НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ

ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У СФЕРІ ЦИВІЛЬНОГО ЗАХИСТУ

Підручник

Рекомендовано до друку і використання в освітньому процесі
вченою радою НУЦЗ України

Харків 2021

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ

ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У СФЕРІ ЦИВІЛЬНОГО ЗАХИСТУ

Підручник

Рекомендовано до друку і використання в освітньому процесі
вченою радою НУЦЗ України

Харків 2021

УДК35.078.3(075.8)

Авторський колектив:

А. Б. Фещенко, кандидат технічних наук, доцент
Л. В. Борисова, кандидат юридичних наук, доцент
О. В. Закора, кандидат технічних наук, доцент
В. О. Собина, кандидат технічних наук, доцент
Д. В. Тарадуда, кандидат технічних наук
М. О. Дement, кандидат педагогічних наук
І. М. Неклонський, кандидат військових наук

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

Рекомендовано до друку і використання в освітньому процесі
вченою радою НУЦЗ України
(протокол від 27.05.2021 № 9)

Фещенко А. Б.
Телекомунікаційні системи та інформаційні технології у сфері цивільного захисту: підручник /А. Б. Фещенко, Л. В. Борисова, О. В. Закора, В. О. Собина, Д. В. Тарадуда, М. О. Дement, І. М. Неклонський. – Х.: НУЦЗУ, 2021. – 728 с.

У підручнику систематизований науково-дослідний підхід по впровадженню і організації експлуатації автоматизованих систем управління діяльністю підрозділів ДСНС Украйни на основі стандартних протоколів та інтерфейсів відомчої цифрової телекомунікаційної мережі, яка утворюється на ресурсах мереж з термінальним кінцевим устаткуванням абонентів. Розглянута система захисту інформаційних ресурсів з обмеженим доступом на об'єктах інформаційної діяльності підрозділів цивільного захисту відповідно до вимог діючих стандартів та нормативних документів.

Підручник призначено для здобувачів вищої освіти, які навчаються на другому (магістерському) рівні в галузі знань 26 "Цивільна безпека".

УДК35.078.3(075.8)
© Фещенко А. Б., Борисова Л. В., Закора О. В., Собина В. О., Тарадуда Д.В., Дement М. О., Неклонський . М. І.,2021
© НУЦЗУ, 2021

ВСТУП

Від ефективного використання сучасних інформаційних технологій існуючих телекомунікаційних мереж, розширення сервісу і поліпшення якості обслуговування залежить ефективність забезпечення державних органів, суб'єктів господарської діяльності і населення країни інформаційними послугами.

Розвиток інфокомунікацій в світі зазнає революційних змін, в основу яких покладені новітні інформаційні технології, що стосуються об'єднання телекомунікаційних, інформаційних технологій та систем безпроводового зв'язку. Будівництво інфокомунікаційних систем нового покоління, спроможних забезпечити мультисервісні послуги, спирається на цілий ряд інформаційних технологій і апаратних рішень, що ґрунтуються на пакетній передачі цифрової інформації в телекомунікаційних мережах.

Проблема, перед якою сьогодні опинилися підрозділи пожежно-рятувальної служби, полягає у тому, що застосовані у цих підрозділах системи автоматизованого зв'язку і оперативного управління перестали задовольняти як за кількістю і якістю наданої персоналу інформації, так і за набором функцій. І справа навіть не в тому, яке програмне забезпечення або які за потужністю засоби обчислювальної техніки при цьому використовуються.

Справа в тому, що змінилася точка зору на основні функції автоматизованих систем, а також у застарілій технології проектування таких систем. Функції існуючих автоматизованих систем (АС) зазвичай обмежуються поточним контролем за основними процесами діяльності, рутинною обчислювальною роботою і, у рідких випадках, автоматизацією виконання локальних оперативних команд.

Функції сучасних і перспективних автоматизованих комп'ютерних систем значно розширюються як стосовно області керуючих впливів, так і в області інформаційного забезпечення. Цей процес зміни функцій супроводжується тим, що стара термінологія, яка відноситься до комп'ютерних технологій, поступово починає витіснятися новою, у якій визначальними стають поняття «інформаційні системи», «інформаційно-управляючі системи», «інтегровані системи управління» і т.п. Даний процес зміни термінології відображає перехід комп'ютерних систем управління на якісно новий рівень, де основну роль грають інформаційні технології, точніше, технології інформаційної підтримки прийнятих (автоматично або людиною) рішень по управлінню процесом оперативної та службової діяльності підрозділів ДСНС.

Виходячи з цього, в даній лекції будуть розглянуті основи організації та побудови автоматизованих інформаційних систем (АІС), принципи їх побудови, функціонування та застосування для забезпечення діяльності підрозділів ДСНС України

РОЗДІЛ 1.
ОСНОВИ ОРГАНІЗАЦІЇ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ В ДСНС УКРАЇНИ

1.1 Терміни та визначення телекомунікацій в цивільному захисті

Телекомунікації (електрозв'язок) – передавання, випромінювання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних або інших електромагнітних системах[12].

Телекомунікаційні системи та інформаційні технології – складова системи управління силами цивільного захисту, що є сукупністю взаємопов'язаних структурних підрозділів ДСНС, мереж та засобів телекомунікацій та інформатизації різного призначення, які діють узгоджено щодо завдань, місця, часу та використовуються. Розгортаються або створюються за планом для вирішення завдань забезпечення управління силами цивільного захисту.

Телекомунікаційна система – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання (випромінювання) або приймання сигналів, знаків, звуків, рухомих чи нерухомих зображень тощо.

Телекомунікаційна мережа(ТМ)– комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням.

Архітектура ТМ – це принцип побудови мережі, що виражає єдність і взаємозв'язок фізичної та логічної структур (табл. 1.1) [20, 21].

ПервинноюТМ називається сукупність мережних вузлів (МВ), мережних станцій і з'єднувальних ліній передачі. процес обробки інформації, звертання до бази даних (БД) і формування управлінських рішень складають єдиний, як правило, незмінний алгоритм роботи персоналу диспетчерської служби і засобів автоматизації.

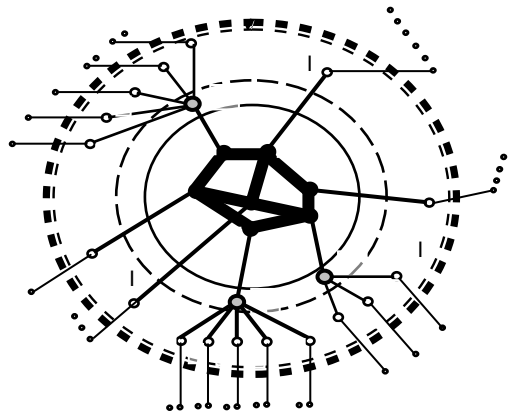
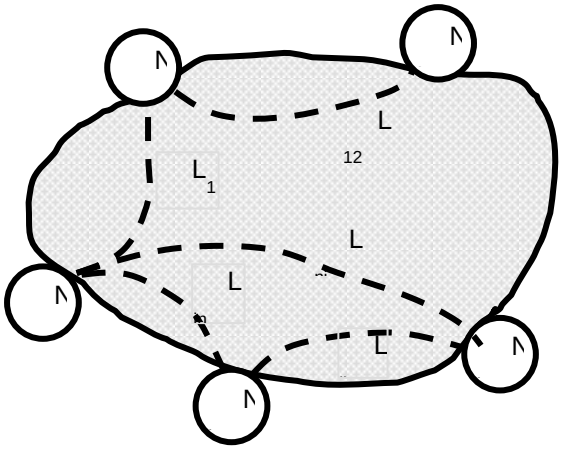
Вторинна ТМявляє собою сукупність комутаційних станцій, вузлів комутації, кінцевих абонентських пристроїв і каналів вторинної мережі, що утворені на базі каналів первинної мережі.

Основні класи багато рангових ТМ:

- ***Локальні мережі***(LocalAreaNetwork – LAN) – мережі, які охоплюють відносно невеликі території і характеризуються наявністю загального високошвидкісного середовища передачі даних.
- ***Мережі району*** (CampusAreaNetwork – CAN) – мережі, які об'єднують значно віддалені одна від одної абонентські системи або локальні мережі, але не вимагають віддалених комунікацій через телефонні лінії та модеми.

- ***Корпоративні мережі***(EnterpriseWideNetwork – EWN) – великі мережі, які працюють з єдиною метою.
- ***Глобальні мережі*** (WideAreaNetwork – WAN) – мережі, які охоплюють, як правило, досить велику територію, і для передачі даних використовують різні середовища, наприклад, виділені лінії зв'язку та лінії зв'язку, що комутуються, мережі передачі даних різних країн.

Таблиця. 1.1 – Структура ТМ

	**Фізична структура ТМ** – це схема зв'язку компонентів мережі, таких, як середовище передачі інформації (даних), апаратура передачі даних, вузли мережі з комплексом апаратури, обчислювальні комплекси, термінальні пристрої, робочі станції.
	***Логічна структура ТМ***– це принципи встановлення зв'язку, алгоритми організації процесів і управління ними, що визначають логіку функціонування програмних і апаратних засобів обміну інформацією

Глобальнамережа (WAN)– це складна система, що складається з великого числа різноманітних компонентів: комп'ютерів, концентраторів, маршрутизаторів, комутаторів, системного та прикладного програмного забезпечення [15, 20]

Глобальні мережі являють собою комбінацію локальних мереж, серверів і комунікаційного устаткування, що з'єднані комунікаційними каналами зв'язку.

***Інтерфейс*ТМ**– це набір функцій, які нижче лежачий рівень ТМ надає вище лежачому.

Правила, що визначають послідовність і структуру (формат) повідомлень, якими обмінюються компоненти ТМ, що лежать на одному рівні, але в різних вузлах, називаються ***протоколом***.

Повний набір протоколів усіх рівнів, що достатній для організації взаємодії вузлів в ТМ, називається ***стеком*** **телекомунікаційних протоколів.**

У моделі взаємодії відкритих систем (**Open System Interconnection, OSI**). засоби взаємодії діляться на сім рівнів: прикладний, представницький, сеансовий, транспортний, мережний, канальний та фізичний рис. 1.1

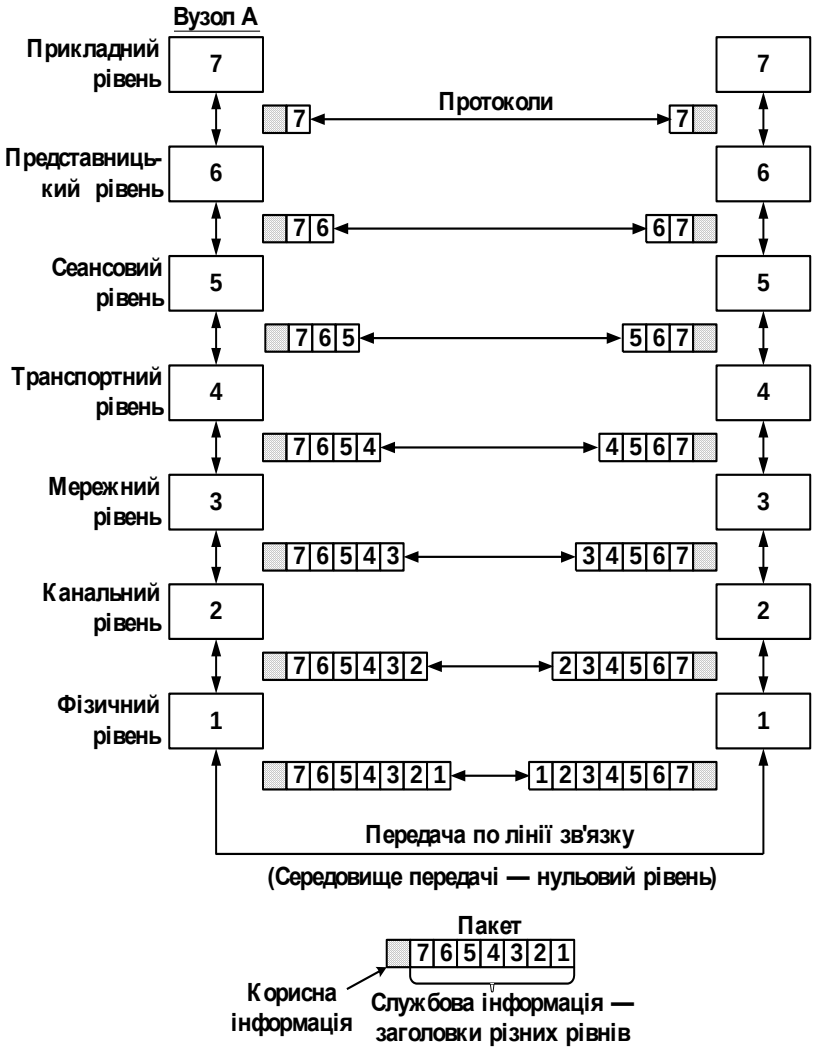


Рис. 1.1– Модель OSI

Найважливішими завданнями телекомунікацій у ДСНС є:

забезпечення оперативного та якісного прийому і передачі інформації про НС (НП);

забезпечення стійкого і безперервного зв'язку для управління силами та засобами при виконанні завдань за призначенням;

організація взаємодії та передачі інформації з іншими центральними органами виконавчої влади та місцевого самоврядування;

забезпечення передачі інформації як між апаратом ДСНС, його територіальними підрозділами, підприємствами, організаціями та установами сфери управління ДСНС, так і всередині них між окремими структурними підрозділами та їх співробітниками.

1.2 Взаємозв'язані телекомунікаційні мережі України

1.2.1 Національна телекомунікаційна мережа і загальнодержавна телекомунікаційна мережа загального користування

Національна телекомунікаційна мережа(НТМ)– сукупність спеціальних телекомунікаційних систем (мереж), систем спеціального зв'язку, інших комунікаційних систем, які використовуються в інтересах органів державної влади та органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону, призначена для обігу (передавання, приймання, створення, оброблення, зберігання) та захисту національних інформаційних ресурсів, забезпечення захищених електронних комунікацій, надання спектра сучасних захищених інформаційно-комунікаційних (мультисервісних) послуг в інтересах здійснення управління державою у мирний час, в умовах надзвичайного стану та в особливий період, та яка є мережею (системою) подвійного призначення з використанням частини її ресурсу для надання послуг, зокрема з кіберзахисту, іншим споживачам [1-12].

Загальнодержавна телекомунікаційна мережа загального користування (ТМЗК) є комплексом технологічно з'єднувальних мереж електрозв'язку на території України, що забезпечений загальним централізованим управлінням.

ТМЗК базується на первинній мережі, що представляє, у свою чергу, загальнодержавну мережу типових каналів і мережних трактів.

Типові канали, а в деяких випадках і типові мережні тракти надаються вторинним мережам: телефонним, телеграфним, передачі даних, телевізійного і звукового мовлення та ін.

Таким чином, передача сигналів електрозв'язку всіх видів здійснюється по каналах і трактах первинної мережі. Ці канали і тракти утворюються за допомогою багатоканальних систем передачі, що складаються з кінцевих, проміжних станцій і середовища поширення сигналів електрозв'язку.

Під час побудови ТМЗК враховано, що визначені технічні засоби беруть участь у процесі передачі незалежно від виду переданих повідомлень, тобто є загальними. Технічно ці засоби виділені до складу окремих структурних елементів: вузлів зв'язку, ліній передачі і мережних трактів. Сукупність цих елементів, що розповсюджені по всій території країни, утворює первинну мережу. Не вдаючись поки в подробиці характеристики названих елементів, зазначимо, що вони дозволяють організувати

мережу каналів передачі і групових трактів. Кожний канал і груповий тракт забезпечує передачу сигналів або у визначеній смузі частот, або у визначений проміжок часу.

Первинна мережа ТМЗК поділяється за територіальною ознакою на місцеву, зонову і магістральну.

Частина мережі, що з'єднує між собою канали різних зонових мереж на всій території країни, складає *магістральну первинну мережу*.

На рис. 1.2 зображена взаємодія первинної і вторинної мереж зв'язку. На схемі наведені дві зони, на території кожної з яких виділені по два міста і одному сільському району. Одне місто обласного значення (центр зони), а інше – районного. Елементами первинної мережі є вузли (ВУЗ) і лінії зв'язку (1, 2, 3).

Місцеві первинні мережі утворені лініями зв'язку 1 і частиною устаткування ВУЗ. На території кожної зони показано три місцеві первинні мережі. Внутрішньозонові первинні мережі представлені відповідним устаткуванням ВУЗ і лініями зв'язку 2. Сукупність місцевих первинних мереж однієї зони і її внутрішньозонової мережі утворюють *зонову первинну мережу*. *Магістральна первинна мережа* зображена двома ВУЗ і лініями зв'язку 3. Основне призначення вузлів зв'язку складається з організації типових каналів і групових трактів, у з'єднанні однойменних каналів і групових трактів різних ліній зв'язку, а також у наданні цих каналів вторинним мережам.

Вузли зв'язку поділяються на *магістральні, внутрішньозонові* і *місцеві*. Магістральні вузли створюються на перетині магістральних ліній зв'язку і розміщуються в обласних центрах.

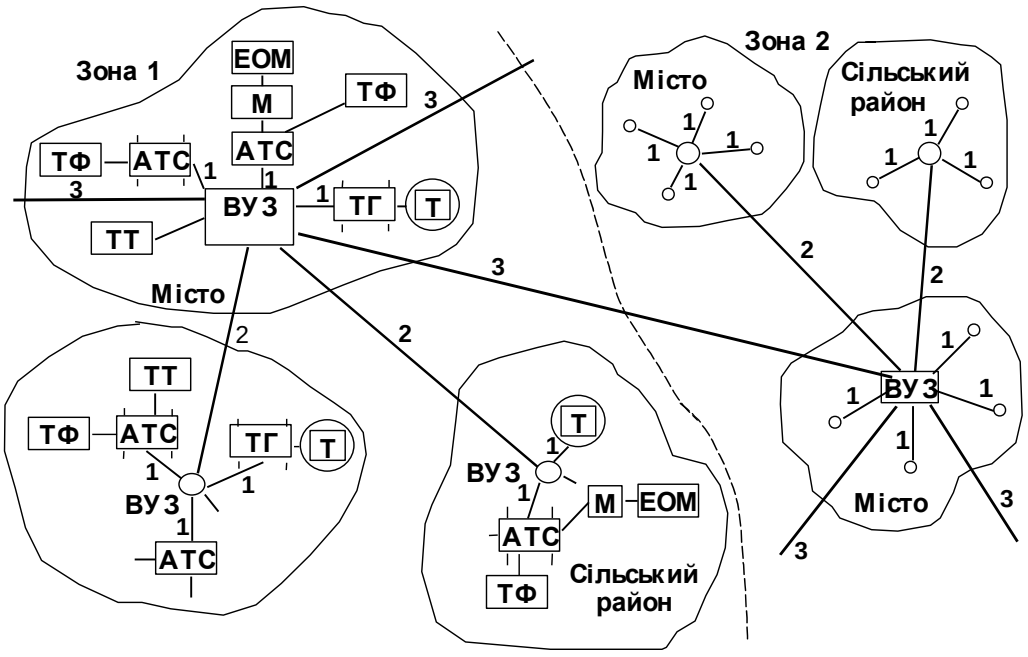


Рис. 1.2 – Взаємодія первинної і вторинної мереж

Для роботи на місцевих мережах призначена цифрова система передачі (ЦСП) ІКМ-30, що дозволяє організовувати до 30 каналів ТЧ, на внутрішньозонових зв'язках – ІКМ-120 і ІКМ-480, а на магістральній мережі – ІКМ-1920 на симетричних, коаксіальних і волоконно-оптичних лініях зв'язку. ЦСП вищих ступенів ієрархії, наприклад, з сучасними технологіями PDH/SDH, дозволяють утворювати потоки: Е1 – типовий цифровий первинний потік (швидкість передачі 2048 кбіт/с), Е2 – вторинний (8448 кбіт/с), Е3 – третинний (34368 кбіт/с), Е4 – четвертинний (139264/155520 кбіт/с) і т.д. Типовому каналу ТЧ при цьому відповідає основний цифровий канал (ОЦК) зі швидкістю передачі 64 кбіт/с. Існує можливість вводити сигнали типових мережних трактів у типові цифрові тракти.

Крім кабельних систем передачі на первинній мережі застосовуються також засоби радіозв'язку: радіорелейні і супутникові системи передачі.

У наш час первинна мережа будується на основі цифрових систем передачі і називається *цифровою первинною мережею*. В основі такої мережі лежать сучасні технології передачі – це так звана технологія синхронної цифрової ієрархії (SDH) і технологія асинхронного режиму переносу (АТМ), перша з яких є фундаментом цифрової первинної мережі.

Незалежно від «внутрішніх» особливостей первинної мережі канали і тракти, як правило, надаються вторинним мережам на місцевих мережних вузлах чи станціях, а іноді – на зонових чи магістральних.

До складу кожної вторинної мережі входять передбачені для неї канали передачі і групові тракти первинної мережі, вузли і станції комутації, абонентські лінії й абонентські апарати.

Вторинна телефонна мережа представлена сукупністю сільських і міських мереж АТС, розташованих на територіях сільських районів і міст, каналів зв'язку первинної мережі й *кінцевих пристроїв* – телефонних апаратів (ТА).

На рис.1.3 наведена структура найбільш розповсюдженої телефонної мережі загального користування (ТМЗК) – автоматична телефонна мережа, що комутується.

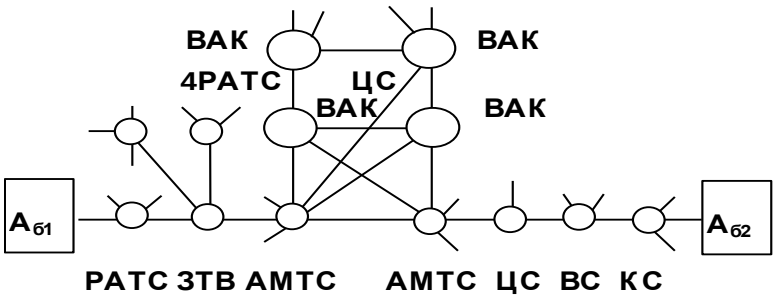


Рис. 1.3 – Структура телефонної мережі ТМЗК

Дана мережа призначена для телефонного зв'язку, але досить часто використовується і для інших видів зв'язку, що здійснюються по каналах ТЧ, а саме: телеграфного, передачі даних і факсимільного зв'язку. Головною станцією внутрішньозонової мережі є автоматична міжміська телефонна станція АМТС, кінцевими – районні АТС (РАТС) міських мереж і центральні телефонні станції ЦС сільських телефонних мереж. При необхідності створюються зонові телефонні вузли (ЗТВ). Місцеві сільські мережі містять вузлові (ВС) і кінцеві (КС) телефонні станції. АМТС має виходи не менш ніж до двох вузлів автоматичної комутації (ВАК), що разом з каналами ТЧ первинної мережі утворюють міжміську телефонну мережу.

1.2.2 Система оперативно-технічного управліннятелекомунікаційними мережами в умовах надзвичайних ситуацій

Постановою КМ України від 29.06.2004 № 812 «Порядок оперативно-технічного управління телекомунікаційними мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану» (редакція від 06.02.2019) визначено: структуру та склад Системи оперативно-технічного управління (СОТУ); основні завдання СОТУ; основні завдання та функції Національного центр управління (НЦУ); завдання та функції центрів управління мережами (ЦУМ); умови взаємодії НЦУ, ЦУМ, спеціальних споживачів та телерадіомовних компаній; обсяги та порядок подання інформації до НЦУ; вимоги до захисту інформації та гарантування безпеки СОТУ.

Рішенням № 579 від 03.12.2019 Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації погоджено проект наказу Адміністрації державної служби спеціального зв'язку та захисту інформації України «Про затвердження Основних вимог до форми і строків подання інформації до Національного центру оперативно-технічного управління мережами телекомунікацій», що забезпечить ефективну взаємодію операторів телекомунікацій, центральних органів виконавчої влади (крім спеціальних споживачів), підприємств, установ та організацій, у власності, користуванні, господарському віданні чи оперативному управлінні яких є засоби та мережі телекомунікацій з НЦУ.

У 2017 році ПрАТ «Діпрозв'язок» за підсумками наукових досліджень проблемних питань управління сучасними телекомунікаційними мережами розроблено структурну (функціональну), інформаційну та фізичну моделі СОТУ, визначено її складові: телекомунікаційні мережі – об'єкти управління в СОТУ, ЦУМ операторів телекомунікацій та НЦУ – суб'єкти управління в СОТУ. Було також визначено організаційні та технічні вимоги до складових СОТУ, які подано на інфограмі (рис.1.4) .

Функцією НЦУ як головної складової Системи оперативно-технічного управління телекомунікаційними мережами України (СОТУ)

є накопичення вихідних даних про мережі, моніторинг стану мереж, забезпечення живучості, реагування на зміни стану мереж, оцінки їх готовності до роботи в умовах надзвичайних ситуацій (у тому числі при кібератаках на системи управління телекомунікаційними мережами) та в умовах надзвичайного і воєнного стану.

Основні критерії для визначення телекомунікаційних мереж об'єктами управління СОТУ такі:

розгалуженість цих мереж та покриття всієї території України або значної її частини, велика потужність та достатні надійність і живучість;

сучасний технологічний рівень і постійний розвиток;

висока якість телекомунікаційних послуг та велика абонентська база;

наявність достатнього мережевого ресурсу, зокрема незадіяного (волокон, каналів, трактів), який можна використати в умовах надзвичайних ситуацій і який забезпечить мобілізаційну готовність в особливий період;

наявність власних центрів управління мережами, високий рівень технічної експлуатації.

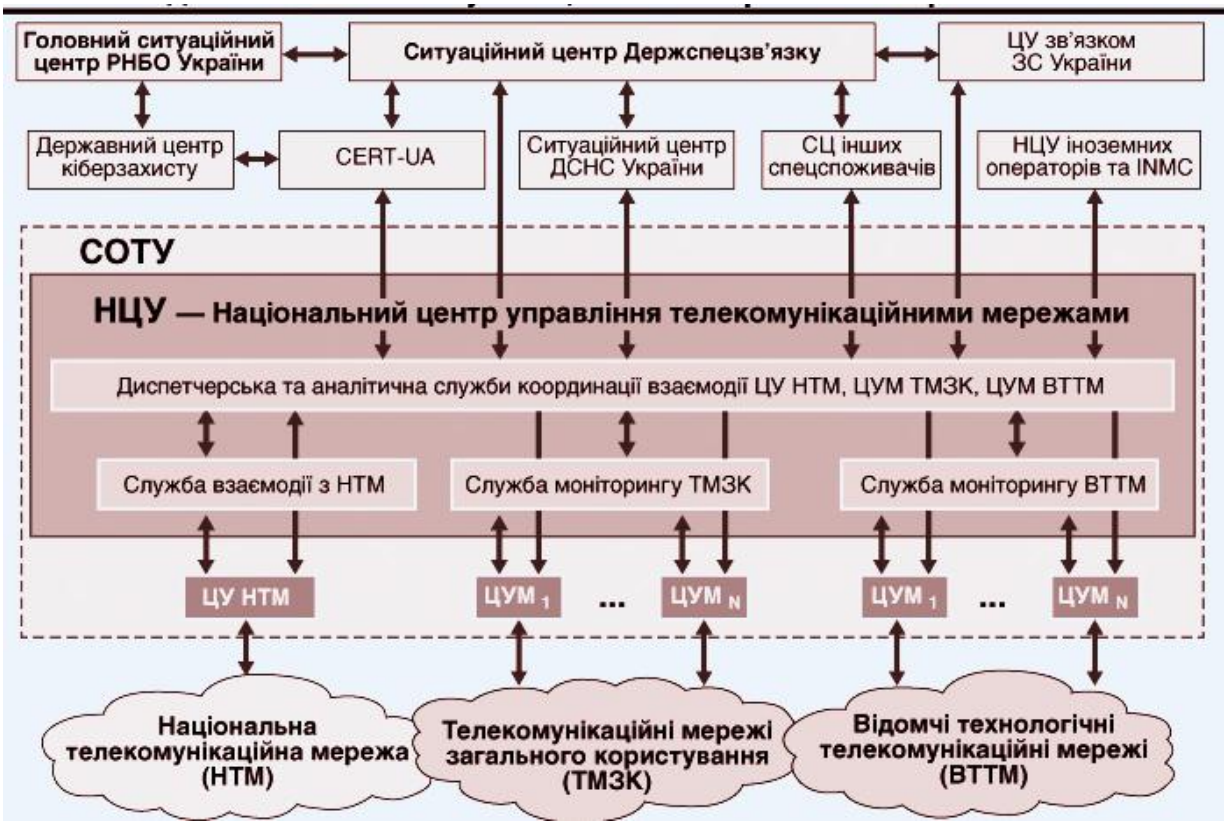


Рис.1.4 – Організація оперативно-технічного управління взаємозв'язаними телекомунікаційними мережами України

Розташування функцій управління НЦУ дозволяє:

забезпечити незалежність функціонування операторів телекомунікацій від НЦУ;

реалізує функції управління мережними ресурсами операторів з боку НЦУ в умовах особливого періоду шляхом створення двох стандартних інтерфейсів.

Організації системи управління мережними ресурсами дозволяє функції управління, притаманні НЦУ, виділити в окремий прошарок, розташований між спільними та індивідуальними функціями управління, що дає можливість НЦУ в разі необхідності здійснювати централізоване управління мережними ресурсами, тому що функції верхнього шару є індивідуальними для кожного оператора. НЦУ не впливає безпосереднього на функції верхнього рівня ієрархії управління. Розташування функцій НЦУ у вигляді відповідного прошарку дозволяє використовувати НЦУ для здійснення незалежного контролю за якістю послуг, що надаються.

СОТУ – це принципи функціонування НЦУ та автоматизація процесів управління багаторівневою системою СОТУ з усіма її складовими для виконання:

забезпечення накопичення вихідних даних про мережі;

моніторингу стану мереж;

оцінки готовності мереж у надзвичайних ситуаціях забезпечити живучість;

реагування на зміни стану мереж;

автоматизації аналітичного оброблення даних;

прогнозування можливих проблемних та критичних ситуацій;

моделювання варіантів розв'язання проблем та підготовки прийняття оперативних рішень щодо виходу з кризових ситуацій і доведення цих рішень (команд) до центрів управління мережами (ЦУМ) для подальшого виконання у межах мереж, ресурсами яких вони управляють.

Дії НЦУ спрямовуються на організацію ефективної взаємодії усіх учасників СОТУ та в будь-яких умовах гарантоване забезпечення спеціальних споживачів, органів державного управління, служб централізованого оповіщення, екстреної допомоги і населення телекомунікаційними ресурсами та телекомунікаційними послугами. Реалізація функцій НЦУ потребує створення єдиного стандартизованого інтерфейсу між НЦУ і верхніми рівнями управління індивідуальних систем управління операторів телекомунікацій, а також інтерфейсу між НЦУ і мережною інфраструктурою цих операторів (тобто нижніми, спільними рівнями управління).

Технічна основа НЦУ:

серверне обладнання, бази даних, автоматизовані робочі місця посадових осіб;

структурована кабельна система;

телекомунікаційне обладнання внутрішніх та зовнішніх комунікацій;

обладнання інженерної інфраструктури (систем енергоживлення, заземлення, охолодження, вентиляції, пожежної та охоронної сигналіза-

ції, захисту інформації, пожежогасіння тощо);

загальне та спеціальне програмне забезпечення для аналітичної обробки, моделювання, прогнозування та підготовки рішень управління;

інформаційно-лінгвістичне забезпечення для побудови підсистем центру;

пристрій відображення колективного користування відеостіна, на якій відображаються основні параметри роботи мереж.

Введення пускового комплексу НЦУ у дослідну експлуатацію було заплановано з листопаду 2020 року.

1.3 Призначення, принципи побудови Відомчої цифрової телекомунікаційної мережі ДСНС України

1.3.1 Призначення відомчої телекомунікаційної мережі ДСНС України

ВЦТМ (відомча цифрова телекомунікаційна мережа ДСНС) – логічна цілісна мультисервісна багаторівнева телекомунікаційна мережа, яка здійснює взаємодію із загальнодержавними телекомунікаційними мережами спеціального зв'язку та загального користування і включає в себе сукупність технічних засобів й обладнання телекомунікаційної мережі доступу і транспортної телекомунікаційної мережі для забезпечення інформаційної взаємодії між суб'єктами ВЦТМ як у мирний час, так і в особливий період.

Суб'єкт ВЦТМ – територіальні органи, заклади освіти, установи та підприємства, які підпорядковуються ДСНС.

Вузол ВЦТМ – сукупність технічних засобів телекомунікацій, які забезпечують доступ до ВЦТМ

Сервіси ВЦТМ – сукупність телекомунікаційних послуг, які надаються за допомогою ВЦТМ.

Локальна телекомунікаційна мережа – комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень і звуків або повідомлень будь-якого виду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням у межах в межах адміністративної будівлі (комплексу адміністративних будівель) суб'єкта ВЦТМ.

ВЦТМ ДСНС зорганізується для:

– забезпечення оперативного управліннясилами і засобами ДСНС;

– оперативної доставки інформації в процесі повсякденної діяльності всіх галузевих служб і підрозділів;

– оперативної взаємодії з органами державного управління та місцевого самоврядування, іншими міністерствами і відомствами.

ВЦТМ ДСНС України створюється як відомча спеціалізована захище-

на телекомунікаційна мережа з національним покриттям та інтеграцією служб.

Відомчий характер ВЦТМ ДСНС визначається її призначенням для оперативного управління органами управління ДСНС, його підрозділами і установами, а також оперативної обробки та передачі встановленої інформації, директив та розпоряджень під час виконання поставлених задач та в повсякденній діяльності, оперативної взаємодії з органами державного управління та місцевого самоврядування, іншими міністерствами і відомствами.

Спеціалізованість послуг ВЦТМ ДСНСозначає:

– чітке визначення категорій та номенклатури користувачів послугами мережі і гарантоване їх обслуговування у визначені терміни та у відповідності до наданих пріоритетів;

– визначення видів і якості послуг, що включають набір спеціалізованих послуг, в тому числі із забезпеченням необхідного рівня захищеності (телефонний и документальний фіксований зв'язок, одночасну передачу мови та даних, передачу графічної інформації, конференцзв'язок, всі види передачі зображення, доступ до послуг Internet и Intranet).

Під *захищеним статусом* ВЦТМ ДСНС розуміється можливість забезпечення передачі нетаємної, але важливої відомчої інформації, порушення конфіденційності, цілісності і (або) доступності до якої може нанести відповідні збитки ДСНС внаслідок її витоку. Захищеність передбачає здійснення протидії несанкціонованому доступу до інформаційних та системних ресурсів, технологічним базам даних і підсистемам управління вузловими комутаторами і всією мережею в цілому, наявність механізмів захисту інформації в каналах зв'язку, автентифікації суб'єктів і ідентифікації об'єктів інформаційного обміну.

Національний статус ВЦТМ ДСНС визначається її розповсюдженням на всі регіони України і можливістю її інтеграції в Єдину національну мережу зв'язку України.

Інтеграція служб в ВЦТМ ДСНС передбачає:

– реалізацію в межах єдиного технологічного простору (на єдиній технічній платформі) всіх передбачених нормативними документами видів зв'язку та інформаційного забезпечення, а саме: диспетчерського зв'язку ДСНС зі службою аварійного телефонного виклику «01»(112), відомчого телефонного зв'язку, відомчих систем документального, факсимільного зв'язку і передачі даних, відомчої системи зв'язку з рухомими об'єктами, відомчої системи розпоряджувально-пошукового зв'язку та оповіщення, системи телевізійного контролю, систем пожежно-охоронної сигналізації тощо;

– пристосованість до роботи з різноманітним спектром сучасних абонентських пристроїв, що побудовані з використанням широкого набору телекомунікаційних стандартів інформаційної взаємодії (в тому чи-

слі з різними типами телефонів, факсів, модемів, комп'ютерів тощо);

– можливість передачі мультимедійної інформації, тобто можливість передачі і обробки сигналів, які суттєво відрізняються за своїми характеристиками (наприклад, графіки, аудіо, комп'ютерні дані, відео тощо);

– можливість надання користувачам широкого спектру телекомунікаційних послуг, які відрізняються своєю структурою, фізичною природою, а також якістю сервісу, що надається (документальний, аудіо-, відеконференцзв'язок, локальна мобільність, наскрізний телефонний персональний номер, голосова пошта, системи обробки викликів Call-центрів тощо).

ВЦТМ ДСНС України є невід'ємною часткою Національної інформаційної інфраструктури, що забезпечує взаємозв'язок та взаємодію всіх мереж телекомунікацій різних форм власності як фіксованих, так і мобільних, з встановленням і без встановлення фізичних з'єднань, з синхронним і асинхронним способами переносу інформації.

1.3.2 Принципи побудови ВЦТМ ДСНС України

Головним принципом побудови ВЦТМ ДСНС є створення на базі існуючих транспортних мереж національної телекомунікаційноїмережі України корпоративної телекомунікаційної мережі з національним покриттям за рахунок використання сучасних систем проводового і безпроводного доступу, засобів захисту інформаційних і системних ресурсів.

1.3.2.1 Топологія ВЦТМ ДСНС

Топологію ВЦТМ визначає територіальне розміщення органів та підрозділів ДСНС, а саме:

- центральний апарат ДСНС України в м. Києві;
- міські управління Києва, обласні управління, що підпорядковані ДСНС України;
- міські та районні управління, що підпорядковані обласним управлінням ДСНС України;
- сили швидкого реагування, що підпорядковані ДСНС України.

Тому за топологією мережа будується за дворівневою радіальною схемою, в якій реалізується:

1-й рівень – центральний апарат ДСНС України в м. Києві, обласні управління, міські управління Києва, сили швидкого реагування центрального підпорядкування;

2-й рівень – Обласні управління, міські управління міст Києва – підпорядковані міські та районні підрозділи.

На всіх рівнях повинно бути забезпечене включення в телефонну мережу загального користування, а також в відомчі телефонні мережі взаємодіючих структур – органів державного управління та місцевого самоврядування, перелік яких визначається відповідними нормативними документами ДСНС України.

Топологія ВЦТМ ДСНС набуває реалізації, як правило, в транспортній мережі на базі каналів зв’язку ДСНС, в мережах доступу операторів (провайдерів) телекомунікацій та державних каналів зв’язку.

1.3.2.2 Транспортна мережа ВЦТМ ДСНС

Транспортна мережа ВЦТМ ДСНС реалізується з використанням як цифрових технологій і забезпеченням швидкості передачі с фіксованою смугою пропускання (швидкістю передачі), так і традиційних симетричних аналогових кабелів і радіорелейних ліній. Транспортний рівень призначений для організації мультисервісного трафіка між елементами мережі, а також трафіка з іншими взаємодіючими мережами (загального користування, корпоративними тощо). Її реалізація здійснюється на умовах оренди каналів діючої інфраструктури приватних операторів (провайдерів) телекомунікацій, що надають послуги з доступу до мережі Інтернет та застосування каналів зв'язку ДСНС, державних каналів зв’язку спеціального призначення – національна телекомунікаційна мережа, телекомунікаційна мережа спеціального призначення.

Схема організації такої транспортної мережі може бути реалізована за дворівневим радіально-кільцевим принципом (рис. 1.5).

Є доцільним застосування можливостей супутникових каналів зв’язку обмеженої пропускної спроможності 64-256 кБіт/с з використанням абонентського обладнання VSAT (Very Small Aperture Terminals – термінали з дуже малою апертурою).

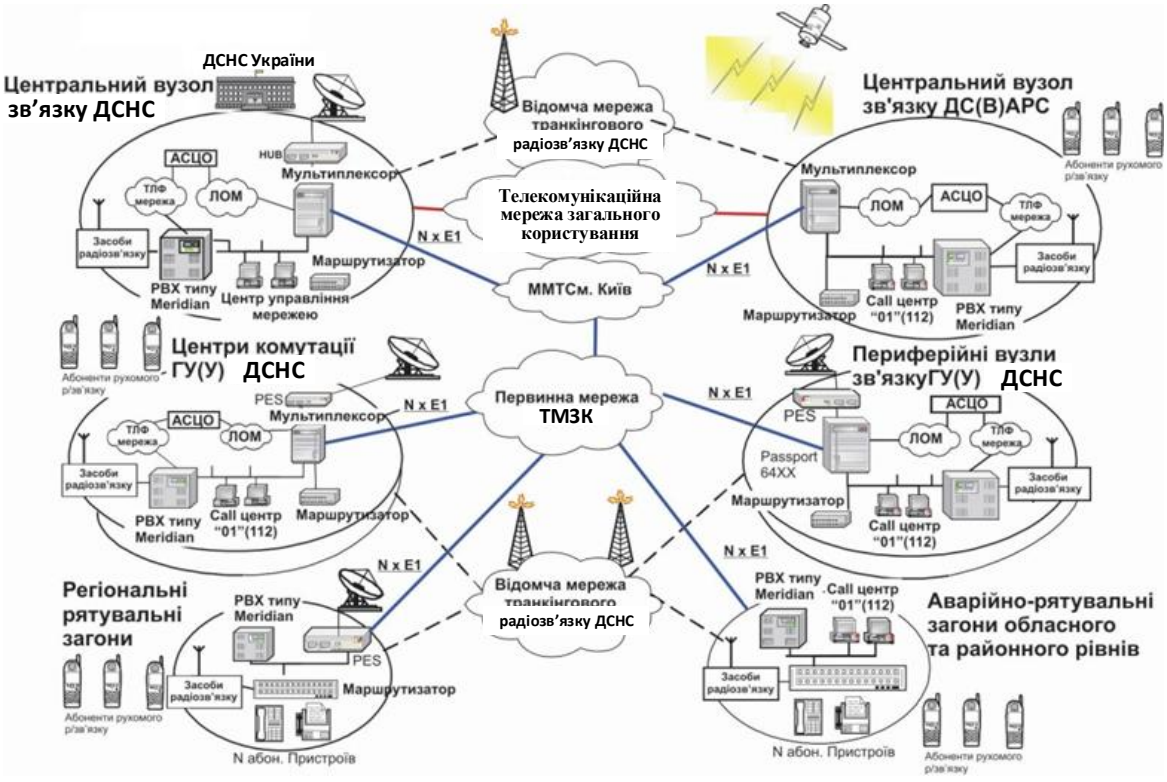


Рис. 1.5 – Схема транспортної мережіВЦТМ ДСНС

Останнє є об’єктивно необхідним при застосуванні сил ДСНС поза межами пунктів постійної дислокації для ліквідації наслідків техногенних аварій та стихійних лих, а також у випадках аварій на проводових транспортних мережах.

1.3.2.3 Мережі доступу ВЦТМ ДСНС

Мережі доступуреалізуються для вирішення проблем «останньої милі» в гарнізонних мережах ВЦТМ ДСНС, підключення до мереж зв’язку загального користування та взаємодіючих структур.

За безпосередніми зв’язками (БЗ), орендованими в місцевих дирекціях ПАТ Укртелеком і організованими на фізичних двохпроводових лініях, можуть реалізовуватись аналогові протоколи включення в зустрічні АТС, такі як двох – та трьох проводові з’єднувальні лінії, двох проводові з отриманням автоматичного визначення номера від спецвузла зв’язку тощо.

Реалізація за БЗ цифрових протоколів, таких як первинний PRI та базовий доступ BRI, R1.5 та R2D здійснюється з використанням різноманітних цифрових модемів, серед яких технології xDSL і (або) безпроводові технології.

Використання технологій xDSL дозволяє вирішити проблему «останньої милі» по існуючій мідній кабельній інфраструктурі із забезпеченням абонентам послуг високошвидкісної передачі мови і даних. Гарантується надійність традиційних телефонних послуг, при цьому трафік даних направляється поза АТС, завдяки чому навантаження на АТС зменшується.

Найбільш доцільно впровадження різновидів технології xDSL/ проаналізуємо їх можливості в динаміку розвитку.

xDSL (англ. *digital subscriber line*, цифрова абонентська лінія) — сімейство технологій, що дозволяють значно підвищити пропускну спроможність абонентської лінії телефонної мережі загального користування шляхом використання ефективних лінійних кодів і адаптивних методів корекції викривлень лінії на основі сучасних досягнень мікроелектроніки й методів цифрової обробки сигналу [13-16].

В абревіатурі xDSL символ «x»використовується для позначення першого символу в назві конкретної технології, а DSL позначає цифрову абонентську лінію **DSL** (англ.*Digital Subscriber Line* – цифрова абонентська лінія; також є інший варіант назви – Digital Subscriber Loop – цифровий абонентський шлейф).

ТехнологіїxDSLз'явилисявсередині90-хроківякальтернативацифровомуабонентськомузакінченнюISDN.

ISDN (англ. Integrated Services Digital Network, Цифрова Мережа з Інтегрованими Послугами (ЦМзІП)) – найперша технологія одночасної передачі цифрових та аналогових даних з використанням однієї лінії зв'язку шляхом розподілення й відокремлення використовуваних окре-

мими послугами частот й, таким чином, забезпечення безперервного використання таких, що використовують аналоговий зв'язок (як то телефон, факс тощо), з такими, що використовують цифровий (фідонет, локальна мережа, інтернет тощо), несумісних до того.

Офіційно, як стандарт, ISDN прийнято 1988 року. Спочатку призначалася для відправки голосових повідомлень. Передача даних зазвичай відбувалась каналами T1/E1 зі швидкість 64 Кбіт/с.

T1 – дуплексні цифрові канали, спроектовані спеціально для передачі цифрових сигналів за рахунок інтеграції цифрових ліній T1 з телефонною мережею. Лінія T1 складається з 24 каналів по 64 кбіт/с, мультіплексорних для передачі мови й даних. Архітектура T1 заснована на ієрархії цифрових сигналів, застосовуваної в Північній Америці для опису телекомунікаційних ліній. При створенні звичайних аналогових телефонних мереж (**POTS** – plain old telephone service) виявилося, що оптимальна пропускна здатність для передачі мови (в чому й полягало призначення телефонів) становить 56 кбіт/с. З урахуванням деяких додаткових бітів для управління передачею оптимальний канал вимагав 64 кбіт/с. Цифрова передача дозволила скоротити непродуктивні втрати при обміні інформацією й використовувати всю смугу 64 кбіт/с. Це значення й стало основною одиницею в ієрархії цифрових сигналів, що одержала позначення DS-0 – 64 кбіт/с.

Лінію T1 можна представити як набір з 24 каналів DS-0-1, комбінація яких дає сукупну пропускну здатність DS-1 – 24 ·64 кбіт/с = 1536кбіт/с / 1024 = 1,5 Мбіт/с, відповідну до лінії DS-1-0.

E1 – стандарт цифрової передачі даних, відповідний до первинного рівня європейського стандарту PDH. Є результатом розвитку американського T1, на відміну від якого має 32 канали, з яких 30 каналів для голосу або даних і 2 канали для сигналізації (30B+D+H). Канали розділяються за часом. Кожний з 32 каналів має пропускну спроможність 64 кбіт/с; таким чином, загальна пропускна здатність E1 дорівнює 32 · 64 кбіт/с = 2048 кбіт/с / 1024 = 2 Мбіт/с). Один з каналів сигналізації служить для синхронізації прикінцевого обладнання, іншій – для передачі даних про встановлювані з'єднання.

На фізичному рівні характеристики інтерфейсу E1 відповідають стандарту ITU-T G.703. Основне призначення ISDN – передача даних зі швидкістю до 64 Кбіт/с 4-х кілогерцною проводовою лінією й забезпечення інтегрованих телекомунікаційних послуг (телефон, факс, і т. д.). Використання для цієї мети телефонних проводів має дві переваги: вони вже існують в приміщеннях будівель і можуть використатися для подачі живлення на термінальне устаткування.

Вибір 64 кбіт/с стандарту визначається наступними міркуваннями. При смузі частот 4 кГц, згідно з теоремою Найквіста-Котельнікова, частота дискретизації повинна бути не нижче 2 ·4 кГц = 8 кгц. Мінімальне

число двійкових розрядів для подання результатів дискретизації голосового сигналу за умови логарифмічного перетворення дорівнює 8. Таким чином, у результаті перемножування цих чисел і виходить значення смуги B-каналу ISDN 8 · 8 кГц = 64 кгц. Базова конфігурація каналів має вигляд 2 × B + D = 2 × 64 кГц + 16 кГц = 144 Кбіт/с. Крім B-каналів і допоміжного D-каналу ISDN може запропонувати й інші канали з більшою пропускною здатністю: канал H10 зі смугою 384 кбіт/с, H11 – 1536 кбіт/с і H12 – 1920 кбіт/с (реальні швидкості цифрового потоку). Для первинних каналів (1544кбіт/с й 2048 кбіт/с) смуга допоміжного D-каналу може становити 64 кбіт/с.

Стандарт мереж ISDN передбачає 2 інтерфейси:

базового рівня (англ. Basic Rate Interface, BRI), у якому загальна пропускна спроможність у 144 кбіт розподілена між двома мовленнєвими каналами типу B зі швидкістю 64 кбіт/с і одним сигнальним каналом типу D зі швидкістю передавання 16 кбіт/с. Описується формулою 2B + D;

первинний доступ (англ. Primary Rate Access, PRA), який дає змогу працювати з каналами T1 (1,5 Мбіт/с) і E1 (2 Мбіт/с), які поділені на 23 і 30 каналів типу B відповідно, та мають один сигнальний D-канал зі швидкістю 64 кбіт/с. Описується формулою 23B + D або 30B + D).

Технології xDSL дозволяють передавати дані зі швидкостями, що значно перевищують ті швидкості, які доступні навіть кращим аналоговим і цифровим модемам ISDN. Ці технології підтримують передачу голосу, високошвидкісну передачу даних і відеосигналів, створюючи при цьому значні переваги як для абонентів, так і для провайдерів. Багато технологій xDSL дозволяють сполучати високошвидкісну передачу даних і передачу голосу по одній і тій же мідній парі.

Існуючі типи технологій xDSL різняться в основному за використовуваною формою модуляції й швидкості передачі даних. Найбільше розповсюджене застосування: ефективна заміна первинних цифрових систем передачі типу T1 або E1 на сполучних лініях місцевих мереж, що не вимагає застосування проміжних регенераторів.

Служби xDSL розроблялися для досягнення певних мет: вони повинні працювати на існуючих телефонних лініях, вони не повинні заважати роботі різної апаратури абонента, такий як телефонний апарат, факс і т. п., швидкість роботи повинна бути вище теоретичної межі в 56 кбіт/с, і нарешті, вони повинні забезпечувати постійне підключення. Широке поширення технологій xDSL повинне супроводжуватися деякою перебудовою роботи постачальників послуг Інтернету й постачальників послуг телефонних мереж, тому що їхнє обладнання тепер повинне працювати спільно. Можливий також варіант, коли альтернативний оператор зв'язку бере оптом в оренду велика кількість абонентських закінчень у традиційного місцевого оператора або ж орендує деяка кількість модемів в DSLAM.

DSLAM (англ. *Digital Subscriber Line Access Multiplexer*) — мультиплексор доступу цифрової абонентської лінії xDSL. Зі сторони мережі в нього WAN-порти, а із сторони клієнта — xDSL напівкомплекти (модеми), до яких підключається абонентська лінія. На іншому кінці абонентської лінії у клієнта знаходиться абонентський ніпівкомплект xDSL (модем) або IAD (Integrated Access Device — пристрій інтегрального доступу). Останній використовується у випадках, коли по xDSL лінії реалізується одночасна передача даних і голосу в цифровому вигляді, тобто VoDSL (Voice over DSL). DSLAM термінує сигнали xDSL. Усього розроблене десятки видів xDSL, які забезпечують високошвидкісний цифровий доступ по абонентській телефонній лінії та різняться методом модуляції при кодуванні даних. Згодом залишилися наступні основні стандарти xDSL:

IDSL (англ. *ISDN Digital Subscriber Line* – цифрова абонентська лінія IDSN).

SDSL (англ: Symmetric Digital Subscriber Line) – симетрична цифрова абонентська лінія;

HDSL (англ: High Data Rate Digital Subscriber Line) – високошвидкісна цифрова абонентська лінія;

SHDSL (англ: Single-pairHigh-speedDigitalSubscriberLine) – однопарна високошвидкісна цифрова абонентська лінія;

UADSL (англ: Universal Asymmetric Digital Subscriber Line) – універсальна асиметрична цифрова абонентська лінія;

ADSL (англ: Asymmetric Digital Subscriber Line) – асиметрична цифрова абонентська лінія;

VDSL (англ: Very High Speed Digital Subscriber Line) – надвисокошвидкісна цифрова абонентська лінія.

Технології xDSL підтримують кілька варіантів кодування інформації:

- 2B1Q: Two-binary, one-quaternary, використовується для IDSL і HDSL
- CAP: Carrierless Amplitude Phase Modulation – використовується для HDSL
- DMT: Discrete multitone modulation, найпоширеніший метод, відомий також як OFDM (мультиплексування з ортогональним частотним розподілом каналів)

Досягнення технологій xDSL багато в чомувизначаються досягненнями техніки кодування, яка за рахунок застосування процесорів DSP (Цифровий сигнальний процесор) змогла підвищити швидкість передачі даних при одночасномузбільшенні відстані між модемом і обладнаннямDSLAM.

Міжнародною організацією, що визначає стандарти (рекомендації, англ. Recommendations) в галузі телекомунікацій та радіо є Міжнародний

союз електрозв'язку (**МСЕ**) (англ. International Telecommunication Union, **ITU**). Мережі доступу на металевих кабелях розглядяються в рекомендаціях МСЕ – Т G.990–G.999. Перелік рекомендацій ITU – Т (укр.: МСЕ-Т) по типам xDSL-технологій зведені до табл. 1.2

Таблиця 1.2 –РекомендаціїITU-T (укр.: МСЕ-Т) по типам xDSL-технологій

Позначення рекомендації	**Назва рекомендації (укр.), посилання**	**Час затвердження (міс./рік)**	**Технологія xDSL**
G.960	Цифрова лінія основного абонентського доступу (ISDN). https://www.itu.int/rec/T-REC-G.960-199303-I/en	03/1993	IDSL (ISDN)
G.961	Цифрова система передачі по металевому кабелю для основного абонентського доступу (ISDN), https://www.itu.int/rec/T-REC-G.961/en	03/1993 виправлення: 08/2000	IDSL (ISDN)
G.9951 (G.989.1)	Прийомопередавачі по лініях телефонної мережі – Основи., https://www.itu.int/rec/T-REC-G.9951-200102-I/en	05/2005 (02/2001)	HomePNA
G.9952 (G.989.2)	Прийомопередавачі по лініях телефонної мережі. Формат корисного навантаження й вимоги до установки з'єднання. https://www.itu.int/rec/T-REC-G.9952-200111-I/en	05/2005 (11/2001)	HomePNA
G.9953 (G.989.3)	Мережеві прийомопередавачі телефонних ліній – Функція розв'язки. https://www.itu.int/rec/T-REC-G.9953-200303-I/en	05/2005 (03/2003)	HomePNA
G.9954	Прийомопередавачі для домашньої мережі – Розширені фізичні характеристики, доступ до медіа та специфікації рівня зв'язку. https://www.itu.int/rec/T-REC-G.9954-200701-I/en	01/2007	HomePNA
G.991.1	Прийомопередавачі високошвидкісної цифрової абонентської лінії (HDSL). https://www.itu.int/rec/T-REC-G.991.1-199810-I/en	10/1998	HDSL
G.991.2	Прийомопередавачі однопарної високошвидкісної цифрової абонентської лінії (SHDSL). https://www.itu.int/rec/T-REC-G.991.2-200312-I/en	12/ 2003	SHDSL
G.992.1	Прийомопередавачі асиметричної цифрової абонентської лінії (ADSL). https://www.itu.int/rec/T-REC-G.992.1-199907-I/en	06/1999 Випр.1 11/2001 Випр.2 07/2002 Попр.1	ADSL “Інтерн.” версія стандарту Т 1.413. і 2

Позначення рекомендації	Назва рекомендації (укр.), посилання	Час затвердження (міс./рік)	Технологія xDSL
		03/2003 Попр.2 12/2003 Дод. H 10/2000	
G.992.2	Прийомопередавачі безсплітерної цифрової абонентської лінії (ADSL). https://www.itu.int/rec/T-REC-G.992.2-199907-I/en	07/1999 Випр.1 07/2002 Попр.1 03/2003 Попр.2 10/2003	Splitterless ADSL (UADSL)
G.992.3	Прийомопередавачі асиметричної цифрової абонентської лінії -2 (ADSL 2). https://www.itu.int/rec/T-REC-G.992.3/en	04/ 2009 Випр. 1,2,3 11/2009, 06/2011, 08/20013 Попр. 1-5 03/2010, 07/2010, 11/2010, 10/2011, 10/2012	ADSL 2
G.992.4	Прийомопередавачі безсплітерної цифрової абонентської лінії 2 (Splitterless ADSL 2). https://www.itu.int/rec/T-REC-G.992.4-200207-I/en	07/ 2002	Splitterless ADSL 2
G.992.5	Прийомопередавачі асиметричної цифрової абонентської лінії 2+ (ADSL 2+). https://www.itu.int/rec/T-REC-G.992.5/en	01/2009 Випр.1 11/2010	ADSL 2+
G.993.1	Прийомопередавачі надвисокошвидкісної цифрової абонентської лінії (VDSL). https://www.itu.int/rec/T-REC-G.993.1-200406-I/en	06/2004	VDSL
G.993.2	Прийомопередавачі надвисокошвидкісної цифрової абонентської лінії 2 (VDSL2)). https://www.itu.int/rec/T-REC-G.993.2-201902-I/en	02/2019	VDSL2
G.993.5	Самопридушення FEXT (векторізація) для використання із прийомопередавачами VDSL2. https://www.itu.int/rec/T-REC-G.993.5-201902-I/en	02/19 Випр.1 03/20	VDSL2
G.994.1	Процедури підтвердження встановлення з'єднання прийомопередавачів DSL. https://www.itu.int/rec/T-REC-G.994.1-202102-I/en	02/2021	xDSL

Позначення рекомендації	Назва рекомендації (укр.), посилання	Час затвердження (міс./рік)	Технологія xDSL
G.Sup50 (G.995.1)	Огляд рекомендацій цифрової абонентської лінії DSL https://www.itu.int/rec/T-REC-G.Sup50-201109-I/en	09/2011 (12/2011 скасов.)	xDSL
G.9960	Уніфіковані високошвидкісні прийомопередавачі для домашньої мережі на основі проводової лінії-Архітектура системи та специфікація фізичного рівня https://www.itu.int/rec/T-REC-G.9960/en	11/2018 Випр.1 09/2019 Попр.1 02/2020 Попр.2 07/2020 Випр.2 10/2020	xDSL

Розглянемо можливості і особливості кожної xDSL-технології для систем передачі даних (СПД) по металевим кабелям телефонних ліній згідно їх хронології розвитку, вказаному в табл. 1..2.

IDSL (англ. *ISDN Digital Subscriber Line* – цифрова абонентська лінія IDSN) – DSL-технологія, заснована на ISDN, що дозволяє забезпечити канал зв'язку для передачі даних по існуючих телефонних лініях на швидкості 144 кбіт/с, небагато більшої, ніж при використанні подвійного каналу ISDN зі швидкістю 128 кбіт/с. Цифрова передача даних обходить телефонну компанію, яка обробляє аналогові сигнали. Технологія IDSL доступна не у всіх країнах. IDSL – це щось середнє між ISDN і xDSL.

SDSL (англ: Symmetric Digital Subscriber Line) – симетрична цифрова абонентська лінія, є одним з видів цифрової абонентської лінії (DSL), яка використовується для забезпечення високошвидкісної взаємодії. Симетричний DSL називається "симетричним", тому що висхідні (від абонента до провайдера послуг) й спадні (від провайдера до абонента) з'єднання мають однакову пропускну здатність, що забезпечує однакову високу швидкість передачі даних в обох напрямках, як убік користувача, так і від нього. SDSL підтримує таку ж працюючи над існуючими кабелями "витої пари", які існують у всьому телефонному обладнанні (див. рис. 1.6)

SDSLвимагає використання тількиоднієїпаримідних провідвляпідтримкиз'єднання.Ціпроводки кабелюможутьдосягатидотрьохкілометрів.SDSLможнарозумітияк:

- у широкомусмислові, як термін для всіх варіантів DSL, які пропонують симетричну смугу пропускання, включаючи IDSL, який пропонує 144 кбіт/с, HDSL, HDSL2, G. SHDSL, який пропонує до 22.784 Мбіт /с по чотирьом парам мідних проводів, а також варіант SDSL;
- у вузькомусмислові, визначений власницький і позаштатний варіант DSL для діяльності на 1.544 Мбіт/с або 2.048 Мбіт/с над одиноч-

ною парою мідних проводів, без підтримки для мережевих-аналогових дзвінків на такій же лінії.

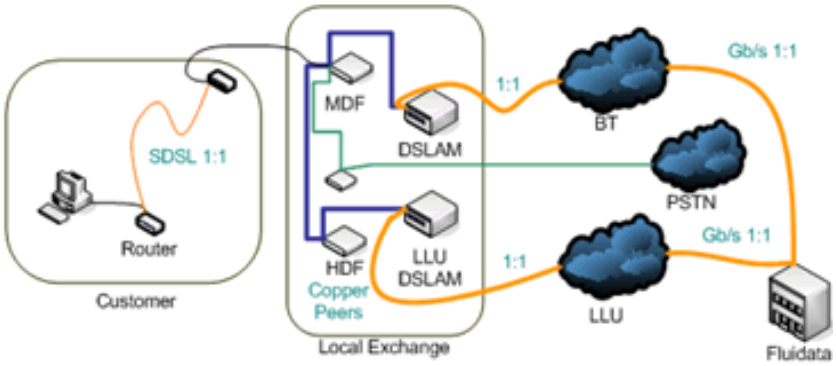


Рис. 1.6 –Виділена лінія SDSL

SDSL забезпечує пропускну спроможність між 72 кбіт/с до 2320 кбіт/с. Найпоширеніші швидкості – 1 або 1,5 Мбіт. Інтернет-провайдери, які пропонують SDSL, звичайно пропонують різні "сервісні шапки", які якимосьобразом обмежують швидкість, щоб клієнти могли платити за рівень продуктивності, який вони вимагають.

Робочий механізм SDSL уважається протилежним технології **ADSL**(англ: Asymmetric Digital Subscriber Line), яка пропонує набагато більш швидке завантаження до користувача, чім швидкість відправки від користувача. Тобто користувачі SDSL сервісів користуються як високошвидкісними завантаженнями, так і високошвидкісними відправками (Див. рис. 1.7).

При цьому відміну від асиметричного ADSL, який докладніше буде розглянутий далі, симетричний SDSL використовує всю доступну смугу пропускання двох мідних проводів. Це означає, що регулярний аналоговий телефонний зв'язок через ТСОП неможливий по тим же проводам. SDSL звичайно дорожче, чим ADSL, але дешевше, чим орендована лінія T1/E1. SDSL перевершує ADSL для виділених підключень для СПД, де спадний і висхідний трафік схожі.

У той час як ADSL-сервіс ідеально підходить для домашніх користувачів, які витрачаютьбільш дев'яноста п'яти відсотків свого часу на завантаження контенту, такого як електронна пошта, веб-сторінки, фільми й музика з інтернету, SDSL-сервіс більше орієнтований на малий бізнес. Малий бізнес буде вестибільшу частину тієї ж самої Інтернет-Діяльності, що й фізичнаособа, але вони, як правило, також будуть мати вимоги, щоб відправити багато більших файлів, передавати або обмінюватися документами, пов'язаними з роботою, або навіть обслуговувати веб-сторінки з веб-сайту, який вони розміщають зі своїх власних офісів. SDSL – це" завжди доступний " сервіс. Використання SDSL означає відсутність очі-

кування підключення або необхідності відключення або скидання служби в будь-який час, крім як при усуненні неполадок або настроюванні. Це означає, що абонент, що використовує SDSL, по суті, підключений до інтернету повний робочий день, 24 години щодня. Це ідеально підходить для підприємств, які використовують Інтернет на ринку або роблять продажу цілодобово, звичайно через веб-сайт.

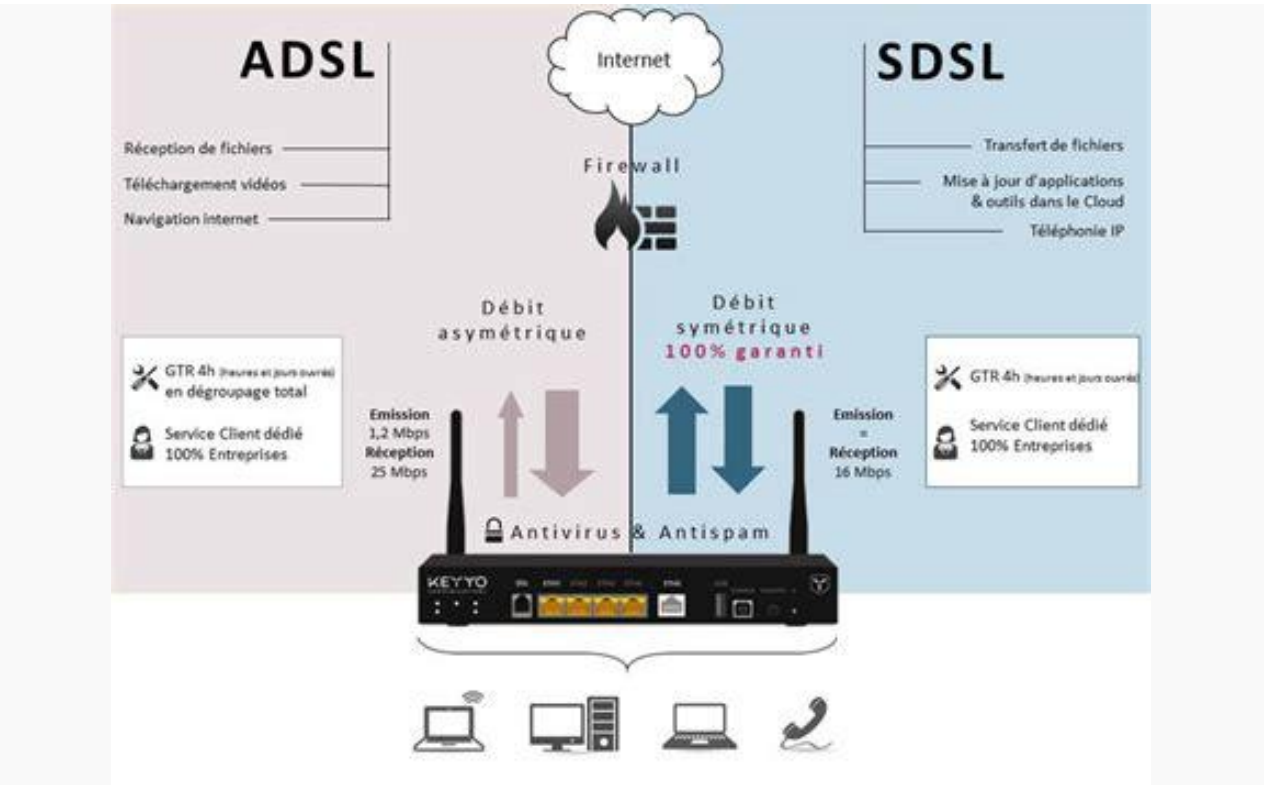


Рис. 1.7 – Відмінність SDSL від ADSL

SDSL послуги доступні від більшості великих інтернет-провайдерів або телефонних компаній у Сполучених Штатах (наприклад: Sprint, Verizon, AT&T), а також в іншій частині Північної Америки, Південної Америки, частини Азії і Європи. Європа використовуєтрохи іншу версію стандарту, яка вимагає небагато іншого обладнання, хоча в основному вона сумісна. SDSL-сервіс меншрозповсюджений в Азії, але він також росте в популярності на цьомуринку.

SDSL звичайно перебуває між ADSL і T1/E1 у ціні й був в основному орієнтований на малий і середній бізнес, який не має потреби в гарантії обслуговування **Frame relay** (з англ. - «ретрансляція кадрів», FR) – протокол канального рівняСПД. Максимальна швидкість, що допускається протоколом FR – 34,368 Мбіт/с (канали E3). Комутація: точка-точкаабобільшвисокоїпродуктивностіорендованоїлінії.

Як це не покажеться дивним, SDSL – це запатентована технологія, яка ніколи не була стандартизована. Як такий вона звичайно взаємодіє тільки із пристроями від того ж постачальника. Це попередник G. SHDSL,

який був стандартизовано в лютому 2001 року МСЕ-Т з рекомендацією G. 991.2. SDSL часто плутають із G. SHDSL і HDSL. У Європі G. SHDSL був стандартизований ETSI з використанням назви "SDSL". Цей варіант ETSI сполучимо зі стандартизованим регіональним варіантом ITU-T G. SHDSL для Європи. Симетричний DSL повільно заміняється на G. SHDSL (Single-Pair High-speed Digital Subscriber Line).

SDSLє прототипом HDSL, у якомувикористовується тільки одна пара кабелю. Відомі дві модифікації цього обладнання: MSDSL (багатошвидкісна SDSL) і HDSL2, що мають вбудований механізм адаптації швидкості передачі до параметрів фізичної лінії.

HDSL (англ: High Data Rate Digital Subscriber Line) – високошвидкісна цифрова абонентська лінія, яка є двонаправленою і симетричною системою передачі, яка дозволяє транспортувати сигнали зі швидкістю передачі даних зі швидкістю T1 (1544 кбіт/с) або E1 (2048 кбіт/с) по мідних кручених парах мережі доступу. Система HDSL використовує техніку лунапоглинання для розділення напрямків передачі, так що одна вита пара може нести обидва напрямки. Рекомендується два різні варіанти коду лінії: імпульсно-амплітудна модуляція 2B1Q (два біти (2B) в один із чотирьох рівнів напруги (1Q)), та CAP – амплітудно-фазової модуляції без несучої. CAP застосовується лише для 2048 кбіт/с, тоді як для 2B1Q визначено два різних кадри для 1544 кбіт/с та 2048 кбіт/с. 2B1Q для 2048 кбіт/с забезпечує як дуплексну передачу на одній парі, так і паралельну передачу на дві або три пари. Це дозволяє розподілити сигнал на кілька пар, зменшити швидкість передачі символів та збільшити довжину рядка. CAP визначається лише для однієї або двох пар, а 1544 кбіт/с 2B1Q-лише для двох пар. Більш низькі швидкості обслуговуються використанням 64 кбіт/с каналів, усередині T1/E1 пакета.

Це звичайно називається потоком T1/E1, і використовується для надання низькошвидкісних каналів користувачам. У таких випадках, швидкість каналу буде повною (T1/E1), але абонент одержить тільки обмежену швидкість 64 кбіт/сзі своєї сторони. Максимальна швидкість СПД HDSL підтримується тільки на відстані не більш 4,5 км при використанніоднієї або двох витих пар кабелю. СПД HDSL може працювати на більших відстанях, за умови використання регенераторів.

SHDSL (Single-pair High-speed Digital Subscriber Line - Рекомендація МСЭ-Т G.991.2) - СПД на основі одинарної високошвидкісної цифрової абонентської лінії у базовому варіанті з двопроводовим режимом роботи прийомопередавачів SHDSL зі швидкістю передачі від 192 кбіт/с до 2312 кбіт/с. використовує 16-позиційну амплітудно-імпульсну модуляцію (AIM) із ґратчастим кодуванням — 16-TCPAM (TCPAM — Trellis Coded PAM). Цей спосіб модуляції забезпечує передачу чотирьох бітів (трьох бітів корисної інформації й додаткового біта кодування) на одному тактовому інтервалі. Використання ґратчастих (trellis) кодів дає виграш в 5 Дб,

що дозволяє знизити ймовірність помилки при передачі й побільшати дальність зв'язку. Для декодування в приймачі використовується ефективний алгоритм Вітербі. Додатковий виграш у SHDSL отриманий за рахунок застосування попередкодування Томлінсона (Tomlinson) — предкорекції сигналу в передавачі на основі знання імпульсної характеристики каналу. У результаті застосування цих алгоритмів SHDSL у порівнянні з однопарним варіантом основі технології HDSL (Рекомендація MCE-T G.991.1), що використовує код 2B1Q, як показала експлуатація, дозволяє побільшати на 35...45% швидкість передачі при тій же дальності або побільшати дальність на 15...20% при тій же швидкості.

Прийомопередавачі SHDSL призначені в основному для дуплексної роботи по двопроводним витим металевим парам змішаної (аналого-цифрової) лінії. Додаткова операція з кількома парами підтримується для додатків із розширеним охопленням. Передбачається застосування додаткових регенераторів сигналів для однопарної та багатопарної роботи. Прийомопередавачі SHDSL розроблені таким чином, щоб вони були спектрально сумісними з іншими технологіями передачі, що використовуються в мережі доступу, включаючи інші технології DSL. Прийомопередавачі SHDSL не підтримують використання технології аналогового розділення для співіснування з POTS або ISDN.

Двопроводовий режим роботи (базовий) для прийомопередавачів SHDSL, здатний підтримувати швидкість передачі даних користувачами (корисним навантаженням) від 192 кбіт/с до 2312 кбіт/с з кроком 8 кбіт/с. Допустимі швидкості визначаються $n \times 64 + i \times 8$ кбіт/с, де $3 \le n \le 36$ та $0 \le i \le 7$. Для $n = 36$ і обмежується значеннями 0 або 1.

Додатковий режим чотирьох проводів був розширений до більш загального багатопарного режиму, який забезпечує додаткову підтримку до чотирьох парних з'єднань. Режим чотирьох проводів ідентичний режиму M-пар з $M = 2$, за винятком методу призначення порядкових номерів парам проводів. У режимі чотирьох проводів порядкові номери (ідентифікаційний номер проводової пари) визначаються під час попередньої активації, де пара 1 визначається як пара, на якій проводиться остаточна транзакція G.994.1, тоді як у режимі M-пари порядкові номери призначаються парам проводів. Для збільшення швидкості передачі в SHDSL передбачена можливість використання одночасно до чотирьох пар, що дозволяє забезпечити швидкість передачі даних від 2*2312 кбіт/с =4624 кбіт/с / 1024 = 4,5 Мбіт/с до 4*2312 кбіт/с =9248 кбіт/с / 1024 = 9 Мбіт/с.

Додаткові розширення, описані у G.991.2 Додатку F, дозволяють підняти швидкість обміну даними користувача до 5696 біт/с. Ця Рекомендація також визначає необов’язковий робочий режим M-пар, здатний підтримувати швидкість передачі даних користувача (корисного навантаження) від $M \times 192$ кбіт/с до $M \times 2{,}312$ Мбіт/с з кроком $M \times 8$ кбіт/с, де $1 \le M \le 4$. Зауважте, що додаткові розширення, описані у Додатку F, дозво-

ляють користувачам отримувати швидкість передачі даних до М × 5696 кбіт/с. В режимі чотирьох проводів ідентичний режиму М-пар з М = 2, розширена швидкість передачі даних може досягти 2 × 5696 кбіт/с = 11392 кбіт/с = 11,125 Мбіт/с.

Додаткові розширення, описані в Додатку F Рекомендації G.991.2, передбачають опцію СПД SHDSL використання як модуляції 16-TCPAM, так і 32-TCPAM, що дозволяє при роботі в чотирипарномурежимі передачі (М = 4) досягати швидкості 4 × 5696 кбіт/с = 22784 кбіт/с = 22,25 Мбіт/с.

За рахунок розширення набору швидкостей передачі СПД SHDSL оператор може вибудувати маркетингову політику, що більш повно задовольняє потребам клієнтів. Крім того, зниження швидкості передачі дозволяє в необхідних випадках добитися збільшення дальності передачі, наприклад. коли установка регенераторів неможлива. При максимальній швидкості передачі довжина цифровий лінії СПД SHDSL становить близько 2 км (для кабелю ТПП із діаметром жили кабелю 0,4 мм), при мінімальної – понад 6 км.

Розглянемо далі докладніше сучасні, найбільш швидкісні СПДADSL і VDSL.

Технології .ADSL і VDSL стрімко розвиваються. Починаючи з 1999 року, коли була прийнята Рекомендація МСЕ-Т G.992.1 (ADSL), стандартизовано 5 типів систем ADSL і 2 типу систем VDSL. Нижче наведений опис кожного із цих типів СПД.

ADSL (англ.*AsymmetricDigitalSubscriberLine*– Асиметрична цифрова абонентська лінія) – модемна технологія, у якій доступна смуга пропускання каналу розподілена між вхідним (спадним) і вихідним (висхідним) трафіком асиметрично. Тому що в більшості користувачів обсяг вхідного трафіка значно перевищує обсяг вихідного, то швидкість вихідного трафіка значно нижче. Це обмеження стало проявлятися ширше у зв'язку з поширенням відеозв'язку і пірінгових мереж – **Peer-to-peer, P2P** (з англ. – рівний до рівного) – варіант архітектури системи, в основі якої стоїть мережа рівноправних вузлів, яка характеризується тим, що її елементи можуть зв'язуватися між собою, на відміну від традиційної архітектури, коли лише окрема категорія учасників, яка називається серверами, може надавати певні сервіси іншим.

СПД ADSL забезпечує базову швидкість «спадного» потоку даних 6,144 Мбіт/с і швидкість «висхідного» потоку даних 640 Кбіт/с.

У Додатку Н (10/2000) до Рекомендації МСЕ-Т G.992.1 описаний симетричний варіант ADSL, що забезпечує швидкість передачі від 192 кбіт/с до 1,6 Мбіт/с як у спадному, так і у висхідному напрямках. Передбачене використання повністю цифрового режиму передачі, коли використовуються несучі із частотами nx4,3125 кГц, де п = 1, 2,..., 5.

Можливість передачі даних STM зі швидкістю 1,544 Мбіт/с додатково підтримується. Прийомопередавачі SSDSL можуть надавати послуги циф-

рових даних на одній витої парі з послугами голосового діапазону (включаючи послуги POTS та послуги передачі даних голосового діапазону). Схема передачі SSDSL займає смугу частот над діапазоном голосового зв'язку і може бути відокремлена від неї фільтрацією. За бажанням, коли служба POTS і фільтрація не використовуються, частоти нижче 26 кГц, включаючи голосовий діапазон, можуть використовуватися в режимі EFT.

У Додатку I (03/2003) Поправка 1: Переглянутий Додаток C, новий Додаток I та новий Додаток V від 2003 р. до Рекомендації MCE-T G.992.1 описаний необов'язковий додатковий режим кадрування з підтримкою більш високої швидкості передачі даних у бік користувача при зрівнянні кодового слова для цього режиму кадрування до однакової довжини N. Відповідна швидкість передачі даних в цьому режимі представлена 32 × (3N – 1) кбіт/с, де N може приймати для цілочисельних значень від 171 до 255. Фактично це описаний прототип ADSL2+, що забезпечує швидкість передачі даних від 32·(3·171-1)=1638416 кбіт/с/1024=16 Мбіт/с до 32·(3·255-1)=24448 кбіт/с/1024≈24 Мбіт/с у спадному напрямку.

Блок СПД ADSL може одночасно передавати все наступне: симплекс за потоком канали, дуплексні канали, аналоговий дуплексний канал базової смуги та накладні витрати на лінію ADSL для кадрування, контроль помилок, експлуатація та обслуговування.

Асиметричність швидкості передачі в комплексі з постійно встановленим з'єднанням (коли виключається необхідність щораз набирати телефонний номер і чекати встановлення з'єднання) робить технологію ADSL ідеальної для організації доступу до мережі Інтернет. Технологія ADSL дозволяє зберегти телефонний зв'язок шляхом використання частотних роздільників (спліттерів) – одного на АТС і інший у приміщенні користувача. До одного входу спліттеру в приміщенні користувача підключається аналоговий телефонний апарат, а до іншого – ADSL– модем, який залежно від реалізації може виконувати також функції маршрутизатора, комутатора або мосту. При цьому робота ADSL-модему не заважає функціонуванню традиційного телефонного зв'язку, що працює незалежно від того, чи функціонує канал ADSL.

Передача даних за технологією ADSL реалізується через звичайну аналогову телефонну лінію за допомогою абонентського пристрою – модема ADSL та мультиплексора доступу (англ.*DSL Access Multiplexer*, DSLAM), який знаходиться на тій же АТС, до якої підключається телефонна лінія користувача, причому включається DSLAM до обладнання самої АТС. DSLAM мультиплексує множину абонентських ліній DSL в одну високошвидкісну магістральну мережу.

Також вони звичайно підключаються до мережі ATM по каналах PVC (постійний віртуальний канал; англ.*Permanent Virtual Circuit*) до провайдерів послуг Internet та інших мереж. Слід відзначити, що два ADSL-модеми не зможуть з'єднатися одне з одним, на відміну від модемів Dial-

Up. Звичайно, через необхідність встановлення обладнання на кожній АТС затрати на побудову і утримання мережі були помітно вищі, ніж у випадку класичного комутованого доступу, коли всі модеми провайдера встановлювались на одній АТС, однак в порівнянні з вартістю інших способів надання високошвидкісного доступу до мережі Інтернет технологія DSL виявилась дуже дешевою.

Частотний план для ADSL показаний на рис. 1.8.

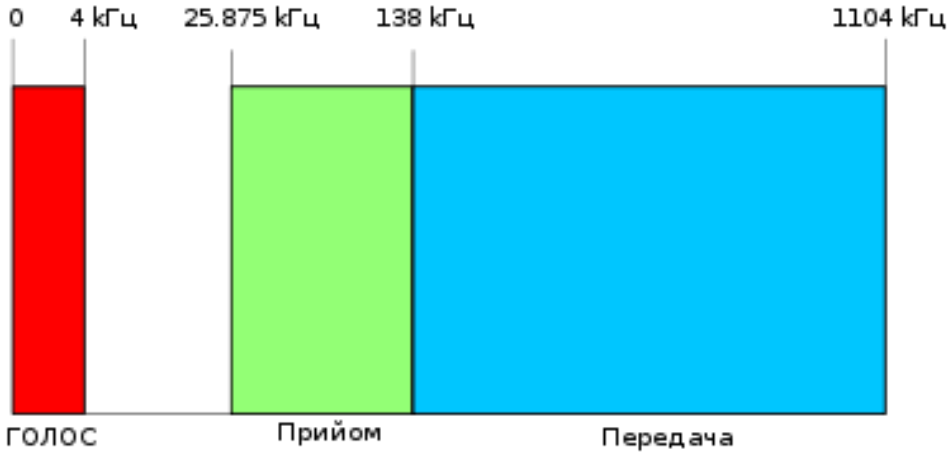


Рис. 1.8 – Принцип роботи ADSL

Червона область – діапазон частот, що використовується звичайним телефоном (голос), зелена та блакитна області використовуються для ADSL (див. рис. 1.8).

В технології ADSL доступна смуга пропускання каналу розподілена між вихідним та вхідним трафіком несиметрично – для більшості користувачів вхідний трафік значно суттєвіший, ніж вихідний, тому використання для нього більшої частини смуги пропускання повністю виправдане (за виключенням пірінгових мереж та електронної пошти, де об'єм і швидкість вихідного трафіку є достатньо важливими). Звичайна телефонна лінія використовує для передачі голосу смугу 0,3…3,4 кГц. Щоб не заважати використанню телефонної мережі за її прямим призначенням, в ADSL нижня межа діапазону частот знаходиться на рівні 26 кГц. Верхня ж межа, виходячи з вимог до швидкості передачі даних і можливостей телефонного кабелю, становить 1,1 МГц. Ця смуга пропускання ділиться на дві частини – частоти від 26 кГц до 138 кГц відведені для вихідного потоку даних, а частоти від 138 кГц до 1,1 МГц – вхідного. Смугу частот від 26 кГц до 1,1 МГц було обрано не випадково. Починаючи з частоти 20кГц і вище, затухання майже не залежить від частоти.

Такий частотний розподіл дозволяє розмовляти по телефону, не перериваючи обмін даними тією ж лінією.

Зрозуміло, можливі ситуації, коли або високочастотний сигнал ADSL-модему негативно впливає на електроніку сучасного телефону, або телефон через яких-небудь особливості своєїсхемотехніки вносить у лі-

нію сторонній високочастотний шум або ж сильно змінює її амплітудно-частотну характеристику (АЧХ) в області високих частот.

Для розділення низькочастотного аналогового сигналу та високочастотного цифрового використовується у телефонну мережу безпосередньо у квартирі абонента встановлюється фільтр низьких частот – частотний розділювач (спліттер, від англ.*Splitter*), що пропускає до звичайних телефонів тільки низькочастотну складову сигналу, що й усуває можливе вплив телефонів на лінію. Перелік ADSL-обладнання складається з DSLAM-лінії, ADSL-модема, ADSL-фільтра а схема його підключення представлена на рис. 1..9.

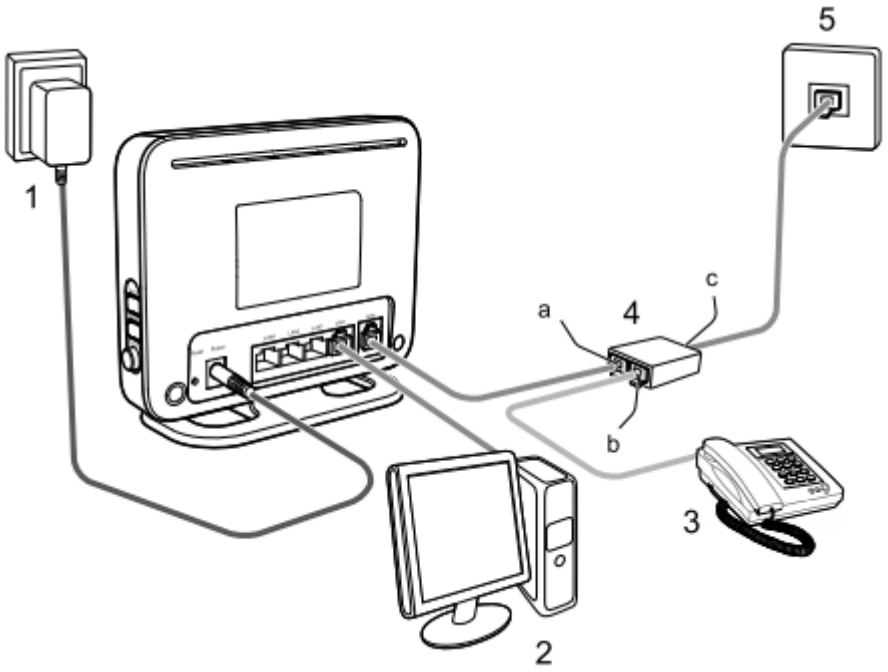


Рис. 1.9 – Підключення ADSL-обладнання:

1 – блок живлення; 2 – комп'ютер; 3 – телефон; 4 – спліттер – ADSL-фільтр (розділювач частот); 5 – телефонна розетка (DSLAM): а – роз'єм DSL (RJ-45); б – роз'єм для телефона (RJ-11); с – роз'єм телефонної лінії (RJ-11

Також замість сплітеру можливе використання мікрофільтрів. Такі фільтри не вимагають додаткового живлення, тому мовний канал залишається в ладі при відключеній електричній мережі й у випадку несправності обладнання ADSL.

В цьому випадку модем підключається до лінії напряму, а всі телефони, факси та ін. аналогові пристрої підключаються до лінії через мікрофільтри.

Головною перевагою при використанні ADSL-модемів є можливість одночасно працювати в Інтернет і розмовляти телефоном. Телефон залишається вільним.

ADSL модеми випускаються з двома типами інтерфейсів: USB і 10/100Base-T. Перші призначені для індивідуального підключення і зручні тим, що не потребують блока живлення. Другі зручніші при багатьох підключеннях і, як правило мають вбудовані роутери, в т.ч. безпроводові (Wi-Fi).

Завдяки тому, що у з'єднанні не використовується комутація телефонної мережі загального користування, яка має високий рівень шуму і завад, виникає значна різниця якості ADSL і звичайної телефонної лінії. Ймовірність помилки на лінії ADSL не значна і становить 10^{-8} – 10^{-10}.

Максимальна швидкість лінії залежить від ряду факторів, таких як довжина лінії, перетин і питомий опір кабелю. Також істотний внесок у підвищення швидкості вносить той факт, що для ADSL лінії рекомендується вита пара, а не так звана «локшина» - телефонний розподільний провід (ТРП), причому екранована, інакше знижується пропускна спроможність каналу передачі даних, а якщо це багатопарний кабель, те й з дотриманням напрямку й кроку плетива.

Поділ переданих і прийнятих даних досягається тим, що при використанні ADSL дані передаються по загальній парі в дуплексній формі. Для того, щоб розділити переданий і прийнятий потік даних, існують два методи: частотний поділ каналів (англ.*Frequency Division Multiplexing*, **FDM**) і лунакомпенсація (англ.*Echo Cancellation*, **EC**)

При використанні даного механізму відбувається частотний розподіл каналів, де низькошвидкісний канал переданих даних розташовується відразу після смуги частот, використовуваної для передачі аналогової телефонії. Високошвидкісний канал прийнятих даних розташовується на більш високих частотах. Смуга частот залежить від числа біт, переданих одним сигналом.

Порівняння методів модуляції FDM і EC:

- Лунакомпенсація (EC) дозволяє поліпшити продуктивність на 2 Дб, однак більш складна в реалізації чім FDM.
- Переваги EC ростуть при використаннібільш високошвидкісних технологій, таких як ISDN або відеотелефонія на швидкості до 384 кбіт/с. У цих випадках FDM вимагає виділення під високошвидкісний канал прийнятихданихбільш високих частот, що приводить до збільшення загасання й скороченню максимальної відстані передачі.
- Суміщення двох каналів в одному частотному діапазоні, при використанні EC приводить до появи ефекту власного NEXT (зв'язок між розташуванням частот спектрів сусідніх каналів), який відсутній при використанні FDM.
- Стандарт ADSL передбачає взаємодію між різним обладнанням, що використовують як механізм FDM, так і EC, вибір конкретного механізму визначається при встановленні з'єднання.

У великих містах розвинутих країн світу ADSL витісняється більш швидкими технологіями доступу Ethernet (ETTH), GPON (FTTH) і DOCSIS (стандарт передачі даних по телевізійному кабелю). Причина цього – обмежена пропускна спроможність у мережах ADSL (до 24 Мбіт/с в ADSL2+), особливо «висхідного потоку» від абонента (до 1,4 Мбіт/с), у той час як Eurodocsis 2.0 забезпечує швидкість передачі даних 50↓/27↑ Мбіт/с, Fast Ethernet – до 100 Мбіт/с, Gigabit Ethernet – до 1 Гбіт/с, 10 Гбіт/с EPON – до 10 Гбіт/с.

Незважаючи на появу більш швидких способів передачі даних, технологія ADSL як і раніше залишається поки ще лідером на ринку широкосмугової передачі даних.

Splitterless ADSL (англ: Splitterless asymmetric digital subscriberline**)** **–** безспліттерна асиметрична цифрова абонентська лінія відповідно до Рекомендації MCE-T G.992.2 – це варіант технології ADSL, що забезпечує швидкість передачі в спадному напрямку до 1,536 Мбіт/с, а у висхідному напрямку – до 512 кбіт/с. Обладнання технології Splitterless ADSL є більш простим в установці й більш дешевим, чім ADSL. Одним зі шляхів спрощення установки модемів Splitterless ADSL стало введення високочастотної частини спліттера в корпус модемів, що позбавило від необхідності установки зовнішнього спліттера.

UADSL (англ: Universal Asymmetric Digital Subscriber Line) – універсальна асиметрична цифрова абонентська лінія, технологія UADSL (стандарт на обладнання високошвидкісного доступу в Internet для масового споживача по звичайних телефонних лініях без частотного роздільника через плату ADSL.

UADSL є спрощеним аналогом технології Splitterless ADSL і орієнтована на абонентів квартирного сектору. Обладнання цієї технології дешевше й простіше в установці.

Максимальні швидкості обміну СПД UADSL становлять:

1, 536 Мбіт/с у напрямку до абонента й 384 кбіт/с – у зворотному напрямку при довжині абонентської лінії до 3,5 км;

640 кбіт/с у напрямку до абонента й 196 кбіт/с – у протилежному напрямку при довжині абонентської лінії до 5,5 км.

HomePNA (англ. HomePhonelineNetworkingAlliance, **HPNA**)– це об'єднана асоціація некомерційних промислових компаній, які просувають і стандартизують технології домашніх мереж за допомогою існуючих у будинкахкоаксіальних кабелів і телефонних ліній. HPNA створює промислові специфікації, які потім стандартизуються MCE (ITU), Найсучасніша на даний момент версія– 3.1 це перший з нового покоління стандартів домашніх мереж, розроблений для нових «розважальних» додатків, таких як IPTV, які припускають наявність високої й стійкої продуктивності в цілому будинку. Технологія цього типу забезпечує додаткові можливості, такі як гарантована якість обслуговування (Quality of Serviceqos) і ви-

користовується більшістю провайдерів для забезпечення комерційного сервісу «triple play» (відео, звук і інформація). HomePNA 3.1 був розроблений як для збільшення функціональності в коаксіальних проводах і розширення їх мережевих можливостей, так і для подолання деяких обмежень телефонних мереж.

Вимоги для HomePNA 3.1:

1. Стандартний телефонний або коаксіальний кабель (той, який використовується зараз для цифрового телебачення)
2. Обладнання, сертифіковане HomePNA.

ADSL2 (англ:Asymmetricdigitalsubscriberlinetransceivers 2**)** – асиметрична цифрова абонентська лінія ADSL2 згідно з Рекомендацією МСЕ-Т G.992.3 є вдосконаленою версією ADSL.Технологія ADSL2 забезпечує швидкість передачі в спадному напрямку до 8 Мбіт/с, а у висхідному напрямку – до 800 кбіт/с. Обладнання більшості виробників забезпечує швидкість передачі до 12 Мбіт/с у спадному напрямку й до 1 Мбіт/с у висхідному напрямку. Збільшення швидкості передачі в порівнянні з ADSL, відповідної до Рекомендації G.992.1, обумовлене внесенням цілого ряду описаних нижче вдосконалень.

1) Більш гнучка й ефективна побудова кадра дозволяє управляти кількістю службової інформації (від 4 до 64 кбіт/с), тобто зменшити її обсяг, а значить побільшати швидкість передачі корисної інформації, що особливо важливо на довгих лініях.

2) Структура кадрів дозволяє більш ефективно використовувати виграш за рахунок кодування Ріда-Соломона.

3) Оновлені процедури діагностики лінії, призначені для виявлення несправностей і моніторингу характеристик ліній ADSL2 під час роботи: прийомопередавачи ADSL2 можуть здійснювати виміру рівня шуму в лінії, загасання й відносини сигнал/шум на обох кінцях лінії. При цьому виміру цих параметрів можуть здійснюватися навіть при неможливості встановлення нормального з'єднання по даній лінії.

4) Додана підтримка однобітних кодових сузір'їв, що дозволяє одержати більшу дальність роботи системи на малих швидкостях.

5) Поліпшені процедури управління передачею. Наприклад, система може адаптувати швидкість передачі даних у режимі реального часу. Це нововведення, називане фоновою адаптацією швидкості (Seamless Rate Adaptation, SRA), дозволяє системам ADSL2 змінювати швидкість передачі даних під час роботи без переривань зв'язку або бітових помилок. Для цього система діагностує зміни характеристик каналу зв'язки (наприклад, коли місцева Am-Радіостанція виключає свій передавач на ніч) і непомітно для користувача міняє швидкість передачі.

6) Додана функція регулювання споживаної потужності, що дозволяє системі, перебуває в стійкому режимі L0 (режимі постійної передачі корисної інформації), режимі низького споживання потужності L2(споживана

потужність залежить від характеру трафіка) або в режимі холостого ходу L3(сплячий режим, коли інформація тривалий час не передається).

7) У системах ADSL2 кількість службових бітів у кадрі може мінятися від 5,12 % до 25 %, на відміну від ADSL, де під службову інформацію постійно відведено 25 % загальної швидкості.

Splitterless ADSL2 (англ: Splitterless asymmetric digital subscriber line transceivers 2) – асиметрична цифрова абонентська лінія ADSL2 без спліттера**,** відповідна до Рекомендації G.992.4, – наступне покоління технології Splitterless ADSL (G.Lite), яке забезпечує швидкість передачі в спадному напрямку до 1,536 Мбіт/с, а у висхідному напрямку – до 512 кбіт/с.. У порівнянні з Splitterless ADSL технологія Splitterless ADSL2 має ряд удосконалень:

- поліпшена підтримка цифрових служб і передачі голосу;
- поліпшена можливість зміни характеристик лінії «на ходу»;
- удосконалені процедури управління спектром передачі;
- додана підтримка однобітових кодових слів;
- доданий повністю цифровий режим роботи.

ADSL2+ (англ: Asymmetricdigitalsubscriberlinetransceivers 2 (ADSL2) – Extendedbandwidth (ADSL2plus)) – СПД ADSL з розширеною пропускною здатністю (прийомопередавач ADSL2+), відповідно до Рекомендації G.992.5, може одночасно передавати все наступне: ряд несучих кадрів у низхідного та висхідного напрямку; простий старий телефонний сервіс базової смуги (POTS)/дуплексний канал ISDN; та службову інформацію для кадрування на лінії ADSL, контролю помилок, операцій та обслуговування. СПД ADSL2+підтримують базову швидкість передачі даних в діапазоні до 16 Мбіт/с у нижньому та 800 кбіт/с у верхньому потоці. Підтримка мережевих швидкостей передачі даних вище 16 Мбіт/с за низхідним потоком та підтримка швидкості передачі даних вище 800 кбіт/с за висхідним потоком є необов'язковою.

ADSL2+ призначена для високошвидкісного доступу до Інтернет та відноситься до класу широкосмугових (broadband) технологій та згідно да Рекомендації ITU T G.992.5 (2009) – Виправлення 1 забезпечує швидкість передачі даних в напрямку абонента – до 24 Мбіт/с, від абонента – до 3.5 Мбіт/с. Така висока швидкість СПД дозволяє комфортно працювати з Web-сайтами, швидко передавати великі файли і документи, працювати з мультимедіа, повноцінно використовувати інтерактивні засоби.

Примітка. Прототип ADSL2+, що забезпечує швидкість передачі до 24 Мбіт/с у спадному напрямку, фактично був раніше описаний розширеннями можливостей СПД ADSL у Додатку I Зміни 1 від 2003 р. до Рекомендації МСЕ-Т G.992.1.

Основні відмінності ADSL2+ від ADSL2:

– підтримка до трьох кодових слів коду Ріда-Соломона на один DMT-Символ;

– удосконалені процедури управління спектром при встановленні з'єднання й під час передачі інформації;

– поліпшена підтримка послуг, що вимагають високих швидкостей передачі даних у спадному напрямку (наприклад, широкосмугові розважальні послуги).

Обладнання ADSL2+ більшості виробників забезпечує швидкість передачі у висхідному напрямку до 1 Мбіт/с, а в спадному напрямку – до 24 Мбіт/с. Таке збільшення швидкості передачі стало можливим за рахунок майже дворазового (до 2,208 Мгц) розширення смуги частот, використовуваної для передачі в спадному напрямку (Див. рис. 1.8).

VDSL (англ: Very high speed Digital Subscriber Line), – надвисокошвидкісна цифрова абонентська лінія, відповідна до Рекомендації МСЕ-Т G.993.1, забезпечує в асиметричному варіанті швидкість передачі в спадному напрямку до 57 Мбіт/с, а у висхідному – до 33 Мбіт/с. У симетричному варіанті швидкість передачі в обох напрямках становить до 33 Мбіт/с. Така висока швидкість передачі досягається тільки на невеликих відстанях: близько 300 м при швидкості 57 Мбіт/с і близько 1,8 км при швидкості 13 Мбіт/с. Технологія VDSL може використовуватися з тими ж цілями, що й ADSL, а також для передачі сигналів телебачення високої чіткості (HDTV), відео по запиту і т.д.

Головне застосування VDSL – цифрові абонентські лінії, у яких потрібно дуже висока швидкість передачі від абонента в мережу. У рішеннях, заснованих на VDSL, центральною точкою системи є спеціалізована, комутуюча система, що ухвалює трансльовані дані із джерела (наприклад, з оптико-волоконного кабелю), і, отже, використовуючи класичні, мідні кабелі, що передає дані цільовому одержувачеві. Правило роботи технології VDSL опирається на використанні широкого діапазону частот сигналів, що посилають у мідних кабелях, і четвертного множення використовуваних діапазонів, з метою відокремити частотні канали. Нижньою граничною частотою є 300 кГц (на практиці застосовується 350 кГц) у ситуації відсутності необхідності передачі сигналів аналогової телефонії. Верхня межа залежить від довжини сегмента кабелів і може становити від 30 МГц для кабелю, що не перевищує 300 м, і до 10 МГц при 500-метровомукабелі.

Такі технічні рішення дозволяють одержати дуже високу пропускну спроможність, однак на відносно коротких відрізках кабелів:

- 56 Мбіт/с на дистанції до 300 метрів (на практиці використовуються сегменти, що не перевищують 200 м;
- 25 Мбіт/с на дистанції 300-900 м;
- 10 Мбіт/с на дистанції до 1500 м.

Після перевищення довжини кабелю в 1500 м, пропускна спроможність, доступна за технологією VDSL, стає нижче, чим у випадку використ-

тання технології ADSL. Із цієї причини, на більших дистанціях зв'язку, засновані на VDSL, не використовуються.

VDSL2 (англ. Very-high data rate Digital Subscriber Line 2) – надвисокошвидкісна цифрова абонентська лінія 2),відповідна до Рекомендації МСЕ-Т G.993.2, що визначає технологію доступу, яка використовує існуючу інфраструктуру мідних проводів, які спочатку були розгорнуті для послуг POTS, котру можна розгортати з центральних офісів, з шаф з подачею волокна, розташованих поблизу приміщень замовника або всередині будівель. Рекомендація МСЕ-Т G.993.2, є вдосконаленням МСЕ Т G.993.1, яка підтримує асиметричну та симетричну передачу і забезпечує при двонаправленій швидкості передачі даних сумарну базову швидкість передачі в спадному й висхідному напрямках до 200 Мбіт/с. на витих парах із використанням смуги пропускання до 30 МГц. Ця Рекомендація визначає лише дискретну багатотонну (DMT) модуляцію та включає компоненти з [ITU-T G.993.1] (VDSL), [ITU-T G.992.3] (ADSL2) та [ITU-T G.992.5] (ADSL2+).

Вирішення VDSL2 дозволяє значно помножити можливу пропускну спроможність, однак, подібно тому як у випадку попередника VDSL, на коротких дистанціях:

- 200 Мбіт/с на дистанції, що не перевищує 300 м (практично не перевищує 200 м);
- 100 Мбіт/с на дистанції 500 м;
- 50 Мбіт/с на дистанції до 1000 м.

На дистанції від 1500 м і вище можлива пропускна спроможність близька до тієї, що доступна за технологією ADSL, і втримується на даномурівні на дистанції до 4–5 км.

Основні відмінності VDSL2 від VDSL:

– визначені плани частот до 30 Мгц, що дозволяє одержати сумарну швидкість передачі до 200 Мбіт/с (швидкість передачі в спадному напрямку плюс швидкість передачі у висхідному напрямку);

– визначена більша кількість профілів для підтримки широкого спектра сценаріїв установки (наприклад, на АТС, у розподільному ящику з підведеної до нього оптоволоконною лінією, у будинку абонента й т.п.);

– збільшено до 20,5 Дб максимальна потужність передачі в спадному напрямку;

– регламентована обов'язкова підтримка ґратчастого кодування;

– поліпшені процедури ініціалізації;

– регламентована обов'язкова підтримка всіх типів сигнальних сузір'їв для передачі від 1 до 15 бітів протягом тактового інтервалу;

– підтримка широкого спектра параметрів тестування (за аналогією з ADSL2);

– поліпшена будова кадра, засноване на ADSL2, з удосконаленим службовим каналом;

– поліпшені можливості надлишкового кодування й перемеження, розширений спектр настроювань пристрою, що кодує, коду Ріда-Соломона й пристрою перемеження;

– підтримка повністю цифрового режиму роботи.

