатора і вентилятора. З часом поняття базової конфігурації поступово змінюється. Корпуси персональних комп'ютерів поставляються разом з блоком живлення, а отже, потужність блока живлення вже стає одним із параметрів корпусу. У сучасних моделей потужність блока живлення становить до 700 Вт.

Зовнішні пристрої

Крім обов'язкових, сучасний персональний комп'ютер може містити різні додаткові пристрої, що в основному підключаються до системного блока через відповідні роз'єми.

Інші пристрої введення та виведення (Input/Output) – це компоненти комп'ютерної системи, призначені для введення даних у комп'ютер і виведення результатів роботи комп'ютера користувачеві.

Пристрої введення

Клавіатура – клавійний пристрій управління персональним комп'ютером, служить для введення алфавітно-цифрових (знакових) даних, а також команд управління. Комбінація монітора і клавіатури забезпечує найпростіший інтерфейс користувача. За допомогою клавіатури користувач управляє комп'ютерною системою, а за допомогою монітора отримує від неї відгук.

Миша – пристрій управління манипуляторного виду. Комбінація монітора і миші забезпечує найбільш сучасний тип інтерфейсу користувача, що називається графічним.

Сенсорний екран – дає змогу користувачеві взаємодіяти з комп'ютером, торкаючись і проводячи пальцем по екрану.

Сканер – використовується для читання та цифрового введення текстових або графічних зображень.

Мікрофон – дає змогу записувати аудіосигнали, наприклад для голосового введення.

Пристрої виведення

Монітор – пристрій візуального подання даних, є головним пристроєм виведення.

Принтер – дає змогу друкувати текстові документи, фотографії та інші матеріали.

Динаміки або навушники – використовуються для відтворення звукових сигналів, музики, мовлення та інших аудіофайлів.

Проектор – виводить зображення на великий екран або стіну, використовується для презентацій чи перегляду відео.

Жорсткий диск або SSD – пристрої зберігання, що виводять інформацію в цифровій формі для читання користувачем.

Це лише деякі з багатьох пристроїв введення та виведення, що можуть використовуватися в комп'ютерних системах. Різноманітність пристроїв введення/виведення дає змогу користувачам ефективно взаємодіяти з комп'ютером та отримувати результати своєї роботи.

Підключення пристроїв введення та виведення може відрізнитися залежно від типу пристрою та його інтерфейсу. Ось деякі загальні способи підключення.

USB. Більшість периферійних пристроїв зараз підключаються через інтерфейс USB (Universal Serial Bus). Для підключення пристрою введення або виведення через USB достатньо вставити відповідний конектор у вільний порт USB на комп'ютері або іншому пристрої.

Bluetooth. Якщо пристрій має функцію Bluetooth, його можна підключити до комп'ютера або іншого пристрою через бездротове з'єднання. Необхідно переконатися, що функція Bluetooth увімкнена на обох пристроях, а потім виконати процедуру зв'язку, що може змінюватись залежно від операційної системи.

Wi-Fi. Деякі пристрої введення та виведення, такі як мережеві принтери або розумні колонки, можуть підключатися до мережі Wi-Fi. Для

цього необхідно налаштувати з'єднання з Wi-Fi за допомогою відповідного програмного забезпечення або інтерфейсу на пристрої.

HDMI, DisplayPort або VGA. Для підключення моніторів, проєкторів або телевізорів до комп'ютера чи ноутбука використовуються різні види відеоінтерфейсів, таких як HDMI (High-Definition Multimedia Interface), DisplayPort або VGA (Video Graphics Array). Необхідно використовувати відповідний кабель для підключення пристрою виведення до комп'ютера або іншого джерела відеосигналу.

Аудіороз'єм. Для підключення аудіопристроїв, таких як навушники, динаміки або мікрофони, використовуються аудіороз'єми. Залежно від пристрою та комп'ютера або аудіоплеєра можуть використовуватися різні типи аудіороз'ємів, такі як роз'єм 3,5 мм для навушників або XLR-роз'єм для професійних мікрофонів.

Порти розширення. Деякі пристрої введення та виведення можуть потребувати підключення через спеціалізовані порти розширення. Наприклад, зовнішні звукові карти можуть бути підключені до комп'ютера через порт PCI або USB, а зовнішні відеокарти можуть потребувати підключення через порт Thunderbolt або PCI Express. Це лише деякі загальні способи підключення пристроїв введення та виведення. Важливо враховувати специфікації та інструкції виробника для кожного конкретного пристрою, щоб правильно здійснити його підключення.

1.3.2. Створення потужних суперкомп'ютерів

Суперкомп'ютери – це високопродуктивні комп'ютерні системи, спеціально розроблені для обробки величезних обсягів даних і виконання складних обчислювальних завдань. Вони використовуються в наукових і дослідних цілях, для моделювання та симуляції фізичних явищ, аналізу геномних даних, розрахунків у галузі клімату і погоди, прогнозування фінансових ринків і багатьох інших сферах, де потрібні високі обчислювальні потужності.

Ось деякі особливості суперкомп'ютерів:

1. *Висока продуктивність.* Суперкомп'ютери мають величезну обчислювальну потужність і здатні виконувати мільйони і мільярди операцій за секунду. Вони застосовуються для вирішення складних завдань, що потребують великих обчислювальних ресурсів.

2. *Паралельна обробка.* Суперкомп'ютери часто засновані на архітектурі з безліччю процесорів або ядер, що працюють паралельно, виконуючи обчислення одночасно. Це дає змогу суперкомп'ютерам значно прискорювати виконання завдань.

3. *Великий обсяг пам'яті.* Суперкомп'ютери зазвичай обладнані великим обсягом оперативної пам'яті, щоб забезпечити доступ до великих масивів даних і результатів обчислень.

4. *Спеціалізоване програмне забезпечення.* Для роботи на суперкомп'ютерах використовуються спеціальні програми та бібліотеки, оптимізовані для високопродуктивних обчислень. Вони дають змогу ефективно використовувати ресурси суперкомп'ютера та управляти розподілом завдань на процесори [14].

5. *Охолодження.* Суперкомп'ютери генерують величезну кількість тепла, тому для їхньої роботи потрібна ефективна система охолодження, щоб запобігти перегріву компонентів.

Приклади суперкомп'ютерів включають системи Summit та Sierra, розроблені в США, Fugaku – Японія, Tianhe-2A – Китай та ін. Ці системи є потужними інструментами для виконання складних обчислень і знаходять застосування в багатьох галузях науки, інженерії та досліджень.

Сучасний суперкомп'ютер – потужний комп'ютер з продуктивністю кілька мільярдів операцій з рухомою крапкою за секунду. Він являє собою багатопроцесорний і/або багатомашинний комплекс, що працює на загальну пам'ять і загальне поле зовнішніх пристроїв.

Багатоядерний процесор – це багатопроцесорна система, реалізована на кристалі, що забезпечує підвищення ефективності роботи обчислювальної системи в цілому.

Реальним шляхом розвитку комп'ютерів є масове застосування багатоядерних систем – одночасне використання в одній електронно-обчислювальній машині декількох процесорів.

Поступово вони стають основною платформою серверів, настільних комп'ютерів, ноутбуків, вбудованих систем тощо. Для вимірювання потужності суперкомп'ютера використовують таке поняття, як *флонс* (англ. Floating-point Operations Per Second, FLOPS) – позасистемна одиниця, використовувана для вимірювання продуктивності комп'ютерів, що показує, скільки операцій з рухомою комою за секунду виконує ця обчислювальна система. *Петафлонс* – тисяча трильйонів операцій з рухомою комою за секунду.

За рахунок чого вдається підвищити продуктивність комп'ютерів?

По-перше, необхідно враховувати прогрес у розвитку елементарної бази електронно-обчислювальних машин.

По-друге, і це, мабуть, є більш вагомим внеском у підвищення продуктивності комп'ютерів, розвиток архітектури, перш за все завдяки впровадженню ідеї паралелізму.

Наприклад, порівняємо суперкомп'ютери EDSAC 1949 року та Cray Titan 2012 року.

У 1949 році EDSAC мав тактову частоту $2 \cdot 10^6$ с і продуктивність 10^2 операцій/с.

У 2012 році Cray Titan мав тактову частоту $4,5 \cdot 10^{10}$ с (2.2 GHz) і продуктивність $1,7 \cdot 10^{16}$ операцій/с.

Підвищення параметрів становлять за тактовою частотою приблизно $4,4 \cdot 10^3$ с, а продуктивністю приблизно $1,7 \cdot 10^{14}$ операцій/с.

Наприклад, Tianhe-2A, також відомий як Milky Way-2A, є суперкомп'ютером, розробленим і побудованим у Китаї на основі власної архітектури, оснащеним процесорами Matrix-2000 і прискорювачами Galaxu-2. Tianhe-2A був розроблений і розгорнутий у Національному суперкомп'ютерному центрі Гуанчжоу і широко застосовується в різних галузях: наукові дослідження, моделювання, економіка та прогнозування.

Наприклад, Summit та Sierra (США) є двома високопродуктивними суперкомп'ютерами, розробленими та побудованими у Сполучених Штатах. Обидва суперкомп'ютери побудовані на архітектурі IBM POWER і оснащені графічними процесорами NVIDIA. Summit був розроблений для використання в національній лабораторії Оак-Рідж, а Sierra – лабораторії Лос-Аламос. Обидва суперкомп'ютери призначені для виконання складних обчислювальних завдань і досліджень у різних галузях: кліматологія, фізика високих енергій та матеріалознавство.

Наведемо ще один приклад. Найпотужнішим суперкомп'ютером у червні 2021 року стала система Fugaku (Supercomputer Fugaku, A64FX 48C 2.2GHz), що розроблена японськими організаціями RIKEN і Fujitsu і має потужність 442,01 петафлопса (табл. 1.2). Він побудований на основі архітектури ARM і має 48-ядерні однокристальні ARM-системи Fujitsu A64FX; загальна вількість ядер у суперкомп'ютері – майже 7,3 млн [21]. Процесори A64FX розроблені спеціально для цього суперкомп'ютера. Fugaku займає лідируючі позиції у світових рейтингах суперкомп'ютерів і застосовується для різних завдань: кліматичне моделювання, медичні дослідження, аеродинаміка тощо.

На сьогодні суперкомп'ютери є унікальними системами, створеними світовими лідерами комп'ютерного ринку, такими як IBM, Hewlett-Packard, NEC та іншими, що об'єднали досвід і технології ранніх компаній. Ці суперкомп'ютери є відомими технологічними досягненнями в галузі обчислювальної потужності і широко використовуються для вирішення складних наукових, інженерних і суспільних завдань.

Порівняння продуктивності суперкомп'ютерів

Продуктивність суперкомп'ютерів		
Назва	Рік	Flops
Флопс	1941	10^0
Кілофлопс	1949	10^3
Мегафлопс	1964	10^6
Гігафлопс	1987	10^9
Терафлопс	1997	10^{12}
Петафлопс	2008	10^{15}
Ексафлопс	2020	10^{18}
Зетафлопс	–	10^{21}
Йотафлопс	–	10^{24}

1.4. Покоління архітектури в парадигмі програмування

Hardware вплив на розвиток мереж

Апаратні засоби (hardware) – це фізичні компоненти, необхідні для функціонування системи, тому можна сказати, що *комп'ютер* – це нерозривне поєднання *харду* (залізо) і *софту* (програми), де *хард* (англ. *hardware* – *апаратне забезпечення*, жаргон – *залізо*) – електронні та механічні частини обчислювального пристрою, що входять до складу системи або мережі, без програмного забезпечення і даних, а *софт* (англ. *software* – *програмне забезпечення*) – програми, процедури, правила та відповідна документація за системою обробки інформації.

Без програмного забезпечення комп'ютер буде просто залізом, що має інтерес тільки для вчених, відповідно без апаратного забезпечення саме програмне забезпечення є нематеріальною субстанцією у вигляді записів програмістів або їхніх «геніальних» думок, які в такому нематеріальному вигляді не цікавлять широке коло користувачів.

Із формули «комп'ютер = hard + software» випливає, що несправність комп'ютера може бути пов'язана як з hard, так і software. Наприклад, якщо вінчестер технічно вийшов з ладу, то жодна програма не здатна це виправити, потрібно реставрувати жорсткий диск.

З урахуванням останніх тенденцій комп'ютер можна розглядати як будь-який пристрій для виходу в Інтернет і хмарні технології.

Суть хмарних технологій полягає в тому, що користувач може працювати в режимі онлайн з необхідними йому програмами і працювати з файлами незалежно від можливостей обладнання, на якому він буде працювати. При цьому потужність комп'ютера практично не відіграє ролі, тому що комп'ютер забезпечує тільки зв'язок «з хмарою», а над хмарними завданнями працюють потужні сервери постачальника хмарних послуг.

Завдяки цим хмарним технологіям ви можете опрацьовувати документи і виконувати роботу в Інтернеті, використовуючи надані постачальником потужності, а результати зберігати також не витрачаючи власні ресурси.

Отже, хмарні онлайн-технології дають нам можливість:

– користуватися потрібними нам програмами без установлення їх на свій комп'ютер або інший пристрій із виходом в Інтернет (звідси і назва «онлайн-додатки» або «онлайн-програми»);

– зберігати свої файли, документи та інші дані в інтернеті (звідси і назва «хмарне сховище»).

Потрібна нам онлайн-програма ніби «ширяє в хмарі», при цьому на перший план виходить підключення до інтернету, а апаратна частина комп'ютера для роботи з цим додатком відходить на другий план. Уже скоро використання хмарних технологій дасть реальну можливість, почавши роботу вдома на ноутбуці, продовжити її виконувати з телефона перебуваючи в дорозі, а завершити її виконання на роботі, використовуючи робочий персональний комп'ютер.

Але поки що ця система має доопрацьовуватися, тому що, як і будь-яка система, має власні недолік:

– вузьким місцем будь-якої системи є її безпекова частина. Конфіденційність особистої інформації, що зберігається в хмарах, потребує ще довго та копіткого доопрацювання. Хоча можна сказати, що будь-який технічний пристрій, підключений до інтернету, також може легко стати жертвою інформаційних шахраїв;

– нестабільний інтернет або його відсутність, наприклад у дорозі, кафе, спортзалі або отелі, де використовується бездротовий Інтернет загального користування, може зіпсувати роботу, і всі наші розробки в «хмарах» стануть для нас недоступними;

– ще однією причиною для хвилювання може стати введення або збільшення плати за користування хмарою власником, а в разі неможливості платежу можна втратити всі напрацювання.

Відсутність або нестабільний інтернет чи введення або збільшення плати за користування хмарою власником можна уникнути, якщо своєчасно дублювати інформацію та оплачувати витрати на роботу у хмарному середовищі.

Активне впровадження багатоядерних систем розуміє істотну зміну стилю програмування: розробники змушені використовувати паралельні потоки, породження і обробку асинхронних подій тощо. Іншими словами, нова апаратна архітектура потребує зміни програмної парадигми – переходу від послідовного стилю програмування до паралельного, що пов'язано зі значними перешкодами.

Паралельна обробка. *Розпаралелювання потоку команд.* Розвиток багатоядерних систем – це шлях до повсюдного використання паралельних обчислень. При цьому найбільш поширеним способом підвищення продуктивності є розпаралелювання потоку команд або потоку даних.

Розпаралелювання потоку команд є мірою того, як безліч операцій в комп'ютерній програмі може виконуватися одночасно.

Є два підходи до виявлення паралелізму на рівні команд:

– **апаратні засоби** – виявленням паралелізму в потоці операцій займаються спеціальні схеми процесора при виконанні коду програм;

– **програмне забезпечення** – виявленням паралелізму займається компілятор, що формує виконуваний код програми під спеціальний процесор.

Розпаралелювання потоку даних – це застосування однієї операції одразу до кількох елементів масиву даних. Паралелізм завдань передбачає розбиття обчислювального процесу на кілька підзадач (процесів, потоків), кожна з яких виконується на своєму ядрі (процесорі). Кілька програмних гілок виконуються одночасно і незалежно, але в певні моменти вони обмінюються даними.

Піонером у паралельній обробці потоків даних був О. А. Самарський, який виконував на початку 1950-х років розрахунки, необхідні для моделювання ядерних вибухів, і розв'язав цю задачу, посадивши кілька десятків людей з арифмометрами за столи, які передавали дані один одному просто на словах і відкладали необхідні цифри на арифмометрах. Отже, було розраховано розповсюдження вибухової хвилі. Роботи було багато, люди втомлювалися, а Олександр Андрійович ходив між ними і підбадьорював. Це, можна сказати, і була перша паралельна система. Тож розрахунки були майстерно проведені, але їхня точність була дуже низькою, тому що вузлів у використовуваній сітці було мало, а часу для розрахунків витрачалося занадто багато.

Паралельна обробка даних умовно має два різновиди ідеї одночасного виконання кількох дій: **конвеєрність** і **власне паралельність**.