Великий радіус дії – одне з головних переваг VDSL2. Системи LR-VDSL2 можуть забезпечувати швидкість порядку 1-4 Мбіт/с (downstream) на відстані 4-5 км, поступово збільшуючи швидкість до симетричних 100 Мбіт/із при зменшенні довжини лінії. Це означає, що VDSL2-системи, на відміну від VDSL1, не обмежуються тільки короткими місцевими лініями, або лініями усередині будівлі, але також можуть бути застосовуватися на середніх відстанях.

VDSL2 — досить складний протокол. Стандарт визначає широкий діапазон профілів, які можуть використовуватися в різній архітектурі розгортання VDSL2: у центральному офісі, у кабінеті або в будинку табл. 1.3.

Таблиця. 1.3 – Профілі архітектурі розгортання VDSL

Профіль	**Діапазон частот (обробка сигналу) (МГц)**	**Кількість несучих**	**Крок несучих (кГц)**	**Потужність (дБм)**	**Макс. швидкість вхідна /вихідна (Мбіт/с)**
8a	8.832	2048	4.3125	+17.5	50 / 16
8b	8.832	2048	4.3125	+20.5	50 / 16
8c	8.500	1972	4.3125	+11.5	50 / 16
8d	8.832	2048	4.3125	+14.5	50 / 16
12a	12	2783	4.3125	+14.5	68 / 22
12b	12	2783	4.3125	+14.5	68 / 22
17a	17.664	4096	4.3125	+14.5	100 / 50
30a	30.000	3479	8.625	+14.5	200 / 50
17a	35.328	8192	4.3125	+17.0	150 / 50
35a	35.328	8192	4.3125	+17.0	250 / 50
35b	35.328	8192	4.3125	+17.0	400 / 50

Додаток PITU G.993.2. описує короткодоступний VDSL2 зі зменшеною потужністю та підвищеною швидкістю передачі даних,де значення мінімальної двонаправленої швидкості передачі даних складає відповідно для профіля 17а – 150 Мбіг/с та для профіля 30а – 250 Мбіг/с.

Додаток Q ITU G.993.2. описує підвищену швидкість передачі даних VDSL2 що дозволяє передавати асиметричний і симетричний трафік (downstream і upstream) по витої парі із використанням смуги пропускання до 35 МГц з інтервалом піднесучих частот 4,3125 кГц, із сумарною швидкістю для профіля 17а – 150 Мбіг/с , та для профіля 35б – 400 Мбіг/с.

Швидкість VDSL2 для профіля 30а починає швидко падати з теоретичного максимуму 250 Мбіт/с до 100 Мбіт/с на відстані 0.5 км і до

50 Мбіт/с на відстані від 1 км. При цьому, однак, слід зазначити, що падіння швидкості стосовно відстані відбувається значно повільніше, чим в VDSL. Починаючи з 1,6 км продуктивність VDSL2 рівна ADSL2+ .

З'єднання (ITU-T G. 998.x) може використовуватися для об'єднання декількох пар проводів для збільшення доступної ємності або розширення охвату мідної мережі. Мережі з гібридним доступом дозволяють поєднувати мережі xDSL з безпроводовими мережами. Це дозволяє провайдерам надавати більш швидкісний доступ в Інтернет по довгих лініях.

В рекомендаціях G.993.5 описаний метод шумозаглушення FEXT (векторізація) для використання із прийомопередавачами VDSL2. Векторизация – це метод передачі, при якому використовується координація лінійних сигналів для зменшення рівнів перехресних перешкод на дальньому кінці (власних перешкод FEXT) в низхідному і висхідному напрямках і поліпшення характеристик роботи. Ступінь поліпшення залежить від характеристик каналу. Векторизация може бути вигідна одному або декільком користувачам. Метод придушення власних перешкод FEXT усуває перешкоди FEXT, створювані групою прийомопередавачів ближнього кінця і заподіюють перешкоди прийомопередавачам далекого кінця тієї ж групи. Це придушення відбувається між приймачами цифрового абонентської лінії з дуже високою швидкістю 2 (VDSL2), але необов'язково одного і того ж профілю. Ця Рекомендація МСЕ-Т G.993.5 призначена для виконання спільно з Рекомендацією МСЕ-Т G.993.2

Зведемо до табл. 1.4 основні характеристики технологій СПД xDSL, регламентовані Рекомендаціями UTU (МСЕ) G.991 ... G.993.

Таблиця. 1. 4 – Порівняльний аналіз характеристик технологій xDSL

Стандарт ITU	**Технологія xDSL**	**Макс. швидкість (прийом/передача)**	**Макс. відстань**	**Кількість телефонних пар (М)**	**Основне застосування**
1	**2**	**3**	**4**	**5**	**6**
G.960	**ISDN**	128 кбіт/с	5,5 км	1	Передача даних
G.961	**IDSL**	144 кбіт/с	5,5 км	1	Передача даних
G.991.1	**HDSL**	2048 кбіт/с	4,5 км	1	Об'єднання мереж, послуги Е1
G.991.2 Європа	**SDSL**	2320 кбіт/с	3 км	1	Об'єднання мереж, послуги Е1
G.991.2	**SHDSL**	2312 кбіт/с 4,5 Мбіт/с 9 Мбіт/с	7,5 км	1 2 4	Об'єднання мереж
G.991.2 Annex F	**SHDSL**	5696 кбіт/с 11,125 Мбіт/с 22,25 Мбіт/с	7,5 км	1 2 4	Об'єднання мереж

1	2	3	4	5	6
G.992.1	**ADSL**	6,144 Мбіт/с / 640 кбіт/с	5,5 км	1	Доступ в Інтернет, голос, відео
G.992.1 Annex H	**ADSL**	1,6 Мбіт/с/ 1,6 Мбіт/с	5,5 км	1	Доступ в Інтернет, голос, відео
G.992.1 Amend. 1	**ADSL**	24 Мбіт/с / 1,4 Мбіт/с	5,5 км	1	Доступ в Інтернет, голос, відео
G.992.2	**Splitterless ADSL**	1,536 Мбіт/с / 512 кбіт/с	3,5 км	1	Доступ в Інтернет, голос, відео
G.992.2	**UADSL**	1, 536 Мбіт/с / 384 кбіт/с	3,5 км	1	Доступ в Інтернет, голос, відео
G.992.3	**ADSL2**	16 Мбіт/с / 800 кбіт/с	5,5 км	1	Доступ в Інтернет, голос, відео
G.992.4	**Splitterless ADSL2**	1,536 Мбіт/с / 512 кбіт/с	5,5 км	1	Доступ в Інтернет, голос, відео
G.992.3	**ADSL2**	8 Мбіт/с / 800 кбіт/с	6,5 км	1	Доступ в Інтернет, голос, відео
G.992.4	**Splitterless ADSL2**	1,536 Мбіт/с / 512 кбіт/с	6,5 км	1	Доступ в Інтернет, голос, відео
G.992.5	**ADSL2+**	16 Мбіт/с / 800 кбіт/с	6,5 км	1	Доступ в Інтернет, голос, відео
G.992.5 Annex M, V	**ADSL2+**	24,432 Мбіт/с/ 3,520 Мбіт/с	6,5 км	1	Доступ в Інтернет, голос, відео
G.993.1	**VDSL**	13-52 Мбіт/с / 11– 16Мбіт/с	1,8 км – 300 м	1	Об'єднання мереж
G.993.2	**VDSL2**	50 – 200 Мбіт/с / 16 – 22 Мбіт/с	1 км – 300 м	1	Об'єднання мереж
G.993.2 Annex P	**VDSL2**	50 – 250 Мбіт/с / 16 – 50 Мбіт/с	1 км – 300 м	1	Об'єднання мереж
G.993.2 Annex Q	**VDSL2**	50 – 400 Мбіт/с / 16 – 50 Мбіт/с	1 км – 300 м	1	Об'єднання мереж

З аналізу даних табл. 1.4 для забезпечення підключення пунктів зв'язку підрозділів ДСНС до ВЦТМ з використанням проводових телефонних каналів зв'язку доцільно обирати сучасні технології xDSL з найбільшою швидкістю, яку мають СПД на основі різновидів і модифікацій технологій SDSL. ADSL, VDSL(див. рис. 1.10).

На даний час найбільш швидкісною xDSL технологією є СПД VDSL2 (див. табл. 1.4). Спочатку вважалося, що саме технологія VDSL2 в майбутньому витисне СПД ADSL, ADSL2, ADSL2+ з ринку телекомунікаційних

послуг. Однак, найбільшим недоліком VDSL2 є необхідність використовувати кабелі вищої категорії, з точно певними фізичними параметрами, особливо на найкоротших, двохсотметрових сегментах. Такі вимоги чітко підвищують загальну вартість реалізації VDSL2, і в невеликих застосуваннях її економічна значимість не висока.

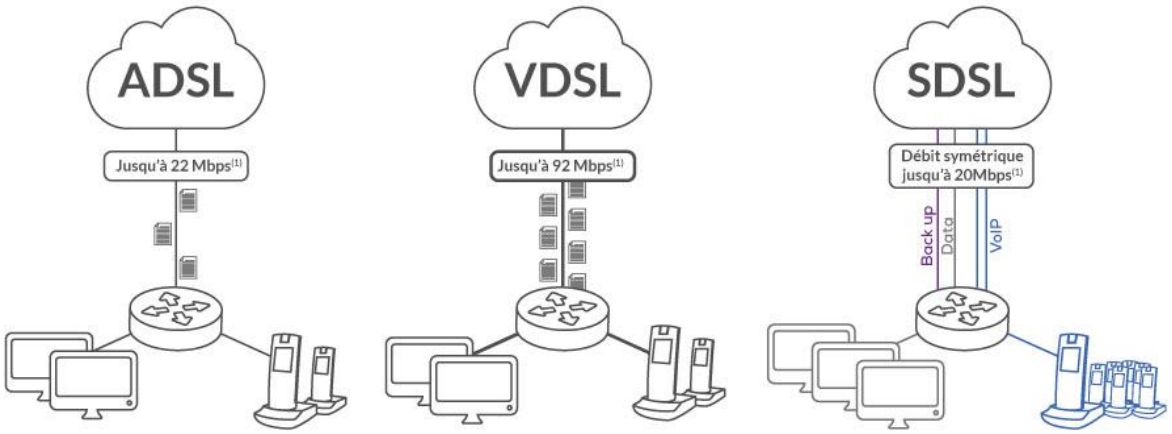


Рис. 1.10 – Відмінності SDSL, ADSL, VDSL технологій

Із цієї причини на вітчизняному ринку телекомунікаційних послуг розвиток мереж на баз СПД VDSL2 на даний час припинене на користь технології FTTX, які широко застосовується, вітчизняними операторами зв'язку, зокрема ПАТ "Укртелеком".

Технології FTTX

Згідно Директиви 2014/61/ЄС Європейського Парламенту та Ради від 15травня 2014 року про заходи, спрямовані на зменшення витрат нарозгортання високошвидкісних мереж електронного зв’язку вп.12 вказано: "Забезпечити послугами базового широкосмугового зв’язку всіх громадян Європейського Союзу до 2013 року, і забезпечення до 2020 року доступу для всіх європейців до високошвидкісного Інтернету, понад 30 Мбіт/с, а також більш ніж 50% домогосподарств Європейського Союзу доступом до Інтернету зі швидкістю, що перевищує 100 Мбіт/с."

Високошвидкісний Інтернет на даний час може бути забезпечений при використанні FTTX-технологій, основні сучасні рекомендації МСЕ-Т для якихзведені до табл. 1.5

Fiber To The X або **FTTX** (англ. *fiber to the x* – оптичне волокно до точки X) – це загальний термін для будь-якої широкосмугової телекомунікаційної мережі передачі даних, що використовує у своїй архітектурі волоконно-оптичний кабель як останню милю для забезпечення всієї або частини абонентської лінії.

Таблиця 1.5 – Сучасні рекомендації FTTX-технологій

Рекомендація МСЕ-Т	**Назва**	**Час затвердження (міс./рік)**
1	**2**	**3**
G.987	Системи пасивної оптичної мережі з підтримкою 10 гігабіт (XG-PON): визначення, скорочення та абревіатури https://www.itu.int/rec/T-REC-G.987-201206-I/en	06/2012
G.987.1	Пасивні волоконно-оптичні мережі з підтримкою 10-гігабітних швидкостей передачі (XG-PON): загальні вимоги. https://www.itu.int/rec/T-REC-G.987.1/en	03/2016 Випр. 1 03/2020
G.987.2	Пассивные волоконно-оптические сетис поддержкой 10-гигабитных скоростейпередачи (XG-PON): спецификация уровня,зависимого от физической среды (PMD) https://www.itu.int/rec/T-REC-G.987.2/en	02/2016 Попр. 1 08/2017 Попр. 2 10/2020
G.987.3	Пассивные волоконно-оптические сети с поддержкой 10-гигабитных скоростей передачи (XG-PON): спецификация уровня конвергенции передачи https://www.itu.int/rec/T-REC-G.987.3/en	01/2014 Попр. 1 03/2020 Попр. 2 05/2021
G.987.4	Пасивні оптичні мережі з підтримкою 10 гігабіт/с (XG-PON): розширення Reach https://www.itu.int/rec/T-REC-G.987.4/en	06/2012
G.988	СпецифікаціяуправлінняONU та інтерфейс контролю (OMCI) https://www.itu.int/rec/T-REC-G.988/en	11/2017 Попр. 1 11/2018 Попр. 2 08/2019 Попр. 3 03/2020
G.989	Пасивні оптичні мережі з підтримкою 40 гігабіт (NG-PON2): визначення, скорочення та абревіатури https://www.itu.int/rec/T-REC-G.989/en	10/2015
G.9804.1	Високошвидкісні пасивні оптичні мережі – Вимоги https://www.itu.int/rec/T-REC-G.9804.1/en	11/2019 Попр. 1 08/2021
G.9806	Високошвидкісна двоспрямована одноволоконна система оптичного доступу "точка-точка" (HS-PtP) https://www.itu.int/rec/T-REC-G.9806/en	06/2020 Попр. 1 10/2020 Попр. 1 05/2021
G.9807.1	Симетрична пасивна оптична мережа з з пропускною спроможністю 10 Гбіт / с (XGS-PON) https://www.itu.int/rec/T-REC-G.9807.1/en	06/2016 Пом. 1 03/2017 Попр. 1 10/2017

Рекомендація МСЕ-Т	Назва	Час затвердження (міс./рік)
1	2	3
		Випр. 1 03/2020 Попр. 2 10/2020
G.9807.2	Пасивні оптичні мережі з пропускною спроможністю 10 Гбіт / с (XG (S) -PON): Розширення охоплення https://www.itu.int/rec/T-REC-G.9807.2/en	08/2017 Попр. 1 11/2018
G.9803 (ex. G.RoF)	Радио по оптоволоконным системам https://www.itu.int/rec/T-REC-G.9803/en	11/2018 Попр. 1 08/2019
G.650.1	Визначення та методи випробування лінійних, детермінованих атрибутів одномодового волокна та кабелю https://www.itu.int/rec/T-REC-G.650.1/en	10/2020
G.651.1	Характеристики багатомодового оптичного волоконно -оптичного кабелю 50/125 мкм для оптичної мережі доступу https://www.itu.int/rec/T-REC-G.651.1/en	11/2018
G.652	Характеристики одномодового оптичного волокна та кабелю https://www.itu.int/rec/T-REC-G.652/en	11/2016
G.653	Характеристики одномодового оптичного волокна та кабелю зі зсувом на дисперсію https://www.itu.int/rec/T-REC-G.653/en	07/2010
G.654	Характеристики одномодового оптичного волокна та кабелю з відсіченням https://www.itu.int/rec/T-REC-G.654/en	03/2020
G.655	Характеристики одномодового оптичного волокна та кабелю з ненульовою дисперсією зі зсувом https://www.itu.int/rec/T-REC-G.655/en	11/2009
G.698.2	Розширені багатоканальні програми мультиплексування з щільним розподілом довжин хвиль з одноканальними оптичними інтерфейсами https://www.itu.int/rec/T-REC-G.698.2/en	11/2018
G.698.4	Багатоканальні двонаправлені додатки DWDM з незалежними від порту одноканальними оптичними інтерфейсами https://www.itu.int/rec/T-REC-G.698.4/en	03/2018 Випр. 111/2018
G.8023	Характеристики функціональних блоків обладнання, що підтримують фізичний рівень Ethernet та інтерфейси FlexE https://www.itu.int/rec/T-REC-G.8023/en	03/2018 Випр. 1 06/2018
G.9991	Високошвидкісний приймач-передавач із видимим світлом у приміщенні-Архітектура сис-	03/2019 Попр. 1

Рекомендація МСЕ-Т	Назва	Час затвердження (міс./рік)
1	2	3
	теми, фізичний рівень та рівень каналу передачі даних https://www.itu.int/rec/T-REC-G.9991/en	07/2020 Випр. 1 10/2020 Попр. 2 04/2021
G.9992	Прийомопередавач зв'язку для внутрішньої оптичної камери-Архітектура системи, фізичний рівень та рівень передачі даних. Специфікація https://www.itu.int/rec/T-REC-G.9992/en	03/2019

Термін є збірним для декількох конфігурацій розгортання оптоволокна – починаючи від FTTN (до вузла) і закінчуючи FTTD (до робочого стола).

У строгому визначенні FTTX є тільки фізичним рівнем передачі даних, однак фактично поняттям охоплюється велика кількість технологій канального й мережевого рівня. Із широкою смугою систем FTTX нерозривно зв'язана можливість надання великої кількості нових послуг. Схема, що ілюструє відмінності архітектури FTTX розміщена на рис. 1.11 .

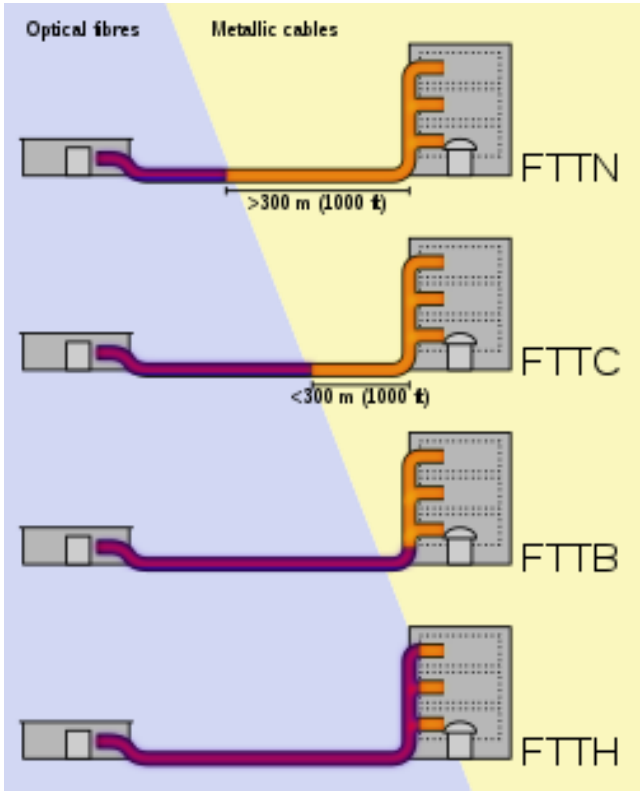


Рис. 1.11 – Різновиди архітектури FTTX

Залежно від умов використання телекомунікаційна галузь розрізняє кілька окремих конфігурацій FTTX:

- **FTTN** (Fiber to the Node) – волокно до мережевого вузла. Оптоволокно кінчається у вуличній комунікаційній шафі, можливо за 1-2 км від кінцевого споживача, з подальшою прокладкою міді – це може бути xDSL або гібридні волоконно-коаксіальні лінії. FTTN найчастіше є проміжним кроком до повного FTTB і, як правило, використовується для доставки розширеного пакета Triple Play телекомунікаційних послуг.
- **FTTC / FTTK** (Fiber to the Curb / Fiber to the kerb) – волокно до мікрорайону, кварталу або групи будинків. Варіант досить схожий на FTTN, але вулична шафа або стовп ближче до приміщень клієнта й перебуває, як правило, у межах 300 метрів – відстані для широкосмугових мідних кабелів, подібних проводовому Ethernet, або зв'язки по ЛЕП IEEE 1901, або безпроводової технології Wi-Fi. Іноді FTTC неоднозначно називають FTTP (fiber-to-the-pole, оптика до стовпа), що викликає плутанину з «Fiber to the premises system» (оптика до системи приміщень).
- **FTTDP** (Fiber To The Distribution Point) – волокно до точки розподілу. Це також схоже на FTTC / FTTN, але ще на один крок ближче. Оптоволокно кінчається в декількох метрах від границі кінцевого споживача й останнє з'єднання кабелів відбувається в розподільній коробці, називаною крапкою розподілу, що дозволяє надавати абонентам швидкість близьку до 1 Гбіт/с.
- **FTTP** (Fiber to the premises) – волокно до приміщення. Це скорочення узагальнює терміни FTTH і FTTB або використовується в тих випадках, коли оптоволокно підведене туди, де одночасно є будинку й малі підприємства.
- **FTTB** (Fiber to the Building) – волокно доходить до границі будинку, такий як фундамент багатоквартирного будинку, підвальне приміщення або технічний поверх із остаточним підключенням кожного житлового приміщення за допомогою інших способів як у конфігураціях FTTN або FTTP.
- **FTTH** (Fiber to the Home) – волокно до квартири або частки будинку. Кабель доводить до границі житлової площі, наприклад, комунікаційної коробки на стіні житла. Далі послуги оператора надаються абонентові за допомогою технології PON і PPPoE за допомогою FTTH-мереж.
- **FTTD / FTTS** (Fiber to the desktop, Fiber to the Subscriber) – оптичне з'єднання приходить в основну комп'ютерну кімнату в термінал або в медіа-конвертор біля робочого стола клієнта.
- **FTTE / FTTZ** (Fiber to the telecom enclosure, fiber to the zone) – вид кабельної системи, звичайно використовуваної в локальній мережі підприємств, коли оптичне з'єднання використовується від серверного

приміщення до робочого місця. Ці види не входять у групу технологій FTTX, незважаючи на схожість у найменуваннях.

Для забезпечення погодженості, особливо при порівнянні між країнами рівня проникнення FTTH, три ради по FTTH – Європи, Північної Америки й Азіатсько-Тихоокеанського регіону в 2006 році погодили між собою визначення FTTH і FTTB, а також уточнювали їх в 2009, 2011 року і в лютому 2015 року. Рада FTTH не встановлював формальних визначень для FTTC і FTTN.

У варіанті FTTNоптоволоконний кабель підводить до мережевого вузла й у зв'язку із цим іноді можуть плутати з підключенням FTTC, коли оптика доводить до вуличної розподільної шафи або стовпа, що несе кабель, з подальшим розведенням по мікрорайону або прилеглих будинках. До кінцевих споживачів, як правило, далі від такої шафи йдуть окремі підключення по коаксіальному кабелю або витої парі. Територія, що обслуговується з однієї вуличної розподільної шафи, звичайно перебуває в радіусі менш 1,5 км і може містити в собі кілька сотень абонентів телекомунікаційних послуг. Якщо від розподільної шафи обслуговується територія з радіусом менш 300 метрів, то таке підключення буде ставитися до FTTC/FTTK.

FTTN дозволяє надавати широкосмугові послуги зв'язку, такі як високошвидкісний доступ в інтернет. На ділянці від кінця оптоволокна до споживача послуг використовуються високошвидкісні протоколи передачі даних подібні тим, що застосовуються при роботі із широкосмугових кабелів зв'язку (звичайно DOCSIS) або деякі види xDSL. Швидкість передачі даних варіюється залежно від використовуваного протоколу й від того, наскільки близько абонент від розподільної шафи.

На відміну від FTTP, в інфраструктурі FTTN найчастіше для забезпечення останньої милі використовується коаксіальний кабель або виті пари, що робить такий варіант менш дорогим для розгортання. Однак, у довгостроковій перспективі потенційна пропускна спроможність при цьому варіанті буде сильно обмежена щодо варіанта із закінченням оптоволокна ближче до абонента.

Технічним різновидом цього варіанта є гібридна оптико-коаксіальна система зв'язку, використовувана операторами кабельного телебачення. Таке підключення ще іноді називають абревіатурою FTTLA (Fiber to the last amplifier, оптика до останнього підсилювача), при заміні таким підключенням останнього підсилювача перед абонентом (або групою абонентів).

Волокно до мікрорайону, кварталу або групи будинків є системою зв'язку, суть якої полягає в запуску платформи на основі оптоволоконних ліній зв'язку, що обслуговує декількох абонентів. Кожний із цих абонентів з'єднаний із платформою коаксіальним кабелем або витою парою. Це може бути встановлюване виносний пристрій або комунікаційна ша-

фа, або ж навіс. Звичайно системи зв'язку, у яких оптоволокно кінчається менш чім за 300 м від установлюваної в приміщенні користувача апаратури, відносять до варіанта **FTTC**.

У цьому варіанті від закінчення волокна до абонента також як і в FTTN використовується DOCSIS або xDSL.

Коли можливо, при прокладці нового кабелю проводять відразу оптичний і мідний Ethernet кабелі. Останній з'єднує районний вузол зв'язку з абонентом на швидкостях 100 Мбіт/с або 1 Гбіт/с.

Розгортання зв'язку по ЛЕП також відносять до FTTC. Використання протоколу IEEE 1901 (або його попередника – Homeplug AV) дозволяє по існуючих електромережах на швидкості до 1 Гбіт/з передавати дані від виносної районної комутаційної шафи до будь-якої розетки змінного струму в будинку – покриття мережею рівноцінно Wi-Fi з додатковою перевагою у вигляді одного кабелю для електроживлення й передачі даних.

Основною відмінністю FTTC від FTTN або FTTP буде місце розміщення комутаційної шафи (рис. 1.12).

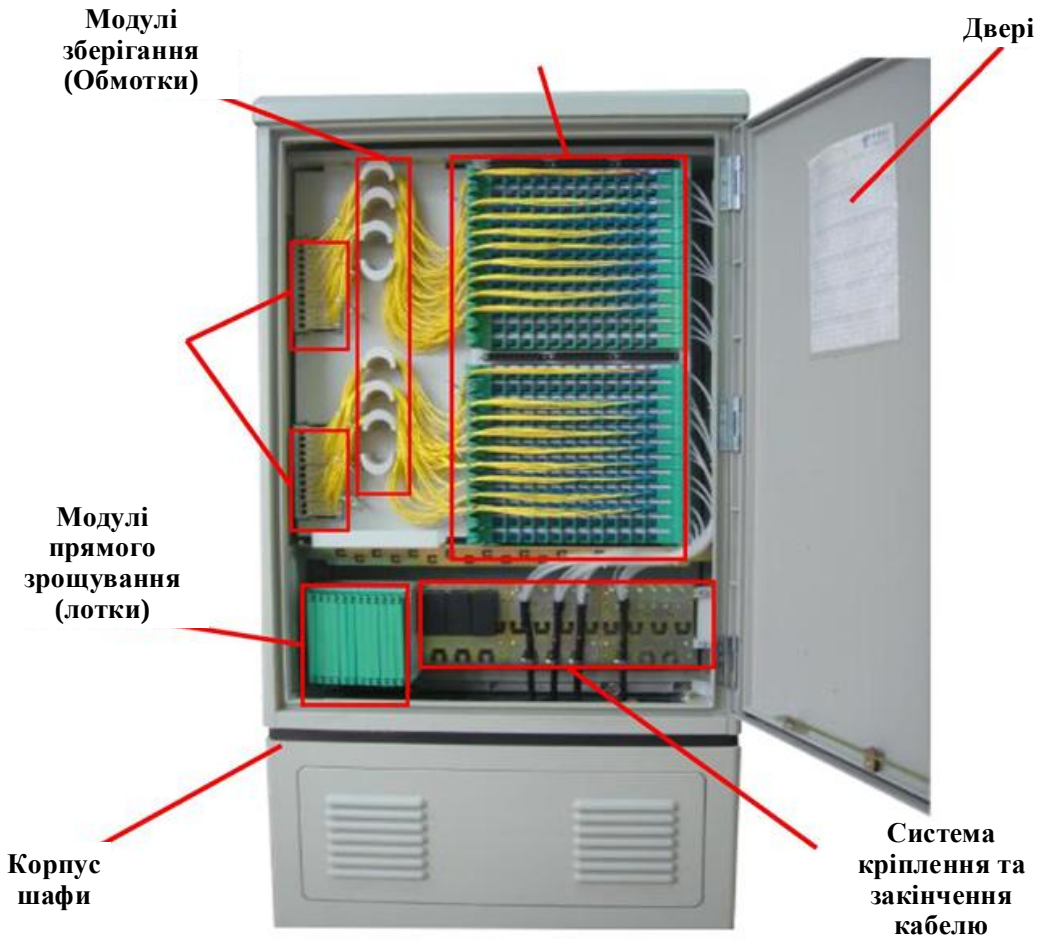


Рис. 1.12 – Зовнішня оптична шафа для перехресного з'єднання

У варіанті підключення FTTC комутація йде, наприклад, від несучого кабельного стовпа на узбіччі дороги в будинку клієнта, тоді як при FTTN комутаційна шафа вдалині від абонента, а при варіанті FTTP комутація безпосередньо в зоні обслуговування клієнтів (рис. 1.13 а, б).



а)



б)

Рис. 1.13:

а) внутрішності оптичної комутаційної шафи. Ліворуч підключений оптоволоконний кабель, а праворуч – мідь для xDSL; б) FTTC під час установки в Німеччині

На відміну від FTTP, у варіанті FTTC для створення останньої милі можуть використовуватися наявні коаксіальні кабелі, вита пара або зв'язок по ЛЕП. Спробою об'єднати такі існуючі кабелі під єдиним керуючим протоколом стали розробки стандартів G.hn і IEEE P1905.

Ідучи від прокладки нового кабелі й пов'язаних із цим витрат, вартість розгортання FTTC менше. Проте цей варіант мережі історично має більш низький потенціал смуги пропускання, чім FTTP. На практиці, відносна перевага використання оптоволокна залежить від смуги пропускання, доступної для транспортної мережі зв'язку, від біллінгових обмежень, що запобігають повне завантаження пропускної здатності останньої милі, від абонентського обладнання, від обмежень обслуговування й вартості експлуатації оптоволокна. Усі ці параметри можуть широко варіюватися виходячи з географічного положення й типу будови.

FTTB (fiber to the building) – оптичне волокно до будинку. У цій архітектурі волокно доходить до комутаційного обладнання оператора, розташовуваного переважно на границі території, що включає в себе вдома або підприємства. З обладнанням установлюється єдиний термінал, а від нього до приміщення або проводять мідний кабель, або використовують безпроводове з'єднання, – у самому приміщенні в основному перебуває тільки один кабель, який підключається до комп'ютера. Архітектура FTTB

одержала найбільше поширення, тому що при будівництві мереж FTTX на базі Ethernet, найчастіше, це єдина технічно можлива схема. Крім того, у структурі витрат на створення мережі FTTX різниця між варіантами FTTC і FTTB відносно невелика, при цьому операційні витрати на експлуатацію мережі FTTB нижче, а пропускна спроможність вище. Архітектура FTTB переважає в знову зводимих будинках і у великих операторів зв'язку, тоді як FTTH буде затребувана тільки в новому малоповерховому будівництві. У першу чергу це пов'язане із суттєво більш високою вартістю її реалізації в порівнянні з вартістю мережі FTTC/FTTB.

FTTH (fiber to the home) – оптичне волокно до житла. У житлі встановлюється термінал, а від термінала кабель до комп'ютера. Дане визначення виключає ті архітектури мережі, у яких оптичне волокно закінчується до досягнення житлових приміщень або офісного простору й лінія триває іншим фізичним середовищем, ніж оптичної.

Однозначно на користь розгортання FTTH виступали експерти компанії Motorola. Вони порівнюють тривалість життєвого циклу інвестицій у будь-яку технологію доступу й прогнозують ріст вимог до пропускної здатності каналів доступу. Проведений аналіз показує, що якщо технічні рішення, які закладаються в основу сегмента доступу мережі в 2015–2018 роках, виявляться нездатними забезпечити швидкість 100 Мбіт/с в 2023–2025 годах, оскільки моральне старіння обладнання відбудеться до закінчення інвестиційного циклу. Оператор повинен обов'язково враховувати ці дані, інакше він ризикує виявитися вразливим перед особою конкурентів у міру прагнення користувачів до одержання послуг усе більш високого класу.

Експерти компанії Alcatel-Lucent перераховують наступні переваги архітектури FTTH:

- із усіх варіантів FTTX вона забезпечує найбільшу смугу пропускання;
- це повністю стандартизований і найбільш перспективний варіант;
- рішення FTTH забезпечують масове обслуговування абонентів на відстані до 20 км від вузла зв'язку;
- вони дозволяють суттєво скоротити експлуатаційні витрати – за рахунок зменшення площі технічних приміщень (необхідних для розміщення обладнання), зниження енергоспоживання й властиво витрат на технічну підтримку.

Апаратна архітектура й типи підключень FTTH представлені на рис. 1.14.

Порівняння, що показує, як типовий AON (зіркоподібна мережа з можливістю багатоадресної передачі) обробляє спадний трафік інакше, чім типова PON (зіркоподібна мережа, що має трохи спліттерів, розміщених в одній шафі (рис. 1.12.)

Найпростішою архітектурою оптичної мережі є пряме волокно. При такому способі кожне волокно в кабелі від приміщень оператора зв'язку йде до одному клієнту. Подібні мережі можуть забезпечити чудову швидкість передачі даних, але вони суттєво дорожче через нераціональне використання волокон і обладнання, що обслуговує лінію зв'язку.

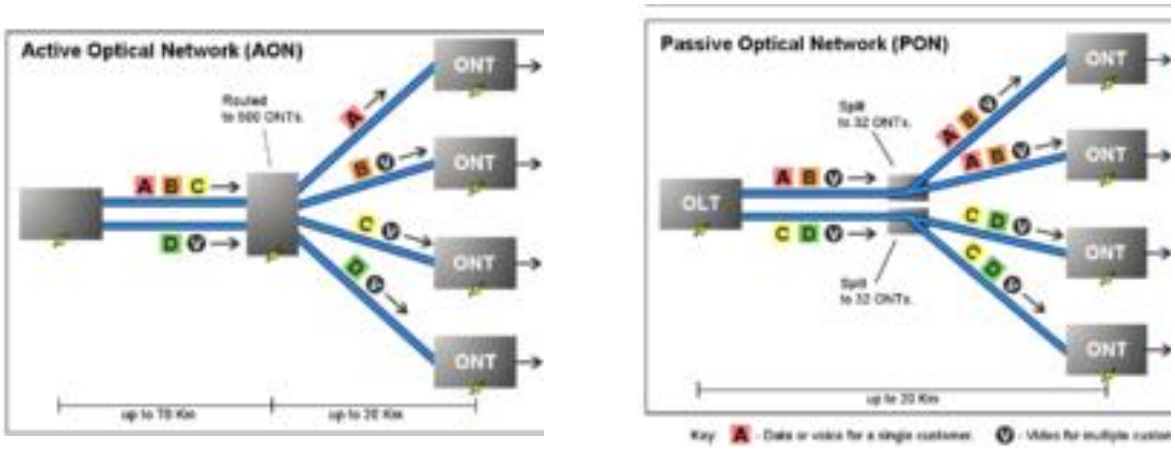


Рис. 1.14 – Типи підключень FTTH:

а) активна оптична мережа (AON) б) пасивна оптична мережа (PON)

Прямі волокна, як правило, надаються великим корпоративним клієнтам або державним структурам. Перевагою є можливість використання 2-го рівня мережевих технологій незалежно від того, будь те активна, пасивна або гібридна оптична мережа.

В інших випадках (масових підключеннях абонентів) кожне волокно, що йде від оператора зв'язку, обслуговує безліч клієнтів. Воно зветься «загальне волокно» (англ. *Shared fiber*). При цьому оптика доводить максимально близько до клієнта, після чого воно з'єднується з індивідуальним волокном, що йде до кінцевого споживача. У такому з'єднанні застосовуються як активні, так і пасивні оптичні мережі.

Залежно від способу побудови оптичні мережі діляться на:

- активні оптичні мережі – із працюючим активним мережевим обладнанням для посилення й передачі сигналу;
- пасивні оптичні мережі – з розгалужувачами оптичних сигналів;
- гібридні оптичні мережі –, що використовують активні й пасивні компоненти одночасно.

Активна оптична мережа (AON) заснована на передачі оптичного сигналу мережевим електрообладнанням, що приймає, підсилює і передає ці сигнали. Це може бути комутатор, маршрутизатор, медіаконвертер – як правило, оптичні сигнали в активній оптичній мережі перетворяться в електричні й назад. Кожний оптичний сигнал від централізованого

обладнання оператора зв'язку йде тільки до того кінцевого користувача, для якого він призначений.

Вхідні з боку абонентів сигнали уникають колізій у єдиному волокні, тому що електрообладнання забезпечує буферізацію. У якості першої милі від обладнання оператора зв'язку використовується обладнання активний ETTH, що включає в себе оптичні мережні комутатори з оптикою, що й служить для передачі сигналу до абонентів.

Подібні мережі ідентичні комп'ютерним Ethernet мережам, використовуваним в офісах і освітніх установах з тим лише виключенням, що вони призначені для підключення будинків і будівель до центрального будинку оператора зв'язку, а не для підключення комп'ютерів і принтерів в обмеженому просторі. Кожна розподільча шафа може обслуговувати до 1000 абонентів, хоча звичайно обмежуються підключенням 400-500 клієнтів.

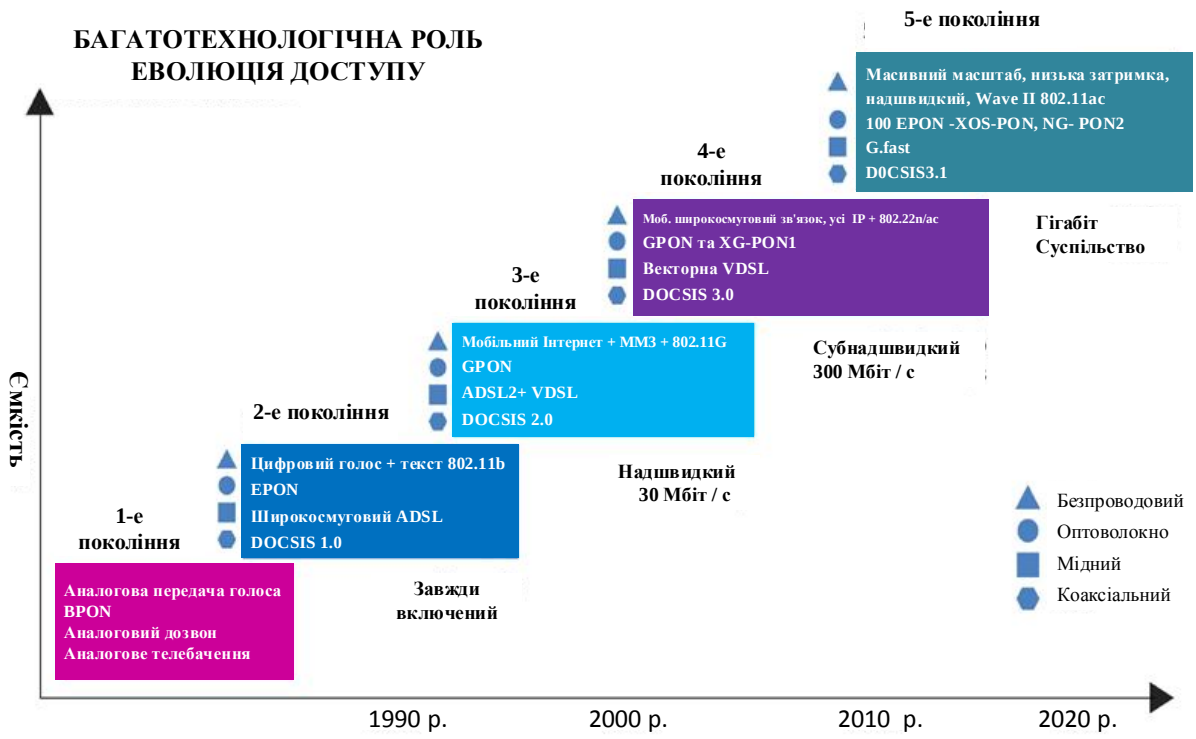
Таке вузлове обладнання забезпечує комутацію другого й третього рівнів, а також маршрутизацію, розвантажуючи тим самим магістральний маршрутизатор оператора зв'язку й забезпечуючи передачу даних у його серверне приміщення. Стандарт IEEE 802.3ah дозволяє провайдерам послуг інтернету надавати швидкості до 100 Мбіт/с і повним дуплексом по одномодовому оптоволоконному кабелю (англ. *Single-mode optical fiber*), підключеному за схемою FTTH. Комерційно доступними також стають швидкості в 1 Гбіт/с.

Пасивна оптична мережа(PON) – це архітектура мережі FTTP з підключенням за принципом точка-багатоточка на основі енергонезалежних оптичних розгалужувачів (спліттерів), що дозволяють по одному оптичному волокну обслуговувати до 128 абонентів. У порівнянні з підключенням по прямому волокну, PON зменшує вимоги до оптичного кабелю й обслуговуючому його обладнанню провайдера. Спадний по волокну сигнал транслюється від обладнання оператора зв'язку до всіх абонентів, що спільно використовують лінію зв'язку. Для запобігання перехоплення трафіка використовується шифрування. Висхідні сигнали від абонентів поєднуються в один потік із застосуванням протоколу множинного доступу, як правило, із часовим розподілом доступу.

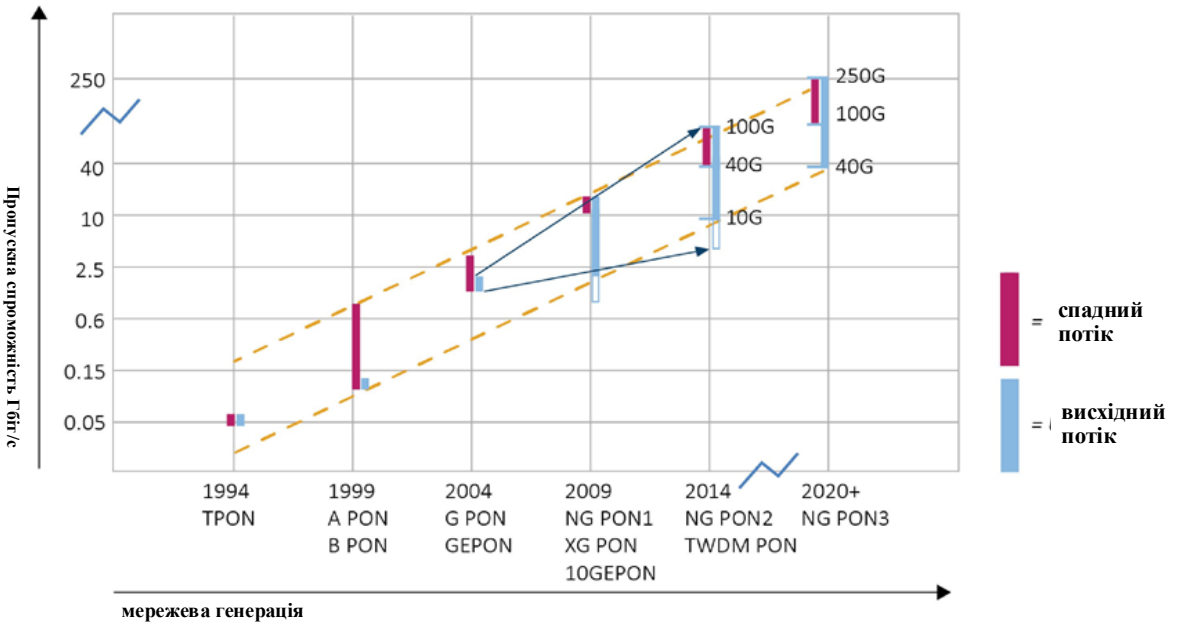
Електрообладнання може бути презентовано, як медіа-конвертер, так і оптичний мережевий термінал (ONT, термін ITU-T) або оптичний мережевий модуль (ONU, аналогічний термін IEEE), що перетворять оптичний сигнал в електричний, з використанням технології тонкоплівкового фільтра. Ці пристрої для своєї роботи вимагають наявності електроенергії, тому їх намагаються підключати до резервних джерел живлення для забезпечення безперебійної роботи в екстрених випадках і при перебоях з подачею електроенергії.

Для варіанта FTTH і деяких видів FTTB загальним для всіх будинків, що підключаються, є забезпечення телефонізації, LAN і систем кабельно-

го телебачення, які підключаються до оптичного мережевого термінала або модуля. Усі ці три системи передачі даних не можуть прямо підключатися до оптичного модуля, але можливо об'єднати їхні сигнали й передавати в єдиному середовищі. Залежно від того, що ближче до користувача, – маршрутизатор, модем або мережева плата, – той пристрій може розділити сигнал і перетворити його до підходящого протоколу.



а)



б)

Рис. 1.15 – Пропускна спроможність і швидкість трафіку для PON

Наприклад, при використанні технології VDSL, комбінований сигнал передається в будинок по існуючому проводовому з'єднанню й входить у житлове приміщення, де VDSL-модем перетворить дані й відеосигнал (послуги телебачення) до протоколу Ethernet, який доставляється до прикінцевого обладнання по витої парі. Далі модуль мережевого інтерфейсу перетворить відеосигнал у радіочастотний, переданий прикінцевому обладнанню по коаксіальному кабелю. Комбінований сигнал також може доходити до телефонного апарата, підключеного через ADSL–сплітер для відділення голосового сигналу від інших, або ж до IP-телефону, який може включатися в локальну мережу.

На даний час СПД на основі оптоволокна працюють зі швидкістю 40 Гбіт/с і більше. Відповідно оцінкам фахівців найближчім часом для передавання трьохмірних відображень буде необхідна швидкість трильйони біт в секунду, тобто збільшиться в 250 разів. Динаміка росту пропускної спроможності і швидкості трафіку для PON наведена на рис. 1.15 а), б)[14].

Прогноз динаміки підключення домів до FTTH / B в Європі наданий на рис. 1.16.

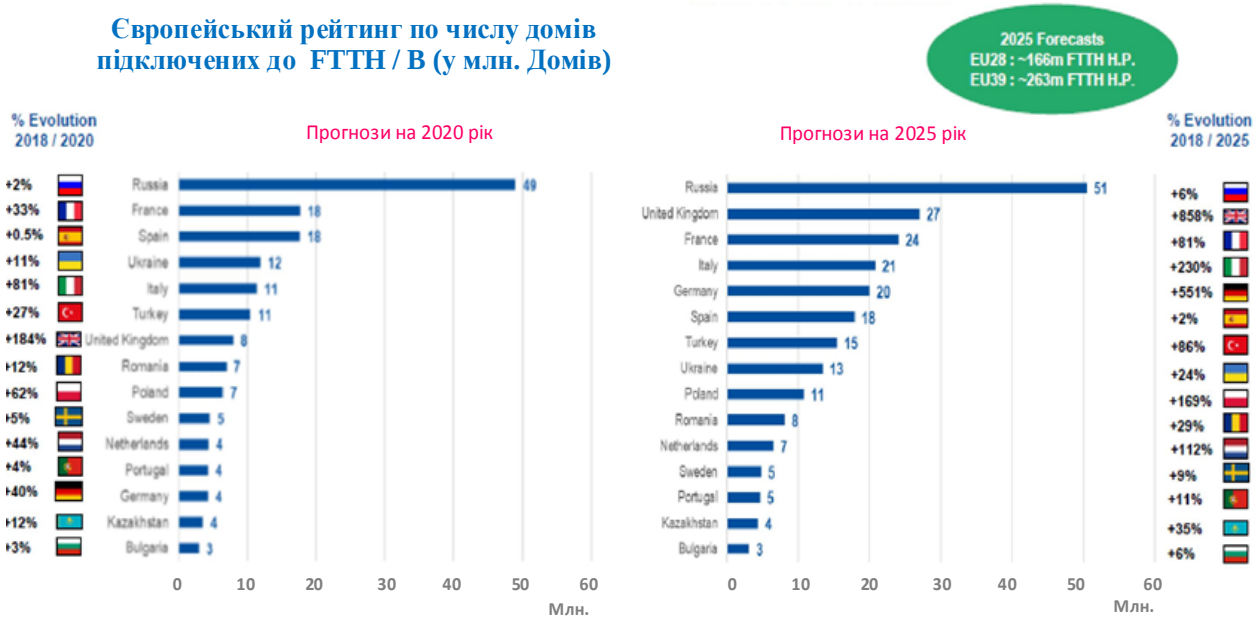


Рис. 1.16 – Топ 15 країн по кількості домів обладнаних FTTH / B, за прогнозами у 2020 та 2025 роках

Архітектура та технологічні тенденції розвитку FTTH / B представлені на діаграмі рис. 1.17

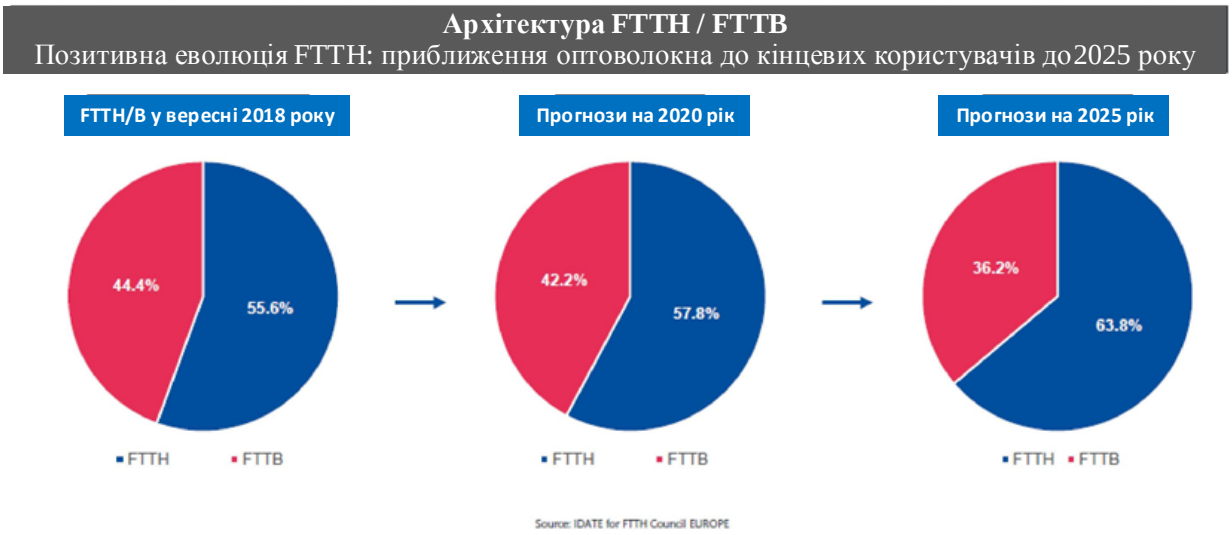


Рис.1.17 – Архітектура та технологічні тенденції FTTH

1.3.2.4 Система інтегрованих послуг

Вся технічна інфраструктура ВЦТМ ДСНС має за мету забезпечити надання сучасних телекомунікаційних та інформаційних послуг користувачам мережі. Ці послуги повинні розглядатись як інтегровані по відношенню до користувачів (тобто кожний з них у відповідності до наданих прав може мати доступ до любої з послуг), так і до каналів зв'язку, каналоутворюючого та комутаційного обладнання, через які вони реалізуються (тобто технічна база ВЦТМ повинна бути максимально уніфікована для обробки любих видів трафіку – мови, даних, відео тощо).

Інтегровані послуги ВЦТМ ДСНС передбачають:

– забезпечення телефонних переговорів з підтримкою послуг ISDN та реалізацією додаткових видів обслуговування ДВО як засобами традиційної телефонії, так і IP-телефонії (VoIP – мова поверх IP);

– обробку даних;

– передачу відеоінформації;

– доступ до інформаційних та довідкових баз даних;

– надання послуг обробки та зберігання абонентських голосових, електронних та факсимільних повідомлень;

– надання послуг телефонного зв'язку з обмеженою мобільністю;

– проведення селекторних нарад (конференц-зв'язку) в аудіо– або відео режимах;

– реалізацію операторських центрів диспетчерських служб ДСНС зі службою аварійного телефонного виклику «101» (112) на базі технологій Call Center і інтерактивного голосового супроводження виклику (Interactive Voice Response, IVR);

– юридичне документування шляхом звукозапису телефонних переговорів операторських центрів з абонентами служби «101» (112) та пі-

длеглими підрозділами.

Найбільш важливою для забезпечення службової діяльності ДСНС є реалізація операторських центрів диспетчерських служб. Вони повинні забезпечувати:

– ідентифікацію абонентів вхідних викликів по лініям «101» (112) через вузол спецзв'язку з автоматичним визначенням телефонного номеру;

– автоматичне розподілення виклику (ACD) з урахуванням категорійності абонентів (їх важливості), активованих на цей час робочих місць операторів, встановленим порядком розподілення викликів між ними (по зонам їх відповідальності – районам міста, важливості об’єктів тощо), практичним досвідом або навантаженням;

– при зайнятості усіх операторів формування черги обслуговування у відповідності до визначених категорій обслуговування. При застосуванні системи IVR інформування абонентів про зайнятість операторів, місця в черзі на обслуговування, які відомості по аварійному виклику необхідно буде надати оператору після з’єднання з ним або забезпечувати першочергове або позачергове з’єднання з операторами;

– видачу оператору з відповідної бази даних диспетчерської служби в екранній формі на ПЕОМ відомостей про абонента (об’єкта), що викликає, відомостей про кількість абонентів в черзі;

– ведення документування телефонних переговорів оператора з абонентом шляхом звукозапису;

– взаємодію з базами даних диспетчерської служби щодо відпрацювання встановлених документів на застосування сил та засобів;

– обслуговування вихідних викликів в формі голосових, факсимільних або електронних повідомлень (заздалегідь або оперативно підготовлених);

– підготовку та передачу необхідних розпорядчих документів у підлеглі підрозділи ДСНС у любому із перерахованих видів;

– реалізацію системи автоматизованого централізованого оповіщення особового складу та підлеглих підрозділів по всім діючим каналам зв’язку (телефонам міської телефонної мережі, міжміському зв’язку, каналам ЦТМ ДСНС тощо) у відповідності до визначених сигналів та категорій оповіщення в формі голосових, факсимільних або електронних повідомлень (заздалегідь або оперативно підготовлених), документування підтвердження про отримання таких сигналів абонентами. Для цього IVR через систему розпізнання мови дозволяє телефонним абонентам в голосовому режимі давати підтвердження про отримання сигналу оповіщення шляхом промови визначених слів, що є доцільним за умов неможливості використання багаточастотного режиму набору номеру DTMF;

– ведення в режимі реального часу збору та накопичування статистичної інформації щодо обслуговування викликів та реакції на них (передачу відповідних розпоряджень в частини ДСНС тощо), результатів проведення централізованого оповіщення, доведення розпоряджень тощо, зберігання такої інформації та видачу аналітичних довідок за відповідні періоди, по операторам, змінам та інших за вимогою;

– реалізацію за необхідності територіально-розподіленого операторського центру, в якому вхідні виклики можуть автоматично переадресовуватись на відповідні територіальні підрозділи ДСНС;

– створення автоматичної інформаційно-довідкової служби ДСНС, яка з використанням функцій IVR без залучення операторів може надавати довідки або переадресовувати вхідні виклики на відповідні служби ДСНС, які компетентні для надання тих чи інших довідок або інформації. IVR повинна використовувати систему розпізнання мови, що дозволить абонентам взаємодіяти з інформаційно-довідковою службою шляхом промови визначених слів або фраз, що є доцільним за умов неможливості використання багато частотного режиму набору номеру DTMF.

1.4 Порядок організації роботи ВЦТМ ДСНС

ВЦТМ складається з центральних вузлів (основний і резервний), окремих вузлів 1-го і 2-го рівнів [5, 12].

Центральний вузол ВЦТМ розміщено в адміністративній будівлі ДСНС. Резервний центральний вузол ВЦТМ розміщено в будівлі, яка належить до сфери відповідальності Центру зв'язку та управління ДСНС України.

На резервному центральному вузлу ВЦТМ здійснюється резервування сервісів ВЦТМ і створено резервний центр обробки даних.

Територіальні органи, підрозділи центрального підпорядкування, заклади освіти, підприємства, організації та установи, які безпосередньо підпорядковуються ДСНС, виступають окремими вузлами ВЦТМ 1-го рівня (далі – окремі вузли ВЦТМ) і мають власну IP-адресацію згідно із додатком 1 до цього Порядку. Фіксована IP-адресація поширюється на підрозділи ДСНС, розташовані в населених пунктах будь-якого типу та їх районах. Підрозділи ДСНС, які не підпорядковуються безпосередньо апарату ДСНС, виступають окремими вузлами 2-го рівня.

Окремі вузли 2-го рівня підключаються до ВЦТМ через окремі вузли ВЦТМ.

Використання технології трансляції мережних адрес в маршрутизаторах (NAT, Network Address Translation) для підключення мережевих пристроїв підрозділів безпосереднього підпорядкування ДСНС до ВЦТМ заборонено.

ВЦТМ поєднує як самостійні підмережі територіальних органів, під-

розділів центрального підпорядкування, закладів освіти, підприємств, організацій та установ сфери управління ДСНС із центральними вузлами ВЦТМ, так і може надавати можливість здійснювати обмін даними між окремими вузлами ВЦТМ без залучення обладнання центральних вузлів ВЦТМ.

Канали зв'язку між вузлами ВЦТМ будуються на базі:

каналів зв'язку ДСНС;

каналів зв'язку операторів (провайдерів) телекомунікацій, що надають послуги з доступу до мережі Інтернет та мають чинні атестати відповідності системи захисту інформації захищених вузлів доступу, видані Державною службою спеціального зв'язку та захисту інформації України;

державних каналів зв'язку спеціального призначення – національна телекомунікаційна мережа, телекомунікаційна мережа спеціального призначення тощо.

Доступ до ВЦТМ підрозділів, які підпорядковані територіальним органам ДСНС, здійснюється через територіальні органи ДСНС.

Схему організації ВЦТМ наведено на рис. 1.18 .

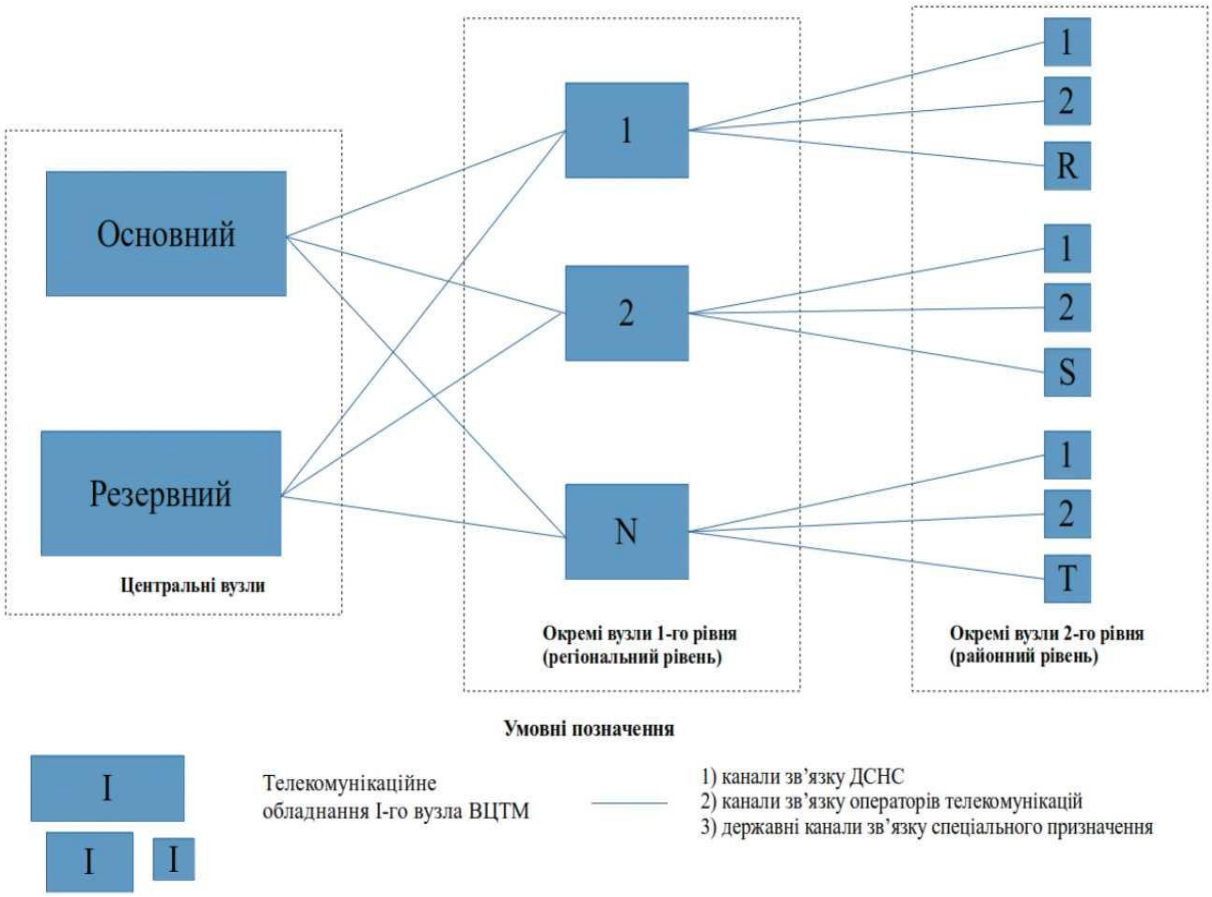


Рис.1.18 – Схема організації ВЦТМ

Топологію мережі центральних вузлів ВЦТМ наведено у рис. 1.19.

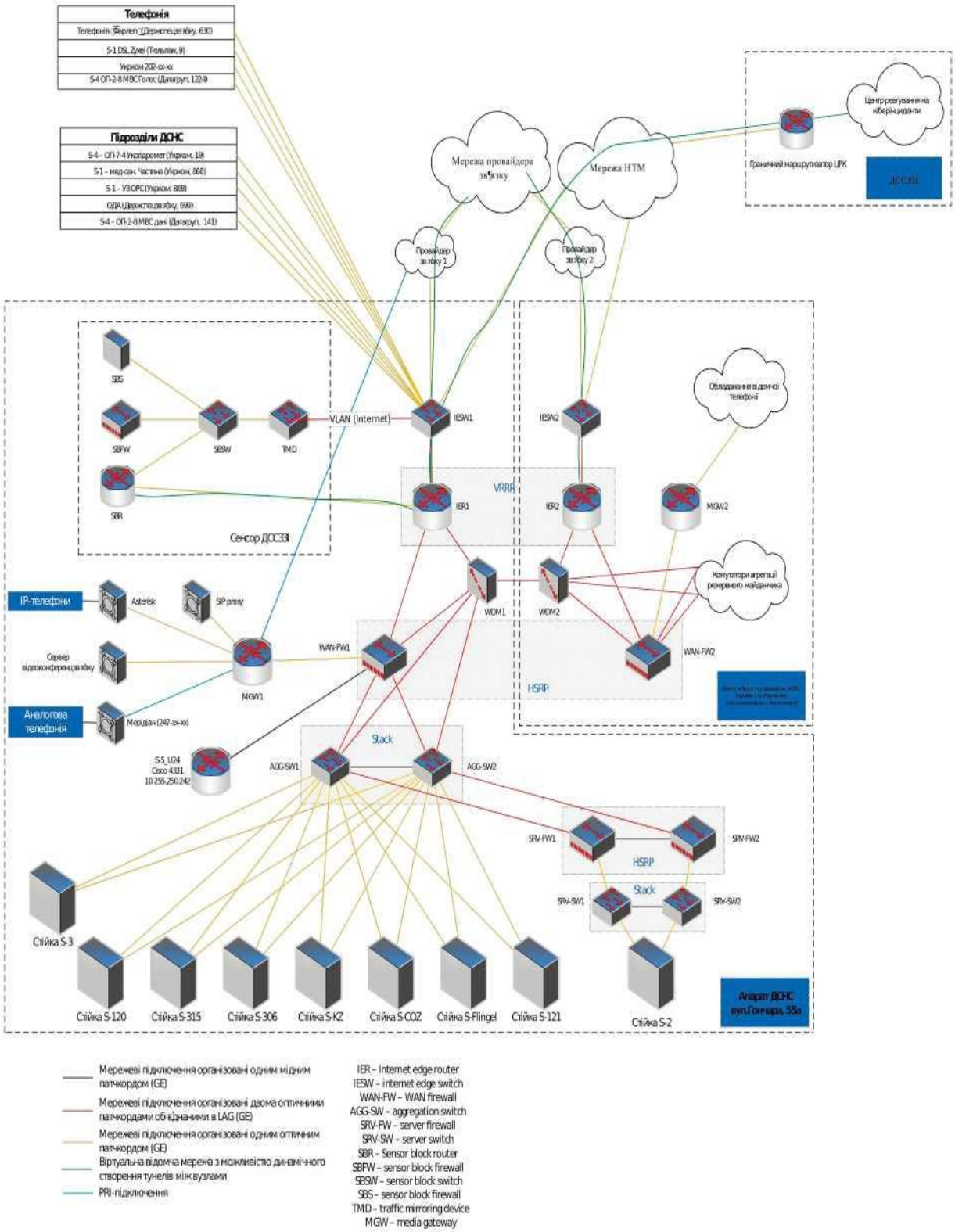


Рис. 1.19 – Топологія мережі центральних вузлів ВЦТМ

Схеми підключення окремих вузлів ВЦТМ до мережі Інтернет та центральних вузлів ВЦТМ погоджуються з апаратом ДСНС. Типову схему наведено на рис. 1.20.

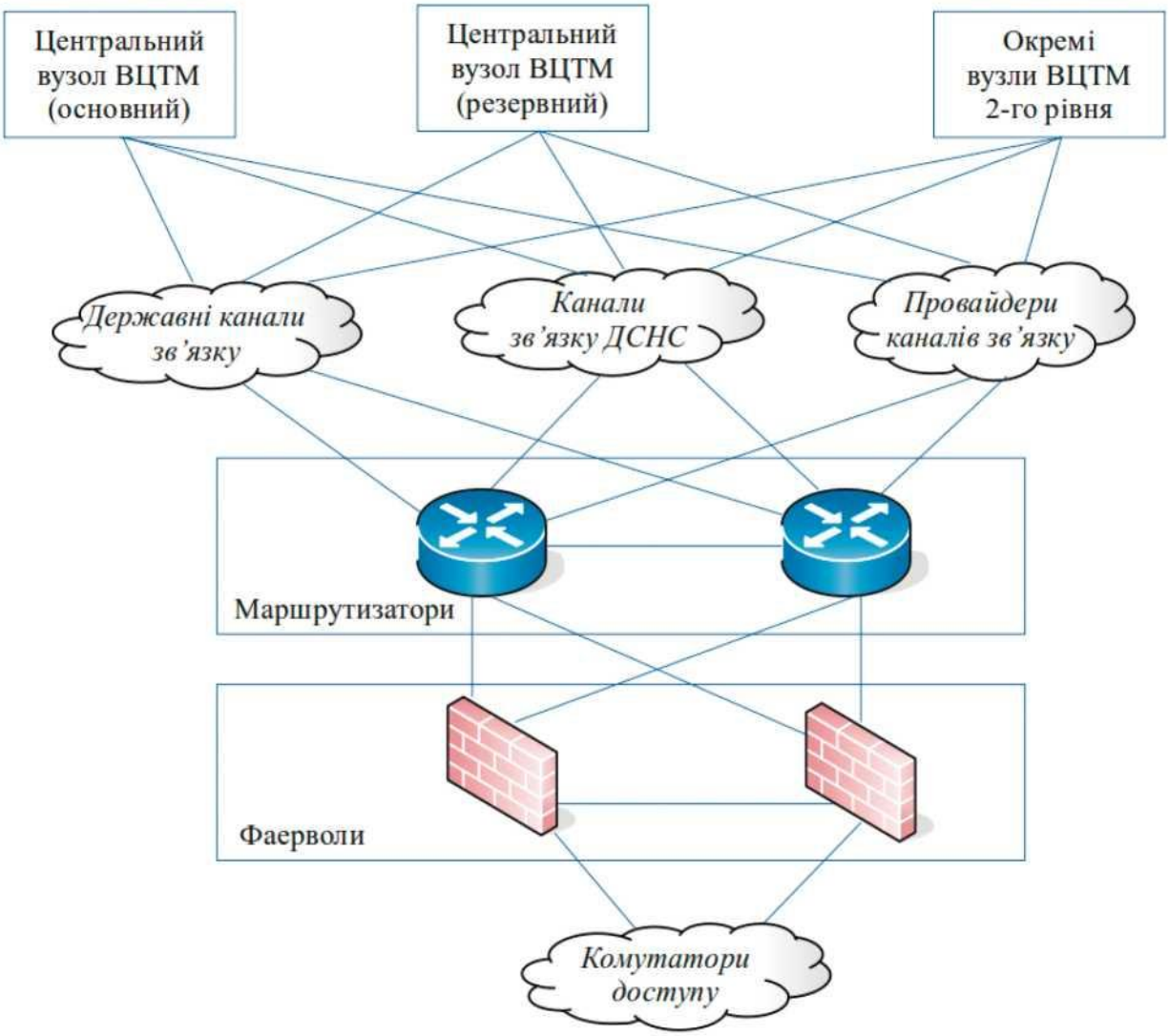


Рис. 1.20 – Схема підключення окремих вузлів ВЦТМ

Модернізацію, вибір обладнання вузлів ВЦТМ необхідно здійснювати за погодженням з апаратом ДСНС.

1.4.1 Використання відомчої VPN

Окремим способом підключення до ВЦТМ виступає під'єднання через відомчий сервер для організації віртуальної приватної мережі (VPN, Virtual Private Netwrok).

VPN виступає складовою ВЦТМ.

Всі абоненти відомчої VPN мають бути ідентифіковані та отримувати фіксовані IP адреси.

Абонентам відомчої VPN надається обмежений доступ до сервісів ВЦТМ (відповідно до визначених потреб).

Заявки на отримання доступу до ВЦТМ через відомчу VPN оформлюються згідно з встановленою формою, та надсилаються адміністратору ВЦТМ.

Відповідно до наданої заявки адміністратором ВЦТМ створюється облікові записи VPN доступу до ВЦТМ з терміном дії на 1 рік. Для продовження дії облікового запису VPN доступу до ВЦТМ необхідно подати повторну заявку у першій декаді останнього місяця дії облікового запису VPN доступу до ВЦТМ. У разі неподання повторної заявки термін дії облікового запису VPN доступу до ВЦТМ по закінченню терміну 1 рік припиняється.

Кількість облікових записів для одного структурного підрозділу обмежена з урахуванням обґрунтованої службової необхідності.

Кінцевим обладнанням для термінації відомчих VPN виступає фаєрвол центрального вузла ДСНС, що поєднує в собі функцію VPN-концентратора та надає обмежений доступ до сервісів ВЦТМ (відповідно до визначених потреб).

1.4.2 Сфери відповідальності за роботу ВЦТМ

1. Налаштуванням мережевого обладнання вузлів відомчої телекомунікаційної мережі в апараті ДСНС та граничних маршрутизаторів та фаєрволів у підпорядкованих підрозділах займаються адміністратори центральних вузлів ВЦТМ.
2. У підпорядкованих підрозділах ДСНС адміністратори підмереж ВЦТМ визначаються власними наказами.
3. Розробленням та супроводом робочої документації ВЦТМ, впровадженням засобів захисту обладнання займається адміністратор відповідної підмережі ВЦТМ.
4. До основної документації на підмережі ВЦТМ відноситься:

наказ про визначення адміністраторів;

схема мережі рівня L1 з позначенням усіх комутаторів, фізичних серверів (файлових сховищ) та місць під'єднання всіх провайдерів, що надають телекомунікаційні послуги (рис.1.21);

схема побудови телекомунікаційної мережі із підпорядкованими підрозділами ДСНС (із зазначенням моделей комутаторів, маршрутизаторів, провайдерів телекомунікаційних послуг та гарантованої швидкості каналів) (рис. 1.22);

схема розташування мережевого обладнання (комутатори, маршрутизатори, модеми, сервери, мережеві принтери, WiFi-точки доступу) і розеток локальної мережі ДСНС та інших організацій по кабінетах на планах поверхів адміністративної будівлі з позначенням розмірів будівлі. У схемі мають бути позначені номери всіх кабінетів та мережевих розеток (рис. 1.23);

таблиця комутації мережевих пристроїв із зазначенням призначення всіх портів комутаторів та маршрутизаторів додаток 9 (1);

схеми організації електроживлення серверного приміщення (рис. 1.24);

план поділу підмережі на VLAN додаток 11 (1);

перелік санкційованих мережевих пристроїв із зазначенням MAC-адрес;

журнал обліку доступу технічних співробітників до серверних приміщень.

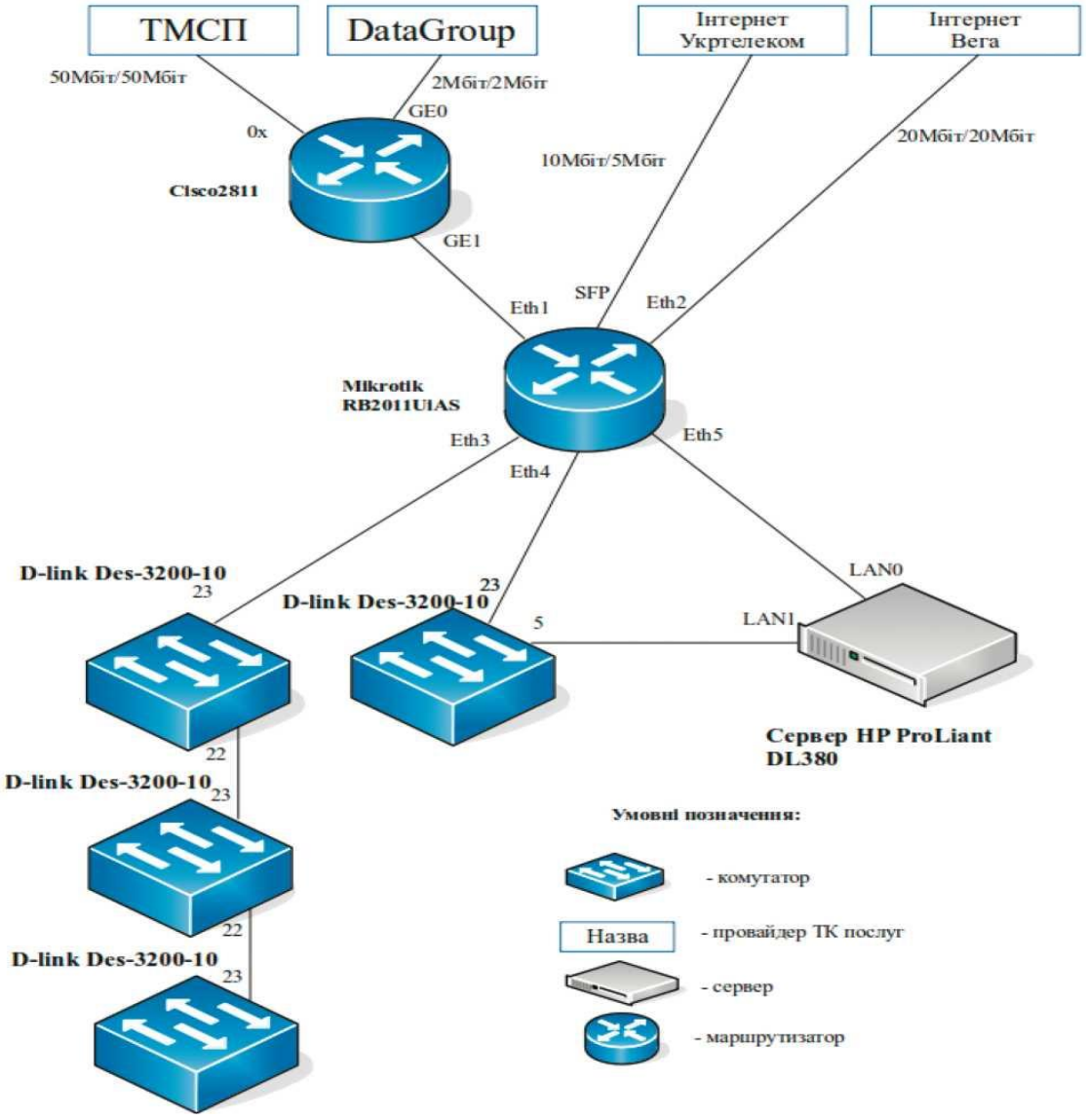


Рис. 1.21 – Приклад оформлення схеми рівня L1

5. Розмежування рівнів доступу адміністраторів мережевого обладнання здійснюється таким чином:

надання адміністраторам центрального вузла ДСНС повного доступу до мережевого обладнання у центральному вузлу ДСНС та в регіональних підрозділах для можливості моніторингу мережі та своєчасного виявлення ризиків;

надання адміністраторам регіональних підрозділів ДСНС обмеженого рівня доступу до мережевого обладнання відповідних окремих вузлів ВЦТМ, еквівалентного рівню базової конфігурації обладнання.

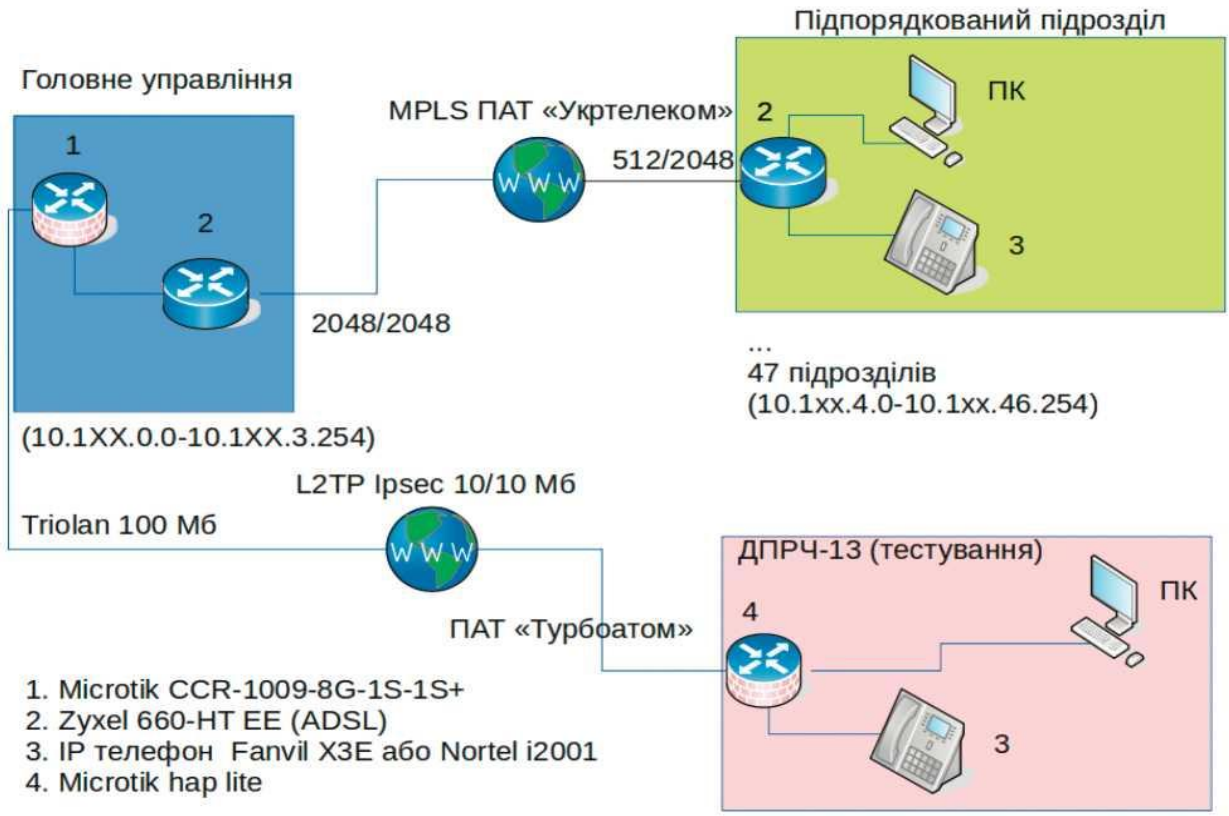


Рис. 1.22 – Приклад оформлення схеми організації мережі між окремими вузлами ВЦТМ та їх підпорядкованими підрозділами

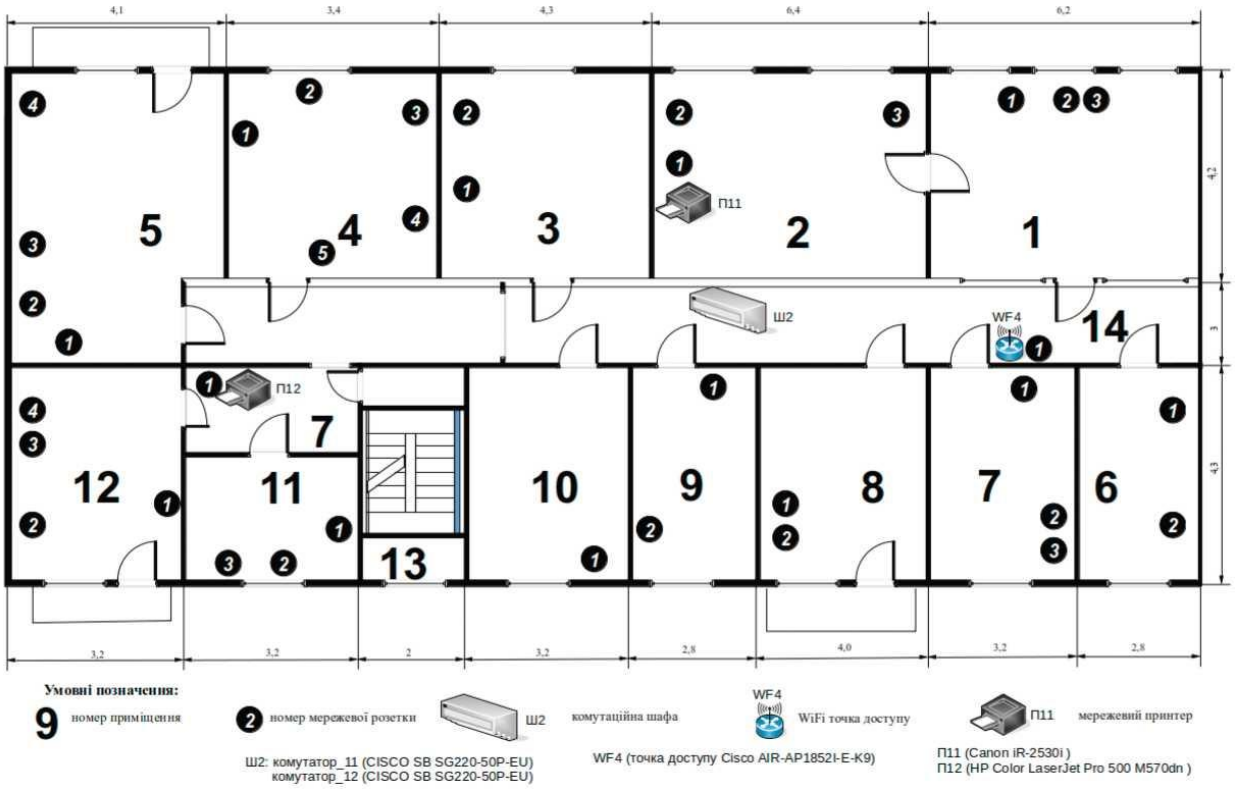


Рис. 1.23-– Приклад оформлення схеми розташування мережевого обладнання в підрозділах ДСНС

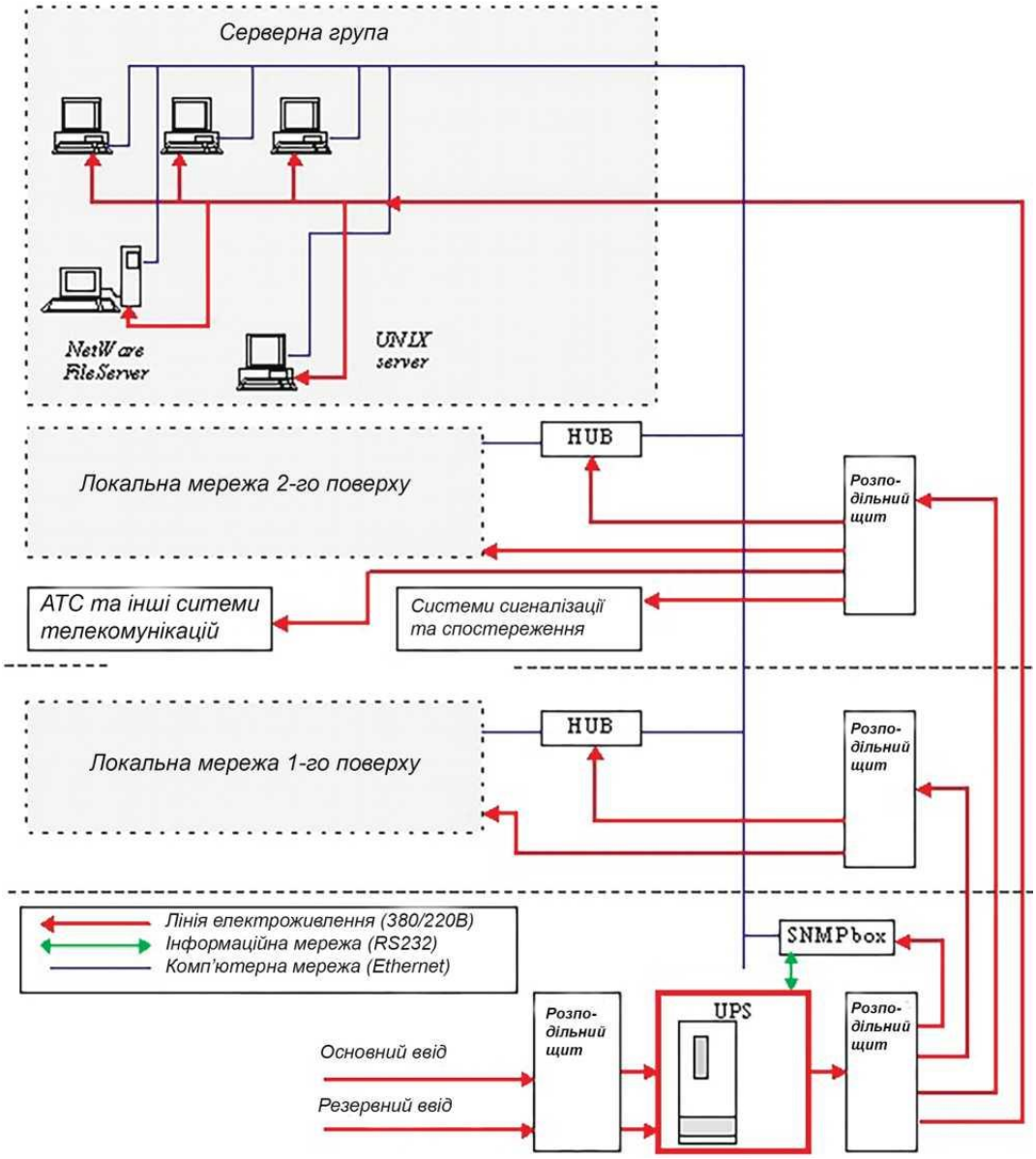


Рис. 1.24-– Приклад оформлення схеми організації електроживлення серверного приміщення

6. Рекомендовано здійснювати безпосереднє підключення до необхідних пристроїв лише за допомогою захищених протоколів, а саме SSH, SFTP та HTTPS.

1.4.3 Вимоги до організації Wi-Fi точок доступу до Інтернет (ВЦТМ)

1. Безпроводова мережа Wi-Fi має бути розгорнута в окремому сегменті мережі, який відокремлений та не перетинається із внутрішньою мережею ДСНС.

2. При налаштуванні обладнання Wi-Fi точок доступу необхідно встановлювати наступні параметри:

приховати ідентифікатор мережі (SSID): ввімкнено;

фільтрація пристроїв по MAC адресами: ввімкнено;

тип автентифікації та шифрування: WPA2 PSK;

функція WPS: заборонено.

3. За погодженням з апаратом ДСНС може бути дозволено організацію доступу до ВЦТМ через WiFi.

1.4.4 Правила побудови мережі в центральних, окремих вузлах 1-го та 2-го рівня ВЦТМ

Структурована кабельна система має відповідати вимогам ДСТУ ISO/IEC 11801-1 та ДСТУ ISO/IEC 11801-2.

При проектуванні локальної мережі до кожного робочого місця має закладатися щонайменше по 2 мережевих кабелі вита пара.

Максимальна відстань горизонтальної проводки не має перевищувати 90 метрів.

Мережеве обладнання та мережеві кабелі мають відповідати категорії CAT5e та вище.

Телефонне обладнання та ПЕОМ дозволяється підключати одним мережевим кабелем через вбудований у телефон комутатор.

Всі мережеві кабелі від абонентів мережі мають підключатися до керованих комутаторів рівня доступу, розташованих на поверхах будівлі. Розташовувати керовані комутатори необхідно таким чином, щоб мінімізувати загальну довжину мережевих кабелів від абонентів підмереж.

Від кожного комутатора рівня доступу має бути прокладено по два оптоволоконних магістральних кабелі до серверного приміщення.

Рекомендовано здійснювати закупівлю комутаторів доступу із функцієюPoE.

Використання некерованих комутаторів при побудові мережі заборонено.

Прокладання кабелю в коридорах має здійснюватися за фальш стелею, за відсутності – в спеціальних кабель-каналах. У приміщеннях підведення мережевого кабелю до робочих місць має здійснюватися у спеціалізованих кабель каналах.

Структурована кабельна мережа має забезпечувати швидку перекомутацію ліній горизонтальної проводки та магістральних кабелів.

1.4.5 Питання безпеки ВЦТМ

На комутаторах рівня доступу та агрегації мають використовуватися такі технології:

деактивація незалучених інтерфейсів на активному обладнанні;

обмеження дозволених для транслювання MAC-адрес та фільтрації MAC-адрес;

ARP фільтрація;

Port Security;

використання списків доступу ACL.

На фаєрволах у центральному вузлі ДСНС та територіальних вузлів зв'язку:

застосування механізму DAI;

використання Anti DDoS лічильників, що обмежують кількість оброблюваних широкомовних пакетів;

використання захищених методів передачі даних, наприклад, IPsec тунелі; використання списків доступу ACL;

блокування TCP/UDP, що не використовуються у повсякденній роботі; застосування фільтрації URL-адрес;

використання захищених протоколів, що передають дані у шифрованому вигляді: HTTPS, SSH, SFTP.

В інформаційно-телекомунікаційних мережах (далі – ІТМ) необхідно здійснювати такі адміністративно-організаційні заходи щодо організації безпеки:

використання міжмережевих екранів (фаєрволів); розмежування корпоративної та публічної мереж;

логування на обладнанні дій персоналу, який обслуговує обладнання ІТМ; розмежування рівнів доступу співробітників;

надання кожному із співробітників, який займається адмініструванням ІТМ,

особистого облікового запису для авторизації на обладнанні;

розробка і дотримання правил щодо складності паролів облікових записів.

Надання доступу до мережі Інтернет необхідно організовувати через фаєрвол з використанням проксі сервера. Використання прямого («прозорого») доступу до мережі Інтернет не рекомендується.

Строк зберігання логів мережевого обладнання – не менше 6 місяців.

Всі абоненти ВЦТМ маються бути ідентифіковані.

Доступ до мережі Інтернет абонентам ВЦТМ має бути обмежено за портами (виключно за потребами пов'язаними з виконанням службових обов'язків).

Адміністративні паролі доступу до пристроїв ВЦТМ мають оновлюватися щонайменше раз у квартал та кожного разу при зміні адміністраторів підмереж ВЦТМ. Адміністративний пароль має складатися щонайменше з 10 символів різного регістру, включно із літерами, цифрами та символами.

У підмережах ВЦТМ мають використовуватися засоби моніторингу мережі, система запобігання вторгненням та фільтрації трафіка по протоколах і портам. Необхідно також здійснення фільтрації http/https трафіка. При модернізації мережі перевага має надаватися апаратним засобам захисту мережі.

Підмережі ВЦТМ має бути поділено на окремі сегменти (VLAN,

Virtual Local Area Network) по функціональному призначенню та/або територіальному розміщенню (будівлям, поверхам, кабінетам). Мінімально має бути створено:

VLAN для управління мережевою інфраструктурою;

VLAN для серверів;

VLAN для пристроїв телефонії;

VLAN для пристроїв фінансового (бухгалтерського) структурного підрозділу, підрозділів по роботі з персоналом, підрозділів служби діловодства та інших.

При модернізації ІТМ необхідно розгорнути загальну систему моніторингу ІТМ з можливістю реалізації такого функціоналу:

моніторинг доступності каналів зв'язку в режимі реального часу; моніторинг завантаженості каналу зв'язку, у тому числі з аналізом типу мережевого трафіка;

моніторинг стану обладнання та активних аварій; опитування обладнання по протоколу SNMP.

Необхідно щонайменше щороку оновлювати вбудований у мережеве обладнання програмний код (firmware).

1.4.6 Вимоги до пріоритетності та якості сервісів ВЦТМ ДСНС (QoS)

Пріоритетність обслуговування сервісів під час передачі даних у ВЦТМ ДСНС за пріоритетністю у порядку спадання:

відомча IP-телефонія;

відомча система відеоконференцзв'язку;

системи оперативного диспетчерського управління;

відомча електронна пошта;

системні мережеві сервіси;

службові інформаційні системи;

довідкові інформаційні системи;

резервування даних;

доступ до публічної мережі Інтернет.

1.4.7 Вимоги до інженерної інфраструктури технологічних приміщень (серверних) для розміщення серверного та телекомунікаційного обладнання ВЦТМ

Телекомунікаційне обладнання ВЦТМ має бути розміщено в окремих спеціально облаштованих серверних приміщеннях (далі – серверні), що складається із зон для розміщення:

серверного та телекомунікаційного обладнання; складових елементів системи електропостачання;

складових елементів систем забезпечення мікроклімату, технічної електробезпеки, технічного захисту інформації, газового пожежогасіння (вогнегасників) та інше обладнання.

Ці приміщення має бути оснащене такими системами:

система контролю доступу;

система відеоспостереження;

система автономного електроживлення;

система пожежегасіння;

система клімат-контролю (вентиляція, температура, вологість); структурованої кабельної системи; системи гарантованого електропостачання.

У серверному приміщенні має бути розташовано щонайменше одну серверну стійку вистою 42U для монтажу 19 дюймового мережевого, кросового та комунікаційного обладнання.

Розміри серверного приміщення визначаються в залежності від кількості серверних стійок та іншого габаритного обладнання. Проходи перед та позаду обладнання мають забезпечувати вільний доступ і складати щонайменше 80 сантиметрів. Площа серверного приміщення має складати від 20 м кв. Перебування в серверному приміщенні людей на постійній основі (використання приміщення як робочого кабінету) заборонено. Також заборонено використання серверних приміщень у якості складських приміщень для зберігання документів, інструменту, будівельних матеріалів, засобів телекомунікацій та інформатизації тощо.

Приміщення серверної рекомендується розташовувати без дотику із зовнішніми стінами будівлі і проходів у сторонні приміщення.

Серверні рекомендується розташовувати в приміщеннях без вікон.

Траси звичайного і пожежного водопостачання, опалення та каналізації повинні бути винесені за межі серверної і не перебувати безпосередньо над нею на верхніх поверхах. Через серверну не повинні проходити будь-які транзитні телекомунікації та кабелі електропостачання.

У серверній не рекомендується розташовувати джерела електромагнітного випромінювання (пристрої для доступу до телекомунікаційних мереж на основі технологій WiFi, GSM, CDMA тощо), які можуть негативно впливати на роботу серверного та телекомунікаційного обладнання.

Конструкція стін (перегородок) і дверей приміщення серверної повинна бути герметичною. Стіни, стеля та підлога повинні бути рівними, без виступів і напливів та мати покриття, яке ускладнює виділення, осідання і накопичення пилу на поверхні. Матеріали не повинні виділяти і накопичувати пил, а також не повинні накопичувати електростатичний заряд.

Будівельні матеріали повинні бути обрані з властивостями для мінімізації утворення цвілі і пошкодження гризунами.

Оздоблювальні поверхні повинні бути світлими для покращення загальної освітленості приміщення.

При виконанні оздоблювальних робіт повинні застосовуватися матеріали, що відповідають санітарним нормам та правилам пожежної безпеки: за групами горючості; поширення вогню; димоутворювальної здатності;

токсичності продуктів горіння та займистості у відповідності з категорією щодо вогнестійкості.

Стелі повинні мати гідроізоляцію для виключення можливості протікання води у приміщення серверної.

Не рекомендується використання в серверному приміщенні підвісної (фальш) стелі.

Приміщення серверної рекомендовано обладнувати фальш підлогою для розміщення комунікацій, конструкція якої повинна:

бути виконана плитами з антистатичним покриттям з негорючих матеріалів або матеріалів відповідних груп горючості і ступенем вогнестійкості;

мати висоту підпільного простору для прокладання в ньому комунікацій не менше 0,2 м;

забезпечувати вільний доступ до комунікацій під час обслуговування; мати стійкість до горизонтальних зусиль при частково знятих плитах; давати можливість вирівнювання поверхонь підлоги за допомогою регульованих опорних елементів;

гарантувати взаємозамінність плит.

Система забезпечення мікроклімату складається з підсистем вентиляції (за необхідності) та кондиціювання.

Структурована кабельна система складається з: підсистеми організації кабельних комунікацій; підсистеми розміщення монтажних шаф.

Системи протипожежного захисту складається з: системи пожежної сигналізації;

автоматичної системи газового пожежогасіння (первинними засобами пожежогасіння);

підсистеми димовидалення (за необхідністю).

Приміщення серверної згідно з ДБН В.2.5-56 обов'язково підлягають обладнанню системою пожежної сигналізації, тип застосовуваного обладнання системи та місця установки датчиків визначається на етапах технічного проектування відповідно до вимог ДБН В.2.5-56, ДСТУ EN 54-14, ДСТУ EN 54-13.

Приміщення серверних, які не підлягають обладнанню згідно з ДБН В.2.5-56 автоматичними системами газового пожежогасіння, мають бути оснащені первинними засобами пожежогасіння (пересувними або переносними газовими вогнегасниками).

Кліматичні умови в серверних приміщеннях характеризуються такими показниками: температура повітря та відносна вологість повітря.

У серверному приміщенні необхідно контролювати температуру і вологість, щоб вони постійно перебували в межах рекомендованих робочих діапазонів відповідно ДСН 3.3.6.042-99 і ANSI/TIA-942-A: температура повітря: від 20°C (68°F) до 25°C (68°F); відносна вологість повітря: від 40 % до 60 %.

Система кондиціонування повинна забезпечувати безперебійність її роботи у разі зникнення первинного електроживлення серверної чи в момент переключення вводу або запуску резервної бензо або дизель-електростанції. Для цього всі елементи системи кондиціонування мають живитися від системи гарантованого електропостанчання.

Рівень резервування системи кондиціонування повинен бути не менше ніж N+1 (бажано – 2N+1), тобто система повинна складатися як мінімум з двох незалежних кондиціонерів, кожен з яких розрахований на самостійне забезпечення заданого мікроклімату в приміщенні.

Для продовження і зрівнювання ресурсу кондиціонерів необхідно передбачити використання пристрою ротації (автоматичного перемикання) кондиціонерів.

Для видалення конденсату, що виділяється при роботі кондиціонерів, потрібно передбачити дренажний стік у систему каналізації.

Система гарантованого електропостачання складається з: підсистеми силової розподільної мережі (силове обладнання), підсистеми безперебійного електропостачання та розподілу електроенергії;

підсистеми резервного електропостачання;

підсистем заземлення (функціональне та захисне заземлення) та блискавкозахисту.

Система електропостачання серверної за своїм функціональним призначення відноситься до електроприймачів критичної (особливої) групи з неперервним режимом роботи та за ступенем надійності електропостачання належить до електроприймачів першої категорії згідно з ДБН В.2.5-23.

Систему електропостачання необхідно забезпечувати електроенергією від двох незалежних взаєморезервуючих джерел живлення. Переривання їх електропостачання, в разі порушення електропостачання від одного з джерел живлення, можна допускати лише на час автоматичного відновлення живлення.

Для електроприймачів особливої групи першої категорії надійності електропостачання необхідно передбачити додаткове живлення від третього незалежного взаєморезервованого джерела живлення, що забезпечує електропостачання визначеної тривалості. Таким джерелом живлення можуть бути згідно з ДБН В.2.5-23 джерела безперебійного живлення або дизельна (бензинова) електростанція.

Електропостачання серверної згідно з ДБН В.2.5-23 повинно виконуватися від мережі з глухозаземленою нейтраллю 380/220 В та із сис-

темою заземлення типу TN-S, яка забезпечує найвищий рівень електробезпеки людей і обладнання.

Опір заземлювального пристрою не повинен перевищувати 4 Ом і 8 Ом відповідно для лінійних напруг 380В і 220В джерела трифазного струму або 220В і 127В джерела однофазного струму згідно з Правилами улаштування електроустановок, затвердженими наказом Міністерства енергетики та вугільної промисловості України від 21.07.2017 № 476. Цей опір необхідно забезпечувати з урахуванням використання всіх заземлювачів, приєднаних до робочого заземлення.

Заземлювальні пристрої мають бути механічно міцними та динамічно стійкими до струмів замикання на землю і не повинні термічно пошкоджуватися за час протікання зазначених струмів. Матеріал і переріз заземлювачів мають забезпечувати їх стійкість до корозії на весь період експлуатації.

Заземлювальний пристрій, який використовують для заземлення, протягом усього періоду експлуатації серверної повинен відповідати всім вимогам до заземлення: захисту людей від ураження електричним струмом у разі пошкодження ізоляції, умовам режимів роботи мереж, захисту електрообладнання від перенапруги, електромагнітної сумісності обладнання, тощо.

Комутатори локальної мережі окремих вузлів ВЦТМ, які під’єднуються до мережевого обладнання в серверному приміщенні, мають бути розміщені в спеціалізованих серверних шафах із замками.

Телекомунікаційне обладнання абонентського доступу встановлюється в телекомунікаційних шафах із замками, які розміщуються на поверхах будівель в коридорних або окремих приміщеннях та живляться від системи резервного (гарантованого) електроживлення.

Серверні приміщення відносять до режимних. Повинно бути визначено внутрішніми наказами перелік осіб, які мають доступ до цих приміщень. Відвідування приміщень має відбуватись із занесенням у журнал інформації про всіх осіб, час та мету їх відвідування.

1.5 Поняття, класифікація й види сучасних інформаційних технологій

Технологія при перекладі із грецького (techne) означає мистецтво, майстерність, уміння, а це не що інше, як процеси. Під процесом слід розуміти певну сукупність дій, спрямованих на досягнення поставленої мети. Процес повинен визначатисяобраною людиною стратегією й реалізуватися за допомогою сукупності різних засобів і методів [17, 18, 19].

Термін***інформація*** походить від латинського слова ***informatio***, що означає «відомості, роз'яснення, виклад». Інформація – це настільки загальне й глибоке поняття, що його не можна пояснити однією фразою. У

це слово вкладається різний зміст у технікові, науці й у життєвих ситуаціях.

Інформація – відомості про об'єкти і явищах навколишнього середовища, їх параметрах, властивостях і стані, які сприймають інформаційні системи (живі організми, машини, щоуправляють ін.) у процесі життєдіяльності й роботи.

*Стосовно до комп'ютерної обробки даних під***інформацією**розуміють деяку послідовність символічних позначень(букв, цифр, закодованих графічних образів і звуків і т.п.) значеннєве навантаження, що несе, і представлену в зрозумілому комп'ютеру виді.Кожний новий символ у такій послідовності символів збільшує інформаційний об'єм повідомлення.

Інформація може існувати у вигляді:

текстів, малюнків, креслень, фотографій;

світлових або звукових сигналів;

радіохвиль;

електричних і нервових імпульсів;

магнітних записів;

жестів і міміки;

запахів і смакових відчуттів;

хромосом, за допомогою яких передаються в спадщину ознаки й властивості організмів, і т.д.

Що можна робити з інформацією? – створювати, приймати, комбінувати, зберігати, передавати, копіювати, обробляти, шукати, сприймати, формалізувати, ділити на частини, вимірювати, використовувати, поширювати, спрощувати, руйнувати, запам'ятовувати, перетворювати, збирати, і т.д. Усі ці процеси, пов'язані з певними операціями над інформацією, називаються **інформаційними процесами.**

Інформація має наступні властивості: достовірність, повнота, точність, цінність, своєчасність, зрозумілість, доступність, стислість і т.д.

Інформаційна технологія – процес, щовикористовує сукупність засобів і методів збору, обробки й передачі даних (первинної інформації) для одержання інформації нової якості про стан об'єкта, процесу або явища (інформаційного продукту).

Ціль інформаційної технології– виробництво інформації для її аналізу людиною й прийняття на його основірішення по виконанню якої-небудь дії.

Класифікація інформаційних технологій (Табл. 1.6)

по способу реалізації,

по ступеню охвату завдань управління,

по класу реалізованих технологічних операцій,

по типу користувацького інтерфейсу,

по способу побудови мережі,

по предметних областях, що обслуговуються, та ін.

По способу реалізації виділяють традиційні й нові інформаційні технології.

Традиційні інформаційні технології (ІТ)існували в умовах централізованої обробки даних і до масового використанняПЕВМ були орієнтовані головним чином на зниження трудомісткості при формуванні регулярної звітності.

Таблиця 1.6 – Класифікація інформаційних технологій

по способу реалізації традиційні; нові	**По типу користувацького інтерфейсу** пакетні, діалогові, мережеві.	**По способу побудови мережілокальні,** багаторівневі, розподілені	**По предметних галузях, що обслуговують,** науково -освітня, економіко – фінансова, телекомунікаційна, цивільний захист
По ступеню охвату завдань управління: електронна обробка даних; автоматизація функцій управління; підтримка прийняття рішень; електронний офіс; експертна підтримка.		**По класу реалізованихтехнологічних операцій** робота з текстовим редактором; робота з табличним процесором; робота із СУБД. робота із графічними об'єктами; мультимедійні системи; гіпертекстові системи	

Нова інформаційна технологія характеризується:

Використанням персональних комп'ютерів і мереж ПК.

Наявністю комунікаційних засобів.

Наявністю діалогової (інтерактивної) роботи з комп'ютером.

Наявністю інтеграційного підходу.

Гнучкістю процесів зміни даних і постановок завдань.

Органічним "вбудовуванням" комп'ютерів в існуючу на підприємствах технологію управління.

Нову інформаційну технологію, якапов'язана з інформаційним забезпеченням процесу автоматизованого управління в режимі реального часуназивають ***Автоматизованою інформаційною технологією (АІТ).***

АІТ – це технологія, яка ґрунтується на застосуванні комп'ютерів, активній участі користувачів (непрофесіоналів в галузі програмування) в інформаційному процесі, високомурівні дружнього користувацького інтерфейсу, широкомувикористанні пакетів прикладних програм загального й проблемного призначення, доступі користувача до віддалених баз даних і програмам завдяки обчислювальним мережам ЕОМ.

По ступеню охвату завдань управління розрізняють наступні АІТ:

електронна обробка економічних даних;

автоматизація функцій управління;

підтримка прийняття рішень;

електронний офіс;
експертна підтримка.

По класу реалізованих технологічних операцій виділяють такі АІТ:
робота з текстовим редактором;
робота з табличним процесором;
робота із СУБД.
робота із графічними об'єктами;
мультимедійні системи;
гіпертекстові системи.

По типу користувацького інтерфейсу розрізняють АІТ пакетні, діалогові, мережеві.

По способу побудови мережі бувають локальні, багаторівневі, розподілені.

По предметних галузях, що обслуговуються, виділяють наукову, освітню, економічну та фінансову , телекомунікаційну, в тому числі у цивільному захисті й ін..

Сучасна АІТ базується на наступних основних принципах.

Інтерактивний (діалоговий) режим роботи з комп'ютером.

Інтегрованість із іншими програмними продуктами.

Гнучкість процесу зміни даних і постановок завдань.

У якості інструментарію інформаційної технології використовуютьсярозповсюджені види програмних продуктів: текстові процесори, видавничі системи, електронні таблиці, системи управління базами даних, електронні календарі, інформаційні системи функціонального призначення.

До основних видів інформаційних технологій відносяться наступні табл. 1.7:

Таблиця. 1.7 – Види інформаційних технологій (ІТ)

ІТ	**Призначення**
обробки даних	вирішення добре структурованих завдань, алгоритми рішення яких добре відомі й для вирішення яких є всі необхідні вхідні дані
управління	інформаційне обслуговування персоналу, пов'язаного із прийняттям управлінських рішень в середовищі інформаційної системи управління
автоматизованого офісу	побудова телекомунікаційної системи забезпечення інформаційної взаємодії персоналу
підтримки прийняття рішень	вироблення управлінського рішення, при участі системи підтримки прийняття рішень (обчислювальна техніка й об'єкт управління) і людей (керівна ланка, що задає вхідні дані й оцінююче отриманий результат)
експертних систем	одержування персоналом консультації експертів по будь-яких проблемах, про яких у системах, заснованих на використанні штучного інтелекту накопичені знання в певної галузі

Інформаційні технології обробки даних призначені для вирішення добре структурованих завдань, алгоритми рішення яких добре відомі й для вирішення яких є всі необхідні вхідні дані. Застосовуються на рівні виконавської діяльності персоналу початкового рівня кваліфікації з метою автоматизації деяких рутинних операцій, що постійно повторюються, управлінської праці. Вони дозволяють обробляти бази даних, складати звіти діяльності й одержувати відповіді на будь-які запити діяльності, підтверджуючи їх документально. Основними їхніми компонентами є збір, обробка й зберіганняданих, а також створення звітів.

Інформаційна технологія управління призначені для інформаційного обслуговування персоналу, пов'язаного із прийняттям управлінських рішень, застосовуються в середовищі інформаційної системи управління й необхідні для обробки даних, які обробляються за допомогою спеціальних інформаційних засобів. Вони вирішують такі функції, як оцінка майбутнього стану діяльності об'єкта, оцінка відхилень отриманого результату від планових показників, виявлення причин, що вплинули на відхилення, аналіз можливих заходів. За допомогою даних технологій формуються регулярні, спеціальні, що підсумують, порівняльні й надзвичайні звіти.

Інформаційна технологія автоматизованого офісу(Call – центру, диспетчерської) покликано доповнити існуючу систему зв'язку персоналу. Автоматизація офісу передбачає організацію й підтримку комунікаційних процесів як усередині організації, так і із зовнішнім середовищем на базі комп'ютерних мереж і інших сучасних засобів передачі й роботи з інформацією. До основних компонентам відносять базу даних, електронну пошту, цифрову АТС, сервер Ір-телефонії й мультімедіа.

Інформаційна технологія підтримки прийняття рішень призначена для вироблення управлінського рішення, щовідбувається в результаті ітераційного процесу, у якому беруть участь система підтримки прийняття рішень (обчислювальналанка й об'єкт управління) і людей (керівналанка, що задає вхідні дані й оцінююче отриманий результат).

Інформаційна технологія експертних систем заснована на використанні штучного інтелекту. Експертні системи дають можливість персоналу одержувати консультації експертів по будь-яких проблемах, про яких у цих системах накопичені знання.

Технічними засобами виробництва інформації є***апаратне, програмне й математичне забезпечення*** цього процесу. З їхньою допомогою проводиться переробка первинної інформації в інформацію нової якості. Окремо із цих засобів виділяються програмні продукти й називаються інструментарієм, тобто програмним інструментарієм інформаційної технології.

Інструментарій інформаційної технології – один або кілька взаємозалежних програмних продуктів для певного типу комп'ютера, технологія роботи в якому дозволяє досягти поставлену користувачем мету.

У якості інструментарію можна використовувати наступні розповсюджені види програмних продуктів для персонального комп'ютера: *текстовий процесор (редактор), настільні видавничі системи, електронні таблиці, системи управління базами даних, електронні записні книжки, електронні календарі, інформаційні системи функціонального призначення (фінансові, бухгалтерські, для маркетингу та ін.), експертні системи* і т.д.

Складові інформаційної технології

Використовувані у виробничій сфері такі технологічні поняття, як норматив, технологічний процес, технологічна операція й т.п., можуть застосовуватися й в інформаційній технології. Перш ніж розробляти ці поняття в будь-який технологи, у тому числі й в інформаційній, завжди слід починати з визначення мети. Потім слід спробувати провести структурування всіх передбачуваних дій, що приводять до наміченої мети, і вибрати необхідний програмний інструментарій.

Процес переробки інформації представляється у вигляді ієрархічної структури по рівнях.

1-й рівень – етапи, де реалізуються порівняно тривалі технологічні процеси, що полягають із операцій і дій наступних рівнів.

2-й рівень – операції, у результаті виконання яких буде створений конкретний об'єкт в обраній на 1-мрівніпрограмномусередовища.

3-й рівень – дії – сукупність стандартних для кожного програмного середовищаприйомів роботи, що приводять до виконання поставленої у відповідній операції мети. Кожнадія змінює зміст екрана.

4-й рівень – елементарні операції по керуванню мишею й клавіатурою.

Із цього обмеженого числа елементарних операцій у різних комбінаціях складається дія, а з дій, також у різних комбінаціях, складаються операції, які визначають той або інший етап. Сукупність технологічних етапів утворює технологічний процес (технологію). Етапи, дії, операції технологічного процесу можуть бути стандартизовані й уніфіковані, що дозволить більш ефективно, здійснювати цілеспрямоване управління інформаційними процесами.

Інформаційна технологія повинна відповідати наступним вимогам:

забезпечувати високий ступінь розчленовування всього процесу обробки інформації на етапи (фази), операції, дії;

включати весь набір елементів, необхідних для досягнення поставленої мети;

мати регулярний характер.

Програмні засоби інформаційних систем

базове програмне забезпечення;

інструментальні засоби;

прикладні засоби.

До базового програмного забезпечення ставляться локальні й мережні операційні системи (Windows, Unix, Solaris, OS/2, Linux і ін.), а також

сервісні засоби для розширення можливостей операційних систем, забезпечення працездатності комп'ютерів і виконання процедур обслуговування АІС (антивірусні програми, архіватори файлів, утиліти для тестування комп'ютерів і мереж і т.п.).

Інструментальні засоби призначені для виготовлення нових програм. Це алгоритмічні мови, інтерпретатори й компілятори до них.

Прикладні програмні засоби включають:

ПС загального призначення (офісні, комунікацій, мультімедіа, видавничі системи, перекладачі та ін.).

Методо-орієнтовані ПС (статистика, бухгалтерський та інші види обліку, планування, управління проектами, експертні системи, штучний інтелект і ін.).

Проблемно-орієнтовані ПС (локальні, комплексні, інтегровані, корпоративні й ін.).

Динаміка впровадження інформаційних технологій представлена на рис.1.25.

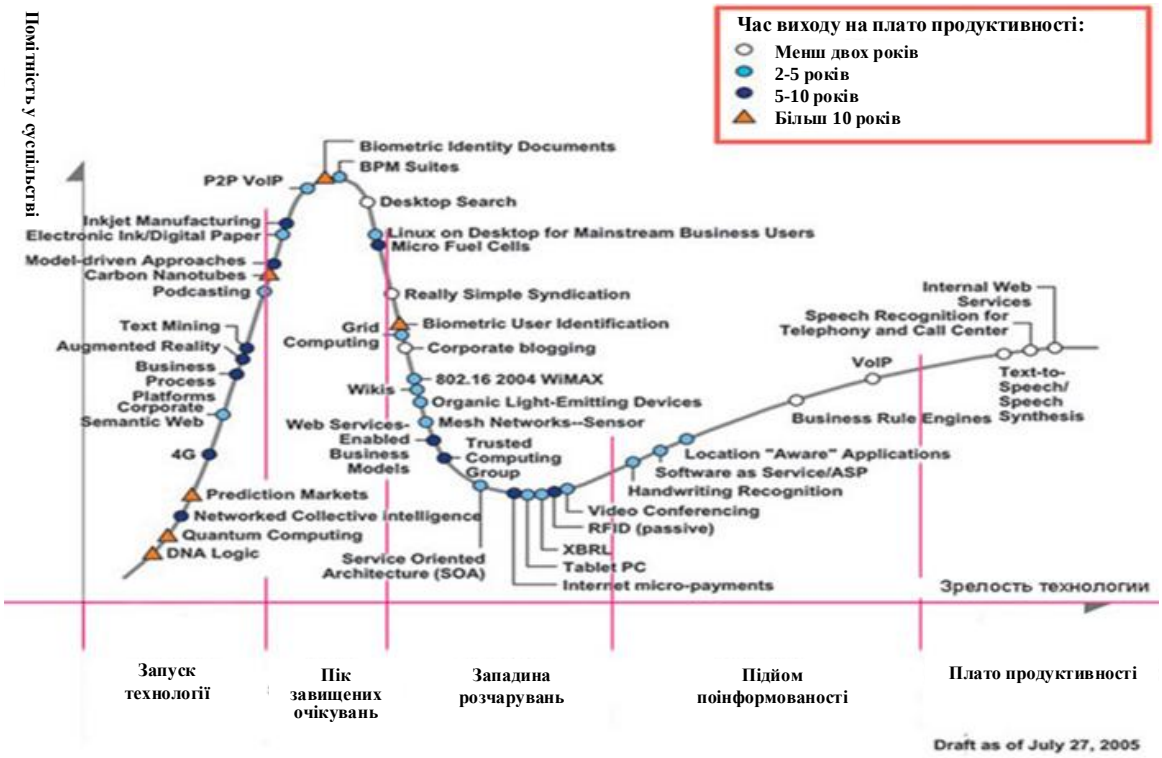


Рис. 1.25 – Динаміка впровадження інформаційних технологій

Інформатизація в ДСНС України – сукупність взаємопов'язаних організаційних, правових і науково-технічних процесів, що спрямовані на створення умов ефективного функціонування системи управління силами цивільного захисту ДСНС в режимах повсякденної діяльності, підвищеної готовності і надзвичайної ситуації на основі створення, розвитку і використання інформаційних систем, мереж, ресурсів та інформаційних

технологій, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки.

Інформаційна система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів.

Засоби інформатизації – електронні обчислювальні машини, організаційна техніка, програмне, лінгвістичне та інше забезпечення, інформаційні системи або їх окремі елементи, інформаційні мережі і мережі зв'язку, що використовуються для реалізації інформаційних технологій.

Інформаційний ресурс – сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо).

Інформаційні ресурси ДСНС – державні інформаційні ресурси, що підлягають захисту відповідно до порядку визначеному законодавством України шляхом впровадженням комплексу технічних, організаційних та інших заходів спрямованих на недопущення блокування інформації, несанкціонованого ознайомлення з нею та/або її модифікації.

Інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Інформація з обмеженим доступом – інформація, що становить державну або іншу передбачену законом таємницю, а також службова та конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України «Про доступ до публічної інформації», та інша конфіденційна інформація, вимога щодо захисту якої встановлена законом.

Упровадження інформаційних технологій (**ІТ**) в діяльність підрозділів ДСНС відбувається шляхом автоматизації процесів управління діяльністю ДСНС, оперативного рішення завдань щодо забезпечення пожежної та техногенної безпеки, адміністративно-господарської діяльності і реалізується через засоби інформатизації, що забезпечує рішення завдань за призначенням.

Основним призначенням упровадження ІТ у ДСНС є автоматизація обробки інформації за напрямками діяльності ДСНС.

Основним завданням ІТ у ДСНС є:

автоматизація системи оперативно-диспетчерського управління;

впровадження та підтримка функціонування системи електронного документообігу;

автоматизація основних напрямків адміністративно-управлінської діяльності (матеріально-технічне забезпечення, фінансово-господарська діяльність, і т.д.);

підтримка функціонування Інтернет-ресурсів ІТС та ТС в ДСНС.

Інформаційні технології повинні забезпечувати:

взаємодію інформаційних потоків усіх рівнів;

збереження цілісності інформаційних баз даних;

оперативність та достовірність інформації;

ефективне й надійне функціонування інформаційних систем та захист від несанкціонованого доступу та кіберзахист.

Використання ресурсів мережі Інтернет (каналів передачі даних, серверів і наданих ними сервісів та інформації, одержуваної з їхньою допомогою) має відбуватися відповідно до вимог нормативних документів щодо правил та порядку використання цих ресурсів.

1.6 Інформаційні системи в цивільному захисті

1.6.1 Призначення і класифікація інформаційних систем в цивільному захисті

Інформаційні системи, а саме інформація і інформаційні технології існували з моменту появи суспільства, оскільки на будь-якій стадії його розвитку існує потреба в керуванні. А для управління потрібно систематизована, попередньо підготовлена інформація.

Таким чином, місія інформаційних систем – виробництво потрібної для організації інформації з метою забезпечення ефективного управління всіма її ресурсами, створення інформаційного і технічного середовища для здійснення управління.

Розглядаючи систему управління, можна виділити три рівні управління: стратегічний, тактичний і оперативний. На кожному з цих рівнів управління вирішуються свої задачі, для рішення яких виникає потреба в інформації, тобто інформаційних запитів до інформаційної системи.

Ці запити спрямовані до відповідної інформації в інформаційній системі. Інформаційні технології дозволяють обробити запити і, використовуючи наявну інформацію, сформувати відповідь на ці запити.

Кожен рівень управління вирішує свої задачі та використовує певну інформацію. Інформація отримується шляхом формування запитів до інформаційної системи (ІС). Конкретні запити спрямовані до відповідної інформації в ІС, яка обробляє запити та по наявної інформації формує відповідь.Таким чином, на кожному рівні управління з'являється інформація, що служить основою для прийняття відповідних рішень (рис. 1.26).

Відповідно до характеру інформації і рішень в організації з'являються інформаційні системи визначеного рівня (рис. 1.27).

Приклади ІС:

– автоматизовані інформаційні системи (АІС) забезпечення і контролю пожежної безпеки об'єктів (АІС пожежного нагляду);

– АІС зв'язку й оперативного управління діяльністю підрозділів ДСНС (АІС оперативно-диспетчерського управління, надалі– СОДУ);

– АІС правового забезпечення діяльності підрозділів ДСНС (АІС управління правовим забезпеченням)і т.п.

Щоб розібратися в роботі інформаційної системи, необхідно зрозуміти суть проблем, що вона вирішує, а також організаційні процеси, у які вона включена.



Рис. 1.26 – Розподіл інформації за рівнями управління



Рис. 1.27 – Зв'язок типів інформаційних систем і рівнів управління

У кожній з таких систем зорганізується і ведеться робота щодо:
- визначення інформаційних потреб;
- здійснення добору джерел інформації;
- збору інформації;
- введення інформації від зовнішніх або внутрішніх джерел;

• дій по обробці інформації, оцінці її повноти і значимості і по формалізації даних (представлення інформації в зручному вигляді);

• виведення інформації для надання споживачам або передачі в іншу систему;

• використання інформації для оцінки тенденцій, розробки прогнозів, оцінки альтернатив рішень і дій, вироблення стратегії;

• організація зворотного зв'язку – за інформацією, переробленою людьми даної організації, здійснення корекції вхідної інформації.

Всі зазначені дії передбачають використання певних інформаційних технологій у рамках інформаційної системи ДСНС України.

Принципово важливим питанням є встановлення регламенту (порядку) функціонування інформаційної системи – від виявлення інформаційних потреб до безпосереднього використання інформації.

Мова йде про типізацію задач, розв'язуваних в підрозділах ДСНС України, встановлення періодичності одержання, обробки і використання інформації, а також щодо стандартизації вхідних і вихідних документів, стандартизації процедур обробки інформації.

Запити до інформаційної системи і, отже, процедури формування відповіді на них можна розподілити на рутинні і не рутинні.

Рутинні процедури характеризуються заданістю вихідної і вихідної інформації, а також визначеністю алгоритму одержання останньої з першої.

Виділення рутинних задач і процедур обробки інформації дозволяє формалізувати ці задачі, а надалі автоматизувати процес їх розв’язання. Складність питання полягає лише в тому, чи спроможні інформаційні технології, які використовуються в підрозділах ДСНС, забезпечити інфраструктуру для цього.

В основі будь-якої системи лежить процес. В основі інформаційної системи – процес виробництва інформації. В цьому змісті ми можемо розглядати інформаційну систему як систему управління, де процес виробництва інформації є об'єктом управління.

Як і в будь-який системі управління, в АІС управління (АСУ) існують органи управління інформаційною системою (табл. 1.8)

Таблиця 1.8 – Інформаційна система як об’єкт управління

Об’єкт управління	**Оперативний рівень управління**	**Тактичний рівень управління**	**Стратегічний рівень управління**
Інформаційна система ДСНС України	Керівний і виконавчій склад ГУ ДСНС України в області	Керівники і виконавці пожежно-рятувальних підрозділів	Керівний склад ДСНС України
Інформаційні технології, що застосовані	Персонал інформаційної системи	Персонал інформаційної системи	Головне керівництво інформаційною системою

Інформаційні системи можуть бути класифіковані по ряду ознак:

за ступенем автоматизації (автоматизовані або неавтоматизовані);

за сферою функціонування об'єкта управління;

за рівнем у системі управління (державні, територіальні, окремого підрозділу ДСНС України і т.п.);

за видом процесів управління (технологічні процеси, управлінські процеси);

за видом використання (емпіричні і теоретичні).

У даний час склалася думка про інформаційну систему як про систему, яка реалізована за допомогою комп'ютерної техніки. Це не так, інформаційні системи, як і інформаційні технології, можуть функціонувати як із застосуванням технічних засобів, так і без такого застосування. Це питання економічної доцільності.

Зростання обсягів інформації в інформаційній системі ДСНС України, потреба в прискоренні і більш складних способах її переробки викликають необхідність автоматизації роботи інформаційної системи, тобто автоматизації обробки інформації.

У неавтоматизованій інформаційній системі всі дії з інформацією, а також прийняття рішення здійснює людина.

Автоматизація процесів обробки інформації призводить до появи, в рамках алгоритмів обробки інформації, вирішальних правил. Це приводить до переростання «чистої» інформаційної системи в інформаційну систему управління. У рамках останньої частково реалізовані функції людини з прийняття рішень.

1.6.2 Структурні компоненти та вимоги до АІС

АІС управління діяльністю підрозділів ДСНС України – є взаємозалежна сукупність даних, устаткування, програмних засобів, персоналу, стандартів процедур, призначених для збору, обробки, розподілу, збереження, видачі (надання) інформації відповідно до вимог, що випливають з цілей діяльності підрозділів ДСНС України.

Як правило, це система для підтримки прийняття рішень і виробництва інформаційних продуктів, що використовує комп'ютерну інформаційну технологію, і персонал, взаємодіючий з комп'ютерами і телекомунікаціями.

Технологія роботи в комп'ютеризованій інформаційній системі повинна бути доступна для розуміння фахівцем некомп'ютерної області і може бути успішно використана для контролю процесів професійної діяльності і управління ними.

За думкою Г.Поппеля і Б.Голдстайна[24], обмін інформацією починається і закінчується мовою, даними або зображенням, сприйманими органами сприйняття людини: слухом, зором і дотиком. А між цими вхід-

ними і вихідними елементами в комп'ютеризованій інформаційній системі знаходиться електронний продукт різних рівнів – операційні системи, системи управління базами даних, прикладне забезпечення і сама інформація. Ця інформація, програмні засоби і компоненти інформаційної системи, за допомогою яких інформація збирається, обробляється і передається, часто недоступні для використання в той самий момент часу. Тому характеристикою таких інформаційних систем є можливість зсуву в часі процесів обробки даних.

Автоматизована інформаційна система має частину забезпечення і функціональну частини (табл. 1.9.).

Таблиця 1.9 – Обов'язкові структурні компоненти АІС

Структурні компоненти інформаційної системи	
Частина забезпечення	
Технічне забезпечення Математичне забезпечення Лінгвістичне забезпечення Програмне забезпечення	Інформаційне забезпечення Організаційне забезпечення Методичне забезпечення Правове забезпечення	Функціональна частина

Частина, що забезпечує, складається з інформаційного, технічного, математичного, програмного, методичного, організаційного і лінгвістичного забезпечення.

Інформаційне забезпечення – сукупність проектних рішень по обсягах, розміщенню, формам організації інформації (єдиної системи класифікації і кодування інформації, уніфікованих систем документації, схем інформаційних потоків), що циркулює в організації, а також методологія побудови баз даних.

Містить у собі: показники, довідкові дані, класифікатори і кодифікатори інформації, уніфіковані системи документації, інформацію на носіях і т.д.

У рамках інформаційного забезпечення маються позамашинні й внутрішньомашинні дані.

Позамашинна інформаційна база сприймається людиною без допомоги технічних засобів – наряди, акти, накладні і т.п.

Внутрішньомашинна інформаційна база утримується на носіях і складається з файлів. Вона може бути створена як сукупність окремих файлів, кожний з яких відбиває деяку множину однорідних управлінських документів (наряди, накладні і т.п.), або як база даних.

В останньому випадку файли будуть залежними і структура одних файлів буде залежати від структури інших, а структури файлів бази даних не будуть відповідати структурі управлінських документів.

В інформаційному забезпеченні розрізняють вхідні і вихідні документи.

Технічне забезпечення – комплекс технічних засобів, призначених для роботи ІС, а також відповідна документація на ці засоби і технологічні процеси.

Містить у собі:

• технічні засоби збору, реєстрації, накопичення, обробки, передачі, відображення, виводу, розмноження інформації;

• комп'ютери будь-яких моделей (персональні комп'ютери і високопродуктивні комп'ютери); комп'ютери можуть поєднуватися в обчислювальні мережі;

• оргтехніку і т.д.;

• пристрої автоматичного зняття інформації;

• експлуатаційні матеріали й ін.

Попередній вибір технічних засобів, організація їхньої експлуатації, технологічний процес обробки даних, технологічне оснащення оформляються документацією. Документацію можна умовно розділити на три групи:

загальносистемну, що включає державні і галузеві стандарти з технічного забезпечення;

спеціалізований, утримуючий комплекс методик по всіх етапах розробки технічного забезпечення;

нормативно-довідкову, яка використовується при виконанні розрахунків з технічного забезпечення.

Математичне забезпечення – сукупність математичних методів, моделей, алгоритмів обробки інформації, як використовуються при рішенні задач в ІС (функціональних і автоматизації проектування інформаційних систем).

До засобів математичного забезпечення відносяться:

засоби моделювання процесів управління;

типові задачі управління;

методи математичного програмування, математичної статистики й ін.

Програмне забезпечення – сукупність програм для реалізації цілей і задач ІС, а також нормального функціонування комплексу технічних засобів.

До складу програмного забезпечення входять загальносистемні і спеціальні програмні продукти, а також технічна документація, у тому числі: операційна система, системи програмування, інструментальні засоби, тестові і діагностичні програми, програмні засоби телекомунікації, захисту інформації, функціональне програмне забезпечення (автоматизовані робочі місця, системи управління базами даних і ін.).

Спеціальне програмне забезпечення являє собою сукупність програм, розроблених при створенні конкретної ІС. У його склад входять пакети прикладних програм, що реалізують розроблені моделі різного ступеня адекватності, що відбивають функціонування реального об'єкта.

Технічна документація на розробку програмних засобів повинна містити опис задач, завдання на алгоритмізацію, економіко-математичну модель задачі, контрольні приклади.

Методичне забезпечення й організаційне забезпечення – сукупність методів, засобів і документів, що регламентують взаємодію персоналу ІС з технічними засобами і між собою в процесі розробки й експлуатації інформаційної системи.

Функціональна частина інформаційної системи забезпечує виконання і призначення ІС. Фактично тут утримується модель системи управління організацією. У рамках цієї частини відбувається трансформація цілей управління у функції, функцій – у підсистеми інформаційної системи. Підсистеми реалізують задачі.

Підсистема – це частина системи, виділена за якою-небудь ознакою. Звичайно в інформаційній системі функціональна частина розбивається на підсистеми по функціональних ознаках:

рівень управління (вищий, середній, нижчий);

вид керованого ресурсу (матеріальні, трудові, фінансові й ін.);

сфера застосування (фінансові, технологічні й ін.);

функції управління і період управління.

Прикладом може служити інформаційна система управління технологічними процесами – комп'ютерна інформаційна система, що забезпечує підтримку прийняття рішень по управління технологічними процесами з заданою дискретністю й у рамках визначеного періоду управління.

Загальні вимоги до ІС

Основними вимогами, актуальними для сучасних інформаційно-управляючих систем, можна вважати:

наявність єдиного інформаційного простору всієї організації, до складу якого повинні входити фактографічні бази даних, як у частині технології, так і адміністративно-господарської діяльності; бази документів, прецедентів і об'єднуючий їхній компонент – предметно-орієнтоване сховище даних, що дозволяє використовувати всю накопичену інформацію для прийняття технологічних і управлінських рішень;

автоматизована підтримка методичного забезпечення аналізу, оцінки і прогнозу діяльності підприємства в цілому, але і також його структурних частин;

орієнтація на створення й ефективне застосування розподілених процесів формування варіантів рішень для керівного персоналу всіх рівнів;

відповідність функціональності автоматизованих робочих місць персоналу організації їхнім посадовим обов'язкам;

підвищення якості управління за рахунок більш оперативного і повного використання інформації про хід управлінського процесу;

наявність корпоративної мережі як інформаційної основи організації;

забезпечення вірогідності і цілісності даних при інформаційному обміні, як усередині організації, так і при виході на зовнішніх користувачів;

технологічна цілісність, що виявляється в застосуванні погодженого набору промислових інформаційних технологій для більш ефективного використання і управління інформаційними ресурсами організації;

інформаційна наступність старих і нових інформаційних систем;

забезпечення високого рівня надійності даних при цілодобовій роботі.

Вимоги до інформаційної системі, не можуть бути задоволені звичайним набором комп'ютерного устаткування і програмних додатків.

Кінцевою метою розробки інформаційної системи повинно бути створення єдиної корпоративної інформаційно-управляючої системи. Сучасна інформаційна система орієнтована не на виконання окремих задач, а на забезпечення раціонального виконання основних функцій організації, тобто на здійснення організаційних, управлінських, і технологічних функцій, що не є допоміжною або сервісною програмою.

Природно, що універсальних рецептів, що могли б однаково успішно застосовуватися у різних організаціях, немає. Але є методи, з використанням яких можуть бути побудовані системи управління діяльністю підрозділів.

Ці методи являють собою формалізовану сукупність понять і процесів, що дозволяє створити інформаційну систему того, як організація повинна працювати, і мають сугубо конструктивний характер, тобто її можна сприйняти як набір інструкцій (алгоритм), розроблених у результаті аналізу діяльності підрозділів визначеної організації.

При цьому принципово важливою якістю такої інформаційної системи є те, що система має можливість розвитку “зверху вниз”, коли в першу чергу автоматизується не діяльність виконавців, а рівень підготовки і структурованого представлення інформації для керівництва організації.

Побудова інформаційної піраміди “зверху вниз” дозволяє:

мінімізувати витрати на формальні заходи, результати яких не будуть затребувані через зміну потреб організації до моменту завершення робіт з автоматизації;

різко скоротити час від початку робіт до одержання практичних результатів;

поміняти місцями групи споживачів (першими користувачами системи, що зможуть оцінити ефект від її впровадження, є не виконавці, а керівники організацій);

оптимізувати інформаційну структуру організації.

1.6.3 Бази та банки даних АІС

База даних (БД) – це електронні сховища інформації з сукупністю відомостей про конкретні об'єкти в певній предметній галузі. Такі відомості звичайно зберігаються на електронних носіях, доступ до яких здійснюється через один чи декілька комп'ютерів

Слушне і таке визначення БД.***БД*** – це сукупність даних, яка зберігається в електронному вигляді і відображує стан об'єктів і їх співвідношень в певній предметній галузі.

На початку ери використання ЕОМ баз даних ще не було розроблено, і користувачі зберігали інформацію в звичайних текстових файлах. Навіть зараз в багатьох випадках для користувачів-початківців текстові файли служать найбільш зручним, а часто і єдиним сховищем різноманітної символьної і навіть числової інформації. Так, прикладами зберігання інформації у текстових файлах можуть служити:

• прізвища та адреси всіх знайомих (або підлеглих);

• листи, згруповані за адресатом;

• документи, набрані за допомогою текстових редакторів, згруповані за темою;

• набір файлів, пов'язаних з фінансовими справами: рахунки, витрати по чековій книжці тощо.

В чому ж недоліки і переваги зберігання інформації в текстових файлах (табл. 1.10).

Таблиця 1.10 – Переваги і недоліки зберігання даних в текстових файлах

Недоліки	Переваги
При великих обсягах інформації важко вводити, редагувати та знаходити потрібну інформацію.	Легко читати, проглядати, копіювати, редагувати, коли обсяг інформації невеликий
Інформацію легко зіпсувати.	Легко проводити простий пошук.
Утруднений пошук, вибірка, систематизація.	

Із-за цих недоліків бази даних мають свій (не текстовий) формат зберігання даних, який описує не тільки певні об'єкти БД, але й зв'язки між ними. Для того, щоб підтримувати діалог користувача з таким чином організованими даними, використовують спеціальні програмні системи – СУБД.

СУБД (система управління базами даних) – універсальний програмний засіб, призначений для створення і обслуговування баз даних на зовнішніх запам'ятовуючих пристроях, насамперед для доступу до даних та їх обробки.

Автоматизованою інформаційною системою (АІС) або банком даних зветься сукупність тим чи іншим засобом структурованих даних (бази даних) і комплексу апаратно-програмних засобів для зберігання даних і маніпулювання ними. На рис. 1.28. наведена схема, яка ілюструє структурні складові АІС.

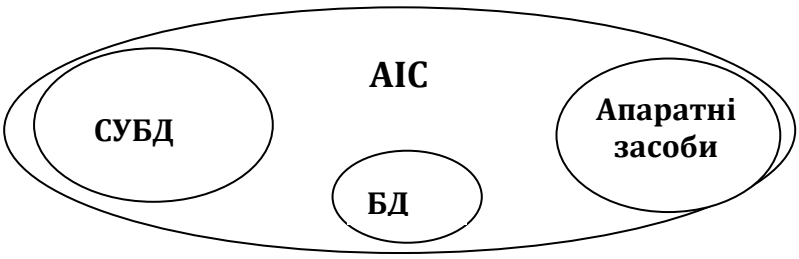


Рис. 1.28 – Склад типової АІС

1.6.4 Функції універсальної АІС (Типові операції при роботі БД)

Зберігання інформації. АІС зберігає структуровану та неструктуровану інформацію про об'єкти конкретної предметної галузі, виконуючи як архівну роль, так і роль постачальника оперативних довідок.

Перегляд та пошук. АІС забезпечує перегляд інформації по заданій користувачем сукупності полів, значення яких упорядковані в сторону збільшення або зменшення (в окремому випадку – по алфавіту). Побутовий аналог – перегляд алфавітного указника в бібліотеці Пошук – це окремий випадок перегляду, коли використовуючи упорядкованість файлу, система швидко вказує на запис (або на перший запис в блоці), який зберігає вказану користувачем сукупність полів, Аналогія із звичайного життя – пошук в алфавітному покажчику автора Петрова або авторів, прізвище яких починається на літеру "П". Після фіксації першого (або одного) запису процес пошуку стає процесом вибірки.

Вибірка. АІС забезпечує вибірку певної сукупності записів файлу, яка задовольняє заданим користувачем вимогам. З вибіркою тісно пов'язане сортування по різноманітних критеріях (по алфавіту, по даті, по збільшенню числових параметрів).

Введення та редагування інформації. АІС забезпечує різноманітні засоби введення та редагування інформації.

Контроль інформації. У багатьох ІС є можливість контролювати коректність інформації, що вводиться, та, крім того, в певних випадках обмежувати доступ до інформації, захищати її.

Відображення інформації. Усі АІС забезпечують різноманітні засоби подання даних у формі, зручній для користувача, як на дисплеї, так і на папері. Інформація в АІС може виводитись у вигляді форм або звітів.

Під формою (шаблоном) буде розумітись електронна форма подання бланка. "Комірки" в формі служать для введення даних в БД або для відображення даних з БД.

Звітом (зведенням) є впорядкований набір даних у певному вигляді для друку.

З функціями перегляду, пошуку, вибірки та сортування пов'язане поняття запиту. Запит – звернення до бази даних з метою вибірки частини інформації за певним критерієм.

1.7 Урядова інформаційно-аналітична система з питань надзвичайних ситуацій

Необхідність створення УІАС НС. Україна є одним з найбільш критичних регіонів Європи з техногенного навантаження та потенційної безпеки шкідливих виробництв для населення і природного середовища. Екологічна небезпека поглиблюється соціально-політичною напруженістю. Все це створює об'єктивні передумови зростання кількості різних надзвичайних ситуацій. Успішне запобігання виникненню НС та ліквідація їх наслідків неможливі без урахування на урядовому рівні екологічних, соціально-економічних та інших передумов. Ці обставини визначили необхідність створення в Україні єдиної Урядової інформаційно-аналітичної системи з питань НС [6-8].

Призначення та мета створення. Оперативне забезпечення Президента України, Верховної Ради України, Кабінету Міністрів України, Ради національної безпеки і оборони України, центральних органів виконавчої влади експертно-аналітичною, прогнозною, довідково-статистичною, фактографічною, контрольно-звітною та управлінською інформацією з використанням сучасних інформаційних технологій для вирішення задач, пов'язаних з техногенне – екологічною безпекою та НС

Основними цілями створення УІАС НС є:

– забезпечення керівництва Кабінету МіністрівУкраїни, Адміністрації Президента України, Верховної Ради України, Ради національної безпеки і оборони України, центральних органів виконавчої влади, обласних, міських, районних держадміністрацій достовірною інформацією, пов'язаною з екологічною безпекою, в тому числі ядерною, та надзвичайними ситуаціями (далі – НС);

– забезпечення сумісності інформації щодо запобігання виникненню НС чи ліквідації їх наслідків на основі використання єдиних принципів побудови баз даних, єдиної сертифікованої картографічної інформації, єдиних класифікаторів стандартів;

– забезпечення оперативного доступу до інформаційних ресурсів УІАС НС;

– науково обґрунтоване прогнозування можливого виникнення НС та їх наслідків;

– забезпечення інформаційної взаємодії та координації роботи органів виконавчої влади щодо запобігання виникненню НС чи ліквідації їх наслідків.

Створення УІАС НС дає змогу:

– автоматизувати процеси одержання та накопичення інформації щодо запобігання виникненню НС чи ліквідації їх наслідків на території України;

– оперативно інформувати керівництво центральних та місцевих органів виконавчої влади щодо запобігання виникненню НС, виникнення чи ліквідації їх наслідків;

– давати експертну оцінку, визначати сили та засоби, необхідні для ліквідації наслідків НС;

– аналізувати передумови виникнення НС та прогнозувати їх виникнення;

– аналізувати та моделювати розвиток НС;

– готувати проекти рішень Кабінету Міністрів України щодо планування заходів із запобігання та ліквідації наслідків НС;

– здійснювати контроль за ходом виконання заходів щодо запобігання виникненню НС, ліквідацією їх наслідків та виконанням рішень органів виконавчої влади з питань НС.

Підстави для створення УІАС НС:

– ПостановаКМУ від 16 грудня 1999 р. N 2303 "Про створення Урядової інформаційно-аналітичної системи з питань надзвичайних ситуацій";

– Постанова КМУ від 9 січня 2014 р. № 11 “ Про затвердження Положення про єдину державну систему цивільного захисту ”.

З 2002 року єдиний замовник створення УІАС НС – МНС України.

Метою створенняУІАС НС є вдосконалення заходів, що здійснюються органами виконавчої влади у галузі техногенно-екологічної безпеки, запобігання надзвичайним ситуаціям.

УІАС НС вирішує завдання обробки, аналізу та надання керівництву органів виконавчої влади повної та достовірної інформації щодо НС при ліквідації їх наслідків, а також прогнозування та моделювання виникнення та розвитку НС.

Основними завданнями Урядової інформаційно-аналітичної системи є:

– поліпшення організації державного управління надзвичайними ситуаціями, а саме:

1) своєчасне*забезпечення* Уряду *достовірною інформацією,* необхідною для підготовки рішень Кабінету Міністрів України з питань запобігання, пом'якшення, локалізації та ліквідації наслідків надзвичайних ситуацій, а також створення умов для оперативного координування ним дій органів державної виконавчої влади у разі виникнення надзвичайних ситуацій;

2) *об'єднання і вдосконалення існуючих відомчих систем* щодо запобігання наслідкам надзвичайних ситуацій та їх ліквідації;

3) проведення регулярного*системного аналізу*найважливіших подій, їх чинників та наслідків, а також багатомірної інтегрованої оцінки факторів і умов, що впливають на розвиток надзвичайних ситуацій;

4) створення і впровадження *нових технологій контролю* за об'єктами підвищеного ризику з урахуванням їх взаємозв'язку, впливу гідрометеорологічних умов та стихійного лиха, суб'єктивних та інших факторів;

5) розроблення і впровадження територіальної системи *моделювання* техногенно-екологічного та епідеміологічного навантаження на відповідну категорію та зменшення невиправданого паралелізму у діях і програмах щодо надзвичайних ситуацій;

6) *систематизація* існуючих розробок у галузі надзвичайних ситуацій;

7) *координація* робіт у рамках державного моніторингу, пов'язаних і: застосуванням єдиної нормативної та довідкової документації;

– створення і впровадження на загальнодержавному, регіональному та місцевому рівнях геоінформаційних систем для прогнозного моделювання надзвичайних ситуацій;

– розроблення та впровадження механізму для забезпечення надходження до Урядової інформаційно-аналітичної системи необхідних даних від міністерств та інших центральних органів державної виконавчої влади.

УІАС НС призначена для інформаційно-аналітичної підтримки процесів підготовки, прийняття та контролю управлінських рішень стосовно надзвичайних ситуацій (НС).

За допомогою УІАС НС вирішуються такі завдання:

– інформування та моніторинг;

– аналіз та прогнозування;

– планування заходів і підготовка рішень;

– контроль за виконанням рішень та заходів.

Структура УІАС НС представлена на рис. 1.29



Рис. 1.29 – Структура УІАС НС

1.7.1 Призначення та побудова геоінформаційної складової УІАС НС

Необхідність удосконалення інформаційних систем, що забезпечують прийняття рішень на державному рівні викликало розвиток та впровадження геоінформаційних ресурсів. Використання ГІС-технологий для забезпечення урядових інформаційних систем навіть позначено у світовій практиці спеціальним терміном "G-Government" (як елемент системи "E-Government" – "електронний уряд"), що підкреслює особливості цієї сучасної й ефективної форми роботи з просторовою інформацією (рис. 1.30).

В Україні одним з важливих кроків у цьому напрямку стало створення УІАС НС.

УІАС НС створена для забезпечення міжвідомчої інформаційної взаємодії та аналітичної підтримки прийняття рішень на основі сучасних методів просторового аналізу, моделювання розвитку надзвичайних ситуацій і прогнозування їхніх наслідків.

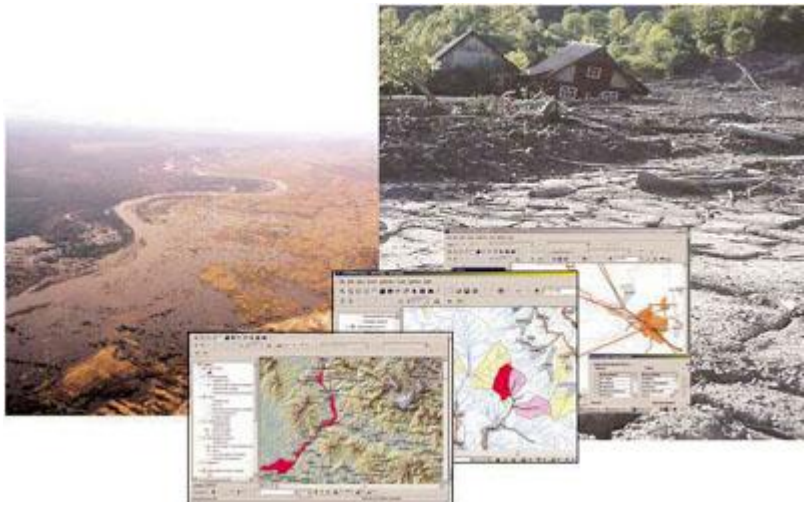


Рис. 1.30– Варіанти аналізу і представлення просторової інформації

Для реалізації настільки масштабних комплексних проектів потрібні чималі фінансові, організаційні й інтелектуальні ресурси. Тому одним з важливих моментів є розгляд місця і ролі геоінформаційних технологій і обґрунтування необхідності їхнього впровадження в загальну інформаційну структуру урядових систем.

Структура ГІС Виходячи з виконуваних функцій, дану інформаційну структуру можна представити у виді трьох блоків: збору даних, аналітичний, підтримки управлінських рішень (рис. 1.31).

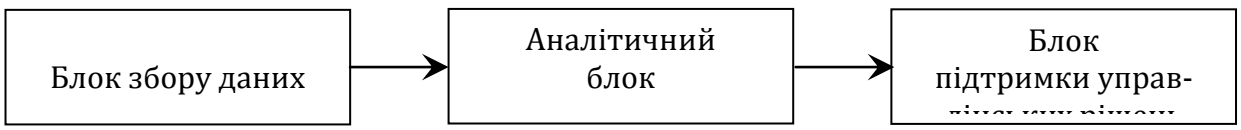


Рис. 1.31 – Структура геоінформаційної складової УІАС

Блок збору даних

Призначення. Цей блок відповідає за оперативне одержання і систематизацію даних з метою їхньої необхідної організації для наступного аналізу.

Світовий досвід показав, що інформаційна структура урядового рівня повинна спиратися на розподілені джерела інформації. У противному випадку забезпечити легітимність і актуальність даних для прийняття рішень буде украй важко. З огляду на це, у процесі створення УІАС НС забезпечується як міжвідомчий обмін електронними інформаційними ресурсами, так і загальне інформаційне середовище для взаємного спілкування державних органів: захищена телекомунікаційна мережа, електронна пошта, електронний документообіг і т.д.

*Джерела інформації.*Блок збору даних УІАС НС одержує й обробляє інформацію від ряду структур і відомств: ДСНС (БД повідомлень про надзвичайні ситуації); Український Гідрометцентр (БД гідрометеорологічної інформації); Міжвідомчий центр електронної картографії (МЦЕК), м. Харків (фонд електронних тематичних карт території України); ін-т Мікрографії, м. Харків (БД "Загальнодержавний реєстр потенційно небезпечних об'єктів") і т.д.

Яке ж місце геоінформаціоної складової в цьому процесі?

У першу чергу, це організація базових електронних карт місцевості і цифрових моделей рельєфу.

Потім – створення тематичних карт, що характеризують стан навколишнього середовища; карт розміщення мереж спостереження за природними і техногенними явищами; схем розподілу сил і засобів реагування на НС із прив'язкою потенційно небезпечних об'єктів і НС, що відбулися.

Ці операції найбільше ефективно виконуються за допомогою геоінформаційних технологій, хоча кожен елемент розподіленої інформаційної бази системи не повинний неодмінно створюватися на платформі ГІС.

Працювати усім в одному програмному середовищі, тим більше в ГІС, звичайно заманливо. Але сам факт забезпечення всіх співвиконавців навіть найсучаснішими ГІС– продуктами ще не означає автоматичного створення єдиного інформаційного середовища. Так, у випадку з УІАС НС, практично всю роботу з організації просторових даних на платформі ГІС могли б узяти на себе розроблювачі фонду електронних тематичних карт (МЦЕК). Виконати це побажання сьогодні заважає лише недолік фінансування.

Таким чином, необхідною умовою для створення блоку збору даних геоінформаційної інфраструктури є наявність хоча б одного розроблювача, що інтегрує просторову інформацію розподілених джерел на платформі ГІС.

Інші постачальники даних можуть передавати інформацію в доступному для них виді – таблиці, бази даних, цифрові карти і т.д., але відпові-

дно до загальних вимог розроблювачів центральної ГІС до організації просторової інформації.

Аналітичний блок

Призначення Аналітичний блок забезпечує аналіз вихідних даних і одержання якісно нової результуючої інформації у формі, оптимальної для підготовки управлінських рішень.

Склад Це визначає наявність у системі прогнозу надзвичайних ситуацій двох підблоків, що можуть бути просторово й організаційно розподілені між організаціями, що здійснюють аналіз і обробку даних:

– блок методик і алгоритмів обробки даних, зв'язаних з нормативно-правовим і методичним забезпеченням прогнозу і ліквідації наслідків НС;

– блок моделюючих систем, що здійснюють власне обробку даних на основі спеціалізованих програмно-технічних комплексів.

Для уніфікованої обробки інформації атрибутивних банків даних за прогнозом і ліквідацією наслідків НС необхідна розробка спеціалізованих регіональних і національних баз даних методик і алгоритмів, а також нормативно-правової інформації на основі застосування телекомунікаційних технологій. Це особливо важливо для регіональних інтегрованих систем міжвідомчого екологічного моніторингу, у структурі яких ряд однакових показників виміряється різними міністерствами й організаціями. Кроки в цьому напрямку вже починаються, але ще більше має бути зробити.

Вибір алгоритму прогнозування просторового розвитку й оцінки наслідків ЧС значною мірою визначається детальністю і повнотою інформації про об'єкт досліджень і його оточення. Досвід робіт зі створення Прогнозно-моделюючих комплексів прогнозування й оцінки наслідків надзвичайних ситуацій (ПМК НС), як аналітичної складової УІАС НС, допомагає виділити кілька типових проблем, що виникають при створенні загальної геоінформаційної інфраструктури.

Блок підтримки управлінських рішень

Механізми і методи автоматизованої підтримки управлінських рішень поки є найбільше слабкою ланкою в системах розглянутого типу.

Задача блоку є вибір оптимального рішення з декількох конкуруючих варіантів, підготовлених і візуалізованих у блоці обробки й аналізу даних.

Критерії оптимізації (пріоритет тактичного або стратегічного аспектів, орієнтація на максимальний економічний або соціальний ефект, вибір найбільш адекватних поставленої мети результатів і т.д.) у даний час практично не формалізовані. Їхній вибір поки визначений або життєвим досвідом особи, що приймає рішення, або корпоративними інтересами.

У цьому плані, такі елементи технології експертних систем, бази знань і бази метаданих, ще не одержали широкого розвитку в Україні.

Роль геоінформаційної складової, досягши максимуму в аналітичному блоці, на даному рівні знижується. Це не дивно, оскільки чиновник,

що приймає рішення на даному рівні, не має можливості освоювати всі технології, за допомогою яких сьогодні готується інформація про ситуації. Він і не повинний цього робити. Його основний інструмент – документ, отже й інформація повинна подаватися у виді документа. Тому мова повинна йти скоріше не про впровадження ГІС у верхній ешелон системи прийняття рішень, а про адаптацію системи електронного документообігу до повноцінного використання інформації, отриманої в результаті ГІС аналізу.

У той же час, на цьому етапі зростає роль наочного відображення всієї доступної просторової інформації про досліджувану надзвичайну ситуацію. Саме логіка візуального сприйняття часто допомагає відтворити цілісну картину явища. Способи відображення можуть використовуватися самі різні – від карт, схем і ілюстрацій до технологій "віртуальної реальності". Досить ефективно віртуальна реальність використовувалася при дослідженні приміщень 4-го блоку ЧАЕС, у яких після аварії перебування людини має бути вкрай обмежене або неможливе. При виборі оптимальних варіантів трас магістральних трубопроводів зазначена технологія дає можливість запросити необхідних експертів до екрана комп'ютера, а не в польову експедицію і, тим самим, заощадити значні засоби і час. Як приклад ефективності застосування ГІС на етапі прийняття рішень, на рис. 1.22 приведена візуальна оцінка прогнозованої зони затоплення 1% забезпеченості в заплаві р. Боржава (Закарпаття, Україна) з використанням технологій "віртуальної реальності", реалізованих у додатку ArcScene системи ArcGIS. Для відтворення актуального покриття землі використовувався космічний знімок Landsat 7. Зона затоплення отримана за даними прогнозування в ПМК НС (рис. 1.32).



Рис. 1.32 – Прогнозна зона затоплення 1% забезпеченості в заплаві р. Боржава

1.7.2 Проблеми створення та функціонування ГІС

Легітимність методичної бази

Обирані методики й алгоритми виконання аналітичних операцій у системах даного типу повинні не тільки забезпечувати рішення поставленої задачі, але і задовольняти жорстким умовам урядових систем, головне з яких – легітимність. Методики й алгоритми обробки даних за прогнозом НС повинні бути сертифіковані і затверджені уповноваженими органами. Однак нормативний дефіцит в області геоінформатики істотно ускладнює рішення цієї задачі.

Характерним наслідком зазначеної ситуації є, наприклад, примітивність алгоритму, прийнятого в ПМК НС для розрахунку зон поразки, зв'язаних з викидом забруднювачів в атмосферу. Фахівці України сьогодні мають у своєму розпорядженні досить точні моделі процесів переносу забруднювачів в атмосфері, здатними врахувати зміна напрямку конвективного переносу з висотою, турбулентність приземного шару атмосфери, можливість "залягання" викиду або виносу його на відносно безпечну висоту. Їхньої реалізації в УІАС НС сьогодні перешкоджають два основних фактори. По-перше, що відповідають алгоритми розраховані на використання прогнозних значень метеопараметрів, переданих по каналах АСПД зі світових метеорологічних центрів типу BRAKNELL або аналогічних йому розроблювачів мезомасштабних моделей, офіційним користувачем яких Україна не є. По-друге, жоден з даних алгоритмів ще не пройшов відповідного тестування, тобто не є легітимним.

З огляду на дану ситуацію, методичним керівництвом для розробки відповідного модуля ПМК НС стала методика, затверджена в ДСНС України в квітні 2001 року. У її основі лежать досить загрублені і застарілі підходи ЦО, що базуються на даних найближчої метеостанції. При цьому заздалегідь відомо, що отриманий результат буде далекий від оптимального, причому реально можливого (рис. 1.23). На цьому рис. 1.23 приведене порівняння інтегрованих у ГІС результатів моделювання міграції викиду в атмосферу, заснованих на даних, переданих з центра BRAKNELL (ліворуч), і реалізую методику, прийняту в ДСНС України (праворуч) (рис. 1.33).

Бази даних, методики і алгоритми в області прогнозу і реагування на НС поки не одержали широкого поширення. Подібна інформація існує, як правило, у паперовому виді, у формі розпорядницьких документів (наказів, методичних указівок, класифікаторів і т. п.), затверджених спеціально уповноваженими органами виконавчої влади.

Прикладом є постійно обновлювані гіпертекстові бази даних "Законодавство України", а також сайти або інформаційні портали органів влади (Парламенту України, Ради міністрів Автономної Республіки Крим, райдержадміністрації і т.д.). Однак ці бази даних поки не включають методик обробки даних, їхньої оцінки й алгоритмів просторового аналізу.

Виключення складають методичні документи міністерств і відомств, що пройшли реєстрацію в Мін'юсту України і його регіональних підрозділів. Крім того, в органах ЦНТІ досить активно переводяться на електронні носії значні обсяги Дст, СНИПов, технічних умов і т.д.

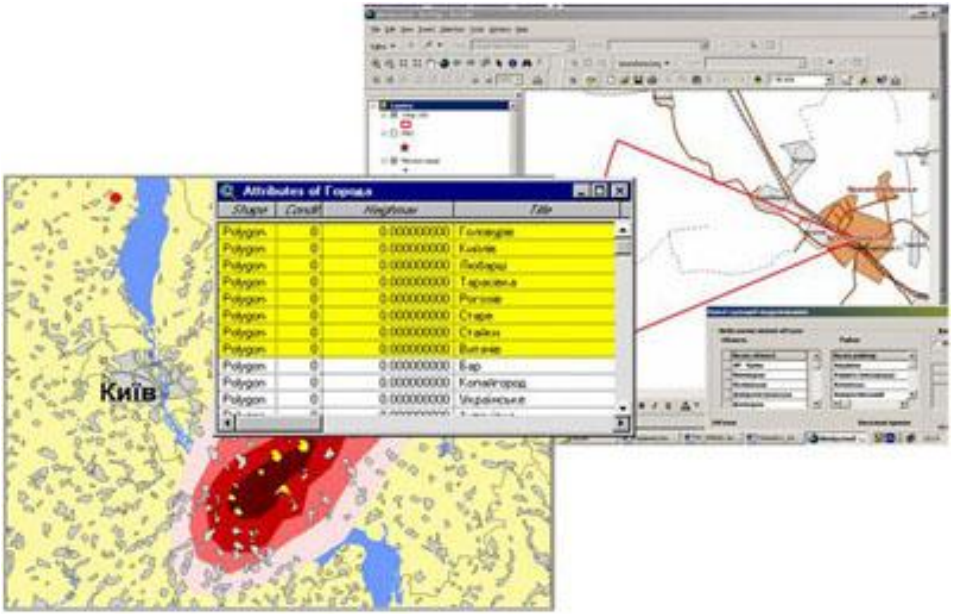


Рис. 1.33 – Порівняння результатів моделювання

Достатність (повнота) вихідних даних(фактор забезпеченості аналітичних систем вихідними даними).

Окремого розгляду заслуговує фактор забезпеченості аналітичних систем вихідними даними, що багато в чому визначає вибір алгоритму аналізу.

За даними Геологічної Служби США, тільки на території штату Північна Дакота, що регулярно страждає від паводкового затоплення, задіяно близько 6000 автоматизованих станцій комплексних гідрометеорологічних спостережень. Для порівняння, на території Закарпатської області (вона на порядок менше по площі, але на ній проживає вдвічі більше людей) знаходиться всього 8 метеостанцій, 2 автоматизованих і 36 неавтоматизованих гідропостів, зв'язок з якими під час розвитку екстремальних гідрометеорологічних ситуацій, як показує практика, ненадійна. Тобто, якість інформації, реально доступної по території України в період розвитку НС, робить неефективним, наприклад, застосування таких визнаних у світі комплексів гідрологічного моделювання, як HEC-RAS, SMS, MIKE-11 і ін.

Можливість складання гідрологічних прогнозів на цю частину території України сьогодні забезпечується застосуванням стохастичних залежностей, отриманих шляхом детального вивчення гідрологічного режиму кожної ріки. Прикладом системи, заснованої на алгоритмі такого

типу, є розроблений фахівцями УкрНІГМІ комплекс гідрологічного моделювання LEVEL_TS_M, що був прийнятий у якості зовнішнього моделюючого блоку ГІС до складу ПМК НС.

З огляду на сказане вище і реальні можливості інформаційно-аналітичних служб ДСНС України, розроблювачі ПМК НС йшли по шляху автоматизації найбільш наукомістких етапів цього процесу і виключення алгоритмів, особливо чутливих до дефіциту вихідних дані або потребуючі залучення фахівців.

Вибір способу програмної реалізації алгоритму

Також досить важливо зробити правильний вибір способу програмної реалізації алгоритму, що особливо включає в себе складні математичні операції.

У загальному випадку, по характеру взаємодії засобів просторового аналізу і моделювання з ГІС можна розділити на дві основні групи:

– власні засоби ГІС-платформ;

– зовнішні спеціалізовані моделюючі блоки, тим або іншим шляхом інтегровані з ГІС.

Прикладом спеціалізованого засобу першого типу є блок інструментів гідрологічного аналізу, що входить до складу модуля ArcGIS Spatial Analyst. Системи такого типу використовують вбудовані функції, що реалізують алгоритми розрахунку площі водозбору, виділення басейнів різних порядків, формування потоків, аналізу ухилів і т.п.

Добре зарекомендували себе також засіб просторового моделювання ГІС-платформ в області побудови цифрових моделей рельєфу, поверхонь забруднення, оцінки зон видимості, реалізації концептуальних моделей оцінки придатності території і т.д.

Проте треба розуміти, що за універсальність відомих Гіс-платформ приходиться розплачуватися істотним спрощенням розрахункових схем спеціалізованих функцій. Тому порівнювати можливості інструментарію даного типу і спеціалізованих моделюючих комплексів не зовсім коректно. Потрібно також враховувати, що основними перевагами ГІС є розвитий графічний інтерфейс і можливості просторового аналізу даних. Виконанню саме цих функцій підлегла ідеологія систем даного типу і можливості підтримуваних ними мов програмування.

У багатьох випадках значно більш ефективним є шлях інтеграції ГІС зі спеціалізованими моделюючими комплексами, що визначають другу групу аналітичних систем. Така взаємодія дозволяє з'єднати надійність, алгоритмічну широту й оперативність розрахункових блоків спеціалізованих моделюючих комплексів із властивої ГІС ефективністю засобів аналізу і відображення просторової інформації.

Роль ГІС при взаємодії такого роду звичайно зводиться до підготовки і схематизації просторової інформації, моделюванню рельєфу місцевості і необхідних нетопографічних поверхонь, формуванню файлу обмі-

ну з зовнішнім моделюючим комплексом, а також просторовому аналізові і відображенню результатів моделювання (рис. 1.34).

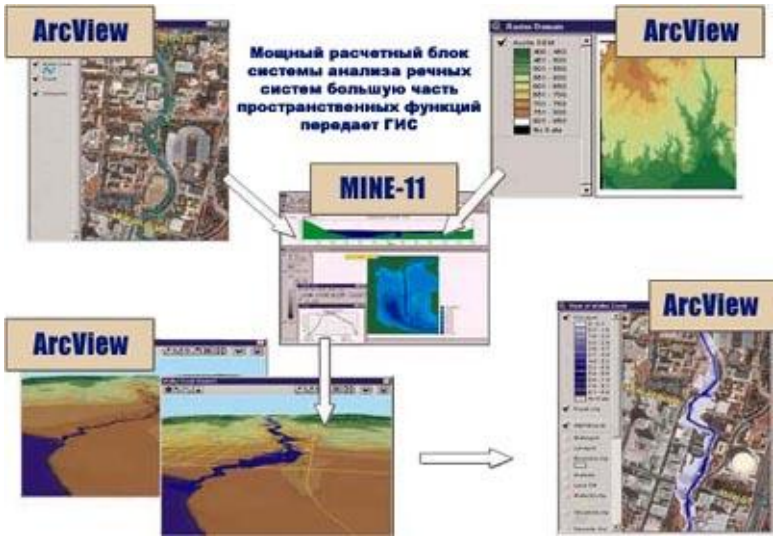


Рис. 1.34 – Приклад взаємодії ГІС і зовнішнього моделюючого блоку

1.8 Єдина інформаційна система Міністерства внутрішніх справ та перелік її пріоритетних інформаційних ресурсів

Положення визначає структуру, загальні засади функціонування єдиної інформаційної системи МВС, регулює порядок її формування та використання.

Єдина інформаційна система МВС – багатофункціональна інтегрована автоматизована система, що безпосередньо забезпечує реалізацію функцій її суб'єктів, інформаційну підтримку та супроводження їх діяльності і становить сукупність взаємозв'язаних функціональних підсистем, програмно-інформаційних комплексів, програмно-технічних та технічних засобів телекомунікації, які забезпечують логічне поєднання визначених інформаційних ресурсів, обробку та захист інформації, внутрішню та зовнішню інформаційну взаємодію [7].

Функціональні підсистеми єдиної інформаційної системи МВС – це сукупність технічних засобів та програмних комплексів, які автоматизують службові процеси суб'єктів єдиної інформаційної системи МВС до рівня стандартів операційних процедур та автоматизованого робочого місця користувача, забезпечують формування, зберігання, спільне використання і верифікацію інформаційних ресурсів єдиної інформаційної системи МВС.

Суб'єкти єдиної інформаційної системи МВС – апарат МВС та його територіальні органи з надання сервісних послуг МВС, Національна гвардія, заклади, установи і підприємства, що належать до сфери управління МВС (далі – система МВС), центральні органи виконавчої влади, діяльність

яких спрямовується і координується Кабінетом Міністрів України через Міністра внутрішніх справ, інші державні органи, які обробляють інформацію в єдиній інформаційній системі МВС для реалізації своїх повноважень.

Інформаційні ресурси єдиної інформаційної системи МВС – визначені групи взаємозв'язаних задокументованих одиниць інформації, які формуються і об'єднуються в автоматизованих інформаційних системах суб'єктів єдиної інформаційної системи МВС за певними ознаками, у тому числі зазначені в переліку пріоритетних інформаційних ресурсів єдиної інформаційної системи Міністерства внутрішніх справ, затвердженому постановою Кабінету Міністрів України від 14 листопада 2018 р. № 1024.

Інтеграція інформаційних ресурсів єдиної інформаційної системи МВС – комплекс методів та процедур, спрямованих на логічне функціональне об'єднання інформаційних ресурсів єдиної інформаційної системи МВС у визначених форматах, за узгодженими показниками, для їх автоматизованої обробки, використання та надання користувачам в уніфікованому вигляді.

Користувачі єдиної інформаційної системи МВС – фізичні особи та уповноважені посадові особи суб'єктів єдиної інформаційної системи МВС, яким в установленому порядку надано відповідні права доступу до інформації в єдиній інформаційній системі МВС.

Сервіс єдиної інформаційної системи МВС – спеціальний програмний засіб, що забезпечує доступ користувачів єдиної інформаційної системи МВС до інформаційних ресурсів єдиної інформаційної системи МВС.

Єдина інформаційна система МВС функціонує з метою оптимізації інформаційної взаємодії суб'єктів єдиної інформаційної системи МВС на рівні загальнодержавних інформаційних ресурсів в інтересах національної безпеки, захисту прав та законних інтересів громадян, суспільства і держави у сферах:

цивільного захисту, захисту населення і територій від надзвичайних ситуацій та запобігання їх виникненню, ліквідації наслідків надзвичайних ситуацій, рятувальної справи, гасіння пожеж, пожежної та техногенної безпеки, діяльності аварійно-рятувальних служб, а також гідрометеорологічної діяльності;

Єдина інформаційна система МВС складається з постійно діючих:

центральної підсистеми;

функціональних підсистем;

транспортної мережі передачі даних;

центрів обробки даних, телекомунікаційних мереж суб'єктів єдиної інформаційної системи МВС;

комплексних систем захисту інформації підсистем єдиної інформаційної системи МВС з підтвердженою в установленому законодавством порядку відповідністю.

Центральна підсистема єдиної інформаційної системи МВС – обчислювальне середовище функціонування автоматизованих сервісів, яке забезпечує безперервність їх обслуговування в інтерактивному режимі реального часу та високий рівень продуктивності.

Центральна підсистема єдиної інформаційної системи МВС функціонує в основному та резервному центрах обробки даних, які забезпечують середовище для її роботи.

До складу центральної підсистеми єдиної інформаційної системи МВС входять:

центральне сховище даних – програмно-технічний комплекс, який складається із серверів баз даних та програмного забезпечення, призначених для безперервної обробки та зберігання інформації, ведення та зберігання системних журналів аудиту роботи користувачів єдиної інформаційної системи МВС, системних журналів реєстрації роботи програмних засобів і журналів аудиту засобів безпеки;

центральний сервер обробки даних – програмно-технічний комплекс, який складається з основного та резервних серверів, баз даних, програмного забезпечення, призначених для безперервного виконання операцій з інформаційного обміну між центральним сховищем даних та суб'єктами і користувачами єдиної інформаційної системи МВС, записування та зберігання системних журналів аудиту приймання-передачі інформації;

сервери додатків – програмно-технічні комплекси, які складаються із серверів та програмного забезпечення, призначених для безперервного функціонування програмних засобів обробки інформації в інтерактивному режимі реального часу, архівування та синхронізації інформації, записування та зберігання системних журналів аудиту приймання-передачі інформації, реєстрації роботи програмних засобів і журналів аудиту засобів безпеки;

шлюзові сервери – програмно-технічні комплекси, які складаються із серверів та програмного забезпечення, призначених для забезпечення захисту інформації під час її приймання та передавання до центрального сховища даних, а також для запобігання можливості блокування доступу до програмно-апаратних ресурсів єдиної інформаційної системи МВС;

інші сервери та телекомунікаційне обладнання, які можуть використовуватися в разі розширення завдань та функцій єдиної інформаційної системи МВС у процесі її роботи;

автоматизовані робочі місця користувачів центральної підсистеми єдиної інформаційної системи МВС – робочі місця, обладнані програмно-технічними засобами доступу до відповідних програмно-інформаційних комплексів функціональних підсистем єдиної інформаційної системи МВС, призначені для забезпечення користувачам можливості обробляти інформацію відповідно до наданих прав;

автоматизовані робочі місця адміністраторів центральної підсистеми єдиної інформаційної системи МВС – робочі місця, обладнані технічними засобами та програмним забезпеченням, призначеними для моніторингу системних журналів реєстрації роботи програмних засобів, аналізу порушень у роботі єдиної інформаційної системи МВС, налагодження параметрів, необхідних для забезпечення стабільної роботи програмних та технічних засобів центральної підсистеми єдиної інформаційної системи МВС;

автоматизовані робочі місця адміністраторів безпеки єдиної інформаційної системи МВС.

Функціональними підсистемами єдиної інформаційної системи МВС є:

національна система біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства;

інформаційний портал Національної поліції України;

Єдиний державний реєстр транспортних засобів;

Реєстр адміністративних правопорушень у сфері безпеки дорожнього руху;

система фіксації адміністративних правопорушень у сфері забезпечення безпеки дорожнього руху в автоматичному режимі;

система екстреної допомоги населенню за єдиним телефонним номером 112;

інтегрована міжвідомча інформаційно-телекомунікаційна система щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон;

інформаційно-телекомунікаційна система прикордонного контролю “Гарт-1”;

інші системи, реєстри та бази (банки) даних, створені суб’єктами єдиної інформаційної системи МВС в межах реалізації владних повноважень.

Структура та порядок роботи функціональних підсистем єдиної інформаційної системи МВС визначаються положеннями про ці підсистеми, які розробляються суб’єктами єдиної інформаційної системи МВС з урахуванням затвердженого МВС Типового положення про функціональну підсистему єдиної інформаційної системи МВС та затверджуються в установленому законодавством порядку.

Транспортна мережа передачі даних – це універсальна мережа, що реалізує функції транспортування/комутації та об’єднує окремі мережі доступу із забезпеченням транзиту трафіку між ними високошвидкісними каналами.

Комплексні системи захисту інформації забезпечують захист інформації в підсистемах єдиної інформаційної системи МВС шляхом здійснення комплексу технічних, криптографічних, організаційних та інших

заходів і використання засобів захисту інформації, спрямованих на недопущення блокування доступу до інформації, несанкціонованого ознайомлення з нею та/або її модифікації.

Пріоритетні інформаційні ресурси єдиної інформаційної системи Міністерства внутрішніх справ (Суб'єкт єдиної інформаційної системи МВС – ДСНС):

реєстр атестованих аварійно-рятувальних служб;

зареєстровані надзвичайні ситуації, у тому числі пожежі.

1.9 Автоматизована система оперативно-диспетчерського управління

1.9.1 Призначення, завдання, можливості автоматизованої системи оперативно-диспетчерського управління

Автоматизована система оперативно-диспетчерського управління (СОДУ) є територіальною підсистемою Урядової інформаційно-аналітичної системи ліквідації надзвичайних ситуацій (УІАСНС) [1-8, 12].

СОДУ призначена для максимальної автоматизації основних функцій оперативно-диспетчерського управління та є інтегруючим інформаційним програмно-технічним комплексом для створення єдиної геоінформаційної системи (далі – ГІС) управління та моніторингу з можливістю передачі інформації в реальному часі від чергових підрозділів до СІЗ.

СОДУ повинна забезпечувати:

надійний прийом, передачу, реєстрацію, обробку і аналіз всієї інформації, яка відноситься до службово-оперативної діяльності, управління підпорядкованими силами постійної готовності та взаємодію з іншими диспетчерськими службами екстреного виклику;

ведення інформаційних баз даних і формування інформаційних та статистичних звітів.

Роль і місце СОДУ в автоматизації діяльності ДСНС України на етапах профілактики, підтримання у готовності сил та засобів, реагування та ліквідація наслідків НС представлено на схемі рис.1.35.

Задачі управління силами та засобами повинні вирішуватися на основі оперативної взаємодії диспетчерів СОДУ. Функції підсистеми і відповідні програмні комплекси повинні бути розподілені між сервером СОДУ, автоматизованими робочими місцями диспетчерів оперативно-диспетчерської служби та автоматизованими робочими місцями диспетчерів ПЗЧ.

Метою провадження СОДУ є максимальна автоматизація диспетчерських функцій, скорочення термінів обробки викликів та висилки техніки, що є вирішальним фактором при ліквідації НС, рятуванні людей.

Реєстрація, обробка викликів та висилка аварійно-рятувальної техніки (АРТ) здійснюється з використанням програмно-апаратного ком-

плексу (ПАК) СОДУ, який в 2007 році вперше на Україні було впроваджено в експлуатацію в м. Львові. Диспетчерська зала СОДУ наведена на рис.1.36.



Рис. 1.35 – Схема автоматизації діяльності ДСНС

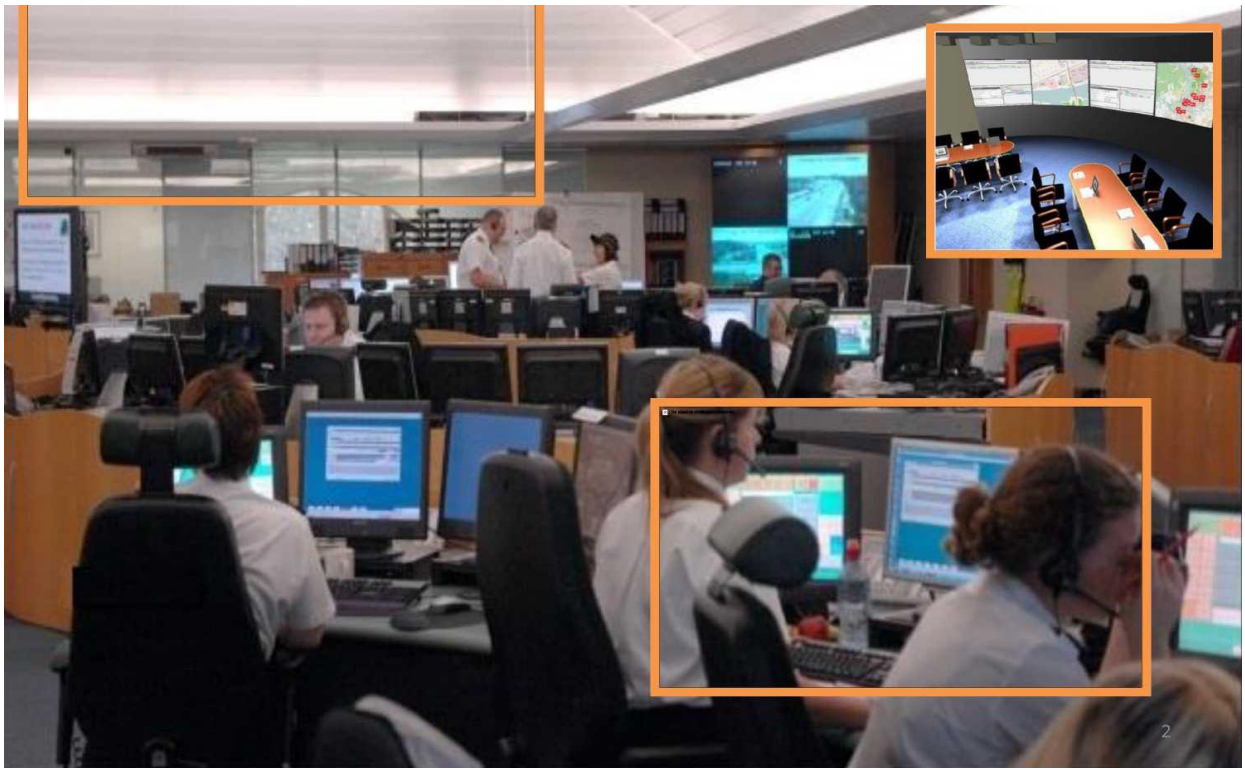


Рис. 1.36 – Диспетчерська зала СОДУ

З врахуванням побажань оперативно – диспетчерської служби фахівцями ГУ ДСНСЛьвовской обл. за часи експлуатаціїбуло допрацьовано програмне забезпечення, а саме:

– удосконалено інтерфейс автоматизованих робочих місць диспетчерів;

– проведено актуалізацію картографічного матеріалу міста Львова;

– впроваджено систему геопозиціонування основної аварійно-рятувальної техніки м. Львова;

– впроваджено додаткові програмні модулі алгоритму дій диспетчера, діагностики роботи системи та стану каналів зв’язку, розрахунку маршрутів руху аварійно-рятувальної техніки;

– доопрацьовано модуль обліку наявності гідрантів, їх технічний стан, розташування на карті;

– з метою збільшення пропускної спроможності наявних каналів зв'язку (передачі даних, автоматизованої висилки сил та засобів) модернізовано відомчу VPN комп'ютерну мережу та організовано додатково по 2 канали IP телефонії з підрозділами області;

– розроблено та встановлено новий програмний геоінформаційний сервер.

Впровадження ПАК СОДУ дозволило максимально автоматизувати роботу оперативно – диспетчерської служби під час реєстрації, обробки викликів та висилки аварійно-рятувальної техніки до місця події.

Протягом 2007-2016 років розроблено та впроваджено в практичну діяльність програмне забезпечення обліку речового майна, використаних енергоносіїв, наявності і технічного стану гідрантів та інтегровано його з системою оперативно-диспетчерського управління.

З метою забезпечення надійного функціонування СОДУ, збільшення пропускної спроможності каналів зв’язку підключено телекомунікаційну мережу ГУ ДСНС України у Львівській області до телекомунікаційної мережі спеціального призначення (ТМСП) Державної служби спеціального зв’язку(ДССЗ) України. Отримано дозвіл ДССЗ України на підключення інформаційно-телекомунікаційних мереж підрозділів області до ТМСП. Управлінням Держспецзв’язку України у Львівській області та ПАТ «Укртелеком» надано технічні умови на підключення телекомунікаційної мережі ГУ ДСНС України у Львівській області та п’яти підпорядкованих підрозділів області (м. Стрий, м. Броди, м. Трускавець, м. Кам’янка-Бузька, м.Яворів) до телекомунікаційної мережі спеціального призначення. Придбано волоконно-оптичний кабель (ВОЛ) та мережеве обладнання для підключення 4-х підрозділів області до ТМСП, прокладено ВОЛ до ТМСП в двох підпорядкованих підрозділах області(м. Стрий та м. Трускавець).

З метою підвищення ефективності управління силами і засобами, забезпечення її функціонування на безоплатних системах з відкритим кодом протягом 2017 року передбачено модернізацію даного ПАК.

У оперативній діяльності ОДС ОКЦ ГУ ДСНС України у Харківській області обмежено використовується геоінформаційна система «ГІС ПО» через застаріле картографічне забезпечення.

Розроблене ПЗ містить дві бази даних і одну базу знань.

ГІС дозволяє відображати на дисплеї та аналізувати оточуючу обстановку на місті НС.

В якості картографічного забезпечення пропонується використовувати карти від компанії «Google», які періодично оновлюються.

Модуль підтримки прийняття рішень автоматизованої системи включає бази даних знань (Knowledgebase) і базу даних (DataBase), підсистему вибору сценарію дій (Механізм виводу).

Система може працювати з Web-ГІС підсистемою геопросторових даних з відкритим вихідним кодом.

У першій базі даних зберігаються дані про чисельність ПРП, місця їх дислокації і райони обслуговування, джерела протипожежного водопостачання.

У другій базі даних зберігаються оперативні дані про НС, які виникали на території міста Харкова.

У базі знань розміщені методи і алгоритми, які дозволяють визначити необхідну кількість та тип оперативних відділень, а також місця дислокації пожежно-рятувальні підрозділи (ПРП) із яких вони будуть направлятися в залежності від особливостей НС і місця її виникнення.

За допомогою вирішувача відбувається визначення необхідної кількості та типів ПРА, які необхідні для обслуговування виклику, а також формування і відправка дорожнього листа на виклик до ПРП із зазначенням рекомендованого маршруту прямування пожежних та/або аварійно-рятувальних автомобілях (ПРА).

Дані, отримані безпосередньо ОДС ОКЦ, забезпечують їх достовірність і повноту, а це дає можливість на основі отриманого аналізу сформувати чіткі прогнозні моделі виникнення НС.

Розроблене програмне забезпечення для ОДСОКЦ ГУ ДСНС України у Харківській області дозволить скоротити час оброблення повідомлень про НС черговими диспетчерами, а врахування дорожньої обстановки при формуванні маршруту прямування сил та засобів ПРП дозволить скоротити час прибуття їх на виклик.

У подальшому планується розробити прогнозну модель виникнення НС на території міста та доповнити нею вже розроблене програмне забезпечення.

1.9.2 Технічні вимоги до програмно-апаратного комплексу СОДУ

Розглянемо проект з модернізації системи СОДУ силами та засобами ДСНС України, як функціональної підсистеми Єдиної інформаційної системи МВС України.

Призначенням проекту є підвищення оперативності та якості прийняття рішень при організації ліквідації наслідків надзвичайних ситуацій, аварій, катастроф, стихійного лиха, гасіння пожеж, рятування людей у підрозділах ДСНС України з використанням новітніх комп'ютерних технологій, телекомунікаційних та геоінформаційних систем.

СОДУ, як функціональна підсистема Єдиної інформаційної системи МВС України призначена для максимальної автоматизації основних функцій оперативно-диспетчерського управління.

СОДУ є складовою системи екстреної допомоги населенню за єдиним телефонним номером «112» та повинна забезпечити:

– оперативну і своєчасну обробку повідомлень про пожежі та інші надзвичайні ситуації від населення, Системи 112, їх аналіз і ініціацію необхідних заходів по ліквідації надзвичайних ситуацій;

– інтеграцію з єдиною інформаційною системою (ЄІС) МВС України для надання необхідних інформаційних даних щодо наявних сил та засобів ДСНС України і оперативної обстановки;

– надання в реальному часі оперативної інформації керівництву ДСНС України та МВС України для планування та управління об'єднаними силами по ліквідації надзвичайних ситуацій та забезпеченню громадської безпеки;

– створення єдиної геоінформаційної системи (далі – ГІС) управління та моніторингу з можливістю передачі інформації в реальному часі від чергових підрозділів та безпосередньо з місць ліквідації надзвичайних ситуацій до ЄІС МВС України та кризового центру ДСНС України;

–інформаційне забезпечення функціонування системи оперативно-диспетчерського управління, а саме координацію та контроль роботи всіх ланок єдиної системи запобігання і реагування на надзвичайні ситуації техногенного та природного характеру, управління підрозділами постійної готовності ДСНС України та взаємодію з іншими екстреними та аварійними службами при виконанні ними поточних і оперативних задач;

– реєстрацію наказів, повідомлень і переговорів по службових лініях і радіоканалах, накопичення і ведення архіву звернень, інформації про надзвичайні ситуації і здійснені заходи і відповідності до вимог (об'єм і термін зберігання);

– надання консультацій населенню при виникненні надзвичайних ситуацій та небезпечних подій.

Система повинна:

1.Забезпечити можливість інформаційної взаємодії з іншими автоматизованими інформаційними системами, що існують чи розроблюються в структурах державного керівництва, Системою 112 на рівні програмних інтерфейсів, баз даних, форматів інформаційного обміну тощо.

2. Базуватися на стандартній операційні системі та використовувати для роботи з даними промислову СУБД.

3. Базуватися на апаратних продуктах відкритого стандарту і не включати якого-небудь специфічного виробника апаратури.

4. Мати резервування апаратної частини, програмного забезпечення, баз даних і працювати з дублюванням в реальному часі.

5. Бути повністю інтегрована система, що включає підтримку телефонії обробки та передачі даних.

6. Забезпечити можливість використання з автоматизованого робочого місця оператора всіх функцій системи, як приклад, прийом телефонних викликів, диспетчеризація, управління ресурсами, тощо.

7. Передбачати лінійне масштабування – від малої системи до системи національного масштабу.

8. Бути готовою до позиціонування абонентів мобільного зв'язку.

9. Мати можливість працювати за будь-якими завчасно створеними алгоритмами дій.

10. Бути спроектована для використання 24 години на добу, 7 днів на тиждень, 365 днів у році.

11. Забезпечити цілісність інформації шляхом створення комплексної системи захисту інформації (вимоги та проведення комплексної системи захисту інформації розробляються та проводяться за окремими угодами).

За допомогою СОДУ повинна забезпечуватися взаємодія з питань ЦЗ інформаційної системи ДСНС, системи моніторингу з інформаційними системи суміжних установ через систему зв'язку та оповіщення ДСНС та суміжні системами зв'язку, як вказано на схемі рис. 1.37.

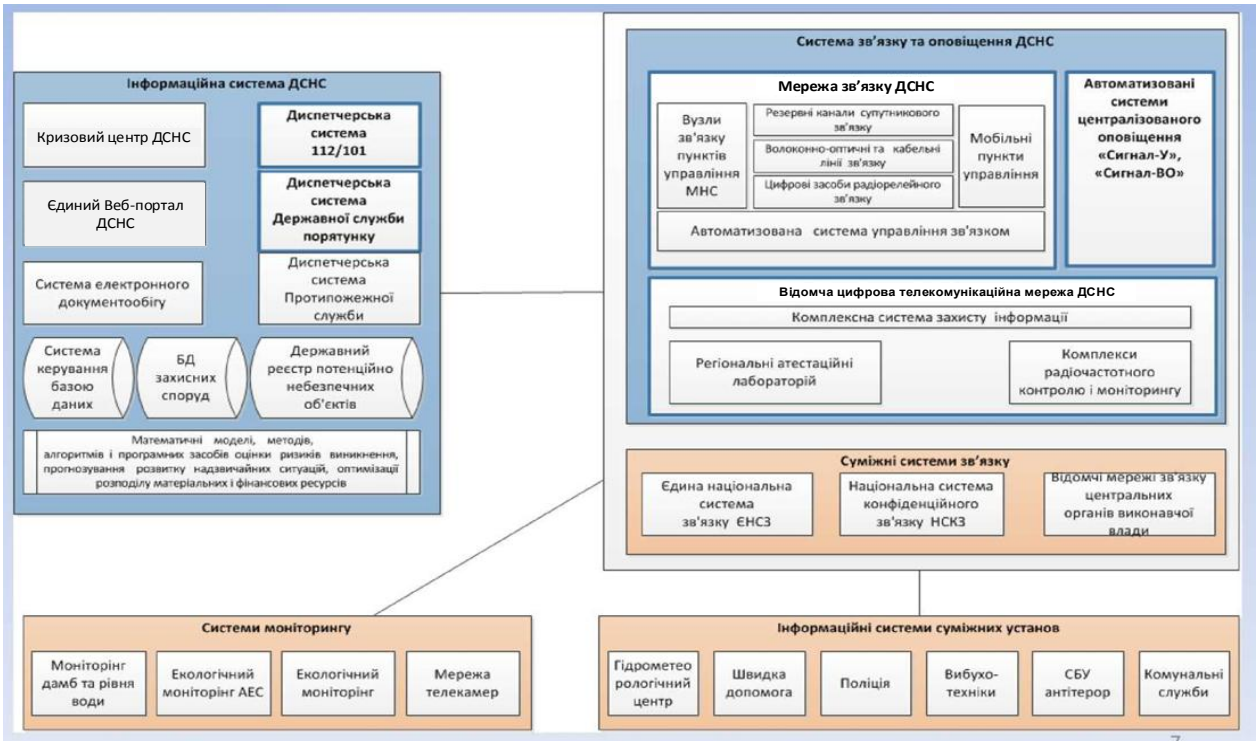


Рис. 1.37 – Схема організації зв'язку та взаємодії СОДУ з суміжними АС

– Інформаційна система ДСНС об'єднує в АС обміну інформацією між структурними підрозділами і програмним забезпеченням наступні елементи:

– Кризовий центр ДСНС
– Єдиний Веб-портал ДСНС
– Система електронного документообігу
– Диспетчерська система 112/101
– Диспетчерська система Державної служби порятунку
– Диспетчерська система Протипожежної служби
– Система керування базою даних
– БД захисних споруд
– Державний реєстр потенційно небезпечних об'єктів
– Математичні моделі, методів, алгоритмів і програмних засобів оцінки ризиків виникнення, прогнозування розвитку надзвичайних ситуацій, оптимізації розподілу матеріальних і фінансових ресурсів.

СОДУ повинна забезпечувати наступні функціональні можливості:

1) Прийом і реєстрацію заявок про НС та НП:

– в автоматизованому режимі при наявності доступу до відповідних баз даних (визначення та відображення просторового місцезнаходження стаціонарних абонентів з використанням автоматичного визначника номера та прийом сигналів від СЦПТС).

– в ручному режимі (прийом адреси і/або назви об’єкта по телефону і введення їх з клавіатури в автоматизовану систему);

2) Автоматичне формування пропозицій по бойовому розрахунку необхідних сил та засобів з врахуванням часу їх прибуття до місця події;

3) Мінімізацію часу прийняття диспетчером кінцевого рішення щодо висилки сил та засобів на основі автоматично сформованої системою пропозиції бойового розрахунку;

4) Перевірку складу бойового розрахунку, при необхідності його корегування, формування бойового наказу.

5) Передачу бойового наказу на виїзд бойової техніки в підпорядковані підрозділи, отримання підтвердження його виконання (для підрозділів обласного центру).

6) Формування протоколу часу виїзду техніки підрозділів.

7) Інформування про виконання бойового наказу керівництва, відповідальних посадових осіб гарнізону, міських аварійних та відомчих служб, інших зацікавлених служб та посадових осіб.

8) Реєстрацію повідомлень від підрозділів про оперативну обстановку на місці події та хід ліквідації НС (НП), отриманих диспетчером по радіомережі;

9) Формування і передача по СКМ інформації щодо досилки, часткового повернення, повного повернення техніки з місця події, отримання підтвердження про виконання наказу підрозділами.

10) Прийом інформації та ведення протоколу всіх повідомлень з місця НС(НП), досилку диспетчером в інтерактивному режимі основної, спеціальної та допоміжної техніки, особового складу, сил та засобів відомчих і міських служби взаємодії (швидка допомога, міліція, газ, водоканал, енерго, тощо).

11) Реєстрацію повідомлень з підрозділів про повернення техніки в місця постійної дислокації.

12) Прийняття та при необхідності корегування формалізованого звіту про НС(НП) з підрозділів.

13) Контроль за всіма виїздами і поверненнями техніки в розташування підрозділів.

14) Формування стройової записки від кожного підрозділу, яка включає: кількість особового складу рядового і керівного, присутнього і відсутнього (з зазначенням причин); кількість аварійно-рятувальної техніки за типами; дані по газозахисній службі; кількість пального; кількість піноутворювача та ін. і введення її в базу даних;

15) По закінченні добового чергування підготовку і друкування короткого добового звіту для доповіді керівництву (добове зведення).

16) Можливість використання підсистеми оповіщення особового складу гарнізону для збору по тривозі при НС, за сигналам цивільної оборони, інших особливих випадках з ідентифікацією голосу абонента та парольним підтвердженням доставки голосового повідомлення.

17) Формування і видачу абсолютних і з наростаючим підсумком результатів оперативної роботи за добу, тиждень, місяць, квартал, півріччя, рік за встановленими формами і окремими довідками.

18) Можливість формування повідомлень та аналітичних звітів і передача формалізованих даних до Системи 112.

19) Формування та передача до ЦП звітних даних для сегменту "Сили та засоби".

Функціонально СОДУ складається з Call-центру, підсистеми оповіщення і диспетчерської системи, які виконують завдання вказані на рис 1.38.

Call-центр виконую наступні завдання:

– прийняття та оброблення екстрених викликів;

– аудіо запис екстрених викликів та збереження аудіо записів;

– розподіл викликів з урахуванням категорії абонентів (їх важливості), між операторами;

– інформування оператора, надання відомостей (з відповідної бази даних) про абонента, який зробив виклик, та про кількість абонентів у черзі;

– керування чергами обслуговування у разі зайнятості операторів відповідно до визначених категорій обслуговування з урахуванням можливості позачергового обслуговування;

– ведення обліку та формування статистичної звітності, зберігання інформації про екстрені виклики;

– отримання інформації з БД операторів фіксованого телефонного зв'язку (прізвище, ім’я, по батькові, найменування та адреса);

– отримання інформації з БД операторів мобільного зв'язку (абонентський номер та місцезнаходження на момент здійснення екстреного виклику.

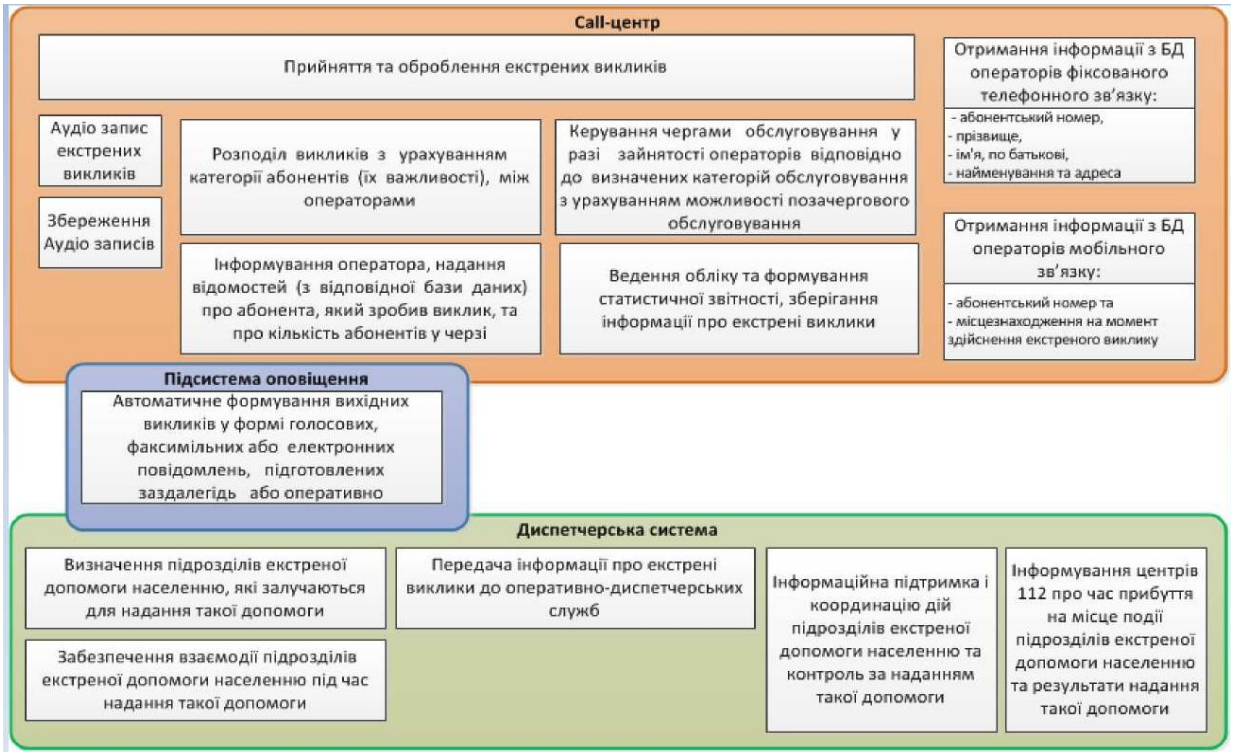


Рис. 1.38 – Функціональна схема СОДУ

Підсистема оповіщення виконує автоматичне формування вихідних викликів у формі голосових, факсимільних або електронних повідомлень, підготовлених заздалегідь або оперативно.

Диспетчерська система виконує наступні завдання:

– визначення підрозділів екстреної допомоги населенню, які залучаються для надання такої допомоги;

– забезпечення взаємодії підрозділів екстреної допомоги населенню під час надання такої допомоги;

– передача інформації про екстрені виклики до оперативно-диспетчерських служб;

– інформаційна підтримка координацію дій підрозділів екстреної допомоги населенню та контроль за наданням такої допомоги;

– інформування центрів 112 про час прибуття на місце події підрозділів екстреної допомоги населенню та результати надання такої допомоги.

СОДУ вміщує в собі з чотири АС рис. 1.39:

– систему відображення ситуації;
– логістичну систему;
– диспетчерську систему;
– систему інформування населення.



Рис. 1.39 – Схема автоматизації СОДУ

В свою чергу ***логістична система*** поділяється на автоматичну маршрутизацію транспортних засобів (AVR), автоматичнестеження за транспортними засобами (AVL) та вибір кращого маршруту транспортного засобу(AVRR).

Система відображення ситуації оперуєданими відеоспостереження, зокрема інцидентів татранспортнихзасобів на мапі GIS.

Диспетчерська система складається з:

– АС Call-центру;
– інтерактивного автовідповідача (IVR);
– системи диспетчеризації реагування на інцидент (CAD);
– автоматичного визначення номера абонента (ANI);
– автоматичного визначення місця розташування абонента (ALI);
– звітної системи.

Система інформування населення представлена WEB-порталом та додатками длямобільних користувачів.

Задачі управління силами та засобами повинні вирішуватися на основі оперативної взаємодії диспетчерів СОДУ.

Функції підсистеми і відповідні програмні комплекси повинні бути розподілені між сервером СОДУ, автоматизованими робочими місцями диспетчерів оперативно-диспетчерської служби та автоматизованими робочими місцями ПЗЧ.

Робочі місця підсистеми повинні бути забезпечені можливістю роботи з просторовими даними у вигляді електронних карт місцевості.

За аналогічними принципами також побудовані сучасні іноземні АСУ диспетчерськими службами в НС – аналоги СОДУ табл. 1.11.

Таблиця 1.11 – АСУ диспетчерськими службами в НС – аналоги СОДУ

Виробник	**Назва системи**	**Країна**
ORACLE	Oracle City Platform + iSafity by Indra	USA
Intergraph	I/CAD	USA
ESRI	ArcGIS for Emergency Management	USA
ООО «Телекомсофт»	АПК ЕДДС-Навигатор	Білорусія

Вимоги до складу програмного забезпечення

Система повинна передбачати три типи клієнтських автоматизованих робочих місць: чергового диспетчера (АРМ – Д), адміністратора системи (АРМ – А), диспетчера аварійно-рятувальних підрозділів (АРМ – ПЗЧ).

Всі типи АРМ'ів повинні взаємодіяти з сервером системи в ВЦТМ і складають ядро системи СІЗ СОДУ(рис. 1.40).

Сервер застосувань повинен бути реалізований у вигляді програм за технологією розподілених додатків та забезпечувати єдиний інтерфейс доступу до баз даних для спеціального програмного забезпечення клієнтських АРМ (СПЗ АРМ).

СПЗ АРМ'ів усіх типів повинно бути реалізовано за уніфікованою схемою взаємодії компонентів на основі набору об'єктів для роботи з базами аналітичними даних та єдиного менеджеру об'єктів. Для кожної бази аналітичних даних необхідно реалізувати відповідний об'єкт, який забезпечуватиме уніфіковану взаємодію з сервером застосувань, а отже і з сервером бази даних, та підтримуватиме екранні форми і елементи управління діалогового інтерфейсу користувача в складі СПЗ АРМ.

Вимоги до просторових даних

Просторові дані СОДУ повинні включати великомасштабні електронні карти населених пунктів, середньо– та мілко масштабні електронні карти області.

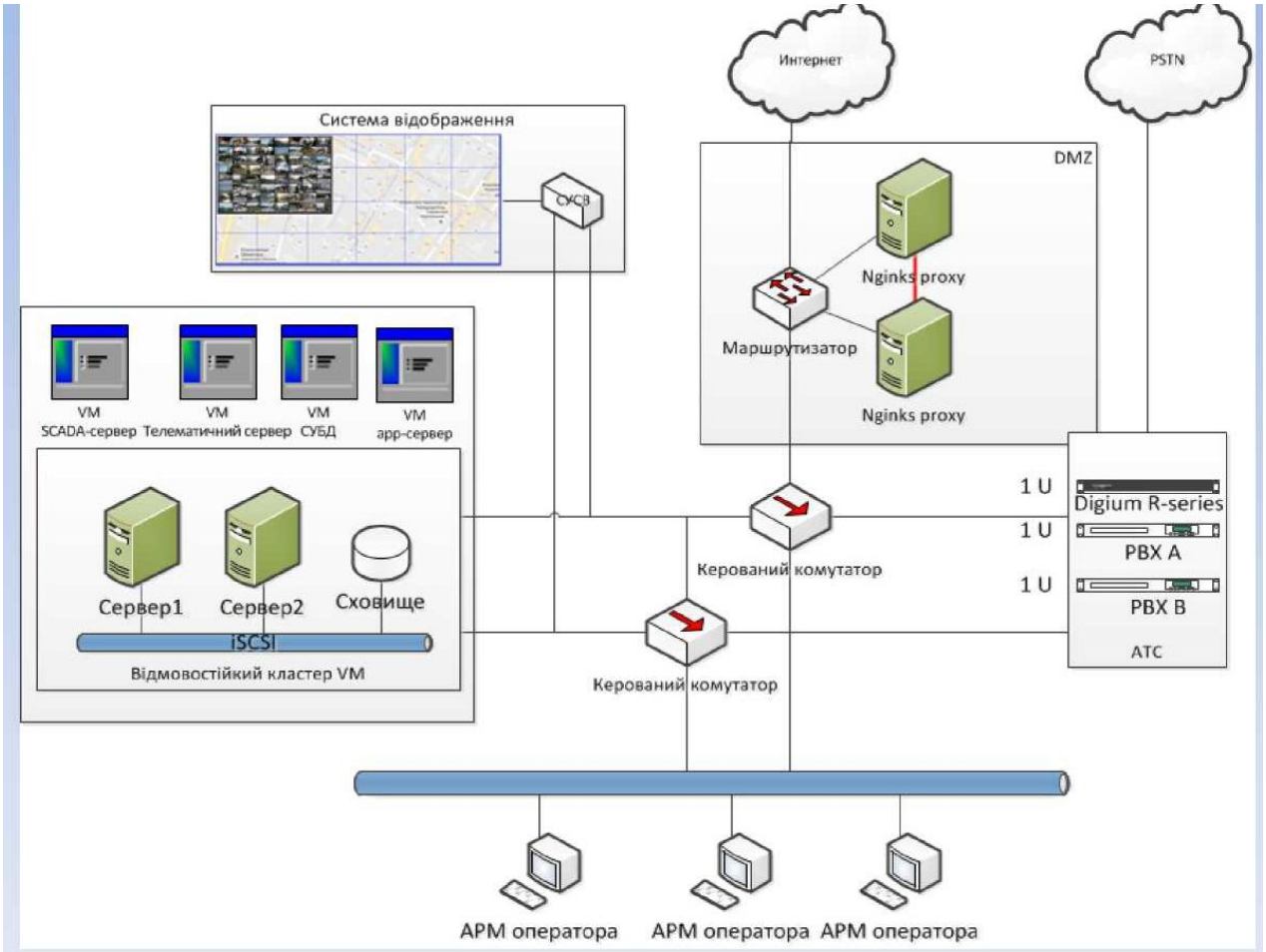


Рис. 1.40 – Схема структурна комплексу технічних засобів СОДУ

Вихідний масштаб використовуваних просторових даних повинен відповідати розв'язуваному завданню.