Щоб розпаралелити програму, потрібно знайти в ній інформаційно незалежні операції, розподілити їх між обчислювальними пристроями і

забезпечити їхню синхронізацію і комунікацію. Іншими словами, щоб написати паралельну програму, потрібно виділити в ній частини, які можуть одночасно обчислюватися різними функціональними пристроями.

Наприклад, для складання двох дійсних чисел, поданих у формі з рухомою комою, потрібно безліч дрібних операцій – порівняння порядків, вирівнювання порядків, складання мантис, нормалізація тощо. Перші процесори для кожної пари аргументів виконували операції послідовно, одна за одною, поки не доходили до остаточного результату, і лише після цього переходили до обробки наступної пари доданків.

Якщо якийсь пристрій виконує одну операцію за одиницю часу, то тисячу операцій воно виконає за тисячу одиниць. Якщо припустити, що є п'ять таких самих незалежних пристроїв, здатних працювати одночасно, то тисячу операцій система з п'яти пристроїв може виконати вже за двісті одиниць часу. Аналогічно, системі з N пристроїв на ту саму роботу знадобиться $1000/N$ одиниць часу. Однак це ідеальний випадок, від якого реальність буває дуже далекою.

Можливість розбиття програми на частини визначається наявністю або відсутністю в ній справжніх інформаційних залежностей, коли результат виконання однієї операції використовується як аргумент в іншій операції.

Конвеєрна обробка (конвеєризація) заснована на поділі функцій, що підлягають виконанню, на більш дрібні частини (ступені) і виділенні для кожної з них окремої частини апаратури.

Конвеєрна обробка машинних команд – спосіб їх виконання процесором, при якому виконання наступної команди починається до повного закінчення виконання попередньої команди.

Можливість такої обробки пов'язана з поділом процесу виконання команд на послідовні етапи:

- вибір команди – IF (за адресою, заданою лічильником команд, з пам'яті витягується команда);
- декодування команди / вибір операндів з регістрів – ID;

- виконання операцій / обчислення ефективної адреси пам'яті – EX;
- звернення до пам'яті – MEM;
- запам'ятовування результатів – WB,

і організацією передавання даних від одного етапу до наступного з одночасним прийманням нової порції вхідних даних.

Отримуємо очевидний *виграш у швидкості обробки за рахунок суміщення раніше рознесених у часі операцій*. При цьому конвеєрну обробку можна використовувати для поєднання етапів виконання різних команд. Продуктивність при цьому зростає завдяки тому, що одночасно на різних ступенях конвеєра виконуються декілька команд.

Конвеєризація збільшує і пропускну здатність процесора (кількість команд, що завершуються в одиницю часу), але і вона не скорочує час виконання окремої команди. *Насправді вона навіть трохи збільшує час виконання кожної команди через накладні витрати, пов'язані з управлінням реєстровими станціями*. Однак збільшення пропускну здатності означає, що програма буде виконуватися швидше порівняно з простою неконвеєрною схемою.

Здавалося б, конвеєрну обробку можна з успіхом замінити паралельною, для чого продублювати основний пристрій стільки разів, скільки ступенів конвеєра передбачається виділити. Однак вартість і складність системи, що вийшла, буде непорівнянна з вартістю і складністю конвеєрного варіанта, а продуктивність виявиться майже такою самою, а то й гірше.

Наприклад, уявіть, що на автозаводі замінили сто етапів збирання машини сотнею бригад, які збирають кожен автомобіль від початку до кінця. Які ж будуть витрати на зарплату працівникам такої високої кваліфікації і оснащення їхніх робочих місць?

Використовуючи паралельну систему з N обчислювальними пристроями, ми, зрозуміло, очікуємо отримати прискорення виконання програми в N разів порівняно з послідовним варіантом. Але дійсність майже завжди виявляється далекою від ідеалу.

Наприклад, один землекоп за одну годину може викопати яму об'ємом один кубометр. Два землекопи, працюючи разом, викопують таку саму яму за пів години. А шістдесят землекопів? Зрозуміло, що вони будуть просто заважати один одному і швидше процес не відбуватиметься.

Сьогодні тільки невелика частина програмного забезпечення може використовувати весь потенціал багатоядерних процесорів, що підтверджують результати тестів синтетичних і призначених для конкретних класів додатків. *Реальне зростання продуктивності дають лише програми, оптимізовані під багатопотоковість.*

1.4.1. Векторно-конвеєрні комп'ютери. Історія виникнення

Середина 1970-х років. *Конвеєрні функціональні пристрої і набір векторних команд – дві головні особливості таких машин.* На відміну від традиційного підходу, векторні команди оперують цілими масивами незалежних даних, що дає змогу ефективно завантажувати доступні конвеєри, тобто команда вигляду $A = B + C$ може означати додавання двох масивів, а не двох чисел. Cray Fortran – перший компілятор з Fortran векторизацією (рис. 1.14).



Рис. 1.14. Суперкомп'ютер Cray 1

1.4.2. Векторно-паралельні комп'ютери

Початок 1980-х років. *Оперативна пам'ять таких комп'ютерів розподіляється декількома однаковими процесорами, завдяки чому знімаються проблеми попереднього класу, але додаються нові – кількість процесорів, що мають доступ до загальної пам'яті, з чисто технічних причин не можна зробити великою.*

Програмування – векторизація внутрішніх процедур і розпаралелювання на зовнішньому рівні, єдиний адресний простір, локальні і глобальні змінні (рис. 1.15).



Рис. 1.15. Суперкомп'ютери Cray X-MP, Cray Y-MP

1.4.3. Масивно-паралельні комп'ютери з розподіленою пам'яттю

Початок 1990-х років. Ідея побудови комп'ютерів цього класу тривіальна: візьмемо тисячу серійних мікропроцесорів, забезпечимо кожен своєю локальною пам'яттю і з'єднаємо за допомогою деякого комунікаційної середовища з певною топологією.

Програмування – обмін повідомленнями, відсутність єдиного адресного простору.

Переваг у такої архітектури багато: якщо потрібна висока продуктивність, можна додати ще процесорів; обмежені фінанси або

заздалегідь відома потрібна обчислювальна потужність – легко підібрати оптимальну конфігурацію тощо.

Однак є і серйозний недолік, який перекреслює більшість переваг. Справа в тому, що міжпроцесорний обмін у комп'ютерах цього класу здійснюється набагато повільніше локальної обробки даних самими процесорами. Саме тому написати ефективну програму для таких комп'ютерів дуже складно, а для деяких алгоритмів іноді просто неможливо. До цього класу можна віднести комп'ютерні мережі – дешева альтернатива вкрай дорогим суперкомп'ютерам (рис. 1.16).



Рис. 1.16. Суперкомп'ютер Cray T3D

1.4.4. Паралельні комп'ютери з загальною пам'яттю

Середина 1990-х років. *Особливість архітектури* – сотні процесорів об'єднуються загальною пам'яттю.

Програмування – єдиний адресний простір, локальні і глобальні змінні, OpenMP. Являє собою комбінації трьох попередніх (рис. 1.17).

Унікальні рішення з рекордними характеристиками зазвичай недешеві, тому і вартість подібних систем ніяк не могла бути порівняна з вартістю систем, що знаходяться в масовому виробництві і широко використовуються в бізнесі.



Рис. 1.17. Dec ALphaServer

Прогрес у галузі мережевих технологій зробив свою справу: з'явилися недорогі, але ефективні рішення, засновані на комунікаційних технологіях. З декількох процесорів (традиційних або векторно-конвеєрних) і загальної для них пам'яті сформуємо обчислювальний вузол. Якщо отриманої обчислювальної потужності недостатньо – об'єднаємо декілька вузлів високошвидкісними каналами. Подібну архітектуру називають *класстерною* (рис. 1.18).

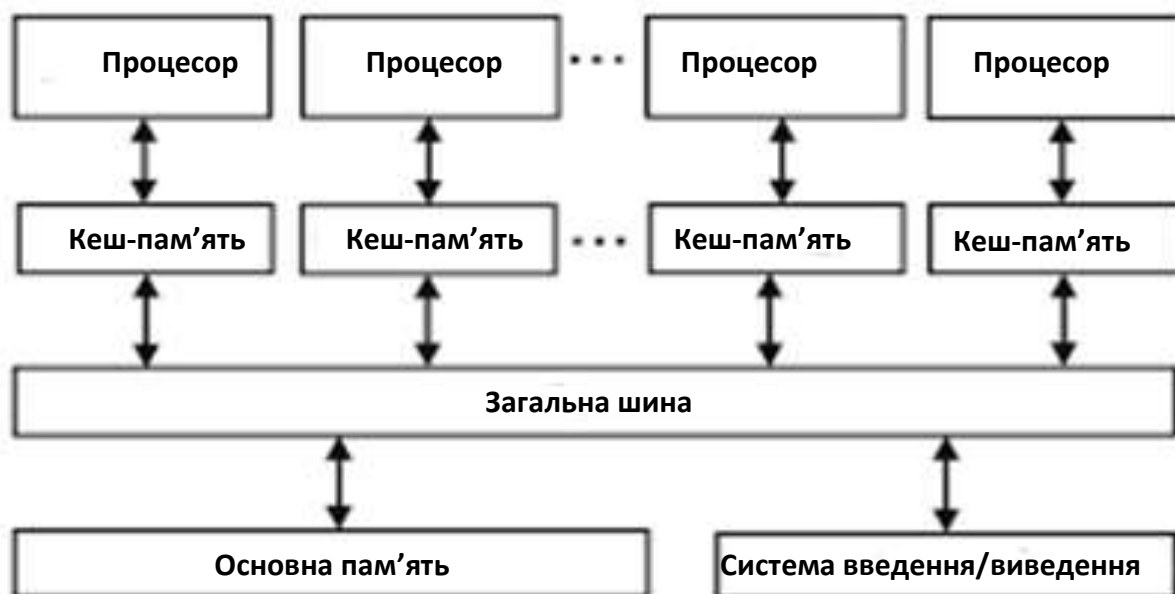


Рис. 1.18. Симетричні мультипроцесорні системи

Кластери. Обчислювальний кластер – це сукупність комп'ютерів, об'єднаних у рамках деякої мережі для вирішення великого обчислювального завдання. Як вузли зазвичай використовуються доступні однопроцесорні комп'ютери, двопроцесорні або чотирипроцесорні SMP-сервери (Symmetric Multiprocessing). Кожен вузол працює під управлінням своєї копії операційної системи, для якої найчастіше використовуються стандартні операційні системи Linux, NT, Solaris тощо. У чотирипроцесорних SMP-серверах кожен процесор має доступ до спільної пам'яті та периферійних пристроїв. Це означає, що всі процесори можуть виконувати завдання одночасно та обмінюватися даними без необхідності синхронізації чи координації через зовнішні засоби зв'язку.

Склад і потужність вузлів може змінюватися навіть у рамках одного кластера, даючи можливість створювати великі гетерогенні (неоднорідні) системи з заданою потужністю.

Вибір конкретного комунікаційного середовища визначається багатьма факторами: особливостями класу вирішуваних завдань, доступним фінансуванням, необхідністю подальшого розширення кластера тощо.

Оскільки кластерне рішення дає змогу досягти найкращого співвідношення ціни і продуктивності, саме воно є в певний час найбільш перспективним для конструювання комп'ютерів з рекордними показниками продуктивності.

Переваги чотирипроцесорних SMP-серверів:

1. Збільшення загальної обчислювальної потужності – за допомогою чотирьох процесорів сервер може виконувати більш складні та вимогливі завдання, прискорюючи загальну продуктивність системи.

2. Легкість розпаралелювання задач – SMP-сервери дають змогу легко розподіляти задачі між кількома процесорами і, отже, ефективно використовувати потужність кожного процесора для прискорення виконання завдань.

3. Підвищена надійність. Якщо один із процесорів виходить з ладу, інші процесори можуть продовжити роботу без простоїв. Це забезпечує більш високу доступність і відмовостійкість системи.

4. Гнучкість і масштабованість – SMP-сервери можуть бути легко масштабовані шляхом додавання додаткових процесорів для збільшення обчислювальних потужностей.

Чотирипроцесорні SMP-сервери широко застосовуються у сфері високонавантажених обчислень, таких як бази даних, вебсервери, наукові та інженерні розрахунки, де потрібна обробка великих обсягів даних і паралельне виконання безлічі завдань одночасно.

Кластерне рішення на чотирипроцесорному SMP-сервері може бути реалізовано шляхом об'єднання декількох таких серверів в обчислювальний кластер. Кожен сервер у кластері матиме чотири процесори, що забезпечить більш високу обчислювальну потужність і можливість розпаралелювання завдань.

Ось приклад можливої архітектури кластерного рішення на чотирипроцесорних SMP-серверах [14]:

- вибір операційної системи. На кожному сервері встановлена операційна система, що підтримує кластерні рішення, наприклад Linux з підтримкою кластеризації (наприклад Red Hat Enterprise Linux або SUSE Linux Enterprise Server);

- мережеве підключення. Кожен сервер у кластері підключений до загальної високошвидкісної мережі, наприклад за допомогою гігабітного Ethernet або InfiniBand. Це забезпечує високу пропускну здатність і низьку затримку між серверами;

- кластерне програмне забезпечення. Встановлення та налаштування програмного забезпечення для управління кластером, наприклад OpenMPI або Intel MPI. Це дає змогу програмам розпаралелюватися та виконувати обчислення на кількох процесорах у кластері;

– планувальник завдань. У кластері може бути налаштований планувальник завдань, що розподіляє роботу між доступними процесорами. Це дає змогу ефективно використовувати ресурси кластера та балансувати навантаження;

– зберігання даних. Для забезпечення доступу до загальних даних у кластері може бути використане мережеве сховище даних, таке як Network File System (NFS) або паралельна файлова система (наприклад Lustre);

– розподілене виконання завдань [14]. Програми мають бути розроблені так, щоб виконуватися на кількох процесорах у кластері паралельно. Кластерне програмне забезпечення розподіляє завдання між процесорами та забезпечує синхронізацію даних і комунікацію між ними.

Таке кластерне рішення на чотирипроцесорних SMP-серверах дає змогу досягти більш високої обчислювальної потужності та паралелізму щодо завдань, які потребують інтенсивних обчислень або обробки великих обсягів даних.

Кластери з вузлів із загальною пам'яттю. Початок 2000-х років. Особливості архітектури – велика кількість багатопроцесорних вузлів об'єднуються разом за допомогою комунікаційної мережі за деякою топологією, розподілена пам'ять; у рамках кожного вузла кілька багатоядерних процесорів об'єднуються загальною пам'яттю.

Кластери з вузлів із загальною пам'яттю – це архітектурна конфігурація в розподілених системах, де кожен вузол у кластері має доступ до спільної пам'яті. Це відрізняється від архітектури з розподіленою пам'яттю, де кожен вузол має власну локальну пам'ять.

У кластерах із загальною пам'яттю вузли з'єднані мережею і мають можливість обмінюватися даними безпосередньо через загальну пам'ять. Це дає змогу розподіленим процесам взаємодіяти і спільно використовувати дані без необхідності явного обміну повідомленнями.

Кластери з загальною пам'яттю часто використовуються для паралельних обчислень, де великі обсяги даних можуть бути ефективно розподілені між вузлами та оброблені паралельно. Вони також можуть бути корисними для розподіленої бази даних, де доступ до даних має бути швидким і низьколатентним.

Приклади архітектур, що підтримують кластери з загальною пам'яттю, включають Symmetric Multiprocessor (SMP), Non-Uniform Memory Access (NUMA) і розподілені файлові системи, такі як Parallel Virtual File System (PVFS).

Однак слід зазначити, що конфігурація з загальною пам'яттю може мати свої обмеження, наприклад обмеження на пропускну здатність мережі або обмеження на масштабованість через обмежену кількість доступної спільної пам'яті. Тому вибір архітектури залежить від конкретних вимог і характеристик додатка.

Кластери з вузлів із загальною пам'яттю з прискорювачами.
Середина 2000-х років. Особливості архітектури – велика кількість багато процесорних вузлів, які об'єднуються разом за допомогою комунікаційної мережі деякої топології з використанням розподіленої пам'яті. У рамках кожного вузла встановлюють декілька багатоядерних процесорів, об'єднаних загальною пам'яттю, і кілька прискорювачів.

Прискорювач забезпечує значне підвищення пропускну здатності: скорочує час завантаження, збільшує ємність Web-вузлів, підвищує рівень безпеки, забезпечує безперервне з'єднання з клієнтами, виконує паралельну обробку запитів Web-об'єктів, а також стиснення даних для підвищення пропускну здатності вузла.

У таких кластерах вузли об'єднані у групу і мають доступ до загальної пам'яті, що дає змогу зручно обмінюватися даними між вузлами.

Прискорювачі, такі як графічні процесори (GPU) або тензорні процесори (TPU), використовуються для прискорення обчислень у

кластерах. Вони мають спеціалізовану апаратну архітектуру, що дає змогу виконувати певні операції швидше, ніж загальні центральні процесори (CPU). Прискорювачі зазвичай використовуються для обробки великих обсягів даних або виконання високопродуктивних обчислень, таких як машинне навчання, глибинне навчання або обчислювальна фізика.