Просторові дані повинні бути представлені в системах координат, що дозволяють використовувати системи супутникового позиціонування.

Просторові дані повинні містити інформацію для рішення завдань маршрутизації й оптимізації переміщення сил і засобів.

Сховище просторових даних повинне бути пристосоване для зберігання растрових зображень місцевості, зокрема, супутникових знімків.

Вимоги до роботи із просторовими даними

При роботі із просторовими даними повинна бути забезпечена наступна функціональність:

– вибір електронної карти з набору карт, що є присутнім у складі СОДУ і перемикання між картами;

– позиціонування на карті, включаючи масштабування, плавне переміщення, позиціонування за допомогою «навігатора»;

– пошук пойменованих об'єктів, включаючи одиниці адміністративно-територіального розподілу України, іменовані проїзди, будови, місця НС і НП, сили й засоби, ПНО;

– відображення інформації про поточне положення курсору;

– одержання інформації про пойменовані об'єкти;

– побудова маршруту пересування по шляхово-транспортній мережі;

– позиціонування вікна карти на обраний оператором об'єкт із виділенням зазначеного об'єкта кольором, яскравістю або іншим добре видимим способом;

– формування відображень карти для одержання твердих копій і включення у звітно-інформаційні документи;

– прийом запиту на установку крапки й установку крапки на ЕК із передачею координат програмі, що запросила;

– взаємодія із суміжним ПЗ на основі Socket TCP/IP, за допомогою спеціального протоколу обміну.

Діалогові вікна і алгоритм обробки звернення в ПАК СОДУ додані на рис. 1.41 – 1.44.

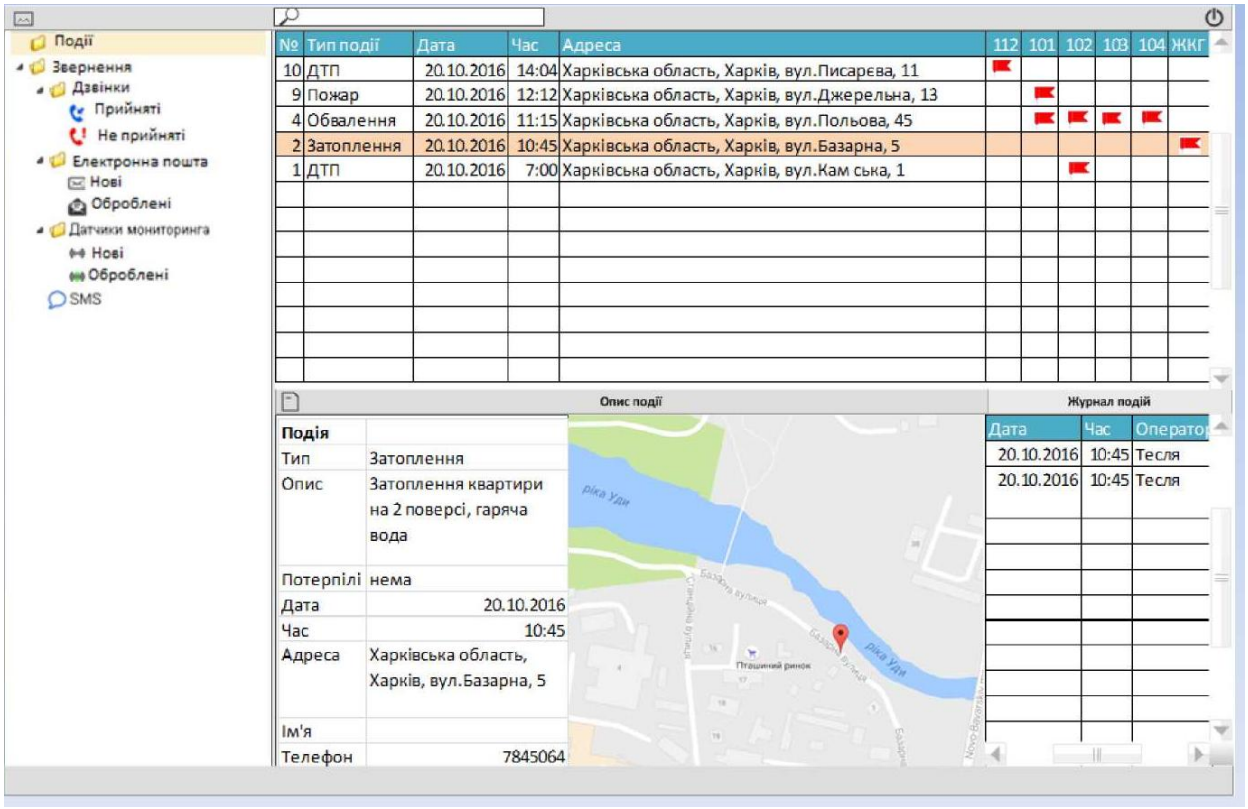


Рис. 1.41 – Діалогове вікно ПАК СОДУ "Список подій"

Вимоги до програмного забезпечення.

Системне програмне забезпечення повинне включити промислову систему управління базами даних та клієнтські операційні системи, які повинні забезпечити:

– підтримку “клієнт-серверної” технології обробки даних;

– розмежування доступу до системних ресурсів та даних;

– резервування та захист інформації.

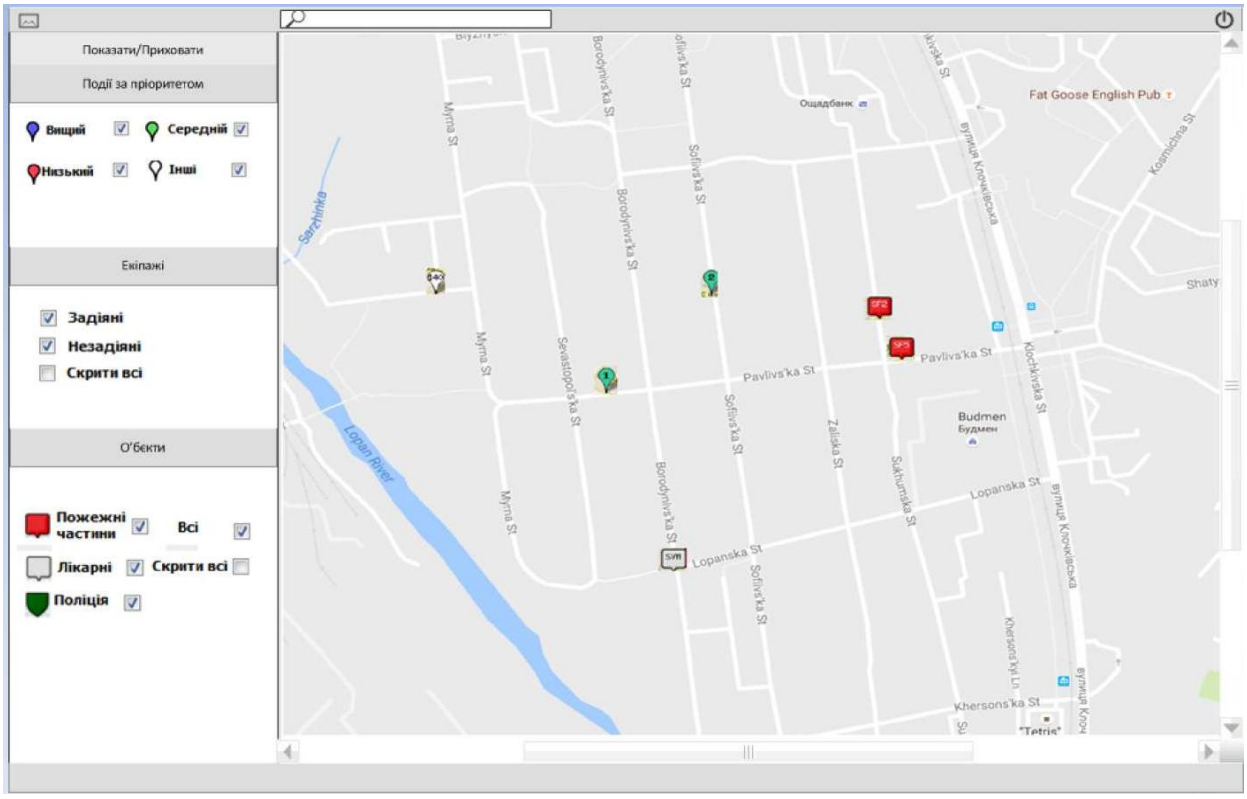


Рис. 1.42 – Діалогове вікно ПАК СОДУ "Карта подій"

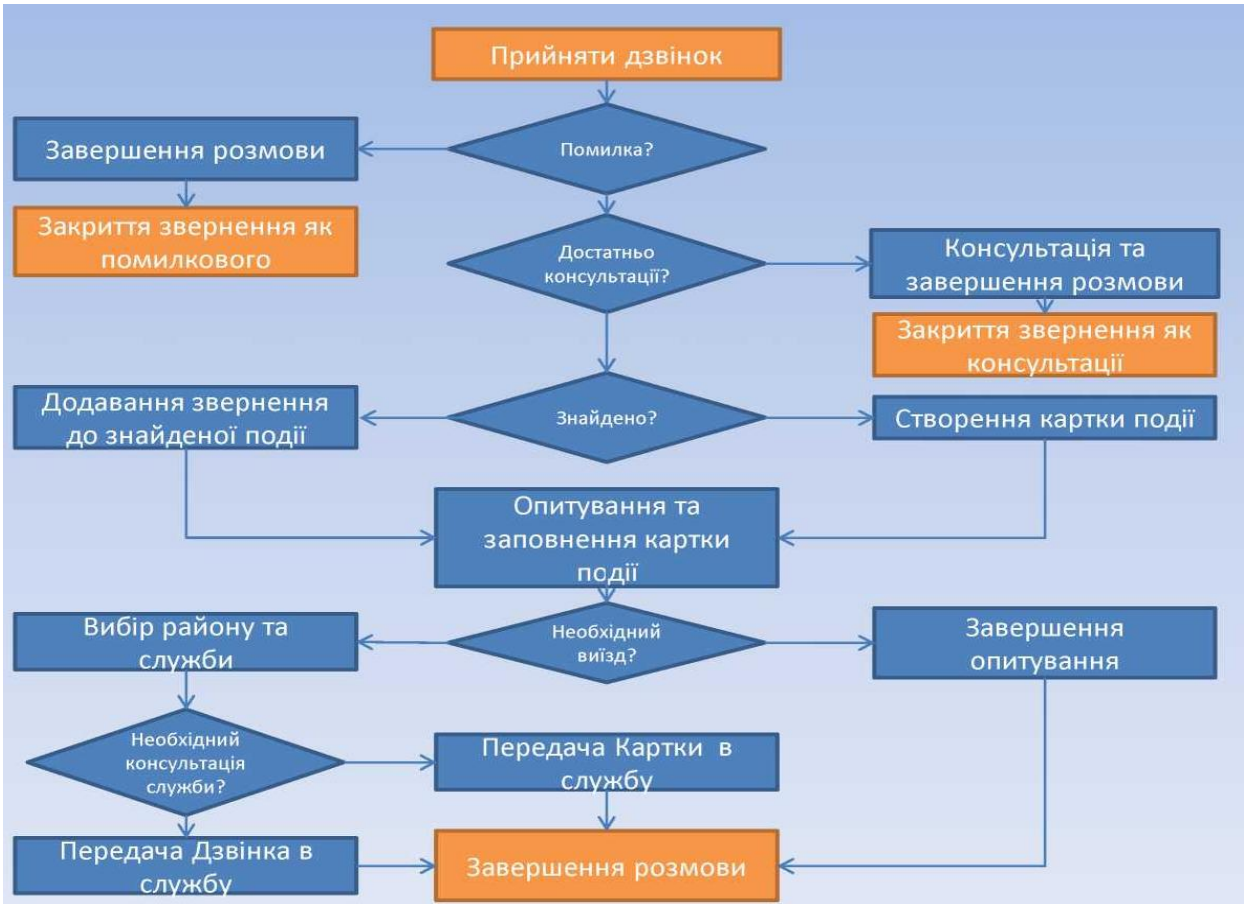


Рис. 1.43 – Алгоритм обробки звернення ПАК СОДУ

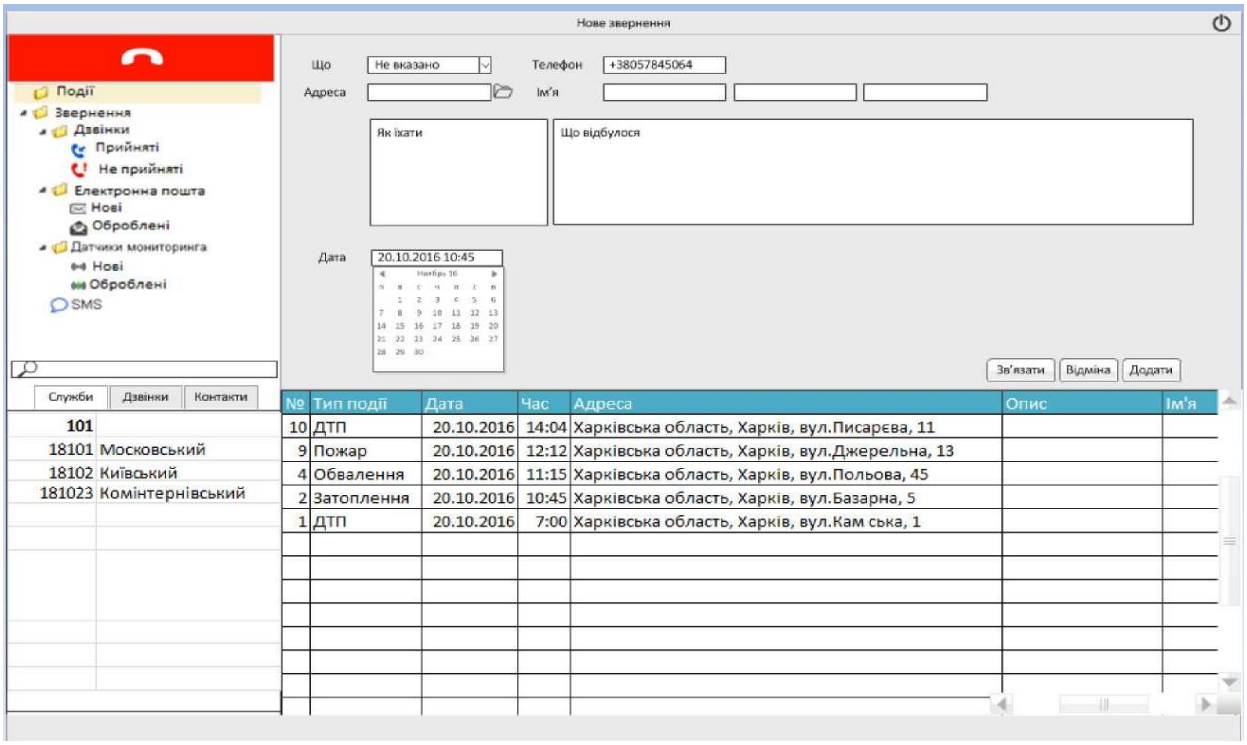


Рис. 1.44 – Діалогове вікно ПАК СОДУ "Нове звернення"

Спеціалізований ПАК повинен включати додатки реалізації з'єднання вибраної СУБД з ГІС-ПЗ рис.1.45, 1.46.

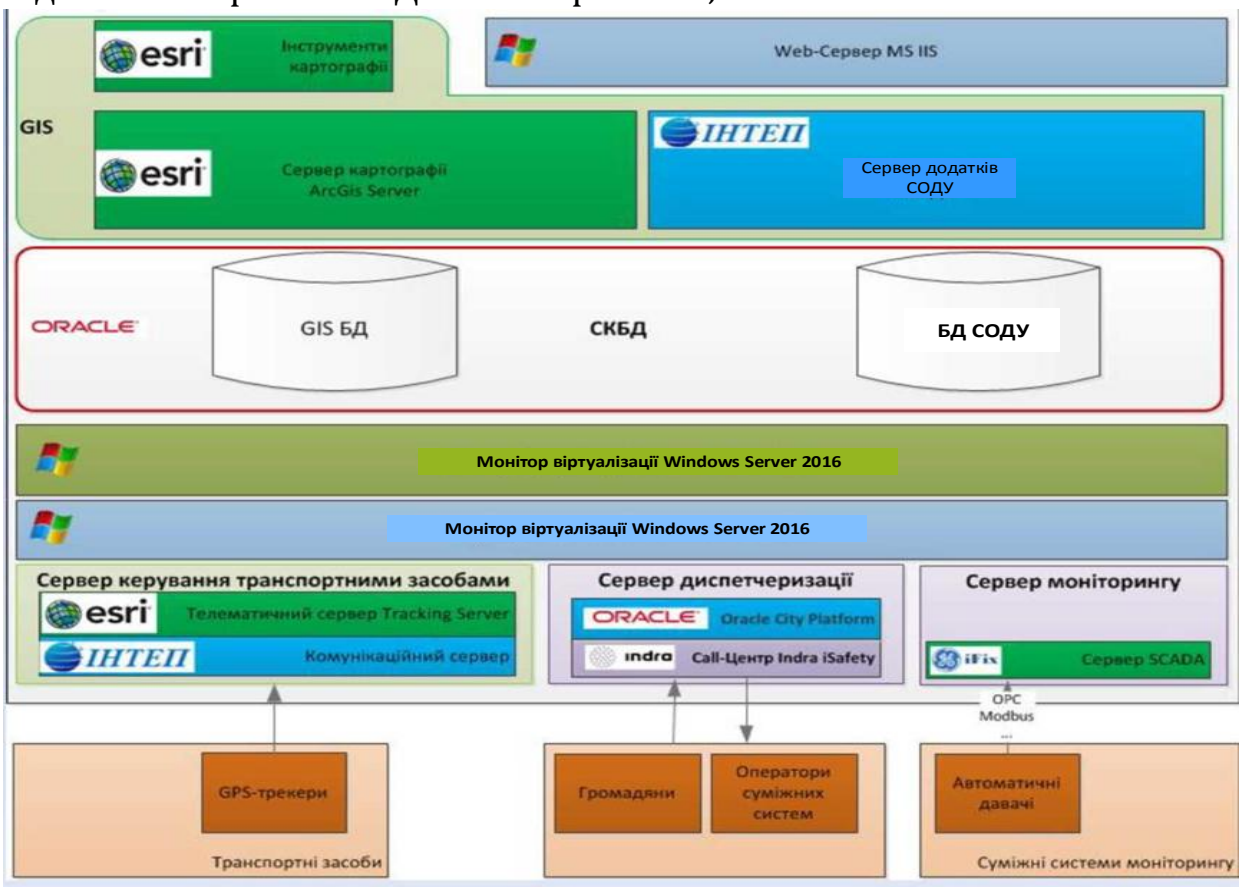


Рис. 1.45 – Схема структурна ПАК СОДУ (варіант: платформа Oracle)

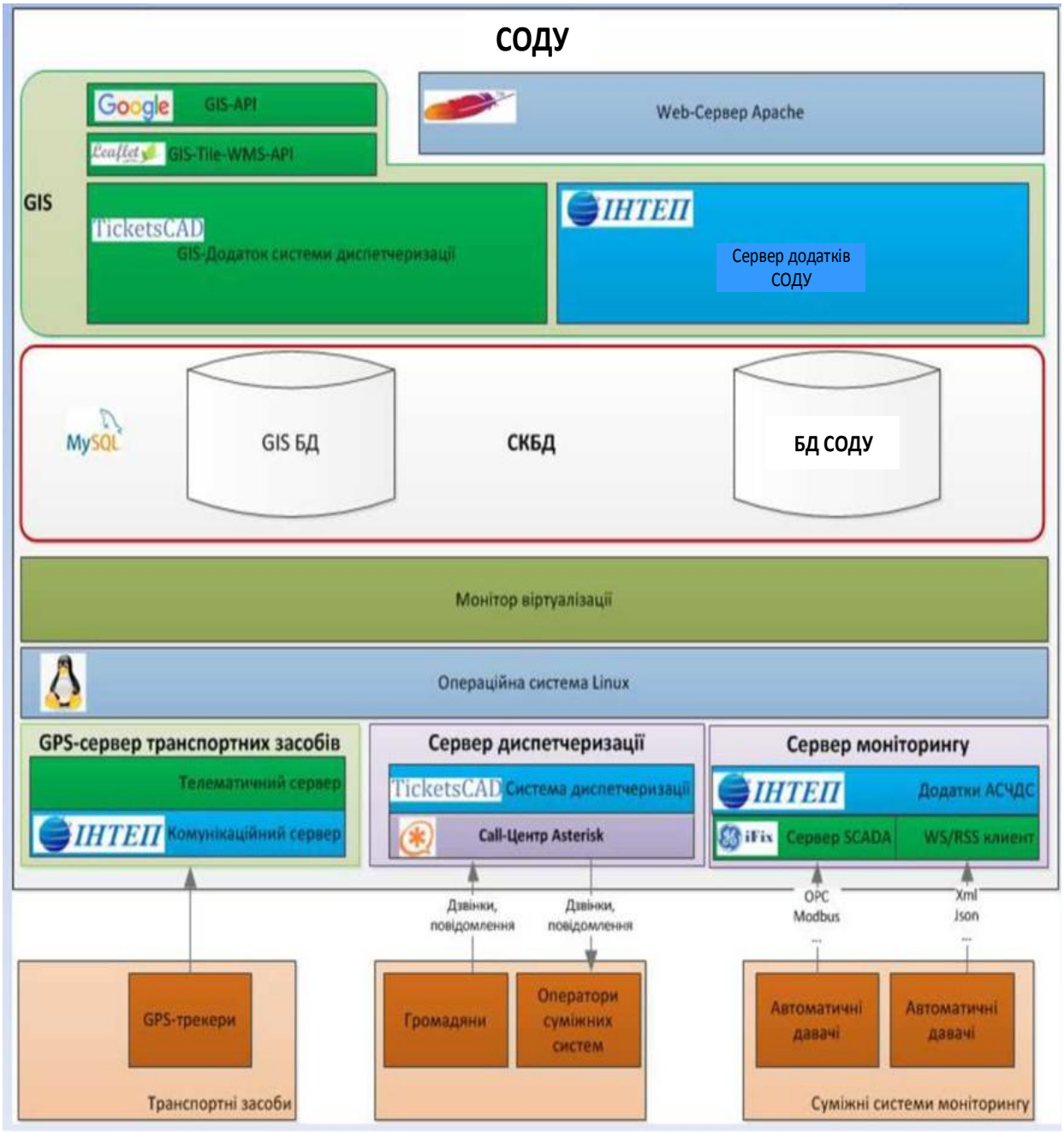


Рис. 1.46 – Схема структурна ПАК СОДУ (варіант: платформа Open Source)

Прикладне програмне забезпечення повинно проектуватися із застосуванням принципів структурного та модульного програмування. Кожна із задач, яка входить в систему повинна бути максимально незалежною від інших. Вимоги до незалежності програмних засобів від засобів обчислювальної техніки, що використовуються, не встановлюються.

Контроль якості програмних засобів, які розробляються, повинен бути забезпечений тестуванням та проведенням дослідної експлуатації.

Сучасний стан модернізації СОДУ ілюструється на рис. 1.47.



Рис. 1.47– І-й етап створення СОДУ

1.10 Система централізованого оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій

1.10.1 Стан технічної модернізації системи централізованого оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій

Концепції розвитку та технічної модернізації системи централізованого оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій представлена до табл. 1.12.

Таблиця 1.12 – Календарний план модернізації системи централізованого оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій

Найменування заходу	Відповідальні за виконання	Строк виконання
1	2	3
1. Розроблення та затвердження технічних вимог до загальнодержавної автоматизованої системи централізованого оповіщення	МВС ДСНС	жовтень 2018 р.
2. Розроблення рекомендацій щодо проектування та розрахунку зони впевненого прийому звукового сигналу небезпеки “Увага всім”	ДСНС	-“-

1	2	3
3. Підготовка та подання на розгляд Кабінету Міністрів України нормативно-правового акта щодо використання телекомунікаційних мереж загального користування в умовах надзвичайних ситуацій (внесення змін до постанови Кабінету Міністрів України від 29 червня 2004 р. № 812 “Деякі питання оперативно-технічного управління телекомунікаційними мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану”)	Адміністрація Держспецзв’язку	листопад 2018 р.
4. Розроблення та затвердження інструкції щодо практик чи процедур проектування, дослідження, введення в експлуатацію, у процесі експлуатації та технічного обслуговування (супроводження) автоматизованих систем централізованого оповіщення	МВС ДСНС	грудень 2018 р.
5. Розроблення положень про територіальні, місцеві системи централізованого оповіщення	обласні та Київська міська держадміністрації органи місцевого самоврядування (за згодою)	грудень 2019 р.
6. Проведення реконструкції загальнодержавної автоматизованої системи централізованого оповіщення:		
1) розроблення нормативно-технічної документації:		
технічного завдання на проведення реконструкції загальнодержавної автоматизованої системи централізованого оповіщення	ДСНС	червень 2019 р.
технічного проекту на проведення реконструкції загальнодержавної автоматизованої системи централізованого оповіщення	-“-	жовтень 2019 р.
2) створення комплексної системи захисту інформації загальнодержавної автоматизованої системи централізованого оповіщення	ДСНС Адміністрація Держспецзв’язку обласні та Київська міська держадміністрації	грудень 2022 р.
3) оснащення державної системи пунктів управління програмно-апаратними комплексами загальнодержавної автоматизованої системи централізованого оповіщення	ДСНС обласні та Київська міська держадміністрації	-“-
4) проведення дослідної експлуатації загальнодержавної автоматизованої системи централізованого оповіщення	-“-	серпень 2023 р.
5) введення в експлуатацію загальнодержавної автоматизованої системи централізованого оповіщення	-“-	грудень 2023 р.

1	2	3
7. Створення дослідного зразка територіальної автоматизованої системи централізованого оповіщення населення: розроблення нормативно-технічної документації на створення територіальної автоматизованої системи централізованого оповіщення населення	ДСНС Львівська, Харківська обласні та Київська міська держадміністрації	червень 2019 р.
впровадження дослідного зразка територіальної автоматизованої системи централізованого оповіщення		червень 2020 р.
проведення дослідної експлуатації територіальної автоматизованої системи централізованого оповіщення		грудень 2020 р.
8. Реконструкція територіальних автоматизованих систем централізованого оповіщення:	облдержадміністрації	грудень 2023 р.
впровадження (створення, модернізація, вдосконалення) територіальних автоматизованих систем централізованого оповіщення в областях		
введення в експлуатацію територіальних автоматизованих систем централізованого оповіщення		
9. Реконструкція місцевих автоматизованих систем централізованого оповіщення: впровадження (створення, модернізація, вдосконалення) місцевих автоматизованих систем централізованого оповіщення	органи місцевого самоврядування (за згодою)	-“-
введення в експлуатацію місцевих автоматизованих систем централізованого оповіщення		

1.10.2 Проектування, дослідження, введення в експлуатацію, експлуатації та технічного обслуговування (супроводження) автоматизованих систем централізованого оповіщення

1.10.2.1 Вимоги до автоматизованої системи централізованого оповіщення:

1) функціональні вимоги:

автоматизоване гарантоване оповіщення осіб керівного складу місцевих органів виконавчої влади, органів місцевого самоврядування та населення, а також підприємств, установ і організацій незалежно від форми власності на території відповідної адміністративно-територіальної одиниці (району, міста, об’єднаної територіальної громади), доведення до громадян сигналів цивільного захисту;

автоматизоване доведення до населення створеної у визначеному районі зони оповіщення попереджувальних сигналів небезпеки «УВАГА ВСІМ!»;

автоматичне або автоматизоване приймання, передавання в реальному масштабі часу та реєстрація вхідної і вихідної інформації;

автоматизоване підтвердження прийому інформації (повідомлень, сигналів, команд, даних, документів) щодо оповіщення та інформування населення про загрозу виникнення або виникнення надзвичайних ситуацій від пунктів управління в будь-якому напрямку оповіщення;

документування (протоколювання) вхідної та вихідної інформації, подій, усіх процесів оповіщення та інформування населення і дій користувачів автоматизованої системи централізованого оповіщення з можливістю формування друкованих звітів;

упровадження єдиної інформаційної бази (бази даних) автоматизованої системи централізованого оповіщення для автоматизованого або автоматичного приймання (передавання) формалізованої інформації (даних, документів) щодо оповіщення та інформування населення та/або інформаційної взаємодії;

інформаційна взаємодія між елементами автоматизованої системи централізованого оповіщення з автоматизованими системами централізованого оповіщення інших рівнів, іншими автоматизованими системами, що належать до єдиної державної системи цивільного захисту;

циркулярне, циркулярне за завчасно визначеними сценаріями, вибіркове або за пріоритетом передавання інформації щодо оповіщення та інформування населення;

доведення сигналів і повідомлень до осіб з фізичними, психічними, інтелектуальними та сенсорними порушеннями, керівників підприємств, установ і організацій УТОСу та УТОГу, інших підприємств, установ і організацій, що надають послуги особам з інвалідністю та маломобільним групам населення, визначених місцевими органами виконавчої влади та органами місцевого самоврядування, або за місцем роботи зазначених осіб (у доступній для них формі), керівників інтернатних закладів, закладів охорони здоров'я, які мають ліжковий фонд, установ виконання покарань, слідчих ізоляторів;

2) вимоги до стійкості роботи системи:

автоматичне збереження інформації у разі відмови та збоїв;

автоматичний контроль та діагностика стану програмних, технічних та комунікаційних засобів;

упровадження багаторівневого доступу згідно зі встановленими пріоритетами і правами доступу до мережевих та інформаційних ресурсів автоматизованої системи централізованого оповіщення;

упровадження технічних і програмних засобів із функціями забезпечення інформаційної безпеки інформаційних та мережевих ресурсів автоматизованої системи централізованого оповіщення;

автоматичне за встановленими сценаріями (алгоритмами) змішане резервування елементів (технічних засобів) автоматизованої системи централізованого оповіщення;

3) вимоги до надійності роботи системи:

коефіцієнт технічного використання – не менш як 0,95;

коефіцієнт готовності – не менш як 0,98;

середній строк служби – не менш як 10 років;

середній наробіток до відмови – не менш як 15000 год;

середня тривалість відновлення – не більше ніж 0,5 год.

2. Вимоги до сумісності:

1) програмно-технічна сумісність складових частин програмно-технічного комплексу із загальним інтерфейсом, що забезпечує введення-виведення даних, єдину структуру даних та базується на єдиних схемних, конструктивних та інших програмно-технічних рішеннях з максимальним використанням уніфікованих елементів програмно-технічного комплексу автоматизованої системи централізованого оповіщення;

2) взаємозамінюваність у програмно-технічному комплексі автоматизованої системи централізованого оповіщення уніфікованих програмних засобів та змінних однотипних виробів, компонентів, модулів.

3. Вимоги до конструкції:

1) використання серверних технічних засобів та технічних засобів телекомунікацій у варіанті для монтажу в стійках або серверних шафах типу Rack Mount;

2) використання технічних засобів, не призначених для монтажу в серверних шафах, у комплекті з полицями для їх монтажу з подальшим поміщенням у серверні шафи типу Rack Mount;

3) відповідність технічних засобів, які можуть застосовуватися в програмно-технічному комплексі автоматизованої системи централізованого оповіщення, вимогам нормативних документів з питань безпечної експлуатації обладнання, інформаційних технологій та безпеки;

4) використання технічних засобів телекомунікацій, включених до Переліку технічних засобів, які можуть застосовуватися в телекомунікаційних мережах загального користування України, відповідно до Положення про порядок визначення переліку технічних засобів, які можуть застосовуватися в телекомунікаційних мережах загального користування України, та погодження застосування засобів телекомунікацій, не внесених до цього переліку, затвердженого наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 17 березня 2014 року № 115, зареєстрованого у Міністерстві юстиції України 10 квітня 2014 року за № 405/25182.

4. Вимоги до програмного забезпечення:

використання операційних систем та систем управління базами даних із відкритими програмними кодами;

наявність прикладних програм функціонального призначення програмно-технічного комплексу системи, що забезпечують:

підтримку дій відповідальних осіб, які приймають (готують) рішення щодо оповіщення населення про загрозу виникнення або виник-

нення надзвичайних ситуацій та контролюють результативність їх виконання;

виконання заданих алгоритмів обробки, маршрутизації, відображення і зберігання інформації та управління інформаційними базами даних з можливістю зміни їх конфігурації та реалізації через стандартні бібліотечні блокові структури;

автоматичний контроль, діагностика та перевірка працездатності;

захист інформації від несанкціонованого доступу і неправильних дій користувачів;

мультисервісний обмін даними між елементами (компонентами) системи;

обмін даними з автоматизованими системами централізованого оповіщення інших рівнів та складовими єдиної державної системи цивільного захисту;

відповідність програмних модулів, які входять до складу прикладної програми, таким умовам:

відсутність ділянок коду, що викликають появу рекурентних циклів або статичних витоків пам'яті;

відсутність системних помилок, що призводять до часткового або повного виходу з ладу прикладної програми або технічних засобів;

компонування елементів програмного коду, що здійснюють обробку даних за стандартними алгоритмами, у вигляді окремих бібліотек, крім критичних до швидкості виконання ділянок коду;

реалізація можливості реструктуризації програмно-технічного комплексу системи без зміни прикладних програм за рахунок незалежності подання даних на концептуальному, програмному і фізичному рівнях;

налаштування прикладної програми під час доопрацювання, зміни переліку і структури вхідної та вихідної інформації без необхідності зміни програмного коду.

5. Вимоги до інформаційного забезпечення та інформаційної взаємодії:

реалізація автоматизованою системою централізованого оповіщення інформаційної взаємодії між складовими частинами програмно-технічного комплексу системи із автоматизованими системами централізованого оповіщення інших рівнів та іншими інформаційними системами єдиної державної системи цивільного захисту за допомогою спеціального програмного забезпечення;

покладення в основу побудови інформаційного забезпечення таких принципів:

спадкоємність із використання накопиченої інформації у функціонуючих системах оповіщення;

мінімізація дублювання з уведення (приймання) і накопичення даних в інформаційній базі даних;

висока ефективність алгоритмів, методів і засобів збору, обробки, зберігання, накопичення, оновлення, пошуку і надання інформації;

простота і зручність доступу до інформації;

перетворення вхідної інформації в цифрову форму якомога ближче до місця її здобуття;

перетворення вихідної інформації із цифрової форми у фізичну форму якомога ближче до місця її використання;

захист від недостовірної і несанкціонованої інформації;

перешкодостійке кодування і захист інформації від руйнування і несанкціонованого доступу;

регламентація доступу до інформаційних даних з різним рівнем доступу, а також часу зберігання документованої інформації;

у всіх випадках багаторазового введення або прийняття інформації передбачення заходів із запобігання розбіжностям та недостовірності інформації, а також із сигналізації про істотну розбіжність інформації в різних складових частинах програмно-технічного комплексу автоматизованої системи централізованого оповіщення;

передбачення заходів з виділення корисних складових інформації під час введення і первинної обробки сигналів (команд) оповіщення;

дотримання під час кодування інформації таких основних вимог:

відповідність набору мнемонічних знаків і їх колірного кодування набору, який прийнятий для автоматизованої системи централізованого оповіщення, і відображення функціонального технологічного вмісту;

кодування нормальної, попереджувальної, аварійної та недостовірної інформації різними кольорами, які не мають використовуватися з іншою метою (системні кольори);

для привернення уваги користувача виділення інформації, що має попереджувальний або аварійний характер, миготінням та супроводження її звуковими сигналами відповідного тону;

відображення недостовірної інформації кольором, який відрізняється від кольору основного фону або позначається миготливим символом;

лаконічність, вичерпність за змістом й однотипність за формою текстів повідомлень;

забезпечення інформаційної сумісності, сумісності взаємодії та інтеграції між автоматизованими системами централізованого оповіщення всіх рівнів шляхом створення єдиного інформаційного середовища на основі протоколу інформаційного обміну даними (взаємодії) прикладного рівня стеку інтернет-протоколу TCP/IP;

відповідність протоколу інформаційної взаємодії між автоматизованими системами централізованого оповіщення всіх рівнів вимогам но-

рмативних документів з питань структури інформаційних повідомлень при управлінні в надзвичайних ситуаціях.

6. Вимоги до інформаційної безпеки і захисту інформації:

надання доступу до функцій прикладних програм та інформації лише авторизованим користувачам з урахуванням їх службових повноважень, а також категорії інформації, яка запитується;

блокування спроб модифікації чи знищення інформації користувачами, які не мають на це повноважень, неідентифікованими користувачами або користувачами з непідтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора;

вирішення технічних рішень авторизованого доступу до інформації наданням кодів (фізичних ключів або логічних паролів) доступу користувачам, забезпечення надання прав доступу користувачам на підставі авторизації, ідентифікації та автентифікації;

визначення таких категорій користувачів:

користувач – відповідальна особа за здійснення заходів згідно з функціональними обов'язками, яка пройшла навчання і допущена до роботи з відповідним автоматизованим робочим місцем, зокрема черговий персонал оперативно-чергових (чергових, диспетчерських) служб;

адміністратор – уповноважена особа, яка пройшла навчання та уповноважена щодо:

перегляду або зміни конфігурації програмно-технічного комплексу та надання кодів доступу за типом (категорією) «користувач»;

перегляду статистичних даних журналів (архіву) за результатами дій користувачів системи за типом (категорією) «користувач»;

здійснення технічного обслуговування програмно-технічного комплексу автоматизованої системи централізованого оповіщення тощо;

розробник – особа, яка пройшла навчання та уповноважена щодо заміни (модифікації) технічних та/або програмних засобів;

впровадження таких рівнів доступу:

рівень доступу 1 – доступ необмеженого кола осіб, відповідальних за первинне реагування на повідомлення (лише статистичний перегляд цієї інформації без будь-якого втручання щодо її обробки);

рівень доступу 2 – доступ користувачів за категорією «користувач»;

рівень доступу 3 – доступ користувачів за категорією «адміністратор» (рівень доступу 3 виконується лише через рівень доступу 2);

рівень доступу 4 – доступ користувачів за категорією «розробник» (рівень доступу 4 виконується лише через рівень доступу 3);

надання прав авторизованого доступу до інформаційного ресурсу та функціонування у складі автоматизованої системи централізованого оповіщення програмним та технічним засобам автоматизованого робочого місця;

проведення авторизації, ідентифікації та автентифікації будь-якого програмного та/або технічного засобу автоматизованого робочого місця з використанням його унікального реєстраційного номера, який присвоюється програмному та/або технічному засобу для конкретного автоматизованого робочого місця;

розділення доступу до функцій прикладних програм програмно-технічного комплексу та інформаційного ресурсу як мінімум на чотири рівні;

створення для автоматизованої системи централізованого оповіщення, її інформаційних баз та сховищ даних (електронних архівів) комплексної системи захисту інформації з підтвердженою відповідністю згідно із Законом України «Про захист інформації в інформаційно-телекомунікаційних системах».

7. Вимоги до автоматизованого робочого місця:

забезпечення за допомогою функціональних можливостей прикладних програм автоматизованого робочого місця ефективного виконання користувачами автоматизованої системи централізованого оповіщення таких етапів дій:

перший етап – сприйняття вхідної інформації (повідомлень, сигналів, команд, документів) щодо оповіщення;

другий етап – оцінка інформації;

третій етап – прийняття рішення про дії на основі аналізу інформації;

четвертий етап – виконання прийнятого рішення шляхом певних дій або надання відповідних розпоряджень (команд);

п’ятий етап – контроль за результативністю виконання прийнятих рішень;

забезпечення екранними інтерфейсами засобів відображення інформації (дисплеї, спеціальні табло) автоматизованого робочого місця можливості швидкого та безпомилкового сприйняття інформації для її оцінки та прийняття правильного рішення;

розташування важливої інформації, яка вимагає прийняття рішення, в межах оптимальної для сприйняття зони відображення;

відображення аварійної інформації (про відмови, несправності, збої) та другорядної, яка використовується періодично, поза межами оптимальної зони відображення;

об’єднання способів і засобів ведення діалогу користувача з прикладним програмним забезпеченням в уніфіковані сценарії з максимальним використанням ієрархій меню;

отримання користувачем повідомлень про наявність помилок у вигляді попереджувальної (звукової та візуальної) сигналізації за допомогою програмного контролю помилкових дій (відображення повідомлен-

ня про наявність помилки і її характер в контрольному рядку або на спеціальній ділянці екрану автоматизованого робочого місця);

забезпечення органів управління інтерфейсу користувача, випадковий вплив на які неприпустимий, спеціальним захистом, зняття якого потребує виконання не менше двох дій;

забезпечення автоматизованого робочого місця таким мінімальним набором функцій:

автоматизоване вибіркове або за пріоритетом передавання оперативної інформації (повідомлень, сигналів, команд, документів) щодо оповіщення;

підготовка та автоматизоване вибіркове або за пріоритетом у будь-якому напрямку передавання формалізованої та/або неформалізованої інформації (повідомлень, документів) про загрозу виникнення, виникнення надзвичайної ситуації (залежно від її рівня: державного, регіонального, місцевого) та оперативної інформації про стан обстановки під час ліквідації наслідків надзвичайної ситуації для її аналізу, прийняття рішень, оповіщення та інформування населення;

введення вручну за допомогою сенсомоторних пристроїв (маніпулятор «миша», клавіатура) текстової та/або символьної (алфавітно-цифрової) інформації;

автоматичне та/або автоматизоване приймання та реєстрація інформації (повідомлень, сигналів, команд, документів);

автоматичне та/або автоматизоване підтвердження приймання інформації (повідомлень, сигналів, команд, документів);

візуальна та/або звукова попереджувальна сигналізація про підтвердження (непідтвердження) приймання переданої інформації;

індикація контролю технічного стану автоматизованого робочого місця і каналів обміну даними (візуальна та/або звукова попереджувальна сигналізація);

індикація контролю технічного стану прикінцевих технічних засобів оповіщення та інформування населення і каналів обміну даними з ними (візуальна та/або звукова попереджувальна сигналізація);

перегляд задокументованої (запротокольованої) вхідної та/або вихідної інформації (повідомлень, сигналів, команд, документів) з можливістю формування друкованих звітів;

підготовка формалізованих статистичних звітів та інших документів.

8. Вимоги до кінцевих технічних пристроїв оповіщення населення:

автоматизоване або автоматичне приведення сигнальних технічних пристроїв (електросирени, спеціальні звукові системи на основі гучномовців, спеціальні світлові джерела візуальних сигналів) протягом 3 секунд з моменту надходження відповідної команди в режим функціонування за призначенням;

безвідмовність, ремонтопридатність, спроможність виконувати необхідні функції в будь-який момент часу;

забезпечення резервним електроживленням з метою збереження працездатності кінцевих технічних пристроїв у разі відключення централізованого енергопостачання або відмови первинного електроживлення;

забезпечення резервним джерелом електроживлення працездатності кінцевих технічних пристроїв оповіщення в черговому режимі протягом 24 годин та в режимі передавання сигналів оповіщення протягом подвоєного часу евакуації, але не менше ніж 30 хвилин;

забезпечення кінцевих технічних пристроїв оповіщення автоматичними зарядними пристроями, якщо як резервне джерело електроживлення використовуються акумуляторні батареї (автоматичні зарядні пристрої мають забезпечувати заряджання акумуляторів до 80 % їх максимальної місткості протягом не більше ніж 24 години, свинцево-кислотні батареї мають бути обладнані пристроями обмеження їх повного розряджання відповідно до рекомендацій виробника);

кінцеві технічні пристрої, що використовуються в системі централізованого оповіщення, повинні мати виданий у встановленому законодавством порядку документ про підтвердження відповідності вимогам нормативних документів у сфері телекомунікацій.

Для потреб автоматизованих систем централізованого оповіщення використовуються ресурси телекомунікаційних мереж загального користування, Національної телекомунікаційної мережі, державної системи урядового зв’язку та Національної системи конфіденційного зв’язку.

Проекти будівництва та реконструкції автоматизованих систем централізованого оповіщення мають передбачати заходи щодо резервування каналів та ліній зв’язку (у тому числі бездротового) для здійснення управління технічними засобами оповіщення, а проектні рішення – встановлення спеціальних технічних засобів для переривання трансляції програм мовлення з метою передавання сигналів та інформації через програми теле– та радіомовлення.

1.10.2.2 Основні заходи та роботи щодо введення в експлуатацію автоматизованої системи централізованого оповіщення:

навчання персоналу й перевірка його здатності забезпечити функціонування автоматизованої системи централізованого оповіщення;

комплектація системи відповідно до проектної документації;

монтаж технічних засобів і засобів телекомунікацій;

автономний пуск та налагодження технічних та програмних засобів і комплексна перевірка функціонування системи в цілому для проведення приймальних випробувань.

2. Режими роботи автоматизованої системи централізованого оповіщення:

штатний режим (основний режим роботи) – забезпечення безперервного виконання всіх функцій системи незалежно від режимів функціонування єдиної державної системи цивільного захисту (повсякденне функціонування, підвищена готовність, надзвичайна ситуація, надзвичайний стан);

режим відновлення після збоїв, відмов (аварійний режим) – відновлення функціонування на основі змішаного резервування (проектні рішення мають передбачати автоматичне відновлення функціонування основних елементів системи без порушення працездатності в цілому);

режим технічного обслуговування (адміністративний, сервісний режим) – проведення заходів щодо супроводу, технічного обслуговування, подальшого вдосконалення та модифікації;

режим навчання персоналу.

3. Контроль стану елементів системи:

1) критерії реалізації моніторингу та контролю (далі – моніторинг) стану елементів (компонентів) програмно-технічного комплексу системи:

повна готовність до виконання покладених функцій;

обмежена здатність щодо виконання покладених функцій;

збій або відмова;

2) у разі виникнення аварійних ситуацій або помилок у роботі програмно-технічного комплексу автоматизованої системи централізованого оповіщення інструменти контролю зберігають повний набір інформації, необхідної користувачеві і розробникові для ідентифікації проблеми (знімки екранів, коди помилки (збою), поточний стан пам’яті та файлової системи програмних засобів);

3) компоненти інструментів контролю:

забезпечують виявлення непрацездатності власних технічних та програмних засобів, які входять до складу елементів (компонентів) програмно-технічного комплексу автоматизованої системи централізованого оповіщення та засобів інформаційного обміну, сумісності і взаємодії;

контролюють канали обміну даними з мережевими телекомунікаційними засобами, які використовуються для передавання/приймання сигналів (команд) оповіщення (як мінімум, фізичне пошкодження внутрішніх каналів обміну даними має бути визначено та розпізнано);

4) у разі несправності каналів обміну даними генерується та подається інформація про їх несправність, а також генерується застережна сигналізація;

5) активація засобів безперервного контролю прикладних програм супроводжується відповідними повідомленнями та застережною сигналізацією.

4. Збереження інформації у разі відмов та збоїв:

1) програмно-технічний комплекс системи:

стійкий до хибних дій користувача (помилки в діях персоналу не мають призводити до відмов (збоїв) у роботі);

забезпечує гарантований контроль вхідної та вихідної інформації;

забезпечує регламентований час відновлення після відмови (збою);

2) інформація зберігається у разі:

збою або відмови технічних засобів;

збою або відключення електроживлення;

відмови каналів обміну даними;

збою або відмови операційної системи;

збою або відмови прикладної програми;

3) прикладні програми:

виконують функції автоматичного дублювання і резервування даних;

відновлюють своє функціонування у разі коректного перезапуску технічних засобів зі збереженням усіх даних;

4) у разі збою або відключення електроживлення апаратних засобів, що призводить до перезавантаження операційної системи і прикладної програми, відновлення прикладної програми відбувається після перезапуску операційної системи і запуску виконуваного файлу прикладної програми. Дані конфігурацій прикладної програми у такому разі не втрачаються;

5) для відновлення даних і прикладної програми з резервної копії використовуються засоби автоматичного та/або ручного резервного копіювання й архівації, які входять до складу програмних засобів. Для скорочення об'єму копійованих даних забезпечується копіювання лише змін з попереднього копіювання, періодичність повного копіювання даних обґрунтовується на етапі проектування;

6) передбачається можливість відновлення даних за допомогою їх повторного введення або імпорту (для даних із зовнішніх систем, що отримуються автоматично).

5. Технічне обслуговування системи:

1) вимоги до технічного обслуговування:

проведення комплексу робіт з підтримки цілодобового функціонування автоматизованої системи централізованого оповіщення в усіх режимах;

забезпечення справного стану програмно-технічних засобів під час їх використання за призначенням та необхідних показників надійності протягом усього строку експлуатації;

постійна присутність персоналу обслуговування технічних засобів автоматизованої системи централізованого оповіщення та її елементів (компонентів, частин) не є обов'язковою;

2) види технічного обслуговування та тривалість технічного обслуговування автоматизованої системи централізованого оповіщення ви-

значаються відповідно до нормативних документів з питань технічного обслуговування;

3) документація на технічне обслуговування автоматизованої системи централізованого оповіщення визначається відповідно до нормативних документів з питань технічного обслуговування.

6. Супровід системи:

1) супровід програмних засобів відповідно до нормативних документів з питань застосування процесів життєвого циклу програмного забезпечення включає коригувальний супровід, адаптивний супровід, супровід із вдосконалення, профілактичний супровід;

2) роботи із супроводу програмних засобів проводяться для вирішення таких завдань:

усунення збоїв;

поліпшення дизайну інтерфейсів користувачів;

реалізація розширень функціональних можливостей;

створення інтерфейсів інформаційної взаємодії з іншими (зовнішніми) інформаційними системами;

адаптація програмних засобів для можливості роботи на іншій технічній платформі (або оновленій платформі), застосування нових системних можливостей, функціонування в середовищі оновленої телекомунікаційної мережі тощо;

виведення окремого прикладного програмного забезпечення з експлуатації.

1.11 Система електронного документообігу в ДСНС України

1.11.1 Структура системи електронного документообігу в органах та підрозділах ДСНС

Електронний документ – це документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа [9, 22, 23].

Електронний документообіг (обіг електронних документів) – сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів. Порядок електронного документообігу визначається державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями всіх форм власності згідно з законодавством:

Конституція України (від 28.06.1996 № 254к/96-ВР),

Цивільний кодексом України (від 16.01.2003 № 435-IV),

Законами України:

"Про інформацію" (від 02.10.1992 № 2657-XII),

"Про захист інформації в автоматизованих системах" (від 31.05.2005 № 2594-IV),

"Про державну таємницю" (від 21.01.1994 № 3855-XII),

"Про телекомунікації" (від 18.11.2003 № 1280-IV),

"Про обов'язковий примірник документів" (від 09.04.1999 № 595-XIV),

"Про Національний архівний фонд та архівні установи" (від 24.12.1993 № 3814-XII),

“Про електронні документи та електронний документообіг”, (від 22.05.2003 № 851-IV).

Наказ ДСНС 03.12.2018 № 700 Інструкція з документування управлінської інформації в електронній формі та організації роботи з електронними документами в діловодстві, електронного міжвідомчого обміну в Державній службі України з надзвичайних ситуацій (5).

Система електронного документообігу в органах та підрозділах ДСНС України є трирівневою.

Перший рівень включає – апарат міністерства та його структурні підрозділи,

До другого рівня можна віднести ГУ(У) ДСНС України в областях, містах Києві та Севастополі, всі навчальні заклади міністерства та інші підрозділи, які безпосередньо підпорядковуються міністерству.

Третій рівень – це безпосередньо ті підрозділи на місцях, які підпорядковуються підрозділам віднесеним до другого рівня

Схематично загальна структура системи електронного документообігу в ДСНС зображена на рис. 1.48.

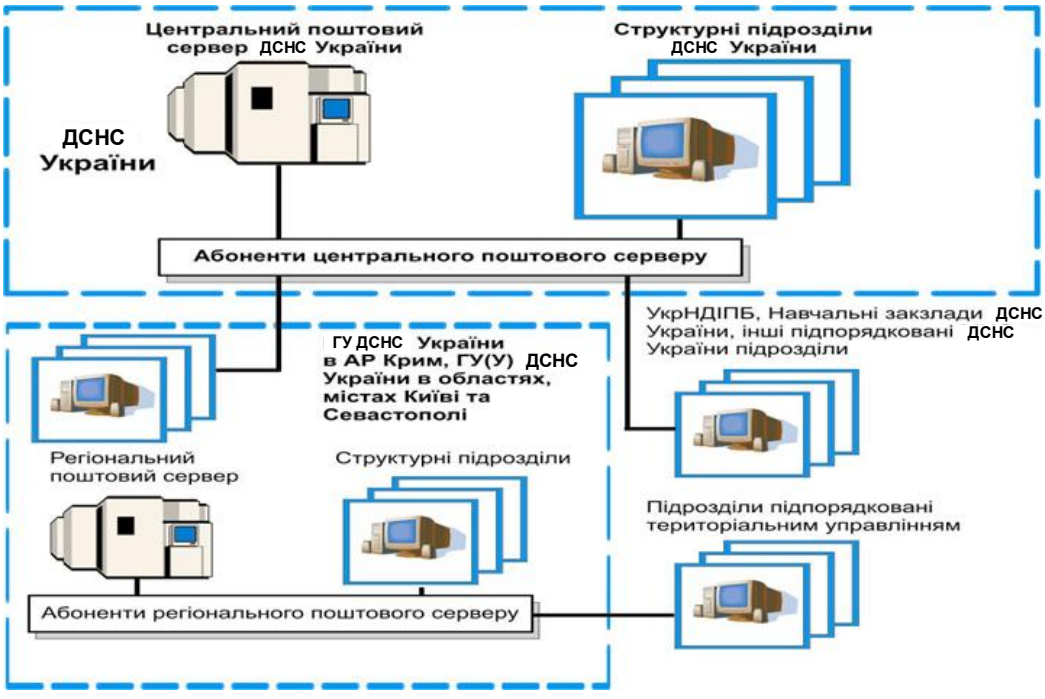


Рис.1.48 – Структура системи електронного документообігу в органах та підрозділах ДСНС

Як зорганізується обмін документами на рівні окремих комп'ютерів ми можемо побачити на схемі, наприклад, організації зв'язку між абонентами центрального поштового сервера ДСНС України. Пояснює рис.1.49.

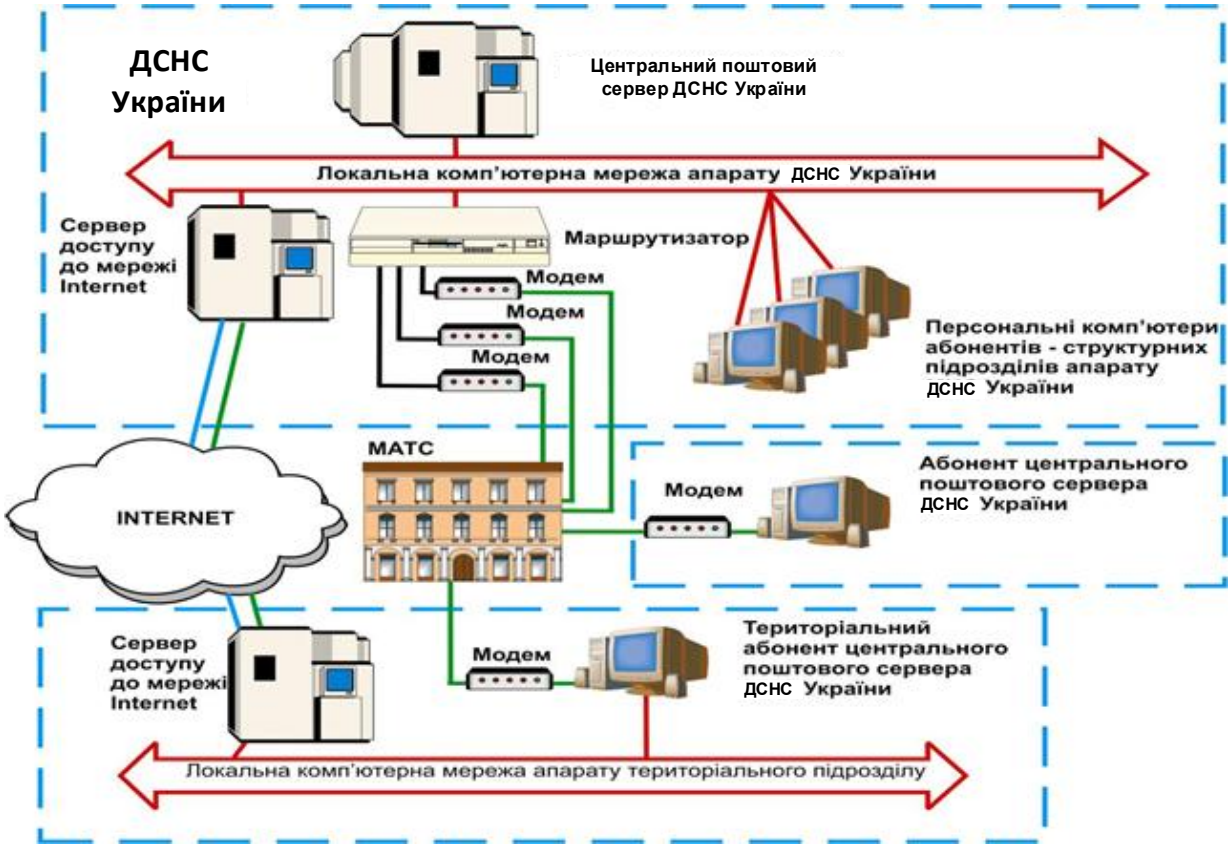


Рис. 1.49 – Схема організації зв'язку між абонентами центрального поштового сервера ДСНС України

Важливу роль в роботі цієї системи належить спеціалізованому програмному забезпеченню системи електронного документообігу.

В плані вивчення дисципліни є розгляд автоматизованої системи контролю та організації діловодства «АСКОД Стандартний», яка в основному вирішує цю задачу [21].

1.11.2 Правила з документування управлінської інформації в електронній формі та організації роботи з електронними документами в діловодстві, електронного міжвідомчого обміну в ДСНС України

Згідно наказу Наказ ДСНС від 03.12.2018 № 700 документування управлінської інформації в електронній формі здійснюється із застосуванням електронного цифрового підпису, електронної печатки та електронної позначки часу, крім випадків наявності обґрунтованих підстав

для документування управлінської інформації у паперовій формі, якими визнаються:

документи, що містять інформацію з обмеженим доступом, вимога щодо захисту якої встановлена законом;

електронні документи, що не можуть бути застосовані як оригінал згідно з вимогами закону;

документи з питань, пов'язаних із запобіганням виникненню надзвичайних ситуацій, ліквідацією їх наслідків, або з інших питань, пов'язаних із виникненням загрози життю та/або здоров'ю населення, а також із невідкладних питань щодо проведення ООС та обороноздатності держави;

документи, вимога щодо опрацювання яких у паперовій формі встановлена актами Кабінету Міністрів України.

Загальні засади документування управлінської інформації та особливості ведення діловодства у паперовій формі визначаються Типовою інструкцією з діловодства в міністерствах, інших центральних та місцевих органах виконавчої влади, затвердженою постановою Кабінету Міністрів України від 17 січні 2018 р. № 55 та Інструкцією з діловодства в апараті Державної служби України з надзвичайних ситуацій (далі – Інструкція з діловодства).

До електронних документів, підписаних (погоджених) із застосуванням електронного цифрового підпису або засвідчених електронною печаткою, вимагати відтворення візуального підпису або відбитка печатки незалежно від особливостей оформлення документів не допускається.

Проходження в діловодстві одного і того ж документа в електронній та паперовій формі не допускається.

1.11.3 Організація документообігу

1. Організація документообігу здійснюється за допомогою АСКОД та веб-модуля системи взаємодії.

Облік обсягу документообігу

1. Облік обсягу документообігу здійснюється у порядку, визначеному Інструкцією з діловодства.

Підсумкові дані обліку обсягу документообігу подаються в електронній формі.

Реєстрація документів

2. Вхідні, внутрішні, вихідні, інші документи незалежно від форми їх створення, підготовлені в ДСНС реєструються в АСКОД.

3. Для забезпечення реєстрації документів в електронній та паперовій формах (далі – документи) в автоматизованому режимі заповнюється реєстраційна контрольно-моніторингова картка, до якої вносяться всі обов'язкові, додаткові та у разі потреби інші реквізити документа відповідно до вимог Інструкції з діловодства.

4. Реєстраційна контрольно-моніторингова картка електронного документа створюється АСКОД в електронній формі.

5. До обов'язкових реквізитів, що вносяться в реєстраційну контрольно-моніторингову картку, належать: вид документа, код уніфікованої форми документа відповідно до Державного класифікатора управлінської документації ДК 010-98, індекс та заголовок справи, кореспондент (установа-відправник), підписувач документа та електронний цифровий підпис підписувача або електронна печатка установи-відправника, адресат (перелік установ, яким адресовано документ), вихідні номер та дата (реєстраційні атрибути кореспондента), вхідні номер та дата (реєстраційні атрибути адресата), вихідний номер та дата реєстрації (реєстраційні атрибути установи), короткий зміст документа, структурний підрозділ, відповідальний за виконання завдання та /або підготовку документа в установі, із зазначенням його індексу, резолюції, відповідальний виконавець (згідно з резолюцією), із зазначенням його прізвища, імені, по батькові, строк та позначка про виконання документа, строк зберігання документа (відповідно до номенклатури справ), кількість сторінок супровідного листа та кількість сторінок додатків, посилання на вже зареєстровані документи (історія питання), індикатори стану виконання документа та строки виконання індикаторів.

6. До додаткових реквізитів, що вносяться в реєстраційну контрольно-моніторингову картку, належать: внутрішнє переадресування документа між структурними підрозділами ДСНС, наявність та перелік додатків, проміжні строки виконання, інформація про зміну та перенесення строків виконання, припинення моніторингу документа, інформаційні повідомлення системи взаємодії, строк передавання до архіву, позначка про належність документа до документів термінового розгляду.

7. Допускається введення інших реквізитів документа, що не звужують та не змінюють застосування обов'язкових і додаткових його реквізитів.

8. Реєстрація вхідної і вихідної кореспонденції здійснюється службою діловодства централізовано.

9. Документи, що стосуються напрямів діяльності структурних підрозділів, можуть реєструватися в цих структурних підрозділах.

10. Електронні документи, що надходять електронною поштою без електронного цифрового підпису (електронної печатки), реєстрації не підлягають.

11. В АСКОД формується єдина централізована база реєстраційних даних в електронній формі, за допомогою якої працівники забезпечуються інформацією про всі документи і їх місцезнаходження.

12. Порядок розміщення реквізитів у реєстраційній контрольно-моніторинговій картці визначається Інструкцією з діловодства.

13. Реєстрація вхідних документів

14. Реєстрація вхідної кореспонденції здійснюється реєстратором лише після проведення попереднього розгляду документа.

15. Не допускається проведення подвійної реєстрації електронного документа в АСКОД та веб-модулі системи взаємодії.

16. На документ, що надійшов у паперовій формі, після реєстрації наноситься його реєстраційний номер, присвоєний АСКОД, дата реєстрації, та створюється фотокопія, яку реєстратор вносить до реєстраційної контрольно-моніторингової картки.

17. Вхідний документ постійного та тривалого (понад 10 років) зберігання, що надійшов у паперовій формі, після реєстрації та створення фотокопії реєстратором передається безпосередньо в структурний підрозділ, визначений в установленому порядку відповідальним за виконання цього документа, лише для зберігання з подальшим формуванням у справи відповідно до затвердженої номенклатури справ.

Перевірка електронного цифрового підпису

1. Для забезпечення перевірки електронних цифрових підписів (електронної печатки) використовуються:

2. встановлений на відповідному робочому місці надійний засіб електронного цифрового підпису для перевірки накладених електронних цифрових підписів;

3. завантажені із сайту акредитованого центру сертифікації ключів сертифікати відкритих ключів, які засвідчують чинність і належність відкритого ключа відповідному підписувачу та списки відкликаних сертифікатів.

4. У ДСНС організовується централізоване сховище сертифікатів відкритих ключів.

5. Перевірка електронного цифрового підпису здійснюється відповідно до вимог Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності, затвердженого постановою Кабінету Міністрів України від 19 вересня 2018 р. № 749.

Реєстрація вихідних документів

1. Реєстрація вихідних документів здійснюється після їх підписання.

2. Надсилання документів незалежно від форми їх створення на адресу користувачів системи взаємодії здійснюється через веб-модуль системи взаємодії.

У разі створення документа у паперовій формі адресату надсилається лише його засвідчена службою діловодства фотокопія через вебмодуль системи взаємодії, крім випадку надсилання документів установі чи особі, які не є користувачами системи взаємодії, та документів, визначених пунктом 2 цієї Інструкції.

3. Якщо адресат не є користувачем системи взаємодії, реєстратор надсилає документ за належністю згідно з вимогами Інструкції з діловодства.

4. У разі надсилання фотокопії документа через систему взаємодії оригінал вихідного документа в паперовій формі (лише для документів постійного та тривалого (понад 10 років) строків зберігання) передається в структурний підрозділ (автору документа) тільки для зберігання з подальшим формуванням у справи відповідно до затвердженої номенклатури справ без передачі їх адресату.

5. Перевірку внесених у реєстраційну контрольно-моніторингову картку обов'язкових та додаткових реквізитів вихідного документа здійснює реєстратор.

Електронна печатка

6. Перелік електронних документів, які потребують засвідчення електронною печаткою, визначається Інструкцією з діловодства на підставі актів законодавства.

7. Порядок використання електронної печатки та уповноважені посадові особи, відповідальні за її застосування, визначаються Інструкцією про порядок виготовлення, обліку, зберігання, використання та знищення печаток і штампів у системі Державної служби України з надзвичайних ситуацій.

ДСНС може засвідчувати електронні копії лише тих документів, що створюються у ній, зокрема на вимогу органів судової влади та правоохоронних органів. Копія документа виготовляється і видається тільки з дозволу Голови ДСНС, його заступників або керівника структурного підрозділу (автора документа).

Організація передавання документів та визначення їх виконавців

8. Зареєстрований документ за фактом внесення реєстратором у реєстраційну контрольно-моніторингову картку відповідального за розгляд документа (згідно з розподілом обов'язків) керівника, який розглядає документ першим (далі – первинний розгляд), автоматично передається на розгляд через АСКОД.

Документ автоматично та одночасно надходить на розгляд одній чи декільком посадовим особам (заступникам Голови ДСНС, директорам департаментів або керівникам інших самостійних структурних підрозділів), які визначені виконавцями (співвиконавцями) зазначеного документа.

9. Документи одразу після їх реєстрації передаються на первинний розгляд.

Голові ДСНС або особі, яка виконує його обов'язки, на первинний розгляд передаються документи, що надійшли від Секретаріату Кабінету Міністрів України, Апарату Верховної Ради України, Адміністрації Президента України, звернення народних депутатів та доручення (листи) установ вищого рівня.

Заступникам Голови ДСНС згідно з розподілом обов'язків на первинний розгляд передаються акти органів державної влади, органів влади Автономної Республіки Крим, документи, що надійшли від територіальних органів, організацій, установ та підприємств, що належать до сфери управління ДСНС, організаційно-розпорядчі та програмні документи загальнодержавного характеру.

Первинний розгляд проектів актів, внесених ДСНС на спільне розроблення, інших документів здійснюється керівниками самостійних структурних підрозділів або особами, які виконують їх обов'язки, в межах їх компетенції.

Резолюція

10. Посадова особа, яка здійснює первинний розгляд документа, накладає на нього резолюцію, в якій визначає головного виконавця, відповідального за організацію виконання документа, та у разі необхідності співвиконавців і строк його виконання.

У резолюції обов'язково зазначаються всі структурні підрозділи, які беруть участь в опрацюванні документа та погодженні проекту відповіді.

Посадові особи, які одночасно розглядають документ, накладають на нього резолюції, в яких визначають відповідальних виконавців та у разі необхідності співвиконавців у межах відповідного структурного підрозділу.

11. Резолюція складається з таких реквізитів: прізвище, ініціал імені виконавця (виконавців) у давальному відмінку, зміст доручення, строк виконання, підпис посадової особи.

У резолюції до документа, що не має строку виконання, зазначення змісту доручення та строку виконання не вимагається.

Резолюція може доповнюватися іншими реквізитами, які не звужують та не змінюють застосування обов'язкових реквізитів.

Неконкретні ("прискорити", "поліпшити", "активізувати", "звернути увагу" тощо) резолюції не допускаються.

12. Усі резолюції, накладені на документ, вносяться до його реєстраційної контрольно-моніторингової картки і нерозривно пов'язані із нею. Резолюція, яка є наслідком виконання резолюції вищого рівня, додатково містить логічне посилання на відповідну резолюцію (дерево резолюцій).

13. Резолюція посадової особи підписується цією ж посадовою особою.

14. До накладання резолюції встановлюються такі особливості:

виконавцями резолюції Голови ДСНС визначаються заступники Голови ДСНС, керівники департаментів або інших самостійних структурних підрозділів, про що інформуються заступники Голови ДСНС, які координують діяльність відповідного структурного підрозділу та у разі потреби мають право доповнити зазначену резолюцію, не змінюючи суті доручення Голови ДСНС та його головного виконавця;

виконавцями резолюції заступників Голови ДСНС визначаються керівники підпорядкованих структурних підрозділів, які входять до складу структурних підрозділів, чию діяльність координує відповідний заступник;

виконавцями резолюції керівника структурного підрозділу визначаються спеціалісти відповідного підрозділу, про що інформуються керівники відповідних підпорядкованих підрозділів, що входять до складу цього структурного підрозділу;

виконавцем резолюції Голови ДСНС, заступників Голови ДСНС може бути будь-який підпорядкований відповідному керівнику співробітник, до компетенції якого належить зазначене в резолюції питання. Про визначення в резолюції виконавця інформується керівництво структурного та підпорядкованого підрозділу даного співробітника;

отримання заступником Голови ДСНС, керівником структурного або підпорядкованого підрозділу інформаційного повідомлення про створення керівником вищого рівня резолюції не передбачає створення відповідним керівником своєї резолюції до цього ж документа, а лише передбачає ознайомлення із документом;

резолюцією може бути визначено головного виконавця, співвиконавців, строки виконання, отримувачів документа “до відома”.

15. Документи надходять до їх виконавців на підставі накладених на них резолюцій.

Документ, виконавцями якого є кілька структурних підрозділів (посадових осіб), надходить одночасно до всіх його виконавців, визначених резолюцією чи переліком розсилки, створеним реєстратором або автором документа.

16. Керівники структурних підрозділів ДСНС опрацьовують документи, отримані внаслідок їх передавання через АСКОД за належністю, на підставі накладених на них резолюцій.

У разі необхідності керівник структурного підрозділу має право делегувати своєму заступнику розгляд частини документів, які надходять на опрацювання до структурного підрозділу.

17. Факти передавання документів виконавцям фіксуються в реєстраційній контрольно-моніторинговій картці із зазначенням інформації про виконавців, яким передано документ.

18. Зміна головного виконавця здійснюється в АСКОД на підставі резолюції керівника, який здійснював первинний розгляд документа.

19. Якщо для документа не встановлено строків виконання, а його опрацювання не потребує підготовки проекту документа на його виконання,відповідальний виконавець має право після ознайомлення з документом внести інформацію про спосіб виконання цього документа (питання вирішено в робочому порядку, взято участь у нараді тощо) та в установленому порядку передати до служби контролю для закриття його “до справи”.

Якщо документ розіслано для ознайомлення, відповідальний виконавець, співвиконавці вносять відмітку про їх ознайомлення, що підтверджується електронним цифровим підписом. У такому випадку в АСКОД генерується лист ознайомлення з документом, у якому зазначається перелік посадових осіб, яким було передано відповідний документ з позначкою про ознайомлення, у такому форматі: прізвище та ініціали, дата надходження електронного документа, дата ознайомлення.

1.11.4 Документування управлінської інформації в електронній формі

Загальні вимоги до створення документів:

1. Документування управлінської інформації в електронній формі полягає у створенні електронних документів, в яких фіксується інформація про управлінські рішення з дотриманням установлених цією Інструкцією правил.

2. Реквізити, визначені цією Інструкцією, вносяться в реєстраційну контрольно-моніторингову картку.

Бланки документів

3. Організаційно-розпорядчі документи ДСНС оформлюються на бланках, що виготовляються згідно з вимогами Інструкції з діловодства.

4. Документ у разі необхідності друкується разом із бланком, без застосування бланків, виготовлених друкарським способом.

5. Бланки документів, створених в електронній формі, не нумеруються та не обліковуються.

Дата підписання, засвідчення та реєстрації

6. Дата підписання електронного документа визначається електронною позначкою часу, що невід'ємно пов'язана з електронним цифровим підписом.

7. Дата засвідчення електронного документа визначається електронною позначкою часу, що невід'ємно пов'язана з електронною печаткою.

8. Дата реєстрації вихідного документа автоматично формується АСКОД (веб-модулем системи взаємодії) у реєстраційній контрольно-моніторинговій картці під час його реєстрації.

9. Обов'язковому датуванню у реєстраційній контрольно-моніторинговій картці підлягають усі службові відмітки, пов'язані з проходженням та виконанням документа (резолюції, відмітки про виконання документа, надсилання його до справи тощо).

Відмітки про наявність додатків

10. На додатках, що затверджуються відповідними актами (положення, інструкції, правила, порядки тощо), проставляється гриф затвердження відповідно до пункту 83 цієї Інструкції. У відповідних пунктах розпорядчої частини документа робиться посилання: "що додається" або "(додається)".

11. На додатках до наказу, положення, правил, інструкції тощо проставляється відмітка у верхньому правому куті першої сторінки додатка, яка включає номер додатка.

1.12 Відомча електронна поштова система

Відомча електронна поштова система ДСНС застосовується для обміну службовими документами каналами телекомунікаційних мереж ДСНС, а також мережею Інтернет [10, 11, 12].

До складу Відомчої електронної поштової системи входить центральний поштовий сервер апарату ДСНС та власні поштові сервери головних управлінь (управлінь) ДСНС України в областях та м. Києві, які побудовано на базі серверного програмного забезпечення, рекомендованого для використання апаратом ДСНС, та функціонують на під доменах dsns.gov.ua.

Відповідальні за адміністрування серверів, що входять до складу Відомчої поштової системи, визначаються внутрішніми наказами відповідних підрозділів ДСНС.

Відомча поштова система використовується в інформаційних цілях, у тому числі з метою інформування, організації роботи, забезпечення внутрішніх та зовнішніх комунікацій.

Обмін електронними повідомленнями в ДСНС та з зовнішніми адресатами здійснюється лише з використанням електронних поштових скриньок в домені dsns.gov.ua.

Закладам освіти, Державному центру сертифікації ДСНС України та Українському гідрометеорологічному центру дозволяється здійснювати обмін електронними повідомленнями в ДСНС та з зовнішніми адресатами з поштових скриньок у під доменах edu.ua та доменах dcs.gov.ua, meteo.gov.ua відповідно.

Обмін інформацією з використанням електронної пошти з використанням сторонніх поштових серверів у системі заборонено.

1.12.1 Загальні положенняз електронної поштової системи

Електронна поштова система (електронна пошта) – система пересилання (передачі) повідомлень будь-якого змісту в електронному вигляді між користувачами обчислювальних машин, в якій комп`ютер (чи інший термінал), підключений до суспільної (мережі загального користування) чи спеціальної телекомунікаційної мережі, приймає на себе функції із зберігання та пересилання повідомлень.

Поштовий вузол – програмно-технічний комплекс з відповідними програмним та технічним забезпеченням електронної пошти, у тому числі з програмними елементами інформаційної безпеки, для обслуговування своїх користувачів в межах гарнізону області.

Сервер електронної поштової системи (поштовий сервер, сервер електронної пошти) – поштовий вузол, територіально розташований в

апаратно-технічному приміщенні відділу оперативного зв’язку, телекомунікаційних систем та інформаційних технологій ОКЦ У ДСНС в області.

Абонент – підрозділ, який має електронну адресу, зареєстровану на сервері електронної поштової системи У ДСНС в області.

Поштова станція – персональна електронно-обчислювальна машина (далі – ПЕОМ) абонента Управління ДСНС України в області з відповідним програмним забезпеченням та допоміжними технічними пристроями.

Електронна поштова скринька (адреса) – область на жорсткому диску сервера електронної поштової системи, де на адресу конкретного абонента розміщуються електронні прийняті файли та файли на відправку.

Користувач – працівник У ДСНС в області, якому надаються послуги електронної пошти.

Відповідальний за роботу електронної пошти – фізична особа, що відповідає за роботу програмно-технічного комплексу сервера електронної поштової системи та поштових станцій ОКЦ У ДСНС в області.

Електронний документ – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа.

Черговий адміністратор:

– фахівець відділу оперативного зв’язку, телекомунікаційних систем та інформаційних технологій ОКЦ У ДСНС в області, який відповідає за роботу у відомчій електронній поштовій системі У ДСНС в області;

– диспетчер чергової зміни ОКЦ У ДСНС в області, який відповідає за роботу у відомчій електронній поштовій системі У ДСНС в області;

– черговий диспетчер (підмінний радіотелефоніст) підпорядкованого підрозділу У ДСНС в області, який відповідає за роботу у відомчій електронній поштовій системі У ДСНС в області.

Електронна поштова система є складовою частиною автоматизованої інформаційної системи управління пожежнорятувальними та аварійно-рятувальними підрозділами У ДСНС в області і надає можливість організовувати оперативний обмін інформацією між ними.

Відомча поштова система використовується в інформаційних цілях, у тому числі з метою інформування, організації роботи, забезпечення внутрішніх та зовнішніх комунікацій.

Обмін електронними повідомленнями в У ДСНС в області та з зовнішніми адресатами здійснюється лише з використанням електронних поштових скриньок в домені dsns.gov.ua.

Абонентами Відомчої поштової системи можуть бути тільки структурні та підпорядковані підрозділи У ДСНС в області.

Електронні поштові адреси Відомчої поштової системи за функціональним призначенням поділяються на:

офіційні електронні адреси – адреси, які зазначаються на офіційних бланках та веб-сторінках підрозділів, у тому числі адреси відділів,

секторів, служб та підпорядкованих підрозділів У ДСНС в області;

персональні поштові адреси – особисті поштові скриньки співробітників У ДСНС в області.

Для надання можливості користування послугами Відомчої поштової системи в підрозділах встановлюються поштові станції для абонентів мережі.

Для забезпечення працездатності Відомчої поштової системи та для координації роботи абонентів Відомчої поштової системи призначається особа, відповідальна за роботу Відомчої поштової системи та адміністрування поштового сервера (далі – Адміністратор).

Заявки про пошкодження працездатності поштової станції в підрозділах У ДСНС в області приймаються, реєструються (чи фіксуються) черговим адміністратором Відомчої поштової системи та передаються Адміністратору Відомчої поштової системи для подальшого усунення пошкоджень.

1.12.2 Правила користуванняелектронною поштовою системою

Вимоги при створенні паролів:

– пароль має налічувати щонайменше 8 символів, включаючи хоча б 1 маленьку, 1 велику літеру та 1 цифру;

– паролі не повинні містити персональної інформації (дати народження своєї та близьких, номерів телефонів, номерів та серій документів, що посвідчують особу, номерів власного автотранспорту, банківської картки, адреси реєстрації тощо);

– пароль не повинен використовуватися в будь-яких інших облікових записах в Інтернеті (соціальних мережах, банківських системах).

Заборонено використовувати Відомчу поштову систему для цілей, не пов’язаних з службовою діяльністю У ДСНС в області.

Заборонено здійснювати вхід до Відомчої поштової системи з персональних пристроїв, на яких не проведено антивірусні заходи.

При отриманні електронних повідомлень забороняється:

– відкривати вкладення в повідомленнях, якщо авторство цих повідомлень викликає сумнів;

– відкривати вкладення у листах, що містять файли з розширеннями: exe, bat, emd, vbs, svf, msi, pif, scr, hta, cpi, jar, msc, vb, vbs, vbe, js, jse, lnk, reg;

– переходити по посиланнях у листах, якщо адреса посилання та опис посилання відрізняються;

– переходити по посиланнях у листах, якщо посилання йде на сайти у доменних зонах *.ru, *.su;

– відкривати посилання і додатки у листах, написаних іноземною мовою, якщо у функціональні обов’язки власника електронної поштової адреси не входить обробка подібних повідомлень;

– відкривати вкладення, якщо в листі містяться помилки перекладу.

Заборонено повідомляти паролі для доступу до персональних електронних поштових адрес Відомчої поштової системи іншим особам.

Заборонено розсилати:

– конфіденційну інформацію, доступ до якої обмежено чинним законодавством, інформація для службового користування,

інформацію, яка містить державну таємницю, персональні дані громадян та матеріали, використання яких порушує права інтелектуальної власності;

– недостовірну інформацію, а також інформацію, що ображає честь і гідність інших осіб, що ганьбить ділову репутацію, пропагує ненависть та/або дискримінацію людей за расовими, етнічними, статевими, релігійними соціальними ознаками, що закладає основи до вчинення протиправних дій;

– матеріали, що містять віруси або інші комп'ютерні коди;

– файли, програми, призначені для порушення, знищення або

обмеження функціональності будь-якого комп'ютерного або телекомунікаційного обладнання; програми для здійснення несанкціонованого доступу.

Користувачі електронної пошти зобов'язані регулярно (не менше двох разів протягом робочого дня) перевіряти надходження пошти на свої електронні адреси.

При відправленні електронного повідомлення обов'язково необхідно:

– вказувати тему, яка відповідає його змісту;

– у разі додавання до електронного повідомлення файлів, зазначити про це в тексті електронного повідомлення;

– в кінці повідомлення використовувати підпис, вказуючи прізвище та ім'я, посаду, місце роботи (структурний підрозділ), номер телефону (службовий, за необхідності – мобільний);

– у разі відправлення багатотомного архіву декількома повідомленнями або декількох вкладень, що не можуть бути додані до одного

повідомлення, в кінці теми кожного такого повідомлення необхідно в дужках зазначити поточний номер частини/повідомлення та загальну кількість, наприклад: (частина 2 із 5).

Підстави для блокування поштової скриньки:

– виявлення здійснення розсилки листів, що містять шкідливі програми, спам, інформацію, поширення якої заборонено чинним законодавством;

– використання електронної пошти не за призначенням;

– при порушенні інших вимог Наказу У ДСНС в області .

Доступ до електронної поштової скриньки може бути відновлено після усунення причин блокування та інформування керівника відповідного структурного чи підпорядкованого підрозділу У ДСНС в області.

Видалення персональних електронних поштових адрес відбувається у разі:

– невикористання електронної поштової адреси (якщо до поштової скриньки не заходили протягом 365 діб);

– отримання Адміністратором звернення власника персональної електронної поштової адреси;

– зміни прізвища або імені власника персональної поштової адреси;

– отримання Адміністратором витягів з наказу про звільнення.

Видалення офіційних електронних поштових адрес здійснюється при отриманні Адміністратором витягу з наказу про ліквідацію підрозділів, їх перейменування чи реорганізацію.

При видаленні персональних електронних поштових скриньок по причині зміни прізвища або імені користувача, офіційних електронних поштових скриньок у зв'язку з перейменуванням структурних підрозділів дані з попередньої поштової скриньки переносяться в нову електронну поштову скриньку.

У разі систематичного (два і більше рази) порушення вимог,

зазначених у Наказі У ДСНС в області може бути притягнутий до дисциплінарної відповідальності.

1.12.3 Права та обов'язки абонента

Абонент має право:

– обмінюватись інформацією в електронному вигляді з поштовими станціями Відомчої поштової системи;

– отримувати консультації у відповідальної особи за роботу Відомчої поштової системи.

Абонент зобов'язаний:

– дотримуватись встановленого порядку роботи у Відомчій поштовій системі;

– виконувати розпорядження Адміністратора Відомчої поштової системи;

– здійснювати по електронній пошті щогодинні перевірки поштових скриньок на наявність вхідної пошти;

– з метою запобігання перевантажень сервера Відомчої поштової системи не допускати відправки поштової кореспонденції об'ємом понад 7 Мегабайт;

– забезпечити виконання вимог по роботі з кореспонденцією згідно затверджених інструкцій щодо порядку обміну інформацією у Відомчій поштовій системі.

Абонент несе повну відповідальність за розповсюдження у Відомчій поштовій системі програм-вірусів, що можуть пошкодити програмне забезпечення поштового сервера та комп'ютерів інших абонентів.

Абонент відповідає за цілісність наданого йому програмного забезпечення та за відсутність можливості несанкціонованого доступу до нього.

Список використаних джерел

Керівні документи

1. Кодекс цивільного захисту України
Кодекс цивільного захисту Ук... | від 02.10.2012 № 5403-VI (rada.gov.ua).

2. Закон України «Про систему екстреної допомоги за єдиним телефонним номером 112» (Відомості Верховної Ради України (ВВР), 2012, № 49, ст.560)
Про систему екстреної допомо... | від 13.03.2012 № 4499-VI (rada.gov.ua).

3. Постанова Кабінету Міністрів України №11 від 9січня 2014р. «Про затвердження Положення про єдину державну систему цивільного захисту»
Про затвердження Положення про єд... | від 09.01.2014 № 11 (rada.gov.ua)

4. Постанова Кабінету Міністрів України № 733 від 27 вересня 2017 р. Про затвердження Положення про організацію оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій та зв'язку у сфері цивільного захисту
Про затвердження Положення про о... | від 27.09.2017 № 733 (rada.gov.ua)

5. Порядок організації роботи відомчої цифрової телекомунікаційної мережі ДСНС Наказ ДСНС 23.10.2019 № 608
Наказ ДСНС України – ДСНС України (dsns.gov.ua)

6. Наказ МВС України 08.02.2019 № 93 Про затвердження Інструкції щодо практик чи процедур проектування, дослідження, введення в експлуатацію, експлуатації та технічного обслуговування (супроводження) автоматизованих систем централізованого оповіщення.
Про затвердження Інструкції щодо ... | від 08.02.2019 № 93 (rada.gov.ua)

7. Наказ МВС України 20.10.2017 № 870 Про затвердження Положення про автоматизовану інформаційну систему оперативного призначення єдиної інформаційної системи МВС.
Про затвердження Положення про а... | від 20.10.2017 № 870 (rada.gov.ua)

8. Деякі питання оперативно-технічного управління телекомунікаційними мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану Постанова Кабінету Міністрів України від 29 червня 2004 р. N 812 Київ.
Деякі питання оперативно-технічн... | від 29.06.2004 № 812 (rada.gov.ua).

9. Наказ ДСНС 03.12.2018 № 700 Інструкція з документування управлінської інформації в електронній формі та організації роботи з електронними документами в діловодстві, електронного міжвідомчого обміну в Державній службі України з надзвичайних ситуацій.Наказ ДСНС України – ДСНС України (dsns.gov.ua)

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

11. Наказ ДСНС від 22.03.2019 № 183 Про використання відомчої електронної поштової системи

Література

12. В. О. Собина, Д. В. Тарадуда, М. М. Піксасов, Л. В. Борисова, О. В. Закора, А. Б. Фещенко, М.В. Маляров, Д. Л. Соколов, Дослідження проблем функціонування системи зв'язку ДСНС, використання засобів телекомунікацій та інформатизації в системі ДСНС, шляхів їх розвитку із застосуванням сучасних телекомунікаційних та інформаційних технологій, Звіт про НДР: № держреєстрації 0119U001009, Х.: НУЦЗУ, 2020. – 85 с. Режим доступу: http://ndr.dsns.gov.ua/?p=7135 .

13. В.А. Балашов, А.Г. Ляшко, Л.М. Ляховецкий. Технологии широкополосного доступа xDSL. Инженерно-технический справочник / Под общей редакцией В.А. Балашова. – М.: Эко-Трендз, 2009. – 256 с.: ил. – ISBN: 978-5-88405-086-0.

14. Каток В. Б. Стандартизация физической телекоммуникационной инфраструктуры ПАО "Укртелеком" -2019. – 51с. Інтернет ресурс: PowerPoint Presentation (itu.int)

15. Довгий С.О., Воробієнко П.П., Гуляєв К.Д. Сучасні телекомунікації: Мережі, технології, безпека, економіка, регулювання. – Видання друге (доповнене). – / За загальною ред. Довгого С.О. – К.: «Азимут-Україна». – 2013. – 608 с.

16. Скляр Бернард. Цифровая связь: теоретические основы и практическое применение / Скляр Б.; Гроза Е.Г. [и др.] (пер. с англ.). – 2-е изд. – М. [и др.] : Вильямс, 2016. – 1099 с.: ил., табл.

17. Сторчак К.П., Ткаленко О.М. Системи розподілу інформації. Навч. посібник, підготовлено для студентів вищих навчальних закладів – Київ: ДУТ, 2018. – 98с.

18. Недашківський О.Л. Перспективні компоненти та засоби інфокомунікаційних технологій, курс лекцій – Київ: ДУТ, 2018. -199 с.

19. Соколов В.Ю. Інформаційні системи і технології: Навч. посіб. – К. : ДУІКТ, 2010. – 138 с

20. Сучасні телекомунікаційні мережі у цивільному захисті: Підручник. / Г.В. Щербак, Л.І. Мельникова, І.В. Рубан, К.В. Садовий, Д.В. Сумцов. – Харків, УЦЗУ, 2007. – 261 с

21. Чуб І.А. та ін. Автоматизовані системи управління та зв`язок у цивільному захисті. – Харків: АЦЗУ, 2005.-240 с.
22. АСКОД система електронного документообігу (АСКОД WEB), інструкція користувача. К.: Інфоплюс центр комп'ютерних технологій. 2019. -145 с.
23. Система електронного документообігу «M.E.doc» звітність, посібник користувача. К.: ЦСК "Україна". 2018. -88 с.
24. Поппель Г., Голдстайн Б. Информационная технология – миллионные прибыли. М.: Экономика, 1990. – 240 с..

Питання та завдання для самостійного контролю знань

Теми аналітичних оглядів

1. Класифікація, склад і принципи побудови АІСУ в пожежно-рятувальній службі.
2. Урядова інформаційно-аналітична система з питань надзвичайних ситуацій
3. Технічні вимоги до програмно-апаратного комплексу системи оперативно-диспетчерського управління силами та засобами ДСНС України (СОДУ), як функціональної підсистеми Єдиної інформаційної системи МВС України.

Контрольні питання

1. Поняття, класифікація й види сучасних інформаційних технологій
2. Телекомунікації в цивільному захисті
3. Загальнодержавні телекомунікаційні мережі спеціального зв’язку та загального користування.
4. Побудова відомчої цифрової телекомунікаційної мережі ДСНС України
5. Порядок організації роботи відомчої цифрової телекомунікаційної мережі ДСНС
6. Система електронного документообігу в ДСНС
7. Загальне призначення і класифікація інформаційних систем
8. Єдина інформаційна система Міністерства внутрішніх справ та переліку її пріоритетних інформаційних ресурсів
9. Концепції розвитку та технічної модернізації системи централізованого оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій
10. Урядова інформаційно-аналітична система з питань надзвичайних ситуацій
11. Автоматизована система оперативно-диспетчерського управління

РОЗДІЛ 2.ОСНОВИ ТЕХНІЧНОЇ ЕКСПЛУАТАЦІЇ І ТЕОРІЇ НАДІЙНОСТІ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

На сучасному етапі розвитку галузі зв'язку велике значення мають організація технічної експлуатації систем та мереж зв'язку України і підготовка фахівців у цьому напрямі.

Нижче коротко викладено: загальні положення та методи технічної експлуатації, загальні положення систем технічного обслуговування оперативного управління та їх завдання. Розглянуті основні параметри систем технічної експлуатації, приведені рекомендації для вибору методів експлуатації.

Досліджено: зв'язок методів експлуатації з методами контролю та оцінка ефективності мережі зв'язку, різновидності систем технічної експлуатації і управління в галузі зв’язку, мережа управління телекомунікаціями (TMN); розвиток управління первинною мережею України; технічне обслуговування систем передавання і апаратури, каналів, трактів СЦІ; автоматизація процесів технічної експлуатації в мережних вузлах (станціях) первинної мережі та програмно-технічні засоби.

Приведені та досліджені параметри і характеристики каналів і трактів аналогових систем передачі;. параметри каналів і трактів ЦСП та методи їх вимірювання.

Приведені сучасні поняття про надійність первинної мережі ЄНСЗУ, оптимізація рішень при проектуванні та організації технічної експлуатації ВОСП за критерієм надійності.

Основою побудови майбутніх телекомунікаційних систем зв'язку можна вважати три основні технології: технологія послуг; технологія телекомунікаційних мереж; технологія компонентів, з яких складається телекомунікаційна мережа. З рис.В1 видно що для створення телекомунікаційних систем необхідною умовою є розвиток технології компонентів. Десь у 1965 році Гордон Мур передбачав, що з кожним роком число транзисторів в чіпі буде подвоюватись. По даним фірми INTEL в її мікропроцесорах це подвоєння відбувається кожні 18 місяців. Сьогодні лабораторії працюють над так званими болістичними транзисторами, час переключення в котрих 10^{15}, що в 10 мільйонів разів швидше ніж зараз. Наступний етап-створення одно-електронного транзистора, в котрому біт інформації є одинокий електрон, що являє собою абсолютну межу в сучасному розумінні фізичних законів.

Головним критерієм в розвитку фотоніки прийнято вважати швидкість передавання по системам оптичного зв’язку та відстань, на котру може бути запроваджене передавання сигналу без регенерації.

Для підтримки технології послуг зв'язку необхідна технологія телекомунікаційних мереж(ТКМ), складові котрої видно з рис. 2.В.

До складу технологій телекомунікаційних мереж входять: архітектура мережі; функції підтримки послуг технології експлуатації; системи передавання.

Практично розділ присвячений функції підтримки послуг технології експлуатації.

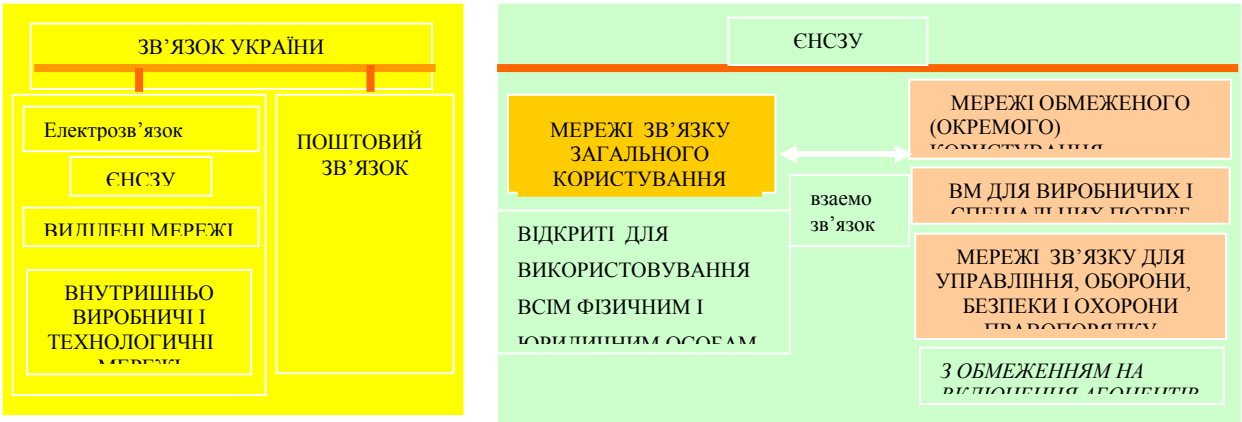


Рис. 2.В – Основні технології побудови майбутніх телекомунікаційних систем

2.1 Основи технічного забезпечення, експлуатації телекомунікаційних систем та мереж

2.1.1 Загальні положення та завдання технічного забезпечення й експлуатації телекомунікаційних систем та мереж

Основна функція систем зв'язку – забезпечення споживачів технічною можливістю для обміну інформацією за даними показниками надійності та якості. Таку можливість забезпечує єдина національна система зв'язку України (ЄНСЗУ).Вона забезпечує споживачів послуг електрозв'язку навсій території України. Склад такої мережі і її архітектура приведені на рис.2.1а, 2.1б, і 2.2 відповідно. Ця функція реалізується за допомогою мереж електро, радіо та поштового зв'язку.



а) б)

Рис. 2.1 – Зв'язок Україниа) загальна структура б) склад ЄНСЗУ

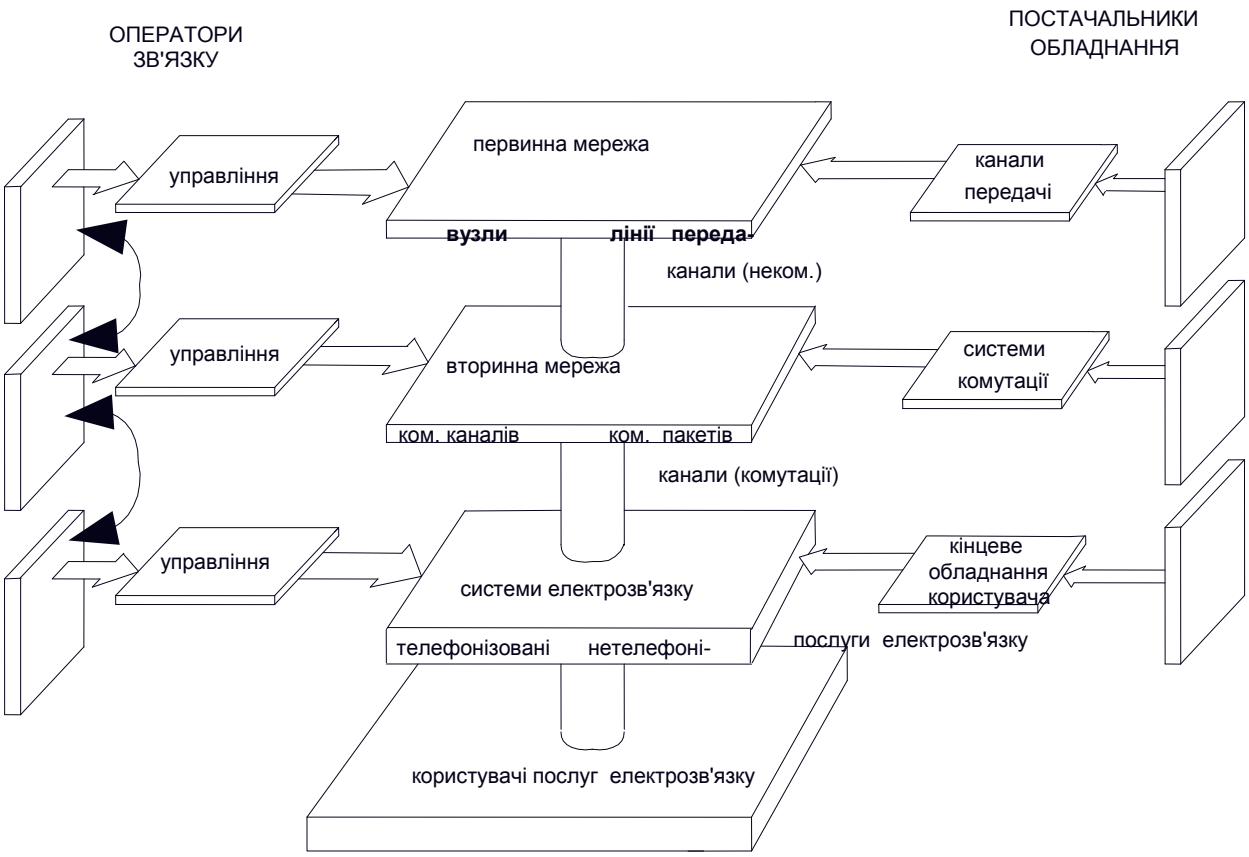


Рис. 2.2 – Архітектура ЄНСЗУ

Основні функції управління технологічними процесами в мережах зв'язку (МЗ) виконуються технологічним обладнанням автоматично, без участі людини. Обладнання не є ідеально надійним. В ньому безперервно проходять процеси розладу, які викликають зниження якості його роботи (виникнення відмов, збоїв та інше). Погіршення якості роботи технологічного обладнання викликає збільшення втрат інформації за рахунок відхилення параметрів технологічних процесів від номінальних значень.

Для того, щоб параметри технологічних процесів більшу частину часу знаходились близько до номінальних значень (в заданих відхиленнях), необхідно виконувати контроль і поновлення обладнання, тобто виконувати технологічне обслуговування.

Технічна експлуатація (ТЕ) – сукупність дій, направлених на підтримку необхідної (заданої) ефективності функціонування технологічного обладнання МЗ. Поняття "технічна експлуатація" більш широке, ніж поняття "технічне обслуговування", бо включає в себе питання організації та управління технічним обладнанням і мережею. Функціональна структура технічної експлуатації мережі зв'язку приведена на рис. 2.3.

Система ТЕ – сукупність методів і алгоритмів управління, програмних і технічних засобів, експлуатаційного персоналу, матеріальних ресурсів, які виконують технічну експлуатацію обладнання і мереж за заданими критеріями управління. СТЕ можна розглядати як багаторівневу

систему управління, в котрій первинним об'єктом управління е технологічне обладнання мережі зв'язку (рис 2.4).

Критерії управління визначаються вибраними показниками ефективності СТЕ.

Основні принципи побудови СТЕ:

– раціональна концепція ресурсів і засобів обслуговування;

– організація функцій контролю і управління;

– раціональна автоматизація процесів збору, обліку і обробки інформації; оптимальне управління.

При вирішенні завдань автоматизації і створенні комплексу технічних засобів СТЕ необхідно враховувати велику кількість контрольованих нормативних параметрів, територіальну рознесеність технологічного обладнання.

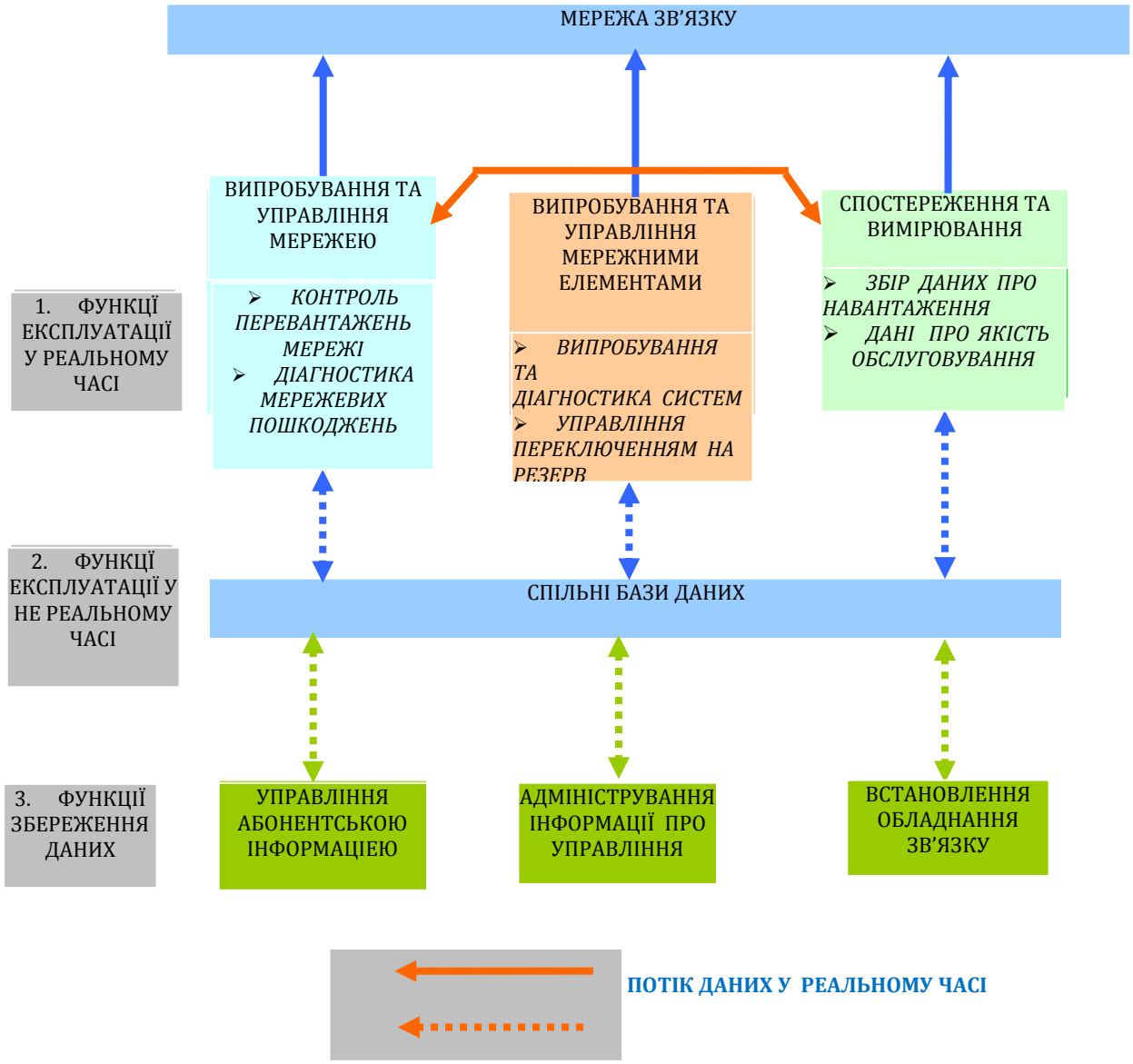
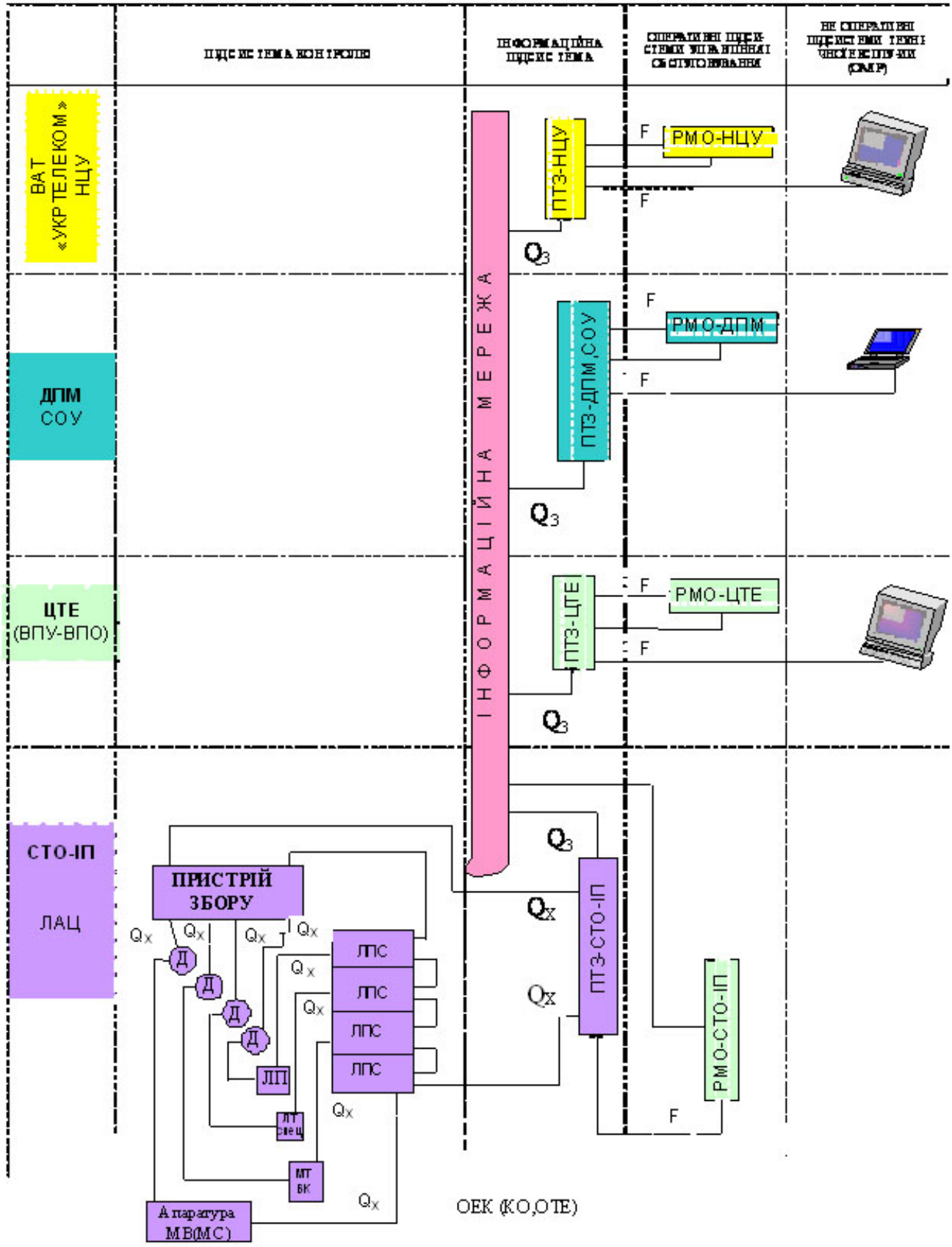


Рис. 2.3 – Функціональна структура ТЕ мережі зв'язку



Основними складовими СТЕ є системи оперативно-технічного обслуговування (СОТО) і оперативно-технічного управління (СОТУ). При автоматизації процесів СОТО і СОТУ вони стають автоматизованими системи – АСОТО і АСОТУ, а СТЕ – АСТЕ.

В галузях зв'язку СТЕ, АСТЕ звичайно будуються за територіально-ієрархічним принципом і включають в себе відповідні ієрархічні рівні.

Основні завдання технічної експлуатації:

– забезпечення ефективного функціонування основних напрямків галузі зв'язку, наприклад, первинної мережі

ЄНСЗУ, при заданій якості та експлуатаційній надійності трактів і каналів передачі;

– подальший розвиток первинної мережі (ПМ) ЄНСЗУ, реконструкція мережних вузлів і станцій МВ (МС) та ліній передачі для задоволення потреб народного господарства і населення;

– систематичне вдосконалення мережі, поліпшення характеристик апаратури, обладнання трактів і каналів передачі.

2.1.2 Загальні положення системи технічного обслуговування та її завдання

Система (автоматизована) оперативно-технічного обслуговування СОТО. (АСОТО), наприклад первинної магістральної мережі (ПММ) ЄНСЗУ, призначена для забезпечення працездатності мережі ЄНСЗУ, утримання споруд, обладнання, апаратури трактів і каналів передачі в межах встановлених експлуатаційних норм. Спрощена структурна схема СОТО приведена на рис 2.5.

Основні завдання СОТО (АСОТО):

– експлуатаційний контроль якості об’єктів експлуатаційного контролю (ОЕК) та їх елементів для виявлення, попередження і прогнозування відмов і підтримання якісних показників споруд, обладнання, апаратури трактів і каналів передачі в заданих межах;

– обробка і аналіз одержаних результатів контролю і, при необхідності, подача заявок і виведення з експлуатації трактів і каналів передачі для усунення виявлених пошкоджень;

– аналіз первинних сигналів і визначення характеру і місця несправності на своєму вузлу (станції), в зоні технічного обслуговування і прилеглої ланки;

– перебудова мережі та введення (відбій) графіків обходів і замін за командами СОТУ (АСОТУ);

– створення постійних банків даних СОТО (АСОТО) точок проходження трактів передачі у вузлу (станції);

– створення карт маршрутів трактів і каналів передачі для різних ситуацій та корекція документації, видача за запитами інформації для обслуговування у відповідній формі;

– облік і контроль виконання директив, постанов, наказів Департаменту зв’язку МТЗ України та вказівок і рекомендацій ВАТ «Укртелеком»;

– реалізація вибраних методів СОТО (АСОТО) на мережі зв’язку та інші.

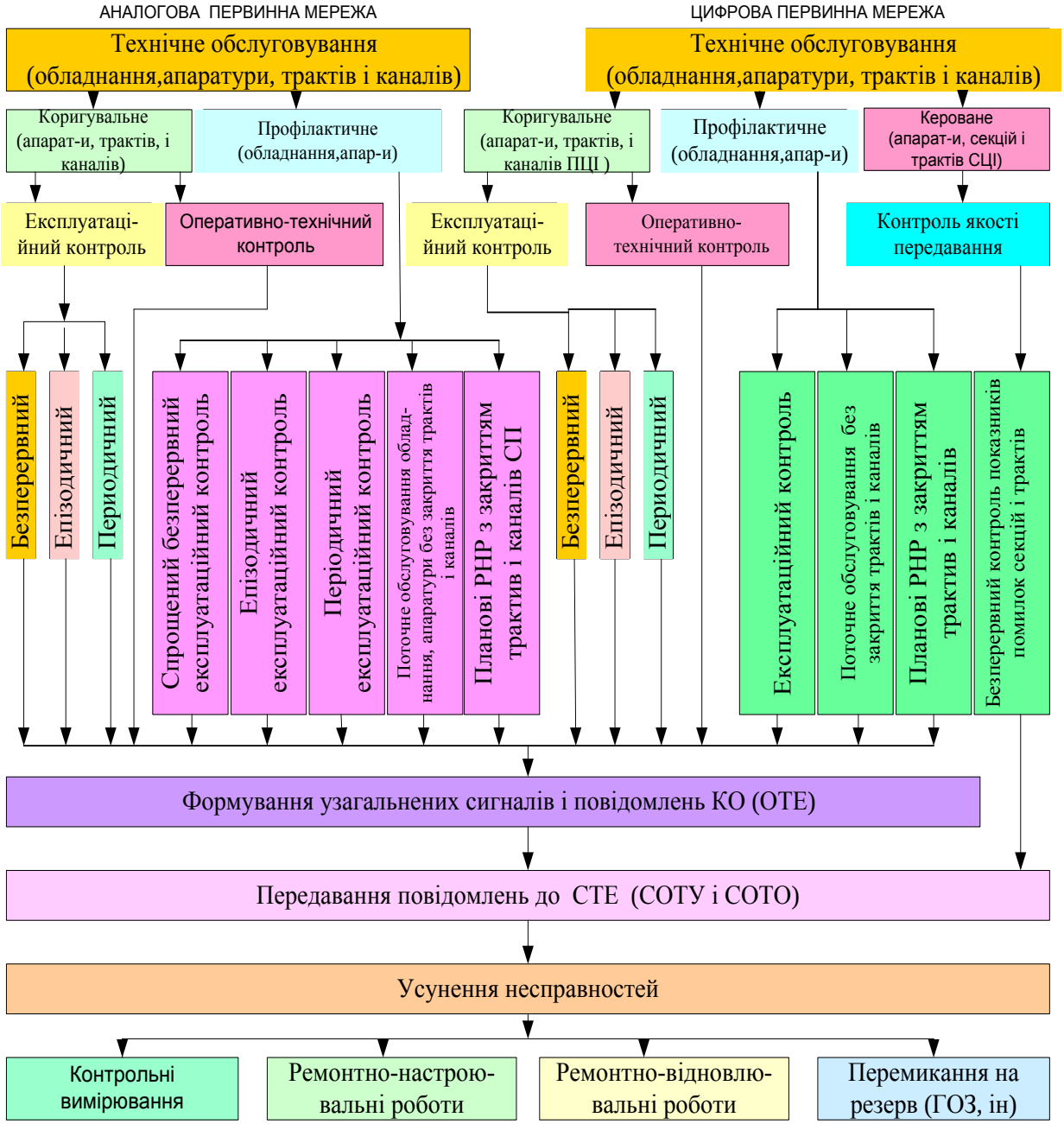


Рис. 2.5 – Спрощена структурна схема технічного і оперативно-технічного обслуговування обладнання, апаратури, трактів і каналів передавання первинної мережі.

2.1.3 Загальні положення та завдання системи оперативного управління

Система (автоматизована) оперативно-технічного управління (СОТУ) призначена для забезпечення функціонування первинної мережі ЄНСЗУ при будь-яких змінах її стану, ефективного використання всіх її можливостей в інтересах вторинних мереж, інших споживачів, скорочення часу поновлення трактів і каналів та підвищення продуктивності праці оперативно-технічного персоналу.

Основні завдання СОТУ (АСОТУ):

– визначення змін стану КО (контрольованих об'єктів);

– збір і аналіз повідомлень про зміну стану КО;

– визначення несправної ланки КО (за рівнями КЧ чи іншим методом);

– прийняття рішень і видача команд підрозділам СТЕ (СОТУ і СОТО) на проведення ремонтно-поновлюючих робіт для усунення несправності, на застосування рухомих вузлів, контроль за ходом робіт по ліквідації несправностей відповідно до прийнятих алгоритмів;

– управління перебудовою на первинній мережі ЄНСЗУ за складним в оперативних умовах або попередньо складеним графіком обходів і замін;

– контроль за введенням і зняттям обходів і змін, розвитком та вдосконаленням СОТУ (АСОТУ) та інше;

– завдання планування.

Система оперативно-технічного управління будується за територіально-ієрархічним принципом.

На первинній мережі ЄНСЗУ введені таки типи КО [7]:

– мережний вузол (станція), який складається з елементів КО-МВ(МС) – цеху електроживлення, ЛАЦ, пожежно-охоронного обладнання та апаратури життєзабезпечення (рис. 2.6)

– лінія передачі, яка розбивається, у випадку необхідності, на ланки КО-ЛП (рис. 2.7)

– лінійний тракт, який розбивається на ланки КО-ЛТ (рис. 2.8)

– мережний тракт, який розбивається, у випадку необхідності, на ланки КО-МТ (рис. 2.9).

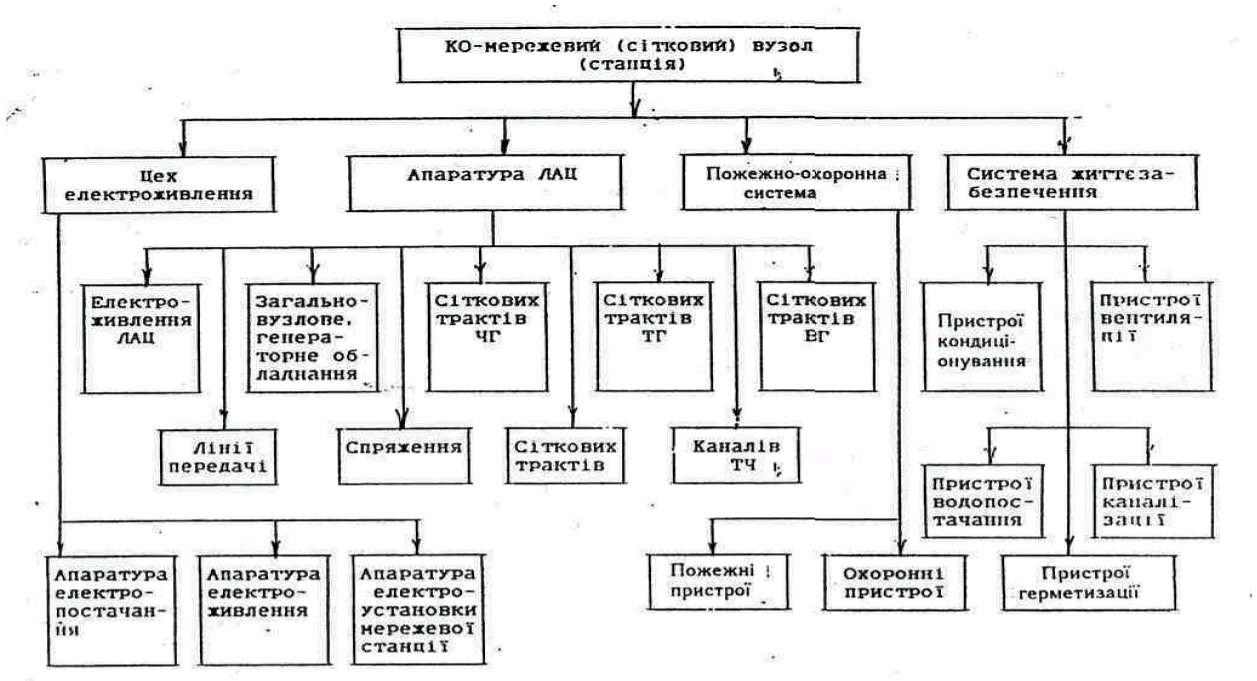


Рис. 2.6 – Структурна схема мережного вузла (станції)

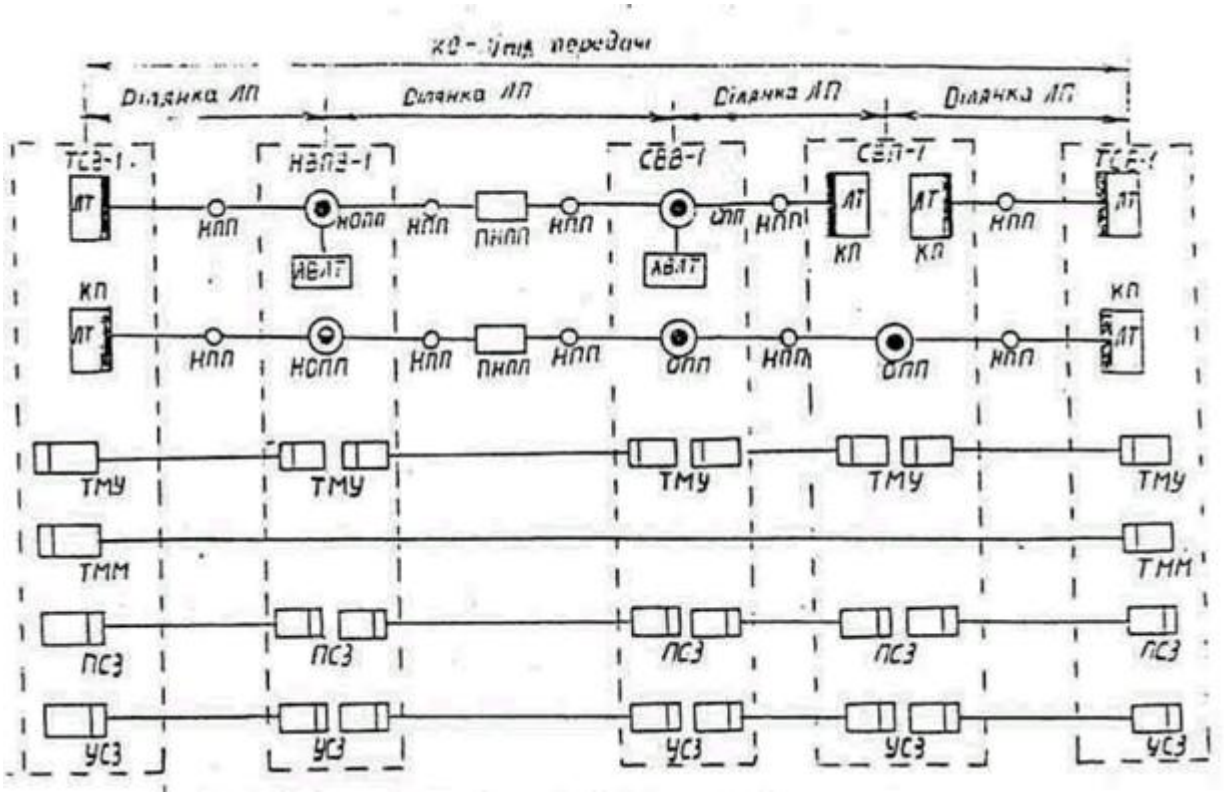


Рис. 2.7 – Структурна схема побудови лінії передачі

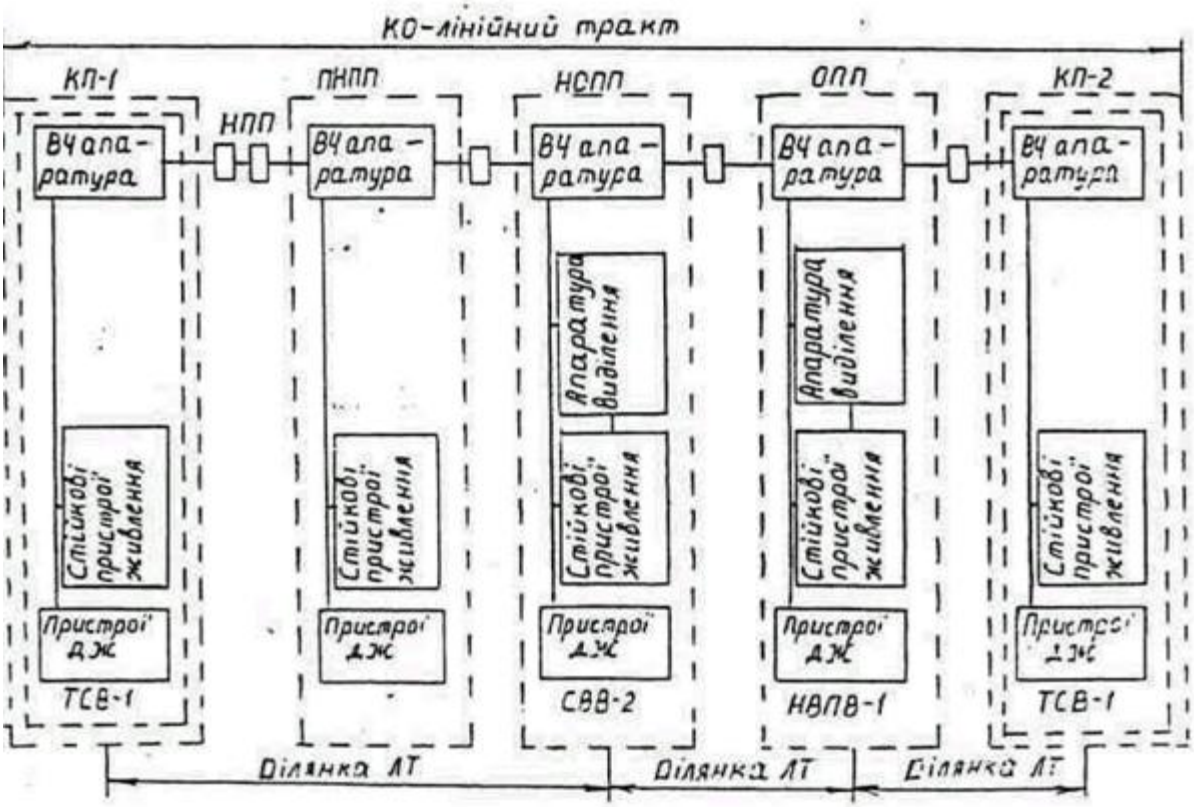


Рис. 2.8 – Структурна схема побудови лінійного тракту

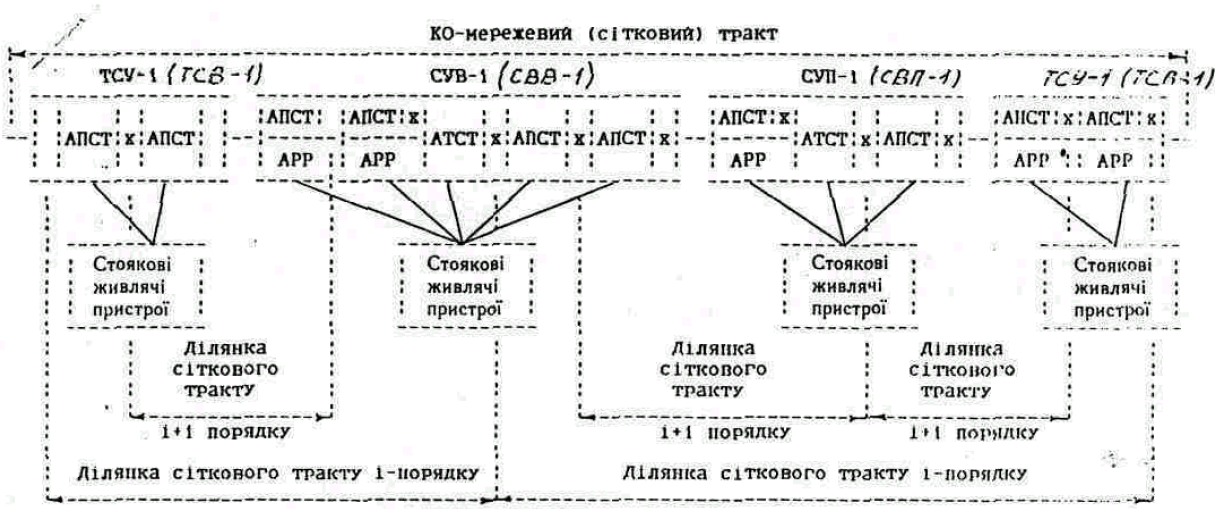


Рис. 2.9 – Структурна схема утворення мережного тракту

В процесі оперативно-технічного контролю за станом первинної мережі наєНСЗУ формуються загальні сигнали про стан КО,ОТЕ: "аварія", "пошкодження", "попередження", "норма".

"Норма" – стан, при якому параметри якості передачі і показники режиму та умов роботи КО і його елементів знаходяться в межах установлених допущень.

"Попередження" – стан, при якому параметри якості передачі знаходяться в межах встановлених допущень, а показники роботи елементів КО, які визначають режим і умови роботи КО, свідчать про підвищену можливість відмови КО;

"Попередження" – технологічний сигнал, який передасться в ЦТЕ або ДПМ. Перелік таких сигналів визначає Укртелеком.

"Пошкодження" – стан, при якому параметри якості передачі вийшли за встановлені межі допущення в результаті порушення режиму чи умов роботи КО та його елементів, але присутність пошкоджень в ньому дозволяє часткове використання на мережах цього КО;

"Аварія" – стан, при якому визначені для контролю параметри якості передачі вийшли за встановлені межі в результаті порушення режиму чи умов роботи КО. Наявність пошкодження в ньому приводить до неможливості його використання на мережі.

Для мереж синхронної цифрової Ієрархії(СЦІ) введено поняття об’єкта технічного обслуговування(ОТЕ) аналогічного КОце: мультиплексна секція(MSOH),регенераційна секція(RSOH) та тракти віртуальних контейнерів(VKn).

В аналогових, цифрових ПЦІ, СЦІ системах для технічної експлуатації і ТО є важливе поняття об’єкт експлуатаційного контролю (ОЕК).В них можуть проводитись вимірювання за допомогою зовнішніх вимірювальних приладів чи за допомогою вбудованої апаратури контролю, а в

СЦІі за допомогою автоматизованої системи обслуговування. В СЦІ до них відносяться:

– інтерфейси NNI;

– компонентні тракти ПЦІ, утворені за допомогою обладнання СЦІ;

– тракти СЦІ (тракти віртуальних контейнерів VC);

– регенераційні секції;

– мультиплексні секції;

– наскрізні з’єднання (ТС) на швидкості STM-1;

– компонентні тракти STM-1, утворені за допомогою обладнання СЦІ.

– наскрізні з’єднання (ТС) на швидкості STM-1;

– компонентні тракти STM-1, утворені за допомогою обладнання СЦІ.

2.1.4 Основні параметри системи технічної експлуатації

В залежності від їх призначення можливий розподіл на три групи:

– глобальні параметри;

– структурні параметри;

– функціональні параметри.

Глобальні параметри займають особливе місце. Вони визначають ідеологію і методи технічної експлуатації. Глобальні параметри не змінюють своїх значень при тиражуванні і значно менше змінюються, порівняно з іншими параметрами, в процесі розвитку СТЕ. Це найбільш консервативні параметри системиЇх зміна пов'язана зі зміною типів технічного обладнання СТЕ, програмного забезпечення, методів експлуатації, що в свою чергу пов'язано зі значними витратами.

Вибір глобальних параметрів – це в першу чергу вибір методів експлуатації, котрі залежать від багатьох факторів, таких як надійність обслуговування обладнання; укомплектованість мережі автоматичною контрольно-вимірювальною апаратурою; наявність обладнання діагностики і можливостей автоматичного усунення несправностей; наявність обладнання обробки та аналізу експлуатаційних даних.

До структурних параметрів можна віднести ті параметри, які задають територіальну структуру СТЕ. Сучасні системи ТЕ виконуються з застосуванням автоматизованих систем, до складу яких входять декілька (від трьох до п'яти) ієрархічних рівнів (рис.2.4).

Так, до першого рівня відносять контроль працездатності систем передачі і ліній передачі за допомогою засобів вбудованих в апаратуру СП або спеціально розроблених засобів.

До другого рівня відносять централізований комплекс, котрий взаємодіє з засобами першого рівня і координує їх роботу.

На третьому рівні виконуються завдання аналізу характеристик і підтримки працездатності мережі в цілому.

При відомих значеннях глобальних і структурних параметрі в можливо вирішити завдання вибору значень функціональних параметрів СТЕ, котрі визначають режим її функціонування. Це найменш стійкі параметри системи, котрі можливо розподілити на параметри потужності та управління.

Основними параметрами потужності підсистем СТЕ є чисельність експлуатаційного персоналу і рівень запасів резервного обладнання.

До параметрів управління відносять параметри систем, з допомогою яких можливо виконати зміну режимів функціонування керованих елементів (елементів систем зв'язку) під дією управляючої інформації, тобто параметри:

– контролю, які визначають межі стану відмови обладнання;

– управління відновлюючими роботами (або просто параметрами відновлення), які визначають пріоритетне обслуговування заявок, політику управління запасами (періодичність поновлення запасів, об'єм партії, правила поставляння замовлення).

2.2 Методи технічної експлуатації

Зараз відомі і використовуються профілактичний, поновлюючий, статистичний методи та їх комбінації.

Основною ознакою розподілу в цій класифікації є спосіб виявлення та попередження відмов.

2.2.1 Профілактичний метод

Профілактичний метод раніше був найбільш розповсюджений для технічної експлуатації систем зв'язку. Метод полягає в проведенні поточного обслуговування: – профілактичних перевірок і вимірювань показників якості обладнання, апаратури, планово-попереджувального ремонту. Період між перевірками менший, ніж середній термін служби кожного блоку апаратури.

Профілактичний метод не потребує капітальних витрат на контрольно-вимірювальну апаратуру, що вважається його перевагою.

Основні недоліки профілактичного методу – це велика трудомісткість і пов'язані з нею високі експлуатаційні витрати. Досвід експлуатації систем передачі засвідчує, що проведення профілактичного обслуговування (вимірювань, регулювання та ін.), постійна присутність обслуговуючого персоналу в ЛАЦ знижують надійність роботи апаратури і ефективність мережі в цілому.

Профілактичний метод експлуатації передбачає повну відсутність безперервного автоматичного чи автоматизованого контролю. Виявлення чи попередження відмов виконується за допомогою планових профілактичних перевірок, планового поточного та капітального ремонту.

2.2.2 Поновлюючий метод

При поновлюючому методі контроль і поновлення обладнання відбуваються за потоком відмов. Відмова – повна зупинка функціонування елементу системи. Контроль якості функціонування відсутній. Профілактичні роботи не проводяться. Обладнання, яке знаходиться в стані відмови, блокується. Носієм інформації про відмову є технічний сигнал, який виробляється вбудованою апаратурою контролю, або заявка абонента.

2.2.3 Статистичний метод

При статистичному методі експлуатації переважає безперервний контроль якості функціонування обладнання. Поновлення обладнання також проводиться за потоком відмов. Однак відмова розуміється в більш широкому понятті, ніж при поновлюючому методі. В цьому разірозглядається науково обґрунтований рівень втрат в системі зв'язку. Величина втрат визначається як результат послідовного статистичного аналізу спостережень. Для статистичного методу необхідний збір і аналіз статистичного матеріалу про роботу обладнання. Цей метод не виключає профілактичних перевірок і вимірювань, а імітує їх об'єм, завдяки застосуванню методів математичної статистики для збору і обробки даних про стан обладнання (внб1рковий метод спостережень). Для використання цього методу необхідні досить великі витрати на аналіз одержаної інформації.

Метод дуже перспективний і дає значний економічний ефект при використанні автоматизованих (автоматичних) вимірювальних комплексів для контрольних вимірювань каналів, трактів і апаратури без закриття їх дії з наступним аналізом результат є вимірювань на ЕОМ.

2.2.4 Вибір методу експлуатації

В реальних системах зв'язку жоден із розглянутих методів експлуатації не зустрічається в чистому вигляді, тому що кожен з них має свої недоліки. Профілактичний метод має цілий ряд недоліків, в тому числі: низьку оперативність виявлення відмов, велику трудомісткість, додатковий потік відмов, які виникають при проведенні профілактичних робіт.

Поновлюючий метод найбільш економічний, однак він не забезпечує потрібної якості зв'язку. Він найбільш ефективний там, де необхідна висока оперативність виявлення відмов і заздалегідь відомо, що відмови пов'язані із значними втратами. Однак в чистому вигляді даний метод не знайшов застосування, головним чином через неможливість створення апаратури контролю, яка може без затримки сигналізувати про всі відмови і пошкодження обслуговуваної апаратури.

Статистичний метод позбавлений недоліків інших методів, однак його застосування, як правило, потребує створення дорогої системи контролю.

В кожній технологічній підсистемі застосовується комбінація поєднання вказаних методів експлуатації. При цьому, як правило, присутні поновлюючий метод для виявлення і усунення великих аварійних відмов і профілактичний або статистичний метод, для виявлення і усунення решти відмов і попередження відмов (в тому числі і аварійних).

Вибір методів експлуатації розглядаємо як вибір в кожній технологічній підсистемі СТЕ оптимальної повноти безперервного автоматизованого контролю. В цілому для СТЕ оптимальним вирішенням може стати комбінація трьох методів експлуатації. Такий метод часто називають "статистично-контрольно-коригуючим", маючи на увазі той факт, що при застосуванні цього методу необхідні постійний збір і аналіз статистичних даних про різні параметри контрольованої апаратури, що дозволяє своєчасно коригувати характеристики, які не відповідають нормам. Комбінований метод є найбільш перспективним, бо забезпечує найвищу ефективність праці обслуговуючого персоналу при заданих вимогах до ефективності роботи мережі

Застосування цього методу проводиться із окремого приміщення за допомогою спеціального обладнання, котре забезпечує постійний статистичний контроль за якістю каналу, тракту, апаратури і систематичний аналіз одержуваних даних. На практиці застосовують загальні положення ТЕ, які приведені в розділі 4 КНД – 45-162-2000:

2.2.5 Загальні положення з технічної експлуатації

Забезпечення ефективного функціонування первинної мережі ЄНСЗ України, при визначеній якості і експлуатаційній надійності трактів і каналів передавання, досягається шляхом відповідної організації технічного обслуговування і оперативно-технічного управління первинною мережею.

Технічне обслуговування (ТО) повинно забезпечувати організацію і підтримування в необхідних межах установлених норм будь-яких ОТЕ первинної мережі, до яких зокрема відносяться технічні засоби електрозв'язку, які є складовою частиною з'єднання в трактах і каналах передавання.

На рис. 2.5 приведена спрощена структурна схема технічного та оперативно-технічного обслуговування обладнання, апаратури, трактів і каналів передавання первинної мережі.

ОТЕ первинної мережі повинні мати стик технічної експлуатації для обміну сигналами контролю і управління, а також обладнання і засоби для підтримування працездатності технічних засобів електрозв'язку.

Для прикладу можна навести такі ОТЕ (КО):

– ЛП та ділянки ліній передавання (ДЛП) кабельних, радіорелейних і супутникових систем передавання (СП);

– ЛТ та ділянки лінійних трактів (ДЛТ);

– МТ та ділянки мережних трактів (ДМТ);
– канали передавання (КП);
– мультиплексні і регенераційні секції цифрових систем передавання (ЦСП) синхронної цифрової ієрархії (СЦІ);
– апаратура і обладнання мережевих вузлів (станцій).

Перелік ОТЕ (КО) і формування узагальнених оцінок їх стану наведені нижче в розділі 8 цього КНД.

Прикладом сучасних ОТЕ є мультиплексні і регенераційні секції ЦСП СЦІ.

Використовуються такі методи ТО:

профілактичне технічне обслуговування (ПТО), яке за допомогою комплексу організаційно-технічних заходів забезпечує своєчасне попередження появи відмов або погіршення функціонування ОТЕ (КО) і усунення пошкоджень шляхом виконання ПТО через визначені проміжки часу або у відповідності з заздалегідь установленими критеріями, в основному, з закриттям трактів і каналів передавання на визначений час;

коригувальне технічне обслуговування (КТО), яке після визнання стану непрацездатності ОТЕ за допомогою комплексу організаційно-технічних заходів забезпечує виявлення несправностей та їх усунення шляхом виконання КТО, в основному, без виведення із експлуатації трактів і каналів передавання;

кероване технічне обслуговування (ОТК), яке за допомогою комплексу організаційно-технічних заходів забезпечує зведення до мінімуму профілактичного технічного обслуговування та скорочення коригувального технічного обслуговування шляхом виконання ОТК за допомогою методів аналізу стану ОТЕ з використанням засобів контролю робочих характеристик ОТЕ, засобів управління якістю передавання і усунення несправностей.

Використовується комбінація визначених методів ТО в залежності від типу обладнання. Для сучасних технічних засобів електрозв'язку основним є застосування ОТК. Цей метод, як правило, проводиться із окремого приміщення секції технічного обслуговування (СТО) в мережному вузлі (станції) за допомогою спеціального обладнання, яке забезпечує постійний контроль за якістю каналів, трактів, апаратури і систематичний аналіз одержуваних даних.

ПТО включає в себе:
– безперервний експлуатаційний контроль;
– періодичний експлуатаційний контроль;
– епізодичний експлуатаційний контроль;
– планові ремонтно-налагоджувальні роботи (РНР) і заміни компонентів апаратури з закриттям трактів і каналів передавання;
– поточне обслуговування обладнання і апаратури без закриття трактів і каналів передавання.

Поточне обслуговування без закриття трактів і каналів передавання полягає в:

– спостереженні за справністю механічних частин обладнання і апаратури;
– регулюванні механічних контактів (вузлів);
– чищенні і регулюванні контактів реле;
– змащуванні механічних контактів кіл електроживлення;
– перевірці напруги живлення і т. ін.

КТО включає в себе:

– безперервний експлуатаційний контроль;
– періодичний експлуатаційний контроль;
– епізодичний експлуатаційний контроль;
– оперативно-технічний контроль;
– ремонтно-відновлювальні роботи (РВР) і РНР.

ОТК включає в себе:

– безперервний контроль робочих характеристик ОТЕ;
– операції управління і перемикання на резерв;
– РВР і РНР.

Виконання функцій технічної експлуатації первинної мережі здійснюється:

- технічним змінним і незмінним персоналом лінійно-апаратних цехів (ЛАЦ) на нижньому рівні системи технічної експлуатації (СТЕ) в мережних вузлах (МВ) і мережних станціях (МС);
- центрами технічної експлуатації (ЦТЕ) на всіх ієрархічних рівнях СТЕ, організованих на основі технічних служб підприємств (операторів) первинної мережі.

В МВ і МС необхідно організовувати секції технічного обслуговування – інформаційно – виконавчі пункти (СТО – ІП) на основі змінного технічного персоналу ЛАЦ.

СТО-ІП і ЦТЕ оснащуються, як правило, програмно-технічними комплексами (ПТК).

В залежності від типу обладнання основні виробничі процеси технічного обслуговування апаратури, трактів і каналів передавання первинної мережі перевірка справності апаратури і вимірювання трактів і каналів передавання, уведення і відбій графіків обходів і замін (ГОЗ) і т. ін.] повинні здійснюватися за:

- програмами ПТК для обладнання сучасних ЦСП плезіохронної цифрової ієрархії (ПЦІ) і СЦІ;
- технологічними картами для обладнання аналогових систем передавання (АСП) і ЦСП з імпульсно-кодовою модуляцією (ІКМ).

Програми ПТК або технологічні карти повинні мати характеристику виробничого процесу:

– послідовність операцій, періодичність і коротке їх описання;

– час, необхідний для виконання окремих операцій і всього процесу;

– порівняння результатів з нормами;

– перелік вимірювальної техніки.

Технічне обслуговування обладнання, апаратури, трактів і каналів передавання проводиться технічним персоналом у відповідності з діючими нормативними документами (НД) з питань технічної експлуатації, наприклад, алгоритмів технічного обслуговування, інструкцій з технічної експлуатації і т. ін. (див. розділ 2 цього КНД).

На МВ і МС, де зорганізується цілодобове чергування змінного персоналу, робота змінного персоналу здійснюється за графіком, який затверджується керівником підприємства (підрозділу). Графік складається не менше, ніж на місяць та повинен бути доведений до змінного персоналу не пізніше, ніж за три дні до уведення його в дію.

Змінний технічний персонал забезпечує:

– виконання роботи з експлуатаційного контролю і поточного обслуговування апаратури трактів і каналів передавання;

– виконання вказівок з перебудови первинної мережі;

– оперативне усунення несправностей;

– приймання на перевірку і здавання в експлуатацію після перевірки або відновлення трактів і каналів передавання вторинним мережам і іншим користувачам;

– обслуговування апаратури електроживильних установок (ЕЖУ);

– ведення оперативно-технічної документації.

Змінний технічний персонал керується відповідними технологічними документами (алгоритмами, інструкціями, і т. ін.) для підрозділів системи оперативно-технічного управління (СОТУ).

Дії змінного технічного персоналу при несправностях ЕЖУ викладені в “Правилах технічної експлуатації електроустановок підприємств електрозв’язку України”.

Незмінний технічний персонал забезпечує:

– виконання робіт з експлуатаційного контролю, поточного ремонту, розвитку і формування мережі;

– виконання РНР і РВР;

– утримування обладнання електроживлення, електропостачання, життєзабезпечення, охоронно-пожежної сигналізації;

– приймання, уведення в експлуатацію трактів і каналів передавання і здавання їх вторинним мережам і іншим користувачам та письмове повідомлення в СОТУ про уведення в експлуатацію трактів і каналів передавання з вказанням дати, а при необхідності, і причину затримки уведення;

– підготовку і уведення виробничої документації, необхідної для технічного обслуговування і оперативно-технічного управління первинною мережею;

– облік і аналіз роботи МВ, МС, ЛП, ЛТ, мультиплексних і регенераційних секцій для ЦСП СЦІ, МТ і каналів передавання;

– розроблення пропозицій з підвищення якості і надійності роботи первинної мережі, контроль за ходом їх впровадження.

Технічний персонал зобов'язаний:

– знати технічні характеристики і схеми обслуговуваних апаратури, обладнання, ЛП, трактів і каналів передавання;

– знати методи вимірювання параметрів апаратури, трактів і каналів передавання;

– знати і виконувати інструкції і керівництва з настроювання та експлуатації обслуговуваних ЛП, трактів і каналів передавання;

– знати схеми організації обслуговуваних трактів і каналів передавання, резервних ЛТ, підмінних трактів, ГОЗ, технологічні карти;

– знати схеми організації тактової мережі синхронізації для цифрової мережі в зоні обслуговування;

– знати і використовувати методи і способи відшукування і усунення несправностей на обслуговуваних ЛП, трактах і каналах передавання;

– знати методи виконання РНР і РВР обслуговуваних ЛП, трактів і каналів передавання, уміло проводити їх і вірно оцінювати одержані результати;

– знати і виконувати посадові інструкції, алгоритми і положення СТЕ і СОТУ первинною мережею, правила технічної експлуатації первинної мережі, керівні вказівки Державного Комітету зв'язку та інформатизації України та НД з технічної експлуатації;

– вести технічну, оперативно-технічну і технологічну документацію за установленими формами;

– виконувати правила внутрішнього розпорядку підприємства;

– знати і виконувати вимоги НД з охорони праці.

Змінний персонал СТО-ІП має такі обов'язки.

Під час приймання і здавання чергування змінний персонал зобов'язаний:

– перевірити стан ОТЕ;

– перевірити наявність документації, інструменту, засобів і шнурів вимірювання, шнурів комутації і засобів захисту;

– перевірити справність дії пристроїв телемеханіки, телеконтролю і телеуправління, каналів службового зв'язку, засобів автоматизованого контролю та оброблення даних;

– перевірити справність дії технічних засобів ПТК та інформаційної мережі;

– звірити відповідність документації і ключів від приміщень затвердженому переліку;

– зафіксувати в оперативному журналі здавання і приймання чергування;

– здійснити інші дії, які визначені місцевими інструкціями з внутрішнього розпорядку.

В процесі чергування змінний персонал зобов'язаний:

– підтримувати апаратуру і обладнання в справності;

– контролювати справність ЛП, мультиплексних і регенераційних секцій для ЦСП СЦІ, трактів і каналів передавання;

– контролювати канали службового зв'язку, системи життєзабезпечення та інше:

– негайно передавати повідомлення про зміну стану ОТЕ (КО) в підрозділи СОТУ;

– замінювати пошкоджені тракти і канали передавання згідно ГОЗ і розпоряджень СОТУ;

– з'ясовувати причини несправностей, оперативно організовувати ліквідацію їх на обслуговуваній ділянці;

– взаємодіяти з ремонтно-відновлювальними бригадами (РВБ) і підрозділами СОТУ при усуненні несправностей;

– контролювати хід РВР і РНР, уводити (відміняти) ГОЗ за командами (з дозволу) підрозділів СОТУ і доповідати про це вищестоячому підрозділу СОТУ. Сповіщати керівництво і підрозділи системи оперативно-технічного обслуговування (СОТО) про несправності і хід РВР;

– контролювати роботу ЕЖУ і при необхідності проводити комутацію і управління відповідними пристроями;

– здійснювати контроль за роботою техперсоналу в необслуговуваному підсилювальному пункті (НПП), необслуговуваному регенераційному пункті (НРП);

– сповіщати вторинні мережі та інших користувачів про зміну стану трактів і каналів передавання.

Керівник зміни один раз за добу (у відповідності з внутрішнім розпорядком) доповідає керівнику цеху МВ (МС) про роботу вузла (станції), ЛП, мультиплексних і регенераційних секцій для ЦСП СЦІ, трактів і каналів передавання за добу, яка пройшла, а керівник цеху не рідше одного разу в тиждень доповідає керівнику МВ (МС).

Незмінний технічний персонал зобов'язаний:

– підтримувати в справності апаратуру і обладнання, включаючи вимірювальну апаратуру і пересувні засоби зв'язку;

– здійснювати приймання і уведення в експлуатацію трактів і каналів передавання та здавання їх вторинним мережам та іншим користувачам;

– проводити РНР і вимірювання ЛП, трактів і каналів передавання і аналізувати дані вимірювань;

– систематично аналізувати записи змінного технічного персоналу, контролювати вірність ведення оперативно-технічної документації;

– проводити аналіз стану трактів, розроблювати і здійснювати заходи, які спрямовані на підвищення якості і надійності роботи трактів;

– виконувати РВР під час усунення несправностей;

– робити установленим порядком ремонт блоків апаратури АСП і ЦСП з ІКМ, здійснювати контроль за справністю підмінних блоків, шнурів і засобів вимірювань;

– своєчасно здавати засоби вимірювання на повірку;

– підтримувати в справності канали службового зв'язку, пристрої телеобслуговування і телеуправління ЛП;

– робити наочне приладдя для змінного технічного персоналу;

– вести технічну, оперативно-технічну і технологічну документацію за встановленими формами.

Обов'язки технічного персоналу вказані в посадових інструкціях на кожному підприємстві в залежності від обсягів робіт, штату, структури даного підприємства та методів технічної експлуатації.

Керівництво технічним обслуговуванням трактів і каналів передавання здійснюється головними і допоміжними керівними станціями (ГКС і ДКС).

Рекомендації ITU-Tз експлуатації сучасних цифрових мереж, заснованих на технологіях xDSLнаведені до табл. 2.1

Таблиця 2.1 – Стандарти ITU – T (укр.: МСЕ-Т) з експлуатації обладнання xDSL

Позначення рекомендації	**Назва рекомендації, посилання**	**Час затвердження (міс./рік)**
1	**2**	**3**
G.994.1	Процедури підтвердження встановлення з'єднання прийомопередавачів DSL https://www.itu.int/rec/T-REC-G.994.1-202102-I/en	02/21
G.Sup50 (G.995.1)	Огляд рекомендацій цифрової абонентської лінії DSL https://www.itu.int/rec/T-REC-G.Sup50-201109-I/en	09/11 (12/2011 скасов.)
G.995.2	Поліпшені граничні значення загального режиму й методи виміру для обладнання приміщень замовника, що працює на мідних парах https://www.itu.int/rec/T-REC-G.995.2-201508-I/en	08/15
G.996.1	Процедури тестування обладнання цифрової абонентської лінії DSL https://www.itu.int/rec/T-REC-G.996.1/en	02/2001 Попр.1 01/2003 Випр.1 03/2003

Продовження таблиці 2.1

1	2	3
G.996.2	Тестування несиметричних ліній для цифрових абонентських ліній https://www.itu.int/rec/T-REC-G.996.2-201811-I/en	11/18
G.997.1	Управління фізичним рівнем прийомопередавачів цифрової абонентської лінії DSL https://www.itu.int/rec/T-REC-G.997.1-201902-I/en	02/2019
G.997.2	Physical layer management for G.fast transceivers Управління фізичним рівнем для приймачів G.fast https://www.itu.int/rec/T-REC-G.997.2/en	03/2019 Випр.1 13/2020 Попр.1 03/2020 Попр.2 12/2020
G.997.3	Управління фізичним рівнем для приймачів MGfast https://www.itu.int/rec/T-REC-G.997.3-202104-I/en	04/2021

Облік і аналіз роботи обладнання, апаратури, трактів і каналів передавання здійснюється у відповідності з діючою “Инструкцией о порядке ведения документации ЛАЦ по учету и анализу простоев трактов и каналов первичной сети ЕАСС”.

2.3 Організація експлуатації засобів телекомунікаційних систем та інформаційних технологій в ДСНС України

Організація та контроль технічної експлуатації телекомунікаційного обладнання та засобів інформатизації в територіальних органах ДСНС покладається на підрозділи зв’язку та телекомунікації (підрозділів, відповідальних за організацію зв’язку і технічну експлуатацію телекомунікаційних систем) ДСНС, посадових осіб, відповідальних за організацію зв’язку і технічну експлуатацію телекомунікаційних систем в ДСНС. Персональну відповідальність за експлуатацію телекомунікаційного обладнання та засобів інформатизації несе безпосередньо користувач.

2.3.1. Введення в експлуатацію телекомунікаційних систем та інформаційних технологій

Стадія введення в дію телекомунікаційних систем та інформаційних
технологій включає:

підготовчі роботи до введення телекомунікаційних систем та інформаційних технологій в дію (реалізація проектних рішень щодо організаційної структури системи, інсталяція програмних засобів, монтаж технічних засобів і ліній зв’язку, пусконалагоджувальні роботи та автономна перевірка технічних і програмних засобів, комплексна перевірка працездатності телекомунікаційних систем та інформаційних технологій), що здійснює виконавець (постачальник);

комплектацію системи відповідно до проектної документації (придбання та постачання необхідних для реалізації проектних рішень технічних і програмних засобів тощо);

підготовку персоналу (навчання персоналу і перевірку його здатності забезпечити функціонування системи згідно з програмою підготовки персоналу), яку здійснює виконавець (постачальник);

проведення попередніх випробувань (виконавцем проекту згідно з програмою і методикою випробувань з наданням результатів випробувань замовнику під час передачі проекту);

проведення дослідної експлуатації згідно з розпорядчим документом у визначені терміни, за підсумками якої складається акт, що затверджується керівником підрозділу;

проведення приймальних випробувань відповідною комісією (випробування на відповідність проектних рішень технічному завданню згідно з програмою та методикою приймальних випробувань) з оформленням акта, в якому зазначаються підрозділи, які використовують телекомунікаційні системи та інформаційні технології, та визначаються відповідальні за її технічний супровід, а також затверджується відповідна нормативна документація за напрямом телекомунікаційних систем та інформаційних технологій.

2.3.2 Введення в експлуатацію технічних засобів

Введення телекомунікаційного обладнання в експлуатацію здійснюється комісією, яка створюється в підрозділах ДСНС. При введенні в експлуатацію стаціонарних телекомунікаційних об'єктів або споруд (в тому числі реконструйованих) до складу комісії включаються представники підрядних проектних, будівельних і монтажних організацій. Участь співробітників підрозділу зв'язку та телекомунікацій ДСНС у роботі комісії є обов'язковою. Комісія складає відповідні документи (формуляр) із зазначенням заводських номерів, року випуску і місця установки на введення в експлуатацію.

Час введення в експлуатацію телекомунікаційного обладнання не повинно перевищувати тридцяти днів з моменту їх надходження в підрозділ ДСНС, за винятком коли потрібне проведення комплексу будівельно-монтажних і пусконалагоджувальних робіт.

Інформацію про введення в експлуатацію, зміні категорії, модернізації або списання телекомунікаційного обладнання записуються в формулярі із зазначенням документа та дати. Записи завіряються підписом матеріально відповідальної особи працівника зв'язку та телекомунікації, або майстерні.

Контроль за правильність ведення формулярів, та їх зберігання покладається на підрозділи за напрямом телекомунікаційних систем та інформаційних технологій, які відповідають за телекомунікаційне облад-

нання, а при їх відсутності – на посадових осіб, відповідальних за організацію зв'язку і технічну експлуатацію телекомунікаційного обладнання ДСНС.

У разі втрати формуляра його дублікат відновлюється на підставі рішення начальника служби зв'язку, після проведення службової перевірки за фактом його втрати.

Монтаж телекомунікаційного обладнання проводиться силами співробітників підрозділів зв'язку та телекомунікації, або підрядних організацій відповідно до експлуатаційно-технічної документації.

Облік телекомунікаційного обладнання здійснюється співробітниками підрозділів зв'язку, та телекомунікації або посадовими особами, відповідальними за організацію зв'язку і технічну експлуатацію телекомунікаційного обладнання ДСНС. Дозволяється вести облік в електронному вигляді.

Розподіл телекомунікаційного обладнання між підрозділами ДСНС проводиться на підставі наказів ДСНС. Закріплення обладнання за співробітниками підрозділів, проводиться безпосередньо в підрозділі отримувача майна, згідно внутрішніх розпорядчих документів. Дані про закріплення телекомунікаційного обладнання заносяться в формуляр обладнання.

Порядок видачі телекомунікаційного обладнання, що знаходиться на зберіганні, визначається нормативно-правовими актами ДСНС, що регламентують організацію їх роботи.

2.3.3. Введення в експлуатацію програмних засобів

Придбання комп'ютерних програм здійснюється лише в разі відсутності аналогів комп'ютерних програм вільного користування та за погодженням із підрозділом, що відповідає за напрям інформаційних і телекомунікаційних технологій апарату ДСНС.

Прикладне програмне забезпечення має бути ліцензійним, по можливості з розширеною підтримкою та обслуговуванням. У разі використання вільного прикладного програмного забезпечення джерелом для його завантаження має виступати офіційний сайт розробника з установленим та дійсним на момент завантаження SSL-сертифікатом.

Не допускається використання програмного забезпечення, якщо розробник знаходиться у переліку фізичних чи юридичних осіб, до яких державою Україна вжито обмежувальних заходів (санкцій).

Установлення програмного забезпечення на комп'ютерах користувачів у системі ДСНС виконують виключно фахівці підрозділів за напрямом телекомунікаційних систем та інформаційних технологій.

Підрозділи ДСНС повинні передбачати заходи з виводу з експлуатації програмного забезпечення, яке вже не підтримується з боку розробника.

Для здійснення внутрішнього електронного документообігу в ДСНС має використовуватися відкритий формат документів (ODF – OpenDocumentFormat).

У разі відправлення документів за межі ДСНС за необхідності вони можуть бути конвертовані (якщо є змога) у формат, який потрібен отримувачу.

Облік програмного забезпечення здійснюють підрозділів за напрямом телекомунікаційних систем та інформаційних технологій.

2.3.4. Технічне обслуговування (супровід) та регламентні роботи телекомунікаційних систем та інформаційних технологій

Технічне обслуговування та проведення регламентних робіт телекомунікаційних систем та інформаційних технологій виконується згідно річного план-графіку який розробляється посадовою особою відповідальною за напрям телекомунікацій та інформатизації та затверджується начальником служби зв'язку.

Стадія технічного обслуговування та супроводу телекомунікаційних систем та інформаційних технологій включає:

гарантійне технічне обслуговування (здійснення робіт з усунення на безоплатній основі виконавцем проектних робіт недоліків, виявлених під час експлуатації телекомунікаційних систем та інформаційних технологій протягом установлених гарантійних термінів і внесення необхідних змін до технічної документації);

післягарантійне технічне обслуговування (комплекс робіт з підтримки цілодобового справного функціонування телекомунікаційних систем та інформаційних технологій протягом усього строку експлуатації);

супровід телекомунікаційних систем та інформаційних технологій(модифікація програмних та/або програмно-технічних засобів телекомунікаційних систем та інформаційних технологій після передачі замовнику виконавцем (постачальником) робіт для коригування виявлених проблем, виявлення та коригування наявних прихованих помилок для запобігання прояву цих помилок під час експлуатації або забезпечення продовження використання телекомунікаційних систем та інформаційних технологій із заданою ефективністю).

За необхідністю для супроводу та післягарантійного технічного обслуговування телекомунікаційних систем та інформаційних технологій на договірній основі можуть залучатися сторонні організації.

2.3.5. Зберігання телекомунікаційного обладнання та засобів інформатизації

Облік, зберігання, порядок перевірки, введення в експлуатацію, технічне обслуговування телекомунікаційного обладнання та засобів ін-

форматизації, що знаходяться на довготривалому зберіганні визначається окремими розпорядчими документами.

На всі інформаційні ресурси в підрозділі має вестись інформаційна картка за формою. За щорічне оновлення і зберігання інформаційних карток на телекомунікаційні системи та інформаційні технології відповідає підрозділ з напрямку телекомунікацій та інформатизації. Інформаційні картки мають бути в актуальному стані і зберігатися в електронній формі.

При зберіганні телекомунікаційного обладнання та засобів інформатизації повинні виконуватися наступні заході:

правильне утримання і використання приміщень складів;

ретельний і кількісний прийом обладнання, яке поступило на зберігання, їх матеріальний облік з повнотою запису всіх даних про обладнання;

створення умов, що забезпечують якісне зберігання для кожного виду техніки відповідно до технічних вимог;

своєчасне проведення технічного обслуговування;

Телекомунікаційне обладнання та засоби інформатизації зберігаються в комплекті поставки. Розукомплектування і роздільне зберігання обладнання допускаються лише за клопотанням начальника служби зв'язку та дозволом начальника територіального підрозділу.

2.3.6.Порядок використання інформаційних та інформаційно–телекомунікаційних систем, використання та облік комп'ютерних програм

Даний Порядок визначає вимоги щодо процедури створення (закупівлі), впровадження, забезпечення супроводу та обліку інформаційних та інформаційно-телекомунікаційних систем (далі — Систем) у Державній службі України з надзвичайних ситуацій.

Терміни, наведені у цьому Порядку, вживаються у таких значеннях:

виконавець — підрозділ організації, підприємства чи установи сфери управління ДСНС чи стороння організація, з якою згідно з чинним законодавством укладено договір, що виконує роботи зі створення та введення в експлуатацію Системи;

замовник — організація, підприємство чи установа сфери управління ДСНС, для якого створюється Система;

інформаційна безпека — забезпечення необхідного рівня конфіденційності, кіберзахисту, цілісності, доступності, автентичності і достовірності інформації та ефективності технічного захисту інформаційного ресурсу ІТ-системи від втрат, спотворення, руйнування і несанкціонованого використання;

інформаційна Система (ІС) — організаційно-технічна Система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;

інформаційно-телекомунікаційна Система (ІТС) — сукупність інформаційних і телекомунікаційних Систем, які в процесі обробки інформації діють як єдине ціле;

постачальник — стороння організація, яка відповідно до договору постачає Систему та виконує роботи щодо її введення в експлуатацію;

технічне завдання ІС/ІТС — це оформлений та затверджений належним чином документ, який визначає обґрунтування доцільності й мету створення ІС/ІТС, вимоги до неї, а також основні засадничі дані та планграфік створення;

установа — ДСНС, ГУ (У) ДСНС України в області чи м. Києві, підприємство, установа чи організація сфери управління ДСНС.

Побудова Систем має відповідати вимогам чинних нормативно-правових актів. Перелік основних нормативних документів стосовно інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем розміщено на Порталі обстеження ІТ-систем органів виконавчої влади (https://audit.gov.ua/).

Мова інтерфейсу програмних продуктів і документації інформаційних систем — українська, а у разі відсутності україномовного інтерфейсу — англомовний.

За можливості створення Систем цілком або виконання частини етапів зі створення без залучення сторонніх організацій підрозділи ДСНС можуть виступати не тільки як замовники, але й як виконавці.

Створення (закупівля) і впровадження нових Систем у ДСНС відбувається за погодженням зі структурним підрозділом, що відповідає за напрям інформаційні технології в апараті ДСНС.

Системи створюються та впроваджуються за обґрунтованим поданням установи для забезпечення підвищення ефективності виконання покладених на установу завдань. Необхідність створення (закупівлі) Систем визначає керівник установи.

Стадія формування вимог до Системи включає:

визначення потреби в Системі та вивчення питання щодо можливості її створення (закупівлі) для забезпечення виконання необхідних функцій;

розроблення техніко-економічного обґрунтування створення (закупівлі) Системи;

обґрунтування необхідності використання особистих немайнових та (або) майнових прав інтелектуальної власності на засоби інформатизації.

Вимоги до Системи формуються і визначаються відповідним структурним підрозділом або робочою групою (за необхідністю), за участю

представників відповідних структурних підрозділів установи, до компетенції яких належать завдання її створення і застосування за призначенням.

Стадія розроблення і затвердження технічного завдання на створення Системи включає:

аналіз та узгодження вимог до Системи;

розроблення та затвердження технічного завдання.

Технічне завдання розробляється відповідно до чинного законодавства, рекомендацій національних стандартів і встановленої практики визначеним виконавцем робіт на основі узгоджених із замовником вимог до Системи. До розробки технічного завдання можуть залучатися на договірних засадах сторонні компетентні організації.

Технічне завдання візується замовником, підписується виконавцем робіт, затверджується керівником установи та погоджується із структурним підрозділом, що відповідає за напрям інформаційних і телекомунікаційних технологій в апараті ДСНС.

Стадія розроблення технічного, робочого або техно-робочого проекту створення Системи включає:

розробку проектних рішень (щодо архітектури Системи, функцій Системи і її підсистем, функцій персоналу та організаційної структури, структури технічних засобів, алгоритмів рішення завдань і мов програмування та інтерфейсу користувача, організації та ведення інформаційної бази, системи класифікації та кодування інформації, програмного забезпечення), їх узгодження та документування відповідно до вимог технічного завдання.

Всі програмні, програмно-технічні (зокрема, вихідний код програмних засобів і команди компілятора, алгоритми, структури і формати даних тощо) та організаційні (регламенти, вимоги, інструкції, обмеження тощо) проектні рішення, які можуть застосовуватися для підтримки потрібного рівня експлуатаційних характеристик (якості) в процесі експлуатації й супроводу Системи, мають бути узгоджені, затверджені та передані замовнику виконавцем робіт (розробником) у задокументованому вигляді, необхідному для опису повної сукупності прийнятих проектних рішень і достатньому для їхнього незалежного використання (без звернення до розробника). Застосування недокументованих рішень заборонено.

Технічний, робочий або техно-робочий проект візується замовником, підписується виконавцем робіт, затверджується керівником установи та погоджується із структурним підрозділом, що відповідає за напрям інформаційних і телекомунікаційних технологій в апараті ДСНС.

Стадія введення в дію Системи включає:

підготовчі роботи до введення Системи в дію (реалізація проектних рішень щодо організаційної структури Системи, інсталяція програмних

засобів, монтаж технічних засобів і ліній зв'язку, пусконалагоджувальні роботи та автономна перевірка технічних і програмних засобів, комплексна перевірка працездатності Системи), що здійснює виконавець (постачальник);

комплектацію Системи відповідно до проектної документації (придбання та постачання необхідних для реалізації проектних рішень технічних і програмних засобів тощо);

підготовку персоналу (навчання персоналу і перевірку його здатності забезпечити функціонування Системи згідно з програмою підготовки персоналу), яку здійснює виконавець (постачальник);

проведення попередніх випробувань (виконавцем проекту згідно з програмою і методикою випробувань з наданням результатів випробувань замовнику під час передачі проекту);

проведення дослідної експлуатації згідно з розпорядчим документом установи у визначені терміни, за підсумками якої складається акт, який підписує керівник підрозділу установи, на базі якого проводилася дослідна експлуатація, та затверджує керівник установи;

проведення приймальних випробувань відповідною комісією (випробування на відповідність проектних рішень технічному завданню згідно з програмою та методикою приймальних випробувань з оформленням акта про приймання Системи в експлуатацію);

введення Системи в експлуатацію наказом керівника установи, в якому зазначаються підрозділи, які використовують Систему, та визначаються відповідальні за її технічний супровід, а також затверджується відповідна нормативна документація Системи (згідно з переліком, зазначеним вище).

Стадія технічного обслуговування та супроводу Системи включає:

гарантійне технічне обслуговування (здійснення робіт з усунення на безоплатній основі виконавцем проектних робіт недоліків, виявлених під час експлуатації Системи протягом установлених гарантійних термінів і внесення необхідних змін до технічної документації);

післягарантійне технічне обслуговування (комплекс робіт з підтримки цілодобового справного функціонування Системи протягом усього строку експлуатації);

супровід Системи (модифікація програмних та/або програмно-технічних засобів Системи після передачі замовнику виконавцем (постачальником) робіт для коригування виявлених проблем, виявлення та коригування наявних прихованих помилок для запобігання прояву цих помилок під час експлуатації або забезпечення продовження використання Системи із заданою ефективністю).

За необхідністю для супроводу та післягарантійного технічного обслуговування Системи на договірній основі можуть залучатися сторонні організації.

Вимоги до складання договорів на розробку/закупівлю Систем включають наступне.

З метою раціонального використання бюджетних коштів, направлених на розробку Систем у договорі, має бути передбачено повне набуття установою майнових прав на об'єкти інтелектуальної власності, недопущення включення до собівартості робіт і послуг витрат, які безпосередньо не пов'язані з виконанням таких робіт і наданням послуг.

Умови використання комп'ютерних програм з метою створення і (або) використання Систем або державних електронних реєстрів мають передбачати, що строком ліцензії є строк чинності виключних майнових прав інтелектуальної власності на відповідну комп'ютерну програму.

Закупівлю комп'ютерних програм, якщо ліцензія передбачає виплату винагороди правовласнику у вигляді відсотків плати за надані від імені держави послуги, заборонено.

Закупівля товарів, робіт і послуг має здійснюватися з дотриманням вимог Закону України "Про публічні закупівлі".

Вимоги до забезпечення організації функціонування Систем охоплюють наступні заходи.

Забезпечення функціонування Систем, як правило, покладається на структурний підрозділ установи, що відповідає за напрям інформаційних і телекомунікаційних технологій, або на визначених керівником установи посадових осіб, які користуються у своїй діяльності Системою (далі — Служба технічної підтримки).

Служба технічної підтримки має забезпечувати виконання таких функцій:

підтримка функціонування програмного забезпечення та телекомунікаційного обладнання Системи;

інформаційної безпеки та цілісності даних;

кібербезпеки;

організації та підтримки інформаційної взаємодії;

надання допомоги користувачам Системи.

Представники Служби технічної підтримки повинні виконувати такі функції:

головний адміністратор Системи;

системний аналітик;

системний адміністратор;

мережевий аналітик;

мережевий адміністратор;

інформаційний аналітик (аналітик даних);

аналітик з інформаційної безпеки та кібербезпеки;

спеціаліст з технічної підтримки користувачів.

На одну особу може бути покладено кілька завдань, за винятком обов'язків осіб, відповідальних за безпеку.

Вимоги щодо документації на Системи включають наступні заходи.

У разі впровадження Систем в установі мають бути розроблені та затверджені такі документи:

положення про Систему;

порядок оброблення інформації в Системі;

схеми фізичного розташування обладнання, електроживлення серверного та комутаційного обладнання, комутаційних з'єднань усієї мережі та логічної взаємодії сервісів і служб у мережі;

план захисту інформації в Системі;

регламент функціонування Системи.

Регламент функціонування Системи включає такі правила:

роботи в Системі (інструкції користувачів та адміністраторів);

доступу до інформаційної інфраструктури установи;

роботи з електронним документообігом, внутрішнім порталом, корпоративною поштою (поштовим сервером);

ідентифікації користувачів у мережі та їх авторизованого доступу (монітор стану).

Також до регламенту входять політики безпеки (інформаційна, мережева, адміністративна), що визначають розмежування прав доступу користувачів до внутрішньої мережі та внутрішньої інфраструктури установи відповідно до їх повноважень (адміністратор, модератор, авторизований користувач тощо), а також порядок резервного копіювання інформації.

У політиці безпеки Системи мають бути розглянуті такі проблеми, як віддалений доступ, перелік критичних ресурсів, керування та конфігурація IP-адрес, безпека засобів телекомунікацій, процедура виявлення вторгнення у мережу.

2.3.7 Контроль за станом систем, технічних і програмних засобів

Контроль за станом систем, технічних і програмних засобів покладається на структурний підрозділ, що відповідає за напрям інформаційних і телекомунікаційних технологій, або на визначених керівником посадових осіб, які користуються у своїй діяльності телекомунікаційні системи та інформаційні технології.

2.4 Основи теорії надійності обладнання телекомунікаційних систем

2.4.1 Основні поняття й визначення надійностіелектрорадіовиробів

Розвиток сучасних електрорадіовиробів (ЕРВ) характеризується значним збільшенням її складності й зростанням важливості розв'язуваних функціональних завдань. Ускладнення ЕРВ обумовлює необхідність

підвищення гарантії своєчасності й правильності розв'язку завдань. Ці фактори визначили необхідність розробки наукових основ експлуатації ЕРВ.

Вивчення теоретичних основ експлуатації почнемо з основних понять і термінів.

Термін «експлуатація» походить від французького слова «exploitation», що означає одержання користі або вигоди із чого-небудь. У широкому змісті слово «експлуатація» означає систематичне використання людиною продуктивних сил.

Експлуатація передбачає наявність із одного боку, людину (будемо звати його оператор), з іншого боку — об'єкта експлуатації (машина, апарат, система й т. п.), над яким оператор повинен робити певні дії для одержання необхідних результатів. У технічному плані експлуатацію можна розглядати як процес використання (керування) оператором об'єкта для досягнення заданого результату.

Визначення даються відповідно до ДСТУ 2860-94 Надійність техніки. Терміни та визначення.

Надалі під терміном *«об'єкт»* будемо понімати систему, споруду, машину, підсистему, апаратуру, функціонує одиницю, пристрій, елемент чи будь яку їх частину, що розглядається з погляду надійності як самостійна одиниця.

Складовою частиною об'єкта є елемент. Це також досить широке поняття, що залежить від змісту, вкладеного в поняття «об'єкта». Якщо об'єктом є система, то елементами його будуть окремі підсистеми й пристрою. Якщо об'єктом є апарат, то елементами його будуть вузли й окремі деталі.

Об’єкт може включати технічні засоби, технічний персонал чи будь-які їх поєднання. Сукупність об'єктів, об’єднаних спільним призначенням і метою функціонування, може розглядатися як об’єкт

Обслуговуваний об’єкт – об’єкт, для якого проведення технічного обслуговування передбачено нормативно-технічною документацією та (чи) конструкторською (проектною) документацією

Необслуговуваний об’єкт – об’єкт, для якого проведення технічного обслуговування не передбачено нормативно-технічною документацією та (чи) конструкторською (проектною) документацією

Функція (об’єкта); задана функція (об’єкта) – виконання в об’єкті процесу, що відповідає його призначенню, виявлення заданої умови чи властивості об’єкта відповідно вимогам нормативної та (чи) конструкторської (проектної) документації

Основна функція; потрібна функція – функція чи сукупність функцій об’єкта, виконання якої розглядають як необхідну умову відповідності об’єкта його призначенню. Всі функції об’єкта можна умовно розподіли-

ти на основні та допоміжні. Допоміжні функції — функції, невиконання яких не порушує відповідності об’єкта його призначенню

Як процес, експлуатація повинна характеризуватися часом і місцем дії.

Процес експлуатації охоплює весь період існування об'єкта з моменту його виготовлення.

Закінчення експлуатації об'єкта визначається його граничним станом, тобто станом, за яким його подальша експлуатація неприпустима чи недоцільна, або відновлення його працездатного стану неможливе чи недоцільне. Граничний стан наступає, наприклад, тоді, коли параметр потоку відмов стає неприйнятним та (чи) об’єкт стає неремонтопридатним внаслідок несправносте(ознаки граничного стану задаються нормативно-технічною документацією на об'єкт).

Якщо об'єкт зазнає середньому або капітальному ремонту, то після його закінчення експлуатація об'єкта триває. поняття, що тому зустрічається в літературі, « термін служби» неідентичне часу експлуатації тому що під *терміном служби слід розуміти календарну тривалість експлуатації об'єкта від початку експлуатації або її поновлення після середнього або капітального ремонту до настання граничного стану.*

Місцем експлуатації може служити підприємство, склад, транспортні засоби, місце застосування по призначенню й т.п.

З погляду користувача об'єкт може бути в одній із двох, що чергуються між собою фаз. підготовки до використання й використання по призначенню.

Фаза підготовки до використання містить у собі ряд етапів експлуатації об'єкта, пов'язаних з підготовкою до його роботи (транспортування, зберігання, обслуговування, ремонт і т.п.).

Залежно від характеру чергування фаз експлуатації розрізняють *об'єкти разового й багаторазового використання.*

Об'єкт разового використання має одну фазу використання по призначенню за весь період експлуатації, а об'єкт багаторазового використання має багаторазове чергування фаз підготовки до використання й використання по призначенню.

Тому що об'єкт експлуатується в різних умовах, те необхідно знати можливі результати впливу цих умов. Крім зовнішніх факторів на поведінку об'єкта будуть впливати особливості його конструювання, виготовлення й налагодження. Немаловажне значення мають ступінь підготовленості операторів, що експлуатують об'єкт, і їх психофізіологічний стан.

Дослідження поведінки об'єкта під час експлуатації й оцінка його експлуатаційних якостей становить предмет теорії надійності. Питаннями взаємодії оператор-об'єкт при експлуатації займається наука — ергономіка. У її функції входить вивчення в самому широкому змісті системи « людина-машина», підходячи до людині як особливій ланці, включеному

в систему різних пристроїв і машин. Такий обмежений у соціальному змісті підхід до особистості оператора дозволяє визначити оптимальні умови функціонування системи оператор-об'єкт при створенні можливо кращих умов праці працюючій людині.

Ергономіка тісно контактує з інженерної психологією, що вивчає умови, процес і знаряддя праці оператора.

Таким чином, теорію надійності, ергономікові й інженерну психологію можна розглядати як складові частини теорії експлуатації, що займається всім комплексом питань аналізу й синтезу оптимальної структури системи експлуатації1 .

У процесі експлуатації об'єкт може перебувати в різних станах.

Стан об'єкта характеризується ступенем відповідності вимогам або параметрам, установлюваним нормативно-технічною документацією на нього.

Усі вимоги можна підрозділити на дві групи: задані, що визначають здатність об'єкта виконувати задані функції (як правило, до них ставляться параметри), і інші, що визначають зручність роботи, зовнішній вигляд, характер фарбування й т.п., що безпосередньо не впливають на виконання об'єктом заданих функцій.

Залежно від ступеня відповідності об'єкта тієї або іншій групі вимог розрізняють стани: *справне й несправне, працездатний й непрацездатний.*

Справним станом (справність) називають стан об’єкта, за яким він здатний виконувати усі задані функції об'єкта.

Несправний стан (несправність) – стан об’єкта, за яким він нездатний виконувати хоч би одну із заданих функцій об’єкта.Несправність чисто є наслідком відмови об’єкта, але може бути й без неї.

Працездатним станом (працездатність) – стан об’єкта, який характеризується його здатністю виконувати усі потрібні функції.

Непрацездатний стан; непрацездатність – стан об’єкта, за яким він нездатний виконувати хоч би одну з потрібних функцій.

В табл. 2.2 наведений перелік несправностей об’єкту.

Як випливає із визначення, поняття «справний стан» більш широке, чому «працездатний стан», тому що об'єкт, наприклад може бути в несправному стані (порушення декоративних покриттів), але нормально функціонувати.

Перехід від справного стану до несправного стану відбувається з інтенсивністю відмов $\lambda(t)$, а перехід від несправного стану до справного

1 Під «системою експлуатації» розуміють операторів, що беруть участь в експлуатації даного об'єкта, технічні й допоміжні засоби, що забезпечують експлуатацію об'єкта, і сам об'єкт у їхній взаємодії на відповідних етапах експлуатації.

стану відбувається з інтенсивністю відновлення $\mu(t)$, яка є показником ремонтопридатності. (рис. 2.10).

Таблиця2.2 – Види несправностей об’єкту

3.2.9 незначна несправність	Несправність, що не порушує жодної з потрібних функцій об’єкта. Примітка. Дефект чи несправність, викликані порушенням допоміжної функції внаслідок ушкодження
3.2.10 значна несправність	Несправність, що порушує хоча б одну з потрібних функцій об’єкта
3.2.11 часткова несправність	Несправність, що викликає нездатність об’єкта виконувати частину потрібних функцій
3.2.12 повна несправність	Несправність, що характеризується повною нездатністю об’єкта виконувати усі потрібні функції
3.2.13 критична несправність	Несправність, що може призвести до травмування людей, значних матеріальних збитків чи інших неприйнятних наслідків
3.2.14 вид несправності	Один з можливих станів несправного об’єкта для деякої заданої функції
3.2.15 несправність через перевантаження	Несправність, викликана прикладанням під час використання об’єкта навантажень, що перевищують його встановлені можливості
3.2.16 несправність через невміле поводження	Несправність, спричинена неправильним чи необережним поводженням з об’єктом
3.2.17 несправність через неміцність	Несправність, спричинена недостатньою міцністю самого об’єкта, який перебуває під навантаженнями, що не перевищують можливостей об’єкта, встановлених відповідною документацією
3.2.18 несправність через зношування та (чи) старіння	Несправність спричинена відмовою, викликаною природними процесами старіння та (чи) зношування, що відбуваються всередині об’єкта
3.2.19 конструкційна несправність	Несправність, спричинена недосконалістю проекту об’єкта
3.2.20 виробнича несправність	Несправність, спричинена невідповідністю ходу виробництва проекту об’єкта чи установленим виробничим процесам
3.2.21 стабільна несправність	Несправність об’єкта, що може бути усунена тільки за допомогою ремонту
3.2.22 прихована несправність	Несправність, яка існує, але ще не виявлена
3.2.23. маскована несправність	Несправність складової частини об’єкта, яка не може бути виявлена через особливості об’єкта чи маскується іншою несправністю цієї чи іншої складової частини об’єкта
3.2.24. дефект	Кожна окрема невідповідність об’єкта встановленим вимогам
3.2.25 пошкодження	Подія, яка полягає у порушенні справного стану об’єкта коли зберігається його працездатність

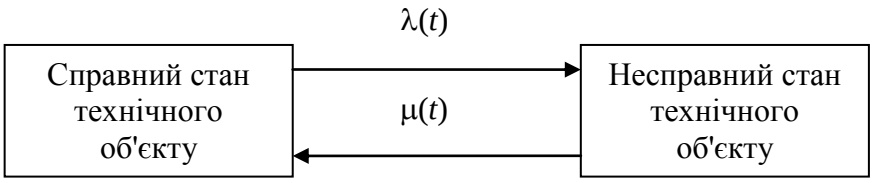


Рис. 2.10 – Стани технічного об’єкту

Відмова – це подія, яка полягає у втраті об’єктом здатності виконувати потрібну функцію, тобто у порушенні працездатного стану об’єкта. За характером виникнення прийнято розрізняти *відмови раптові*, які неможливо передбачити попередніми дослідженнями або технічним оглядом, і *поступові відмови*, спричинені поступовими змінами значень одного або декількох визначальних параметрів об’єкта.

Поступову відмову можна передбачити попередніми дослідженнями чи технічним оглядом, інколи її можна підвернути заходами технічного обслуговування

Критичний стан – стан об’єкта, що може призвести до травмування людей, значних матеріальних збитків чи інших неприйнятних наслідків. Критичний стан назавжди е наслідком критичної несправності. Для конкретного об’єкта повинні бути встановлені критерії критичного стану.

Критерій критичного стану – ознака чи сукупність ознак критичного стану об’єкта, встановлених нормативною та (чи) конструкторською (проектною) документацією.

Граничний стан – стан об’єкта, за яким його подальша експлуатація неприпустима чи недоцільна, або відновлення його працездатного стану неможливе чи недоцільне. Граничний стан наступає, наприклад, тоді, коли параметр потоку відмов стає неприйнятним та (чи) об’єкт стає неремонтопридатним внаслідок несправності

Критерій граничний стану – ознака чи сукупність ознак граничного стану об’єкта, встановлених нормативною та (чи) конструкторською (проектною) документацією. Залежно від умов експлуатації для одного й того ж об’єкта можуть бути встановлені два чи більше критеріїв граничного стану

Об'єкт характеризується рядом властивостей, що визначають його придатність виконувати задані функції. Одним з них є надійність.

Надійність – властивість об’єкта зберігати у часі в установлених межах значення всіх параметрів, які характеризують здатність виконувати потрібні функції в заданих режимах та умовах застосування, технічного обслуговування, зберігання та транспортування.

Надійність є комплексною властивістю, що залежно від призначення об’єкта і умов його застосування, може містити в собі *безвідмовність,*

довговічність, ремонтопридатність та збережуваність чи певні поєднання цих властивостей.

Безвідмовність (властивість) – властивість об'єкта виконувати потрібні функції в певних умовах протягом заданого інтервалу часу чи наробітку

Довговічність – властивість об'єкта виконувати потрібні функції до переходу у граничний стан при встановленій системі технічного обслуговування та ремонту

Збережуваність – властивість об'єкта зберігати в заданих межах значення параметрів, що характеризують здатність об'єкта виконувати потрібні функції, під час і після зберігання та (чи) транспортування

Ремонтопридатність (властивість) – властивість об'єкта бути пристосованим до підтримання та відновлення стану, в якому він здатний виконувати потрібні функції за допомогою технічного обслуговування та ремонту

Готовність – властивість об'єкта, бути здатним виконувати потрібні функції, в заданих умовах у будь-який час чи протягом заданого інтервалу часу за умови забезпечення необхідними зовнішніми ресурсами. Ця властивість залежить від поєднання властивостей безвідмовносте, ремонтопридатності та забезпечення технічного обслуговування і ремонту. Необхідні зовнішні ресурси, що не належать до ресурсові технічного обслуговування та ремонту, не впливають на властивість готовності об'єкта

Властивості надійності об'єкту надані на рис. 2.11



Рис. 2.11 – Властивості надійності

Залежно від призначення об'єкта й умов його експлуатації надійність може включати всі ці властивості або їх комбінацію.

Поняття «умови використання» має самий широкий зміст, включаючи всі фактори, що впливають на об'єкт! характер роботи, умови зовнішнього середовища, ступінь підготовленості операторів і т.п.

Перехід об'єкта з одного стану в інший будемо називати подією.

Подія, що полягає в порушенні справного стану об'єкта або його складових частин під дією зовнішніх впливів, що перевищують рівні, установлені в нормативно-технічній документації на об'єкт, і в переході його в несправний стан, називають ушкодженням.

Подія, що полягає в порушенні працездатності об'єкта, називають відмовою, що є одним з найважливіших понять теорії надійності. Як випливає із визначення, під відмовою потрібно розуміти не тільки повну втрату працездатності, але і її погіршення внаслідок зміни значення параметрів. Причина відмови — це вплив (навантаження), який привів об'єкт у непрацездатний стан. Ознаками відмови є безпосередні або непрямі впливи на органі почуттів операторів певних станів або процесів, властивих непрацездатному стану об'єкта (виникнення стукотів у двигуні, зникнення вихідного сигналу, зміна показань приладів і т.п.), визначних нормативно-технічною документацією на даний об'єкт.

Слід розрізняти відмову об'єкта й відмову елемента об'єкта. Можливі наступні випадки:

а) відмова елемента одночасно означає й відмову об'єкта;

б) відмова елемента не означає відмову об'єкта;

в) порушення працездатності об'єкта при відсутності елементів, що відмовили (помилки оператора, експлуатація в умовах, не передбачених технічною документацією, і т.п.).

Критерій відмови характеризується ознакою чи сукупністю ознак порушення працездатного стану об’єкта, які встановлені у нормативній та (або) конструкторській (проектній) документації.

Механізм відмови і характер виникнення відмови зумовлені фізичним, хімічним або іншим процесом, що привів до відмови

Вид відмови характеризується формою прояви відмови. наприклад, обривом чи закороченням кола, змінами коефіцієнта підсилення тощо.

Через складну природу відмов теорія надійності дає досить широку їхню класифікацію. Їх підрозділяють у такий спосіб:

1) по характеру зміни параметра до моменту виникнення відмови на *раптові й поступові*:

раптовою називають відмову, що характеризується стрибкоподібною зміною одного або декількох заданих параметрів об'єкта, яку неможливо передбачити попередніми дослідженнями чи технічним оглядом,

поступовою називають відмову, що характеризується поступовою зміною значень одного або декількох заданих параметрів об'єкта, яка спричинена поступовими змінами значень одного чи декількох параметрів об’єкта. Поступову відмову можна передбачити поперед-

німи дослідженнями чи технічним оглядом, інколи її можна підвернути заходами технічного обслуговування;

2) по взаємозв'язку між собою — на *залежні й незалежні*:

з а л е ж н о ю н а з и в а ю т ь в і д м о в у, якаспричинена прямо чи непрямо відмовою або несправністю іншого об’єкта;

н е з а л е ж н о ю називають відмову об’єкта, яка не спричинена прямо чи непрямо відмовою або несправністю іншого об’єкта;

3) по характеру часу порушення працездатності — *на збої й повторювальні:*

з б о є м називають самоусувну відмову або одноразову відмову, яку незначним втручанням усуває оператор;

п о в т о р ю в а л ь н о ю називають самоусувну відмову одного й того ж характеру, що виникає багаторазово;

4)із причин виникнення — на *конструкційні*, *виробничі і систематичні*:

к о н с т р у к ц і й н о ю називають відмову, що спричинена недосконалістю чи порушенням встановлених правил і (чи), норм проектування та конструювання об’єкта;

в и р о б н и ч о ю називають відмову, що спричинена невідповідністю виготовлення об’єкта до його проекту чи до норм виробничого процесу,

с и с т е м а т и ч н о ю називають відмову, що однозначно пов’язана з певною причиною, яку можна усунути лише тільки після модифікації проекту чи виробничого процесу, правил експлуатації, документації чи інших чинників, що враховуються.

5)за об’ємом та наслідками відмови таких як явища, процеси, події та стани, зумовлені виникненням відмови об’єкта – *часткові, повні,*

ч а с т к о в а відмова призводить до неспроможності об’єкта виконувати частину з потрібних функцій;

п о в н а відмова призводить до повної неспроможності об’єкта виконувати жодну з потрібних функцій;

6)*за критичністю відмови* – сукупністю ознак, що характеризують наслідки відмови.. Класифікацію відмов за критичністю, наприклад, за рівнем прямих та непрямих втрат, пов’язаних з появою відмови, чи трудомісткістю відновлення після відмови встановлюють в нормативній та (або) конструкторській (проектній) документації за згодою з замовником на підставі техніко-економічних міркувань і вимог до забезпечення безпеки – *ресурсні та критичні:*

р е с у р с н а це відмова така, внаслідок якої об’єкт досягає граничного стану;

к р и т и ч н а відмова така, що за оцінками може привести до травмування людей, значних матеріальних збитків чи до інших неприйнятних наслідків.

7)за причинами відмови до яких відносяться обставини під час проектування, виробництва чи використання об’єкта, які привели до відмови через *перевантаження, неправильне поводження, неміцність, деградацію*:

відмова через перевантаження спричинена діянням під час використання об’єкта навантажень, що перевищують його встановлену спроможність;

відмова через неправильне поводження спричинена неправильним чи необережним поводженням з об’єктом;

відмова через неміцність спричинена неміцністю самого об’єкта, коли діяння навантаження на об’єкт не перевищують встановлену спроможність об’єкта. Неміцність може бути властива об’єктові чи запозичена;

деградовна відмова спричинена процесами деградації в об’єкті при дотриманні усіх встановлених правил і (чи) норм його проектування, виготовлення та експлуатації.

8)за обліком у технічно-експлуатаційної документації об’єкту *ураховувала і невраховувані:*

урахована відмову належить заносити у пояснювальну записку до наслідків випробувань чи експлуатації або у розрахунок величини показника безвідмовності. Повинні бути встановлені критерії врахування відмови;

неврахована відмову належить вилучити з пояснювальної записки до наслідків випробувань чи експлуатації або з розрахунків величини показника безвідмовності. Примітка. Повинні бути встановлені критерії вилучення відмови.

9)за виявленням – *явні та приховані:*

явна відмовавиявляється візуально чи штатними методами і засобами контролю та діагностування під час підготовки об’єкта до використання чи в процесі його використання за призначенням;

прихована відмова не виявляється візуально чи штатними методами і засобами контролю та діагностики, але виявляється під час проведення технічного обслуговування чи спеціальними методами діагностики.

Завершуючи характеристику об'єкта, необхідно згадати й такі поняття, як *відновлюваний об'єкт* і *невідновлюваний об'єкт, ремонтовний об’єкт та неремонтовнийоб'єкт*.

Відновлюваний об’єкт – ремонтовний об’єкт, який після відмови та усунення несправносте знову стає здатним виконувати потрібні функції з заданими кількісними показниками надійності

Невідновлюваний об’єкт – об’єкт, ремонт якого неможливий чи не дозволяє відновити працездатність із заданими кількісними показниками, надійності. Невідновлюваний об’єкт може бути як *ремонтовним* так і *неремонтовним*

Ці поняття характеризують умови використання об'єкта, досить важливі при розгляді його надійності. Слід чітко представляти, що залежно від умов той самий об'єкт може бути відновлюваним і невідновлюваним (апаратура ракети до пуску — відновлювана, а після — н е в і д н о в л ю в а н а).

Поняття «відновлюваний» об'єкт і «невідновлюваний об'єкт» слід відокремлювати від понять «ремонтовний об'єкт» і «неремонтовний об'єкт», тому що останнє характеризує властивості об'єкта.

Ремонтовний об'єкт; ремонтопридатний об'єкт – об'єкт, ремонт якого можливий та передбачений нормативною, ремонтною та (чи) конструкторською (проектною) документацією

Неремонтовний об'єкт; неремонтопридатний об'єкт – об'єкт, ремонт якого неможливий чи непередбачений нормативною, ремонтною та (чи) конструкторською (проектною) документацією

У ряді випадків ці поняття можуть збігатися (радіолампа — невідновлюваний об'єкт, вона ж і *неремонтопридатний* об'єкт).

При оцінці надійності об'єкта необхідно знати спосіб з'єднання складових його елементів. З'єднання елементів з погляду надійності, як правило, не відповідає їхній електричній схемі з'єднання, тому що воно здійснюється насамперед з урахуванням впливу кожного елемента на працездатність усього об'єкта. Розрізняють наступні з'єднання елементів: *послідовне, паралельне й змішане* (рис. 2.12)

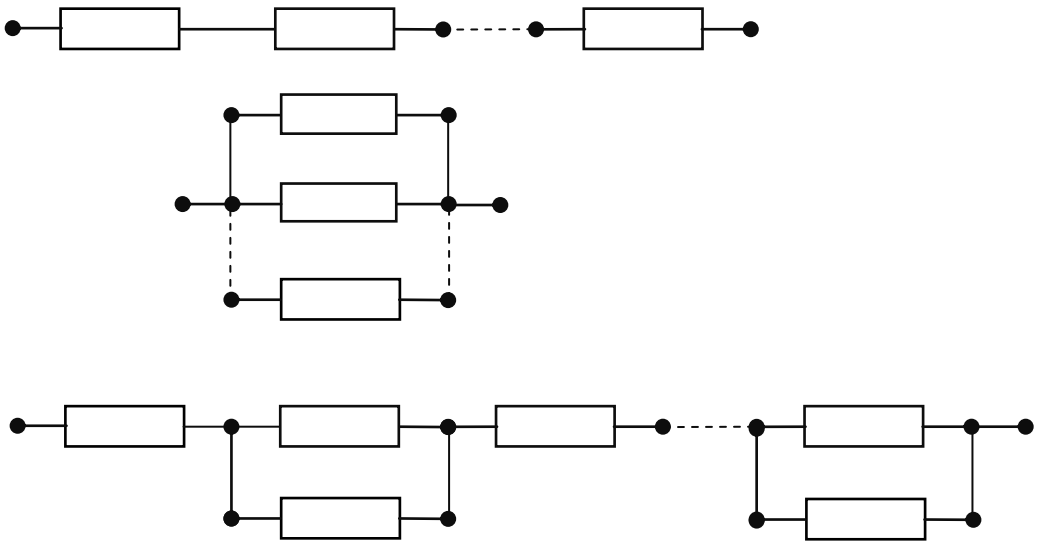


Рис. 2.12– Види з'єднання елементів в теорії надійності:

а) послідовне б) паралельне в) змішане

П о с л і д о в н и м з ' є д н а н н я м елементів називають таке з'єднання, при якому відмова хоча б одного елемента приводить до від-

мови в роботі всього об'єкта (рис. 2.12, а). Цей тип з'єднання в теорії надійності є основним.

П а р а л е л ь н и м з'єднаннямелементів називають таке з'єднання, при якому відмова в роботі відбувається тільки при відмові всіх елементів, що утворюють даний об'єкт (рис. 2.12, б).

З м і ш а н и м з ' є д н а н н я м е л е м е н т і в називають комбінація послідовного й паралельного з'єднань елементів (рис. 2.12, в).

Таким чином, надійність об'єкта розглядається в часі й залежить від якості його проектування, виготовлення й організації експлуатації.

2.4.2 Показники надійності

Розглянуті в 2.8 поняття й визначення є якісними характеристиками надійності. Для кількісного вираження надійності (її складових) об'єкта й для планування експлуатації використовують спеціальні характеристики — показники надійності. Вони дозволяють оцінювати надійність об'єкта або його елементів у різних умовах і на різних етапах експлуатації. Показники надійності можуть мати розмірність або бути безрозмірними величинами.

П о к а з н и к н а д і й н о с т і є кількісна характеристика однієї чи декількох із тих властивостей, які в сукупності складають надійність об’єкта.

Оскільки на надійність об'єкта впливають численні фактори, то кількість показників надійності може бути більша. Для обмеження цього їх доцільно підкорити певним вимогам:

а) погодженість із поняттям «надійність»;

б) можливість їх числового визначення або завдання;

в) можливість їх розрахунків за даними експлуатації й проектування;

г) достатня універсальність;

д) простота й зручність застосування.

Показники надійності повинні характеризувати кількісно властивості конкретного об'єкта, що визначають його надійність.

При вивченні показників надійності слід розрізняти:

а) найменування;

б) чисельне значення, яке може змінюватися залежно від умов експлуатації об'єкта й ступені його досконалості;

в) формулювання, що містить вказівки про способи визначення чисельного значення.

По кількості характеризуємих властивостей показники надійності підрозділяються на дві групи: *одиничні показники й комплексні показники.*

О д и н и ч н и й п о к а з н и к н а д і й н о с т і характеризує одну із тих властивостей, які в сукупності складають надійність об’єкта.

К о м п л е к с н и й п о к а з н и к н а д і й н о с т і характеризує

декілька властивостей, із тих, які в сукупності складають надійність об’єкта.

Залежно від умов одержання необхідних для розрахунків статистичних даних показники надійності можуть мати значення (табл. 2.3): *експлуатаційний*, *експериментальний*, *розрахунковий,екстрапольований, прогнозований, середній, гамма-відсотковий нестаціонарний стаціонарний.*

Таблиця2.3 – Значення показників надійності

Експлуатаційний показник надійності; спостережений показник надійності	Показник надійності, точкову чи інтервальну оцінку якого визначають за наслідками експлуатації
Експериментальний показник надійності; оцінний показник надійності	Показник надійності, точкову чи інтервальну оцінку якого визначають за даними випробувань
Розрахунковий показник надійності	Показник надійності, значення якого визначають шляхом розрахунку
Екстрапольований показник надійності	Показник надійності, отриманий шляхом екстраполяції чи інтерполяції для наробітку та (чи) умов, що відрізняються від тих, у яких отримано спостережений або оцінний показник надійності
Прогнозований показник надійності	Показник надійності, який розрахований на основі спостережених оцінних чи екстрапольованих показників надійності для частин об’єкту у заданих умовах експлуатації з врахуванням особливостей конструкції об’єкта
Середній показник надійності	Значення, отримане у вигляді математичного сподівання випадкової змінної величини (наробітку до відмови чи до граничного стану, терміну збережуваності, тривалості відновлювання) чи середнє значення наробітку до відмови (до граничного стану) всіх об’єктів у виборці при заданих умовах
Гамма-відсотковий показник надійності	Значення величини наробітку, терміну збережуваності, тривалості відновлення, протягом якого подія (відмова, досягнення граничного стану, відновлення) не виникає з імовірністю γ, визначеною у відсотках
Нестаціонарний показник надійності	Значення змінного у часі показника надійності у заданий момент часу
Стаціонарний показник надійності	Значення змінного у часі показника надійності, яке він приймає в умовах роботи об’єкта, коли параметри його характеристик залишаються незмінними

Слід ураховувати, що одиничні показники надійності для відновлюваних і невідновлюваний об'єктів можуть бути різними. Тому що надійність складна властивість, те повинні бути різні одиничні показники для оцінки її приватних властивостей: *безвідмовності*, *довговічності*, *ремонтопридатності й збережуваності* [6].

П о к а з н и к и б е з в і д м о в н о с т і

Невідновлюваний об'єкт*:*

1) імовірність безвідмовної роботи $R(t_1,t_2)$;
2) середній наробіток до відмови T_o;
3) інтенсивність відмов $\lambda(t)$;
4) середня інтенсивність відмов $\lambda(t_1, t_2)$;

Відновлюваний об'єкт*;*

1) імовірність безвідмовної роботи $R(t_1,t_2)$;
2) параметр потоку відмов $Z(t)$;
3) середній параметр потоку відмов $Z(t_1, t_2)$;
4) середній наробіток на відмову $T_{сер}$;
5) гамма-відсотковий наробіток на відмовуγ;

П о к а з н и к и д о в г о в і ч н о с т і

Невідновлюваний об'єкт:

1) середній ресурс;
2) гамма-відсотковий ресурс;
3) середній повний ресурс
4) середній термін служби;
5) гамма-відсотковий термін служби;
6) середній повний термін служби;

Відновлюваний об'єкт:

1) середній ресурс;
2) гамма-відсотковий ресурс;
3) середній повний ресурс;
4) середній ресурс між середніми (капітальними) ремонтами;
5) середній ресурс до середнього (капітального) ремонту;
6) середній термін служби;
7) гамма-відсотковий термін служби;
8) середній повний термін служби;
9) середній термін служби до середнього (капітального) ремонту;
10) середній термін служби між середніми (капітальними) ремонтами.

П о к а з н и к и р е м о н т о п р и д а т н о с т і :

1) Імовірність відновлення M(t);
2) Середня тривалість відновлення MTTR;
3) Гамма-відсоткова тривалість відновлення;
4) Інтенсивність відновлення $\mu(t)$;
5) Середня інтенсивність відновлення $\mu(t_1, t_2)$;
6) Середня трудомісткість технічного обслуговування [ремонту].

П о к а з н и к и з б е р е ж у в а н о с т і

1) середній термін збережуваності;
2) гамма-відсотковий термін збережуваності.

До к о м п л е к с н и х показників надійності ставляться;

1) коефіцієнт готовності; A(t);
2) коефіцієнт неготовності; коефіцієнт простою U(t);
3) середній коефіцієнт готовності; A (t_1, t_2);
4) стаціонарний коефіцієнт готовності A;
5) коефіцієнт оперативної готовності;
6) коефіцієнт технічного використання;
7) коефіцієнт збереження ефективності.

Розглянемо перелічені показники надійності більш детально у наступних параграфах.

2.4.3 Безвідмовність

Поняття безвідмовності є одним з найважливіших у теорії надійності, тому що воно безпосередньо пов'язане з виконанням об'єктом своїх функцій. Часто в літературі, особливо колишніх випусків, надійність розглядається у вузькому змісті слова й ототожнюється в першу чергу з безвідмовністю об'єкта. Математичні методи оцінки безвідмовності розвинені найбільше повно.

Надалі*під* б е з в і д м о в н і с т ю *будемо розуміти властивість об'єкта виконувати потрібні функції в певних умовах протягом заданого інтервалу часу чи наробітку* 2.8.) [6].

Н а р о б і т о к ; н а п р а ц ю в а н н я є тривалість чи обсяг роботи об'єкта. Наробіток може бути як неперервною величиною (тривалість роботи в годинах, кілометрах пробігу тощо), так і цілочисельною величиною (кількість робочих циклів, запусків тощо)

Для кількісної оцінки безвідмовності невідновлюваних об'єктів будемо використовувати одиничні показники безвідмовності.

Основним кількісним показником є й м о в і р н і с т ь б е з в і д м о в н о ї р о б о т и $P(t) = R(t_1,t_2)$ Імовірність того, що протягом заданого наробітку $t=t_2-t_1$ відмова об'єкта не виникне.

Звичайно вважають, що на початку інтервалу часу чи наробітку об'єкт у змозі виконувати потрібні функції.Виникнення відмови є випадковою подією, тому час появи відмови t_o — також випадкова величина.

Згідно з визначенням для ймовірності безвідмовної роботи можна записати

$$p(t) = R(t \le t_o), \qquad (2.1)$$

де t — поточний час,

Надалі для позначення ймовірності безвідмовної роботи або ймовірності появи відмови елемента будемо використовувати p и q, а систем — P и Q

Імовірність появи відмови – величина зворотна ймовірності безвідмовної роботи

$$q(t) = 1 - p(t) = F(t \geq t_o), \qquad (2.2)$$

тобто вірогідність появи відмови можна розглядати як імовірність того, що випадкова величина t_o прийме значення менше розглянутого часу t. Це дозволяє розглядати $q(t)$ як функцію розподілу $F(t \geq to$ випадкової величини t_0 -часу до появи першої відмови.