У кластерах з вузлами з загальною пам'яттю і прискорювачами кожен вузол має свою локальну пам'ять, але також може мати доступ до загальної пам'яті, до якої можуть звертатися інші вузли. Це спрощує обмін даними між вузлами та дає змогу виконувати паралельні обчислення, розподіляючи завдання між вузлами.

Кластери з вузлами з загальною пам'яттю і прискорювачами використовуються у сферах із великим обсягом даних, науковими дослідженнями, кібернетиці тощо. Вони дають змогу розподіляти завдання між вузлами та використовувати прискорювачі для забезпечення високої продуктивності обчислень.

Серверні кімнати – це спеціально обладнані приміщення, призначені для розміщення та обслуговування серверного обладнання та інших мережевих компонентів. Ці кімнати створюються з урахуванням певних вимог щодо безпеки, охолодження, пожежної безпеки та електроживлення для забезпечення надійної роботи серверів.

Ось деякі особливості та компоненти серверних кімнат:

– рек-кабінети – це металеві стійки, призначені для встановлення серверів, комутаційного обладнання та інших мережевих пристроїв. Реки дають змогу ефективно використовувати простір і забезпечують зручний доступ до обладнання;

– кліматичний контроль – серверне обладнання потребує певних умов температури та вологості для нормальної роботи. У серверних кімнатах зазвичай встановлені системи кондиціонування та вентиляції, а також системи контролю вологості;

– джерело безперебійного живлення (ДБЖ) – використовується для забезпечення безперервного живлення серверів у разі вимикання основного джерела живлення. Це допомагає запобігти втратам даних і тимчасовим простоям;

– пожежна безпека – у серверних кімнатах зазвичай встановлюють системи виявлення пожежі та пожежогасіння, такі як детектори диму, вогнегасники та системи автоматичного пожежогасіння. Це допомагає захистити обладнання від пошкодження;

– фізична безпека – важливо забезпечити фізичний захист серверної кімнати від несанкціонованого доступу. Це може включати використання систем контролю доступу, відеоспостереження, а також механічних заходів безпеки, таких як замки і системи сигналізації;

– мережева інфраструктура – серверні кімнати зазвичай мають спеціальну мережеву інфраструктуру, включаючи комутатори, маршрутизатори, фаєрволи та інше мережеве обладнання, що забезпечує зв'язок між серверами та зовнішніми мережами.

Конкретні вимоги та компоненти в серверних кімнатах можуть відрізнятися залежно від потреб організації та масштабу серверної інфраструктури (рис. 1.19).



Рис. 1.19

1.5. Класифікація обчислювальних систем

М. Флінном (M. I. Flynn) була запропонована класифікація обчислювальних систем залежно від кількості використовуваних у них операційних блоків (процесорів), характеристик потоків оброблюваних даних і організації їхньої обробки (рис. 1.20) [12, 14, 15].

Організація обчислювальної системи					
Одинарний потік команд, одинарний потік даних (SISD-система)	Одинарний потік команд, множинний потік даних (SIMD-система)		Множинний потік команд, одинарний потік даних (MISD-система)	Множинний потік команд, множинний потік даних (MIMD-система)	
	Однопроцесорний комп'ютер				
	Векторна обчислювальна система	Система обробки масивів		Система з загальною пам'яттю	Система з розподіленою пам'яттю
				Симетрична мультипроцесорна система (SMP-система)	Кластери

Рис. 1.20. Класифікація обчислювальних систем залежно від кількості процесорів

Розглянемо подані на схемі (рис. 1.21) різновиди організації обчислювальних систем.

Система з одинарним потоком команд і одинарним потоком даних – SISD-система (single instruction, single data stream)

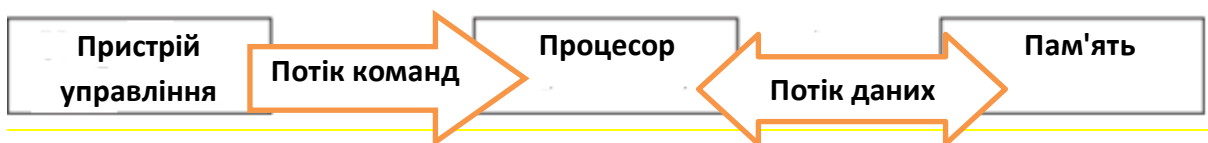


Рис. 1.21. Система з одинарним потоком команд і одинарним потоком даних

У такій системі єдиний процесор виконує єдиний потік команд з урахуванням того, що в кожен момент часу виконується одна команда, і обробляє єдиний потік використовуваних цими командами даних, які зберігаються в єдиному блоці пам'яті.

До цієї категорії належать усі класичні однопроцесорні системи.

Система з одинарним потоком команд і множинним потоком даних – SIMD-система (single instruction, multiple data stream (рис. 1.22).

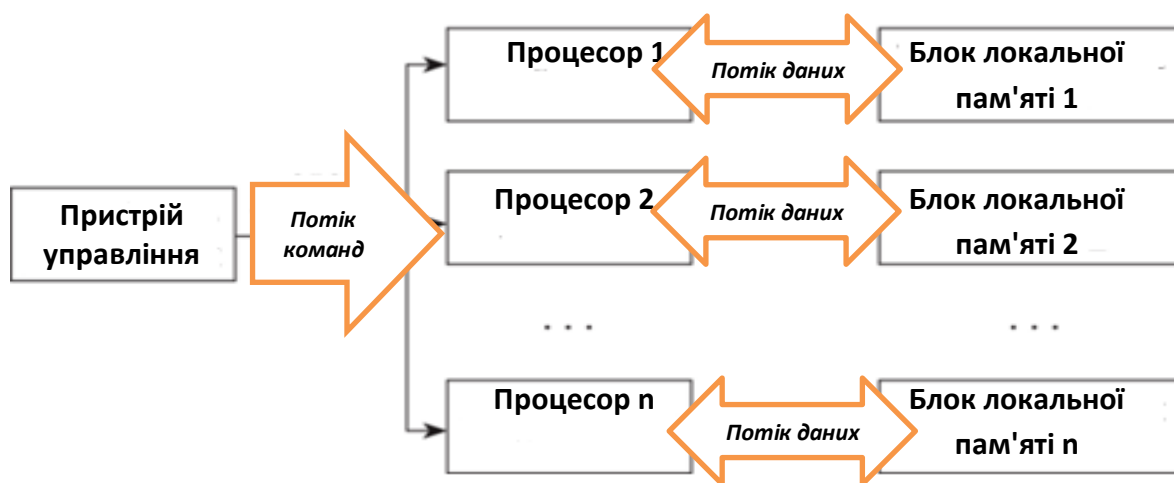


Рис. 1.22. Система з одинарним потоком команд і множинним потоком даних

У такій системі є кілька однакових процесорів, кожний з яких виконує однакову команду з єдиного потоку команд, що формується загальним для них пристроєм управління. Кожен процесор пов'язаний зі своїм блоком пам'яті даних. Тобто кожен процесор паралельно обробляє свої власні дані, але за одним і тим самим алгоритмом.

До цієї категорії обчислювальних систем належать векторні системи.

Система з множинним потоком команд і одинарним потоком даних – MISD-система (multiple instruction, single data stream)

У такій системі єдиний потік даних проходить через кілька процесорів, кожний з яких виконує свою послідовність команд. Принципово ця система дуже нагадує систему з конвеєрною обробкою, але на цей раз на кожній робочій позиції (станції) вирішується своє завдання, а не виконується етап обробки машинної команди.

Така структура досі не знайшла практичного втілення і застосування.

Система з множинним потоком команд і множинним потоком даних – MIMD-система (multiple instruction, multiple data stream)

У такій системі є безліч процесорів, що одночасно виконують різні послідовності команд, обробляючи при цьому різні набори даних.

Розрізняють дві конфігурації таких систем – *MIMD-системи з загальною пам'яттю* і *MIMD-системи з розподіленою пам'яттю*.

MIMD-система з загальною пам'яттю

У такій системі всі процесори однакові і працюють з єдиним полем загальної пам'яті, тобто кожен із процесорів може отримати доступ до всіх команд і даних, що зберігаються в пам'яті.

Такі системи отримали назву симетричні багатопроцесорні системи, або SMP-системи (symmetric multiprocessor).

До цього класу належать, наприклад, сучасні багатоядерні процесори, комп'ютери з декількома процесорами, у тому числі і багатоядерними, розташованими на одній материнській платі, нарешті, суперкомп'ютерні системи, що містять тисячі процесорів (рис. 1.23).

MIMD-система з розподіленою пам'яттю

У такій системі всі процесори однакові, але, на відміну від SMP-систем, працюють кожен зі своїм власним запам'ятовуючим пристроєм. Взаємний обмін інформацією між процесорами здійснюється через локальну мережу.

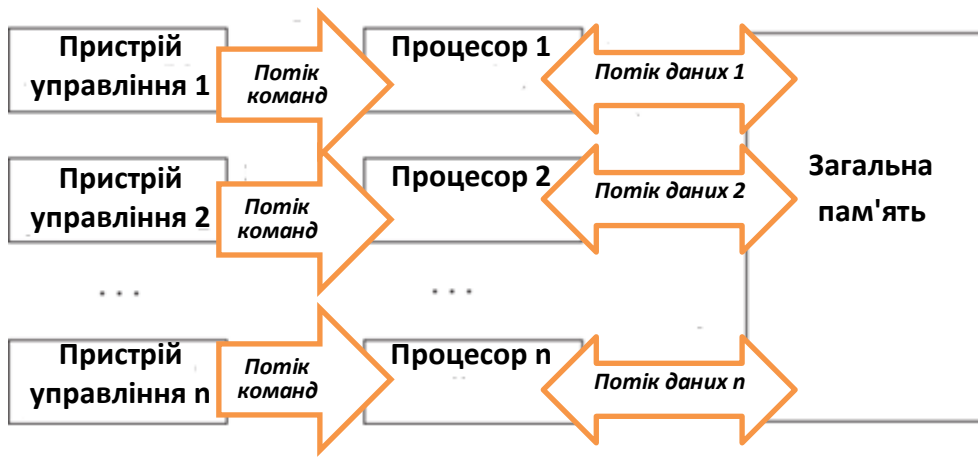


Рис. 1.23. MIMD-система з загальною пам'яттю

Дивлячись на схему, подану на рис. 1.24, треба звернути увагу на те, що структура кожного процесорного вузла повністю збігається з поданою на рис. 1.21 схемою системи з одинарними потоками команд і даних, простіше кажучи, зі схемою класичної однопроцесорної електронно-обчислювальної машини.

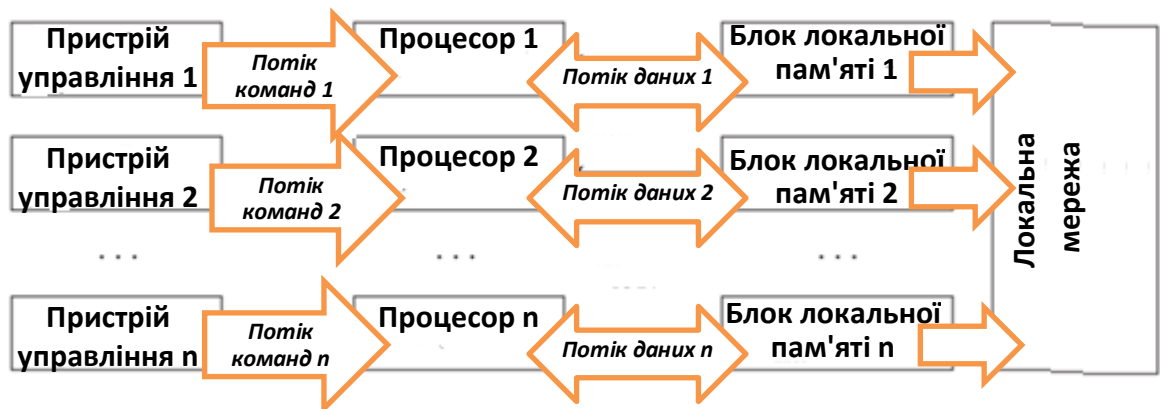


Рис. 1.24. MIMD-система з розподіленою пам'яттю

Обидві ці схеми (із загальною і розподіленою пам'яттю) багатопроцесорних систем на сьогодні знайшли широке застосування.

Технології суперкомп'ютерів і кластерів спочатку застосовувалися в основному до наукових потреб – вирішення фундаментальних і прикладних

завдань з фізики, механіки, астрономії, метеорології, опору матеріалів тощо, де були потрібні величезні обчислювальні потужності. Велика продуктивність потрібна при проектуванні складних керованих систем (літаків, ракет, космічних станцій), створення синтетичних ліків із заданими властивостями, у генній інженерії, передбаченні погоди та природних катаклізмів, для підвищення ефективності та надійності атомних електростанцій, прогнозування макроекономічних ефектів тощо.

Приклади завдань для високопродуктивних систем наведено на рис. 1.25.



Рис. 1.25. Завдання для високопродуктивних систем

Досить тривалий час розміри обчислювальних пристроїв постійно зменшувалися. У 1965 році Гордон Мур сформулював емпіричний «закон», за яким продуктивність обчислювальних систем подвоюється кожні вісімнадцять місяців.

Але на початку XXI століття щорічне зменшення на 10-30 % розмірів елементарних обчислювальних модулів призвело до практичного застосування пристроїв з елементарними модулями розміром в 100-200 ангстрем (0,01-0,02 мк), тобто розмір елементарного обчислювального пристрою наблизився до молекулярних розмірів. На такому рівні закони класичної фізики вже не працюють, і починають

діяти квантові закони, які для багатьох важливих динамічних задач ще не описані теоретично. Для опису роботи таких пристроїв не застосовні класичні об'єкти і методи інформатики. За квантовим принципом невизначеності Гейзенберга, у таких мікроскопічних системах нема аналога поняття «bit».

Незважаючи на великі очікування і зусилля з розроблення, квантовий комп'ютер створити не вдалося, і закон Мура довелося «поховати» – розміри комп'ютерів перестали зменшуватися, навпаки, вони збільшуються (через свою багатоядерність). Якщо швидкодія суперкомп'ютерів ще якось збільшується, то швидкодія персональних комп'ютерів зупинилася на рівні приблизно 2-3 ГГц і останні 10 років не змінюється. Про обіцяний наприкінці ХХ століття персональний комп'ютер зі швидкострільністю 1000 ГГц не йдеться.

Японія залишається невеликим гравцем на ринку суперкомп'ютерів. Для порівняння, на Китай у списку Top500 припадає 226 систем, США – 114.

Перспективи розвитку побутових комп'ютерів – скоріше регрес, ніж прогрес. Проте в науково-дослідних лабораторіях найбільших університетів і транснаціональних ІТ-компаній розглядаються кілька можливих напрямів створення елементної бази нового покоління обчислювальних пристроїв на принципах ядерного магнітного або електронного парамагнітного резонансу.

Вважається, що квантові комп'ютери дадуть змогу різко збільшити швидкість обчислень за рахунок паралельного виконання багатьох операцій на одному і тому самому процесорі.

Наприклад, якщо на класичному комп'ютері злом ключа до сучасного шифру потребує великої кількості часу, то на квантовому він при використанні алгоритму Шора займе стільки ж, скільки і саме шифрування, що полягає в перемноженні двох дуже великих чисел.

Харківський національний університет радіоелектроніки почав реалізацію проєкту, що став переможцем конкурсу з кібербезпеки США і

України 2021 року, організованого Фондом цивільних досліджень і розвитку США. У його рамках буде проведено аналіз, проектування, створення і застосування квантових обчислень і квантово-стійких методів для забезпечення безпеки сучасних 5G мереж.

Створити квантовий комп'ютер у принципі можна з будь-якої системи, що підкоряється законам квантової механіки, такі спроби робилися. Комп'ютери збирали і на квантових точках, і спінах електронів або атомів, і надпровідниках.

Істотні недоліки цього підходу в деяких випадках призводять до принципової неможливості створення конкурентоспроможного обчислювального пристрою. Характерним прикладом є проєкт корпорації ІВМ, яка тільки на перший етап розроблення молекулярної елементної бази нового покоління виділила 17 мільярдів доларів на п'ять років.

У результаті був створений макет, що оперує з п'ятьма або сімома квантовими бітами, вагою близько 7 т, здатний вирішувати тільки примітивні завдання типу розкладання числа 15 на два множники: 5 і 3. Реальних досягнень на цьому напрямі (як і на всіх інших) поки не видно. Нічого не вийшло і зі штучним інтелектом.

Традиційні *методики оцінювання продуктивності комп'ютерних систем* поступово втрачають свою ефективність – комп'ютери все активніше взаємодіють один з одним, людьми і зовнішнім світом, що призводить до появи стилю комп'ютерної обробки, яка визначається сценаріями розвитку подій, а це відкриває еру нових інтелектуальних пристроїв і одночасно породжує абсолютно нові потреби в оцінюванні їхньої продуктивності.