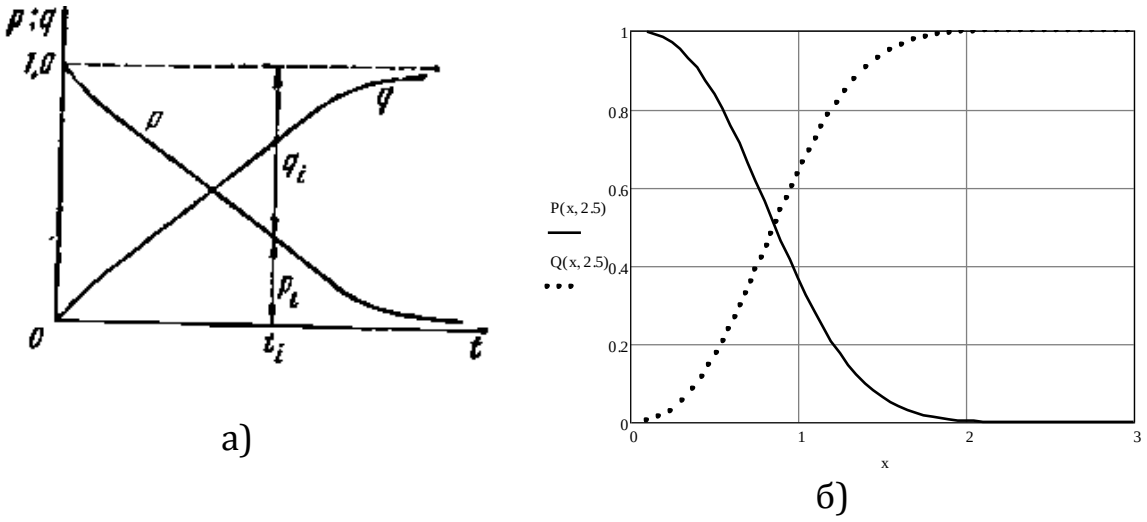
Як функція розподілу q (t) має наступні властивості:

а) не убутна, тобто при $t_2 > t_1$ $q(t_2) > q(t_1)$;

б) у початковий момент відліку часу при t = 0 $q(t) = 0$;

в) у межіпрагне до одиниці: $\lim_{t\to\infty} q(t) = 1$.

Функціональні залежності $p(t)$ і $q(t)$ показані на рис. 2.13.



а) б)

Рис. 2.13 – Функціональні залежності $p(t)$ і $q(t)$ а) та їх нормованих аналогів $P(x)$ і $Q(x)$ б), де $x=t/T_0$

Крім інтегральної характеристики, який є функція розподілу $q(t)$, широке поширення знаходить диференціальна характеристика у вигляді функції щільності розподілу — $f(t) = \frac{dq(t)}{dt}$:

$$f(t) = \frac{q(t+\Delta t)-q(t)}{\Delta t} = q'(t) \quad при\ \Delta t \to 0 \qquad (2.3)$$

або

$$q(t) = \int_0^t f(\tau)d\tau. \qquad (2.4)$$

З врахуванням вираження (2.4) вираження (2.1) може бути записане як

$$p(t) = 1 - \int_0^t f(\tau)d\tau = \int_0^\infty f(\tau)d\tau. \qquad (2.5)$$

Диференціюємо за часом вираження (2.2), неважко одержати

$$q'(t) = f(t) = -{}^{dp(t)}\!/_{dt} = -p'(t). \qquad (2.6)$$

Вираження (2.4), (2.5) і (2.6) визначають взаємозв'язок $p(t)$, $q(t)$ і $f(t)$.

Важливою характеристикою безвідмовності є інтенсивність відмов $\lambda(t)$ — умовна густина імовірності виникнення відмови об'єкта, яка визначається за умови, що до цього монету відмова не виникла.

Інтенсивність відмов є показником безвідмовності неремонтованих і невідновлюваних об'єктів.

Сходячі з визначення для моменту часу $(t, t + \Delta t)$з урахуванням вираження (2.4) можна записати:

$$q(t, t + \Delta t) = p(t)\lambda(t)\Delta t = f(t)\Delta t, \qquad (2.7)$$

З вираження (2.7) випливає

$$\lambda(t) = {}^{f(t)}\!/_{p(t)} \qquad (2.8)$$

як зо скористуватися виразами (2.6) і (2.8), можна скласти диференціальне рівняння безвідмовності:

$$\lambda(t) = -\frac{dp(t)}{p(t)dt}; \quad \lambda(t)dt = -\frac{dp(t)}{p(t)} \qquad (2.9)$$

Розв'язок цього диференціального рівняння відносно p(t) має вигляд

$$p(t) = e^{-\int_0^t \lambda(t)dt} + C$$

Значення постійної С знайдемо скориставшись початковими умовами t= 0: $p(0) = 1$, отже, $C = 0$.

Остаточний розв'язок диференціального рівняння (2.9) ухвалює вид

$$p(t) = e^{-\int_0^t \lambda(t)dt}. \qquad (2.10)$$

З виразу (2.9) одержимо

$$\int_0^t \lambda(t)dt = -\ln p(t) \qquad (2.11)$$

Скориставшись виразами (2.8), (2.10) і (2.11), знайдемо вираження, що зв'язує їх між собою:

$$f(t) = -\lambda(t)p(t) = \lambda(t)e^{-\int_0^t \lambda(t)dt} \qquad (2.12)$$

Скориставшись отриманим виразами(2.3 – 2.12), знаючи одну з функцій, можна знайти інші.Зв'язок між показниками безвідмовності наданий до табл. 2.4

Таблиця 2.4 – Зв'язок між показниками безвідмовності

Відома функція	Функція, яку знаходять			
	P(t)	*Q(t)*	*F(t)*	λ(t)
P(t)	—	1-*P(t)*	$-\frac{dP(t)}{dt}$	$-\frac{dP(t)}{P(t)dt}$
Q(t)	1 – *Q(t)*	—	$\frac{dQ(t)}{dt}$	$\frac{1}{1-Q(t)} \cdot \frac{dQ(t)}{dt}$
f(t)	$\int_t^\infty f(t)\,dt$	$\int_0^t f(t)\,dt$	—	$\frac{f(t)}{\int_t^\infty f(t)\,dt}$
λ(t)	$exp\left[-\int_0^t \lambda(t)\,dt\right]$	$1 - exp\left[-\int_0^t \lambda(t)\,dt\right]$	$\lambda(t) \cdot exp\left[-\int_0^t \lambda(t)\,dt\right]$	—

Якщо об'єкт містить, *N* послідовно включених однотипних елементів, то інтенсивність відмов визначається вираженням

$$\Lambda(t) = N\lambda(t) \ \ [1/год.] \qquad (2.13)$$

При наявності в об'єкті *K* груп різних елементів вираження (3/13) прийме вид

$$\Lambda(t) = \sum_{i=1}^{K} N_i\lambda_i(t) \ \ [1/год.] \qquad (2.14)$$

Залежність інтенсивності відмов від часу експлуатації для складних об'єктів ЕРВ показана на рис. 2.14.

Середня інтенсивність відмов $\lambda(t_1, t_2)$ – середнє значенню інтенсивності відмов у заданому інтервалі часу

$$\lambda(t_1,t_2) = \frac{1}{t_2-t_1}\int_{t_1}^{t_2} \lambda(t)dt \qquad (2.15)$$

На ньому чітко різняться три ділянки: *I* — приробітки; *II* — нормальної експлуатації; *III* — старіння.

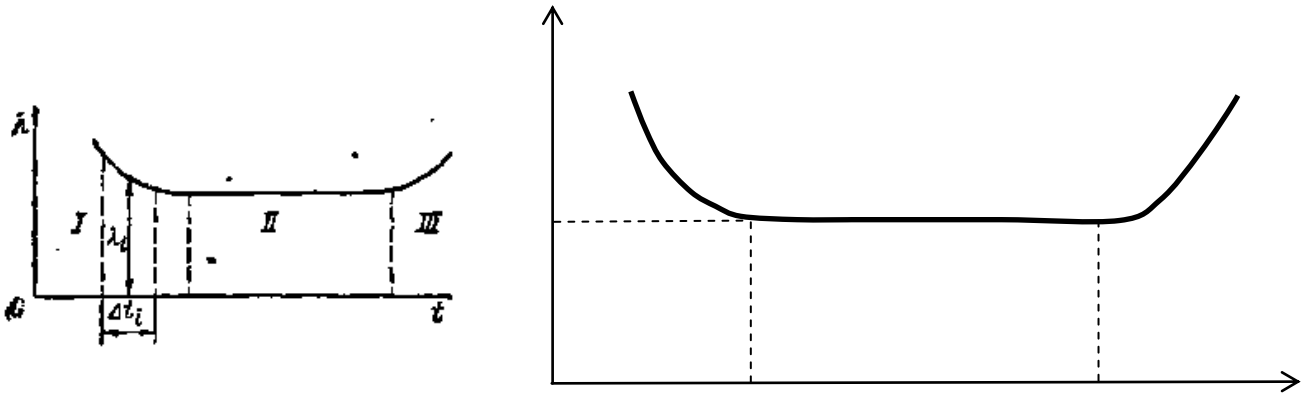


Рис. 2.14 – Залежність інтенсивності відмов від часу експлуатації

Характерним для першої ділянки є зниження інтенсивності відмов згодом. Це пояснюється швидким виявленням найменш надійних – об'єктів (елементів). Друга ділянка відбиває період, коли інтенсивність відмов стабілізується $\lambda(t)=const=\lambda_e$. Третя ділянка показує різке збільшення відмов, що пояснюється наближенням об'єктів до граничного стану. Цей період з експлуатації» як правило, виключається.

Тривалість чи обсяг роботи об'єкта характеризуються наробітком. Наробіток може бути як неперервною величиною (тривалість роботи в годинах, кілометрах пробігу тощо), так і цілочисельною величиною (кількість робочих циклів, запусків тощо).

Середній наробіток до відмови (T_0) – наробіток об'єкта від початку експлуатації до виникнення першої відмови, визначається як математичне очікування наробітку до першої відмови.

Відповідно до визначення

$$T_o = \int_0^\infty tf(t)dt = -\int_0^\infty tp'(t)dt. \qquad (2.16)$$

Інтегруючи отримане вираження вроздріб, одержуємо

$$T_o = \int_0^\infty tf(t)dt = -tp(t)|_0^\infty + \int_0^\infty p(t)dt = \int_0^\infty p(t)dt. \qquad (2.17)$$

Згідно з вираженням(2.17)*наробіток до відмови дорівнює площі під кривої ймовірності безвідмовної роботи*(див. рис. 2.13).

Для відновлюваних об'єктів характерне чергування справного стану й відновлення після відмови, тобто процес їх експлуатації можна представити як послідовне чергування інтервалів часу працездатного й непрацездатного станів (рис.2.15).

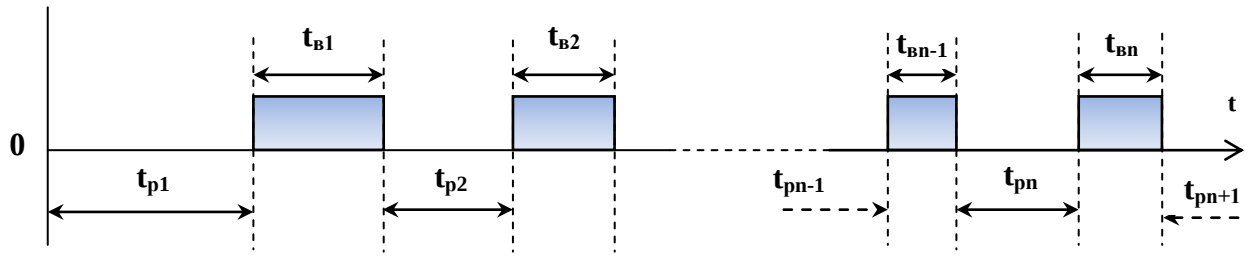


Рис. 2.15 – Характеристика процесу експлуатації відновлюємого об'єкту:

t_{pi} – час наробітку між сусідніми відмовами;$t_{ві}$– час відновлення після i – ї відмови

Поява відмов у кожному з N об'єктів можна розглядати як потік вимог для відновлення. Математичне очікування числа відмов за час t розглянутого потоку може бути визначене вираженням

$$M(t) = \lim \frac{1}{N} \sum_{i=1}^{N} m_i(t) \tag{2.18}$$

де $m_i(t)$— число відмов і-го об'єкта за час t.

У складному об'єкті результуючий потік відмов дорівнює сумі потоків відмов окремих пристроїв. Відповідно до [8, 9] результуючий потік буде найпростішим.

Нагадаємо, що найпростіший потік відмов повинен задовольняти умовам: *ординарності*, *стаціонарності й відсутності післядії*.

О р д и н а р н і с т ь п о т о к у означає, що ймовірність появи двох *і* більш відмов у той самий момент часу величина вищого порядку малості, тобто практично відсутня.

С т а ц і о н а р н і с т ь п о т о к у означає, що ймовірність появи рівно m відмов за проміжок $t, t + \Delta t$часу не залежить від t, а є функцією $\Delta t i\ m$.

В і д с у т н і с т ь п і с л я д і ї полягає в тому, що для двох відрізків часу Δt_1 і Δt_2 число відмов в одному з них не залежить від числа відмов, що потрапили в інший.

Основним типом потоку відмов ЕРВ *в умовах експлуатації можна вважати найпростіший.*

Основною характеристикою потоку відмов є п а р а м е т р п о т о к у в і д м о в Z(t) — відношення математичного сподівання кількості відмов відновлюваного об'єкта за досить малий його наробіток до значення цього наробітку

$$\mathrm{Z(t)}={M(t)}/{\Delta t} \tag{2.19}$$

Параметр потоку відмов характеризує щільність імовірності виникнення відмови відновлюваного об'єкта в розглянутий момент часу.

Середній параметр потоку відмов $Z(t_1, t_2)$ є середнє значення параметра потоку відмов у заданому інтервалі часу

$$Z(t_1, t_2) = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} Z(t)\, dt \qquad (2.20)$$

Для ординарних потоків без післядії параметр потоку пов'язаний з математичним очікуванням числа відмов вираженням

$$M(t) = \int_0^t Z(t)\, dt \qquad (2.21)$$

У випадку експонентного розподілу $f(t)$ (див. надалі § 2.11.)

$$Z(t) = \lambda = const \qquad (2.22)$$

Наробіток між відмовами – наробіток об'єкта від завершення відмовлення його працездатного стану після відмови до виникнення наступної відмови.

Для відновлюємих об'єктів замість показника «середній наробіток до відмови» T_o застосовується показник середній наробіток між відмовами; середній наробіток на відмову; $T_{сер}$ (MTTF), який визначається відношенням сумарного наробітку відновлюваного об'єкта до математичного сподівання числа його відмов протягом цього наробітку.

Згідно визначеннята формули (2.21)

$$T_{сер} = \frac{t_2 - t_1}{\int_{t_1}^{t_2} Z(t)dt} = \frac{t_2 - t_1}{M(t_2) - M(t_1)} \qquad (2.23)$$

При використанні вираженій (2.10) і (2.21, 2.23), неважко знайти вираження для ймовірності безвідмовності роботи відновлюваних об'єктів:

$$p(t_1, t_1 + t_2) = e^{-\int_{t_1}^{t_2} Z(t)dt} = e^{-[M(t_2) - M(t_1)]} = e^{-\frac{t_2 - t_1}{T_{сер}}}. \qquad (2.24)$$

Ці показники можуть бути використані для будь-якої фази й для будь-якого етапу експлуатації.

Гамма-відсотковий наробіток на відмову T_γ – наробіток, протягом якого відмова об'єкта не виникне з імовірністю γ, вираженою у відсотках.

Припустимо що в (2.24) $T_\gamma = t_2 - t_1$, тоді

$$T_\gamma = -T_{сер} \cdot ln\left(p_\gamma(t_1, t_1 + t_2)\right) = -\frac{ln\left({}^{\gamma}/_{100}\right)}{\lambda}\ , \tag{2.25}$$

де $\gamma = p_\gamma(t_1, t_1 + t_2) \cdot 100\%$ – імовірність не виникнення відмови об'єкта $p_\gamma(t_1, t_1 + t_2)$, виражена у відсотках.

Значення розглянутих параметрів можуть бути також знайдені на підставі обробки статистичного матеріалу результатів експлуатації або ж спеціально проведеного експерименту с групою об'єктів даного типу.

2.4.4 Загальні відомості про закони розподілу часу безвідмовної роботи

На поведінку об'єкта і його елементів у процесі експлуатації впливають численні зовнішні й внутрішні фактори. Вони є причиною появи відмов. Останні, наприклад, можуть виникати внаслідок впливу зовнішніх навантажень, вологи, нестабільності живлячих напруг через відхилення певних параметрів за межі допусків і т.п.

Відмови, особливо на ранніх стадіях експлуатації, можуть також виникати через недоліки проектування, виготовлення, порушень правил експлуатації.

Різні матеріали й елементи, використовувані в ЕРВ, викликають різноманітні форми впливу розглянутих факторів на виникнення відмови й, отже, на розподіл часу безвідмовної роботи.

З великої кількості існуючих законів розподілу випадкових величин необхідно використовувати ті, які найбільше повно описують розподілу, що цікавлять нас, часу безвідмовної роботи. Основним критерієм для цього повинен бути аналіз залежностей між механізмом відмов, що враховують фізикові реальних процесів при експлуатації, і функцією інтенсивності відмов.

Час безвідмовної роботи є безперервна випадкова величина й для опису її розподілу в теорії надійності використовуються наступні закони: Вейбулла, експонентний, Релея, нормальний і ін.

Розподіл Вейбулла-Гнеденка. Функція щільності розподілу

$$f(t) = \frac{b}{a}\left(\frac{t}{a}\right)^{b-1} \cdot e^{-\left({}^{t}/_{a}\right)^{b}}, \tag{2.26}$$

де a й b — параметри закону розподілу.

Скориставшись вираженнями (2.5, 2.26), знайдемо ймовірність безвідмовної роботи:

$$P(t) = 1 - \int_0^t f(\tau)d\tau = 1 - \int_0^t \frac{b}{a}\left(\frac{\tau t}{a}\right)^{b-1} \cdot e^{-(\tau/a)^b} d\tau\,. \qquad (2.27)$$

Інтегруймо отримане вираження. одержимо

$$P(t) = e^{-(t/a)^b} \qquad (2.28)$$

Використовуючи вираження (2.8) і (2.26, 2.28), одержимо вираження для інтенсивності відмов:

$$\lambda(t) = f(t)\Big/p(t) = \frac{b}{a}\left(\frac{t}{a}\right)^{b-1} \qquad (2.29)$$

З виразів (2.16) і (2.26) випливає:

$$T_o = \int_0^\infty tf(t)dt = \int_0^\infty t\frac{b}{a}\left(\frac{t}{a}\right)^{b-1} \cdot e^{-(t/a)^b} dt = \Gamma\left(1 + \frac{1}{b}\right) \qquad (2.30)$$

де $\Gamma\left(1 + \frac{1}{b}\right)$ — табульована гамма-функція,

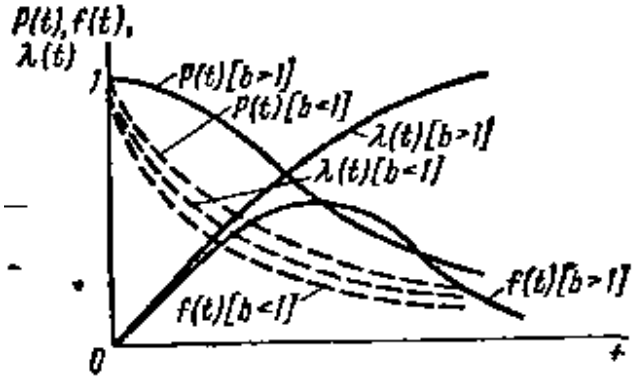
Залежності показників безвідмовності від часу дані на рис. 2.16

Цьому закону досить добре підкоряються розподіли відмов в об'єктах, що містять велику кількість однотипних невідновлюваних елементів, особливо коли відмова пов'язаний з погіршенням їх параметрів. Закон Вейбулла добре описує поведінка деяких типів електровакуумних, напівпровідникових і НВЧ – приладів.

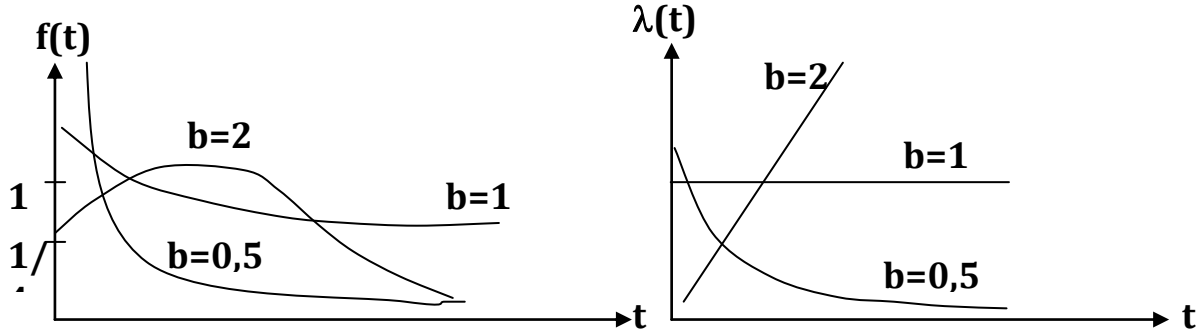
Параметри закону розподіли можуть бути визначені для конкретного випадку на підставі обробки статистичних відомостей по експлуатації даного типу об'єктів (елементів).

Оскільки параметр $a = T_0 = 1/\lambda$ має розмірність [год.] і може приймати різні значення, то форми функцій щільності розподілу $f(t, b, a)$ будуть різниця за масштабом і мати також розмірність [год.$^{-1}$]. Зручніше побудувати розрахункові нормовані до параметра a графіки залежностей $f(x, b)$ від безрозмірної нормованої змінної $x = \frac{t}{a} = \frac{t}{T_0} = \lambda t \geq 0$. Скористуємось стандартними функціями безрозмірного розподілу Вейбулла за допомогою програмного середовищем MathCad 14 для розрахунку $f(x, b), \lambda(x, b), Q(x, b), P(x, b)$:

$$\begin{cases} f(x, b) = \text{dweibull(x, b)} = b(x)^{b-1} \cdot e^{-(x)^b}; \\ \lambda(x, b) = b(x)^{b-1}; \\ (x, b) = \text{pweibull(x, b)} = 1 - e^{-(x)^b} \\ P(x, b) = 1 - \text{pweibull(x, b)} = e^{-(x)^b} \end{cases} \qquad (2.31)$$



а)



б) **в)**

Рис. 2.16– Показники безвідмовності при *b>1* и *b<1* а), аналітичні графіки функції густини імовірності розподілу відмов *f(t)* при *b=0,5, 1, 2* (б) й інтенсивності відмов *λ(t)*при *b=0,5, 1, 2*(в) для розподілу Вейбулла-Гнеденка

Розрахункові графіки нормованих функції густини імовірності розподілу відмов f(x,b), інтенсивності відмов λ(x,b), ймовірностей відмов Q(x,b) й безвідмовної роботи P(x,b) для розподілу Вейбулла представлені на рис. 2.17, 2.18.

***Експонентний розподіл*.** Його можна розглядати як окремий випадок розподілу Вейбулла при $b = 1$. Дійсно, якщо у виразах (2.26), (2.28, 2.29) і (2.30) підставити b = 1 , то ми отримаємо наступні формули $f(t), P(t), \lambda(t), T_o$ для експонентного розподілу

$$\begin{cases} f(t) = \frac{1}{a} \cdot e^{-t/a}; \\ P(t) = e^{-t/a}; \\ \lambda(t) = 1/a = \lambda = const \\ T_o = 1/\lambda = a \end{cases} \quad (2.32)$$

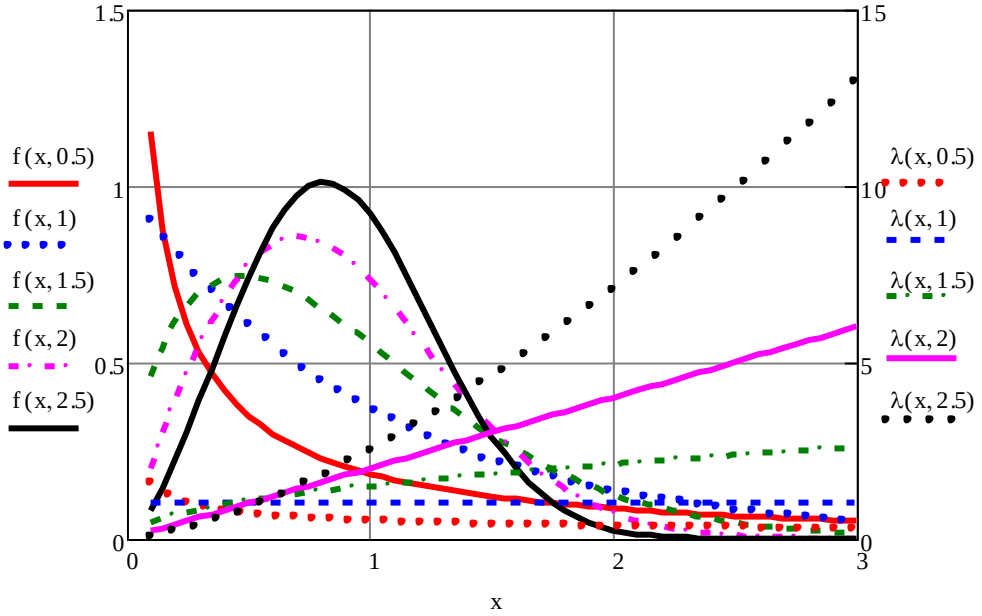


Рис. 2.17 – Розрахункові графіки нормованих функції густини імовірності розподілу відмов f(x,b) й інтенсивності відмов λ(x,b) для розподілу Вейбулла

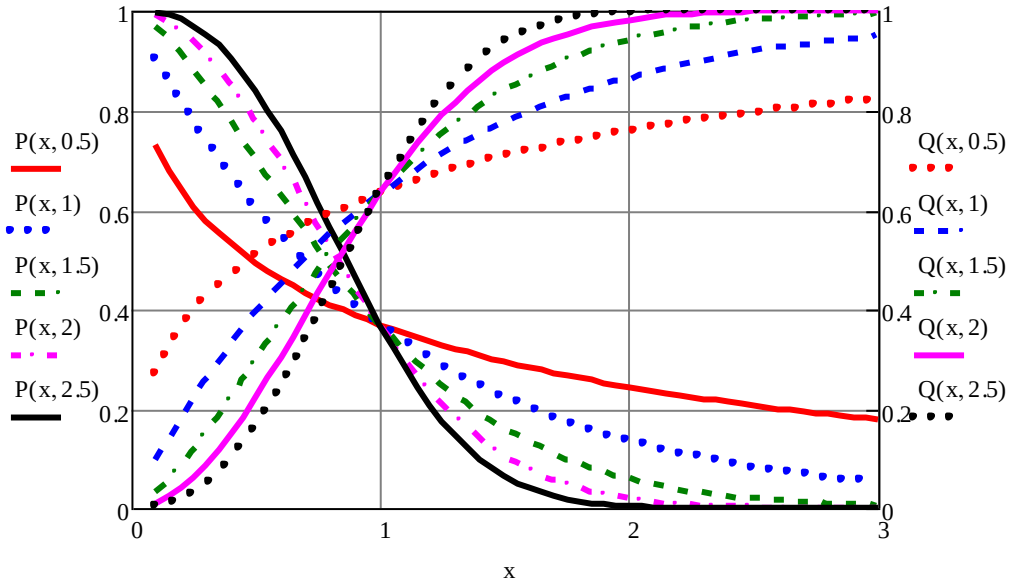
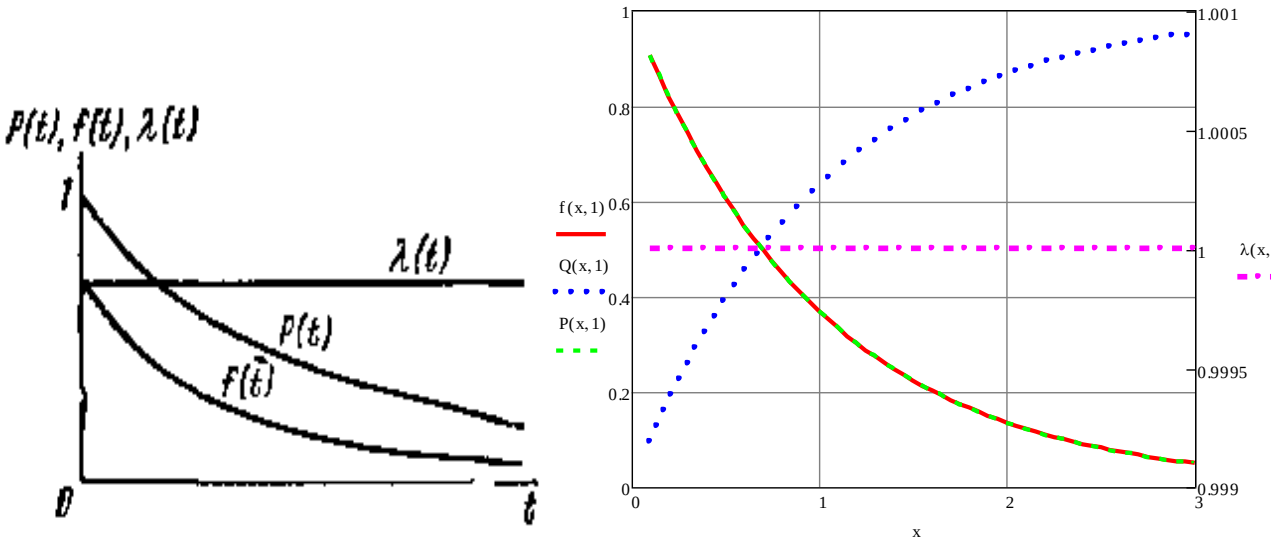


Рис. 2.18 – Розрахункові графіки нормованих функцій ймовірностей відмов Q(x,b) й безвідмовної роботи P(x,b) для розподілу Вейбулла

Цей розподіл типовий для більшості складних об'єктів ЕРВ, що містять велику кількість різних невідновлюваних елементів, що мають переважно раптові відмови, коли явища зношування й старіння виражені слабко. Експонентний розподіл також застосовується до відновлюваних об'єктів з найпростішим потоком відмов (2.22), а також у ряді випадків для наближеної оцінки безвідмовності.

Скористуємось стандартними функціями (2.32) безрозмірного розподілу Вейбулла для розрахунку нормованих функцій густини імовірності розподілу відмов f(x,1), й інтенсивності відмов λ(x,1), ймовірностей відмов Q(x,1) й безвідмовної роботи P(x,1) для експонентного розподілу

за допомогою програмного середовищем MathCad 14, відповідні графіки представлені на рис. 2.19.



а) **б)**

Рис. 2.19– Аналітичні показники безвідмовності а),розрахункові графіки нормованих функцій густини імовірності розподілу відмов f(x,1), й інтенсивності відмов λ(x,1), ймовірностей відмов Q(x,1) й безвідмовної роботи P(x,1) б) для експонентного розподілу часу безвідмовної роботи

Розподіл Релея. Його можна так само розглядати, як окремий випадок розподілу Вейбулла при $b = 2$.

Підставляючи у вираження (2.26), (2.28), (2.29) і (2.30) зазначене значення $b=2$ одержимо

$$\begin{cases} f(t) = \frac{2t}{a^2} \cdot e^{-(t/a)^2} \\ P(t) = e^{-(t/a)^2} \\ \lambda(t) = \frac{2t}{a^2} = \frac{2t}{T_o^2} \\ T_{сер} = a\frac{\sqrt{\pi}}{2} \approx 1{,}253a \end{cases} \quad (2.33)$$

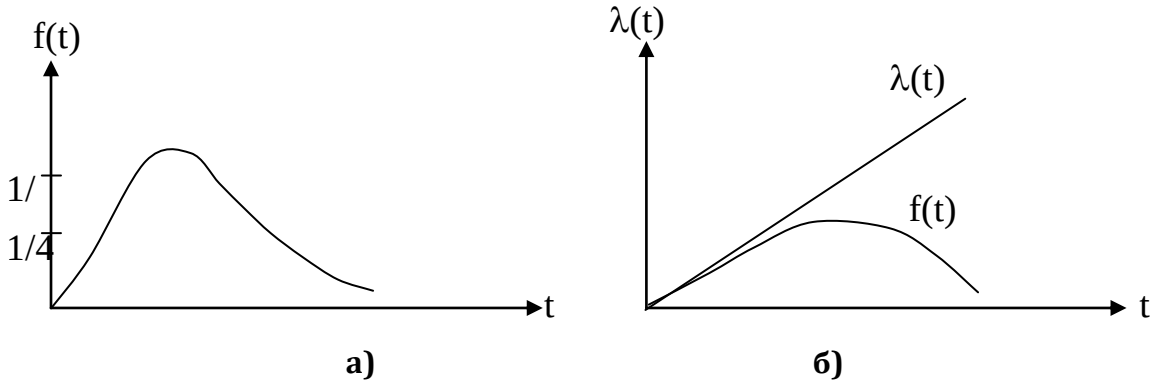
де $a=T_o$ – параметр розподілу [8, 9].

Розподіл Релея достатньо повно описує поведінку технічних об’єктів і їх елементів з явно вираженим ефектом старіння і зношеності.

Середнє квадратичне відхилення середнього наробітку до відмови

$$\sigma_t = \sqrt{(T_{сер})^2 - (T_o)^2} = \sqrt{\left(T_o \cdot \sqrt{\frac{\pi}{2}}\right)^2 - (T_o)^2} = \sqrt{\frac{\pi}{2} - 1} \cdot T_o = 0{,}755 \cdot T_o \quad (2.34)$$

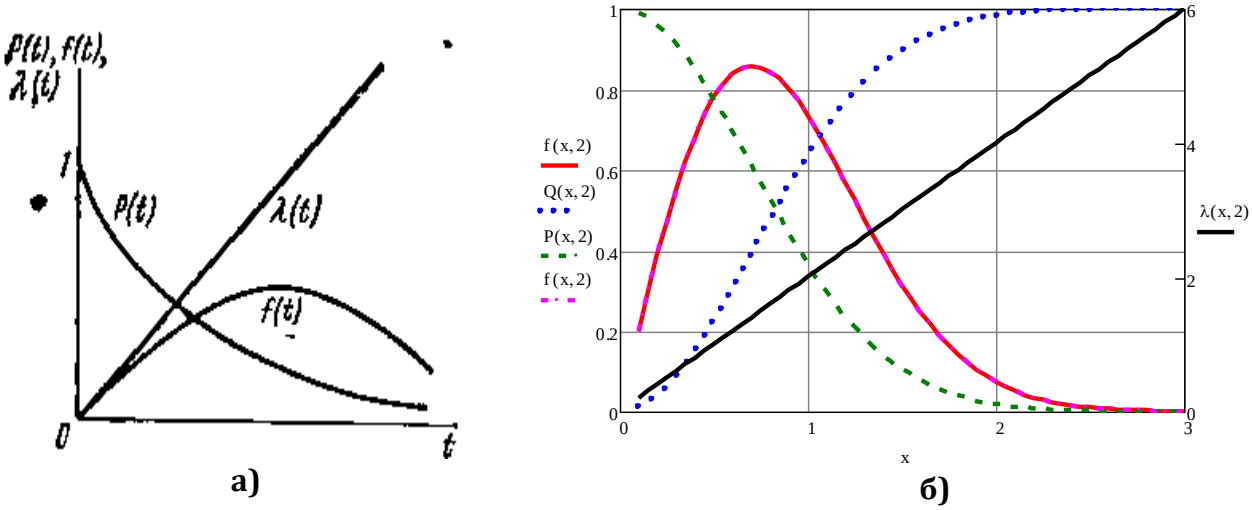
Залежності показників безвідмовності від часу у випадку розподілу за законом Релея дані на рис. 2.20.



а) **б)**

Рис. 2.20 – Аналітичні графіки залежності густини імовірності відмов *f(t)* (а) інтенсивності відмов λ(*t*) (б) для розподілу часу безвідмовної роботиза законом Релея

Скористуємось стандартними функціями (2.23) у випадку нормованого розподілу Релея для розрахунку нормованих функцій густини імовірності розподілу відмов f(x,1), й інтенсивності відмов λ(x,1), ймовірностей відмов Q(x,1) й безвідмовної роботи P(x,1) за допомогою програмного середовищем MathCad 14 , відповідні графіки представлені на рис. 2.21.



а) **б)**

Рис. 2.21– Аналітичні показники безвідмовності (b=2) а) та розрахункові графіки нормованих функцій густини імовірності розподілу відмов f(x,2), й інтенсивності відмов λ(x,2), ймовірностей відмов Q(x,2) й безвідмовної роботи P(x,2) для розподілу часу безвідмовної роботи за законом Релея

Нормальний розподіл. Цей розподіл, широко використовуване в теорії імовірності, також знайшло застосування й у теорії надійності.

Щільність розподілу

$$f(t) = \frac{1}{\sigma_t \sqrt{2\pi}} e^{-\frac{(t-t_{cp})^2}{2\sigma_t{}^2}} \tag{2.35}$$

де $t_{\text{ср}}$ — математичне очікування часу появи першої відмови;
σ_t — середнє квадратичне відхилення.

Тому що для більшості практичних випадків $t_{cp}/\sigma_t > 2$ то нема необхідності враховувати усікання закону розподілі про зв'язок з тим, що час може змінюватися тільки в межі $0 \div \infty$. При цьому для розрахунків зручно скористатися центрованою й нормованою величиною $z = \frac{t-t_{cp}}{\sigma_t} = \frac{t}{\sigma_t} - \frac{t_{cp}}{\sigma_t}$. У цьому випадку при $t_{cp} = 0, \sigma_t = 1$маємо наступний вигляд виражень для нормального розподілу:

$$\begin{cases} f_0(z) = \sigma_t f(z) = \frac{1}{\sqrt{2\pi}} e^{-\frac{z^2}{2}} \\ Q(z) = 0{,}5 + F(z) \\ P(z) = 0{,}5 - F(z) \\ \lambda(z) = \frac{f_0(z)}{P(z)} \\ T_o = t_{cp} + \sigma_t \frac{\lambda(z=0)}{\sqrt{2\pi}} \end{cases} \tag{2.36}$$

де $F(z) = \begin{cases} F_0(z), \text{як що } z \geq 0 \\ -F_0(|z|), \text{як що } z \leq 0 \end{cases}$ – функція центрованого й нормованого нормального розподілу;

$F_0(z) = \frac{1}{\sqrt{2\pi}} \int_0^z e^{-\frac{t^2}{2}} dt$ — інтеграл ймовірностей (інтеграл Лапласа).

Функції $f_0(z)$ та $F_0(z)$ табульовані, що полегшує розрахунки [9].

Нормальний закон розподілу описує надійність об'єктів, яким характерне типове зношуванняоднорідних елементів, при цьому всі відмови однорідні по якості й мають *малий* розкид зношування.

Час відновлення ремонтованих об'єктів і сумарний наробіток об'єкта до середнього (капітального) ремонту в ряді випадків можуть бути також описані нормальним законом.

Безпосередньо в такому вигляді закон може застосовуватися для випадків $T_{\text{сер}} >> \sigma_t$. Це пов’язане з тим, що при нормальному розподілі випадкова величина може мати будь-які значення від -∞ до ∞. Оскільки можливі значення випадкової наробітки до відмови можуть бути тільки позитивними, її розподіл слід приймати зрізано нормальним, або зви-

чайним нормальним при $T_{сер}>>\sigma_t$. Вже при $T_{сер}/\sigma_t>2{,}5$ від'ємна гілка закону вносить зневажливо малу вагу в загальний результат.

Аналітичний виглядзалежності показників безвідмовності від часу при нормальному законі розподілу дано на рис 2.13.

Скористуємось [9] та стандартними функціями (2.36) центрованого й нормованого нормального розподілу для розрахунку нормованих функцій густини імовірності розподілу відмов f(z), й інтенсивності відмов λ(z), ймовірностей відмов Q(z) й безвідмовної роботи P(z) за допомогою програмного середовищем MathCad 14, аналітичні та розрахункові графіки представлені на рис. 2.22, 2.23.

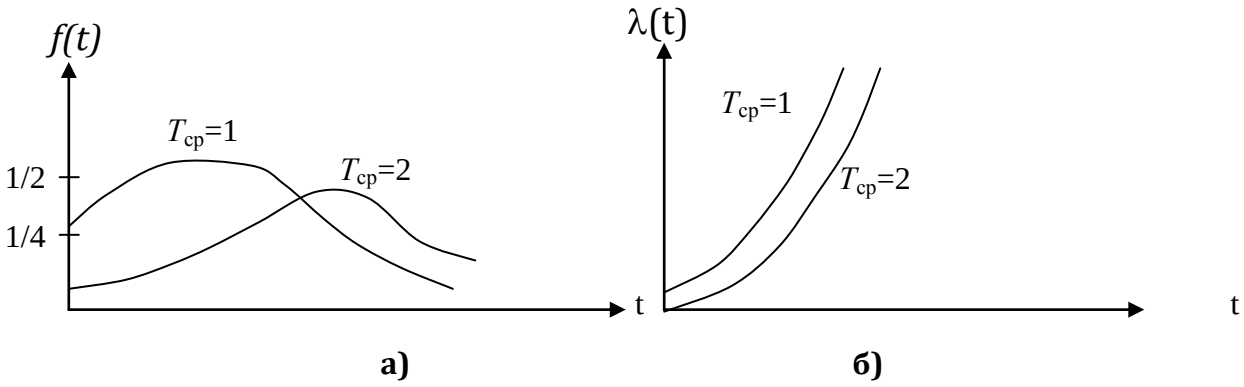


Рис. 2.22 – Аналітичні графіки густини імовірності f(t) при σ_t=1 (а) і інтенсивність відмов λ(t) (б) для нормального розподілучасу безвідмовної роботи

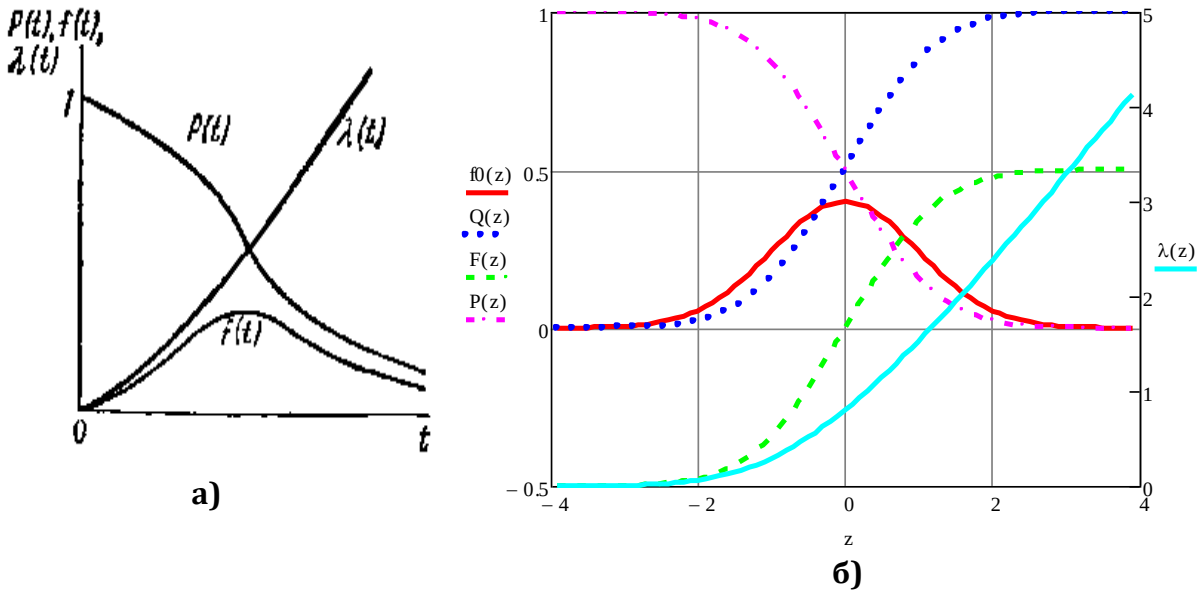


Рис. 2.23 – Аналітичні показники безвідмовності а)та розрахункові графіки нормованих функцій густини імовірності розподілу відмов $f_0(z)$ функції нормованого й центрованого нормального розподілу F(z), й інтенсивності відмов λ(z), ймовірностей відмов Q(z) й безвідмовної роботи P(z) для нормального розподілу часу безвідмовної роботи

Розподіл Пуассона описується наступним вираженням

$$f_k(t, t+\Delta t) = \frac{[M(t,t+\Delta t)]^k}{k!} e^{-M(t,t+\Delta t)}, \qquad (2.37)$$

де $f_k(t, t+\Delta t)$ — імовірність того, що відбудеться рівно k відмов на інтервалі часу $t, t+\Delta t$;

$M(t, t+\Delta t)$— математичне очікування числа відмов на інтервалі часу $t, t+\Delta t$.

Якщо пуассоновій потік задовольняє умові стаціонарності, то вираження (2.37) прийме вид

$$f_k(\Delta t) = \frac{(\omega \Delta t)^k}{k!} e^{-\omega \Delta t} = \frac{m^k}{k!} e^{-m}, \qquad (2.38)$$

де $m = \omega \Delta t = \lambda \Delta t$ – середнє число відмов в інтервалі $(t, t+\Delta t)$

Розподіл Пуассона, досить широко використовуваному в теорії надійності. Інтервали часу між відмовами в пуассоновому потоці відмов взаємонезалежні й розподілені за експонентним законом, тобто пуассоновій потік задовольняє властивостям ординарності й відсутності післядії. Розподіл Пуассона застосовний для відновлюваних об'єктів з найпростішим потоком відмов (2.22), а також для ділянки приробляння (рис. 2.24).

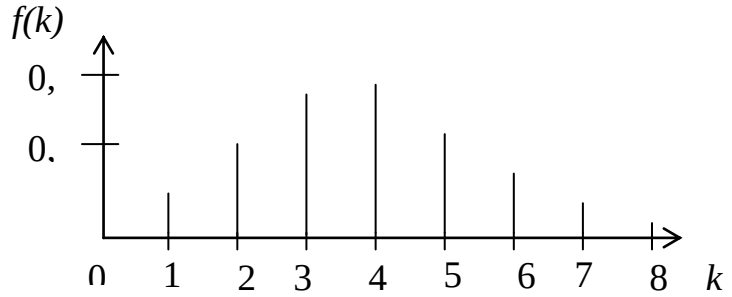


Рис. 2.24 – Аналітичний графік розподілу часу безвідмовної роботиза законом Пуассона

Розподіл Пуассона (рис. 2.13) описує поведінку дискретних випадкових величин. Випадкова величина t розподілена за законом Пуассона, якщо імовірність того, що воно прийме деяке значення k, виражається формулою (2.38)

Дисперсія випадкової величини t дорівнює її математичному сподіванню

$$D_t = m. \qquad (2.39)$$

Інтенсивність відмов дорівнює

$$\lambda(t) = m/\Delta t \qquad (2.40)$$

Оскільки функція $f_k(t)$ – дискретна, то в неї нема похідних.

Дискретні значення не повинні бентежити, оскільки практично всі експериментальні спостереження за безвідмовністю роботи технічного об'єкту проводяться в дискретному часі.

Скористуємось стандартними функціями (2.38) розподілу Пуассона для розрахунку функцій густини імовірності розподілу відмов *f(k,m)*, й інтенсивності відмов *λ(k,m)*, ймовірності появи не менш *k* відмов *Q(k,m)* й імовірності появи не більш *k* відмов*P(k,m)* при математичному очікуванні кількості відмов *m=5* за допомогою програмного середовищем Math-Cad 14, розрахункові графіки представлені на рис. 2.25.

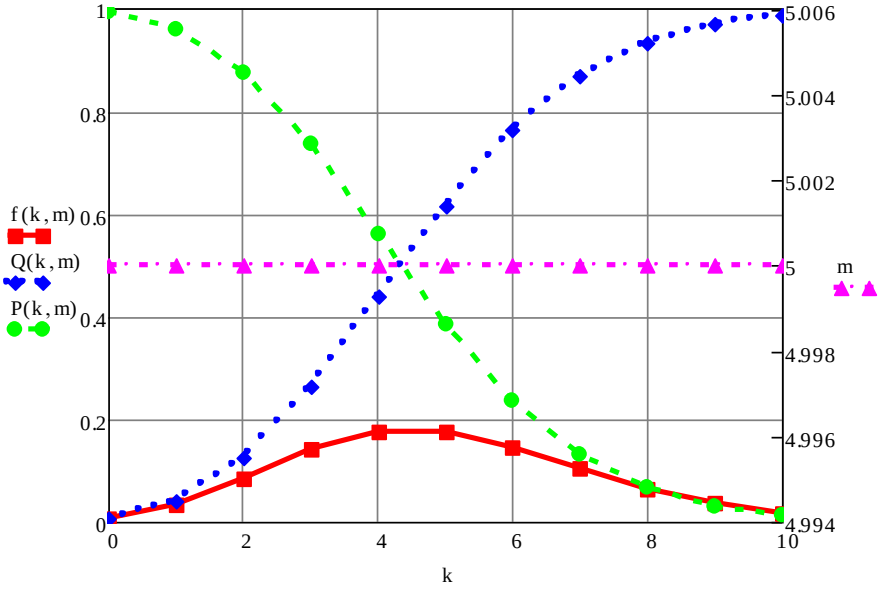


Рис. 2.25 – Розрахункові графіки нормованих функцій розподілу Пуассона: густини імовірності розподілу відмов *f(k,m)*, , ймовірності появи не менш *k* відмов *Q(k,m)* й імовірності появи не більш *k* відмов*P(k,m)* при математичному очікування кількості відмов *m=5*

Імовірність безвідмовної роботи об'єкту *P(t)* означає, що за час періоду експлуатації роботи $t, t + \Delta t$відмов в апаратурі не виникло, тобто кількість відмов дорівнює нулю (k=0), тому *P(t)* може бути отримана з (2.37) по наступній розрахунковій формулі

$$P_{k=0}(\Delta t) = f_{k=0}(\Delta t) = e^{-\omega \Delta t} = e^{-\lambda \Delta t}$$
$$P_{k=0}(m) = e^{-m}, \qquad (2.41)$$

Це відоме для ймовірності безвідмовної роботи експонентного розподілу вираження (2.32)

Для найпростішого потоку справедливо

$$\begin{cases} f_{k=0}(m) = e^{-m}; \\ P_{k=0}(m) = e^{-m}; \\ Q_{k=0}(m) = 1 - e^{-m} \\ m = \lambda \cdot \Delta t; \\ \lambda(\Delta t) = {}^{m}/_{\Delta t} \\ T = T_o = {}^{1}/_{\lambda} \end{cases} \quad (2.42)$$

Скористуємось стандартними функціями (2.42) нормованого розподілу Пуассона для розрахунку нормованих функцій густини імовірності розподілу відмов *f(0,m)*, й інтенсивності відмов $\lambda_n(0,m)$, ймовірності відмови *Q(0,m)* й імовірності безвідмовної роботивідмов*P(k,m)* при *k=0* та в залежності від нормованого значення математичного очікування кількості відмов m=0…5 за допомогою програмного середовищем MathCad 14, розрахункові графіки представлені на рис. 2.26.

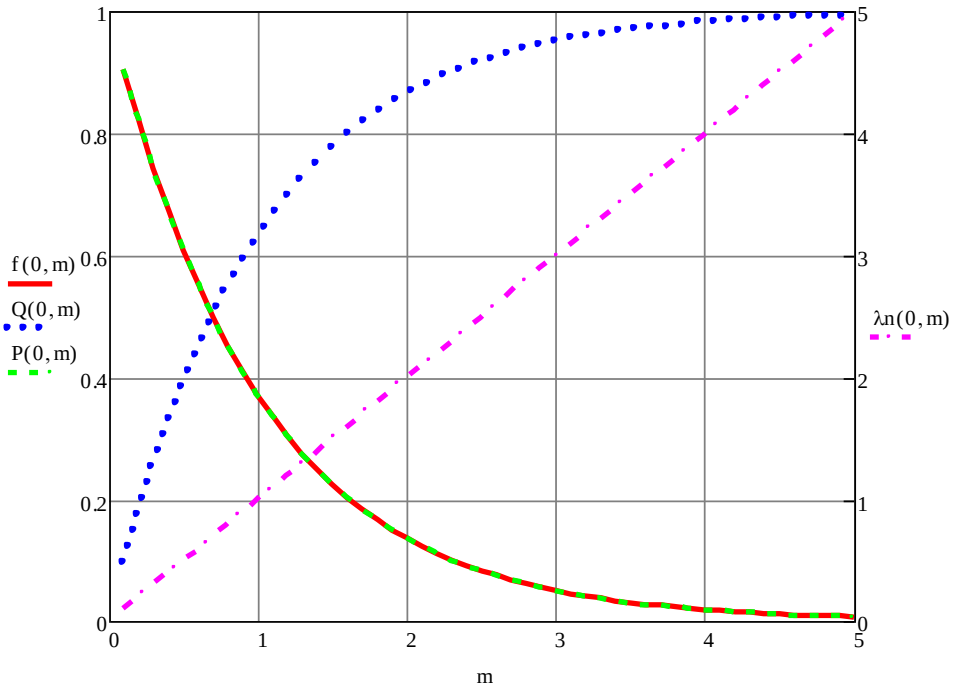


Рис. 2.26 – Розрахункові графіки нормованих функцій розподілу Пуассона: густини імовірності розподілу відмов *f(0,m)*, інтенсивності відмов $\lambda_n(0,m)$, ймовірності відмови *Q(0,m)* й імовірності безвідмовної роботи*P(0,m)* в залежності від нормованого значення математичного очікування кількості відмов *m=0…5*

Помітимо, що на графіку (рис. 2.26) траєкторії нормованих функцій імовірності безвідмовної роботи *P(0,m)* та імовірності розподілу відмов *f(0,m)* збігаються і практично зменшуються до нуля починаючи з нормованого значення математичного очікування відмов m>5, а значення інтенсивності відмов $\lambda_n(0,m)$ лінійно зростають з підвищенням m.

Рівномірний розподіл використовується при оцінці надійності об'єктів щодо повторюваних відмов для деякого інтервалу часу $t_2>t>t_1$, в якому щільність розподілу відмов постійна, тобто $f(t)=\frac{1}{a}$, а за його межами дорівнює нулю $f(t)=0$ (рис. 2.27).

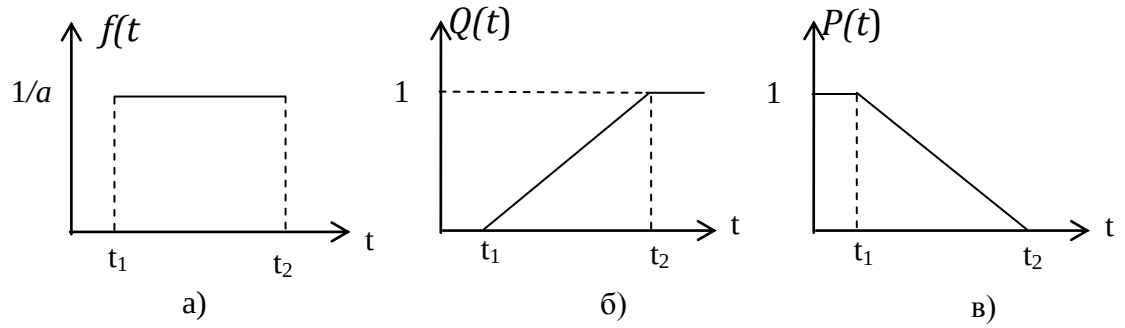


Рис. 2.27 – Аналітичні графіки густини імовірності відмов *f(t)* (а) й імовірності відмов *Q(t)* (б) імовірності безвідмовної роботи *Q(t)* (в) для рівномірного закону розподілу часу безвідмовної роботи

Постійна величина a може бути визначена з умови рівності одиниці площі, обмеженої кривій розподілу та тому дорівнює наробітку $a=t_2-t_1$ на обраному інтервалі $[t_2,t_1]$.

Знайдемо функцію розподілу *F(t),* яка визначає імовірність відмови*Q(t)=F(t)* та імовірність безвідмовної роботи *P(t)* на інтервалі $[t_2,t_1]$

$$Q(t)=F(t)=\int_{-\infty}^{t}f(t)dt=\int_{t_1}^{t}\frac{1}{t_2-t_1}dt=\frac{t}{t_2-t_1}|_{t_1}^{t}=\frac{t-t_1}{t_2-t_1} \qquad (2.43)$$

$$P(t)=1-Q(t)=1-\frac{t-t_1}{t_2-t_1} \qquad (2.44)$$

Для того, щоб випадкова величина t підкорялася закону рівномірного розподілу необхідно, щоб її значення лежали усередині деякого певного інтервалу, і усередині цього інтервалу значення цієї випадкової величини були б рівно імовірними.

Визначимо математичне очікування й дисперсію випадкової величини t, підкореній рівномірному закону розподілу.

$$m_t=\int_{t_1}^{t_2}t\cdot f(t)dt=\int_{t_1}^{t}\frac{t}{t_2-t_1}dt=\frac{t^2}{2\cdot(t_2-t_1)}|_{t_1}^{t_2}=\frac{t_2+t_1}{2}$$

$$m_{t^2}=\int_{t_1}^{t_2}t^2\cdot f(t)dt=\int_{t_1}^{t}\frac{t^2}{t_2-t_1}dt=\frac{t^3}{3\cdot(t_2-t_1)}|_{t_1}^{t_2}= \qquad (2.45)$$

$$= \frac{{t_2}^3 - {t_1}^3}{3 \cdot (t_2 - t_1)} = \frac{{t_2}^2 + t_2 t_1 + {t_1}^2}{3}$$

$$D_t = {m_t}^2 - {m_t}^2 = \frac{{t_2}^2 + t_2 t_1 + {t_1}^2}{3} - \frac{{t_2}^2 + 2t_2 t_1 + {t_1}^2}{4} = \frac{{t_2}^2 - 2t_2 t_1 + {t_1}^2}{12}$$

$$= \frac{(t_2 - t_1)^2}{12}$$

$$\sigma_t = \sqrt{D_t} = \frac{t_2 - t_1}{2 \cdot \sqrt{3}}$$

Імовірність влучення рівномірно розподіленої випадкової t величини в заданий інтервал:

$$F(t_\alpha < T < t_\beta) = \int_{t_\alpha}^{t_\beta} f(t)dt = \int_{t_\alpha}^{t_\beta} \frac{1}{t_2 - t_1} dt = \frac{t}{t_2 - t_1}\Big|_{t_\alpha}^{t_\beta} = \frac{t_\beta - t_\alpha}{t_2 - t_1} \qquad (2.46)$$

Отримані параметри рівномірного розподілу зведемо у систему формул (2.47)

$$\begin{cases} f(t) = \frac{1}{a} = \frac{1}{t_2 - t_1} = const; \\ Q(t) = \frac{t - t_1}{t_2 - t_1} \\ P(t) = 1 - \frac{t - t_1}{t_2 - t_1}; \\ m_t = T_o = \frac{t_2 + t_1}{2} = \frac{2t_1 + a}{2}; \ при < \ t_1 < t < t_2 \\ \sigma_t = \sqrt{D_t} = \frac{t_2 - t_1}{2 \cdot \sqrt{3}}; \\ \lambda = {}^1\!/_{T_o} = \frac{2}{t_2 + t_1} \\ F(t_\alpha < T < t_\beta) = \frac{t_\beta - t_\alpha}{t_2 - t_1} \end{cases} \qquad (2.47)$$

Скористуємось стандартними функціями (2.42) центрованого й нормованого рівномірного розподілу для розрахунку нормованих функцій густини імовірності розподілу відмов *f(x)*, й інтенсивності відмов *λ(x)*, ймовірностей відмов *Q(x)* й безвідмовної роботи *P(x)* при $x=t/t_2, t_1=0, t_2=1$ за допомогою програмного середовищем MathCad 14, аналітичні та розрахункові графіки представлені на рис. 2.28.

Крім розглянутих законів у деяких випадках можуть застосовуватися й інші. Так, для об'єктів з відмовами внаслідок втомленого руйнування, а також для деяких видів електровакуумних приладів застосовують логарифмічно нормальний розподіл.

Застосовність того або іншого закону також визначається часом експлуатації об'єкта і її етапом.

Дослідження показали, що поведінка багатьох складних об'єктів ЕРВ на першій ділянці експлуатації (див. рис. 2.12) досить добре описується законом розподілу Вейбулла з b<1 на другій ділянці — експонентним законом, а на третьому — розподілом Релея.Тому що основною ділянкою нормальної експлуатації є другою (див. рис. 2.3), те основним законом для розрахунків безвідмовності слід уважати експонентний.

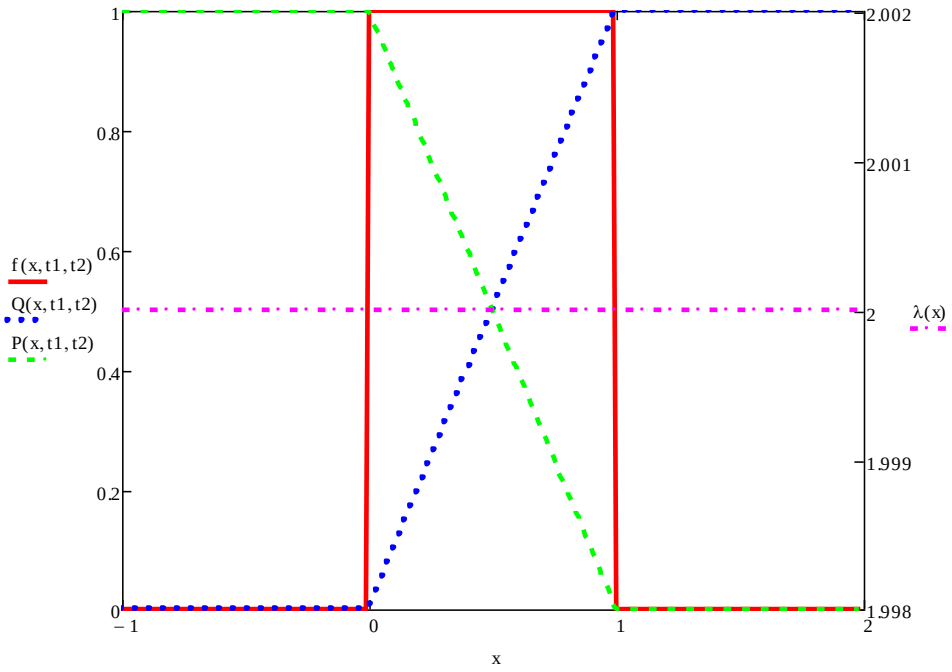


Рис. 2.28– Розрахункові графіки центрованих нормованих функцій густини імовірності розподілу відмов *$f_0(x)$*, інтенсивності відмов *$\lambda(x)$*, ймовірностей відмов *$Q(x)$* й безвідмовної роботи *$P(x)$* для рівномірногорозподілу, де *$x=t/t_2, t_1=0, t_2=1$*.

2.4.5 Довговічність

Час нормального функціонування всякого об'єкта обмежене неминучою зміною властивостей матеріалів і деталей, з яких він виготовлений. Тому період нормального функціонування різних об'єктів ЕРВ буде не однаковий, тому що його тривалість залежить від властивостей, властивих даному об'єкту. Ці властивості визначають терміном «довговічність».

Під д о в г о в і ч н і с т ю мається на увазі – *властивість об'єкта виконувати потрібні функції до переходу у граничний стан при встановленій системі технічного обслуговування та ремонту* (§ 2.8)[6].

Слід звернути увагу на те, що на відміну від визначення безвідмовності (де головним є безперервність збереження працездатності) визначення довговічності пов'язане зі збереженням працездатності до заданого межі з необхідними перервами.

Для невідновлюваних елементів (електровакуумні прилади, резистори, конденсатори, діоди, транзистори, інтегральні мікросхеми й т.п.) значення довговічності збігається із часом їх експлуатації до відмови.

З метою кількісної оцінки властивостей об'єкта, поєднуваних поняттям «довговічність», використовуються одиничні показники довговічності: т е р м і н с л у ж б и й р е с у р с .

Т е р м і н с л у ж б и визначається календарною тривалістю експлуатації об’єкта від початку чи її поновлення після ремонту до переходу в граничний стан.

При використанні показників довговічності слід вказувати початок відрахунку та вид дії після настання граничного стану, наприклад, гамма-відсотковий ресурс від другого капітального ремонту до списання.

Показники довговічності, які відраховуються від введення об’єкта в експлуатацію до повного зняття з експлуатації, називаються: середній повний ресурс (термін служби), гамма-відсотковий повний ресурс (термін служби)

Для відновлюваних і невідновлюваних об'єктів розрізняють *середній термін служби;гамма-відсотковий термін служби;середній повний термін служби.*

С е р е д н і й т е р м і н с л у ж б и $T_{ср.\ сл.}$ — математичне сподівання терміну служби;

$$T_{ср\,сл} = \int_0^\infty t_{слі}\, f(t_{сл}) t \tag{2.48}$$

де $t_{слі}$— термін служби *i* – го об'єкта;

$f(t_{сл})$— функції щільності розподілу часу терміну служби.

С е р е д н і й п о в н и й т е р м і н с л у ж б и $T_{ср.\ сл.\ п.}$ – календарна тривалість експлуатації від введення об’єкта в експлуатацію до повного зняття з експлуатації.

Значення цієї величини визначається на підставі статистичних, даних експлуатації певної апаратури.

Г а м м а - в і д с о т к о в и й т е р м і н с л у ж б и $T_{сл.\ \gamma}$ – календарна тривалість експлуатації, протягом якої об’єкт не досягне граничного стану з імовірністю γ, вираженою у відсотках, визначається вираженням

$$1 - Q(T_{сл.\ \gamma}) = P(T_{сл.\ \gamma}) = \frac{\gamma}{100} \tag{2.49}$$

де $Q(T_{сл.\ \gamma})$ – функція розподілу терміну служби.

Уважаючись закон розподілу часу безвідмовної роботи елементів об'єкта експонентним і скориставшись вираженням (2.33) і (2.49), напишемо

$$P(t) = e^{-\lambda T_{сл.\ \gamma}} = \frac{\gamma}{100} \tag{2.50}$$

Логарифмуючи дане вираження, одержимо

$$T_{сл.\ \gamma} = -\frac{1}{\lambda}\ln\frac{\gamma}{100} = T_o\left(-ln\frac{\gamma}{100}\right). \qquad (2.51)$$

Вираження (2.51) дозволяє зв'язати безвідмовність комплектуючих елементів об'єкту з його довговічністю. При $\gamma = 90\%$з вираження (2.34) випливає $T_{сл.\ \gamma} = 0{,}105T_o$.

Стосовно до відновлюваних об'єктів розрізняють також*середній термін служби до середнього (капітального) ремонту; середній термін служби між середніми (капітальними) ремонтами.*

Середній термін служби до середнього (капітального) ремонту $T_{ср.\ сл.\ ср\ (к.р)}$— середній строк служби від початку експлуатації об'єкта до його першого середнього (капітального) ремонту.

Значення цієї величини визначається на підставі статистичних даних експлуатації даної апаратури.

Середній термін служби між середніми (капітальними) ремонтами $T_{ср.\ сл.\ мр}$— середній строк служби між суміжними середніми (капітальними) ремонтами.

Його значення також визначається на підставі статистичних даних експлуатації апаратури.

Як ми вже відзначали, існує зв'язок між терміном служби складного об'єкта й довговічністю комплектуючих його елементів. Момент відмови об'єкта наступає тем раніше, чим менше довговічність комплектуючих елементів.

Ресурс; технічний ресурс – сумарний наробіток об’єкта від початку його експлуатації чи поновлення після ремонту до переходу в граничний стан.

Для відновлюваних і невідновлюваних об'єктів розрізняють *призначений ресурс*, *середній ресурс; гамма-відсотковий ресурс;середній повний ресурс.*

Призначений ресурс $R_н$— сумарний наробіток, при досягненні якого експлуатацію об’єкта належить припинити незалежно від його технічного стану.

Середній ресурс $R_{ср}$ — математичне сподівання ресурсу:

$$R_{ср} = \int_0^\infty r_i f(r)\,dr \qquad (2.52)$$

де r_i— ресурс роботи і-го елемента (об'єкта);

$f(r)$— функція щільності розподілу величини r .

Гамма-відсотковий ресурс R_γ— сумарний наробіток, протягом якої об’єкт не досягне граничного стану з імовірністю γ, вираженою у відсотках.

Для визначення відсоткового-гамма-процентного ресурсу можна скористатися вираженням (2.51), підставляючи замість функції розподілу терміну служби значення функції розподілу ресурсу

$$R_\gamma = -R_o\left(-ln\frac{\gamma}{100}\right). \qquad (2.53)$$

Крім розглянутих показників для відновлюваних об'єктів розрізняють*середній ресурс між середніми (капітальними) ремонтами, середній повний ресурс й середній ресурс до середнього (капітального) ремонту.*

Середній ресурс між середніми (капітальними) ремонтами $R_{ср.м.р}$— середній ресурс між суміжними середніми (капітальними; ремонтами. Його значення визначається, на підставі статистичних даних експлуатації апаратури.

Середній повний ресурс $R_{ср.\ п}$ — середній ресурс об'єкта від введення об'єкта в експлуатацію до повного зняття з експлуатації. Його значення визначається також на підставі статистичних даних експлуатації апаратури.

Середній ресурс до середнього (капітального) ремонту $R_{ср.с.р(к.р)}$— середній ресурс від початку експлуатації об'єкта до його першого середнього (капітального) ремонту, визначається на основі статистичних даних експлуатації, що цікавить апаратури.

2.4.6 Ремонтопридатність

Термін «ремонтопридатність» оцінює властивості об'єкта, пов'язані з підтримкою й відновленням його працездатності.

Під ремонтопридатністю розуміють властивість об'єкта бути пристосованим до підтримання та відновлення стану, в якому він здатний виконувати потрібні функції за допомогою технічного обслуговування та ремонту (§ 2.1)[6].

Технічне обслуговування передбачає сукупність технічних і організаційних заходів, що забезпечують підтримку об'єкта в працездатному стані на різних фазах і етапах експлуатації.

Під ремонтом розуміють організацію й виконання робіт по відбудові працездатності й ресурсу роботи об'єкта (елемента).

Слід підкреслити, що як відновлювані, так і невідновлювані об'єкти (елементи), підлягають технічному обслуговуванню для попередження й виявлення відмов.

Тому що поняття «ремонтопридатність» — якісна характеристика об'єкта, то для його кількісної оцінки застосовуються одиничні показники ремонтопридатності: *імовірність відновлення в заданий час і середній час відновлення.* Природно, що ці показники ставляться тільки до відновлюваних об'єктів.

Імовірність відновлення (M(t)),$P_в(t)$ — імовірність того, що час відновлення працездатного стану об’єкта не перевищить заданого значення. Математично це може бути записане у вигляді

$$P_в(t) = M(t \le t_в) \tag{2.54}$$

де $t_в$— час відновлення об'єкта.

Імовірність відновлення може розглядатися як функція розподілу випадкової величини $t_в$ часу відновлення об'єкта.

Для зручності математичного опису процесу відновлення введемо поняття Інтенсивність відновлення $\mu(t)$– умовна густина імовірності відновлення працездатності об’єкта, визначена для одного моменту часу, за умовою, що до цього моменту відновлення не завершилося.

Середня інтенсивність відновлення $\mu(t_1, t_2)$ – середнє значення інтенсивності відновлення в заданому інтервалі часу

$$\mu(t_1, t_2) = \frac{1}{t_2 - t_1}\int_{t_1}^{t_2} \mu(t)dt \tag{2.55}$$

Для простоти розгляду будемо вважатися, що час відновлення розподілений за експонентним законом. Ця умова саме по собі є твердим і в ряді випадків, що добре описують реальні процеси.

У випадку реалізації зазначеного умови $\mu(t) = \mu = const$будемо розглядати відновлення об'єкта в проміжку часу $t, t + \Delta t$.Імовірність цієї події може бути розглянута як імовірність реалізації двох неспільних подій: відновлення об'єкта до моменту t і відновлення об'єкта за проміжок часу $t + \Delta t$.У цьому випадку

$$P_в(t, t + \Delta t) = P_в(t) + [1 - P_в(t)]\mu\Delta t \tag{2.56}$$

Перейдемо до межі, одержуємо диференціальне рівняння першого порядку

$$\frac{dP_в(t)}{dt} = [1 - P_в(t)]dP \tag{2.57}$$

Рішення цього рівняння з урахуванням початкових умов $[t = 0, P(0) = 0]$ має вигляд

$$P_в(t) = 1 - e^{-\mu t} \tag{2.58}$$

Середня тривалість відновлення (MTTR) $T_{в.\,сер}$ — математичне сподівання часу відновлення працездатного стану об’єкта після відмови

Згідно з визначенням неважко записати

$$T_{в.\ ср} = M_в(t) = \int_0^\infty t f_в(t) dt \qquad (1.59)$$

де $f_в(t) = P'_в(t) = {dP_в(t)}/{dt}$ — щільність розподілу випадкової величини часу відновлення.

Для випадку експонентного розподілу часу відновлення

$$T_{в.\ ср} = \int_0^\infty t P'_в(t) dt = \int_0^\infty t\mu e^{-\mu t} dt = \frac{1}{\mu} \qquad (2.60)$$

Гамма-відсоткова тривалість відновлення $T_{в.\ \gamma}$ – інтервал часу, протягом якого відновлення працездатності об'єкта здійсниться зі імовірністю γ, вираженою у відсотках.

$$T_{в.\ \gamma} = -\frac{1}{\mu} \ln \frac{\gamma}{100} = T_{в.\ сер} \left(-ln \frac{\gamma}{100}\right) \qquad (2.61)$$

Середня трудомісткість технічного обслуговування [ремонту] $Н_{в.сер}$– математичне сподівання трудомісткості технічного обслуговування та (чи) ремонту, виражене в людиногодинах.

У ряді випадківексплуатації, особливо коли об'єкт ЕРВ по призначенню працює з перервами, можна вказати припустимий час простою для відшукання й усунення відмови $T_{п.\ д}$ виходячи з умов його застосування. Якщо задовольняється нерівність $T_{п.\ д} < T_{в.\ ср}$ те такий об'єкт не буде припиняти свого функціонування. Дійсно, якщо час простою для об'єктів дискретної ЕРВ менше часу між двома послідовними повідомленнями, те така апаратура буде функціонувати без перебоїв.

Звідси можна зробити вивід про те, що якщо замість елемента, що відмовив (при наявності достатньої їхньої кількості) можна встигнути із запасу включити новий, те не всі *можливі* n відмов будуть відмовами всього об'єкта.

У цьому випадку число відмов усього об'єкта буде характеризуватися вираженням

$$n(T_в > T_{п.\ д}) = n - nP_в(T_{п.\ д}) = n(1 - P_в(T_{п.\ д})) \qquad (2.62)$$

де n — загальне число відмов;

$P_в(T_{п.\ д}) = 1 - e^{-\mu T_{п.\ д}} = 1 - e^{-T_{п.\ д}/T_{в.\ сер}}$— імовірність відновлення об'єкта за час $T_{п.\ д}$.

Тоді середній наробіток до відмови T_0за припущенням, що

$\frac{T_{p\Sigma}}{n} = T_{сер} + T_{в.\ сер}$визначається вираженням:

$$T_0 = \frac{T_{p\Sigma}}{n(T_в > T_{п.\ д})} = \frac{T_{p\Sigma}}{n(1-P_в(T_{п.\ д}))} = \frac{T_{p\Sigma}/n}{(1-P_в(T_{п.\ д}))} = \frac{T_{сер}+T_{в.\ сер}}{(1-P_в(T_{п.\ д}))}.$$

(2.63)

де $T_{p\Sigma}$ — сумарний час роботи об'єкта;

$T_{в.\ сер}$ – середня тривалість відновлення;

$T_{сер}$ -середній наробіток між відмовами (середній наробіток на відмову).

Вираження для імовірності безвідмовної роботи за умов, що t=$T_{п.\ д}$,$T_{п.\ д} < T_{в.\ сер}$,прийме вид

$$P(t) = P(P_в, \alpha, \beta) = e^{-\frac{t}{T_0}} = e^{-\frac{[1-P_в(T_{п.\ д})]}{T_{сер}+T_{в.\ сер}}T_{п.\ д}} = e^{-\frac{(1-P_в(T_{п.\ д}))T_{п.\ д}}{(\frac{T_{сер}}{T_{в.ср}}+1)T_{в.ср}}} = e^{-(1-P_в(T_{п.\ д}))\frac{\alpha}{(\beta+1)}}$$

(2.64)

де $\alpha = \frac{T_{п.\ д}}{T_{в.\ сер}}$ – співвідношення припустимого часу простою для відшукання й усунення відмови до середньої тривалості відновлення $T_{в.\ ср}$.;

$\beta = \frac{T_{сер}}{T_{в.\ сер}}$ – співвідношення середнього наробітку на відмову $T_{сер}$ до середньої тривалості відновлення $T_{в.\ ср}$.

З виразу (2.64) випливає, що якщо значення $P_в(T_{п.\ д})$ досить велике, то може бути досягнутий значний виграш в імовірності безвідмовної роботи об'єкта.

Отже, ремонтопридатність об'єкта може прямо впливати на його безвідмовність і може її для ряду об'єктів ЕРВ ефективно підвищувати (при досить більших значеннях $P_в(T_{п.\ д})$. Це наочно показане на рис. 2.29.

При зменшені співвідношення $\alpha = \frac{T_{п.\ д}}{T_{в.\ сер}}$ на рис. 2.29 спостерігається значне підвищення імовірності безвідмовної роботи $P(P_в, \alpha, \beta)$.

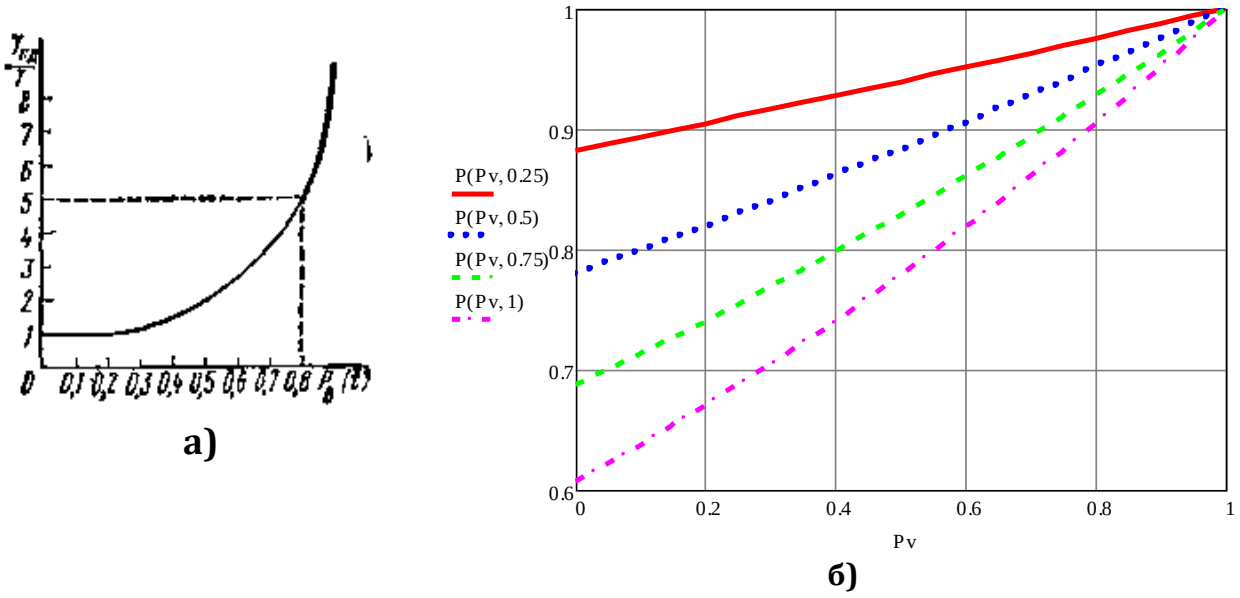
В свою чергу імовірність відновлення в значній мірі також залежить від співвідношення припустимого часу простою до середнього часу відновлення $\alpha = \frac{T_{п.\ д}}{T_{в.\ сер}}$.

Перетворимо вираження (2.64) з урахуванням (2.58, 2.60) до наступного виду за умов, що $t = T_{п.\ д}$,$T_{п.\ д} < T_{в.\ сер}$, отримаємо

$$P(t, \alpha, \beta) = P(\alpha, \beta) = e^{-(1-(1-e^{-\mu t}))\frac{\alpha}{(\beta+1)}} = e^{-(e^{-\frac{T_{п.\ д}}{T_{в.\ сер}}})\frac{\alpha}{(\beta+1)}} = e^{-(e^{-\alpha})\cdot\frac{\alpha}{(\beta+1)}}$$

(2.65)

Графіки імовірності безвідмовної роботи $P(\alpha, \beta)$ наведені на рис. 2.30



а)

б)

Рис. 2.29 – Аналітична залежність виграшу в надійності відновлюваного об'єкта від імовірності відновлення а) та розрахункові графіки залежності імовірності безвідмовної роботи $P(P_в, \alpha, \beta)$відімовірності відновлення $P_в$. *б)* при $\alpha = \frac{T_{п.\,д}}{T_{в.\,сер}} = 0,25; 0.5; 0.75; 1; \beta = 1$

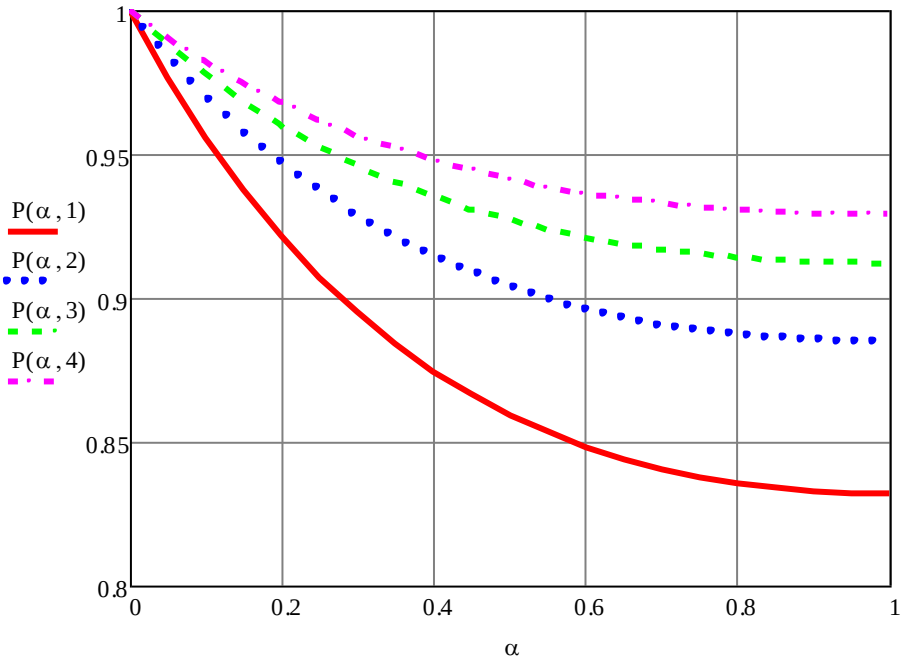


Рис. 2.30 – Розрахункові графіки залежності імовірності безвідмовної роботи $P(\alpha, \beta)$. при $\alpha = \frac{T_{п.\,д}}{T_{в.\,сер}} = 0 \div 1; \beta = \frac{T_{сер}}{T_{в.\,сер}} = 1; 2; 3; 4$

На графіку рис. 2.30 помитне, що чим більш співвідношення $\beta = \frac{T_{сер}}{T_{в.\,сер}} \geq 1$тим більш імовірності безвідмовної роботи $P(\alpha, \beta)$, тобто висока надійність об'єкту може бути досягнута при умові $T_{сер} \gg T_{в.\,сер}$.

При малих значеннях співвідношення $\alpha = \frac{T_{п.\ д}}{T_{в.\ сер}}$ на рис. 2.21 спостерігається також значне підвищення імовірності безвідмовної роботи $P(\alpha, \beta)$.

На величину співвідношення $\alpha = \frac{T_{п.\ д}}{T_{в.\ сер}}$ значний вплив виявляють конструктивні характеристики об'єктів ЕРВ й кваліфікація обслуговуючого персоналу.

Отже, ремонтопридатність об'єкта значною мірою визначається заходами, передбаченими й проведеними при його проектуванні й виготовленні.

Чималий вплив на ремонтопридатність виявляє також експлуатація об'єкта, тому що в цей період діють такі фактори, як організація технічного обслуговування й відновлення, підготовка операторів, постачання запасними елементами й т.п.

Дослідження останніх років показали, що, незважаючи на велику різноманітність об'єктів ЕРВ, є багато загальних закономірностей в організації технічного обслуговування й відновлення, що дозволяють використовувати загальну методику підходу до її вирішення.

Організація експлуатації ЕРВ, відновлення й ремонту повинна ґрунтуватися на виводах і рекомендаціях теорії експлуатації.

2.4.7.Збережуваність

Немаловажним, особливо для об'єктів із тривалими строками зберігання, є властивість об'єкта зберігати на етапах зберігання й транспортування свої задані експлуатаційні властивості. Ці властивості об'єкта визначаються поняттям «збережуваність».

З б е р е ж у в а н і с т ь – властивість об’єкта зберігати в заданих межах значення параметрів, що характеризують здатність об’єкта виконувати потрібні функції, під час і після зберігання та (чи) транспортування(§ 2.8) [6].

Слід зазначити, що згідно з визначенням збережуваність може розглядатися як специфічний випадок безвідмовності, розповсюджуваний тільки на етапи зберігання й транспортування. Це викликане значною питомою вагою цих етапів в експлуатації об'єктів ЕРВ.

У якості одиничних показників, що дозволяють кількісно визначити збережуваність, використовують *середній термін збережуваності* й *гамма-відсотковий термін збережуваності*.

С е р е д н і й т е р м і н з б е р е ж у в а н о с т і $T_{зб.\ ср}$ — математичне сподівання строку збережуваності

$$T_{зб.\ ср} = \int_0^\infty t_{збі}\, f(t_{зб}) t \qquad (2.66)$$

де $t_{збі}$ — збережуваність і – го об'єкта (елемента);

$f(t_{зб})$– функція густини розподілу величини $t_{зб}$.

Гамма-відсотковий термін збережуваності $T_{зб.\ \gamma}$ — термін збережуваності, що його досягає об'єкт із заданою імовірністю γ, вираженою у відсотках.

Гамма-відсотковий термін збережуваності може бути визначений вираженням (2.51), якщо підставити замість функції розподілу терміну служби значення функції розподілу терміну зберігання.

$$T_{зб.\ \gamma} = -\frac{1}{\lambda_{зб}} \ln \frac{\gamma}{100} = T_{зб.\ ср} \left(-ln \frac{\gamma}{100}\right) \tag{2.67}$$

Аналітично показники збережуваності можна розрахувати, використовуючи вираження (2.32) (при експонентному розподілі часу безвідмовної роботи елементів) і підставляючи в нього значення λ – показників елементів для етапів зберігання$\lambda_{зб}$ й транспортування λ_m.

2.4 8Комплексні показники надійності

У ряді випадків для оцінки експлуатаційних якостей об'єкта одиничних показників надійності буває недостатньо. Виникає необхідність у більш складних показниках, які ставилися б відразу до декільком властивостям, що становлять надійність об'єкта. Такі показники називають комплексними показниками надійності.

До них ставляться*: коефіцієнт готовності, коефіцієнт неготовності (коефіцієнт простою), коефіцієнт технічного використання, коефіцієнт оперативної готовності й коефіцієнт збереження ефективності.*

Коефіцієнт готовності (A(t))$K_Г(t)$ — імовірність того, що об'єкт виявиться працездатним у довільний момент часу, крім запланованих періодів, протягом яких використання об'єкта за призначенням не передбачено.

$$K_г(t) = \frac{\mu(t)}{\lambda(t)+\mu(t)} \tag{2.68}$$

Середній коефіцієнт готовності (A(t_1,t_2)) $K_Г(t_1,t_2)$– середнє значення нестаціонарного коефіцієнта готовності у заданому інтервалі часу

$$K_г(t_1, t_2) = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} K_г(t)dt \tag{2.69}$$

Якщо прийняти найпростішу систему експлуатації об'єкта робота – відновлення (негайний початок) — робота, то можливо застосовувати стаціонарний коефіцієнт готовності (A) $K_Г$ – значення коефіцієнта готовності, визначене для умов роботи об'єкта, коли серед-

ній параметр потоку відмов і середня тривалість відновлення залишаються сталими, тоді можна записати

$$K_г = \frac{\mu}{\lambda+\mu} = \frac{T}{T+T_в} \tag{2.70}$$

де $T = T_{сер} = \frac{1}{\lambda}$ — середній наробіток на відмову;

$T_в = T_{в.\ сер} = \frac{1}{\mu}$ — середня тривалість відновлення.

За статистичним даними експлуатації коефіцієнт готовності об'єкта визначається як відношення сумарного часу перебування спостережуваного об'єкта в працездатному стані $T_{пр.\ ст.\Sigma}$до всього часу його експлуатації $T_{p\Sigma}$.

$$K_{г\ стат.} = \frac{T_{пр.\ ст.\Sigma}}{T_{p\Sigma}} \tag{2.71}$$

Коефіцієнт готовності може бути визначений як для одиночного об'єкта, так і для групи об'єктів.

З наведеного вираження випливає, що побільшати значення коефіцієнта можна, збільшуючи безвідмовність об'єкта або ж усіляко скорочуючи час відновлення.

К о е ф і ц і є н т н е г о т о в н о с т і ; к о е ф і ц і є н т п р о с т о ю U (t) $K_П(t)$– імовірність того, що об’єкт виявиться непрацездатним у довільний момент часу, крім запланованих періодів, протягом яких використання об’єкта за призначенням не передбачено. Кількісна оцінка «коефіцієнта неготовності» є доповненням до 1 «коефіцієнта готовності» оскілки коефіцієнти готовності й простою є ймовірностями протилежних випадкових подій:

$$K_г(t) + K_П(t) = 1 \implies K_П(t) = 1 - K_г(t) = \frac{\lambda(t)}{\lambda(t)+\mu(t)} \tag{2.72}$$

Дозволяється [6] використовувати показник, аналогічний «коефіцієнтові неготовності», визначений як доповненні до 1 «середнього коефіцієнта готовності» чи «стаціонарного, коефіцієнта готовності», який має назву відповідно «середній коефіцієнт неготовності (простою)» чи «стаціонарний коефіцієнт неготовності (простою)». Згідно формул (2.68 – 2.70) отримаємо:

$$K_п(t_1, t_2) = 1 - K_г(t_1, t_2) = 1 - \int_{t_1}^{t_2} K_г(t)dt$$

$$K_п = 1 - K_г = 1 - \frac{\mu}{\lambda+\mu} = 1 - \frac{T}{T+T_в} = \frac{T_в}{T+T_в} \qquad (2.73)$$

де $K_п(t_1, t_2)$ – середній коефіцієнт неготовності (простою);

$K_п$ – стаціонарний коефіцієнт неготовності (простою);

Режим очікування являє собою режим експлуатації, коли об'єкт перебуває в стані повної або полегшеного навантаження чекаючи виконання своїх функцій по призначенню. Необхідність використання виникає раптово, після чого об'єкт безвідмовно функціонує протягом часу $t_р$. Для виконання завдання в момент вступу вимоги об'єкт повинен бути працездатним. Отже, у режимі очікування можлива поява відмов і виникає необхідність його відновлення. Для оцінки надійності об'єктів подібного типу використовується комплексний показник — коефіцієнт оперативної готовності.

Коефіцієнт оперативної готовності $K_{ог}$ — імовірність того, що за винятком тих запланованих періоді», протягом яких використання об’єкта за призначенням не передбачено, він у довільний момент часу виявиться у працездатному стані і надалі протягом заданого інтервалу часу.

Якщо відома ймовірність безвідмовної роботи об'єкта за час $t_р$і вона не залежить від моменту вступу вимоги, то можна записати

$$K_{ог} = K_г P(t_р) \qquad (2.74)$$

Коефіцієнт збереження ефективності $K_{зб\,еф.}$ – відношення значення показника ефективності використання об’єкта за призначенням за певну тривалість експлуатації до номінального значення цього показника, розрахованого за умови, що відмови об’єкта протягом того ж періоду не виникають

$$K_{зб\,еф.} = \frac{E_{експл.}}{E_н} \qquad (2.75)$$

Коефіцієнт технічного використання $K_{т\,в}$— відношення математичного сподівання сумарного часу перебування об’єкта у працездатному стані за деякий період експлуатації $T_{пр.\ ст.\Sigma}$до математичного сподівання сумарного часу перебування об’єкта в працездатному стані та у простоях, зумовлених технічним, обслуговуванням $T_{то\,\Sigma}$і ремонтом $T_{рем\,\Sigma}$за той самий період.

$$K_{т\,в} = \frac{T_{пр.\ ст.\Sigma}}{T_{пр.\ ст.\Sigma}+T_{то\,\Sigma}+T_{рем\,\Sigma}} \qquad (2.76)$$

Важливим для оцінки умов експлуатації об'єкта є коефіцієнт навантаження, що дозволяє враховувати вплив різних факторів на об'єкт у період його експлуатації.

К о е ф і ц і є н т н а в а н т а ж е н н я $K_н$ — відношення реального робочого навантаження, що діє на об'єкт (елемент) у даних умовах, до номінального навантаження, передбаченого для даного об'єкта (елемента) у заданих умовах експлуатації:

$$K_н = \frac{H_p}{H_н} \tag{2.77}$$

де H_p — реальне навантаження, $H_н$ — номінальне навантаження.

У цьому випадку поняття навантаження має самий широкий зміст: теплове навантаження, електричне навантаження, механічне навантаження й т.п.

Розглянуті комплексні показники надійності визначаються на підставі статистичних даних експлуатації, що цікавлять об'єктів *відразу* на підставі даних спеціально проведених експериментів із цими об'єктами.

Методика визначення й оцінки їх статистичних значень викладені в гл. IV.

Крім розглянутих у ряді випадків ухвалюють і інші комплексні показники надійності. Наприклад, для оцінки вартості експлуатації: вартість технічного обслуговування, вартість ремонтів і т.п. Про їхнє застосування й способах визначення буде сказано в наступних главах.

На закінчення відзначимо, що в літературі з питань експлуатації й надійності також широко використовують замість термінів «об'єкт» і «елемент» терміни «устаткування» і «апаратура». Надалі при розгляді експлуатації реальних об'єктів ЕРВ в книзі використані й ці терміни.

Крім коефіцієнта технічного використання для оцінки трудомісткості технічного обслуговування також використовують і інші показники.

С е р е д н я с у м а р н а т р у д о м і с т к і с т ь т е х н і ч н о г о о б с л у г о в у в а н н я — математичне очікування сумарних працезатрат на проведення технічного обслуговування об'єкта (елемента) за певний період експлуатації.

Відношення цього показника до математичного очікування сумарної наробітку об'єкта (елемента) за той же період експлуатації називають п и т о м о ю с у м а р н о ю т р у д о м і с т к і с т ю т е х н і ч н о г о о б с л у г о в у в а н н я.

Для оцінки трудомісткості ремонтів використовують д і а л о г і ч н и й п о к а з н и к — середню сумарну трудомісткість ремонтів, розуміючи під цим математичне очікування сумарних працезатрат на всі види ремонтів об'єкта (елемента) за певний період експлуатації. Відношення цього показника до математичного очікування сумарного наробі-

тку об'єкта (елемента) за той же період експлуатації називають питомою сумарною трудомісткістю ремонтів.

Для ряду об'єктів ЕРВ характерними є тривалі періоди очікування використання по призначенню (наприклад, телефонний апарат в абонента АТС).

2.4.9 Вплив різних факторів на показники надійності

У процесі виробництва й експлуатації на ЕРВ діє безліч різних факторів, що впливають на її надійність. Їхній вплив на складові надійності і їх показники по-різному. В табл. 2.5 наведена класифікація цих факторів.

Усі фактори можна підрозділити так дві групи: *об'єктивні фактори* й *суб'єктивні фактори.*

До групи об'єктивних факторів ставляться *експлуатаційніклімати-чні й біологічні*.

До групи суб'єктивних факторів ставляться помилки людей при *розробці, виробництва й експлуатації.* До факторів, що визначають надійність ЕРВ на етапах розробки й виробництва, ставляться: вибір схемних рішень, вибір елементів і режим їх роботи, вибір конструктивних рішень, вибір і дотримання технології виробництва, автоматизація виробництва, тренування елементів і апаратури, контроль якості й т.п. Усі перераховані фактори значно впливають на надійність ЕРВ, що надходить в експлуатацію. Про цей досить докладно викладене в літературі [8].

Надалі зупинимося більш докладно на об'єктивні й деяких суб'єктивних факторах, що впливають на надійність ЕРВ в процесі її експлуатації, тому що на їхню частку доводиться більш 30% від усіх відмов. До них ставляться: час експлуатації, електричні режими, температура середовища, вологість і атмосферні опади, знижений тиск, сонячні й інші види радіації і різного роду домішки в повітрі, механічні навантаження (перевантаження, удари й вібрації), біологічні фактори (грибки, цвіль, комахи й гризуни), діяльність обслуговуючого персоналу (кваліфікація, проведення профілактичних заходів, організація експлуатації, наявність інструкцій для експлуатації даного типу апаратури) і т. п.

Час експлуатації. Час експлуатації є одним з основних факторів, що визначають надійність апаратури на всіх етапах.

На рис. 2.5 показана залежність інтенсивності відмов від часу експлуатації апаратури Технологічні й конструктивні недоліки найчастіше виявляються в перший період експлуатації, коли інтенсивність відмов у багато разів більше, чим у нормальний період експлуатації; так, наприклад, для електронних ламп вона в 2-5 раз вище. Вихід з ладу конденсаторів у більшості випадків відбувається через пробій діелектрика в результаті чого до 70% усіх вийшовших з ладу конденсаторів припадає на цей період експлуатації.

Таблиця 2.5 – Класифікація факторів, що впливають на показники надійності

ФАКТОРИ, ЯКІ ВПЛИВАЮТЬ НА НАДІЙНІСТЬ					
об'єктивні			суб'єктивні		
експлуатаційні	**кліматичні**	**біологічні**	**при розробці**	**при виробництві**	**при експлуатації**
час експлуатації	вологість і атмосферні опади	грибки	вибір схемних рішень	вибір технології та її дотримання	кваліфікація операторів
температурні режими	температура середовища	цвіль	вибір конструкційних рішень	тренування елементів й апаратури	опис, інструкцій для експлуатації
електричні режими, електростатичні заряди	блискавки, електромагнітні імпульси	комахи	вибір елементної бази	ступінь автоматизації виробництва	організація експлуатації
механічне навантаження	знижений тиск	гризуни	вибір режимів роботи	контроль якості	проведення профілактичних заходів
штучна ядерна радіація.	сонячні й природня радіація	домашні тварини			
агресивні речовини і середовища	хімічні домішки в повітрі				
велика концентрація пилу	механічні домішки в повітрі				

Таким чином, у період приробляння виявляються багато явні й приховані дефекти апаратури в цілому і її елементів. У цей же період здійснюється вихідний контроль ЕРВ на її виробництві, що виготовляє.

Тривалість цього періоду для різної апаратури може коливатися від декількох десятків до сотень годин (від 1 до 15% від тривалості періоду нормальної експлуатації). Найбільш важливу апаратуру прийнято піддавати попередньому тренуванню протягом певного часу для того, щоб ще до експлуатації в споживача вона виробила час приробляння й ненадійні елементи й вузли були б вчасно усунуті. Це пов'язане з витратою певного ресурсу роботи апаратури, але зате зменшує кількість відмов, що доводяться на етап використання по призначенню. Як ми вже відзначали, для періоду нормальної експлуатації слушний експонентний закон надійності.

Після досить тривалої експлуатації апаратури наступає останній, третій період, який характеризується значним зростанням інтенсивності відмов через старіння й зношування елементів. Цей період для ЕРВ наступає після декількох сотень або тисяч годин роботи. Зростання інтенсивності відмов пояснюється необоротними змінами параметрів і характеристик елементів.

Процеси старіння йдуть безупинно, але можуть прискорюватися під впливом різних факторів (тепло, волога, світло, тиск і т.п.).

Причиною старіння є складні фізико-хімічні процеси, що відбуваються в елементах апаратури протягом усього часу її експлуатації. До них ставляться: структурні зміни в діелектриках і провідниках, окиснення поверхонь провідників, хімічні перетворення в єднальних і просочувальних матеріалах, порушення електричної й механічної міцності матеріалів, діелектрика й елементів конструкції, порушення герметизації внаслідок появи тріщин і наскрізних каналів, підвищення водопроникності матеріалів і т.п.

Структурні зміни полягають у тому, що із часом відбувається кристалізація провідного шару в резисторів, що неминуче спричиняє зміна величини його опору. У полімерах структурні зміни приводять до появи тріщин, ламкості ізоляції і т.д.

Сорбція (поглинання) газів і пар води навколишнього середовища обумовлює зміна механічних і електричних властивостей пластмас, каучуку, що проводить шару більшості плівкових резисторів (ВР, МЛТ, УЛМ і т.д.), поверхонь контактів, руйнування сполучного матеріалу об'ємних резисторів і т.п.

З метою затримки процесу старіння широко застосовують герметизацію елементів або цілих вузлів. Наприклад, її успішно використовують при виготовленні конденсаторів. Так, для паперових герметизованих конденсаторів зниження опору ізоляції до 25% від первісного значення відбувається тільки після 5000 год. роботи. Особливо показовий вплив герметизації для електролітичних конденсаторів, у яких значно вповільнене старіння в перші 3000-4000 год. роботи (до порушення герметизації), після чого його характеристики різко погіршуються [8].

Найбільше швидко старіють деталі пластмасові із пресованого порошку (каркаси котушок, корпуси перемикачів і т.п.). У змінних резисторів старіння полягає в зміні опору провідного шару і його стирання, порушенні контакту між провідним шаром і движком. Монтажні проведення робляться непридатним через висихання й розтріскування ізоляції. Швидко старіє пластмасове кріплення, армований металом.

На механічні й електромеханічні елементи й вузли більший вплив, чому старіння, виявляє зношування (редуктори, сельсини, реле, підшипники й т.п.).

Швидкість старіння також визначається режимами роботи й інтенсивністю впливу інших факторів, у ряді випадків суттєво прискорювальні цей процес.

Вибір технології та її дотримання, Ступінь автоматизації виробництва Тренування елементів й апаратури, контроль якості.

Електричні режими. Зміни електричних режимів роботи радіотехнічних елементів впливають на стабільність і довговічність їх характе-

ристик і параметрів і, отже, на довговічність і надійність усієї системи або об'єкта.

Усі елементи характеризуються припустимими навантаженнями по потужності розсіювання, струмам, напругам і т.п.. Отже, робота елементів при гранично припустимих навантаженнях скорочує їхній термін служби й не гарантує надійної роботи. Зменшення фактичних навантажень збільшує надійність роботи.

Про величину реального навантаження судять за статистичним даними експлуатації й вимірам режимів роботи елементів. Для оцінки режиму роботи використовують *коефіцієнти навантаження* (див вираження (2.78) *по потужності й по напрузі.*

Коефіцієнт навантаження по потужності

$$K_{нР} = \frac{P_р}{P_н} \tag{2.78}$$

де $P_р$ —робоче значення потужності розсіювання;

$P_н$— номінальне значення потужності розсіювання.