Штучний інтелект останнім часом стає все більш популярним через вимирання природного.

1.6. Принципи нейронної обробки інформації

Нейронні мережі та нейрокомп'ютери – один з напрямів комп'ютерної індустрії, в основі якого лежить ідея створення штучних інтелектуальних пристроїв за образом і подобою мозку людини (рис. 1.26).

Нейрокомп'ютери складаються з великої кількості паралельно працюючих простих обчислювальних елементів (нейронів) [12, 15, 22].

Елементи пов'язані між собою, утворюючи нейронну мережу, виконують однакові обчислювальні дії і не потребують зовнішнього управління. Велика кількість обчислювальних елементів, що паралельно працюють, забезпечують високу швидкодію (рис. 1.26).

На відміну від цифрових систем, що являють собою комбінацію процесорних і запам'ятовуючих блоків, нейропроцесори містять пам'ять, розподілену у зв'язках між дуже простими процесорами, які часто можуть бути описані як формальні нейрони або блоки з однотипних формальних нейронів.

Тим самим основне навантаження на виконання конкретних функцій процесорами лягає на архітектуру системи, деталі якої у свою чергу визначаються міжнейронним зв'язком.

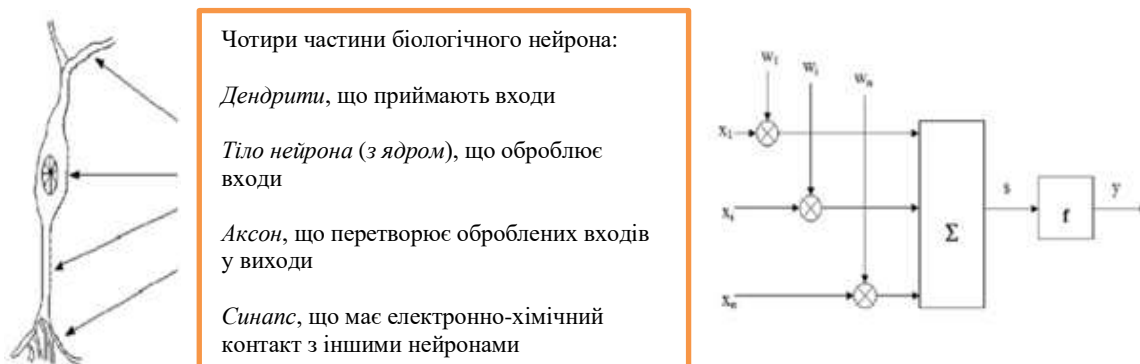


Рис. 1.26. Біологічний (ліворуч) і базовий штучний (праворуч) нейрони

Основні переваги нейрокомп'ютерів

Три основні переваги нейрокомп'ютерів:

- усі алгоритми нейроінформатики високо паралельні, що є запорукою високої швидкодії;
- нейросистеми можна легко зробити дуже стійкими до перешкод і руйнувань;
- стійкі і надійні нейросистеми можуть створюватися і з ненадійних елементів, що мають значний розкид параметрів.

Розробники нейрокомп'ютерів прагнуть об'єднати стійкість, швидкодію і паралелізм АОМ (аналогових обчислювальних машин) з універсальністю сучасних комп'ютерів.

Як і людський мозок, нейромережа здатна виводити закономірності, робити припущення, відкривати закони природи. Але, як і людина, нейромережа не здатна чітко формулювати алгоритм, який дав би змогу зробити той чи інший умовивід.

Відомі випадки, коли нейромережі демонструють феномен, так зване шосте почуття. Вони з успіхом отримують знання з аналізу інформації, з якої, здавалося б, ці знання отримати неможливо.

Нейрокомп'ютери відрізняються від електронно-обчислювальної машини попередніх поколінь не просто великими можливостями. Принципово змінюється спосіб використання машини. Місце програмування займає навчання, нейрокомп'ютер вчиться вирішувати неформалізовані завдання.

Навчання – корегування ваги зв'язків, у результаті якої кожний вхідний вплив призводить до формування відповідного входу. Після навчання мережа може застосовувати отримані навички до нових вхідних сигналів.

При переході від програмування до навчання підвищується ефективність вирішення інтелектуальних завдань.

Навчити нейронну мережу означає повідомити її, чого від неї чекають. Показавши дитині зображення літери і отримавши неправильну

відповідь, їй називають ту, яку хочуть отримати. Дитина запам'ятовує цей приклад із правильною відповіддю, і в її пам'яті відбуваються зміни в потрібному напрямку (рис. 1.27, а). Основний принцип навчання полягає в тому, що якщо мережа видає неправильну відповідь, важелі корегуються, щоб зменшити похибку (рис. 1.27, б).

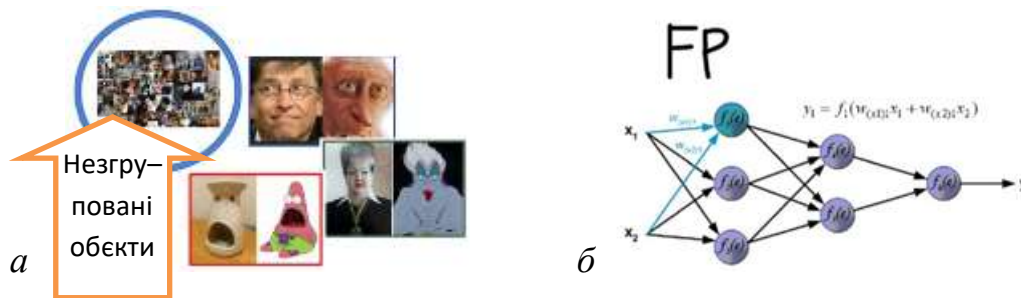


Рис. 1.27. Навчання нейронної мережі:

а – мережі для спеціальних задач: кластеризація або «угруповання за нечіткою ознакою»; б – алгоритми зворотного поширення помилок

На сьогодні розроблення нейрокомп'ютерів ведеться переважно промислово розвиненими країнами. Незважаючи на недоліки, нейрокомп'ютери дають змогу з високою ефективністю вирішувати цілий ряд інтелектуальних завдань:

- розпізнавання образів: людських облич, букв і ієрогліфів, сигналів радара і сонара, відбитків пальців у криміналістиці, захворювань за симптомами, наприклад у медицині, і місцевостей, де слід шукати корисні копалини, у геології за непрямими ознаками;

- управління в режимі реального часу літаками, ракетами і технологічними процесами безперервного виробництва – металургійного, хімічного тощо;

- прогнози – погоди, курсу акцій та інших фінансових показників; результати – лікування, політичних подій, зокрема результатів виборів; поведінки противників у воєнному конфлікті і економічній конкуренції;

– оптимізація і пошук найкращих варіантів при конструюванні технічних пристроїв, виборі економічної стратегії і лікуванні хворого.

Список можна продовжувати безкінечно.

Організація Over the Bridge випустила альбом «Втрачені записи клубу 27» («Lost Tapes of the 27 Club»), який складається з пісень у стилі культових рок-музикантів, створених штучним інтелектом Magenta. Музичні стилі Емі Вайнхаус, The Doors, Nirvana і Джими Хендрікса вдалося відтворити настільки точно, що є відчуття реальності авторства.

Для оранжирування пісень MIDI-файли розбивають на треки – бас, соло-гітара, ритм-гітара та інші, які по одному оброблюються програмними засобами.

На аукціоні Christie's картина, створена штучним інтелектом, була продана за 432,5 тисячі доларів. Картина називається «Портрет Едмона Беламі» і є частиною серії «Сім'я Беламі», створеної французьким колективом Obvious за допомогою штучного інтелекту, на основі 15 000 портретів XIV-XX століть [30].

Контрольні запитання

1. Який тип мереж з'явився першим і чому?
2. Що таке локальні обчислювальні мережі?
3. Що таке глобальні мережі?
4. Назвіть відмінності між локальними і глобальними мережами.
5. Що таке регіональні обчислювальні мережі?
6. На основі чого відбувається зближення локальних і глобальних мереж?
7. Що таке мережева технологія?
8. Назвіть можливості хмарних онлайн-технологій.
9. Hardware – переваги і недоліки.

Розділ 2. ЗАГАЛЬНІ ПРИНЦИПИ ПОБУДОВИ МЕРЕЖ. ІНФОРМАЦІЙНА БЕЗПЕКА

2.1. Найпростіша мережа з двох комп'ютерів

2.1.1. Спільне використання ресурсів

Історично головною метою об'єднання комп'ютерів у мережу був *розподіл ресурсів* – користувачі комп'ютерів, підключених до мережі, або додатки, що виконуються на цих комп'ютерах, отримують можливість автоматичного доступу до різних ресурсів інших комп'ютерів мережі, до яких належать [5, 6, 12]:

– периферійні пристрої, такі як диски, принтери, плотери, сканери тощо;

– дані, що зберігаються в оперативній пам'яті або на зовнішніх запам'ятовуючих пристроях;

– обчислювальна потужність (за рахунок віддаленого запуску «своїх» програм на «чужих» комп'ютерах).

Щоб забезпечити користувачів різних комп'ютерів можливістю спільного використання ресурсів мережі, комп'ютери необхідно оснастити додатковими *мережевими засобами*.

Розглянемо найпростішу мережу, що складається з двох комп'ютерів, до одного з яких підключений принтер (рис. 2.1).



Рис. 2.1. Найпростіша мережа

Які додаткові засоби мають бути передбачені в обох комп'ютерах, щоб із принтером міг працювати не тільки користувач комп'ютера 2, до якого цей принтер безпосередньо підключений, але й користувач комп'ютера 1?

Розглянемо більш складну мережу. Локальну мережу (LAN), що є мережевою інфраструктурою, обмеженою географічно, і зазвичай використовується всередині організації, офісу або будинку. Ось приклад складу типової локальної мережі для невеликого офісу:

1. Комп'ютери та пристрої. У локальній мережі можуть бути різні комп'ютери та пристрої, такі як настільні комп'ютери, ноутбуки, принтери, сервери, маршрутизатори, комутатори та Wi-Fi точки доступу.

2. Маршрутизатор. Маршрутизатор є центральним пристроєм у локальній мережі. Він зазвичай підключається до модема для доступу до Інтернету та надає доступ до мережі всім пристроям у локальній мережі.

3. Комутатор. Комутатор використовується для зв'язку між пристроями локальної мережі. Він може бути використаний для підключення комп'ютерів, серверів та інших пристроїв до маршрутизатора.

4. Сервер. У локальній мережі може бути сервер, який надає різні служби для користувачів у мережі. Наприклад, сервер файлів може зберігати і забезпечувати доступ до спільних файлів і папок, а сервер друкування може управляти спільними принтерами.

5. Кабелі. Для підключення пристроїв до локальної мережі можуть використовуватися мережеві кабелі, такі як кабелі Ethernet. Кабелі підключають комп'ютери, комутатори та інші пристрої до мережевих портів на маршрутизаторі або комутаторі.

6. Wi-Fi точки доступу. Якщо вам потрібен бездротовий доступ до Інтернету або локальної мережі, то в локальній мережі може бути точка доступу Wi-Fi. Вона дає змогу пристроям підключатися до мережі бездротового з'єднання.

7. IP-адреса. У локальній мережі кожному пристрою надається унікальна IP-адреса, що використовується для ідентифікації та маршрутизації даних у мережі.

Це лише загальний приклад локальної мережі, і конкретна конфігурація може відрізнитися залежно від вимог і обсягу мережі.

2.1.2. Мережеві інтерфейси

Для зв'язку пристроїв у них насамперед мають бути передбачені *зовнішні інтерфейси* – у широкому змісті – *формально визначена логічна та/або фізична межа між взаємодіючими незалежними об'єктами* [3, 5, 12, 13, 15, 16].

Інтерфейс задає параметри, процедури та характеристики взаємодії об'єктів. Разом із зовнішніми електронні пристрої можуть використовувати внутрішні інтерфейси, що визначають логічні та фізичні межі між модулями, що входять до їхнього складу. Так, відомий інтерфейс «загальна шина» є внутрішнім інтерфейсом комп'ютера, що пов'язує оперативну пам'ять, процесор та інші блоки комп'ютера.

Виділяють *фізичний* і *логічний* інтерфейси.

Фізичний інтерфейс (що також називається **портом**) – визначається набором електричних зв'язків і характеристиками сигналів. Звичайно він являє собою роз'єм з набором контактів, кожний з яких має визначене призначення, наприклад це може бути група контактів для передавання даних, контакт синхронізації даних тощо. Пара роз'ємів з'єднується **кабелем**, що складається з набору проводів, кожний з яких з'єднує відповідні контакти. У таких випадках говорять про створення **лінії**, або **каналу**, зв'язку між двома пристроями (більш детально розглянемо у другій частині посібника).

Логічний інтерфейс (що також називається **протоколом**) – це набір інформаційних повідомлень визначеного формату, якими обмінюються два

пристрої або дві програми, а також набір правил, що визначають логіку обміну цими повідомленнями.

Інтерфейс комп'ютер – комп'ютер дає змогу двом комп'ютерам обмінюватися інформацією. З кожного боку він реалізується парою:

– *апаратним модулем, що називається мережевим адаптером, або мережевою інтерфейсною картою (Network Interface Card, NIC);*

– *драйвером мережевої інтерфейсної карти – спеціальною програмою, що управляє роботою мережевої інтерфейсної карти.*

Інтерфейс комп'ютер – периферійний пристрій (у нашому випадку інтерфейс комп'ютер – принтер) дає змогу комп'ютеру управляти роботою периферійного пристрою (ПП). Цей інтерфейс *реалізується:*

– з боку комп'ютера – **інтерфейсною картою та драйвером** периферійного пристрою (принтера), подібним до мережевої інтерфейсної карти та її драйвера;

– з боку периферійного пристрою – **контролером ПП** (принтера), що звичайно являє собою апаратний пристрій, що приймає від комп'ютера як дані, наприклад байти інформації, яку потрібно роздрукувати на папері, так і команди, які він відпрацьовує, управляючи електромеханічними частинами периферійного пристрою, наприклад виштовхуючи аркуш паперу з принтера або переміщаючи магнітну головку диска.

Класифікація комп'ютерних мереж відіграє важливу роль при їхньому плануванні, налаштуванні та адмініструванні. Мережі можуть бути класифіковані за різними ознаками:

1) за масштабом.

Локальна мережа (Local Area Network – LAN) – охоплює невелику територію, таку як будинок, офіс чи навчальний заклад. Приклади включають Ethernet та Wi-Fi мережі в будинках чи офісах.

Метрополітенська мережа – охоплює місто або міську область. Прикладом може бути міська мережа, що поєднує різні офіси та установи в межах міста.

Глобальна мережа (Wide Area Network – WAN) – охоплює великі географічні області, такі як країни чи континенти. Прикладом є Інтернет, який поєднує комп'ютери та мережі по всьому світу;

2) *технологією передавання даних.*

Дротова мережа використовує фізичні кабелі передавання даних – вита пара, оптоволокло або коаксіальний кабель. Приклади – Ethernet та коаксіальні кабелі.

Бездротова мережа передавання даних здійснюється через радіохвилі, наприклад Wi-Fi, Bluetooth або стільниковий зв'язок;

3) *топологією.*

Зірка – усі пристрої підключені до однієї центральної точки (наприклад комутатора або маршрутизатора).

Шина – пристрої підключені до одного центрального кабелю (наприклад коаксіального кабелю або кабелю Ethernet).

Кільце – пристрої з'єднані в замкнений кільцевий маршрут.

Дерево – мережа має ієрархічну структуру з головним вузлом і підсітками, що гілкуються;

4) *використанням.*

Приватна мережа – належить і використовується однією організацією або компанією для внутрішніх комунікацій [31].

Вільного доступу – належить одній організації, компанії або приватній особі, але надається вільний доступ, наприклад кафе, заклади освіти тощо;

5) *протоколами.*

Ethernet – один із найпоширеніших протоколів для передавання даних у локальних мережах.

TCP/IP: протоколи TCP (Transmission Control Protocol) і IP (Internet Protocol) використовуються в Інтернеті і широко застосовуються для передавання даних у мережах різних масштабів.

Wi-Fi: протокол бездротового зв'язку дає змогу пристроям підключатися до локальної мережі за допомогою радіохвиль.

HTTP (Hypertext Transfer Protocol): протокол, використовуваний для передавання вебсторінок та інших даних в Інтернеті.

FTP (File Transfer Protocol): протокол передавання файлів між комп'ютерами в мережі.

Приклади: локальна мережа (LAN) із використанням Ethernet-кабелів в офісі компанії; метрополітенська мережа (MAN) для зв'язку офісів і навчальних закладів усередині міста з використанням оптоволоконних кабелів; глобальна мережа (WAN), така як Інтернет, що об'єднує комп'ютери та мережі по всьому світу за допомогою TCP/IP протоколу.