Коефіцієнт навантаження по потужності використовують для оцінки режимів роботи резисторів і ламп. В останньому випадку вираження (2.51) прийме вид

$$K_{нР} = \frac{P_а+P_н+\Sigma P_с}{P_{н.\ н}+P_{н.\ а}} \tag{2.79}$$

де $P_а$, $P_с$, $P_н$ — робочі значення потужності, що розсіюється анодом, сітками й ниткою розжарення; $P_{н.\ н}$ — номінальне значення потужності розжарення,

$P_{н.\ а}$ -номінальне значення потужності в ланцюзі анода.

Коефіцієнт навантаження по напрузі

$$K_{нU} = \frac{U_р}{U_н} \tag{2.80}$$

де $U_р$ — робоче значення напруги;

$U_н$— номінальне значення напруги.

Коефіцієнт навантаження по напрузі використовують для оцінки режиму роботи різних конденсаторів, ізоляторів і т.п.

Вплив електричних навантажень головним чином зводиться до погіршення температурного режиму й появі перенапруги, що може викликати пробій ізоляції.

Як той, так і інший фактори приводять до зниження надійності, появі передчасних відмов. Електричні режими також впливають на залежність надійності від числа включень, тому що сприяють виникненню перенапруг при включеннях.

Елементи, що працюють у ЕРВ, повинні мати відповідний запас електричної міцності, обумовлений прийнятим значенням коефіцієнта навантаження.

Чим нижче значення коефіцієнта електричного навантаження, тем надійніше буде працювати елемент, однак значне його заниження спричиняє збільшення ваги, габаритів, вартості елементів і в цілому всієї апаратури. При проектуванні звичайно ухвалюють коефіцієнт електричного навантаження радіотехнічних елементів порядку 0,4-0,6.

Температура навколишнього середовища. ЕРВ експлуатують у різних температурних умовах. Температурний вплив тим більше, чим більше швидкість і частота зміни температури. Найбільш важкими є польові умови роботи апаратури, робота ЕРВ в космічних апаратах, ракетах і літаках. У табл. 2.6 наведені сезонні й добові коливання температури на території СНД [8].

Таблиця 2.6 – Сезонні й добові коливання температури на території СНД

Найменування області	**Сезонні коливання температури °С**	**Добові коливання температури, °С**
Пустеля	$(-10) \div (+50)$	40
Помірний пояс	$(-20) \div (+40)$	25
Арктична зона	$(-50) \div (+35)$	20

Температура навколишнього середовища суттєво впливає на температуру усередині апаратури й температуру окремих елементів. Так, в апаратурі, що перебуває під прямим впливом сонячних променів, при темному фарбуванні поверхні можливе підвищення температури на 35° С и більш. Тому що температура елемента визначається власним нагріванням і температурою середовища, то таке збільшення температури середовища приведе до підвищення температури елемента. Отже, фактичне значення коефіцієнта навантаження виявиться вище розрахункового. Цей фактор особливо важливе значення набуває для супутників землі й космічних апаратів, у яких сторона, звернена до сонця досить інтенсивне нагріта, а тіньова сторона холодна.

Немаловажним фактором, що впливають на надійність, є швидкість і циклічність зміни температури в апаратурі. Ці фактори приводять до появи механічних знакозмінних зусиль і, як наслідок, до ослаблення механічних кріплень, появі втомлених тріщин, відпріванню й т.п.

Так, для авіаційної ЕРВ різниця температур може досягати 80° С, зі швидкістю зміни до 50° С у хвилину, а для бортового встаткування ракет і того більш.

При низьких температурах пластмаси втрачають міцність, гумові вироби стають тендітними й розтріскуються, метали робляться ламкими. У тріщини, що утворювалися, ізоляції попадає волога, знижуючи її електричну міцність. При низьких температурах легко руйнуються з'єд-

нання пластмас із металами, спаї металів зі склом, порушується пайка, регулювання зазорів, падає ємність електричних конденсаторів і т.п.

Підвищена температура сприяє прискоренню розпаду органічних ізоляційних матеріалів, перегріву й виходу з ладу напівпровідникових приладів, прискореному старінню ламп. Слід ураховувати, що невагомість у космосі може привести до погіршення дії системи примусового охолодження й до перегріву ЕРВ. Високі температури погіршують ізоляційні властивості різного роду заливань, обмоток, механічні властивості більшості полімерів, що приводить до деформації деталей і виходу їх з ладу або ж появі необоротних змін" параметрів.

Періодичні зміни низьких і високих температур особливо швидко приводять до руйнування різного роду обмоток.

Вплив температури на інтенсивність відмов ЕРВ прийнято оцінювати температурним коефіцієнтом інтенсивності відмов

$$K_t = \left(\frac{t_p}{t_н}\right)^a \qquad (2.81)$$

де t_p — робоча температура елемента; $t_н$ — номінальна температура елемента; a — показник ступеня, обумовлений типом елемента.

ЕРВ, установлена на космічних апаратах, зазнає впливу теплових потоків випромінювання Сонця, Землі, планет, відбитого від землі випромінювання, а також нагріванню за рахунок потоків мікрометеорів і заряджених часток. Величина температури поверхні в сильному ступені залежить від стану поверхні і якості покриття ЕРВ, що перебуває на зовнішній поверхні.

Вологість і атмосферні опади. Вологість є одним з найбільше сильно Діючих факторів. Вологість навколишнього повітря прийнято оцінювати відносною вологістю, що представляє собою вимірюване у відсотках відношення вологи, що фактично втримується в повітрі, до максимально можливого її змісту при даній температурі. Нормальною вологістю вважається відносна вологість 60-65%. При вологості в 80% повітря вважається сирим.

Для багатьох тропічних районів характерна підвищена вологість (90—98%), супроводжувана високими температурами (35—40°С).

Тому елементи й ЕРВ, призначені для роботи в тропіках, повинні нормально функціонувати в умовах температури 40° С и вологості 98%.

Вплив вологи й атмосферних опадів на ЕРВ можливо в наступних умовах:

а) поглинання водяних пар з повітря;

б) конденсації водяних пар на поверхні апаратури або в повітрі (туман);

в) змочування бризами води (дощ, сніг);

г) занурення у воду.

Слід зазначити, що завдяки досить малому ефективному діаметру молекули води (2,58А) вона активно взаємодіє з матеріалами, застосовуваними в ЕРВ.

Здатність матеріалу адсорбувати воду в сильному ступені залежить від мікрорельєфу поверхні й структури матеріалу. Так, діелектрики із шорсткуватою поверхнею здатні адсорбувати вологи більше ніж із гладкою поверхнею.

Матеріали, що не поглинають воду (стекло, кераміка) можуть утворювати плівку вологи на поверхні вже при 30% вологості, що приводить до зниження їх поверхневого опору.

У пористих неорганічних діелектриках (слабко відпалена кераміка) відбувається полімолекулярна конденсація пар води в порах матеріалу, а при більших розмірах пор відбувається капілярна конденсація води із заповненням усіх капілярів водою.

У неорганічних діелектриках має місце неактивована сорбція вологи.

У випадку органічних діелектриків має місце процес обмеженого розчинення води в матеріалі з можливим його набряканням. Молекули води в результаті коливань молекул матеріалу впроваджуються усе глибше в товщу матеріалу. Ступінь проникнення вологи визначається щільністю макромолекул матеріалу і його станом.

Крім розглянутих сорбційних зв'язків води з матеріалом можливий і хімічний зв'язок. На відміну від сорбційної зв'язки, де вода не викликає необоротних змін матеріалу, при хімічному зв'язку вона входить у структуру матеріалу, приводить до одержання нових речовин, до перестройки кристалічних ґрат.

У деяких типах діелектриків (папір, ефіри, целюлоза й ін.) вода зв'язується з матеріалом водневими зв'язками.

Таким чином, поглинаючи воду, діелектрики погіршують свої електричні характеристики: падають питомі об'ємний і поверхневий опір, зменшується електрична міцність. Усі ці фактори приводять до зміни фактично діючого коефіцієнта % навантаження й зниженню надійності.

Те саме кількість вологи по-різному впливає на різні матеріали. Одні матеріали різко й швидко погіршують свої властивості, а інші порівняно мало й повільно. Визначальним фактором погіршення характеристик є не кількість поглиненої вологи, а її розподіл у матеріалі, що обумовлене фізико-хімічною структурою матеріалу.

Ефект впливу вологи може збільшуватися за рахунок дефектів поверхні елементів; появи тріщини у покритті, порушення герметизації й т.п. Зміна характеристик діелектриків добре ілюструє табл. 2.7.

Таблиця. 2.7 – Характеристики діелектриківпри вологості

Матеріали	ρ_0, Ом, при вологості		ρ_s,Ом при вологості	
	30% |	100%	0%	98%
Слюда мусковіт	$1{,}05 \cdot 10^{10}$	$1{,}1 \cdot 10^{7}$	$2{,}0 \cdot 10^{14}$	$5{,}0 \cdot 10^{9}$
Скло лужне	—	—	$3{,}0 \cdot 10^{14}$	$5{,}0\ 10^{9}$
Ультрафарфор (чистий)	—	—	$1{,}2\ 10^{18}$	$1{,}0\ 10^{13}$
Полістирол	—	—	$5{,}0\ 10^{17}$	$2{,}8\ 10^{15}$
Фторопласт-4	—	—	$5{,}0 \cdot 10^{17}$	$5{,}0\ 10^{17}$
Поліхлорвініл	—	—	$1{,}3\ 10^{17}$	$4{,}2\ 10^{14}$
Амінопласт	—	—	$2{,}1\ 10^{14}$	$3{,}8\ 10^{13}$
Поліуретан	—	—	$5{,}0\ 10^{16}$	$7{,}0\ 10^{14}$
Поліхлорвініл	—	—	$6{,}6\ 10^{14}$	$3{,}0\ 10^{14}$

При добових змінах температури відбувається часткова конденсація вологи в апаратурі, що погіршує умови її роботи. волога, що конденсувався, заповнює всі тріщини й нещільності в ізоляторах і покриттях, погіршуючи їх ізоляційні властивості, збільшує втрати енергії у хвилеводах, знижуючи чутливість прийомних пристроїв, погіршуючи стабільність частоти гетеродинів, знижуючи к. п. буд. передавачів і приводячи до загального порушення режимів роботи апаратури.

Вплив вологості прискорює руйнування лакофарбових захисних покриттів, порушує герметизацію й заливання.

Найбільше сильно від вологи страждають негерметизовані конденсатори. У конденсаторах типу КСО волога поступово проникає в місця розташування дротових виводів і знижує ізоляційні властивості слюди. У добре герметизованому конденсатори волога безпосередньо не проникає, але різко знижує поверхневий опір ізоляції й приводить до руйнування виводів.

Значна вологість збільшує втрати в контурних котушках, проникаючи в негерметизованих дроселі й трансформатори, і може привести до пробою. Тому найбільш важливі елементи апаратури герметизуються або заливаються епоксидною смолою.

Підвищена вологість також руйнує структуру резисторів, збільшуючи дійсне значення опору, і різко знижує їхня стійкість.

Вплив вологи на елементи ЕРВ при зберіганні, як правило, оборотне, але при проходженні через них токи, що мають місце фізико-хімічні процеси стають необоротними. Особливо сильно це позначається на тонкоплівкових резисторах.

Волога також впливає й на інші елементи ЕРВ, погіршує їх характеристики: окиснює контакти, зменшуючи опір між виводами, приводячи до корозії металевих частин конструкції.

Слід зазначити, що крім прямого впливу на електричні параметри елементів волога при циклічній зміні позитивних і негативних температур, проникаючи в тріщини й ушкоджуючи герметизацію, сприяє їхньому механічному ушкодженню.

Таким чином, підвищена вологість сильно знижує надійність ЕРВ, погіршуючи її експлуатацію.

Атмосферні опади сприяють зростанню вологості з усіма наслідками, що випливають. Особливо слід указати на такі види атмосферних опадів, як зледеніння й сніг. Зледеніння впливає на зовнішні елементи ЕРВ, приводячи до погіршення роботи всієї апаратури, а в ряді випадків і її (механічному) руйнуванню. Сніг небезпечний особливо в арктичних умовах, коли в результаті вітру він забивається в усі щілини, під чохли, у фільтри й т.п., що неминуче приводить до погіршення роботи апаратури або до її відмови.

Знижений тиск. Вплив зниженого тиску в основному поширюється на апаратуру, використовувану в літаках, вертольотах, космічних апаратах, ракетах, а також у гірській місцевості на висоті понад 1000 м.

Величина атмосферного тиску залежить від висоти підйому температури й ширини місцевості. Залежність атмосферного тиску від висоти представлена в табл. 2.8.

Зниження тиску на ЕРВ виявляє двоякий вплив: безпосередньо змінює електричні характеристики й побічно погіршує умови охолодження.

Таблиця 2.8 – Залежність атмосферного тиску від висоти

Висота км	**Тиск. Па**	**Висота, км**	**Тиск* Па**
0,1	$9.2 \cdot 10^2$	30,0	$1,1\ 10^3$
1,0	$8{,}8 \cdot 10^4$	100,0	$1,3 \cdot 10^{-2}$
3,0	$6,8 \cdot 10^4$	2000,0	$1{,}3\ 10^{-11}$
5,0	$5{,}0 \cdot 10^4$		

Знижений тиск впливає на ізоляційні властивості повітря, приводить до зміни ємності повітряних конденсаторів і характеристик інших елементів, у яких повітря використовується як ізолятор. При зниженому тиску легко виникає тліючий розряд між провідниками, що перебувають під високою напругою. При зміні висоти з 1000 до 1600 м величина пробивної напруги повітря зменшується в чотири рази.

Глибокий вакуум, властивий для космічних апаратів, може викликати сублімацію металевих і неметалічних матеріалів, випар змащення, погіршення теплопередачі. Крім цього глибокий вакуум приводить до погіршення тертя й зварюванню контактуючих поверхонь, на поверхнях діелектриків накопичуються електричні заряди, що приводить до посилення поверхневих струмів витоку.

Зниження тиску погіршує відвід тепла від елементів ЕРВ, що може привести до їхнього перегріву, особливо на більших висотах, тому що вже на висоті 6 км теплоємність повітря падає у два рази в порівнянні з його теплоємністю в землі.

У зв'язку із цим необхідно відповідне охолодження апаратури, що слід ураховувати при виборі розмірів і стану випромінюючої поверхні, герметизація апаратури, заходу примусового охолодження.

Радіація. Радіація може бути *природньої* й *штучної.*

Джерелами природньої радіації є: космічне випромінювання, розпад природніх радіоактивних елементів, радіація радіаційних поясів Землі й випромінювання Сонця.

Для наземної польовий ЕРВ основним джерелом природньої радіації слід уважати Сонце, особливо його теплове й ультрафіолетове випромінювання.

Корпускулярне випромінювання Сонця й космічне випромінювання в значній мірі поглинається земною атмосферою, створюючи разом з розпадом природніх радіоактивних елементів радіаційне тло на поверхні Землі. Його рівень піддається флуктуаціям. Особливо сильні зміни радіаційного тла можливі при спалахах сонячної активності.

Природний радіаційний фон практичного впливу на ЕРВ не виявляє.

Як ми вже відзначали, теплове випромінювання Сонця погіршує умови охолодження ЕРВ й може сприяти її місцевому або загальному перегріву.

Вплив ультрафіолетового випромінювання, хоча й значно ослабленого атмосферою, приводить до активізації фізико-хімічних процесів старіння, у результаті чого прискорюються окисні процеси й розпад багатьох органічних діелектриків, руйнуються лакофарбові покритий, прискорюється корозія деяких металів.

Для ЕРВ, що працює в космічному просторі, також істотний вплив корпускулярного випромінювання Сонця, енергія часток якого може доходити до 20 МеВ, і вплив радіації радіаційних поясів Землі. Так, на висоті 3600 км його енергія досягає 700 МеВ при потужності потоку до $2 \cdot 10^5$ протон/см^2.

Штучна радіація створюється при атомних і термоядерних вибухах, атомними реакторами й підсилювачами часток високих енергій. Рівні штучної радіації можуть досягати дуже високих значень, що перевищують природню радіацію.

Ступінь впливу на елементи ЕРВ визначається видом радіації й умовами впливу. Найбільше сильно піддані впливу штучної радіації елементи ЕРВ, що використовують органічні й напівпровідникові матеріали. Вплив радіації також залежить від технології виготовлення елементів ЕРВ. Так, планарні транзистори більш стійкі до радіації, чому транзистори з мезаструктурою, а тонкоплівкові транзистори на 2-3 порядку більш стійкі, чому монокристалічні.

При опроміненні швидкими нейтронами порушується структура матеріалу, підвищується його температура, а і результаті захвату нейтронів утворюються домішки інших елементів.

Опромінення електронами й протонами на структуру речовини практично не впливає, але викликає іонізацію. При опроміненні речовини електронами великої енергії може виникнути тверде рентгенівське випромінювання. При опроміненні гамма-променями можуть активізуватися деякі реакції усередині речовини.

Під впливом такого роду радіації в матеріалах ЕРВ можуть відбуватися необоротні зміни, тимчасово необоротні, що зникають після закінчення деякого часу після припинення опромінення, і оборотні.

По даним [8] припустимим для ЕРВ рівнем опромінення вважається: доза гамма-випромінювання — 10^6 р, потік нейтронів — 10^{13} нейтронів/див^2, теплове випромінювання до 100 кал/див^2.

Тому для ЕРВ космічних апаратів і ракет важливо підібрати найбільш стійкі до опромінення матеріали й елементи, а також вжити заходів спеціального захисту найбільш уразливих частин ЕРВ.

Чистота повітря. На надійність ЕРВ помітний вплив виявляє забруднення повітря механічним і хімічними домішками.

пил, що перебуває в повітрі, являє собою дрібні частки гірських порід, ґрунту, диму промислових підприємств, залишки рослинних і тваринних організмів. У повітрі залежно від ступеня його забруднення може втримуватися до 60 мг/м^3 пилу.

Пил, що перебуває в атмосфері, легко проникає в негеометризовану ЕРВ, знижуючи поверхневий опір, прискорюючи зношування частин, що рухаються, контактів, змінюючи, у ряді випадків, параметри елементів.

Особливо сильно пил погіршує характеристики апаратури, виконаної на друкованому монтажі, не захищеному спеціальним покриттям, тому що вона утворює струмопровідні перемички між провідниками. З метою запобігання друкованих плат від впливу пили й вологи їх покривають міцною ізоляційною плівкою.

Зволоження пили підсилює її вплив на електричні параметри ЕРВ. Так поверхневий опір неочищеної поверхні ультрафарфору при вологості 0% — $1 \cdot 10^{16}$ Ом, а той же поверхні при 100% вологості — $1 \cdot 10^9$Ом.

Немаловажне й те, що осілий пил у певних умовах прискорює вплив біологічних факторів.

Більші механічні частки розміром до 0,8 мм (пісок) руйнують захисні покриття, підшипники й інші елементи.

Крім пилу в атмосфері можуть бути сильнодіючі хімічні домішки, що викидаються промисловими підприємствами й різного роду машинами (солі, окисли кислоти й т.п.). Так, сірчистий газ утримується у вихлопних газах автомашин, газах металургійних і хімічних підприємств. Окисли азоту й хлор утримуються в газах ряду хімічних підприємств. Вони збільшують корозію металів, прискорюють процес старіння в пластмасах і органічних діелектриках. Ступінь впливу цих домішок значно збільшується у вологому повітрі.

Особливо впливають на надійність ЕРВ солі й солоні тумани на море й морському узбережжі. Висока вологість атмосфери й насиченість її солями суттєво прискорюють процес появи відмов. Для зменшення впливу цих факторів необхідно застосовувати герметизацію елементів і апаратури в цілому, спеціальні волого– і солестойки покриття. У випадках примусового охолодження апаратури — протипилові фільтри або замкнену систему охолодження.

Механічні навантаження. Механічні навантаження викликаються ударами й вібраціями при транспортуванні, при впливі вітру, аеродинамічними впливами й т.п.

Удари й вібрації можуть привести до порушення цілісності пайок, контактів, руйнуванню електронних ламп, кріпильних деталей, порушенням регулювань.

Механічні впливи визначаються в одиницях сили ваги. Ударне прискорення

$$g\frac{v^2}{2\cdot 9{,}81\cdot s} \qquad (2.82)$$

де g — прискорення сили ваги; v— миттєва швидкість у момент удару, див/з; s — переміщення при ударі або сумарна величина пружних і залишкових деформацій, що вдаряються предметів, мм.

Прискорення при вібраціях

$$g\frac{4\pi^2 f 2s}{9810} \qquad (2.83)$$

де f — частота коливань, Гц; s — амплітуда переміщень, мм.

У табл. 2.9 наведені характеристики по вібраціях і перевантаженням різних видів перевезень.

Таблиця 2.9 – Характеристики по вібраціях і перевантаженням різних видів перевезень

Вид перевезень	**Вібрації, Гц**	**Перевантаження, g**	**Значення частот, відповідних до максимуму перевантажень, Гц**
Морські	0 — 30	**1**	10 — 30
Залізничні	1,5 — 400	2	2 — 8.30 — 400
Автомобільні	0 — 200	4 — 5	2—8, 20 — 150
Авіаційні	5 — 500	20	150 — 300
Апаратура в ракетах	30 — 2000	10 — 70	—

Практика показує, що найнебезпечнішими є вібрації із частотами 15-150 і 175-500 Гц. Першому діапазону частот відповідають резонансні явища в конструкціях апаратури, а другому– резонансні явища в елект-

ронних лампах, які можуть привести до руйнування спаїв скла з металом, ушкодити слюдяні ізолятори, змінити міжелектродні відстані й т.п. Внаслідок вібрації й ударів параметр потоку відмов літакової ЕРВ майже в 10 раз, а ракетної в 100 раз вище наземної.

Механічні ушкодження апаратури може викликати й обслуговуючий персонал при недостатній кваліфікації й недбалому обігу з нею.

Правильний вибір амортизаційних пристроїв кріплення, що відповідає розміщення й, елементів ЕРВ, правильний вибір схем дозволяють знизити на 90% число відмов, пов'язаних з механічними впливами.

До механічних впливів слід також віднести вплив гідрометеорів на елементи ракет і літаків, а також мікрометеорів на космічні апарати й елементи ЕРВ, що перебувають у космосі. Їхні удари викликають ерозію матеріалу, порушення захисних покриттів, зниження механічної міцності й герметичності.

Особливу небезпеку для космічної апаратури представляють зустрічі з потоками мікрометеоритної речовини. Це пояснюється тим, що, хоча маса часток мала (10-3 г і менш), вони мають дуже більші швидкості (10—70 км/с), що при зіткненні викликає поява ударної хвилі й зміни структури речовини. На висотах 100—200 км щільність потоку таких часток може досягати 0,3—0,7 $1/м^2 \cdot с$. Зустріч із таким потоком може викликати загибель ЕРВ.

Біологічні фактори. Під біологічними факторами розуміють вплив на ЕРВ живих організмів, тобто вплив грибкових утворів, комах, гризунів і т.п.

Грибкові утвори можуть значно знизити надійність. Як правило, вони виникають у вологій атмосфері на деталях з органічних матеріалів, харчуючись продуктами їх розкладання. При наявності пили грибковий утвори розбудовуються значно інтенсивніше й можуть розбудуватися на будь-якому матеріалі. Найбільш сприятливими для їхнього розвитку вважаються підвищена вологість і температура 25—35°С. Ріст цвілі припиняється при температурі нижче 7° С.

Грибкові утвори знижують поверхневий опір ізоляторів, утворюють провідні перемички між провідниками, руйнують металеві й неметалічні деталі за рахунок впливу виділюваних кислот. Найбільше сильно страждають від цвілі виробу з натуральних волокнистих матеріалів (бавовна, льон і т.п.).

Комахи й гризуни рідше впливають на ЕРВ, але такі випадки на практиці зустрічаються. Комахи й гризуни руйнують оболонки кабелів, М'які пластмасові покриття, дерев'яні деталі, приводять до замикань контактів, рознімань, кабелів. За даними літератури, до 0,5% відмов обумовлене впливом біологічних факторів. Для зменшення шкідливого впливу комах і гризунів застосовують пластмаси зі спеціальними добавками відпугиваючої або отруйного дії.

Дії обслуговуючого персоналу. З позицій ергономіки, помилки оператора в системі людей-машина приводять до часткового або повному невиконанню завдання системою.

Вплив дій обслуговуючого персоналу в ряді випадків буває більш значним, чому всіх інших факторів. Так, за американським даними, до 30% відмов апаратури є наслідком недостатньої кваліфікації обслуговуючого персоналу. Дослідження показали, що при гарній підготовці операторів і правильної організації експлуатації польовий ЕРВ надійність в 3-5 раз вище, чим при поганій організації й низькій підготовці операторів.

Серед факторів, що визначають ступінь впливу обслуговуючого персоналу при експлуатації на надійність ЕРВ, необхідно відзначити:

а) кваліфікацію обслуговуючого персоналу;

б) дотримання правил технічної експлуатації;

в) ступінь організованості системи технічного обслуговування.

Одним з основних факторів є кваліфікація обслуговуючого персоналу. Під цим терміном надалі будемо розуміти ступінь підготовленості обслуговуючого персоналу, яка визначається знанням пристрою й призначення апаратури, умов і правил її експлуатації, умінням підтримувати її в справному стані, попереджати появу деяких відмов, усувати відмови, що з'явилися, правильно організувати роботу па ефективному використанню її по призначенню. Так, при слабко підготовлених операторах кількість відмов апаратури в першу добу після проведення регламентних робіт в 8-10 раз перевищує число відмов за добу перед регламентними роботами. Це пояснюється невмінням обслуговувати ЕРВ, невмінням виявити несправності, неправильними діями, що викликають поява нових несправностей. Природно, що добре підготовлений персонал може забезпечити експлуатацію ЕРВ з меншими витратами сил і засобів.

Недостатня кваліфікація обслуговуючого персоналу може бути до деякої міри компенсована автоматизацією контролю працездатності й процесу пошуку несправностей, зменшенням числа регулювань і т.п.

Незважаючи на це, питанню підготовки обслуговуючого персоналу повинне приділятися першорядне значення особливе для складних систем ЕРВ.

Строге дотримання правил технічної експлуатації сприяє змісту ЕРВ в справному стані, тому що ці правила передбачають саме такі дії обслуговуючого персоналу, які краще забезпечують експлуатацію даної апаратури.

Ступінь організованості системи технічного обслуговування визначає кращі методи й форми організації експлуатації ЕРВ, при яких забезпечується висока безвідмовність і довговічність апаратури. Вона передбачає організацію ряду заходів (профілактика, ремонт, постачання запасними деталями й т.п.), спрямованих на

забезпечення експлуатації з найбільш високим значенням коефіцієнта готовності.

Слід зазначити, що поліпшенню експлуатації сприяє надійне складання й обробка даних експлуатації ЕРВ. Отримані в результаті аналізу статистичних даних експлуатації результати допомагають краще організувати систему технічного обслуговування, забезпечення запасними деталями й прогнозувати можливі відмови. Ці результати також корисні й при розробці нової апаратури, тому що допомагають заздалегідь урахувати особливості експлуатації й недоліки попередніх розробок.

У процесі експлуатації на ЕРВ тією чи іншою мірою діють усі фактори, які повинні правильно враховуватися обслуговуючим персоналом.

2.5 Методи розрахунків надійності

2.5.1 Класифікація методів розрахунків безвідмовності

Під розрахунками надійності будемо розуміти визначення числових значень показників надійності по тем або іншим вихідним даним. Певні значення показників надійності дозволяють оцінити експлуатаційні властивості об'єкта ЕРВ на етапі його проектування або ж експлуатації. Це допомагає зробити висновок про їхню відповідність заданим значеннями при необхідності вжити заходів до підвищення надійності.

Як правило, розрахунки надійності зводиться до визначення показників безвідмовності й, що значно рідше, показників інших складових надійності.

Сутність розрахунків зводиться до визначення основних показників надійності ЕРВ за відомими показниками надійності її елементів. Відповідні показники комплектуючих елементів беруться на підставі довідкових даних або результатів експлуатації й спеціально планованих експериментів.

Як приклад у табл. 2.10 наведені усереднені дані про інтенсивність відмов ряду елементів ЕРВ,

Таблиця 2.10 – Інтенсивність відмов ЕРВ

Найменування елементів	**Інтенсивність відмов $x10^{-5}$. 1/ч**	**Найменування елементів**	**Інтенсивність відмов $x10^{-5}$, 1/год**
Електровакуумні прилади	0,1—34,5	Напівпровідникові діоди	0,012—50
Резистори	0,001—1,5	Напівпровідникові тріоди	0,01—90
Конденсатори	0,001—16,4		
Трансформатори	0,002—6,4	Комутаційні обладнання	0,0003—2,8
Дроселі, котушки індуктивності	0,002—4,4		
		Штепсельні рознімання	0,001—9,1
Реле	0,05—101	З'єднань пайкою й проведення	0,01—1
Сельсини, електродвигуни	0,1—33		
		Гіроскопи	100—600

При розгляді методів розрахунків безвідмовності будемо вважатися, що ніяких попередніх заходів для її підвищення не прийняте, використовувані елементи типові й з'єднані між собою послідовно.

Розглянемо випадок довільного закону розподілу часу безвідмовної роботи. Знайдемо зв'язок між показниками безвідмовності об'єкта й показниками безвідмовності комплектуючих його елементів.

Для оцінки безвідмовності одного елемента можна скористатися вираженням (1.25). Воно дозволяє визначити ймовірність безвідмовної роботи елемента по відомій інтенсивності відмов Даного типу.

Лічачи первинні відмови елементів даного об'єкта подіям незалежними, для ймовірності безвідмовної роботи всього об'єкта можна записати

$$P = p_1(t) \cdot p_2(t) \cdot \ldots \cdot p_n(t) = \prod_{i=1}^{n} p_i(t) \qquad (2.84)$$

де $p_i(t)$— імовірність безвідмовної роботи і-го елемента.

З урахуванням вираження (1.28) вираження (2.84) прийме вид

$$P = \prod_{i=1}^{n} p_i(t) = \prod_{i=1}^{n} e^{-\int_0^t \lambda_i(t)dt} = e^{-\sum_{i=1}^{n} \int_0^t \lambda_i(t)dt} = e^{-\int_0^t \Lambda(t)dt} \qquad (2.85)$$

де $\Lambda(t) = \sum_{i=1}^{n} \lambda_i(t)$

Тому що будь-який об'єкт ЕРВ складається з декількох груп однотипних елементів із приблизно однаковими показниками безвідмовності, то для кожної групи з *ni* елементів справедливе вираження (2,85), а для всього об'єкта

$$\Lambda(t) = \sum_{i=1}^{k} n_i \lambda_i(t) \qquad (2.86)$$

де k — кількість груп елементів, що утворюють даний об'єкт»

$$P(t) = e^{-\sum_{i=1}^{k} n_i \int_0^t \lambda_i(t)dt} \qquad (2.87)$$

Аналіз отриманого вираження дозволяє зробити наступні висновки:

а) безвідмовність об'єкта буде тем нижче, чим, більше елементів входить до його складу (більше *n* и *k*);

б) імовірність безвідмовної роботи об'єкта буде завжди нижче ймовірності безвідмовної роботи самого ненадійного елемента.

Найбільший інтерес представляє розрахунки надійності для ділянки нормальної експлуатації, де слушний експонентний закон розподілу часу безвідмовної роботи $\lambda_i(t) = \lambda_i$.. Для цього випадку

$$P(t) = e^{-\sum_{i=1}^{n} n_i \lambda_i t} = e^{-\Lambda t} = e^{-t/T_o} \quad (2.88)$$

де $\Lambda = \sum_{i=1}^{n} n_i \lambda_i; T_o = \frac{1}{\Lambda}$.

У зв'язку з відмінністю в механізмі виникнення раптових і поступових відмов, розрізняють розрахунки надійності по раптових і по поступових відмовах. Залежно від типу вихідних даних для розрахунків вибирають методи розрахунків за довідковим даними або методи розрахунків за статистичним даними. Залежно від повноти розрахунків також розрізняють повний і неповний розрахунки надійності.

Тому що в цей час розроблене значну кількість методів розрахунків безвідмовності, то для зручності знайомства з ними на рис. 2.31 наведена їхня класифікація.

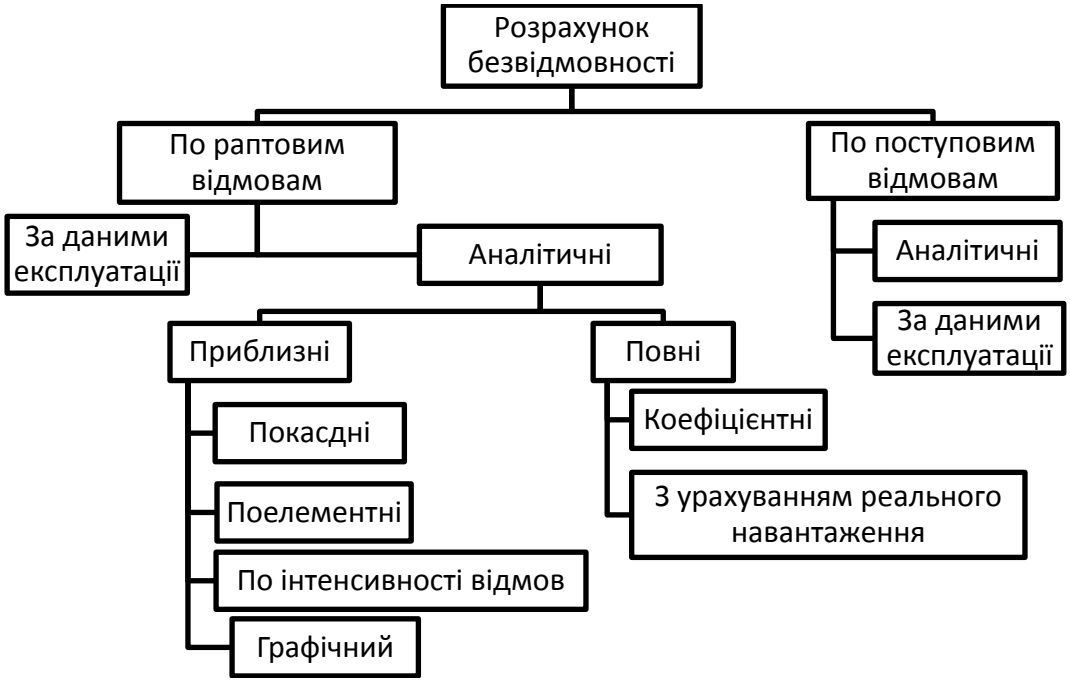


Рис. 2.31 – Класифікація методів розрахунків безвідмовності

2.5.2 Аналітичні методи розрахунків безвідмовності

Для розрахунків безвідмовності об'єкт необхідно представити у вигляді розрахункової схеми. Незалежно від складності об'єкта ЕРВ й реальних зв'язків комплектуючих його елементів розрахункова схема може бути представлена у вигляді послідовного з'єднання тих же елементів. Така схема оцінює роль кожного елемента у втраті працездатності об'єктом. Показники безвідмовності розраховуються по раніше отриманих виразах (§ 1.34-1.8).

Залежно від повноти вихідних даних розрізняють наближений і повний розрахунки безвідмовності. Для наближеного розрахунків безвідмовності достатньо знання функціональної схеми об'єкта (до каскаду).

При повному розрахунках безвідмовності необхідне знання принципової схеми об'єкта (до елемента), λ-характеристики елементів, їх режими роботи й навантаження, що діють на елемент.

Розрахунки безвідмовності по раптових відмовах, У якості наближених методів розрахунків безвідмовності можуть бути використані: *покаскадний, заелементний, по інтенсивності відмов, графічний.*

Покаскадний метод розрахунків дає оцінку безвідмовності в першому наближенні, застосовують його на самих ранніх етапах проектування. У якості вихідних даних використовуються число каскадів у проектованій апаратурі й приналежність її до тієї, або іншій групі.

Розрахунки показників надійності здійснюється за допомогою вираженій (2.85) -2.88). Для оцінки значення сумарної інтенсивності відмов використовується вираження

$$\Lambda\,1/\text{ч} = 10^{-4}\,\frac{n_{\text{к}}}{k_{\text{а}}}\quad , \tag{2.89}$$

де $n_к$ — кількість каскадів у проектованої ЕРВ; *ka* — коефіцієнт, що враховує умови експлуатації ЕРВ залежно від її приналежності до тієї або іншій групі, рівний:

Для наземної ЕРВ	l,8
Для літакової ЕРВ	0,25
Для корабельної ЕРВ	1,4

Коефіцієнт 10^{-4} визначений на підставі аналізу інтенсивності відмов різних типів елементів ЕРВ. Рівняння дає трохи завищені дані по інтенсивності відмов.

Заелементний метод розрахунків дозволяє одержати більш точну оцінку безвідмовності, його застосовують на наступних етапах проектування. У якості вихідних даних використовується: загальне число елементів, що комплектують проектовану ЕРВ, і їх тип, а також дані експлуатації аналогічного типу ЕРВ (по схемному використанню елементів і їх навантаженням).

Розрахунки показників безвідмовності здійснюється за допомогою виразів (2.84) – (2.88). Для оцінки значення сумарної інтенсивності відмов використовують дані, отримані при експлуатації аналогічної ЕРВ. Для цього випадку справедливо

$$\lambda_{\text{ср}},\,1/\text{ч} = \frac{\Lambda_{\text{э.а}}}{n_{\text{э.а}}} = \frac{\Lambda_{\text{п.а}}}{n_{\text{п.а}}} \tag{2.90}$$

де $\Lambda_{э.а}, \Lambda_{п.а}$ — сумарні інтенсивності відмов відповідно експлуатованого аналога ЕРВ й проектованої апаратури; $n_{\text{э.а}}, n_{\text{п.а}}$ кількість елементів відповідно до експлуатованої й проектованої ЕРВ.

З вираження (2.7) випливає

$$\Lambda_{\text{п.а}} = \frac{n_{\text{п.а}}}{n_{\text{э.а}}}\Lambda_{\text{э.а}} \qquad (2.91)$$

Метод розрахунків по інтенсивності відмов дозволяє досить повно оцінити безвідмовність проектованої апаратури. У якості вихідних даних використовуються: принципова схема ЕРВ, відомості про кількість груп і типів комплектуючих елементів і їх інтенсивності відмов для легких і тяжких умов застосування.

Розрахунки показників безвідмовності здійснюється за допомогою вираженій (2.84)-(2.88). Порядок проведення розрахунків наступний:

1) згідно із принциповою схемою й специфікації на неї роблять розбивку всіх елементів ЕРВ на групи, що мають приблизно однакові інтенсивності відмов. Підраховують число елементів у кожній групі — n_i.

2) за довідковим даними для використовуваних елементів знаходять максимальні й мінімальні значення інтенсивності відмов — $\lambda_{i\max}$, $\lambda i_{\min}$;

3) визначають максимальні й мінімальні групові інтенсивності відмов $ni\ \lambda i_{\max}$ і $ni\ \lambda i_{\min}$,

4) визначають загальну інтенсивність відмов по вираженню (2.88);

5) використовуючи це ж вираження, визначають імовірність безвідмовної роботи й середній час наробітку до відмови (розрахунки ведеться для значень $\lambda i_{\max}$ і $\lambda i_{\min}$).

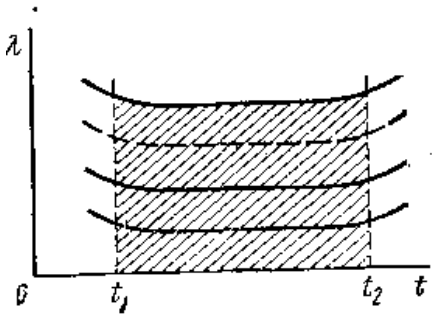


Рис. 2.32

Графічний метод розрахунків безвідмовності застосовують, якщо відома залежність інтенсивності появи відмов від часу.

У цьому випадку розрахунки показників безвідмовності також здійснюється за допомогою вираження (2.2). Розрахунки сумарної інтенсивності відмов об'єкта виконують графічно по відомих залежностям$\lambda = f(t)$. Із цією метою роблять підсумовування ординат характеристики $\lambda i\ (t)$ (рис, 2.2).

Потім визначають площа по кривій Λ (t):

$$S_\lambda = \int_{t_1}^{t_2} \Lambda(t)dt. \qquad (2.92)$$

Підраховане значення *Si* підставляють у вираження (2.2), яке прийме вид

$$P = e^{-\int_{t_1}^{t_2} \Lambda(t)dt.} = e^{-S_\lambda} \qquad (2.93)$$

Повний розрахунки безвідмовності має на увазі облік режимів роботи комплектуючих об'єкт елементів. Залежно від повноти обліку розрізняють *коефіцієнтний метод* і *метод обліку реальних навантажень елементів.* Усі перераховані методи розрахунків припускають наявність повних відомостей про об'єкт ЕРВ й умовах його експлуатації.

Коефіцієнтний метод дозволяє одержати досить повні й достовірні дані при наявності досить повних даних про коефіцієнти надійності застосовуваних елементів. Коефіцієнтний метод припускає наявність найпростішого потоку відмов.

Коефіцієнт надійності являє собою відношення інтенсивності відмов елементів і-*й* групи *λі* за даних умов експлуатації до інтенсивності відмов деякого основного елемента *λо,* кількісні характеристики якого в досить близьких умовах експлуатації вірогідно відомі, тобто

$$k_i = \lambda_i / \lambda_o \qquad (2.94)$$

Це вираження припускає однаковий вплив режимів роботи як на основний елемент, так і на всі інші.

При значних відмінностях в умовах експлуатації в значеннях коефіцієнтів навантаження використання співвідношення (2.11) стає неправомочним. У якості основного елемента, як правило, використовують резистор. У табл. 2.11 наведені максимальні й мінімальні значення коефіцієнтів надійності ряду елементів ЕРВ.

Таблиця 2.11 – Коефіцієнти надійності ряду елементів ЕРВ.

Найменування елемента	$\mathbf{k_{min}}$	k_{max}
Електровакуумні прилади	19	7
Резистори	1	1
Конденсатори	0,25	0.83
Трансформатори	1.3	3
Дроселі, котушки індуктивності	1	2
Реле	1	10
Напівпровідникові діоди	1.3	30
Транзистори	1,3	75
Електродвигуни	10	40

Розрахунки безвідмовності здійснюється допомогою виразів *(2.84)*-(2.88).

Використовуючи вираження (2.11), вираження (2.5) можна написати у вигляді

$$\Lambda = \lambda_0 \sum_{i=1}^{k} n_i K_i; \qquad (2.95)$$

Облік умов експлуатації в коефіцієнтному методі здійснюється за допомогою обліку впливу цих умов на поведінку основного елемента:

$$\Lambda(\mathrm{z}) = \lambda_0(\lambda \sum_{i=1}^{k} n_i K_i; \qquad (2.96)$$

де $\lambda_0(\lambda$ – інтенсивність відмов основного елемента з урахуванням впливу z-го фактору.

Для підвищення вірогідності й точності оцінки безвідмовності необхідно значення коефіцієнтів K_i уточнювати іузгоджувати їх з реальною конструкцією ЕРВ, умовами її експлуатації й реальними режимами роботи елементів.

Розрахунки безвідмовності доцільно вести поблочне з метою виявлення слабких місць даного типу ЕРВ.

Метод обліку реальних навантажень елементів дозволяє одержати результати, найбільше близькі до дійсності, тому що в розрахунки вводиться дійсне значення інтенсивності відмов з урахуванням реальних режимів роботи й впливу відповідних факторів.

У якості вихідних даних використовують усі наявні дані про досліджуваний об'єкт ЕРВ, а також залежності інтенсивності відмов комплектуючих його елементів від впливу реально діючих у заданих умовах експлуатації факторів, тобто $\lambda_i(\lambda$. У цьому випадку вираження (2.88) прийме вид

$$\Lambda(\mathrm{z}) = \sum_{i=1}^{k} \lambda_i(z); \qquad (2.97)$$

В іншій частині розрахунки не відрізняється від раніше описаних і проводиться по виразам (2.84)-(2.88).

Розрахунки по поступових відмовах. Поряд у раптовими відмовами, особливо для складних об'єктів ЕРВ, характерно значна кількість поступових відмов, особливо в період старіння. Число таких відмов може досягати до 50% від загального числа всіх відмов I44J. Облік старіння елементів особливо важливий для ЕРВ с більшим строком зберігання.

Основою розрахунків є дані про закономірності зміни визначальних параметрів даного об'єкта в часі, а також установлені на них допуски.

Дослідження поведінки параметрів численних типів об'єктів ЕРВ показують, що розподіл часу безвідмовної роботи при поступових відмовах відповідає нормальному закону; отже. для кожного параметра можуть бути знайдені свої значення t_{cpi}і σi.

Як було показано в § 2.3.3, імовірність безвідмовної роботи з і-*му* параметру буде визначатися вираженням

$$P_{ni}(t) = \frac{F_0\left(\frac{t_{cpi} - t}{\sigma_i}\right)}{F_0\left(\frac{t_{cpi}}{\sigma_i}\right)} \qquad (2.98)$$

У цьому випадку ймовірність безвідмовної роботи всього об'єкта ЕРВ по поступових відмовах, якщо вважати відмови елементів ЕРВ незалежними, можна знайти з вираження

$$P_o(t) = \prod_{j=1}^{\Delta} P_{oj}(t) \qquad (2.99)$$

де Δ — число визначальних параметрів об'єкта.

Значення t_{cpi} і σ_i, як правило, знаходять на підставі статистичних даних експлуатації подібного типу об'єктів ЕРВ.

На закінчення відзначимо, що ймовірність безвідмовної роботи об'єкта з обліком раптових і поступових відмов визначається вираженням

$$P_{\Sigma}(t) = P_{\text{в}}(t)P_o(t) = e^{-t\sum_{i=1}^{k} n_i\lambda_i} \prod_{j=1}^{\Delta} P_{oj}(t) \qquad (2.100)$$

2.6 Методи підвищення надійності

2.6.1 Загальні методи підвищення надійності

Як відзначалося в гл. I, надійність електрорадіовиробів (ЕРВ) залежить від безлічі факторів. Згідно із класифікацією цих факторів (див. рис. 1.10) основними з них є суб'єктивні: помилки розробки, помилки виробництва й помилки експлуатації. У літературі приводиться наступний розподіл відмов: помилки розробки — 40%, помилки виробництва — 30% і помилки експлуатації — 30%.

К е р у в а н н я н а д і й н і с т ю – цілеспрямована діяльність щодо обґрунтування, планування, забезпечення, підвищення та підтримки характеристик безвідмовності, ремонтопридатності, довговічності та збережуванності об’єктів, що розглядаються.

П р о г р а м а з а б е з п е ч е н н я н а д і й н о с т і – документ, що встановлює комплекс взаємообумовлених організаційно-технічних вимог та заходів, які належить проводити на певних етапах життєвого циклу об’єкта і спрямованих на забезпечення заданих вимог до надійності та (або) на підвищення надійності.

Висока надійність об'єкта на стадії проектування забезпечується за рахунок наступного:

а) вибору схемних рішень;

б) вибору елементів, матеріалів і режимів їх роботи;

в) вибору конструктивних рішень;

г) обліку умов роботи й досвіду експлуатації аналогічної апаратури;

д) розробки заходів щодо зручності технічного обслуговування й експлуатації;

е) обліку можливостей оператора й вимог ергономіки.

При виборі принципових схем ЕРВ перевага віддається найбільш простим схемам з найменшим числом елементів, схемам, що не вимагають спеціального добору елементів, що мають мінімальне число органів регулювання, схемам, що стійко працюють у широкому інтервалі впливів дестабілізуючих факторів.

Однак повне задоволення всіх цих умов неможливо й конструкторові доводиться шукати компромісні рішення.

У проектованій апаратурі необхідно використовувати елементи, надійність яких відповідає вимогам до надійності самої апаратури.

У зв'язку з ростом обсягу й відповідальності, розв'язуваних ЕРВ завдань, вимоги до надійності апаратури безупинно ростуть. Це у свою чергу пред'являє усе більш високі вимоги до надійності комплектуючих елементів. Однак, незважаючи на досить високу якість елементів, що випускаються промисловістю, вони не завжди відповідають пропонованим вимогам. Так, середня інтенсивність відмов серійних елементів порядку $1\cdot(10^{\sim 5}—10^{-6})$, 1/год. Уважаються, що шляхом подальшого вдосконалювання виробництва можна знизити інтенсивність відмов до $1 \cdot 10^{-8}$, 1/год. Це зажадає істотної перебудови технології, значного часу й більших засобів.

Тому перед конструктором залишається завдання забезпечення необхідної надійності ЕРВ без істотної зміни надійності її елементів.

Важливим фактором підвищення надійності є правильний вибір режимів роботи елементів. Уважається, що оптимальні електричні навантаження елементів не повинні перевищувати 25% від номінальних. У менш відповідальних випадках їх можна побільшати до 40% і трохи вище.

Правильний вибір конструкційних матеріалів для ЕРВ також сприяє підвищенню її надійності. Застосовувані матеріали повинні мати таку швидкість старіння, яка забезпечувала б нормальну експлуатацію апаратури протягом усього терміну служби й зберігала б необхідні механічні й електричні характеристики.

Конструктивні рішення прямо й побічно впливають на надійність ЕРВ. Невдалий конструктивний розв'язок може привести до передчасної відмови. Великоблочна конструкція технологічно складна й незручна при ремонті, тому перевага необхідно віддавати модульної конструкції. Вирішуючи це питання, слід знаходити оптимальне число блоків, тому що при великій їхній кількості на надійність будуть суттєво впливати міжблочні з'єднання, знижуючи її надійність. Також важливий правильний вибір монтажу. Наприклад, друкований монтаж значно надійніше, чим навісний, але він менш зручний у ремонті.

Конструктивні рішення повинні забезпечити й необхідні теплові режими елементів ЕРВ, необхідний мікроклімат, безвідмовність в умовах впливу ударних і вібраційних навантажень.

Конструктивні рішення тісно пов'язані з наступною експлуатацією й відновленням апаратури. Тому при конструюванні треба передбачати контрольні гнізда, легкий доступ до всіх блоків апаратури, зручність контролю її стану й настроювання, зміни блоків, заходи, що забезпечують безпеку обслуговуючого персоналу й ін.

Ергономіка вимагає обліку психофізіологічних можливостей операторів і створення для них оптимальних умов. Органі керування й контролю повинні розташовуватися таким чином, щоб не стомлювали зори оператора, не викликали зайвих напруг, не вимагали більших фізичних зусиль. При конструюванні також треба враховувати швидкість реагування оператора й необхідний рівень його підготовки.

На цьому ж етапі необхідно вирішувати питання про резервування й контроль працездатності ЕРВ в процесі експлуатації.

Не менш важливим є забезпечення заданої надійності в процесі виробництва, яка досягається наступними заходами:

а) вибором відповідної технології й строгим її дотриманням;
б) впровадженням автоматизації;
в) вхідним контролем матеріалів і елементів;
г) попередні тренуванням елементів і апаратури;
д) вибором методики настроювання й налагодження апаратури;
е) поточними й вихідним контролями.

Правильний вибір технології й строге її дотримання, безперервне її вдосконалювання відіграють істотну роль у забезпеченні необхідної надійності ЕРВ.

Особливо важливу роль відіграє автоматизація виробництва, тому що дозволяє одержати найбільшу відтворюваність параметрів серійної ЕРВ.

Автоматизація дозволяє звести до мінімуму вплив суб'єктивних факторів на якість продукції.

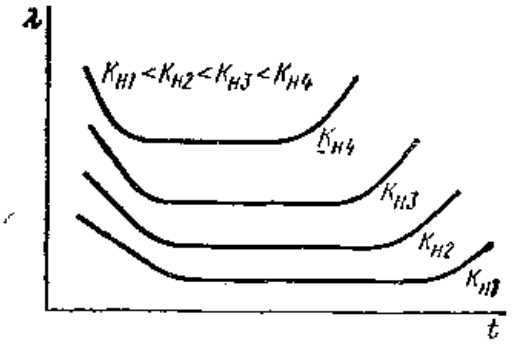


Рис. 3.33 – Залежності інтенсивності відмов від коефіцієнта навантаження

Вхідний контроль матеріалів і елементів не допускає у виробництво недоброякісні матеріали й елементи, що мають відхилення від заданих вимог.

Попереднє тренування елементів іапаратури скорочує етап приробляння апаратури, дозволяє оцінити правильність обраного коефіцієнта навантаження, відбракувати малонадійні елементи.

Особливо це корисно для апаратури одноразового застосування. Елементи при тренуваннях ставлять **у** більш тяжкі умови, чому при нормальній експлуатації. Режим вибирають на основі залежності інтенсивності відмов від коефіцієнта навантаження (рис. 4.1). Як випливає з цього графіка, з ростом коефіцієнта навантаження криві $\lambda = f(t)$ зміщаються вліво, а ділянка нормальної експлуатації скорочується. Вибираючи потрібне значення коефіцієнта навантаження, при тренуванні створюють необхідні умови для прискорених випробувань елемента, що відповідають його тривалій роботі в апаратурі.

Приріб (для ремонтопридатного об'єкта) – процес підвищення показників безвідмовності об'єкта, який використовує функціонування кожного виробу в належних навколишніх умовах з його успішним неплановим ремонтом після кожної відмови, протягом періоду ранніх відмов

Приріб (для неремонтопридатного об'єкта) – процес підвищення показників безвідмовності об'єкта, який використовує його функціонування у заданих умовах.

Усі описані заходи дозволяють зменшити ймовірність появи раптових відмов.

Зростання безвідмовності; підвищення безвідмовності – процес прогресуючого покращеній показників безвідмовності об'єкта з часом.

У процесі настроювання й налагодження апаратури виникають поступові відмови, обумовлені змінами параметрів елементів. Тому повинні бути передбачені такі настроювання й регулювання, при яких зміни параметрів елементів не приводили б до порушення працездатності.

У зв'язку з тим, що змінюються параметри елементів, як правило, в одному напрямку, регулювання за середніми значенням параметрів не завжди дає бажані результати. Тому характер регулювань повинен ретельно продумуватися на підставі аналізу обраної схеми й попереднього досвіду експлуатації.

Контроль надійності – перевірка відповідності об'єкта до заданих вимог щодо надійності.

При контролі надійності застосовуються наступні методи визначення надійності: *розрахунковий,. експериментальний, розрахунково-експериментальний, статистичного моделювання.*

Розрахунковий метод визначення надійності – метод, який ґрунтується на розрахунку показників надійності за даними довідників з надійності компонентів і комплектувальних елементів об'єкта, за даними про надійність об'єктів-аналогів, за даними про властивості матеріалів та іншої інформації, наявної на час проведення розрахунку.

Розрахунково-експериментальний метод визначення надійності – метод, коли показники надійності всіх чи деяких складових частин об'єкта визначають за результатами випробувань і (чи) експлуатації, а показники надійності об'єкта в цілому розраховують за математичною моделлю .

Експериментальний метод визначення надійності – метод, що базується на статистичному обробленні даних, одержаних у випробуваннях чи в експлуатації об'єкта.

Визначення надійності методом статистичного моделювання – спосіб визначення числових значень показників надійності об'єкта, який проектують на ЕОМ, шляхом моделювання процесів функціонування об'єкта, виникнення та усунення відмов

Випробування на надійність – випробування, які виконують для визначення чи контролю показників надійності в заданих умовах.

Існують *визначальні, контрольні, нормальні* та *прискорені* випробування на надійність.

Визначальні випробування на надійність – випробування, для визначення показників надійності зі заданою точністю та вірогідністю.

Контрольні випробуванім на надійність – випробування, які виконують для контролю за показниками надійності.

Нормальні випробування на надійність – випробування на надійність, методи та умови проведення яких забезпечують необхідний обсяг інформації в той самий термін, що й у передбачених умовах експлуатації.

Прискорені випробування на надійність – випробування, в яких рівень діючого навантаження вибирають вищим, ніж рівень навантаження у початкових умовах, щоб скоротити час, необхідний для спостереження характеристики навантаження об'єкта чи для її підсилення за заданий час.

Вірно обґрунтоване прискорене випробування не повинно змінювати основні види несправностей та характер виникнення відмов або їх відносну перевагу.

На різних стадіях виробництва ЕРВ проводиться поточний контроль, який дозволяє виявити й не допустити некондиційні елементи й вузли на подальше складання, виявити відступи від прийнятої технології. Випробування проводяться в умовах, найбільше близьких до експлуатаційних, ураховується вплив різного роду вібрацій, перевантаження, вологості й т.п.

Необхідність таких контролів випливає з того, що в процесі механічного складання допускається до 5% від загального числа відмов, а при електричному монтажі – до 24%.

Вихідний контроль є остаточною перевіркою ЕРВ після складання й настроювання.

Поточні й вихідний контролі можуть бути суцільними або вибірковими (статистичними). Останній найменш трудомісткий і при правильній організації дає гарні результати.

До експлуатаційної групи ставляться фактори, що впливають на надійність ЕРВ безпосередньо в процесі експлуатації. Вони у свою чергу складаються із груп об'єктивних факторів (вплив зовнішнього середовища й т. п.) і групи суб'єктивних факторів, пов'язаних з підготовкою обслуговуючого персоналу, організацією експлуатації й т. п.

При відповідній організації експлуатації можна зменшити вплив як тієї, так і іншої групи факторів на надійність ЕРВ, що підвищить значення *P(t)* і побільшає наробіток на відмову.

Для збільшення значення коефіцієнта готовності необхідно проводити заходи, що сприяють:

а) збільшенню часу наробітку на відмову;

б) зменшенню часу простою.

Слід зазначити, що найбільше просто й з достатнім ефектом реалізуються заходи другої групи. До них необхідно віднести:

а) підвищення кваліфікації обслуговуючого персоналу;

б) поліпшення організації технічного обслуговування;

в) удосконалювання технічних засобів обслуговування;

г) прогнозування поступових відмов;

д) зменшення часу на відшукання й усунення відмов.

Підвищення кваліфікації обслуговуючого персоналу, як ми вже відзначали (§ 1.9), у першу чергу передбачає поглиблене вивчання конкретної ЕРВ, особливостей її експлуатації, досвіду експлуатації подібного типу апаратури й т.п. Це допомагає свідомо експлуатувати апаратуру, найбільше ефективно проводити профілактичні заходи, скорочувати час на відшукання й усунення несправностей.

Поліпшення організації технічного обслуговування передбачає також організацію, при якій мінімальна витрата сил і засобів забезпечила б найбільше значення коефіцієнта готовності. Сюди входять питання підготовки обслуговуючого персоналу, планування профілактичних робіт (з урахуванням рекомендацій теорії надійності й досвіду експлуатації (ЕРВ), забезпечення технічними засобами профілактичних робіт (різна діагностична й профілактична апаратура), автоматизація контролю стану ЕРВ, планування запасних елементів й вузлів і т.п.

Організація прогнозування поступових відмов дозволяє підвищити ймовірність безвідмовної роботи протягом часу експлуатації.

Уважаючись поступові й раптові відмови взаємонезалежними відповідно до вираження (1.46), можна записати

$$K_{\text{г. в}} = \frac{T_{\text{р}\Sigma\text{в}}}{T_{\text{р}\Sigma\text{в}}+T_{\text{п}\Sigma\text{в}}};\ K_{\text{г. п}} = \frac{T_{\text{р}\Sigma\text{п}}}{T_{\text{р}\Sigma\text{п}}+T_{\text{п}\Sigma\text{п}}} \tag{2.101}$$

де $T_{\text{р}\Sigma\text{в}}$, і $T_{\text{р}\Sigma\text{п}}$— загальний час наробітку об'єкта (елемента) відповідно між раптовими й поступовими відмовами за якийсь час експлуатації;

$T_{\text{п}\Sigma\text{в}}$ і $T_{\text{п}\Sigma\text{п}}$ — загальний час простою об'єкта (елемента) відповідно через раптові й поступові відмови за тій же час експлуатації.

На рис. 3.34 наведена характеристика процесу експлуатації деякого об'єкта протягом певного часу.

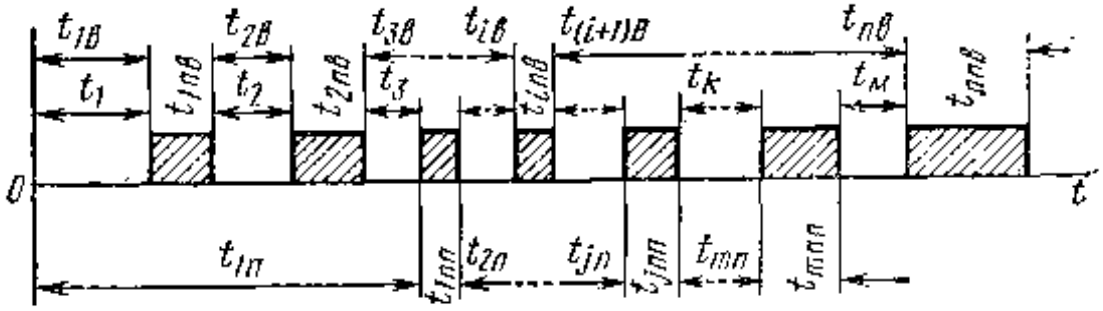


Рис. 3.34 – Характеристика процесу з урахуванням раптових та поступових відмов

За цей час в об'єкті мало місце M відмов, з них m поступових і n раптових. Для цього випадку можна записати

$$T_{\text{р}\Sigma\text{в}} = \frac{1}{n}\sum_{i=1}^{n} t_{i\ \text{в}} = \frac{1}{n}\left(\sum_{k=1}^{M} t_k + \sum_{j=1}^{m} t_{j\ \text{п. п}}\right)$$

$$T = \sum_{j=1}^{n} t_{j\ \text{п}} = \frac{1}{m}\left(\sum_{k=1}^{M} t_k + \sum_{i=1}^{n} t_{i\text{п. в}}\right) \tag{2.102}$$

де $\sum_{k=1}^{M} t_k = k$—загальний час роботи об'єкта за період експлуатації; $\sum_{j=1}^{m} t_{j\ \text{п. п}} = j$—загальний час простою об'єкта через поступові відмови за період експлуатації; $\sum_{i=1}^{n} t_{i\text{п. в}} = i$—загальний час простою об'єкта через раптові відмови за період експлуатації.

Підставляючи ці значення у вираз (3.1) і роблячи необхідні перетворення, можна записати

$$K_{\text{г. в}} + K_{\text{г. п}} = \frac{MT}{MT + mT_{\text{п}\Sigma\text{п}} + nT_{\text{п}\Sigma\text{в}}} + 1.$$

Враховуючи, що $K_{\text{г}} = \frac{MT}{MT + mT_{\text{пΣп}} + nT_{\text{пΣв}}}$ є загальний коефіцієнт готовності, остаточно можна записати

$$K_{\text{г}} = K_{\text{г. в}} + K_{\text{г. п}} - 1 \qquad (2.103)$$

Як випливає із вираження (2.103), прогнозування поступових відмов дозволяє побільшати значення загального коефіцієнта готовності об'єкта.

Тому що значення коефіцієнта $K_{\text{г. в}}$ головним чином визначається середнім часом відшукання елементів, що відмовили, то основна увага необхідно приділяти полегшенню пошуку, що відмовив елемента, а також прогнозуванню можливих відмов (діагностиці). Час відшукання елемента, що відмовив, може коливатися в значних межах — від декількох хвилин до десятків годин. Прогнозування відмов, програмування пошуку елементів, що відмовили, дозволяють зменшити цей час у кілька раз.

Якщо врахувати, що поступові відмови становлять до 50% від загального числа відмов [8], то можна вважати, що з обліком цього вираження (2.103) прийме вид $T_{\text{пΣв}} = T_{\text{пΣп}}$

$$TK_{\text{г. п}} = 0{,}5(1+K_{\text{г}}) \qquad (2.104)$$

Уважаючись для складних ЕРВ значення $K_{\text{г}} = 0{,}5 \div 0{,}9$, неважко одержати для коефіцієнта готовності при прогнозуванні поступових відмов $K_{\text{г. п}} = 0{,}75 \div 0{,}95$

Як бачимо, експлуатаційна група факторів містить ряд складових, сприяють підвищенню надійності ЕРВ, які можуть бути реалізовані як у період проектування й виготовлення апаратури, так і в період її безпосередньої експлуатації.

2.6.2 Загальні відомості про резервування

Серед методів підвищення надійності, що передбачаються при проектуванні, особливе місце займає використання н а д м і р н о с т і , тобто введення додаткових засобів або можливостей понад мінімально необхідні для виконання об'єктом заданих функцій. Сам же метод підвищення надійності об'єкта шляхом уведення надмірності прийнято називати р е з е р в у в а н н я м .

Р е з е р в у в а н н я – спосіб забезпечення надійності об’єкта за рахунок використання додаткових засобів та (або) можливостей, надлишкових відносно мінімально необхідних для виконання потрібних функцій.

Р е з е р в – сукупність додаткових засобів і (або) можливостей, що використовуються для резервування.

Особливе місце, що приділяється цьому методу, пояснюється тим,

що резервування найбільш повне дозволяє розв'язати завдання одержання необхідної надійності ЕРВ при відносно малонадійних елементах. Іноді й у процесі експлуатації може бути передбачений резерв у вигляді окремих блоків або систем для підвищення надійності всього об'єкта.

Слід ураховувати, що резервування пов'язане зі зростанням ваги, габаритів, вартості апаратури й у ряді випадків споживаної потужності електроживлення.

Класифікація існуючих методів резервування представлена на рис. 2.35.

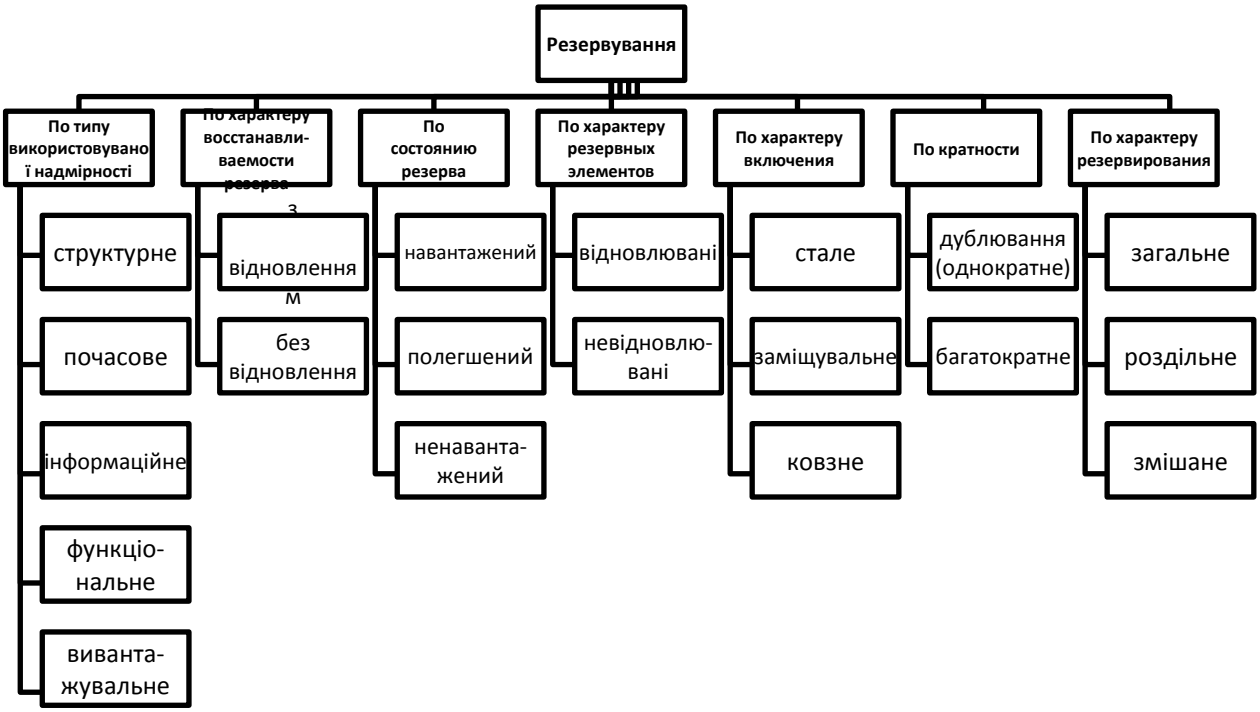


Рис. 2.35 – Класифікація резервування

Залежно від типу створюваної в об'єкті ЕРВ надмірності, розрізняють резервування:

С т р у к т у р н е р е з е р в у в а н н я – резервування з застосуванням резервних елементів структури об’єкта. Цей вид резервування передбачає використання надлишкових елементів у структурі об'єкта (уведенням додаткових вузлів, блоків і елементів аналогічних наявним);

П о ч а с о в е р е з е р в у в а н н я – резервування з застосуванням резервів часу. При цьому використовується надлишковий час, який може бути при відповідній структурі часу в інформації, що надходить на об'єкт.

І н ф о р м а ц і й н е р е з е р в у в а н н я – резервування з застосуванням резервів інформації. Воно припускає використання надмірності інформації, що надходить на об'єкт;

Функціональне резервування – резервування, при якому використовується здатність елементів об’єкта виконувати додаткові функції.

Вивантажувальне резервування – резервування, при якому використовується здатність елементів об’єкта сприймати додаткові навантаження поверх номінальних.

Надалі будемо розглядати лише структурне резервування, тому що інші види ставляться до специфічних умов експлуатації ЕРВ. Слід зазначити, що в ряді випадків в об'єкті можуть бути використано кілька видів резервування одночасно (структурне й навантажувальне, структурне й тимчасове й т. п.).

Говорячи про структурне резервування слід розрізняти *основний елемент,* тобто елемент структури об'єкта, мінімально необхідний для виконання об'єктом заданих функцій, і *резервний,* тобто елемент, призначений для забезпечення працездатності об'єкта у випадку відмови основного елемента. Природно, що резервний. елемент повинен мати характеристики, аналогічні основному.

Основний елемент – елемент об’єкта, необхідний для виконання потрібних функцій без використання резерву.

Резервований елемент – основний елемент, на випадок відмови якого а об’єкті передбачені один або декілька резервних елементів.

Резервний елемент – елемент, призначений дня виконання функцій основного елемента в разі його відмови

Слід також указати на те, що поняття «елемент» у резервуванні не ідентично такому ж поняттю, розглянутому в § 1.1. Це пояснюється тим, що в якості резервного елемента може виступати як комплектуючий об'єкт елемент, так і сам об'єкт.

Відповідно до цього розрізняють резервування:

Загальне резервування – резервування, в якому резервується об’єкт в цілому.

Роздільне резервування – резервування, в якому резервуються окремі елементи об’єкта чи їх групи.

Змішане резервування – поєднання різних видів резервування в одному об’єкті.

Резервування з відновленням – резервування, в якому відновлення основних і (чи) резервних елементів у випадку їх відмови, технічно можливе без порушення працездатності об’єкта в цілому та передбачено експлуатаційною документацією.

Резервування без відновлення – резервування, при якому відновлення основних і (чи) резервних елементів у випадках їх відмови технічно неможливе без порушення працездатності об’єкта в цілому та (або) не передбачене експлуатаційною документацією

Відношення кількості резервних елементів до кількості резервованих ними елементів, виражене нескоротним дробом. носить найменування – к р а т н і с т ь р е з е р в у .

Кратність резервування прийнято позначати *m*. Наприклад, якщо *m=3*, то це означає що: основний пристрій — одне, число резервних пристроїв — три, а загальне число пристроїв рівно чотирьом.

Розрізняють д у б л ю в а н н я – резервування з кратністю резерву один до одного. яка дорівнює одиниці *m=1* (однократне резервування), і багатократне резервування, кратність резерву якого більше одиниці *m>1*. Багатократне резервування застосовують у тих випадках, коли необхідно забезпечити досить високі показники надійності.

Приєднання резервних елементів до основних повинне проводитися паралельно. Визначимо безвідмовність об'єкта, що полягає з *m* паралельно з'єднаних елементів. Імовірність появи загальної відмови

$$Q =\cdot q_1 \cdot q \cdot q_i \cdot \ldots \cdot q_m = \prod_{i=1}^{m} q_i$$

де q_i — імовірність появи відмови і-*го* елемента.

$$P = 1 - Q = 1 - \prod_{i=1}^{m} q_i = 1 - \prod_{i=1}^{m}(1 - p_i) \qquad (2.106)$$

Як що об'єкт (елемент) складається з *K* груп однотипних елементів, то вираження (2.6) ухвалює вид

$$P = 1 - \prod_{i=1}^{K}(1 - p_i)^{m_i} \qquad (2.107)$$

З отриманих виразів випливає, що безвідмовність паралельно з'єднаних об'єктів (елементів) завжди буде вище безвідмовності одного об'єкта (елемента).

Вибираючи відповідну кількість паралельних галузей, можна за допомогою щодо малонадійних елементів забезпечити високу надійність об'єкта.

На рис. 2.36 наведена залежність імовірності безвідмовної роботи резервованого об'єкта від кількості паралельно включених гілок.

Визначимо безвідмовність об'єкта при загальному резервуванні (рис. 2.37).

Скориставшись вираженням (2.106) для випадку, представленого на рис. 2.37, можна записати

$$P_{\text{заг}} = 1 - \prod_{i=1}^{m}(1 - p_i) \qquad (2.108)$$

де p_i— імовірність безвідмовної роботи і-*го* об'єкта, що резервує.

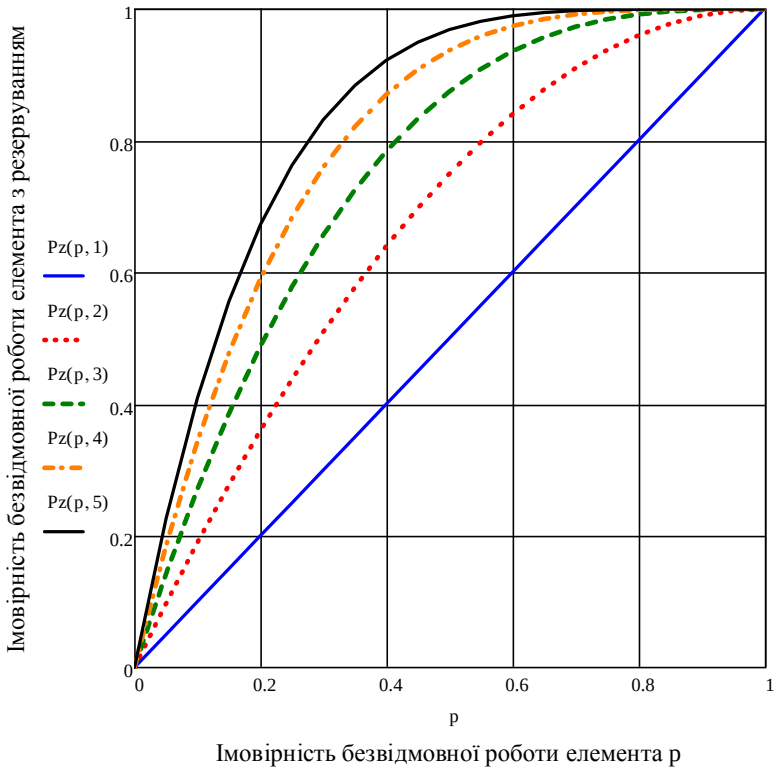


Рис. 2.36 – Залежність імовірності безвідмовної роботи резервованого елемента від кратності резервування m=1, 2, 3,4, 5, при p = 0÷1

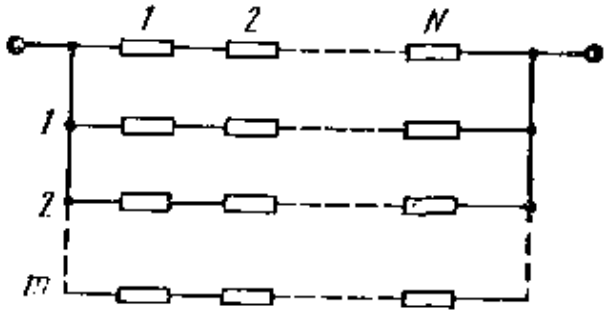


Рис. 2.37 – Схема загального резервування

Для одного об'єкта, що полягає з N послідовно з'єднаних елементів, можна записати

$$P_i = \prod_{i=1}^{N} p_i \qquad (2.109)$$

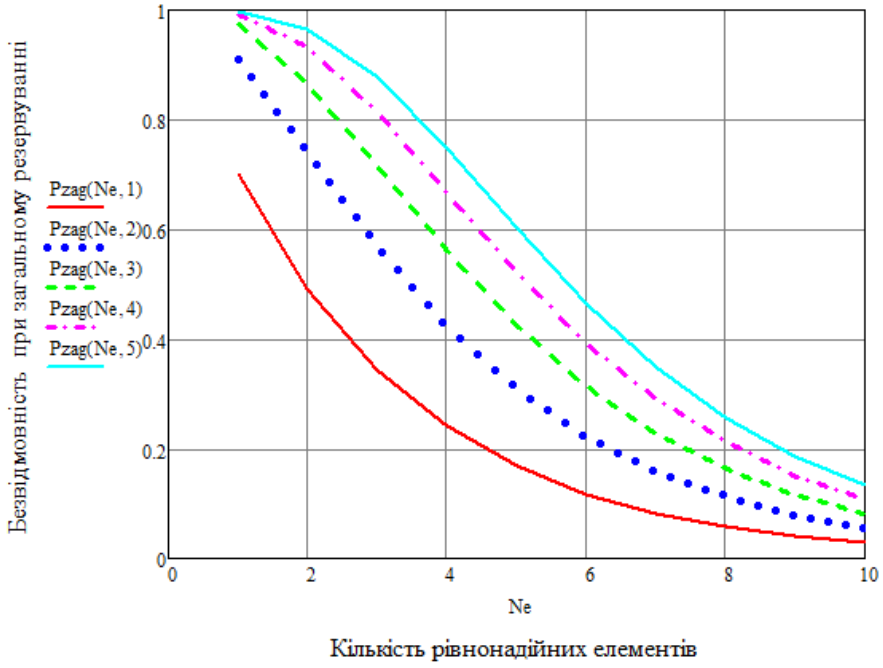
З урахуванням вираження (2.109) вираження (2.108) прийме вид

$$P_{\text{заг}} = 1 - \prod_{i=1}^{m}\left(1 - \prod_{i=1}^{N} p_i\right) = 1 - \prod_{i=1}^{m}\left(1 - \prod_{i=1}^{N}(1 - q_i)\right) \qquad (2.110)$$

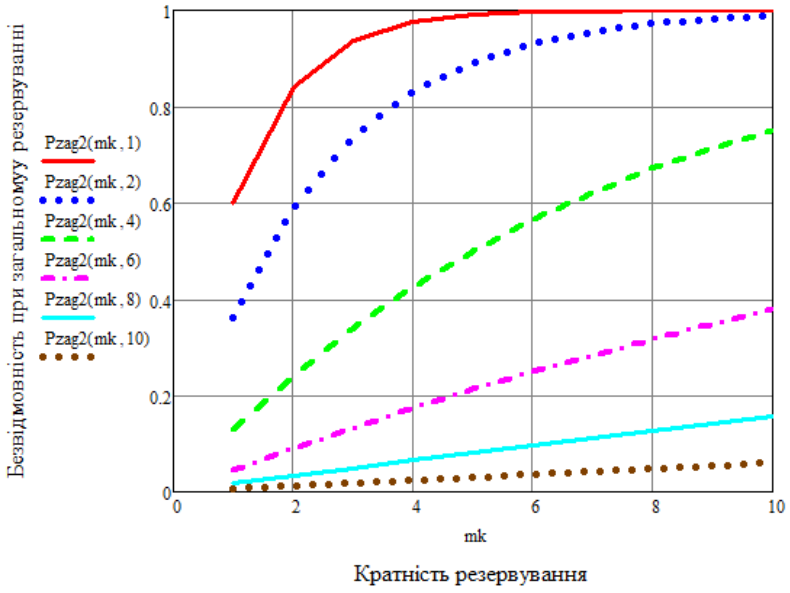
Для випадку рівнонадійних елементів вираження (2.10) можна) записати у вигляді

$$P_{\text{заг}} = 1 - [1 - p^N]^m = 1 - [1 - (1 - q)^N]^m \qquad (2.111)$$

З отриманих виразів випливає, щоймовірністьбезвідмовної роботи системи із загальним резервуванням при підвищенні числа послідовно з'єднаних елементів N зменшується до нуля, а при збільшенні числа m паралельних гілок (кратності резервування) суттєво збільшується (рис. 2.38 а), б)).



а)



б)

Рис. 2.38 – Залежність імовірності безвідмовної роботи об'єкта при загальному резервуванні від кількості N=1÷10 равнонадійних елементів p = 0,8 і кратності резервування m=1, 2, 3,4, 5 а);від кратності резервування m=1÷10, при кількості равнонадійних елементівN=1, 2, 4, 6, 8

Випадок роздільного резервування представлений на рис. 2.39.

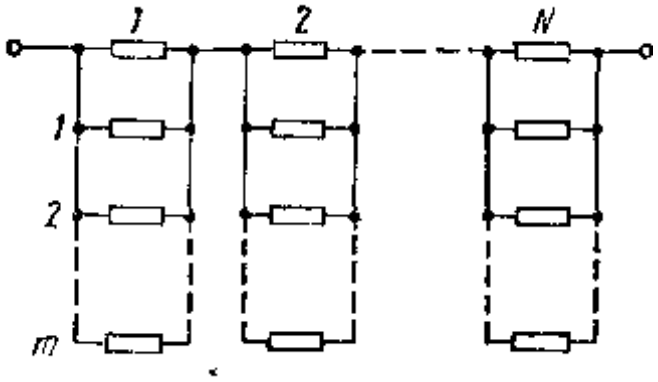


Рис. 2.39 – Схема роздільного резервування

У цьому випадку для окремої групи з *m*паралельно включених елементів може бути застосоване вираження (2.106):

$$P_j = 1 - \prod_{i=1}^{m}(1 - p_i) = 1 - \prod_{i=1}^{m}(q_i) \qquad (2.112)$$

Для ймовірності безвідмовної роботи всього об'єкта з роздільним резервуванням справедливо

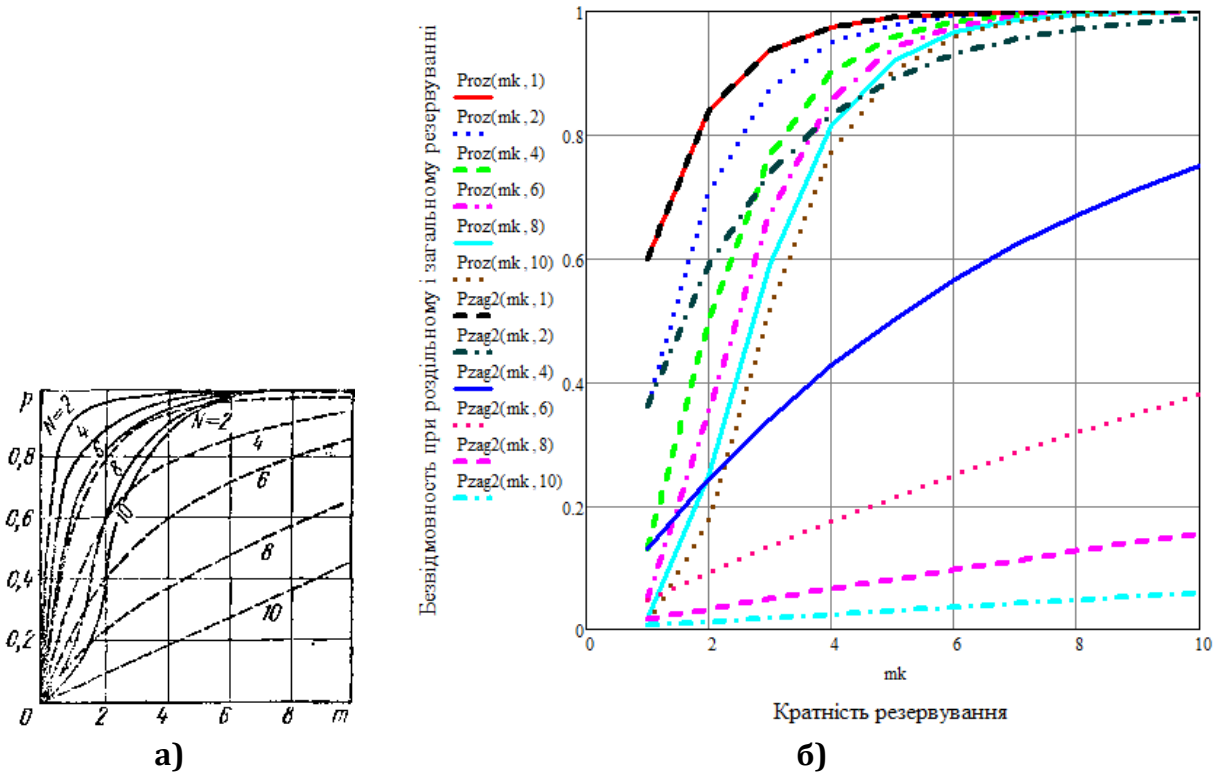
$$P_{\text{роз}} = \prod_{j=1}^{N} P_j = \prod_{j=1}^{N}[1 - \prod_{i=1}^{m}(1 - p_i)] = \prod_{j=1}^{N}[1 - \prod_{i=1}^{m}(q_i)] \qquad (2.113)$$

або для випадку рівнонадійних елементів

$$P_{\text{роз}} = [1 - (1 - p)^m]^N = [1 - q^m]^N \qquad (2.114)$$

З отриманого вираження (2.114) випливає, що ймовірність безвідмовної роботи наближається до одиниці при безмежному збільшенні числа елементів, що резервують, у групах, навіть якщо число послідовне з'єднаних груп також наближається донескінченності (на рис. 2.40 а, б) суцільні лінії), тобто роздільне резервування має певну перевагу перед загальним у змісті підвищення надійності.

Для змішаного резервування, знаючи число послідовно включених резервованих груп — N_i; і число паралельних резервних ланцюгів у кожній групі — m_j,користуючись виразами (2.11) і (2.13), можна оцінити ймовірність безвідмовної роботи. Порівнюючи між собою різні системи резервування, неважко дійти висновку, що при загальному резервуванні для повної відмови об'єкта досить, щоб у кожній, з ланцюгів вийшло з ладу по одному елементу.



а) **б)**

Рис. 2.40 – Залежність кімовірності безвідмовної роботи об'єкта при загальному й роздільномурезервуванні від значенькратності резервування m=1÷10 і кількості равнонадійних елементів N=1, 2, 4, 6, 8, 10

При роздільному й змішаному резервуванні відмова об'єкта відбувається тільки в тому випадку, якщо в кожній групі вийдуть із ладу всі елементи. Природно, що ймовірність цієї події мала.

Для кількісного порівняння з метою одержання більш простих виразів будемо вважатися, що всі елементи даного об'єкта рівнонадійни.

Скориставшись виразами (2.1121) і (2.114), напишемо для ймовірності появи відмови

$$Q_{\text{заг}} = [1 - p^N]^m = [1 - (1 - q)^N]^m$$
$$Q = 1 - [1 - (1 - p)^m]^N = 1 - [1 - q^m]^N \qquad (2.115)$$

Розкладемо праві частини рівності (2.115) у статечній ряд і враховуючи, що при нормальній експлуатації $q \ll$одержимо спрощені вираження:

$$\begin{cases} Q_{\text{заг}} \approx N^m q^m \\ Q_{\text{роз}} \approx N q^m \end{cases} \qquad (2.116)$$

Остаточно для кількісної оцінки способів резервування можна записати

$$Q_{\text{заг}}/Q_{\text{роз}} = N^m q^m / N q^m = N^{m-1} \quad (2.117)$$

З отриманого вираження випливає, що роздільне резервування дає виграш у безвідмовності. Це наочно видне на рис. 2.6, якщо зрівняти хід кривих при однакових значеннях m і N.

У практиці може виникнути завдання, зворотна розглянутим: відома ймовірність безвідмовної роботи однієї гілки $P = p^N$, потрібно знайти число паралельних гілок m.

Для випадку загального резервування скористаємося вираженням

$$1 - P_{\text{заг}} = 1 - P \quad (2.117)$$

Логарифмуємо праву й ліву частини рівності, одержимо

$$m_{\text{заг}} = \frac{\lg(1-P_{\text{заг}})}{\lg(1-P)} \quad (2.118)$$

де $P_{\text{заг}} = P_{\text{н}}$ — необхідна ймовірність безвідмовної роботи резервованого об'єкта.

Для випадку роздільного резервування скористаємося вираженням (2.13)

$$P_{\text{роз}}{}^{1/N} = 1 - (1-p)^{m_{\text{роз}}} \quad (2.119)$$

Логарифмуючи праву й ліву частини рівності, одержимо

$$m_{\text{роз}} = \frac{\lg(1-P_{\text{роз}}{}^{1/N})}{\lg(1-p)} \quad (2.120)$$

На закінчення відзначимо, що резервування може бути з відновленням будь-якого основного й резервного елемента в процесі експлуатації об'єкта, так зване *резервування з відновленням,* і без відновлення елементів, так зване *резервування без відновлення.* Сам резервний елемент може бути відновлюваним, тобто у випадку його відмови підлягає відновленню, і невідновлюваним..

2.6.3 Способи включення резерву

Існують три способи включення резерву: *стале, заміщувальне і ковзне* (див. рис. 2.1).

Стале резервування; паралельне резервування – резервування, в якому використовують навантажений резерв і в якому, якщо відмовляє будь-який елемент в резервованій групі, виконання об’єктом погрібних функцій забезпечується без перемикань рештою елементів.

Природно, що резервні елементи перебувають у такому ж режимі, як і основні, і їх ресурс роботи витрачається з моменту включення на роботу всього об'єкта. Тому що резервні елементи функціонують нарівні з основними, тобто несуть навантаження, те такий резерв називають н а в а н т а ж е н и м .

Навантажений резерв – резерв, що містить один чи декілька резервних елементів, які перебувають у режимі основного елемента.

Основними властивостями сталого резервування є: простота включення й миттєва готовність резерву до роботи, тому що немає необхідності в підключенні резерву замість основного об'єкта (елемента).

Недолік сталого резервування полягає в тому, що з появою відмов у резерві змінюються параметри всієї системи, а це в ряді випадків може привести до зміни режимів роботи. Безвідмовність системи з постійним резервуванням може бути визначена за допомогою виразів (2.110) і (2.112).

Резервування, при якому функції основного елемента передаються резервному тільки після відмови основного елемента, називають з а м і щ у в а л ь н и м р е з е р в у в а н н я м .

При заміщувальному резервуванні обов'язкова наявність комутуючого пристрою для підключення резервних елементів замість, що відмовили основних елементів.

К о в з н е р е з е р в у в а н н я - заміщувальне резервування, в якому група основних елементів резервується одним чи декількома резервними елементами, кожний з яких може замінити будь-який з елементів цієї групи у випадку його відмови.

Елементи, що резервують, можуть, перебувати в різних режимах*: навантаженому, полегшеному й ненавантаженому.*

Н а в а н т а ж е н и й р е з е р в – резерв, що містить один чи декілька резервних елементів, які перебувають у режимі основного елемента.

Навантажений резерв (як і при постійному резервуванні) має резервні елементи, що перебувають у тому ж режимі, що й основні елементи. Це дозволяє гранично скоротити час перекладу резервного елемента в робочий стан.

П о л е г ш е н и й р е з е р в – резерв, що складається з одного чи декількох резервних елементів, які перебувають у режимі меншого навантаження порівняно з основним елементом.

Полегшений резерв має резервні елементи, що перебувають у менш навантаженому режимі ніж основні (наприклад, в електровакуумних приладах включене розжарення, а анодна напруга не подана й т. п.). Ресурс роботи резервних елементів витрачається з моменту включення об'єкта в роботу, але інтенсивність витрати до підключення значно нижче чому в основних елементів. Тому закон розподілу часу їх безвідмовної

роботи трохи відмінний від розподілу часу безвідмовної роботи основних елементів.

Час переходу резервних елементів у робочий стан більше, чим при навантаженому резерві.

Ненавантажений резерв – резерв, що складається з одного чи декількох резервних елементів, які перебувають у ненавантаженому стані до початку виконання ними функцій основного елемента.

Ненавантажений резерв має резервні елементи, що практично не несуть навантажень. Ресурс роботи ненавантаженого резерву починає витрачатися тільки з моменту його включення. Закон розподілу часу безвідмовної роботи резервних елементів такий же, як і в аналогічних типів елементів у режимі зберігання. Час переходу резервних елементів у робочий стан найбільше.

Перевага заміщувального резервування полягає в тому, що більшою мірою може зберігатися ресурс роботи резервних елементів (полегшений і ненавантажений резерви), не змінюються режими роботи об'єкта (елементів) при відмовах, відпадає необхідність у спеціальних регулюваннях при відмовах, з'являється можливість використовувати один резервний елемент для резервування декількох однотипних основних елементів.

До недоліків потрібно віднести: необхідність комутуючого пристрою для підключення резерву, додаткового часу на перемикання резерву й вихід його на режим (полегшений і ненавантажений резерви). Включення резервних елементів може здійснюватися вручну або автоматично (автоматичне резервування).

Становить практичний інтерес облік впливу надійності комутуючого пристрою на загальну надійність резервованої системи (рис. 2.41).

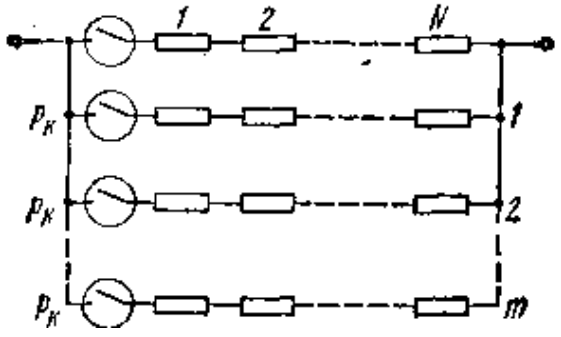


Рис. 2.41 – Схема реалізації ненавантаженого резерву

Імовірність успішного переходу на резерв – імовірність того, що перехід на резерв відбудеться без відмови об’єкта, тобто відбудеться за час, який не перевищує допустимого значення перерви у функціонуванні та (чи) без зниження якості функціонування.

Будемо вважатися відмови комутуючого пристрою й ланцюгів незалежними. Для цього випадку справедливо

$$P_{\text{р.з}} = P_{\text{рез}} P_{\text{к}} \tag{2.121}$$

де $P_{\text{рез}}$ — імовірність безвідмовної роботи ланцюгів резервування;

$P_{\text{к}}$— імовірність безвідмовної роботи комутуючого пристрою.

Скориставшись вираженням (2.121), для випадку загального резервування можна записати

$$P_{\text{р. з. заг}} = 1 - \prod_{i=1}^{m}\left(1 - P_{\text{к}} \prod_{i=1}^{N} p_i\right) = 1 - \prod_{i=1}^{m}\left(1 - (1 - Q_{\text{к}}) \prod_{i=1}^{N}(1 - q_i)\right) \tag{2.122}$$

Для випадку роздільного резервування вираження прийме вид

$$P_{\text{р. з. роз}} = \prod_{j=1}^{N} p_j = \prod_{j=1}^{N}[1 - \prod_{i=1}^{m}(1 - P_{\text{к}} p_i)] = \prod_{j=1}^{N}[1 - (1 - Q_{\text{к}}) \prod_{i=1}^{m}(q_i)] \tag{2.123}$$

де $P_j = 1 - \prod_{i=1}^{m}(1 - P_{\text{к}} p_i) = 1 - \prod_{i=1}^{m} Q_{\text{к}} q_i$

При виводі виразів (2.20) і (2.21) передбачалося, що комутуючі пристрої є у всіх ланцюгах і вони всі рівнонадійни.

Порівнюючи два способи резервування (загальне й роздільне), неважко дійти висновку, що при роздільному резервуванні знадобиться більша кількість комутуючих пристроїв. У той же час роздільне резервування дозволяє одержати істотні переваги в підвищенні безвідмовності в порівнянні із загальним резервуванням, дозволяє застосовувати більш гнучкі й економічні схеми резервування з використанням пристроїв для аналізу відмов і вибору резерву.

Внаслідок цього виникають певні вимоги до надійності комутуючих пристроїв, тому що їхня низька надійність може суттєво вплинути на надійність усього об'єкта. Очевидно, що роздільне резервування заміщенням буде тільки тоді виправданим, коли надійність у такий спосіб резервованого об'єкта буде не нижче надійності об'єкта із загальним резервуванням, тобто повинне виконуватися нерівність

$$P_{\text{роз}} > P_{\text{заг}} \tag{2.124}$$

Будемо вважатися гірший випадок, коли в системі загального резервування ймовірність безвідмовної роботи комутуючого пристрою дорівнює одиниці, а в об'єкті з роздільним резервуванням *Рк.* Для цього випадку нерівність (2.124) з урахуванням вираженій (2.121) і (2.123) можна записати

$$[1 - (1 - P_{\text{к}} p)^m]^N > 1 - [1 - (1 - q)^N]^m \tag{2.125}$$

При малих $q \ll$нерівність (2.124) прийме вид

$$[1-(1-P_{к}p)^{m}]^{N} > 1-(Nq)^{m} \qquad (2.125)$$

Вирішуючи отриману нерівність відносно $P_к$, одержимо

$$(1-P_{к}p)^{m} > [1-(Nq)^{m}]^{1/N} \qquad (2.126)$$

або

$$P_{к} > \frac{1-\left\{1-[1-(Nq)^{m}]^{1/N}\right\}^{1/m}}{p} = \frac{1-\left\{1-[1-N^{m}(1-p)^{m}]^{1/N}\right\}^{1/m}}{p} \qquad (1.127)$$

Як випливає із отриманих виразів, значення $P_к$ повинне бути більше ймовірності безвідмовної роботи складових елементів.

У ряді випадків об'єкт ЕРВ містить кілька груп однотипних основних елементів. Використовуючи резервування заміщенням, у цьому випадку немає необхідності мати таке ж кількість резервних елементів. Для резервування досить мати один або кілька резервних елементів (менше, ніж число основних в об'єкті).

Як відомо, заміщувальне резервування, в якому група основних елементів резервується одним чи декількома резервними елементами, кожний з яких може замінити будь-який з елементів цієї групи у випадку його відмови називають ковзним резервуванням.

На рис. 2.42 показана схема ковзного резервування. Ковзне резервування дозволяє при відносно невеликих витратах (тому що кількість резервних блоків менше кількості основних) і незначному збільшенні ваги й габаритів підвищити надійність об'єкта.

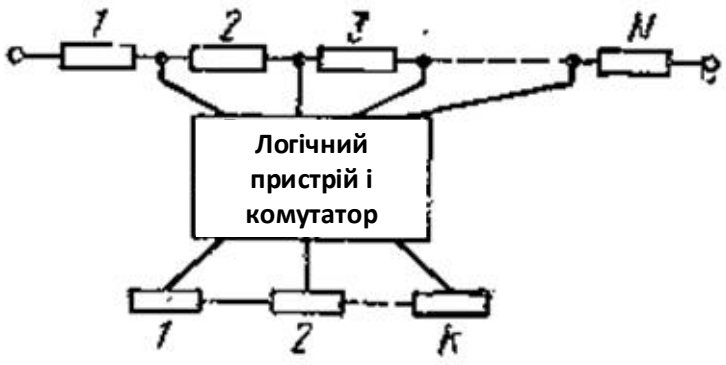


Рис. 2.42 – Схема реалізації ковзного резервування

Для невідновлюваного об'єкта при найпростішому потоці відмов і безвідмовному комутуючому пристрої ймовірність безвідмовної роботи при ковзному резервуванні визначається вираженням [8]

$$P_{\text{к}}(k) = \prod_{i=0}^{n-1} \Lambda_j \sum_{i=0}^{n-1} \frac{e^{-\Lambda_i}}{\Lambda_i \prod_{\substack{i=0 \\ i\neq 1}}^{n-1} (\Lambda_j - \Lambda_i)} \quad (2.128)$$

де k — число основних функціональне необхідних елементів;

n – 1 – число резервних елементів;

Λ_j – інтенсивність переходу об'єкта зі стану H_i у стан H_{i+1}.Кількість, станів відповідає числу елементів, що відмовили.

Для випадку рівнонадійних комутуючих пристроїв і ненавантаженого резерву вираження (2.128) прийме вид

$$P_c^{\text{н. н}}{}_c(k) = \text{e}^{-k(\lambda-\lambda_k)t} \sum_{i=1}^{n-1} \frac{[k(\lambda-\lambda_k)t]^i}{i!} \quad (2.129)$$

де λ_k — інтенсивність відмов комутуючого елемента.

Доцільність застосування ковзного резервування встановлюється порівнянням надійності об'єкта з резервом і без нього, т, е. P_c/P.

Слід зазначити ще одну важливу особливість резервування заміщенням — можливість відновлення резерву, що відмовив в той час, поки об'єкт працює з іншими резервними елементами. Це дозволяє суттєво підвищити ймовірність безвідмовної роботи, тому що наробіток на відмову завжди більше середнього часу відновлення. Отже, елемент, що відмовив, буде відновлений (якщо він відновлюваний) раніше, чим відбудеться чергова відмова в об'єкті, тобто в цьому випадку буде мати місце безперервне поповнення резервних елементів.

Умовою безвідмовної роботи такого об'єкта з відновлюваним резервом є вимога, щоб число блоків, що *відмовили,* Е не перевищило числа резервних *блоків* M, т. е, виконувалася нерівність $0 \leq E \leq M$.

Використовуючи методи теорії масового обслуговування [7, 81, неважко знайти ймовірність того, що в стаціонарному потоці, що встановився, на відновленні будуть перебуватирівноЕоб'єктів;

$$P_E = \frac{\left(\frac{N\lambda}{\mu}\right)^E}{\sum_{k=0}^{n}\left(\frac{N\lambda}{\mu}\right)^E} \quad (2.130)$$

де n — кількість резервних елементів ковзного резерву,

Вираження (2.130) справедливо для експонентного закону розподілу часу безвідмовної роботи й часу відновлення при наявності одного робочого місця для відновлення резервних елементів.

При ковзному резервуванні ймовірність безвідмовної роботи об'єкта визначається виходячи з наступних міркувань. Нехай об'єкт складається з N послідовних елементів і m резервних, при цьому будь-який резервний елемент за допомогою комутатора може заміщати кожної з N,

що відмовили основних елементів. об'єкт буде працездатним якщо з N+m елементів безвідмовно будуть працювати не менш чому N. За правилами комбінаторики кількість варіантів (число комбінацій), у яких з'явиться не більш k відмов рівно C_{N+m}^{k}, де $0 \le k \le m$

Для умови рівної надійності основних і резервних елементів $p_i = p$ імовірність появи не більш k відмов відповідає ймовірності безвідмовної роботи об'єкта при наскрізному резервуванні та з урахуванням надійності комутатора$p_{\text{ком}}$ складає

$$P_{\text{ковзн}} = p_{\text{ком}} \sum_{k=0}^{m} C_{N+m}^{k} p^{m+n-k} \cdot (1-p)^{k} \qquad (2.134)$$

2.6.4 Оптимізація резервування

Під оптимальним резервуванням розуміють резервування, що забезпечує одержання найбільшого ефекту підвищення надійності з найменшими витратами.

Під «витратами» будемо розуміти фактори, що визначають оптимальність резервування залежно від конкретних вимог. У більшості випадків ці фактори зв'язані між собою лінійною залежністю (кількість елементів і вартість, кількість елементів і споживана потужність живлення і т. п.) і задоволення одного з них спричиняє задоволення інших.