Класифікація мереж за різними ознаками допомагає організувати і розуміти різні типи мереж і їхні особливості.

Це важливо при проєктуванні, налаштуванні та управлінні комп'ютерними мережами.

2.2. Мережеве програмне забезпечення

Мережеве програмне забезпечення (МПЗ) – це набір програмних компонентів та інструментів, призначених для управління та забезпечення роботи комп'ютерних мереж. Це дає змогу встановити з'єднання між комп'ютерами або пристроями, обмінюватися даними і ресурсами, а також забезпечує функціональність мережевих служб.

Мережеве програмне забезпечення складається з мережевих служб, мережевої операційної системи та мережевих додатків.

2.2.1. Мережеві служби та сервіси

Потреба в доступі, наприклад до віддаленого принтера, може виникати в користувачів різних додатків: текстового редактора, графічного

редактора, системи управління базою даних. Очевидно, що дублювання в кожному з додатків загальних для всіх функцій з організації віддаленого друку є зайвим [4-6, 12].

Більш ефективним є підхід, при якому ці функції виключаються з додатків і оформляються у вигляді пари спеціалізованих програмних модулів – *клієнта і сервера друкування* (рис. 2.2). Ця пара (клієнт-сервер) може бути використана будь-яким додатком, що виконується на комп'ютері 1.

Узагальнюючи такий підхід стосовно інших типів розподілених ресурсів, дамо такі визначення.

Клієнт – це модуль, призначений для формування та передавання повідомлень-запитів до ресурсів віддаленого комп'ютера від різних додатків з наступним прийманням результатів із мережі та передаванням їх відповідним додаткам.

Сервер – це модуль, що постійно очікує надходження з мережі запитів від клієнтів і, прийнявши запит, намагається його обслужити, як правило, за участю локальної операційної системи; один сервер може обслуговувати запити одразу декількох клієнтів (по черзі або одночасно).

Пара клієнт-сервер, що надає доступ до конкретного типу ресурсу комп'ютера через мережу, утворює **мережеву службу**.

Кожна служба пов'язана з визначеним типом мережевих ресурсів. Так, на рис. 2.2 модулі клієнта і сервера, що реалізують віддалений доступ до принтера, утворюють мережеву **службу друкування**.

Файлова служба дає змогу отримувати доступ до файлів, які зберігаються на диску інших комп'ютерів. Серверний компонент файлової служби називають **файл-сервером**.

Для пошуку і перегляду інформації в Інтернеті використовується **вебслужба**, що складається з **вебсервера** та клієнтської програми, яка називається **веббраузером** (web browser). Розподіленим ресурсом у

цьому випадку є *вебсайт* – у певний спосіб організований набір файлів, що містять пов'язану в змістовому відношенні інформацію та зберігаються на зовнішньому накопичувачі вебсервера.

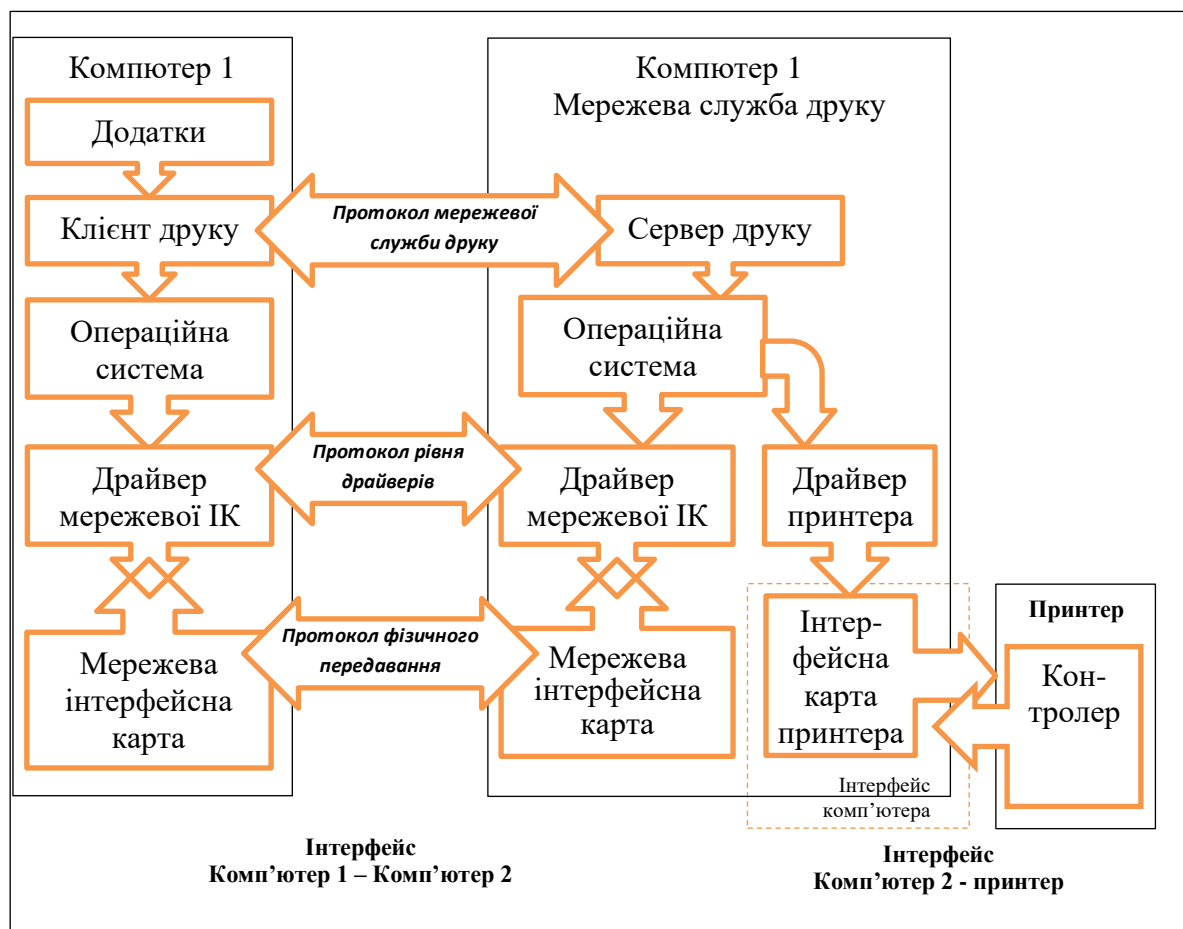


Рис. 2.2. Спільне використання принтера в комп'ютерній мережі за допомогою мережевої служби друку

Розглянемо деякі служби і сервіси, які надають різні послуги на основі мережевих технологій:

1. *Інтернет-провайдери* – компанії, які надають доступ до Інтернету через дротове підключення (наприклад DSL, кабельний Інтернет), або бездротовий зв'язок (наприклад Wi-Fi, 4G/5G).

2. *Соціальні мережі* – платформи, які дають змогу людям спілкуватися, обмінюватися інформацією, фотографіями та відео, створювати профілі і мережі контактів (наприклад Facebook, Twitter, Instagram).

3. *Електронна пошта* – сервіси електронної пошти дають змогу користувачам відправляти, отримувати і управляти своєю електронною кореспонденцією (наприклад Gmail, Outlook).

4. *Хмарні сервіси* – платформи, що надають доступ до зберігання даних, резервного копіювання, спільного використання файлів і програмного забезпечення через Інтернет (наприклад Google Drive, Dropbox).

5. *Відеоконференції* – сервіси, які дають змогу проводити відеозв'язок і зустрічі в режимі реального часу в мережі Інтернет (наприклад Zoom, Microsoft Teams).

6. *VPN (віртуальна приватна мережа)* – технологія, яка дає змогу забезпечити безпеку та приватність з'єднання між комп'ютерами через публічну мережу (наприклад NordVPN, ExpressVPN).

7. *Онлайн-банкінг* – сервіси, які надають можливість клієнтам банків здійснювати фінансові операції через Інтернет, включаючи перекази коштів, оплату рахунків і управління фінансами.

8. *Ігрові сервіси* – платформи, де користувачі можуть грати в комп'ютерні ігри онлайн, спілкуватися з іншими гравцями та отримувати доступ до різних ігрових послуг (наприклад Steam, PlayStation Network).

9. *Пошукові системи* – сервіси, які дають змогу користувачам здійснювати пошук інформації в Інтернеті на основі ключових слів (наприклад Google, Bing).

Це лише кілька прикладів мережевих служб і сервісів, які широко використовуються в сучасному світі. Із зростанням технологій і розвитком мережевого середовища з'являються нові сервіси, що задовольняють різні потреби користувачів.

2.2.2. Мережева операційна система

Операційну систему комп'ютера часто визначають як взаємопов'язаний набір системних програм, що забезпечує ефективне управління ресурсами комп'ютера (пам'яттю, процесором, зовнішніми пристроями, файлами тощо), а також надає користувачу зручний інтерфейс для роботи з апаратурою комп'ютера та розроблення додатків.

Говорячи про мережеву операційну систему, необхідно розширити границі керованих ресурсів за межі одного комп'ютера.

Мережевою операційною системою (МОС) називають операційну систему комп'ютера, яка, окрім управління локальними ресурсами, надає користувачам і додаткам можливість ефективного та зручного доступу до інформаційних і апаратних ресурсів інших комп'ютерів мережі.

Мережеві операційні системи – операційні системи, спеціально розроблені для роботи в мережах комп'ютерів. Вони надають функціонал для управління мережевими ресурсами, комунікації між комп'ютерами і обробки мережових запитів.

Ось деякі приклади мережових операційних систем:

– *Windows Server* – це версія операційної системи Windows, спеціально розроблена для використання на серверах. Вона має вбудовані функції для управління мережею, такі як доменний контролер Active Directory, служби доменних імен (DNS) і служби директорій;

– *Linux* – має багато різних дистрибутивів, які можна використовувати як мережеві операційні системи. Наприклад, Ubuntu Server і CentOS – це популярні дистрибутиви Linux, що можуть бути використані на серверах для управління мережею;

– *FreeBSD* – операційна система з відкритим вихідним кодом, яка також може бути використана як МОС. Вона надає широкий спектр функцій для мережевої роботи і має добру підтримку мережових протоколів;

– Cisco IOS – операційна система, використовувана на мережевих пристроях Cisco, таких як маршрутизатори і комутатори. Вона надає функціонал для управління мережею, налаштування маршрутизації і комутації, а також моніторингу та діагностики.

На андроїдах можна встановлювати різні мережеві операційні системи (ОС) залежно від потреб і вимог користувача. Деякі з популярних мережевих ОС для андроїд-пристроїв включають:

– Kali NetHunter – мережева ОС, розроблена на базі Kali Linux, спеціально для проведення тестування на проникнення мережі і аудиту безпеки. Вона має широкий набір інструментів для аналізу мережі та виявлення вразливостей;

– BackTrack – ОС також спеціалізується на мережевому тестуванні та аудиті безпеки. Вона містить набір інструментів, розроблених для виявлення вразливостей, отримання доступу до систем та аналізу мережевого трафіка;

– Paranoid Android – ОС базується на стандартному Android, але має ряд додаткових функцій і налаштувань для поліпшення приватності та безпеки користувача. Вона надає більше контролю над дозволами програм, захист від витоку даних та інші функції;

– LineageOS – одна з найпопулярніших операційних систем на базі Android з відкритим вихідним кодом. Вона пропонує широкі можливості налаштування, включаючи функції безпеки та приватності. LineageOS також підтримує широкий спектр пристроїв.

Існує багато інших операційних систем, які також можуть бути використані для управління мережами. Вибір операційної системи залежить від конкретних потреб і вимог вашої мережі.

Перед встановленням будь-якої ОС завжди рекомендується ретельно ознайомитися з документацією, оскільки це може потребувати спеціальних навичок і мати певні ризики.

Сьогодні практично всі операційні системи є мережевими. *Віддалений доступ до мережесих ресурсів забезпечується* [4, 5, 7, 12]:

- мережевими службами;
- засобами транспортування повідомлень по мережі (у найпростішому випадку – мережевими інтерфейсними картами та їхніми драйверами).

Отже, саме ці функціональні модулі слід додати до операційної системи, щоб вона могла називатися мережевою.

Серед мережесих служб можна виділити такі, що орієнтовані не на простого користувача, як файлова служба або служба друкування, а на адміністратора. Такі служби спрямовані на організацію роботи мережі. Наприклад, *централізована довідкова служба*, або *служба каталогів*, призначена для ведення бази даних про користувачів мережі, усі її програмні та апаратні компоненти. Як інші приклади можна назвати *службу моніторингу мережі*, що дає змогу захоплювати і аналізувати мережесий трафік, *службу безпеки*, до функцій якої може входити, зокрема, виконання процедури логічного входу з перевіркою пароля, *службу резервного копіювання та архівування*.

Крім мережесих служб мережева операційна система має включати ***програмні комунікаційні (транспортні) засоби***, що забезпечують разом з апаратними комунікаційними засобами передавання повідомлень, якими обмінюються клієнтські та серверні частини мережесих служб. Завдання комунікації між комп'ютерами мережі вирішують драйвери та протокольні модулі. Вони виконують такі функції, як формування повідомлень, розбиття повідомлення на частини (пакети, кадри), перетворення імен комп'ютерів у числові адреси, дублювання повідомлень у випадку їх втрати, визначення маршруту в складній мережі тощо.

І мережесі служби, і транспортні засоби можуть бути невід'ємними (вбудованими) компонентами операційної системи або існувати у вигляді окремих програмних продуктів. Наприклад, мережева файлова служба

звичайно вбудовується в операційну систему, а от веббраузер найчастіше встановлюється окремо. Типова мережева операційна система має у своєму складі широкий набір драйверів і протокольних модулів, однак у користувача, як правило, є можливість доповнити цей стандартний набір необхідними йому програмами.

Мережева служба може бути подана в операційній системі або обома – клієнтською та серверною частинами, або тільки однією з них. У першому випадку операційна система, що називається **одноранговою**, не тільки дає змогу звертатися до ресурсів інших комп'ютерів, але й надає власні ресурси в розпорядження користувачів інших комп'ютерів. Наприклад, якщо на всіх комп'ютерах мережі встановлені і клієнти, і сервери файлової служби, то всі користувачі мережі можуть спільно застосовувати файли один одного. Комп'ютери, що поєднують функції клієнта і сервера, називають **одноранговими вузлами**.

Операційна система, що переважно містить клієнтські частини мережевих служб, називається **клієнтською**. Клієнтські операційні системи встановлюються на комп'ютери, що звертаються з запитом до ресурсів інших комп'ютерів мережі. За такими комп'ютерами, що також називаються **клієнтськими**, працюють звичайні користувачі. Клієнтські комп'ютери належать до класу відносно простих пристроїв.

До іншого типу операційних систем належить **серверна операційна система** – вона орієнтована на обробку запитів з мережі до ресурсів свого комп'ютера і містить в основному серверні частини мережевих служб. Комп'ютер із встановленою на ньому серверною операційною системою, що займається винятково обслуговуванням запитів інших комп'ютерів, називають **виділеним сервером мережі**. За виділеним сервером, як правило, звичайні користувачі не працюють.

2.2.3. Мережеві додатки

Мережеві додатки, також відомі як мережеві програми – це програмні засоби, використовувані для передавання інформації, спільної роботи, забезпечення доступу до ресурсів та інших мережевих функцій. Комп'ютер, підключений до мережі, може виконувати такі *типи додатків*:

– **локальний додаток** цілком виконується на певному комп'ютері і використовує тільки локальні ресурси. Для такого додатка не потрібно ніяких мережевих засобів, він може бути виконаний на автономно працюючому комп'ютері;

– **централізований мережевий додаток** цілком виконується на певному комп'ютері, але звертається в процесі свого виконання до ресурсів інших комп'ютерів мережі. Очевидно, що робота такого типу додатків неможлива без участі мережевих служб і засобів транспортування повідомлень;

– **розподілений мережевий додаток** складається з декількох взаємодіючих частин, кожна з яких виконує якусь визначену закінчену роботу з розв'язання прикладної задачі, причому кожна частина може виконуватися і, як правило, виконується на окремому комп'ютері мережі. Частини розподіленого додатка взаємодіють один з одним, використовуючи мережеві служби і транспортні засоби ОС. Розподілений додаток у загальному випадку має доступ до всіх ресурсів комп'ютерної мережі.

Існує безліч різних типів мережевих додатків:

– веббраузери – додатки, що дають змогу користувачам переглядати вебсторінки та взаємодіяти з ними. Вони використовують протокол НТТР для завантаження вебсторінок з серверів інтернету;

– електронна пошта – поштові клієнти або програми електронної пошти, використовувані для створення, відправлення та отримання електронних листів через мережу. Вони використовують різні протоколи, такі як SMTP, POP або IMAP, для обміну повідомленнями;

– прикладні програми для обміну повідомленнями: такі додатки, як Skype, WhatsApp, Telegram і Viber, дають змогу користувачам обмінюватися текстовими повідомленнями, голосовими дзвінками та відеовикликами через мережу;

– файлообмінні додатки – це програми, що дають змогу користувачам передавати файли через мережу. Наприклад, Dropbox, Google Drive та OneDrive завантажують файли до хмарного сховища та обмінюються ними з іншими користувачами;

– віртуальні приватні мережі (VPN) – VPN-клієнти дають змогу створювати зашифроване з'єднання з віддаленим сервером через інтернет. Вони використовуються для забезпечення безпеки та конфіденційності під час передавання даних через публічну мережу;

– соціальні мережі – веб- або мобільні додатки, що дають змогу користувачам спілкуватися, ділитися вмістом і будувати мережі знайомств. Прикладами таких додатків є Facebook, Instagram, Twitter і LinkedIn.

2.3. Інформаційна безпека

2.3.1. Основні поняття інформаційної безпеки

Інформація – сукупність даних, фактів, знань або повідомлень, які є достовірними, повними (містять усі необхідні дані), актуальними та доступними і використовуються для передавання або отримання розуміння та прийняття рішень. Вона може бути подана в різних формах, таких як текст, зображення, звук, відео та ін.

Р. Хартлі та К. Шеннон розвинули концепцію *кількості інформації*, але в різні часи і різних контекстах.

Ральф Хартлі, англійський математик, у 1928 році запропонував формулу для обчислення кількості інформації. Ця формула, відома як формула Хартлі, використовується для вимірювання кількості інформації в

термінах бінарних одиниць, таких як біти. За цією формулою, кількість інформації виражається як логарифм з основою 2 від кількості можливих станів системи. Формула Хартлі виглядає так:

$$I = \log_2(N),$$

де I – кількість інформації, біт;

N – кількість можливих станів системи.

Клод Шеннон, американський математик та інженер, у 1948 році випустив у світ свою революційну роботу «Теорія інформації», у якій розробив математичну теорію інформації: вводить поняття біт як одиниці вимірювання інформації. Шеннон встановив, що кількість інформації може бути виміряна як величина ймовірності події. Він також визначив поняття ентропії як міру невизначеності інформації в деякій системі.

Отже, Р. Хартлі та К. Шеннон робили внесок у розвиток теорії інформації, проте їхні підходи та формули для обчислення кількості інформації трохи відрізняються. Формула Хартлі використовується для вимірювання кількості інформації в бітах, у той час як робота Шеннона дала більш загальну математичну теорію інформації, у якій використовуються поняття біта, ймовірності та ентропії.

Для людей інформація є цінним ресурсом, використовуваним для прийняття рішень, вирішення проблем, отримання знань, розвитку.

Визначимо системи, у яких інформація накопичується, обробляється та передається:

– *комп'ютерна система* – обчислювальна система, що складається з апаратних і програмних компонентів, які співпрацюють між собою для оброблення інформації. Вона може включати комп'ютери, мережі, сховища даних та інші компоненти;

– *автоматизована система (АС)* – комплекс програмних і апаратних засобів, призначений для виконання різних завдань і операцій без значного

втручання людини. АС може автоматизувати процеси управління, виробництва, обліку, аналізу даних, оброблення інформації та інших сфер діяльності;

– *комп'ютерні системи і мережі* – сукупність обладнання, програмного забезпечення і комунікаційних засобів, використовуваних для оброблення, передавання і збереження інформації;

– *інформаційна система* – система, що збирає, обробляє, зберігає та передає інформацію з метою підтримки прийняття рішень або виконання різних функцій;

– *інформаційна мережа* – з'єднує комп'ютерні системи та інші пристрої для передавання інформації (Інтернет, корпоративні та локальні мережі);

– *система управління базами даних (СУБД)* – програмне забезпечення, що дає змогу організовувати, зберігати, управляти та отримувати доступ до даних в базах даних. Вона забезпечує ефективне зберігання та швидкий доступ до даних;

– *хмарна система* – інформаційна система, базована на використанні розподіленого обчислювального ресурсу, такого як хмарні сервери, для оброблення, зберігання та передавання даних через мережу.

Автоматизовані системи на залізничному транспорті включають різні технології і пристрої, що допомагають забезпечити безпеку, ефективність і точність руху поїздів:

– *система автоматичного блокування* – контролює рух поїздів на залізничних ділянках і забезпечує безпечний інтервал між ними. Базується на використанні сигналів і датчиків, що передають інформацію про положення поїздів;

– *система автоматичного регулювання швидкості* – контролює швидкість руху поїздів, щоб запобігти перевищенню допустимих меж і забезпечити рівномірний рух. Використовує датчики, що вимірюють швидкість, і системи автоматичного гальмування;

– *система автоматичного пуску та зупинки* – контролює процес пуску та зупинки поїздів на станціях. Вона забезпечує точне зупинення поїзда на платформі та безпечно його пуск після посадки пасажирів;

– *системи моніторингу та діагностики* – датчики та монітори, що стежать за станом рухомого складу, рейок, сигнальних систем та інших компонентів, які надають операторам залізниці важливу інформацію про стан обладнання та дають змогу вчасно виявляти проблеми;

– *електронні квиткові системи* – дають змогу пасажирам купувати квитки онлайн, безпосередньо на станції або в поїзді. Можуть включати системи контролю доступу, які перевіряють валідність квитків під час посадки пасажирів.

Ці та багато інших систем допомагають підвищити безпеку, ефективність і комфорт на залізничному транспорті, сприяють зменшенню інцидентів, поліпшенню точності руху поїздів та поліпшенню послуг пасажирам.

Комп'ютерні мережі передають інформацію за допомогою різних протоколів і технологій. Основні *види інформації*, що можуть передаватися в комп'ютерних мережах:

– *текстові дані* – електронні листи, повідомлення, вебсторінки, текстові документи тощо. Текстові дані зазвичай передаються у вигляді кодуваного тексту, такого як ASCII або Unicode;

– *графічні дані* – зображення, фотографії, малюнки та графічні елементи векторного або растрового формату. Графічні дані можуть бути передані у форматі JPEG, PNG, GIF тощо;

– *аудіо та відео* – це музика, звукові записи, відеофайли, потокове відео, що, можуть бути у форматах MP3, WAV, MP4, AVI тощо;

– *програмний код* – інструкції, написані певною мовою програмування, що виконуються на комп'ютері. Програмний код може бути переданий через мережу для виконання на віддаленому комп'ютері або сервері;

– *бази даних* – структуровані набори даних, що можуть зберігати інформацію про клієнтів, продукти, транзакції тощо та бути передані через мережу для обміну даними між різними системами;

– *системні повідомлення* – методи, що передаються між комп'ютерами для управління мережею, такі як повідомлення про помилки, запити на авторизацію, управління ресурсами тощо;

– *соціальні медіа та комунікації* – класи, що передаються через соціальні мережі, месенджери, відеозв'язок та інші інтернет-сервіси для спілкування, обміну повідомленнями, фотографіями, відео тощо.

Залежно від призначення мережі та використовуваних протоколів, можуть бути інші специфічні види інформації.

У комп'ютерних мережах терміни «дані» і «інформація» використовуються для позначення *двох різних концепцій*.

Дані – сирий матеріал, що являє собою факти, спостереження або символи без організації або контексту. Вони можуть бути числами, текстом, зображеннями, звуком, вібрацією тощо. Дані самі по собі є безпосередніми спостереженнями або вимірюваннями і не мають особливого значення для кінцевого користувача без подальшої обробки або інтерпретації.

Інформація – результат обробки, організації або контекстуалізації даних, що надає їм значення, розуміння або корисність для отримувача. Інформація виникає, коли дані структуруються, аналізуються і відображуються у формі, зрозумілій і корисній людині. Наприклад, коли дані про продажі сортуються, групуються і відображуються у вигляді звіту про продажі за місяць, ця інформація дає користувачеві загальну картину стану справ для розуміння і прийняття рішень.

Основні засоби передавання інформації в комп'ютерних мережах:

Електричні кабелі – вита пара (наприклад Ethernet-кабелі); коаксіальні кабелі – на основі електричного сигналу, який може мати різні рівні напруги або струму.

Оптичні кабелі – у волоконно-оптичних мережах (наприклад Optical Fiber Networks) – на основі світлових сигналів на великі відстані з дуже високою швидкістю передавання даних.

Коаксіальні кабелі – високочастотні мережі (наприклад кабельне телебачення або деякі типи комп'ютерних мереж).

Бездротові засоби передавання – радіохвилі, інфрачервоне випромінювання або інші бездротові технології – Wi-Fi, Bluetooth, NFC (Near Field Communication) та інші на основі протоколів передавання даних [32].

Супутникові засоби передавання – до та від супутників, що обертаються навколо Землі, забезпечуючи глобальне покриття для передавання даних на великі відстані.

Більш детально ці питання викладено у другій частині навчального посібника.

Автоматизовані системи ухвалення рішень користувачем з використанням комп'ютерних мереж — це програмні або апаратні системи, розроблені для підтримки ухвалення рішень користувачем шляхом автоматизації процесів збирання, аналізу та надання інформації.

Такі системи використовують комп'ютерні мережі для обміну даними між різними компонентами системи, що можуть бути розташовані на різних комп'ютерах або серверах. Користувач може взаємодіяти з системою через зручний інтерфейс, отримуючи доступ до різних функцій і можливостей при прийнятті рішень.

Приклади автоматизованих систем прийняття рішень:

– *управління клієнтськими відносинами (CRM)* – дають змогу організаціям ефективно управляти взаємовідносинами з клієнтами, збирати та аналізувати дані про клієнтів, відстежувати продажі та забезпечувати персоналізоване обслуговування;

– *управління виробництвом (MES)* – забезпечують автоматизацію процесів виробництва, даючи змогу управляти інвентаризацією, розкладом виробництва, контролювати якість, відстежувати продуктивність;

– *управління запасами* – допомагають організаціям оптимізувати управління запасами, автоматизуючи процеси замовлення, доставки та відстеження запасів;

– *управління проектами* – надають інструменти для планування, управління та контролю за проектами, даючи змогу управляти завданнями, ресурсами, термінами, бюджетом проектів;

– *управління навчальними закладами* – допомагають школам та університетам автоматизувати процеси навчання здобувачів – розкладом занять, аналізом успішності та іншими адміністративними завданнями, для інших сфер, у яких такі системи можна застосувати.

Окремо можна виділити *автоматизовані системи прийняття рішень у комп'ютерних мережах (ADMS)* програмними засобами, що приймають рішення без прямого втручання людини. Вони використовуються для виконання різних завдань, пов'язаних з управлінням і контролем самих комп'ютерних мереж.

Завдання автоматизованої системи прийняття рішень:

– *маршрутизація трафіка* – системи маршрутизації приймають рішення щодо передавання даних у комп'ютерних мережах. Вони визначають оптимальні шляхи передавання даних, враховуючи різні фактори, такі як пропускна здатність мережі, затримка та наявність несправностей;

– *балансування навантаження* – ADMS може використовуватися для розподілу навантаження між серверами мережі. Вони можуть аналізувати завантаження серверів і приймати рішення про перенаправлення запитів клієнтів на доступні сервери для оптимального розподілу навантаження;

– *безпека мережі* – ADMS використовуються для виявлення та запобігання загрозам безпеці в комп'ютерних мережах. Вони можуть автоматично аналізувати мережевий трафік, виявляти аномалії та вживати заходів для блокування або обмеження доступу до потенційно шкідливих чи небажаних ресурсів;

– *управління пропускнуою здатністю* – ADMS можуть контролювати використання пропускнуої здатності мережі та приймати рішення про пріоритети доступу до ресурсів мережі, наприклад встановлювати обмеження використання смуги пропускання для певних типів трафіка чи додатків;

– *оптимізація ресурсів* – ADMS можуть аналізувати використання ресурсів у мережі, таких як пропускна здатність, процесорний час і пам'ять, і приймати рішення про виділення ресурсів на основі заданих критеріїв і пріоритетів.

Усі ці системи прийняття рішень зазвичай ґрунтуються на алгоритмах і правилах, визначених розробниками або адміністраторами мережі. Можуть використовувати дані з різних джерел, включаючи моніторинг мережі, журнали подій і статистику використання ресурсів, для аналізу та прийняття рішень у реальному часі.

2.3.2. Правове та законодавче регулювання в Україні

Нормативно-правова база України з захисту інформації включає законодавчі акти, накази, постанови та розпорядження, що регулюють захист інформації в різних сферах діяльності. Основними нормативними актами щодо захисту інформації в Україні є:

– Конституція України (ст. 17) – встановлює загальні принципи правового захисту прав людини, включаючи право на конфіденційність і захист інформації;

– Закон України «Про основи національної безпеки України» (ст. 8) – визначає основні напрями державної політики з питань національної безпеки в інформаційній сфері, визначає комплексні заходи щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України;

– Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» – визначає правові та організаційні засади захисту інформації в Україні, а також встановлює вимоги до захисту інформаційних систем та обмеження доступу до конфіденційної інформації;

– Закон України «Про оперативно-розшукову діяльність» – регулює діяльність правоохоронних органів у сфері оперативно-розшукової діяльності, включаючи захист інформації, що підлягає конфіденційності;

– Закон України «Про інформацію» – визначає правові засади отримання, поширення та захисту інформації, включаючи права та обов'язки суб'єктів інформаційних відносин;

– Закон України «Про охорону персональних даних» – регулює збір, зберігання, використання та захист персональних даних громадян;

– Закон України «Про кібербезпеку» – встановлює правові засади забезпечення кібербезпеки в Україні, включаючи захист інформаційних систем від кіберзагроз;

– Закони України «Про інформатизацію», «Про державну таємницю», «Про захист персональних даних» – визначають законодавче оформлення статусу, володарів і користувачів інформації, систем обробки та захисту інформації.

Крім того, існують інші закони, постанови та нормативні акти, що регулюють захист інформації в конкретних сферах, наприклад фінансовій, медичній, банківській тощо. Нормативно-правова база України постійно розвивається та оновлюється з метою вдосконалення захисту інформації та пристосування до сучасних викликів.

Державними органами, що створюють та впроваджують у життя політику інформаційної безпеки, є Президент України та Рада Національної безпеки України, Кабінет Міністрів України, Верховна рада України, Служба спеціального зв'язку та захисту інформації України (Держспецзв'язку України – уповноважений орган регулювання відносин у галузі інформаційної безпеки в Україні).

Основу системи стандартизації в Україні, що регулює відносини в зазначених напрямках діяльності, становлять Закони України «Про сертифікацію», «Порядок проведення робіт із сертифікації засобів забезпечення технічного захисту інформації загального призначення» (введений у дію Наказом ДСТСЗІ СБ України і Держстандарту України від 09.07.2001 року № 329/32), «Положення про державну експертизу в сфері технічного захисту інформації» (затверджено наказом Департаменту спеціальних телекомунікаційних систем і захисту інформації Служби безпеки України від 29.12.1999 року № 62) тощо.

Відповідальність громадян за порушення законодавства в галузі інформаційної безпеки визначаються ст. 361-363 розд. XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Кримінального кодексу України.

Нормативно-правову базу захисту інформації в Україні становлять закони, стандарти та нормативно-правові документи, перелік яких наведено в дод. 1. Нормативно-правові документи міжнародних стандартів на території України мають рекомендаційний характер.

Нормативно-правова база України з захисту інформації включає різні законодавчі акти, накази, постанови та розпорядження, що регулюють захист інформації в різних сферах діяльності. Основними нормативними актами, захисту інформації в Україні є:

– Конституція України – встановлює загальні засади правової захисту прав людини, включаючи право на конфіденційність і захист інформації;

– Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» – визначає правові та організаційні засади захисту інформації в Україні, а також встановлює вимоги щодо захисту інформаційних систем та обмеження доступу до конфіденційної інформації;

– Закон України «Про оперативно-розшукову діяльність» – регулює діяльність правоохоронних органів у сфері оперативно-розшукової діяльності, включаючи захист інформації, що підлягає конфіденційності;

– Закон України «Про інформацію» – визначає правові засади отримання, поширення та захисту інформації, включаючи права та обов'язки суб'єктів інформаційних відносин;

– Закон України «Про охорону персональних даних» – регулює збір, зберігання, використання та захист персональних даних громадян;

– Закон України «Про кібербезпеку» – встановлює правові засади забезпечення кібербезпеки в Україні, включаючи захист інформаційних систем від кіберзагроз.

Крім того, існують інші закони, постанови та нормативні акти, що регулюють захист інформації в конкретних сферах, наприклад фінансовій, медичній, банківській тощо. Нормативно-правова база України постійно розвивається та оновлюється з метою удосконалення захисту інформації та пристосування до сучасних викликів у цій сфері.

2.3.3. Загрози безпеці інформації в мережах

Загроза в кібербезпеці належить до потенційної можливості спричинити шкоду комп'ютерним системам, мережам або даним. Це може бути предмет, подія або дія, що може призвести до порушення безпеки і викликати негативні наслідки. Загрози включають такі фактори, як зловмисні програми (віруси, черв'яки, троянські коні), хакерські атаки,

соціальний інжиніринг, витоки інформації, фізичний доступ до комп'ютерних систем тощо.

Атака в кібербезпеці – конкретний спосіб або метод, використовуваний для виконання зловмисних дій або незаконного доступу до комп'ютерних систем, мереж або даних. Атаки можуть бути різного типу і мети, наприклад введення зловмисного коду, отримання несанкціонованого доступу до системи, викрадення конфіденційної інформації, розповсюдження дезінформації тощо. Атаки можуть бути спрямовані на певну організацію, систему або особу.

Кібератака – специфічний вид атаки, виконуваний із використанням комп'ютерних систем і мереж. Це зловмисна діяльність, спрямована на порушення безпеки цифрових систем, викрадення, пошкодження або незаконний доступ до даних, перешкоджання нормальному функціонуванню комп'ютерних мереж або навмисне завдання шкоди комп'ютерним системам чи інфраструктурі. Кібератаки можуть включати різні методи, такі як DDOS-атаки (атаки на відмову в обслуговуванні), фішинг, введення зловмисного коду, розповсюдження шкідливих програм тощо. Кібератаки можуть бути спрямовані на різні суб'єкти, включаючи урядові структури, бізнес-організації, особисті комп'ютери тощо.

Отже, *загроза* – це потенційна можливість, атака – конкретний метод, а кібератака – це атака, виконувана з використанням комп'ютерних систем і мереж.

Вразливість системи – це слабкість, дефект або недолік у системі, що може бути використаний для незаконного вторгнення, втручання або зловживання. Вразливості можуть існувати на різних рівнях системи, включаючи апаратне забезпечення, операційну систему, мережеві протоколи, додатки та інтерфейси користувача. Вразливості можуть бути викликані різними факторами, такими як програмні помилки, недоліки в проєктуванні, недостатня аутентифікація або авторизація, незахищені мережеві протоколи, некоректна конфігурація системи тощо.

Недоліки захисту – це проблеми або недоліки в механізмах захисту системи, що призводять до недостатньої ефективності або обходу заходів безпеки і можуть виникати через неправильну конфігурацію, слабкі паролі, недостатнє відстеження подій, недостатнє оновлення програмного забезпечення або недоліки в самому захисті.

Нижче перераховані деякі загальні приклади вразливостей і недоліків захисту:

- вразливість введення – програмне забезпечення не перевіряє вхідні дані на належність інформації або дає змогу виконувати код, введений користувачем, що може призвести до виконання шкідливих команд або отримання несанкціонованого доступу;

- вразливість переповнення буфера – програма не контролює обсяг даних, що вводяться в буфер, що може призвести до перезапису даних або виконання шкідливого коду;

- вразливість вебдодатків – недостатні перевірки автентифікації, контроль доступу до вебресурсів, XSS (міжсайтовий скриптинг) або SQL-ін'єкції;

- вразливості операційних систем – слабкі паролі адміністратора, недостатнє оновлення патчів і вразливість до відомих атак, таких як атаки переповнення буфера або атаки відмови в обслуговуванні (DoS);

- вразливості мережевих протоколів: деякі протоколи можуть мати слабкі місця, що дають змогу атакам здійснювати перехоплення даних, підробку пакетів або DoS-атаки;

- недоліки захисту паролів – слабкі паролі, використання одного пароля для кількох акаунтів, недостатнє шифрування паролів можуть зробити систему вразливою до атак на паролі;

- недоліки захисту: неправильна конфігурація – неправильне налаштування системи або додатків може призводити до вразливостей, наприклад неналежна конфігурація файрволу, що дає змогу небажаним зовнішнім з'єднанням проникати в систему;

– недоліки захисту: слабкі паролі – використання слабких паролів або використання одного і того самого пароля для кількох ресурсів може зробити систему легкодоступною для несанкціонованого доступу;

– недоліки захисту: недостатнє відстеження подій – недостатній моніторинг і аналіз подій у системі може призвести до непомічення аномальної або зловмисної активності, наприклад відсутність системи журналювання подій або недостатнє аналітичне програмне забезпечення;

– недоліки захисту: недостатнє оновлення програмного забезпечення – непостійне оновлення програмного забезпечення і патчів може залишити систему вразливою до відомих атак і вразливостей;

– недоліки захисту: недоліки в самому захисті – іноді в системах можуть бути виявлені недоліки або вразливості, що дають змогу обходити заходи безпеки, наприклад уразливість у механізмах автентифікації або авторизації.

Можливі способи здійснення загрози:

– технічними каналами, що включають канали побічних електромагнітних випромінювань і наведень, акустичні, оптичні, радіо- та радіотехнічні, хімічні та інші канали;

– каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;

– несанкціонованим доступом шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм і вкорінення комп'ютерних вірусів.

Перші два способи за принципом належать до *фізичного* доступу, останній – *логічного* доступу.

Загроза спрямована на порушення таких властивостей інформації або АС:

– *конфіденційності*;

- цілісності;
- доступності інформації;
- спостереженості та керованості АС.

Ці приклади вразливостей і недоліків захисту нагадують про необхідність постійно оновлювати і підтримувати системи та програмне забезпечення, використовувати сильні паролі, оновлювати програмне забезпечення і виконувати адекватне моніторингове забезпечення, регулярно перевіряти системи на наявність вразливостей і вживати відповідних заходів безпеки для запобігання атакам.

Осіб, які реалізують загрози, називають порушником, зловмисником або хакером – це терміни, що можуть мати різні значення залежно від контексту.

Порушник (англ. User violator) – це особа, яка порушує правила, закони або норми, може бути причетною до різних видів порушень.

Зловмисник – це особа, яка вчиняє злочини або вчиняє дії, що завдають шкоди іншим людям.

Хакер (англ. hacker) – це особа, яка експерт у галузі комп'ютерної технології і використовує свої знання для отримання несанкціонованого доступу до комп'ютерних систем або мереж. Хакери можуть займатися різними видами активності, від доброзичливих (етичного хакінгу для виявлення вразливостей у системах) до зловмисницьких (незаконного злому, крадіжки даних тощо).

Важливо пам'ятати, що ці терміни мають різні конотації, і не всі порушники, зловмисники або хакери є злочинцями. Також слід зазначити, що хакерство в більшості країн є незаконним, але існують експерти, які використовують свої знання для доброзичливих цілей, таких як забезпечення кібербезпеки.

Модель порушника – це всебічна структурована характеристика порушника, використовувана сумісно з моделлю загроз для розроблення політики безпеки інформації.

В Україні *структура моделі порушника* включає:

– *категорію осіб, до якої може належати порушник* (внутрішні порушники; користувачі; інженерний склад; співробітники відділів, що супроводжують ПЗ; технічний персонал, що обслуговує будинок; співробітники служби безпеки; керівники; зовнішні порушники);

– *мету порушника* (отримання необхідної інформації; отримання можливості вносити зміни в інформаційні потоки відповідно до своїх намірів; завдання збитків шляхом знищення матеріальних та інформаційних цінностей);

– *повноваження порушника в АС* (запуск фіксованого набору задач (програм); створення і запуск власних програмних засобів; управління функціонуванням і внесення змін до конфігурації системи; підключення чи зміна конфігурації апаратних засобів);

– *технічну оснащеність порушника* (апаратні засоби; програмні засоби; спеціальні засоби).

2.3.4. Несанкціонований доступ до інформації

Історія розвитку інформаційних систем свідчить про те, що системи постійно зазнають нових вразливостей. Хоча ці вразливості врешті-решт нейтралізуються, це відбувається з певним запізненням. Протягом цього періоду система залишається особливо вразливою і може стати об'єктом компрометації. Особливо небезпечно, коли нові вразливості виявляються вперше самими потенційними зловмисниками. Тому *послідовний* підхід до забезпечення інформаційної безпеки є неефективним. *Упереджений захист* інформації стає більш ефективним за допомогою передбачення всіх можливих, передбачуваних і потенційних загроз, а також розроблення *комплексної системи захисту інформації*.

Комплексна система захисту інформації (КСЗІ) – сукупність технологій, процедур і політик, використовуваних для захисту

конфіденційності, цілісності та доступності інформації в організації або компанії. КСЗІ використовується для захисту інформації в комп'ютерних системах, мережах зв'язку, базах даних та інших інформаційних ресурсах.

Типові атаки на розподілені автоматизовані системи [8-11]:

– *віддалене проникнення (remote penetration)*. Атаки, що дають змогу реалізувати віддалене управління комп'ютером через мережу;

– *локальне проникнення (local penetration)*. Атака, що призводить до отримання несанкціонованого доступу до вузла, на якому вона ініційована;

– *віддалена відмова в обслуговуванні (remote denial of service)*. Атаки, що дають змогу порушити функціонування системи або перезавантажити комп'ютер через мережу (у тому числі Інтернет);

– *локальна відмова в обслуговуванні (local denial of service)*. Атаки, що дають змогу порушити функціонування системи або перезавантажити комп'ютер, на якому вони ініційовані. Приклади атак цього типу: аплет, що перезавантажує процесор (наприклад відкриттям великої кількості вікон великого розміру), що призводить до неможливості оброблення запитів інших програм;

– *сканування мережі (network scanning)*. Аналіз топології мережі і активних сервісів, доступних для атаки. Атака може здійснюватись за допомогою службового програмного забезпечення;

– *використання сканерів вразливостей (vulnerability scanning)*. Сканери вразливостей призначені для пошуку вразливостей на локальному або віддаленому комп'ютері. Вони в першу чергу призначені служити діагностичним інструментом системних адміністраторів, але можуть бути використані і як зброя для розвідки й атаки. Найвідоміші з таких програмних засобів – SATAN, SystemScanner, Xspider, nessus;

– *злом паролів (password cracking)*. Для цього використовуються програмні засоби, що підбирають паролі користувачів. Залежно від надійності системи зберігання паролів можуть використовуватись методи злому або підбору пароля за словником;

– *аналіз протоколів (sniffing – прослуховування трафіка)*. Пасивна атака, спрямована на розкриття конфіденційних даних, зокрема ідентифікаторів і паролів доступу.

До цієї класифікації не потрапили численні атаки, спрямовані на введення в оману протоколів пошуку в мережі. На наш погляд, слід додати такий пункт:

– *підміна об'єкта (spoofing)*. Типові приклади – несправжній DNS-сервер, підміна IP-адреси джерела (IP spoofing), несправжній ARP-запит (ARP spoofing).

Неважко помітити, що запропонована класифікація не є цілком послідовною. Перші чотири класи атак розрізняються здебільшого за кінцевим результатом (або метою реалізації), а наступні – способом їх здійснення.

Основні складові комплексної системи захисту інформації включають:

– *автентифікацію і авторизацію* – механізми використовуються для ідентифікації користувачів і надання їм відповідних прав доступу до інформаційних ресурсів;

– *криптографічні засоби* – використовуються для шифрування і розшифрування інформації з метою забезпечення конфіденційності, а також підписування даних для забезпечення цілісності;

– *захист мережевої інфраструктури* – включає мережеві файрволи, системи виявлення вторгнень (IDS), віртуальні приватні мережі (VPN) та інші засоби для захисту мережевих комунікацій;

– *фізичний захист* – забезпечує безпеку фізичного доступу до інформаційних ресурсів, таких як серверні приміщення, дата-центри та інші важливі точки інфраструктури;

– *управління доступом* – встановлює політики доступу до різних рівнів інформації та ресурсів, контролює і аудитує дії користувачів;

– *безпеку даних* – включає захист даних від несанкціонованого доступу, втрати або пошкодження шляхом використання резервного копіювання, реплікації та шифрування;

– *управління загрозами* – виявлення, моніторинг і відповідь на потенційні загрози безпеці інформації.

Ці компоненти працюють разом, щоб забезпечити повний цикл захисту інформації в організації або компанії. Розроблення і впровадження КСЗІ вимагає комплексного підходу та врахування специфіки конкретної організації і її потреб у захисті інформації.

Способи несанкціонованого доступу:

1. Непрямі методи доступу:

- *фотографування моніторів;*
- *підслуховування;*
- *відео- та аудіоспостереження.*

2. Прямі методи доступу:

а) прямі без зміни структури системи:

- *копіювання носіїв даних;*
- *несанкціоноване використання терміналів інших користувачів;*
- *маскування під зареєстрованого користувача;*

б) прямі зі зміною структури системи:

- *використання програмних пасток;*
- *використання «троянських коней»;*
- *незаконне підключення до апаратури чи ліній зв'язку системи;*
- *виведення з ладу механізму захисту.*

Непрямі методи доступу. До непрямих методів відносять підслуховування, візуальне спостереження, розкрадання документів і машинних носіїв інформації, програм і атрибутів системи захисту, підкуп і шантаж співробітників, збір і аналіз відходів машинних носіїв інформації.

Наприклад, до технічних засобів підслуховування можна віднести лазерний мікрофон, надчутливі направлені мікрофони, стетоскопічні мікрофони (рис. 2.3, а) і диктофони (рис. 2.3, б).

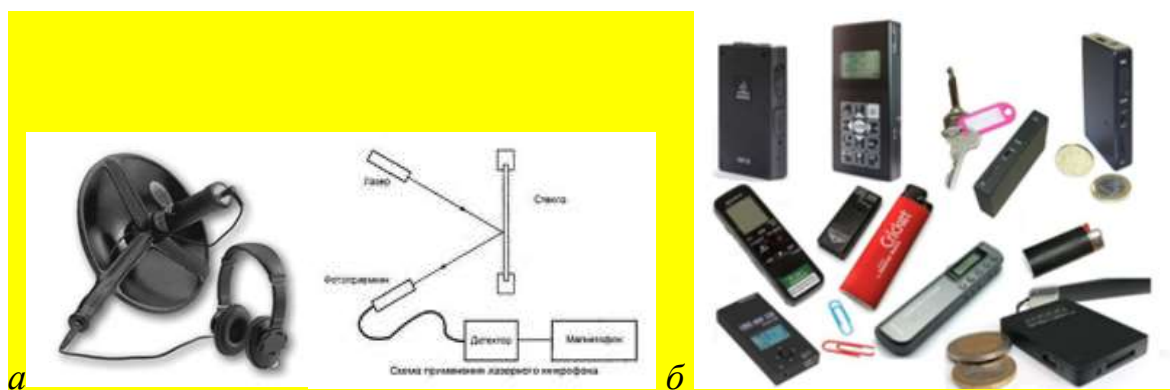


Рис. 2.3. Непрямі методи доступу: а – мікрофони; б – диктофони

До непрямих методів візуального спостереження можна віднести, наприклад, мініатюрні роботи-шпигуни Орнітоптер Nano-Hummingbird зі швидкістю 18 км/год, вагою 19 г, обладнаних відеокамерою, що виглядає як колібри (рис. 2.4); мініатюрні роботи-шпигуни, також відомі як мікророботи або нанороботи, що є робототехнічними пристроями, зазвичай мають розміри від кількох міліметрів до кількох сантиметрів і можуть бути створені з різних матеріалів, таких як метал, пластик або силікон (рис. 2.4). Мініатюрні роботи-шпигуни можуть мати вбудовані камери, мікрофони, сенсори руху та інші пристрої для збору інформації. Вони можуть бути використані для здійснення розвідувальних місій у важкодоступних місцях, таких як щілини, підлоги, стелі або навіть внутрішні органи людського організму.

Їхнє призначення – здійснення різних завдань, включаючи шпигунство або розвідувальні операції. Наприклад, вони можуть бути використані військовими для отримання розвідувальної інформації, у поліції для проведення оперативних заходів, медицині для внутрішнього обстеження

пацієнтів, комерційних цілях, наприклад для вивчення недоступних місць у будівництві або інженерних дослідженнях.

Слід зазначити, що з використанням мініатюрних роботів-шпигунів постає питання щодо приватності та етичності. У деяких країнах існують правові обмеження щодо використання таких роботів, особливо щодо їхнього застосування у приватних сферах.



Рис. 2.4. Різні типи непрямих методів візуального спостереження

Непрямі методи розкрадання документів і машинних носіїв інформації за допомогою *закладних пристроїв* – дротових, що демаскуються дротом, або бездротових, що демаскуються випромінюванням (рис. 2.5).



Рис. 2.5

До *прямих методів доступу без модифікації структур* належать *комп'ютерні віруси* – це невеликі програми, що після впровадження в електронно-обчислювальну машину самостійно поширюються шляхом

створення своїх копій, а при виконанні певних умов мають негативний вплив на комп'ютерні системи.

Слід звернути увагу на такі типи комп'ютерних вірусів, як логічні бомби, хробаки, троянські коні.

Принцип дії

Логічні бомби – це програми, що постійно перебувають в електронно-обчислювальній машині та виконуються тільки при дотриманні певних умов.

Хробаки – це програми, що виконуються кожного разу при завантаженні системи, мають здатність переміщуватися в ПК або мережі і самовідтворюватися.

Троянські коні – це програми, отримані шляхом явної зміни або додавання команд до програм користувача.

Ланцюжкові віруси. У зв'язку з помилковими повідомленнями про неіснуючі віруси з'явилася дотепна пародія на ланцюжковий вірус. Не дивлячись на те, що вона була повністю вигаданою, багато користувачів Internet під дією вірусної істерії сприйняли її серйозно. Ось яскраві фрагменти з опису: «...Він не чіпатиме дані на вашому жорсткому диску, натомість зітре все з комп'ютерів, розташованих ближче, ніж у 20 футах від вашого... Він зіпсує магнітні смуги на ВСІХ ваших кредитних картках... Він перенастроюватиме ваш холодильник так, що все ваше морозиво розтане, а молоко скисне... Він перепрограмує ваш телефон так, що по ньому можна буде додзвонитися тільки вашій матері... Він примусить вас бігати з ножицями, поки ви не виколете кому-небудь око... Він перетворить все ваше м'ясо в спам (оригінальне значення слова spam — консервованій ковбасний фарш, заміник м'яса; переносне – одержані вами непотрібні вам листи, найчастіше рекламного характеру)... Це лише деякі ознаки інфекції!» [4].

Прямі методи з модифікацією структур. *Модифікація структур* – це несанкціонована заміна алгоритмічної, програмної та/або технічної

структури системи з метою отримання несанкціонованого доступу до інформації.

Модифікація структури реалізуються *створенням закладок* або *люків*.

Закладкою називається несанкціонована зміна структури комп'ютерних систем на етапах розроблення і модернізації.

Люк – це програма або апаратна закладка для здійснення неконтрольованого входу в програми, використання привілейованих режимів роботи, обходу засобів захисту інформації.

Висновок: для незалежного захисту інформації необхідно зробити кроки за такими напрямками:

- по-перше, обов'язково мати комплексний характер захисту;
- по-друге, регламентувати коло осіб, здатних мати доступ до інформації;
- по-третє, регламентувати рівні доступу до інформації;
- по-четверте, використовувати програмне забезпечення власного розроблення;
- по-п'яте, забезпечити своєчасний антивірусний захист.

Методи захисту інформації від випадкових загроз

Для захисту інформації від випадкових загроз використовують комплекс методів:

- дублювання інформації;
- підвищення надійності технічних засобів обробки інформації;
- підвищення відмовостійкості технічних засобів обробки інформації;
- блокування помилкових дій користувачів і персоналу;
- оптимізація взаємодії користувачів та обслуговуючого персоналу;
- мінімізація втрат від аварій і стихійних лих.

Контрольні запитання

1. Назвіть типи додатків, що може виконувати комп'ютер, підключений до мережі.
2. Дайте визначення і призначення поняттю мережевій операційній системі.
3. Дайте визначення таким поняттям: файлова служба, файл-сервер, вебслужба, вебсервер, веббраузер, вебсайт.
4. Дайте визначення поняттю мережових інтерфейсів і визначте призначення фізичного, логічний інтерфейсів, інтерфейсу комп'ютера.
5. З чого складається найпростіша мережа?

Бібліографічний список

1. Jamsa K. Hacker Proof Paperback. Hacker_Proof. 2002. 750 p.
2. Nilsson N. J. Principles of Artificial Intelligence. Tioga– Springer–Verlag, 1980. 164 с.
3. Банкет В. Л., Іващенко П. В., Іщенко М. О. Завадостійке кодування в телекомунікаційних системах. Одеса: ОНАЗ ім. О. С. Попова, 2011. 100 с.
4. Бізюк А. В., Бізюк І. Г. Створення WEB-сторінок. Харків: УкрДАЗТ, 2008. 68 с.
5. Воробієнко П. П., Каразей В. М., Скопа О. О. Протоколи міжмережної взаємодії. Одеса: УДАЗ ім. О. С. Попова, 1999. Вип. 1. 50 с.
6. Воробієнко П. П., Нікітюк Л. А., Резніченко П. І. Телекомунікаційні та інформаційні мережі. Київ: САММІТ-Книга, 2010. 708 с.
7. Захарченко М. В. Системи передачі даних. Т. 1. Завадостійке 3-38 кодування. Одеса: Фенікс, 2009. 448 с.
8. Кононович В., Кононович І., Тардаскіна Т. Основні принципи інформаційної безпеки відкритих систем. Ч. 3. Ієрархія систем та вимог до безпеки. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. Київ, 2007. Вип. 1 (14). С. 88–98.
9. Кононович В., Тардаскіна Т. Основні принципи інформаційної безпеки відкритих систем. Ч. 1. Міри інформації та властивості інформаційних процесів відкритих систем. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. Київ, 2006. Вип. 1 (12). С. 44–55.
10. Кононович В., Тардаскіна Т. Основні принципи інформаційної безпеки відкритих систем. Ч. 2. Міри інформації та властивості інформаційних процесів відкритих систем. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. Київ, 2006. Вип. 1 (12). С. 84–95.

11. Матов О. Я., Василенко В. С. Модель загроз у розподілених мережах. *Реєстрація, зберігання і обробка даних*. 2008. Т. 10. № 1. С. 91–102.
12. Мінухін С. В., Кавун С. В., Знахур С. В. Комп'ютерні мережі. Загальні принципи функціонування комп'ютерних мереж. Харків: ХНЕУ, 2008. 210 с.
13. Микитишин А. Г., Митник М. М., Стухляк П. Д. Телекомунікаційні системи та мережі. Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2017. 384 с.
14. Нікітюк Л. А. Архітектура інформаційних мереж / за ред. М. В. Захарченка. Одеса: УДАЗ ім. О. С. Попова, 2000. 60 с.
15. Руденко О. Г., Бодяньський Є. В. Штучні нейронні мережі. Харків: ТОВ «Компанія СМІТ», 2006. 404 с.
16. Сторчак К. П., Ткаленко О. М. Системи розподілу інформації: навч. посіб. Київ: ДУТ, 2018. 98 с.
17. Centre for computing history. Digital Micro PDP-11/53. URL: <https://www.computinghistory.org.uk/det/39684/Digital-Micro-PDP-11-53/>.
18. Enterprise Networking Design, Support, and Discussion. URL: www.reddit.com/r/networking.
19. Network Security. *TechTarget Networking*. URL: searchnetworking.techtarget.com.
20. Network World – новости, аналитические статьи и обзоры по компьютерным сетям, технологиям сетей. *Онлайн-издание*. URL: www.networkworld.com.
21. Portrait by AI program sells for \$432,000. Get the new BBC technology newsletter. URL: <https://www.bbc.com/news/technology-45980863>.
22. Tanenbaum A., Wetherall D. Computer Networks. *5th Edition*. *Pearson Prentice Hall*. URL: www.goodreads.com/book/show/84567783.
Tanenbaum_Wetherall.

23. Бездротовий інтерфейс. Як працює NFC, Bluetooth і чому повернувся ІК-порт? Сайт компанії «Сота хата». URL: <https://sotahata.com.ua/wireless-technology.html>.
24. Безпека та відеоспостереження. Перспективи Bluetooth Mesh для розумного будинку. URL: <https://oxorona.com/bluetooth-mesh/>.
25. Комп'ютери, мережі та ІТ-технології. Український портал. Фірма «UKRCOMP». URL: www.ukrcomp.com.ua.
26. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р. URL: <https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text>.
27. Розвиток інтелектуального транспорту за допомогою штучного інтелекту, 5G та граничних обчислень. Інтерв'ю з Ван Ліном та Кунхонг Ченом. 11.08.2022. *ПРОКСИС™ промислові комп'ютери і системи*. URL: <https://www.proxis.ua/uk/show-article/531/>.
28. ТОП-3 технології майбутнього, які змінюють логістику. ТРАНС.ЄУ Україна. Логістична Платформа Trans.eu. URL: <https://www.trans.eu/ua/blog/lohistyka-4-0/technologii-majbutniogo/>.
29. Швидкий Ю. Як використовують хмари в ІТ: все, що ви хотіли знати про хмарні технології. URL: <https://highload.today/uk/blogs/yak-vikoristovuyut-hmari-v-it-vse-shho-vi-hotili-znati-pro-hmarni-tehnologiyi/>.
30. Що таке модуляція і різновиди модульованих сигналів? URL: <https://conture.by/post/422>.
31. Що таке приватна мережа передачі даних та як вона допомагає працювати бізнесу? KYIVSTAR BUSINESS HUB. URL: <https://hub.kyivstar.ua/news/shho-take-pryvatna-merezha-peredachi-danyh-ta-yak-vona-dopomagaye-praczuuvaty-biznesu/>.
32. Що таке технологія NFC і як вона з'явилася? Сайт «Смарт-карти України» – компанії з продажу та впровадження RFID-систем будь-якого рівня складності. URL: <https://idcard.com.ua/ua/blog/chto-takoe-tehnologiya-nfc-istoriya-ee-vozniknoveniya/>.

Нормативно-правові документи України

1. Закон України «Про інформацію» № 2657-XII від 02.10.1992 р. (ВВР. 1992. № 48. Ст. 650).
2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 р. № 80/94-ВР (зі змінами, внесеними згідно з Законом України № 1703-IV від 11.05.2004 р., у редакції Закону України № 2594-IV від 31.05.2005 р. (ВВР. 2005. № 26. Ст. 347)).
3. Закон України «Про державну таємницю» № 3855-XII від 21.01.1994 р. (ВВР. 1994. № 16. Ст. 93) (остання редакція № 1519-IV від 19.02.2004 р.).
4. Закон України «Про електронний цифровий підпис» № 852-IV від 22.05.2003 р. (ВВР. 2003. № 36. Ст. 276).
5. Закон України «Про електронні документи і електронний документообіг» № 851-IV від 22.05.2003 р. (ВВР. 2003. № 36. Ст. 275) (зі змінами, внесеними згідно з Законом України № 2599-IV від 31.05.2005 р. (ВВР. 2005. № 26. Ст. 349)).
6. Закон України «Про телекомунікації» № 1280-IV (ВВР. 2004. № 12. Ст. 155) (остання редакція від 01.02.2007 р.).
7. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» від 23.02.2006 р. № 3475-IV (ВВР. 2006. № 30. Ст. 258).
8. Концепція технічного захисту інформації в Україні: затв. Постановою Кабінету Міністрів України від 08.10.1997 р. № 1126.
9. Положення про технічний захист інформації в Україні: затв. Указом Президента України від 27.09.1999 р. № 1229.
10. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.

11. НД ТЗІ 1.1-002-99. Загальні положення по захисту інформації в комп'ютерних системах від несанкціонованого доступу: затв. Наказом ДСТСЗІ СБ України від 28.04.1999 р. № 22.

12. НД ТЗІ 1.1-003-99. Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу: затв. Наказом ДСТСЗІ СБ України від 28.04.1999 р. № 22.

13. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: затв. Наказом ДСТСЗІ СБ України від 28.04.1999 р. № 22.

14. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу: затв. Наказом ДСТСЗІ СБ України від 28.04.1999 р. № 22.

15. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі: затв. Наказом ДСТСЗІ СБ України від 04.12.2000 р. № 53.

16. НД ТЗІ 3.7-001-99. Методичні вказівки по розробці технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі: затв. Наказом ДСТСЗІ СБ України від 28.04.1999 р. № 22.

17. НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу: затв. Наказом ДСТСЗІ СБ України від 20.12.2000 р. № 60.

18. НД ТЗІ 2.1-001-01. Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення: затв. Наказом ДСТСЗІ СБ України від 09.02.2001 р. № 2.

19. НД ТЗІ 2.5-008-02. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2: затв. Наказом ДСТСЗІ СБ України від 13.12.2002 р. № 84.

20. НД ТЗІ 2.5-010-03. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу: затв. Наказом ДСТСЗІ СБ України від 02.04.2003 р. № 33.

21. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі: затв. Наказом ДСТСЗІ СБ України від 08.11.2005 р. № 125.

22. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт: затв. Наказом Держстандарту України від 19.12.1996 р. № 511.

23. Положення про державну експертизу в сфері технічного захисту інформації: затв. Наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 29.12.1999 р. № 62, зареєстр. в Міністерстві юстиції України 24.01.2000 р. за № 40/4261.

24. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок (ТР ЕОТ-95): затв. Наказом ДСТЗІ від 09.06.1995 р. № 25.

25. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок (ТР ТЗІ-ПЕМВН-95): затв. Наказом ДСТЗІ від 09.06.1995 р. № 25.

26. Порядок проведення робіт із сертифікації засобів забезпечення технічного захисту інформації загального призначення: введ. в дію Наказом ДСТСЗІ СБ України і Держстандарту України від 09.07.2001 р. № 329/32, зареєстр. в Міністерстві юстиції України 26.07.2001 р. за № 640/5831.

27. Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах: затв. Постановою Кабінету Міністрів України від 16.02.1998 р. № 180.

28. ГОСТ 34.201-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначения документов при создании автоматизированных систем (взамен ГОСТ 24.101-80, ГОСТ 24.102-80).

29. ГОСТ 34.601-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания (взамен ГОСТ 24.601-86, ГОСТ 24.602-86).

30. ГОСТ 34.602-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы (взамен ГОСТ 24.201-85).

31. ГОСТ 34.603-92. Информационная технология. Виды испытаний автоматизированных систем (взамен ГОСТ 24.104-85 в части разд. 3).

32. РД 50-34.698-90. Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы – требования к содержанию документов.

33. Закон України «Про захист персональних даних».

Нормативно-правові документи міжнародних стандартів:

34. Common Criteria for Information Technology Security Evaluation: Version 2.1. CCIMB-99-031. August 1999.

35. Common Methodology for Information Technology Security Evaluation: Version 2.3. CCMB-2005-08-004. - August 2005.

36. ISO/IEC 10745:1995. Information technology – Open Systems Interconnection – Upper layers security model.

37. ISO/IEC 13594:1995. Information technology – Lower layers security.

38. ISO/IEC 10181-1:1996. Information technology – Security frameworks for open systems: Overview.

39. ISO/IEC 10181-2:1996. Information technology – Security frameworks for open systems: Authentication framework.
40. ISO/IEC 10181-3:1996. Information technology – Security frameworks for open systems: Access control framework.
41. ISO/IEC 10181-4:1996. Information technology – Security frameworks for open systems: Non-repudiation framework.
42. ISO/IEC 10181-5:1996. Information technology – Security frameworks for open systems: Confidentiality framework.
43. ISO/IEC 10181-6:1996. Information technology – Security frameworks for open systems: Integrity framework.
44. ISO/IEC 10181-7:1996. Information technology – Security frameworks for open systems: Security audit framework.
45. ISO/IEC 18045:2005. Information technology – Security techniques – Methodology for IT security evaluation.
46. ISO/IEC 7498-1:1994. Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model.
47. ISO/IEC 9545:1994. Information technology – Open Systems Interconnection – Application Layer Structure.
48. ISO/IEC 8822:1994. Information technology – Open Systems Interconnection – Presentation Service Definition.
49. ISO/IEC 8326:1996. Information technology – Open Systems Interconnection – Session Service Definition.
50. ISO/IEC 8072:1996. Information technology – Open Systems Interconnection – Transport Service Definition.
51. ISO/IEC 8348:2002. Information technology – Open Systems Interconnection – Network Service Definition.
52. ISO/IEC 8886:1996. Information technology – Open Systems Interconnection – Data Link Service Definition.

53. ISO/IEC 10022:1996. Information technology – Open Systems Interconnection – Physical Service Definition.
54. ISO/IEC 7498-2:1989. Information processing systems – Open Systems Interconnection - Basic Reference Model – Part 2: Security Architecture.
55. IT Baseline Protection Manual – BSI (Federal Agency for Security in Information Technology). – October 2000.
56. Security Architecture for Open Systems Interconnection for CCITT Applications. Recommendation X.800 – CCITT, Geneva, 1991.
57. ISO/IEC 17799:2000. Information technology – Code of practice for Information security management. International Standard.
58. ISO/IEC 15408-1:2005. Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.
59. ISO/IEC 15408-2:2005. Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements.
60. ISO/IEC 15408-3:2005. Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements.
61. ISO/IEC 27001:2005. Information technology – Security techniques – Information security management systems – Requirements.
62. ISO/IEC 27002:2005. Information technology – Security techniques – Code of practice for information security management.
63. IEEE802.10B. IEEE Standards for Interoperable Local Area Network (LAN) Security (SILS): Part B - Secure Data Exchange. – April 1992.

Навчальний посібник

Бантюков Сергій Євгенович,
Бізюк Ірина Григорівна,
Казанко Олександр Віталійович

Серія Комп'ютерні науки
МЕРЕЖЕВІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Частина 1

Відповідальний за випуск Бізюк І. Г.

Редактор Ібрагімова Н. В.

Підписано до друку 07.06.2023 р.
Умовн. друк. арк. 7,5. Тираж . Замовлення № .
Видавець та виготовлювач Український державний університет
залізничного транспорту,
61050, Харків-50, майдан Фейєрбаха, 7.
Свідоцтво суб'єкта видавничої справи ДК № 6100 від 21.03.2018 р.