Говорячи про оптимальність резервування, у першу чергу потрібно розв'язати питання про вибір оптимального числа ділянок при роздільному резервуванні. Максимальна надійність апаратури з роздільним резервуванням може бути забезпечена тільки лише при деякому оптимальному числі елементів, що резервують, якщо відома ймовірність відмов комутуючих пристроїв і кратності резервування. Для вибору оптимального числа ділянок резервування використовуємо вираження (2.13). Розв'язок можна проводити або графічними, або аналітичними методами.

У першому випадку, задаючись різною кількістю ділянок, що резервуються *S.* будують сімейство кривих *P=f(S)* для різних значень *P* і $P_к$ і по них знаходять значення S_{opt}, відповідне до максимального значення ймовірності безвідмовної роботи.

У другому випадку дорівнюють нулю першу похідну dp/ds = 0 і вирішують отримане рівняння відносно S_{opt}. Випливає, однак, відзначити, що другий метод не завжди виявляється досить простим і зручним через громіздкість обчислень,

У деяких випадках для систем з малим часом роботи (літаки, ракети й т.п.), враховуючи, що $q_к \ll 1$ і $q_i \ll 1$ можна праву частину вираження розкласти в ряд по ступенях $q_к$ і q_i, зневажаючи членами вищих порядків малості,

Необхідно враховувати, що число ділянок резервування визначається не тільки бажанням одержати максимальну надійність, але й рядом конструктивних міркувань, які іноді можуть перешкоджати реаліза-

ції обчисленого значення S_{opt}. Тому в інженерній практиці при виборі S_{opt} необхідно враховувати обоє вимоги.

Здійснюючи оптимізацію резервування з урахуванням обмежень за вартістю, вазі або габаритам, слід розглядати два аспекти цього завдання:

1) забезпечення заданої надійності при мінімальних витратах на резервування;

2) забезпечення максимальної надійності при відомих припустимих витратах на резервування.

Суть першого завдання зводиться до відшукання мінімуму функції

$$C \sum_{i=1}^{N} (C_i m_i + C_0) \qquad (2.135)$$

при $P \geq P_{потр}$.

У другому випадку завдання зводиться до відшукання максимуму функції

$$P \prod_{i=1}^{N} p_i(m_i) \qquad (2.136)$$

при $C \leq C_{зад}$

У рівностях (2.135) і (2.136):

C — загальна вартість системи (об'єкта),

$C_{зад}$ — задана вартість системи (об'єкта);

C_i — вартість однієї ділянки резерву;

m_i — кількість резерву;

C_0 — початкова вартість системи (об'єкта) без резерву;

$p_i(m_i)$ — імовірність безвідмовної роботи *і-го* ділянки системи m_i резерву.

Реалізацію оптимізації системи (об'єкта) можна представити у вигляді наступного процесу: у якості вихідної розглядається система (об'єкт) без резерву, а потім відшукується ділянка для резервування найбільший результат, що дає. Далі відшукується нова ділянка резервування для нової системи (системи з однією зарезервованою ділянкою). Аналогічно процес триває доти, поки не буде задоволена умова однієї із завдань. Більш докладно ідеї оптимального резервування викладені в літературі по теорії надійності.

На закінчення необхідно відзначити, що вибір критерію оцінки оптимальності залежить від конкретних умов, тобто обліку конкретних домінуючих факторів. Так, для бортової апаратури ракет, почасти літаків факторами, що домінують, будуть габарити й вага, а не вартість.

2.6.5 Види резервування в засобах інформаційних технологій

В засобах інформаційних технологій застосовуються чотири основні види резервування:

- Апаратне резервування, наприклад, дублювання (рис. 2.43 – 2.45);

- Інформаційне резервування, наприклад — методи виявлення і корекції помилок;
- Почасове резервування, наприклад, методи альтернативної логіки;
- Програмне резервування, застосування незалежних функціонально рівноцінних програм.

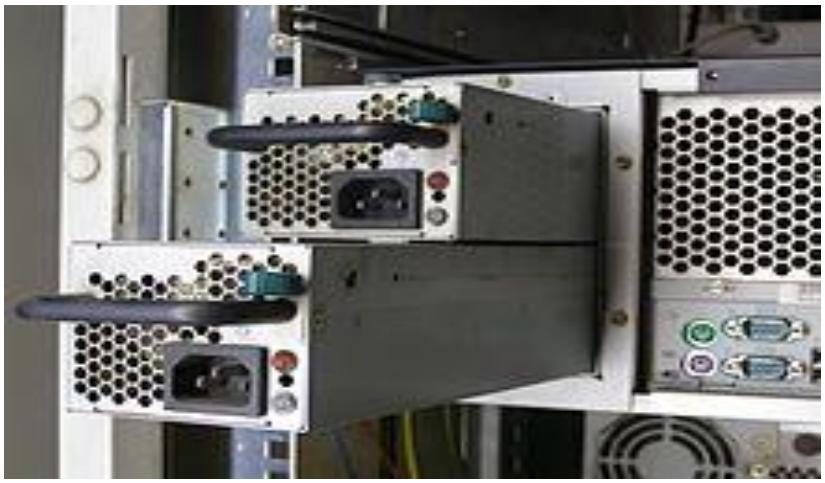


Рис. 2.43– Резервування блоку живлення (дублювання).



Рис. 2.44 – Резервування серверу промислової задачі.



Рис. 2.45– Резервування жорстких дисків

Висновки за розділом 2

Резервування – спосіб забезпечення надійності об'єкта за рахунок використання додаткових засобів та (або) можливостей, надлишкових відносно мінімально необхідних для виконання потрібних функцій.

Доцільність застосування резервування визначається наступними чинниками:

- початковим рівнем надійності комплектуючих виробів;
- заданим часом експлуатації;
- наявністю ефективної системи контролю і періодичністю проведення профілактики;
- можливостями використовування менш надмірних методів підвищення надійності.

Резервування широко застосовується на небезпечних промислових об'єктах, у багатьох випадках його необхідність диктується вимогами промислової безпеки або державних правил і стандартів.

В резервованому виробі відмова наступає тоді, коли вийдуть з ладу основний пристрій (елемент) і всі резервні пристрої (елементи). Група елементів вважається резервованою, якщо відмова одного або декількох її елементів не порушує нормальної роботи схеми (системи), а справні елементи, що залишилися, виконують ту ж задану функцію. Таке резервування називається функціональним.

Кратність резервування — відношення числа резервних елементів до числа основних елементів пристрою. Кратність резервування прийнято позначати *m*. Наприклад, якщо *m=3*, то це означає що: основний пристрій — одне, число резервних пристроїв — три, а загальне число пристроїв рівно чотирьом. Однократне резервування називається дублюванням.

За станом резервних елементів до моменту включення їх в роботу розрізняють резерв навантажений (гарячий**)** — резервні елементи навантажені так само, як і основні; полегшений (який чекає) — резервні елементи навантажені менше ніж основні; і ненавантажений (холодний) — резервні елементи практично не несуть навантаження. Використовування полегшеного або ненавантаженого резерву дає можливість понизити витрату енергії, споживаною резервованою системою і збільшити надійність апаратури ($T_{ср\ р\ ненагр} > T_{срр\ обл} > T_{срр\ нагр}$), оскільки надійність резервних пристроїв вище, ніж основних. Проте слід враховувати, що перерва на перемикання з основного пристрою на резервний допустима не у всіх схемах.

Залежно від масштабу і прийнятої одиниці резервування розрізняють загальне, в якому резервується об'єкт в цілому, і роздільне (поелементне), в якому резервуються окремі елементи об'єкта чи їх групи (блоки, вузли, елементи); можливо також різних видів резервування в

одному об’єкті — так зване змішане резервування.

Окремим випадком змішаного (поелементного) резервування є різновид заміщувального резервування – ковзне резервування, в якому група основних елементів резервується одним чи декількома резервними елементами, кожний з яких може замінити будь-який з елементів цієї групи у випадку його відмови, що можна використовувати, якщо резервувати групу однакових елементів.

Список використаних джерел

Керівні документи

1. В. О. Собина, Д. В. Тарадуда, М. М. Піксасов, Л. В. Борисова, О. В. Закора, А. Б. Фещенко, М.В. Маляров, Д. Л. Соколов, Дослідження проблем функціонування системи зв’язку ДСНС, використання засобів телекомунікацій та інформатизації в системі ДСНС, шляхів їх розвитку із застосуванням сучасних телекомунікаційних та інформаційних технологій, Звіт про НДР: № держреєстрації 0119U001009, Х.: НУЦЗУ, 2020. – 85 с. Режим доступу: http://ndr.dsns.gov.ua/?p=7135 .

2. Порядок організації роботи відомчої цифрової телекомунікаційної мережі ДСНС Наказ ДСНС 23.10.2019 № 608.

3. Наказ МВС України 08.02.2019 № 93 Про затвердження Інструкції щодо практик чи процедур проектування, дослідження, введення в експлуатацію, експлуатації та технічного обслуговування (супроводження) автоматизованих систем централізованого оповіщення.

4. Наказ МВС України 20.10.2017 № 870 Про затвердження Положення про автоматизовану інформаційну систему оперативного призначення єдиної інформаційної системи МВС.

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

6. ДСТУ 2860-94 Надійність техніки. Терміни та визначення

Література

7. Бондаренко В.Г. Технічна експлуатація систем і мереж зв'язку. Підручник для студентів вищих навчальних закладів за напрямком "Телекомунікації" -700с з .іл. Бібліогр. в кінці розд. ISDN 966-575-039-9– К. ДУІКТ, К-2002, 700с.

8. Вишнівський В.В., Василенко В.В., Гніденко М.П., Звенігородський О.С.,Зінченко О.В., Іщеряков С.М.Основи надійності та діагностики інформаційних систем. Навчальнийпосібник підготовлено для самостійної роботи студентів та аспірантів вищихнавчальних закладів. Київ: ННІІТ ДУТ, 2020. – 184 с.

9. Надежность технических систем: Справочник / Ю. К. Беляев, В. А. Богатырев, В. Болотин и др.; Под ред. И. А. Ушакова. — М.: Радио связь, 1985. — 608 с., ил.

Питання та завдання для самостійного контролю знань

Теми аналітичних оглядів

1. Аналітичний оглядзагальної структури, складу архітектури ЄНСЗУ.
2. Аналітичний огляд функціональної структуритехнічної експлуатаціїтелекомунікаційної мережі ЄНСЗУ.
3. Аналітичний огляд автоматизованої системи технічного і оперативно-технічного обслуговування обладнання, апаратури, трактів і каналів передавання первинної мережіЄНСЗУ.
4. Аналітичний огляд структури побудови лінії передачі і утворення мережного трактуЄНСЗУ.
5. Аналітичний огляд методів і основних параметрів системи технічної експлуатаціїЄНСЗУ.
6. Класифікація і аналітичний огляд методів розрахунків безвідмовності.
7. Аналітичний огляд впливу різних факторів на показники надійності.
8. Аналітичний огляд загальних методів підвищення надійності.
9. Аналітичний огляд видів резервування.
10. Аналітичний огляд залежності імовірності безвідмовної роботи об'єкта при загальному й роздільному резервуванні.
11. Аналітичний огляд способів включення резерву.
12. Аналітичний огляд оптимізації резервування.

Контрольні питання

1. Загальні положення з технічної експлуатації телекомунікаційних систем та мереж ЄНСЗУ.
2. Введення в експлуатацію технічних засобів телекомунікаційних системДСНС
3. Введення в експлуатацію програмних засобів інформаційних систем ДСНС.
4. Технічне обслуговування (супровід) та регламентні роботи телекомунікаційних систем та інформаційних технологій.
5. Зберігання телекомунікаційного обладнання та засобів інформатизації .
6. Контроль за станом систем, технічних і програмних засобів.
7. Основні поняття й визначення надійності електрорадіовиробів.

8. Види несправностей, стани технічного об’єкту.
9. Властивості надійності.
10. Види з’єднання елементів в схемах надійності об’єктів.
11. Значення показників надійності.
12. Показники безвідмовності.
13. Залежність інтенсивності відмов від часу експлуатації.
14. Характеристика процесу експлуатації відновлюємого об’єкту.
15. Розподіл часу безвідмовної роботи за законом Вейбулла-Гнеденка.
16. Експонентний розподіл часу безвідмовної роботи.
17. Нормальний розподіл часу безвідмовної роботи.
18. Розподіл часу безвідмовної роботи за закономПуассона.
19. Рівномірний розподілчасу безвідмовної роботи.
20. Розподіл часу безвідмовної роботи за законом.
21. Поняття і показники довговічності.
22. Поняття і показникиремонтопридатності.
23. Поняття і показникизбережуваності.
24. Поняття комплексних показників надійності.
25. Залежність імовірності безвідмовної роботи об’єкта при загальному резервуванні.
26. Залежність імовірності безвідмовної роботи об'єкта при роздільному резервуванні
27. Види резервування в інформаційних системах.

РОЗДІЛ 3. КІНЦЕВЕ ОБЛАДНАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Кінцеве обладнання – обладнання, призначене для з'єднання з пунктом закінчення телекомунікаційної мережі з метою забезпечення доступу до телекомунікаційних послуг [1-4].

Основним елементом кінцевого обладнання ВЦТМ ДСНС є персональний комп'ютер (ПК), тому в даному розділі ретельно розглянемо систему сучасного ПК.

3.1 Корпуси й блоки живлення ПК

3.1.1 Корпуси ПК

У корпусі знаходяться усі внутрішні компоненти настільного комп'ютера, такі як блок живлення, материнська плата, центральний процесор (ЦП), пам'ять, дискові накопичувачі й різні плати адаптерів [5-8].

Як правило, корпусу комп'ютерів виготовляють із пластику, сталі або алюмінію.

Корпус забезпечує розміщення, захист і охолодження внутрішніх компонентів.

Формфактор пристрою – це його конструкція й зовнішній вигляд.

Корпуси настільних комп'ютерів випускаються в різних формфакторах, включаючи зазначені нижче.

Горизонтальний корпус – такі корпуси були популярні на зорі розвитку комп'ютерних систем. Корпус розташовувався на столі горизонтально, а на нього ставився монітор. Корпуси такого формфактора вже не популярні й практично не використовуються.

Повнорозмірний вертикальний корпус (Full-Size Tower, FST) (див. рис. 3.1) – корпус комп'ютера, розташований вертикально. Звичайно його встановлюють на підлогу поруч зі столом або під ним. У ньому з легкістю можна розмістити додаткові компоненти, такі як дискові накопичувачі, плати адаптерів і багато чого іншого. До нього підключаються зовнішні клавіатура, миша й монітор.

Компактний вертикальний корпус (див. рис. 3.2) – зменшена версія повнорозмірного вертикального корпусу. Такі корпуси найчастіше зустрічаються в корпоративному середовищі. Такі корпуси також називають моделями малого формфактора **(Small Form Factor, SFF**), або мінікорпусами. Його можна розмістити як на робочому столі, так і на підлозі. У ньому можна розмістити обмежена кількість додаткових компонентів. До нього підключаються зовнішні клавіатура, миша й монітор.

Моноблок (див. рис. 3.3) – усе компоненти такого комп'ютера розміщаються в корпусі монітора. Звичайно такі комп'ютери оснащуються сенсорним дисплеєм, а також вбудованими динаміками й мікрофоном. Залежно від моделі можливості установки додаткових компонентів об-

межені або зовсім відсутні. До нього підключаються зовнішні клавіатура, миша й блок живлення.



Рис. 3.1 – Корпус комп'ютера, розташований вертикально



Рис. 3.2 – Зменшена версія повнорозмірного вертикального корпусу (модель малого формфактора)



Рис. 3.3 – Моноблок

Примітка. Цей список не є вичерпним, оскільки в багатьох виробників є власна термінологія відносно моделей корпусів. До них ставляться вертикальний корпус дуже великого розміру, повнорозмірний вертикальний корпус («повна вежа»), вертикальний корпус середнього розміру («середня вежа»), міні-корпус («міні-вежа»), корпус-куб і багато інші.

Під час роботи компоненти комп'ютера виділяють багато тепла, тому в корпусах є вентилятори для подачі повітря й відведення тепла. Повітря, проходячи повз нагріті компоненти, відбирає в них тепло й ви-

ходить із корпусу. Цей процес охороняє компоненти комп'ютера від перегріву. Корпуси також допомагають захистити обладнання від ушкоджень, викликуваних статичною електрикою. Внутрішні компоненти комп'ютера заземлені, будучи прикріпленими до корпусу.

Примітка. Корпус ще називають шасі, шафою, тауером, вежею, системним блоком або «системніком» (якщо в ньому встановлені компоненти).

3.1.2 Блоки живлення ПК

В електричну розетку подається перемінний струм (alternating current, AC). Однак для роботи всіх компонентів комп'ютера необхідний постійний струм (direct current, DC). Для перетворення живлення перемінного струму в низьковольтний постійний струм служить блок живлення, як на рис. 3.4.



Рис. 3.4 – Блок живлення комп’ютера

Нижче перелічені блоки живлення різних формфакторів, які одержали розвиток із часом.

Advanced Technology (AT) – вихідний блок живлення для застарілих комп'ютерних систем, який у цей час також є застарілим.

AT Extended (ATX) – оновлена версія блоків живлення AT, проте теж уже застаріла.

ATX12V – блок живлення цього формфактора найбільше часто використовується в сучасних комп'ютерах. Він оснащений додатковим силовим з'єднувачем для окремого живлення ЦП на материнській платі. Існує кілька версій ATX12V.

EPS12V – такі блоки живлення споконвічно розроблялися для мережних серверів, однак у цей час вони одержали широке розповсюдження у високотехнологічних моделях настільних комп'ютерів.

Блок живлення оснащується роз'ємами різних типів, як показано на рис. 3.5.



Рис. 3.5 – Роз'єми блоку живлення

Вони використовуються для живлення різних внутрішніх компонентів, таких як материнська плата й дискові накопичувачі. Роз'єм оснащені «ключами» і спроектовані так, щоб їх неможливо було вставити неправильно. У табл. 3.1 представлений опис найпоширеніших силових роз'ємів.

Таблиця 3.1 – Опис найпоширеніших силових роз'ємів

Найпоширеніші роз'єм блоку живлення	
Роз'єм	**Опис**
20– або 24-контактний роз'єм	Підключається до материнської плати 24-контактне роз'єм має два ряди по 12 контактів у кожному 20-контактне роз'єм має два ряди по 10 контактів у кожному
Роз'єм живлення SATA із ключем	Призначений для живлення дискових накопичувачів Роз'єм ширше й тонше, чим роз'єм Mo1ex
Роз'єм Molex із ключем	Призначений для живлення жорстких дисків, приводів оптичних дисків і інших пристроїв
Роз'єм Berg із ключем	Служить для підключення застарілих приводів гнучких дисків Роз'єм менше, чим роз'єм Mo1ex
4– або 8-контактний роз'єм для додаткового живлення	Роз'єм має два ряди по 2 або 4 контакту й служить для живлення різних областей материнської плати Роз'єм для додаткового живлення має ту ж форму, що й основний, але його розмір менше
6– або 8-контактний силовий роз'єм PCIe	Роз'єм має два ряди по 3 або 4 контакту й служить для живлення внутрішніх компонентів

Різні роз’єм служать для подачі живлення різної напруги. Як правило, блоки живлення дають напруга в 3,3 В, 5 У и 12 В. Напруга в 3,3 У и 5 В звичайно подається на цифрові мікросхеми, а напруга в 12 В – на двигуни дискових накопичувачів і вентилятори. У табл. 3.2 представлені відомості про різні типи напруги, що подаються з блоку живлення. Блок живлення може мати одну, дві або кілька шин живлення для певної напруги.

Шина живлення або лінія – це друкована плата усередині блоку живлення, до якої підключені кабелі, що йдуть назовні. У блоці живлення з однієї шиною всі роз’єм підключені до одній друкованій платі, а в блоці живлення з декількома шинами для кожного роз’єм є власна друкована плата. Комп'ютер здатний працювати при незначних коливаннях напруги мережі, однак значне відхилення напруги може викликати збій блоку живлення.

Таблиця 3.2 – Відомості про різні типи напруги, що подаються з блоку живлення

Напруга блоку живлення					
Напруга	**Колір проводу**	**Використання**	**Стандарт блоку живлення**		
			AT	**ATX**	**ATX12V**
+ 12 В	**Жовтий**	Двигуни дискових приводів, вентилятори, що прохолоджують пристрої й гнізда системної шини.	•	•	•
-12 В	**Синій**	Деякі види схем послідовних портів і ранні типи програмувальної пам'яті «тільки для читання» (ЕППТЧ).	•	•	•
+3,3 В	**Жовтогарячий**	Більшість сучасних ЦП, деякі види системної пам'яті й відеокарти AGP.		•	•
+5 В	**Червоний**	Материнська плата, Baby AT і ранні типи ЦП, а також багато компонента материнської плати.	•	•	•
-5 В	**Білий**	Плати шини ISA і ранні типи програмувальної пам'яті «тільки для читання» (ЕППТЧ).	•	•	•
0 В	**Чорний**	Земля – контакт для створення повного ланцюга.	•	•	•

3.1.3 Потужність блоку живлення

Потужність блоку живлення звичайно виміряється у ватах (Вт). У табл. 3.3 представлений опис чотирьох основних одиниць електрики, які повинен знати кожний комп'ютерний інженер.

В основному рівнянні, відомому також як закон Ома, напруга виражена як добуток сили струму на опір: **U = IR**. В електросистемі потужність дорівнює добутку напруги й сили струму: **P = UI**.

Для комп'ютерів звичайно використовуються блоки живлення з вихідною потужністю в діапазоні від 250 до 800 Вт. Проте, деяким ком-

п'ютерам потрібні блоки живлення потужністю 1200 Вт і більш. При зборці комп'ютера вибирайте блок живлення таким чином, щоб його потужності вистачило для всіх компонентів. Кожний компонент комп'ютера споживає певну потужність. Відомості про потужність наведені в документації, надаваної виготовлювачем устаткування. Здобувайте блок живлення, потужність якого перевищує потреби вже встановлених компонентів. Блок живлення з більш високою потужністю має більший запас, отже, до нього можна підключити додаткові пристрої.

Таблиця 3.3 – Чотири основні одиниці виміру електрики

Одиниця електрики	**Виміряється у...**	**Опис**
Напруга (U)	Вольти (В)	Одиниця виміру роботи, яку потрібно проробити для переміщення заряду з одного місця в інше. Блок живлення подає напруга декількох значень.
Сила струму (I)	Ампери (А)	Величина, відповідна до кількості електронів, що переміщаються по ланцюгу в секунду. Блок живлення комп'ютера подає різний струм на лінії з різною вихідною напругою
Опір (R)	Оми (Ом)	Фізична величина, що характеризує властивість провідника перешкоджати проходженню електричного струму. Більш низький опір дозволяє проходити по ланцюгу більшому струму. Гарний запобіжник має низький опір, майже рівне 0 Ом.
Потужність (P)	Вати (Вт)	Величина роботи, необхідної для переміщення електронів по електричному колу (напруга), помножена на кількість електронів, що переміщаються по цьому ланцюгу в секунду (струм). Комп'ютерні блоки живлення характеризуються по потужності

На задній панелі багатьох блоків живлення розташований невеликий перемикач, який називається перемикачем напруги (див. рис. 3.6). Він дозволяє встановлювати вхідну напруга блоку живлення рівним 110 В/115 В або 220 В/230 В. Блок живлення, оснащений таким перемикачем, називається блоком живлення, розрахованим на роботу із двома номінальними напругами. Необхідне положення перемикача напруги визначається країною, де використовується даний блок живлення. Невірний вибір положення перемикача напруги може привести до ушкодження блоку живлення й інших деталей комп'ютера. Якщо блок живлення не оснащений подібним перемикачем, він призначає необхідну напругу й переходить на нього автоматично.

УВАГА! Не розкривайте блок живлення. Електронні конденсатори, які перебувають усередині блоку живлення (показані на рис. 3.7), можуть утримувати заряд протягом тривалих періодів часу.

Додаткову інформацію про блоки живлення див. здесь.



Рис. 3.6 Задня панель блоку **живлення**



Рис. 3.7 Відкритий блок **живлення**

Блок живлення в комп'ютері (БЖ) – це самостійний імпульсний електронний пристрій, призначене для перетворення напруги змінного струму в ряд постійних напруг (+3,3/ +5 / +12 і -12) для живлення материнської плати, відеокарти, вінчестера й інших блоків комп'ютера.

Із блоку живлення комп'ютера виходить товстий джгут проводів різного кольору й на перший погляд, здається, що розібратися з розпіновкою роз'ємів неможливо. Але якщо знати правила колірного маркування проводів, що виходять із блоку живлення, то стане зрозуміло, що означає колір кожного проводу, яка напруга на ньому є присутнім і до яких вузлів комп'ютера проводу підключаються.

Довідкові дані колірного маркірування, величини напруг і розмаху пульсацій на роз'ємах БЖ знаходяться у табл. 3.4.

Таблиця 3.4 – Колірне маркірування, величини напруги і розмаху пульсацій на роз'ємах БЖ

Таблиця колірного маркірування проводів, вихідних напруг і розмаху пульсацій БЖ АТХ							
Вихідна напруга, В	**+3,3**	**+5,0**	**+12,0**	**-12,0**	**+5,0 SB**	**+5,0 PG**	**GND**
Колірне маркування проводів	**жовтогарячий**	**червоний**	**жовтий**	**синій**	**фіолетовий**	**сірий**	**чорний**
Припустиме відхилення, %	±5	±5	±5	±10	±5	–	–
Припустима мінімальна напруга	+3,14	+4,75	+11,40	-10,80	+4,75	+3,00	–
Припустима максимальна напруга	+3,46	+5,25	+12,60	-13,20	+5,25	+6,00	–
Розмах пульсації не більш, мВ	50	50	120	120	120	120	–

Проводи одного кольору, що виходять із блоку живлення комп'ютера, припаяні усередині до одній доріжці друкованої плати, тобто з'єднані паралельно. Тому напруга на всіх проводи одного кольору однакової величини.

Напруга +5 В SB (Stand-by) – (проводу фіолетового кольору) виробляє вбудований у БП самостійне малопотужне джерело живлення виконаний на одному польовому транзисторі й трансформаторі. Ця напруга забезпечує роботу комп'ютера в черговому режимі й служить тільки для запуску БЖ. Коли комп'ютер працює, то наявність або відсутність напруги +5 В SB ролі не відіграє. Завдяки +5 В SB комп'ютер можна запустити натисканням кнопки «Пуск» на системному блоці або дистанційно, наприклад, із Блока безперебійного живлення у випадку тривалої відсутності живлячого напруги 220 В.

Напруга +5 В PG (Power Good) – з'являється на сірому проводі БЖ через 0,1-0,5 секунд у випадку його справності після самотестування й служить роздільним сигналом для роботи материнської плати.

При вимірі напруги «мінусової» кінець щупа приєднує до **чорного** проводу (загальному), а «плюсової» – до контактів у роз’ємі. Можна проводити виміри вихідних напруг безпосередньо в працюючому комп'ютері.

Напруга мінус 12 В (проводу синього кольору) необхідно тільки для живлення інтерфейсу RS-232, який у сучасні комп'ютери не встановлюють.

Тому в блоках живлення останніх моделей ця напруга може бути відсутньою.

Відхилення живлячих напруг від номінальних значень не повинне перевищувати значень, наведених у табл.3.4. Як тестером або мультіметром вимірювати напругу Ви можете довідатися зі статті «Измерение напряжения».

При вимірі напруги на проводах блоку живлення, він повинен бути обов'язково підключений до навантаження, наприклад, до материнської плати або саморобного блоку навантаження.

Системні блоки перших персональних комп'ютерів комплектувалися Блоками живлення типу AT рис.3.8 . До материнської плати підходило одне роз’єм, що полягає із двох половинок. Його треба було вставляти таким чином, щоб чорні проведення були поруч. Живляча напруга в ці блоки живлення подавалося через вимикач, який установлювався на лицьовій панелі системного блоку. Проте, по виводу PG, сигналом з материнської плати була можливість включати й виключати блок живлення.

У цей час блоки живлення AT практично вийшли з експлуатації, однак їх з успіхом можна використовувати для живлення будь-яких інших пристроїв, наприклад, для живлення ноутбука від мережі, у випадку виходу з ладу його штатного блоку живлення, живити паяльник на 12 В, або низьковольтні лампочки, світлодіодні ленти і багато чого іншого. Головне не забувати, що блок живлення AT, як і будь-який імпульсний

блок живлення, не допускається включати в мережу без зовнішнього навантаження.



Рис.3.8 – Блок живлення типу АТ



Рис.3.9 – Колірна розпіновка роз’ємів блоку живлення комп'ютера

У сучасних комп'ютерах застосовуються блоки живлення АТХ, а для подачі напруги на материнську плату використовується 20 або 24 контактний роз’єм. 20 контактне роз’єм живлення використовувалося при переході зі стандарту АТ на АТХ. З появою на материнських платах шини PCI-express, на блоки живлення стали встановлювати 24 контактні и (рис.3.10).



Рис. 3.10 – 24 контактний роз’єм блоку живлення АТХ

20 контактне роз’єм відрізняється від 24 контактного роз’єм відсутністю контактів з номерами 11, 12, 23 і 24. На ці контакти в 24 контактному роз’ємі подається про дубльована вже наявна на інших контактах напруга.

Контакт 20 (білий провод) раніше служив для подачі –5 В в джерелах живлення комп'ютерів АТХ версій до 1.2. У цей час ця напруга для роботи материнської плати не потрібна, тому в сучасних джерелах живлення не формується й контакт 20, як правило, вільний.

Іноді блоки живлення комплектуються універсальним роз’ємом для підключення до материнської плати. Роз’єм складається із двох. Один є двадцяти контактним, а другий – чотирьох контактний (з номерами контактів 11, 12, 23 і 24), який можна пристебнуть до двадцяти контактному розніманню й, вийде вже 24 контактний рис. 3.11.

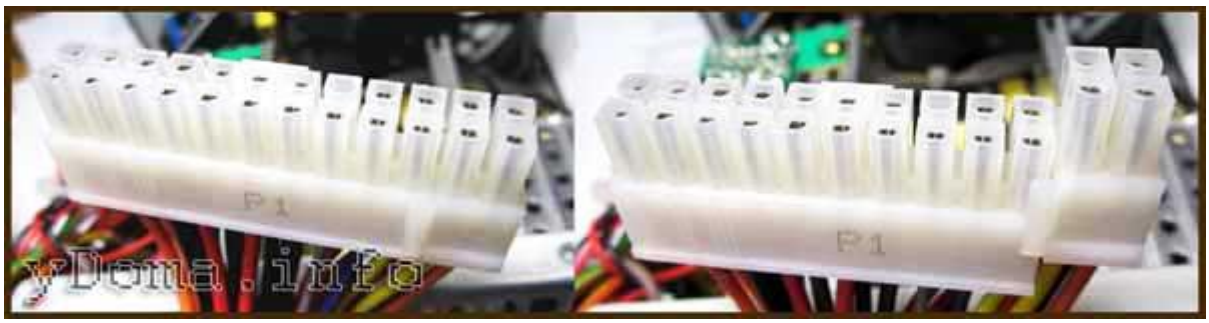


Рис. 3.11 – Універсальний роз’єм для підключення до материнської плати

Тому якщо будете міняти материнську плату, для підключення якої потрібний не 20, а 24 контактний роз’єм, то варто звернути увагу, цілком можливо підійде й старий блок живлення, якщо в його наборі роз'ємів є універсальний 20+4 контактний.

У сучасних Блоках живлення АТХ, для подачі напруги +12 В бувають ще допоміжні 4, 6 і 8 контактні роз’єм. Вони служать для подачі додаткової живлячої напруги на процесор і відеокарту.

Як видне на фото рис. 3.12. провідник, що живить, +12 В має **жовтий** колір із чорною частковою смугою.



Рис. 3. 12 – Чотирьох контактна вилка

Чотирьох контактна вилка нижче на фото (рис. 3.12 є самої довго застосовуваною. Вона служить для подачі живлячого напруги +5 і +12 В на знімні пристрої, вінчестери, дисководи й інші.

Але її вже почав витісняти більш сучасне роз'єм типу Serial ATA, у якому подається ще й напруга +3.3 В рис.3.13.

От ще один 4 контактне роз'єм, яке служить, а точніше дослужує, і призначений для підключення дисководу для читання й запису з 3,5 дюймових дискет.

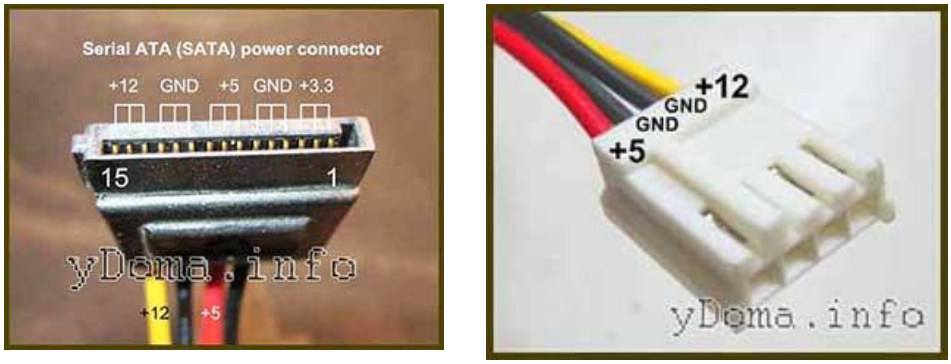


Рис.3.13 – Роз'єм типу Serial ATA

У сучасні комп'ютери дисководи Floppy disk не встановлюються, тому що вони морально застаріли.

3.1.4 Установка в блок живлення комп'ютера додаткового роз'єм для відеокарти

Іноді бувають, видалося б, безвихідні ситуації. Наприклад, Ви купили сучасну відеокарту, вирішили встановити в комп'ютер. Потрібний слот на материнській платі для установки відеокарти є, а підходящого роз'єм на проводах, для додаткового живлення відеокарти, що йдуть від блоку живлення немає. Можна купити перехідник, замінити блок живлення цілком, а можна самостійно встановити на блок живлення додаткове роз'єм для живлення відеокарти рис. 3.14. Це просте завдання, головне мати підходяще роз'єм, його можна побрати від несправного блоку живлення.



Рис. 3.14 – Додатковий роз'єм для живлення відеокарти

Спочатку потрібно підготувати проводи, що йдуть від роз'ємів для з'єднання зі зсувом, як показано на фотографії рис. 3.15. Додаткове роз’єм для живлення відеокарти можна приєднати до проводів, що йдуть наприклад, від блоку живлення на дисковід А. Можна приєднатися й до будь-яких інших проводів потрібного кольору, але з таким розрахунками, щоб вистачило довжини для підключення відеокарти, і бажане, щоб до них нічого більше не було підключено. Чорні проводи (загальні) додаткового роз’єм для живлення відеокарти з'єднуються із чорним проводом, а жовті (+12 В), відповідно із проводом жовтого кольору.

Проводи, що йдуть від додаткового роз’єму для живлення відеокарти, щільно овівають не менш чому трьома витками навколо проводу, до якого вони приєднуються. Якщо є можливість, то краще з'єднання пропаять паяльником. Але й без пайки в цьому випадку контакт буде досить надійним.

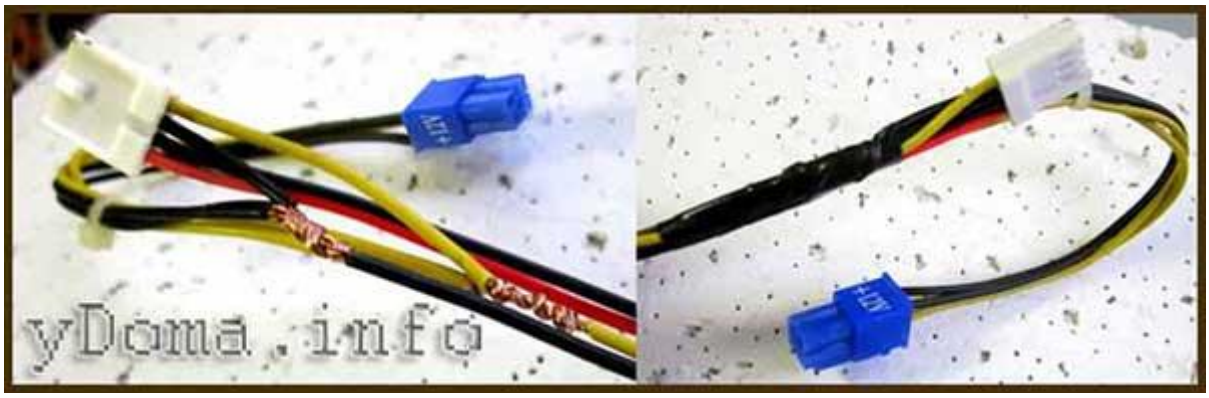


Рис. 3.15 – Підготовка проводів, що йдуть від роз'ємів

Завершується робота з установки додаткового роз’єм для живлення відеокарти ізолюванням місця з'єднання, кілька витків і можна підключати відеокарту до блоку живлення. Завдяки тому, що місця скруток зроблені на видаленні друг від друга, кожну скрутку ізолювати окремо немає необхідності. Досить покрити ізоляцією тільки ділянку, на якій оголені проводи.

3.1.5 Доробка роз’єм блоку живлення для підключення материнської плати

При виході з ладу материнської плати або модернізації (апгрейді) комп'ютера, пов'язаного із заміною материнської плати, неодноразово доводилося зустрічатися з відсутністю в блоку живлення роз’єм для подачі живлячого напруги з 24 контактами.

Наявне роз’єм на 20 контактів добре вставлявся з материнську плату, але працювати комп'ютер при такому підключенні не міг. Необхідний був спеціальний перехідник або заміна блоку живлення, що було дорогим задоволенням рис. 3.16.



Рис. 3.16

Але можна зекономити, якщо небагато самому попрацювати руками. У блоку живлення, як правило, є багато незадіяних роз'ємів, серед них може бути й чотирьох, шести або восьми контактний. Чотирьох контактне роз’єм, як на фотографії вище рис.3.16, відмінно вставляється у відповідну частину роз’єму на материнській платі, яка залишилася незайнятою при установці 20 контактного роз’єму.

Зверніть увагу, як у роз’ємі, що йде від блоку живлення комп'ютера, так і у відповідній частині на материнській платі кожний контакт має свій ключ, що виключає неправильне підключення. У деяких ізоляторів контактів форма із прямими кутами, а в інших кути зрізані. Потрібно роз’єм зорієнтувати, щоб він входив. Якщо не вийде підібрати положення, то зрізати кут, що заважає.

Окремо як 20 контактний, так і 4 контактний роз’єм вставляються добре, а разом не вставляються, заважають один одному. Але якщо небагато сточити прилеглі сторони обох роз'ємів напилком або наждаковим папером, те добре вставляться рис. 3.17.



Рис. 3.17

Після припасування роз'ємів корпусів можна приступати до приєднання проводів 4 контактного роз’єм до проводів 20 контактного. Ко-

льори проводів додаткового 4 контактного роз’єм відрізняються від стандартного, тому на них не потрібно обертати уваги й з'єднати, як показано на фотографії рис. 3.18.

Будьте вкрай уважними, помилки неприпустимі, згорить материнська плата! Близький лівий, контакт №23, на фото рис. 3.18 чорний, приєднує до червоного проводу (+5 В). Близький правий №24, на фото рис. 3.18 жовтий, приєднує до чорного проводу (GND). Далекий лівий, контакт №11, на фото рис. 3.18 чорний, приєднує до жовтого проводу (+12 В). Далекий правий, контакт №12, на фото рис. 3.18 жовтий, приєднує до жовтогарячого проводу (+3,3 В).



Рис. 3.18

Залишилося покрити місця з'єднання декількома витками ізоляційної стрічки й нове роз’єм буде готовий до роботи рис. 3.19.

Для того, щоб не замислюватися як правильно встановлювати збірне роз’єм в роз’єм материнської плати слід нанести за допомогою маркера мітку.



Рис. 3.19

3.1.6 Як подається на блок живлення комп'ютера живляча напруга від електромережі

Для того щоб постійні напруги з'явилися на кольорових проводах блоку живлення, на його вхід потрібно подати живлячу напругу. Для цього на стінці, де звичайно встановлений кулер, є трьох контактне роз’єм. На світлині це роз’єм праворуч угорі. У ньому є три штирі. На крайні за допомогою мережного шнура подається живляча напруга, а середній є заземлюючим, і він через мережний шнур при його підключенні з'єднується із заземлюючим контактом електричної розетки. Нижче на деяких блоках живлення, наприклад на цьому, установлений мережний вимикач рис. 3.20.



Рис. 3.20 – Задня стінка блоку живлення

У будинках старої будування електропроводка виконана без заземлюючого контуру, у цьому випадку заземлюючий провідник комп'ютера залишається не підключеним. Досвід експлуатації комп'ютерів показав, що якщо заземлюючий провідник не підключений, те це на роботу комп'ютера в цілому не позначається.

Мережевий шнур для підключення блоку живлення до електромережі являє собою трижильний кабель, на одному кінці якого є трьох контактне роз’єм для підключення безпосередньо до блоку живлення. На другому кінці кабелю встановлена вилка С6 із круглими штирями діаметром 4,8 мм із заземлюючим контактом у вигляді металевих смужок з боків її корпусу рис. 3.21.

Якщо розкрити пластмасову оболонку кабелю, то можна побачити три кольорові проведення. **Жовто** – **зелений** – є заземлюючим, а по ко-

ричневому й синьому (можуть бути й іншого кольору), подається живляча напруга 220В.

Жовто – **зелене** проведення в качані 36 приєднується до заземлюючих бічних смужок. Тому якщо прийде заміняти вилку, не забудьте про це. Усе про електричні качани й правилах їх підключення можете довідатися зі статті сайту «Электрическая вилка».



Рис. 3.21 – Мережевий шнур для підключення блоку живлення до електромережі

3.1.7 Про перетин проводів, що виходять із блоку живлення комп'ютера

Хоча струми, які може віддавати в навантаження блок живлення, становлять десятки амперів, перетин вихідних провідників, як правило, становить усього 0,5 мм^2, що допускає передачу струму по одному провіднику величиною до 3 А. Більш докладно про навантажувальну здатність проводів Ви можете довідатися зі статті «О выборе сечения провода для электропроводки». Однак усі проведення одного кольору запаяні на друкованій платі в одну точку, і якщо блок або модуль у комп'ютері споживає більший, ніж 3 А струм, через роз’єм підводить напруга по декільком проводам, включеним паралельно. Наприклад до материнської плати напруга +3,3 У и +5 В підводить по чотирьом проводам. Таким чином, забезпечується подача струму на материнську плату до 12 А.

3.1.8 Фактори при виборі блоку живлення

Багато з нас, як правило, починаються й закінчуються наші пошуки, дивлячись на один показник продуктивності джерела живлення: максимальне вихідне. Потім ми судимо різних джерел живлення, використовуючи тільки цей показник. Це безперечно не Рекомендований підхід, вибираючи блок живлення, який пасує вимогам потужності вашої системи є більш складним, чому просто порівнювати цифри проведення. У цьому розділі ми розглянемо й одержати загальну виставу про найбільш важливі характеристики живлення/функцій і що вони роблять.

Максимальна потужність

Блоки живлення в основному диференціюється по вихідній потужності, яка цитує по "максимальній потужності" на виході. Максимальна потужність-це не просто число, це також дає вистава про те, як багато пристроїв (і який тип пристроїв, з погляду енергоспоживання) блок живлення могтиме прокормити.

Однак, максимум одна цифра потужності не достатньо, щоб визначити, чи є блок живлення здатний диску вашого комп'ютера. Кожна напруга рейки вимагає уваги, але найбільше уважності повинен іти на +12В, із процесора й відео-карти Рсіе одержують свою владу від них. Блок живлення повинен видавати не менш 18А на +12В для основний актуальну комп'ютеру; більш 24А для системи з одним ентузіастом-відеокарта; і не менш 34А, коли справа доходить до високого класу, як що/Кроссфайр системи. На виході показник струму ми говоримо тут-це комбінований показник для блоків живлення пропонує більше чім одну +12В. Звичайно, ця загальна кількість вихід треба шукати, і не завжди можна додати на+12В, щоб розрахувати сукупний обсяг виробництва. Наприклад, БЖ із написом з написом рейки +12В1@18А, +12V2@16А може мати тільки 30А комбіновану. Вихідна потужність замість 34А. Шукати цю інформацію в докладні специфікації товару або на інформаційній етикетці БЖ.

Якщо ви збираєтеся працювати в конфігурації SLI/Crossfire конфігурацій, будь ласка, переконаєтеся, що +12В надати не менш 34А в комбінації. Різні блоки живлення мають різне маркування – деякі показують максимальну силу струму, представленою на кожної напрямної, а деякі надають максимальну сумарну. Максимальна потужність, наприклад 396W, який рівний 396W / 12В = 33А.

Безперервна й Пікова потужність

Зверніть увагу, що постійна потужність і Пікова потужність різні. Як правило, "Максимальна потужність" фігура живлення ставиться до постійного (стабільного) живлення блок живлення незмінно, у той час як Пікова потужність означає підвищений максимум (сплеск) потужність БЖ можна поставити, нехай і за дуже короткий проміжок часу (наприклад, 15 секунд).

Роз’єм

Роз’єм, надані ваше живлення визначити типи пристроїв, які можна підключати до нього. Тому надто важливо, що ви вибираєте блок живлення з усіма роз’ємами (тип і кількість) котрі вимагають ваші компоненти.

Основний силовий роз’єм й роз’єм живлення процесора

Основне роз’єм живлення використовується для підключення безпосередньо до материнської плати й блоку живлення. Два типи основні роз’єм живлення часто використовуються в сучасному блоці живлення: 20-контактний і 24-контактний формати. Як описано в розділах вище, 24-контактне основне роз’єм живлення було введено з ATX12У v2.0 специфіка-

ція, і усе більше й більше материнських плат, забезпечуючи 24-контактне роз'єм живлення розетки (багато материнських плат з 24-pin сокет однаково може працювати з 20-контактним роз'єм джерела живлення) рис. 3.22.

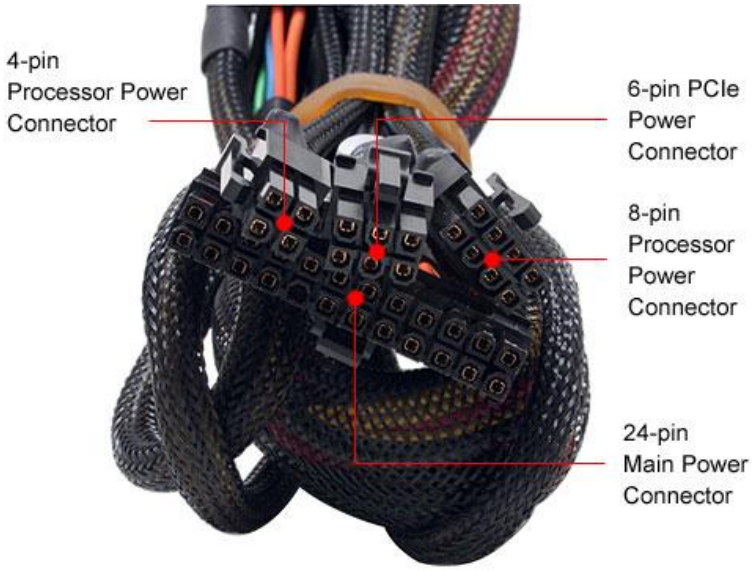


Рис. 3.22

Щоб забезпечити сумісність зі старими материнськими платами з 20-контактне роз'єм живлення конструкції, деякі блоки живлення дають 20+ 4-контактного роз'ємів живлення. Як на зображенні вище, цей тип роз'єм живлення дуже універсальні й може легко використовуватися з 20-контактний і 24-контактний материнської плати рис. 3.23.

Процесор роз'єм живлення (+12В роз'єм живлення) повинні бути підключені також до материнської плати й подає живлення безпосереднє до процесора. Існують також різні 4-контактний і 8-контактний (1,2 мм) роз'єм – 4-контактний Тип частіше використовується, у той час як 8-контактне роз'єм можна знайти на деякі материнські плати (ви усе ще можете використовувати потужність 4-контактне роз'єм на багато 8-контактний материнських плат) рис. 3.24.



Рис 3.23 – 20-контактний і 24-контактний роз'єм материнської плати



Рис 3.24 – 20-контактний для 24-контактнго кабелю перетворювача (ліворуч) і 4-контактний для 8-контактного кабелю живлення перетворювача (праворуч)

Зображення вище Рис 3.24 показує 20-контактний для 24-контактний кабель перетворювача (ліворуч) і 4-контактний для 8-контактний кабель живлення перетворювача (праворуч). Перший перетворить 20-контактне роз'єм живлення основне роз'єм живлення 24-контактне роз'єм, і, отже, може бути використаний на будь-якому 24-контактне роз'єм материнської плати (цей збіг, що має значення). Є також 24-контактний для 20-контактний і 8-контактний до 4-контактний конвертер кабелі також доступні.

Інші роз'єми живлення

Є й інші роз'єм живлення від блоку живлення, включаючи роз'єм дисководу (А.К.А. міні-роз'єм), роз'ємів PCIe (для високопродуктивних відеокарт, 6-pin) і двох типів наведені нижче (Рис 3. 25., Рис 3. 26)



Рис 3.25 – 4-контактний периферійного роз'єм Molex



Рис 3.26 – Роз'єм SATA для SATA дисків

4-контактний периферійний роз'єм, також називаний Molex роз'єм, найбільше часто використовуваний тип роз'єму живлення в корпусі ПК і використовується для підключення жорстких дисків, оптичних приводів, окремі вентилятори й інші обладнання. Деякі нові обладнання з інтерфейсом SATA почали використовувати роз'єм живлення SATA, і багато джерел живлення забезпечують занадто роз'ємів SATA. Якщо живлення немає роз'ємів SATA, ви можете використовувати роз'єм для живлення SATA конвертер кабелі, щоб зробити роботу.

Будь ласка, переконаєтеся, що є досить роз'ємів на блоці живлення вам вибрати, як він повинен мати можливість для підключення й живлення всіх ваших обладнань. І звичайно, ви можете використовувати кабель-розгалужувач для підключення декількох обладнань до одному розніманню живлення (Molex або SATA роз'єм тільки).

3.1.9 PFC

PFC (корекція фактору сили) – це метод, який протидіє небажаних ефектів електричного навантаження (реактивної потужності), що робить коефіцієнт потужності менше 1. Коефіцієнт потужності (ПФ) розуміється відношення активної потужності (виміряється у Вт) до повної потужнос-

ті (множить напругу на струм вольти х ампери або ВА), який містить у собі як активну й реактивну потужність, а тільки активна потужність здатна робити роботу. Для блоку живлення, чим вище значення ПФ, тем краще він здатний перетворювати струм у корисній потужності.

Для житлових і комерційних користувачів, тільки активна потужність виміряється й заряджений (повна потужність виміряється й заряджений для промислових споживачів), тому ПФ БП не впливає прямо на електроенергію насправді. Однак, ПФ має значення в загальній картині, тому що, чим більше реактивна потужність, тем менше активна потужність може бути передана – це виразно порожня витрата енергії.

Блоки живлення без вбудованого ККМ ланцюга часто мають низькі значення ПФ, іноді нижче 0.60. Для блоків живлення із вбудованим ККМ схеми, є два типи ККМ використовується активний і пасивний. **Пасивний PFC** складається з компонентів, які не мають потреби в енергії, щоб працювати, наприклад, ферритовый сердечник котушки; і **активний PFC** використовує компоненти, такі як інтегральні схеми й транзистори, які дійсно потрібні сили для роботи. Пасивний PFC може привести до значень ПФ між 0.60 ~ 0.80, у той час як активний PFC здатний доправити 0.95 ~ 0.99.

Ефективність

Ефективність блоку живлення становить відсоток від загальної потужності постійного струму стосовно загальної вхідної потужності змінного струму. Частина губиться в процесі перетворення, в основному у вигляді тепла.

Цей показник прямо пов'язаний з ваших рахунків сили. Наприклад, якщо ваш комп'ютер споживає 300 Вт потужності, використовуючи блок живлення із ККД 85% буде потрібно близько 353W Споживана потужність, і на 70% БП потягне потужність 428W від стіни. Це не важко зрозуміти, скільки грошей ви збираєтеся платити, використовуючи низьку ефективність живлення, і це число, як правило, ростуть із часом.

Блоки живлення з високим ККД не тільки допоможе зберегти витрати – втрати тепла будуть значно нижче, а також, підвищивши надійність і довговічність, а також може допомогти зменшити шум як вентилятор може працювати на більш низьких швидкостях і забезпечувати достатнє охолодження.

Інші проблеми

Фани (вентилятори для охолодження)

Без електропостачання в цей час у стані досягтися 100% ККД, а значить завжди буде тепло під час роботи. Як правило, більш високий вихід БП у результаті більше тепла виробляється. Більшість джерел живлення використовують один або кілька вентиляторів для охолодження рис. 3.27.



Рис. 3.27 – Вентилятори для охолодження блоку живлення

Шум-Це завжди проблеми скрізь, де вболівальників. Деякі блоки живлення використовують більші вентилятори (діаметр 12см) на низьких обертах (обертів у хвилину), щоб зменшити шум. Виробники також використовують інші методи, щоб знизити рівень шуму, таких як автоматичне регулювання швидкості вентилятора залежно від температури – при БП стає жарке, швидкість вентилятора збільшується, і навіть може повністю зупинитися, якщо температура досить низька.

Є також деякі "безвентиляторні" блоки живлення, які використовують пасивне охолодження й не мають яких-небудь вентиляторів і інших, що рухаються частин рис. 3.28. Ці блоки живлення найчастіше збройні радіатори, які забезпечують більшу поверхню (внутрішніх і/або зовнішніх), а максимальна потужність цих моделей звичайно обмежені. "Безвентиляторний" блоки живлення роблять майже ніякого шуму, що робить їх надзвичайно привабливими для власного.



Рис. 3.28 – Безвентиляторний блок живлення

"Безвентиляторні" блокі живлення не рекомендується використовувати в системах з високими характеристиками споживання живлення, якщо температура навколишнього середовища дуже низька й вентиляція корпуса комп'ютера відмінна.

Модульна система

Модульна система дозволяє користувачеві вибрати тип і кількість роз'ємів живлення (в основному периферійні й SATA роз'єм живлення й PCIe), які будуть використовуватися. На рис. 3.29 знизу показаний блок живлення з модульною системою роз'ємів кабелю для забезпечення основного живлення й живлення процесора роз'єм за замовчуванням, тому що практично кожна система зажадає цих двох з'єднань. Інші силові кабелі (звичайно із блоку живлення) повинні бути підключені до наявної розетки в міру необхідності.



Рис. 3.29 – Блок живлення з модульною системою роз'ємів кабелю

Блок живлення з модульним здатність кабелю дозволяє зменшити кількість невикористовуваних роз'ємів живлення/кабелі у вашому випадку систему, і, як правило, сприяє охайніше й чистіше, дивлячись у випадку внутрішніх органів, а також кращого потоку повітря.

Підтримка SLI і Crossfire

SLI і Crossfire на системах вимагають могутніші джерела живлення, а дві або навіть більш відеокарти, особливо високого класу відео карти споживають набагато більше енергії, чім одиночна конфігурація Рис 3. 30.



Рис 3. 30 SLI і Cross fire ATI логотип

Тому багато SLI /сертифікованих поставок в Crossfire потужності стали доступні й здатні задовольнити вимоги до живлення мульті-відео-карт системи.

Якщо ви є користувачем SLI і Crossfire, а сли/сертифікований в Crossfire живлення може бути необхідно (деякі високоякісні блоки живлення без сли сертифікації/перехресний вогонь усе ще може забезпечити достатню потужність для підтримки конфігурацій SLI/Crossfire конфігурацій).

Захист від перенапруги

Захисту від перенапруги ставиться до ланцюга або механізму, який виключає блок живлення, якщо вихідна напруга перевищує задана межа напруги, яка часто вище, чим Номінальна вихідна напруга. Цей захист дуже важливий, оскільки висока вихідна напруги може привести до ушкодження компонентів комп'ютера, які підключені до джерела живлення.

Захист від перевантаження/захист від перевантаження

Схожі на захист від перенапруги, перевантаження по струму й захистом від перевантаження, схеми захисту блоку живлення й комп'ютера з вимиканням блоку живлення, коли немає надмірного струму або потужності навантаження визначається, у тому числі струмів короткого замикання.

3.1.10 Рекомендації по вибору блоку живлення

Важлива примітка: будь ласка, почніть із вибору блоку живлення, який підтримує ваша материнська плата Тип роз'єм (20 або 24-pin) і забезпечує достатню потужність, Роз'єм для підключення всіх ваших пристроїв.

Наші рекомендації спрямовані головним чином на максимальну потужність, оскільки ми вже ввели багато інших важливих функцій/аспектів у розділах вище. Будь ласка, прочитайте ці розділи, перш ніж вибрати свій БЖ, якщо Ви не зовсім знайомі з ними. У таблиці нижче представлена загальна (не точне) вистава про сучасну потребу в енергії кожного типу компонента. Ви можете додати все компоненти разом, і помножити споживну потужність на 1.4 ~ 1.5 (для компенсації пульсації й розширення) на основну максимальну потужність, яку ваш блок живлення повинен запропонувати табл. 3.5.

Таблиця 3.5 – Типове енергоспоживання компонентів

Component Typical Power Requirements	
Processor (Typical)	65W ~ 130W
Motherboard	30W ~ 60W
Memory	15W per 1GB
AGP Video Card	30W ~ 70W
PCI Express Video Card (Single)	30W ~ 150W
PCI add-in Card (Average, per one)	5W ~ 10W
Optical Drive	20W ~ 30W
Hard Drive	15W ~ 30W
Case/CPU Fans	2W ~ 3W
USB Device (per one)	5W
IEEE1394/FireWire Device (per one)	8W

Удома/Офісу

Для більшості домашніх і офісних користувачів, а потужність 400W повинне бути цілком достатньо – але це не завжди вірно, якщо у вас го-

лодний процесорів/відеокарт або кілька підключених пристроїв табл.3.6 . Якщо це так, будь ласка, будьте впевнені, щоб подивитеся на вищенаведену табл. 3.5 й розрахуйте свої вимоги грубої сили.

Таблиця 3.6 – Типова потужність комп'ютерів домашніх і офісних користувачів

Type	ATX12V, SFX12V or ATX
Maximum Power	200W ~ 400W
PFC	Yes (Active or Passive) or No

Мультімедіа/Більші користувацькі сховища

Якщо у вас багато пристроїв схову, наприклад жорстких дисків, оптичних приводів або інших пристроїв, блок живлення не менш 450 Вт-Це необхідність табл.3.7.

Таблиця 3.7 – Типова потужність комп'ютерів, в яких багато пристроїв схову

Type	ATX12V or EPS12V
Maximum Power	350W ~ 500W or more
PFC	Active

Примітка: будь ласка, звернетеся до " типове енергоспоживання компонентів " табл. 3.5 й розрахуйте свій певний максимум вимоги до живлення.

Аматор Геймер

Для геймерів з конфігураціями SLI або Crossfire, для живлення потужністю більш 500 Вт мінімальна вимога, з 550W ~ 600Вт рекомендується табл. 3.8. Будь ласка, переконаєтеся, що +12В надає не менш 34А (**змішана**), коли ви збираєтеся запустити високого класу для SLI/Crossfire на систему.

Таблиця 3.8 – Типова потужність комп'ютерів геймерів з конфігураціями SLI або Crossfire

Type	ATX12V or EPS12V
Maximum Power	>500W
PFC	Active
SLI/CrossFire Support	Yes

Примітка: будь ласка, звернетеся до " типове енергоспоживання компонентів " табл. 3.5 й розрахуйте свій певний максимум вимоги до живлення.

3.2 Материнські плати ПК

Материнська плата, яка також називається системною або основною платою, є основою комп'ютера. Як показано на рис.. 3.30, материнська плата являє собою друковану плату, на якій розміщені шини (або електричні доріжки) для з'єднання електронних компонентів один з одним [5-7].

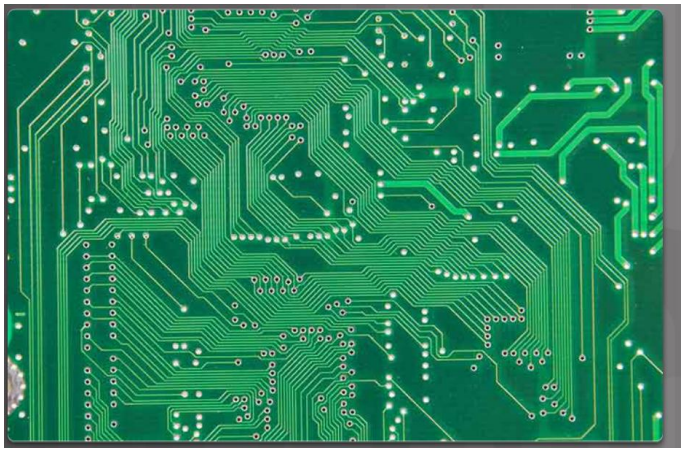


Рис. 3.30 – Друкована материнська плата

Такі компоненти можуть бути як вбудованими в материнську плату, так і встановлюватися додатково у відповідні роз’єм, слоти розширення й порти.

Нижче перелічені деякі з роз'ємів на материнській платі, у які можна встановлювати додаткові компоненти, як показано на рис. 3.31

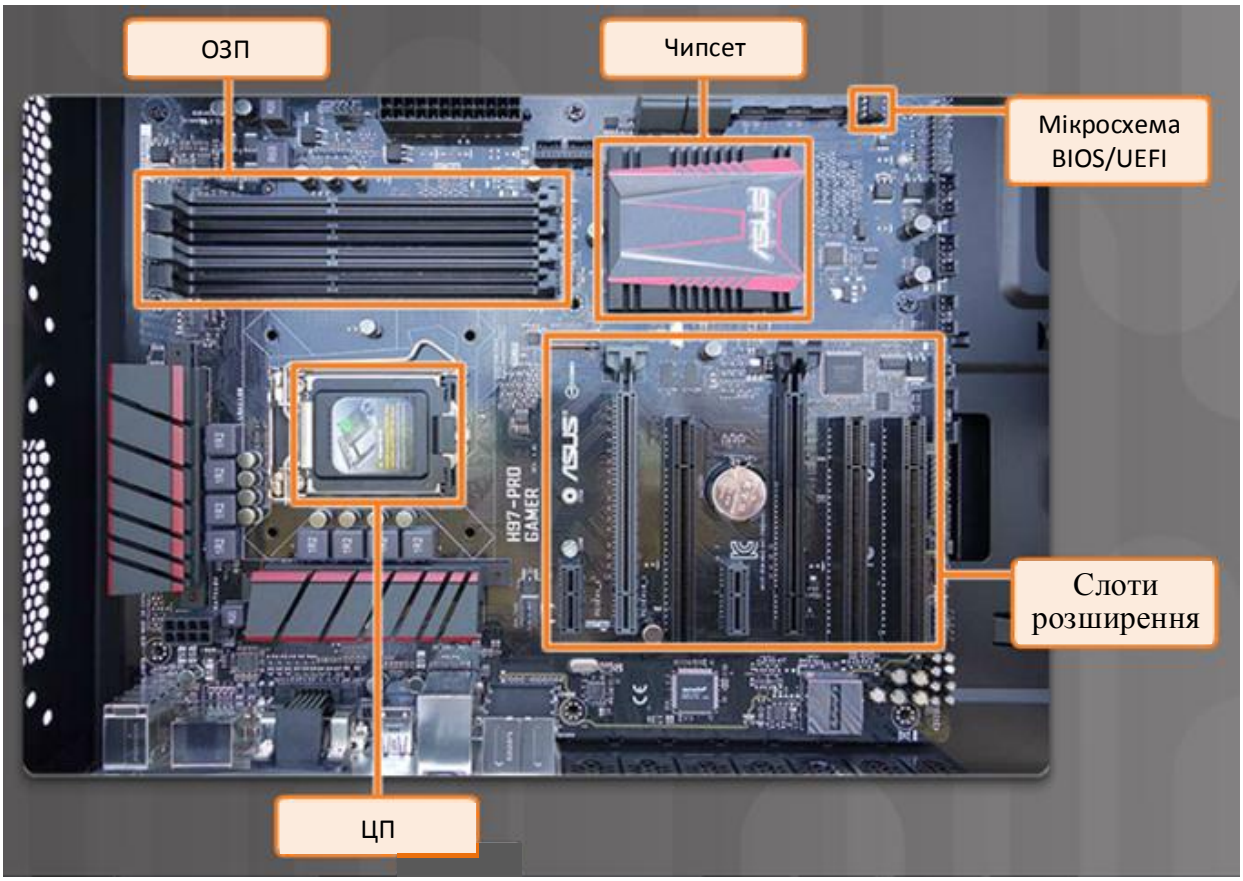


Рис. 3.31 – Підключення на материнській платі

Центральний процесор (ЦП) – уважається мозком комп'ютера.

Оперативний запам'ятовувальний пристрій (ОЗП) – тимчасове сховище для даних і додатків.

Слоти розширення – служать для підключення додаткових компонентів.

Чипсет – включає набір вбудованих схем на материнській платі, призначених для управління взаємодією апаратного забезпечення системи зі ЦП і материнською платою. Він також визначає, скільки пам'яті можна додати до материнської плати, і тип роз'ємів материнської плати.

Мікросхема **базової системи введення-виводу (Basic input/output system, BIOS)**і мікросхема **єдиного розширюваного мікропрограмного інтерфейсу (Unified Extensible Firmware Interface, UEFI)** – BIOS використовується для завантаження комп'ютера й керування потоками даних, якими обмінюються жорсткий диск, відеоадаптер, клавіатура, миша й інші компоненти комп'ютерної системи. Недавно BIOS була поліпшена за рахунок UEFI. UEFI являє собою інший програмний інтерфейс для завантаження й служб середовища виконання, однак у його основі лежить традиційна система BIOS для конфігурування системи, самотестування при включенні живлення POST і настроювання інших параметрів.

На рис. 3.32 показана материнська плата з додатковими компонентами.



Рис. 3.33 – Материнській плата з встановленими компонентами

Більшість чипсетів складається з наступних компонентів:

Північний міст – служить для управління високошвидкісним доступом до ОЗУ й відеоадаптеру. Він також відповідає за управління швидкістю взаємодії ЦП із іншими компонентами комп'ютерної системи. У ряді випадку відеоадаптер вбудований у північний міст.

Південний міст – забезпечує взаємодія ЦП із пристроями з більш низькою швидкістю роботи, такими як жорсткі диски, порти універсальної послідовної шини (USB) і слоти розширення.

На рис. 3.34 показане, як материнська плата забезпечує підключення різних компонентів.

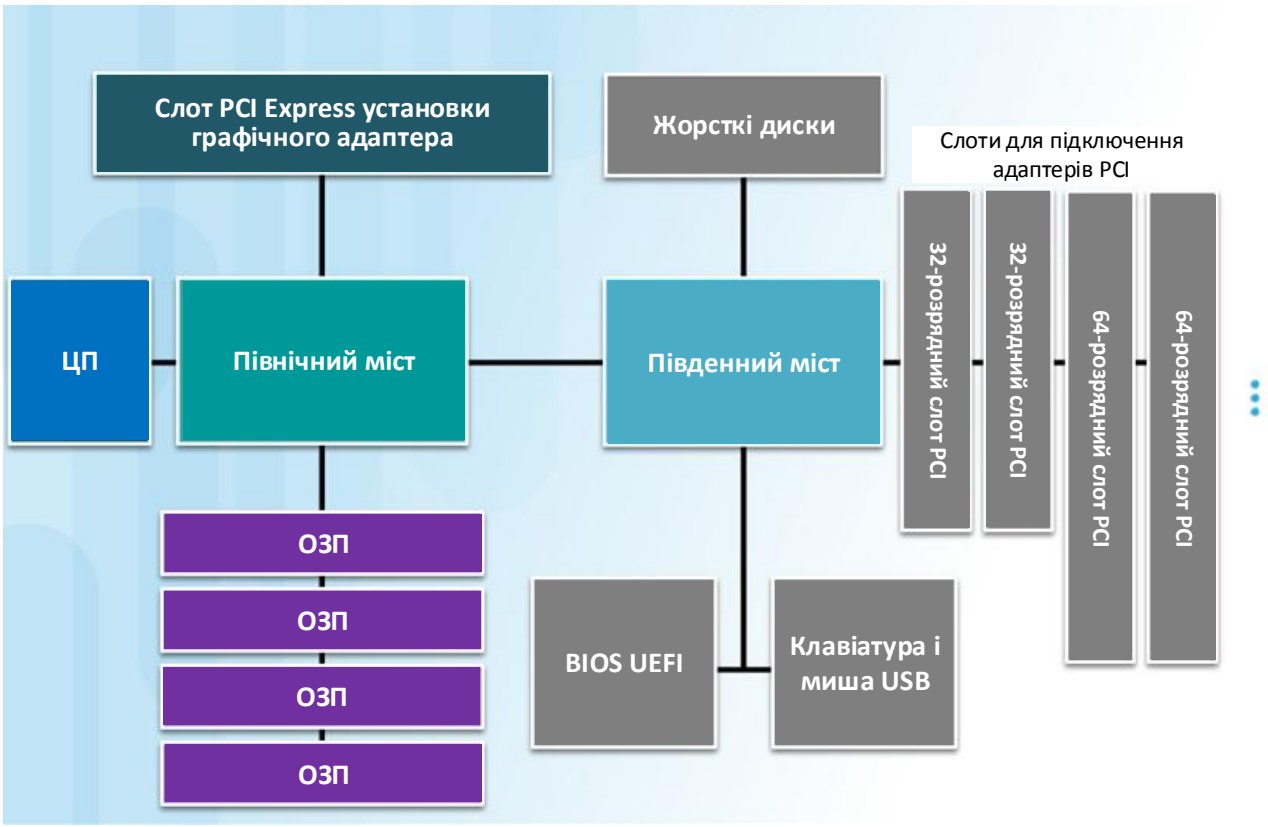


Рис. 3.34 – Підключення компонентів материнської плати

Формфактор материнських плат – їх розмір і форма. Він також характеризує фізичне розташування компонентів і пристроїв на платі.

За минулі роки була розроблена безліч варіантів материнських плат. Існують три основні формфактори материнських плат:

Advanced Technology extended (ATX) – найпоширеніший формфактор. У корпусі стандарту ATX розміщаються інтегровані порти введення-виводу стандартної материнської плати ATX. Блок живлення ATX підключається до материнської плати через цей 20-контактне роз'єм.

Micro-ATX – формфактор меншого розміру, назад сумісний з формфактором ATX. Для материнських плат Micro-atx часто використовуються ті ж набори мікросхем (північний міст і південний міст) і ті ж роз'єм живлення, що й для повнорозмірних материнських плат ATX, для них також можна використовувати безліч загальних компонентів. Звичайно материнські плати Micro-atx можна розмістити в стандартному корпусі ATX. Проте, материнські плати Micro-atx, як правило, менше по розміру, чому плати ATX, і мають менше слотів розширення.

ITX – формфактор ITX одержав широке поширення завдяки своєму дуже компактному розміру. Існує безліч типів материнських плат ITX, однак більшу популярність завоював формфактор Mini-ITX. Формфактор Mini-itx використовує дуже малу потужність, тому для його охолодження не потрібні вентилятори. Материнська плата типу Mini-ITX має тільки

один слот PCI для плат розширення. Комп'ютер на основі формфактора Mini-ITX можна використовувати в тих випадках, коли незручно використовувати великий або шумний комп'ютер.

У табл. 3.9 представлені відомості про різні формфактори.

Таблиця 3.9 – Формфактори материнської плати

Формфактор	Опис
ATX	Advanced Technology extended. Найпоширеніший формфактор. 30,5 x 24,4 см.
Micro-ATX	Займає менше місця, чім ATX. Одержав широке поширення в настільних ПК і комп'ютерах малого формфактора. 24,4 x 24,4 см.
Mini-ITX	Розроблений для невеликих пристроїв, таких як тонкі клієнти й телевізійні приставки. 17x17 см.
ITX	Аналогічний формфактору Micro-ATX. 21,5 x 19,1 см.

Примітка. Важливо розуміти відмінності між формфакторами, оскільки формфактор материнської плати визначає форму корпусу комп'ютера, тип необхідного блоку живлення й спосіб підключення окремих компонентів до неї. Деякі виготовлювачі встаткування мають власні формфактори, засновані на схемі ATX. Із цієї причини деякі материнські плати, блоки живлення й інші компоненти бувають несумісними зі стандартними корпусами ATX.

3.2.1 Архітектури ЦП

Якщо материнську плату називають основою комп'ютера, то центральний процесор (ЦП, CPU) уважається мозком комп'ютерної системи. З погляду обчислювальної потужності ЦП, який найчастіше називають просто процесором, є найбільш важливим елементом системи комп'ютера. У центральному процесорі виконується більшість обчислювальних операцій.

ЦП поставляються в різних формфакторах, кожний з них вимагає специфічного гнізда або роз’єм на материнській платі. У число найбільш популярних виробників ЦП входять Intel і AMD.

Роз’єм (або сокет) ЦП – це місце підключення процесора до материнської плати. Нижче перераховані архітектури сучасних роз'ємів ЦП і процесорів.

Pin Grid Array (PGA) (див. рис. 3.35) – в архітектурі PGA контакти перебувають на звороті процесора й вставляються в сокет ЦП на материнській платі з використанням роз’єм типу ZIF (нульове зусилля вставки). Термін «нульове зусилля вставки» означає, що для установки ЦП у роз’єм або гніздо материнської плати практично не потрібно застосовувати силу.

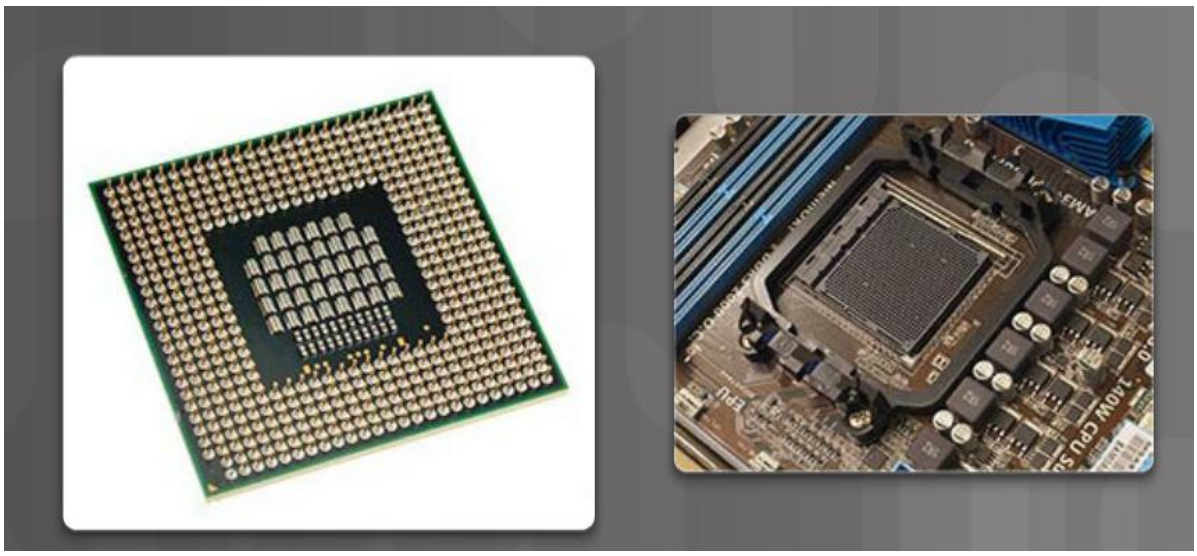


Рис. 3.35 – ЦП і роз'єм типу PGA

Land Grid Array (LGA) (див. рис. 3.36) – в архітектурі LGA контакти перебувають у самому роз’ємі, а не на процесорі.



Рис. 3.36 – ЦП і роз'єм типу LGA

Програма – це послідовність збережених команд. ЦП виконує ці команди, керуючись певним набором інструкцій.

Існує два типи наборів інструкцій для ЦП:

Комп'ютер зі скороченим набором інструкцій (Reduced Instruction Set Computer, RISC) – у такій архітектурі використовується щодо невеликий набір інструкцій. Мікросхеми RISC спроектовані таким чином, щоб дуже швидко виконувати ці команди.

Комп'ютер зі складним набором інструкцій (Complex Instruction Set Computer, CISC) – у таких архітектурах використовується широкий набір інструкцій, завдяки чому кожна операція вимагає меншої кількості тактів.

У той час як ЦП виконує один крок програми, інші команди й дані зберігаються в особливій високошвидкісній пам'яті, називаної кешем.

3.2.2 Підвищення продуктивності ЦП

Різні виробники ЦП доповнюють свої продукти функціями, що дозволяють підвищити продуктивність ЦП. Наприклад, компанія Intel для цих цілей використовує технологію гіперпотоків (Hyper-Threading). При гіперпотоків кілька фрагментів коду (потоків) виконуються в ЦП одночасно. Для операційної системи один ЦП із підтримкою Hyper-Threading при обробці декількох потоків функціонує як два ЦП.

Процесори виробництва AMD для збільшення своєї продуктивності використовують шину Hypertransport.

Шина Hypertransport – це високошвидкісне підключення між ЦП і північним мостом.

Потужність ЦП виміряється з погляду швидкості й обсягу даних, який він може обробити. Швидкість ЦП виміряється в циклах у секунду, наприклад мільйонах циклів у секунду, називаних мегагерцами (МГц), або мільярдах циклів у секунду, називаних гігагерцами (ГГц). Обсяг даних, який ЦП може обробити за одиницю часу, залежить від ширини системної шини. Її також називають шиною ЦП або шиною даних процесора. Побільшавши ширину шини ЦП, можна підвищити продуктивність його роботи. Ширина системної шини виміряється в бітах. Біт – це найменша одиниця виміру даних у комп'ютері.

У сучасних процесорах використовуються 32-розрядні або 64-розрядні системні шини.

Перевищення тактової частоти (розгін) процесора – приймання, використовуваний для того, щоб процесор працював швидше, чим зазначене в його специфікації. Не рекомендується використовувати розгін для підвищення продуктивності комп'ютера, оскільки це може привести до ушкодження ЦП. Пропуск тактів ЦП є прямою протилежністю розгону.

Пропуск тактів ЦП – це прийом, використовуваний у тих випадках, коли процесор працює на швидкості менше, чим номінальна, для економії електроенергії або зниження нагрівання. Пропуск тактів широко використовується на ноутбуках і інших мобільних пристроях.

Поява новітніх технологій в області виробництва процесорів привело до того, що виробники ЦП знайшли способи встановити більш одного ядра ЦП на одну мікросхему. Багатоядерні процесори являють собою два або більш процесорів в одній інтегральній схемі. У табл. 3.10 представлений короткий опис відмінностей багатоядерних процесорів.

Завдяки інтеграції процесорів на одному кристалі досягається висока швидкість взаємодії між ними. Багатоядерні процесори виконують команди швидше, чим одноядерні. Можна розподілити команди на всі

процесори одночасно. Процесори мають загальний доступ до ОЗП, оскільки ядра перебувають на одному кристалі.

Таблиця 3.10 – Короткий опис відмінностей багатоядерних процесорів.

Багатоядерні процесори	
Число ядер	**Опис**
Одноядерний ЦП	Одне ядро в одному ЦП, що виконує всю обробку. На материнській платі можуть бути роз'єм для декількох процесорів, що дозволяє зібрати потужний багатопроцесорний комп'ютер.
Двоядерний ЦП	Два ядра в одному ЦП, які можуть обробляти інформацію одночасно.
Трьохядерний ЦП	Три ядра в одному ЦП. Це чотирьохядерний процесор, у якому відключено одне ядро.
Чотирьохядерний ЦП	Чотири ядра в одному ЦП.
Шестиядерний ЦП	Шість ядер в одному ЦП.
Восьміядерний ЦП	Вісім ядер в одному ЦП.

Багатоядерний процесор рекомендується використовувати в комп'ютерах, призначених для ігор або редагування фото– і відеоматеріалів.

Високе споживання електроенергії приводить до виділення великої кількості тепла усередині корпусу. Багатоядерні процесори заощаджують електроенергію й роблять менше тепла, чім кілька одноядерних процесорів, у такий спосіб підвищуючи рівень продуктивності й ефективності роботи.

Іншим поліпшенням ЦП є так званий біт NX, він же «біт заборони виконання». Дана функція забезпечує захист областей пам'яті, у яких перебувають файли операційної системи, від атак шкідливого ПО (за умови, що ця функція підтримується ОС і включена в ній).

3.2.3 Системи охолодження

У результаті проходження електричного струму між електронними компонентами виділяється тепло. Компоненти комп'ютера працюють краще в охолодженому стані. Без відводу тепла робота комп'ютера може сповільнитися. Надмірне виділення тепла може привести до збоїв роботі й ушкодженню компонентів комп'ютера. Тому комп'ютер повинен в обов'язковому порядку включати систему охолодження.

Примітка. Для охолодження компонентів використовуються системи активного й пасивного охолодження. Для роботи системи активного охолодження потрібна електроенергія, а для пасивного охолодження – немає.

Збільшення потоку повітря в корпусі комп'ютера дозволяє відвести більше тепла. Система активного охолодження включає вентилятори усередині корпусу, які відводять із нього гаряче повітря (див. рис.. 3.37). Для збільшення потоку повітря в деяких корпусах установлюють кілька

вентиляторів – один вентилятор забезпечує приплив свіжого повітря, а іншої видуває гаряче повітря назовні.



Рис. 3.37 – Вентилятор корпусу

ЦП виділяє дуже багато тепла. Для відводу тепла від ЦП на нього встановлюють радіатор, як показано на рис. 3.38. Радіатор має більшу площу з металевими тепловідводами для розсіювання тепла. Таке охолодження називається пасивним. Між радіатором і ЦП наносять термопасту. Вона дозволяє побільшати ефективність теплообміну між ЦП і радіатором, заповнюючи собою будь-які дрібні зазори.



Рис. 3.38 – Радіатор ЦП

Багатоядерні ЦП або процесори з підвищеною тактовою частотою виділяють набагато більше тепла. Вентилятор звичайно встановлюють прямо на радіатор, як показано на рис. 3.39. Вентилятор відводить тепло від металевих ребер радіатора. Таке охолодження називається активним.

Інші компоненти також можуть бути ушкоджені в результаті перегріву й найчастіше оснащуються вентиляторами. У більшості відеоадаптерів є власний процесор (графічний процесор, graphics-processing unit,

GPU), який також виділяє багато тепла. Деякі відеоадаптери оснащуються одним або декількома вентиляторами (рис. 3.40а).

У комп'ютерах з надзвичайно швидкими центральними й графічними процесорами може використовуватися система водяного охолодження, як показано на рис. 3.41б. На процесорі розміщається металева пластина, і через її верхню частину прокачується вода, що збирає вироблюване процесором тепло. Вода подається в радіатор, прохолоджується повітрям і потім вертається назад.



Рис. 3.39 – Вентилятор ЦП





Рис. 3.40:

а) система охолодження графічної карти; б) водяна система охолодження

Вентилятори ЦП видають багато шуму й можуть дратувати користувача, коли працюють на високих обертах. Альтернативою вентиляторній системі охолодження ЦП є система теплових трубок. У герметичній тепловій трубці перебуває рідина, яка циклічно випаровується й конденсується.

3.2.4 Постійні запам'ятовувальні пристрої

Комп'ютер оснащується різними типами пам'яті. Однак незважаючи на різниці дані у всіх типах пам'яті зберігаються у вигляді байтів. Байт – це одна з одиниць цифрової інформації, що представляє букви, числа й

символи. Зокрема, байт являє собою блок з восьми бітів одиниць, що зберігаються в пам'яті у вигляді нулів і одиниць.

Важливим компонентом комп'ютера є **постійний запам'ятовувальний пристрій (ПЗП)**. Мікросхеми ПЗП перебувають на материнській платі й на інших друкованих платах. У них утримуються команди, до яких ЦП може одержати безпосередній доступ. До команд, які зберігаються в ПЗП, ставляться команди для виконання базових операцій, таких як завантаження комп'ютера й операційної системи.

На рис. 3.41 представлені докладні відомості про різні типи ПЗП.

Важливо відзначити, що мікросхеми ПЗП зберігають усі дані, навіть якщо комп'ютер відключений. Ці дані не вдасться просто стерти або змінити.

Примітка. ПЗП іноді називають мікропрограмним забезпеченням або прошиванням. Це не зовсім точно, оскільки мікропрограмне забезпечення – це ПО, яке зберігається в мікросхемі ПЗП.

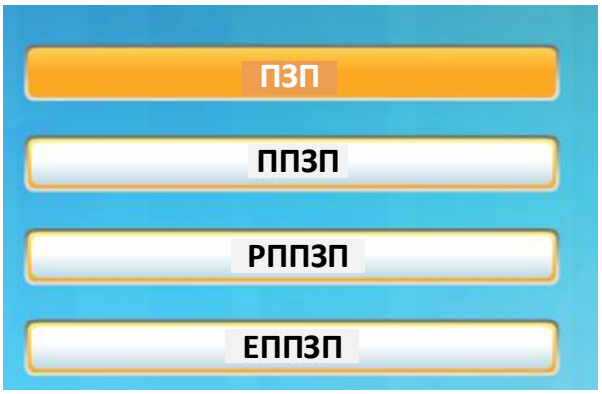


Рис. 3.41 – Типи ПЗП

Мікросхеми ПЗП тільки для читання. Дані записуються в мікросхеми ПЗП на виробництві. Дані в мікросхемі ПЗП не можна стерти або переписати. ПЗП програмуються заводом виробником і виконують збереження і видачу постійно записаної інформації, зміст якої не змінюється під час роботи системи: стандартні підпрограми, табличні дані, константи. Мікросхеми даного типу є застарілими.

ППЗП – програмувальне ПЗП із перемичками, що перепалюються, яке програмуються одноразово користувачем.

РПЗП – репрограмувальне ПЗП яке програмуються багаторазово користувачем.

ЕППЗП – електронне програмувальне ПЗП, котре є частиною інтегральної схеми мікропроцесора та використовується для зберігання даних. Дані в ЕППЗП можуть бути записані тільки один раз і не можуть бути вибірково стерті.

3.2.5 Оперативні запам'ятовувальні пристрої

Оперативний запам'ятовувальний пристрій (ОЗП) – це тимчасове сховище даних і програм, до яких звертається ЦП.

У комп'ютері використовуються різні типи ОЗП. На рис. 3.42 представлені більш докладні відомості про них.

На відміну від ПЗП, оперативна пам'ять ОЗП є енергозалежною. Це значить, що її вміст віддаляється при відключенні живлення комп'ютера.

Примітка. ПЗП є енергонезалежною пам'яттю. Його вміст не віддаляється при відключенні живлення комп'ютера.

Додавання в комп'ютер ОЗП, як правило, поліпшує його продуктивність. Наприклад, чим більше ОЗП комп'ютера, тим більше файлів і програм він може одночасно тримати в пам'яті й обробляти. Якщо обсягу встановленої оперативної пам'яті недостатньо, комп'ютеру доводиться для звільнення ОЗП тимчасово переміщати частину даних у файл підкачування, який перебуває на набагато більш повільному жорсткому диску. Максимальний обсяг ОЗП, який можна встановити на комп'ютер, обмежується можливостями материнської плати.



Рис. 3.42 – Типи ОЗП

Динамічне ОЗП (DRAM – Dynamic Random Access Memory) – це інтегральна схема, використовувана в якості основної пам'яті. Динамічному ОЗП необхідно постійне електроживлення для збереження даних.

Статичне ОЗП (СОЗП або SRAM – Static Ramdom Accesse) – це напівпровідникова енергозазалежна оперативна пам'ять, що забезпечує зберігання даних. Мікросхема статичної пам'яті має довільний доступ до збереженої інформації й дозволяє вибирати для читання або запису будь-які біти або байти. Головним достоїнством статичної пам'яті є її висока швидкодія, що перевищує показники динамічної пам'яті. Завдяки мінімальному часу доступу, що не перевищує 2 нс, мікросхеми статичної пам'яті можуть працювати синхронно із процесорами, забезпечуючи високу швидкодію.

До достоїнств статичної пам'яті також слід віднести:

мале енергоспоживання;

простоту інтерфейсу;

надійність в експлуатації.

Головним недоліком СОЗП є те, що її мікросхема має набагато меншу щільність зберігання даних, чім динамічна ОЗП. Це означає збільшені габарити, більш високу вартість і меншу ємність зберігання даних. По своїх габаритах мікросхеми пам'яті SRAM у середньому в 30 раз перевищують розміри й вартість динамічної пам'яті, що робить недоцільним її використання як оперативну пам'ять.

Синхронне динамічне ОЗП (SDRAM – англ. Synchronous Dynamic Random Access Memory) – синхронна динамічна пам'ять із довільним доступом використовується в комп'ютері й інших цифрових пристроях у якості ОЗП.

В SDRAM, на відміну від DRAM, що використовували асинхронний обмін даними, відповідь на керуючий сигнал, що зробив в пристрій, вертається не відразу, а лише при одержанні наступного тактового сигналу. Тактові сигнали дозволяють організувати роботу SDRAM у вигляді кінцевого автомата, що виконує вхідні команди.

DDR (від англ. Double Data Rate – подвійна швидкість передачі даних) – один з типів ОЗП SDRAM, які використовуються в комп'ютерах. Технологія DDR SDRAM дозволяє передавати дані по обох фронтах кожного тактового імпульсу, що дозволяє подвоїти пропускну здатність пам'яті.

Зарактеристики DDR згідно стандарту JEDEC Solid State Technology Association, раніше відома як англ. Joint Electron Device Engineering Council (JEDEC) або Спільної Ради Інженерів з електронних пристроїв – це комітет інженерної стандартизації напівпровідникової продукції при Electronic Industries Alliance (EIA), промислової асоціації, що представляє всі галузі електронної індустрії зведені до табл. 3.11.

Таблиця 3.11 – Характеристики DDR згідно стандарту JEDEC

Стандартна назва	Частота пам'яті	Час циклу	Ефективна (подвоєна) швидкість, передачі даних в млн./сек.	Назва модуля	Пікова пропускна здатність
DDR-200	100 МГц	10 нс	200	PC-1600	1600 МБ/с
DDR-266	133 МГц	7.5 нс	266	PC-2100	2133 МБ/с
DDR-333	166 МГц	6 нс	333	PC-2700	2667 МБ/с
DDR-400	200 МГц	5 нс	400	PC-3200	3200 МБ/с

Основна відмінність DDR2 від DDR – удвічі більша частота роботи зовнішньої шини, по якій дані передаються в буфер мікросхеми пам'яті. При цьому робота самого чипа залишилася такою ж, як і у просто DDR, тобто з такими ж затримками, але при більшій швидкості передачі інформації. При порівнянні роботи мікросхем DDR та DDR2 на однаковій тактовій частоті DDR2 матиме удвічі більші затримки й загальна продуктивність буде гіршою. Характеристики DDR2 згідно стандарту JEDEC зведені до табл. 3.12 До найбільш розповсюджених DDR2 відносяться DDR2-400, 533, 667,800,1066.

DDR3 SDRAM (від англ. Double Data Rate 3 Synchronous Dynamic Random Access Memory – синхронна динамічна пам'ять із довільним доступом та подвоєною швидкістю передачі даних, третє покоління) –

це тип оперативної пам'яті, що використовується в обчислювальній техніці як оперативна та відео-пам'ять. Прийшла на зміну пам'яті типу DDR2 SDRAM.

Таблиця 3.12 – Характеристики DDR2

Стандартна назва	Частота пам'яті	Ефективна (подвоєна) швидкість, передачі даних в млн./сек.	Назва модуля	Пікова пропускна здатність
DDR2-400	200 МГц	400	PC2-3200	3,200 ГіБ/с
DDR2-533	266 МГц	533	PC2-4200	4,200 ГіБ/с
DDR2-667	333 МГц	667	PC2-5300	5,300 ГіБ/с[1]
DDR2-675	337 МГц	675	PC2-5400	5,400 ГіБ/с
DDR2-700	350 МГц	700	PC2-5600	5,600 ГіБ/с
DDR2-711	355 МГц	711	PC2-5700	5,700 ГіБ/с
DDR2-750	375 МГц	750	PC2-6000	6,000 ГіБ/с
DDR2-800	400 МГц	800	PC2-6400	6,400 ГіБ/с
DDR2-888	444 МГц	888	PC2-7100	7,100 ГіБ/с
DDR2-900	450 МГц	900	PC2-7200	7,200 ГіБ/с
DDR2-1000	500 МГц	1000	PC2-8000	8,000 ГіБ/с
DDR2-1066	533 МГц	1066	PC2-8500	8,500 ГіБ/с
DDR2-1111	до 1111 МГц	1111	PC2-8888	8,888 ГіБ/с
DDR2-1142	до 1142 МГц	1142	PC2-9136	9,136 ГіБ/с
DDR2-1250	до 1250 МГц	1250	PC2-10000	10,000 ГіБ/с

В DDR3 зменшено на 40% споживання енергії порівняно з модулями DDR2 SDRAM, що обумовлено зменшеною (1,5 В, в порівнянні з 1,8 В для DDR2 SDRAM та 2,5 В для DDR-SDRAM) напругою живлення гнізд пам'яті.

Характеристики DDR3 згідно стандарту JEDEC зведені до табл. 3.13

Модулі пам'яті із дворядним розташуванням виводів (DIMMs), використовувані в настільних ПК, являють собою маленькі друковані плати, на яких розміщаються групи чипів пам'яті. У модулів DIMM більш широкий тракт підключення із двома рядами контактів на кожній стороні, що забезпечує більш швидку передачу даних у порівнянні з однобічними модулями пам'яті (Simms). Як і SIMM, модулі DIMM можуть випускатися в однобічному або двосторонньому виконанні. Модулі DIMM можна не додавати попарно й можна використовувати з іншими модулями DIMM з ідентичним числом контактів. Наприклад, модуль DIMM на 1 ГБ можна встановити на материнську плату поруч із модулем DIMM на 2 ГБ.

Таблиця 3.13 – Характеристики DDR3

Стандартна назва	Частота пам'яті, МГц.	Час циклу, нс.	Частота шини, МГц.	Ефективна (подвоєна) швидкість, млн. передач даних в сек.	Назва модуля	Пікова швидкість передачі даних при 64-бітній шині даних в одноканальному режимі, МБ/с.
DDR3-800	100	10,00	400	800	PC3-6400	6400
DDR3-1066	133	7,50	533	1066	PC3-8500	8533
DDR3-1333	166	6,00	667	1333	PC3-10600	10667
DDR3-1600	200	5,00	800	1600	PC3-12800	12800
DDR3-1866	233	4,29	933	1866	PC3-14900	14933
DDR3-2133	266	3,75	1066	2133	PC3-17000	17066
DDR3-2400	300	3,33	1200	2400	PC3-19200	19200

Швидкість роботи DIMM-модулів не може бути вище частоти системної шини. Якщо встановлено кілька модулів DIMM з різними робочими частотами, то робоча частота всієї встановленої пам'яті буде дорівнює робочій частоті модуля DIMM з найменшою швидкістю.

DDR4 SDRAM – новий тип оперативної пам'яті, що є еволюційним розвитком попередніх поколінь DDR (DDR, DDR2, DDR3) рис. 3.43.



Рис. 3.43 – Пара планок пам'яті 8 GB DDR4-2133 ECC 1.2 V

Відрізняється підвищеними частотними характеристиками і зниженою напругою. Основна відмінність DDR4 полягає у подвоєному

до 16 числі банків, що дозволило вдвічі збільшити швидкість передачі – до 3,2 Гбіт / с. Пропускна здатність пам'яті DDR4 досягає 34,1 ГБ/с (у разі максимальної ефективної частоти 4266 МГц, визначеної специфікаціями). Крім того, підвищена надійність роботи за рахунок введення механізму контролю парності на шинах адреси і команд. Підтримує ефективні частоти від 1600 до 4266 МГц.

Для розрахунку максимальної пропускної здатності пам'яті SDRAM наприклад DDR4 необхідно її частоту помножити на 64 біта (8 байт), тобто розмір даних, що може бути переданий за 1 такт роботи пам'яті.

Для пам'яті з частотою 2133 МГц (найнижча частота для пам'яті DDR4) максимальна пропускна спроможність складе 2133 * 8 = 17 064 Мегабайт / с

Для пам'яті з частотою 4266 МГц (найбільша частота, визначена в стандарті) максимальна пропускна спроможність складе 4266 * 8 = 34 128 Мегабайт / с

Пам'ять SDRAM типу DDR використовується в ПК тільки, якщо комп'ютер поставляється з модулями DDR-SDRAM.

3.2.6 Модулі пам'яті

На ранніх моделях комп'ютерів ОЗП були встановлені на материнських платах у вигляді окремих мікросхем. Окремі інтегральні схеми, називані мікросхемами із дворядним розташуванням виводів (dual inline package, DIP), були незручні в установці й часто розхитувалися. Для розв'язку цієї проблеми проектувальники об'єднали інтегральні схеми в друковану плату, створивши модуль пам'яті, який установлюється у відповідне роз'єм на материнській платі.

Типи модулів пам'яті наведені на рис. 3.44.

DIP – Мікросхема із дворядним розташуванням виходів (DIP) – окрема інтегральна схема пам'яті. Вона має подвійний ряд штирків, використовуваний для її підключення до материнської плати.

SIMM (англ. Single In-line Memory Module – модуль пам'яті з однорядним розташуванням виводів) – форм-фактор модулів пам'яті DRAM. В модулях використовувалися мікросхеми пам'яті FPM, EDO і BEDO (Burst-EDO).



Рис. 3.44 – Модулі пам'яті

Конструктивною особливістю модулів є те, що у них з'єднано між собою контакти, розташовані один навпроти одного на протилежних сторонах плати. По такій парі контактів передається один і той же сигнал. Мікрос-

хеми в модулях SIMM можуть встановлюватися як на одній, так і на обох сторонах плати.

30-виводні модулі SIMM мали ширину шини даних 8 біт та могли мати додатковий біт контролю парності. Використовувалися в персональних комп'ютерах на основі 16-бітних процесорів (встановлювалися парами) та перших 32-бітних процесорів (встановлювалися групами по 4).

72-виводні модулі SIMM мали ширину шини даних 32 біти (4 байти) і могли мати чотири додаткових біти для побайтового контролю парності або ECC – кодів корекції помилок.

Використання 30-контактних модулів в системах з 64-бітною шиною пам'яті неефективно, оскільки для заповнення одного банку пам'яті 64-розрядних систем необхідно вісім таких модулів. Для заповнення одного банку пам'яті в 64-розрядних системах 72-контактні SIMM необхідно встановлювати парами. В таких системах модулі SIMM було витіснено 64/72-бітними модулями DIMM.

DIMM (англ. англ. Dual In-line Memory Module, двосторонній модуль пам'яті) – форм-фактор модулів пам'яті DRAM. Даний форм-фактор прийшов на зміну форм-фактору SIMM. Основною відмінністю DIMM від попередника є те, що контакти, розташовані на різних сторонах модуля, є незалежними, на відміну від SIMM, де симетричні контакти, розташовані на різних сторонах модуля, замкнуті між собою і передають одні й ті ж сигнали. Конструктивно являє собою модуль пам'яті у вигляді довгої прямокутної плати з рядами контактних площинок з обох боків уздовж її довгої сторони, яка встановлюється в роз'єм підключення і фіксується за обидва її торця засувками. Мікросхеми пам'яті можуть бути розміщені як з одного, так і з обох сторін плати.

На відміну від форм-фактора SIMM, використовуваного для асинхронної пам'яті FPM і EDO, форм-фактор DIMM призначено пам'яті типу SDRAM. Виготовлялися модулі розраховані на напругу живлення 3,3 В і (рідше) 5 В.

Надалі в модулі DIMM стали упаковувати пам'ять типу DDR, DDR 2, DDR 3 і DDR 4, що відрізняється підвищеною швидкодією

Модулі DIMM для ПК повинні відповідати наступним вимогам:

- Число контактів на модулі DIMM повинне відповідати типу роз’єму.
- Для пам'яті **DDR** потрібно 184-контактний роз’єм й робоча напруга 2,5 В.
- Пам'ять **DDR2** несумісна з пам'яттю DDR1, і для неї потрібний 240-контактне роз’єм, а також робоча напруга 1,8 В.
- Пам'ять **DDR3** забезпечує смугу пропущення, що приблизно вдвічі перевищує смугу пропущення DDR2.

Модулі пам'яті **DDR3** несумісні з пам'яттю DDR1 або DDR2.

Для установки модулів **DDR3** DIMM потрібно 240-контактне рознімання й робоча напруга 1,5 В. Роз'єм для пам'яті DDR3 улаштований інакше, чім для DDR2 або DDR. Не намагайтеся встановлювати модуль пам'яті DDR3 на материнську плату, призначену для DDR або DDR2. А якщо ні, то можливо необоротне ушкодження материнської плати й модулів DIMM.

SO-DIMM – малі модулі пам'яті із дворядним розташуванням контактів використовуються в ноутбуках і моноблоках. Вони менше й тонше, чим інші модулі DIMM, тому використовуються, коли є обмеження по місці в шасі. Модуль SO-DIMM призначений для використання в ноутбуках (моноблоках) або як розширення пам'яті на платі, тому відрізняється зменшеним розміром.

Модулі SO-DIMM для ноутбука (моноблока) повинні відповідати наступним вимогам:

- Число контактів на модулі SO-DIMM повинне відповідати типу роз'єму.
- Для установки модулів SO-DIMM потрібен 200-контактний роз'єм.
- DDR2 SO-DIMM несумісні з модулями пам'яті DDR1 DIMM і DDR2 DIMM.
- DDR3 SO-DIMM несумісні з модулями DDR1 або DDR2, і для їхньої установки потрібен 204-контактний роз'єм.
- DDR4 SO-DIMM несумісні з модулями DDR1, DDR2 або DDR3, для їхньої установки потрібен 260-pin контактний роз'єи

Примітка. Модулі пам'яті бувають однобічними й двосторонніми. На однобічних модулях пам'яті мікросхеми ОЗП напаяні тільки з однієї сторони. На двосторонніх модулях пам'яті мікросхеми ОЗП розташовані по обидва боки.

Швидкість роботи пам'яті впливає на обсяг даних, який може обробити процесор за зазначений проміжок часу. З підвищенням швидкості роботи процесора швидкість роботи пам'яті також повинна зростати. Для збільшення пропускної здатності пам'яті також використовується технологія багатоканальної обробки. Стандартна оперативна пам'ять є одноканальною, тобто система звертається до всіх роз'ємів ОЗП одночасно. Також існує двоканальна оперативна пам'ять. Це означає, що система звертається одночасно до двом модулям по різних каналах. У випадку із трьохканальною оперативною пам'яттю задіється вже три канали.

Найбільша швидкодія забезпечує статичний ОЗП (SRAM), який використовується в якості кеш-пам'яті для зберігання недавно використаних процесором даних і команд. SRAM забезпечує процесору більш швидкий доступ до даних у порівнянні з більш повільним динамічним ОЗП (DRAM), або основною пам'яттю.

Кеш (від англ. cache – схованка) – особлива швидкісна пам'ять або частина оперативної пам'яті, де зберігаються копії часто використовуваних даних. Забезпечує до них швидкий доступ. Кеш пам'ять зберігає вміст і адресу даних, до яких часто звертається процесор. Під час чергового звертання процесора до адреси пам'яті, перевіряється наявність цієї адреси у кеші. Якщо відповідні дані наявні, вони передаються процесору з кешу. Це дозволяє скоротити тривалість обміну, оскільки швидкодія кешу більша за швидкодію звичайної пам'яті. Вибір даних зі звичайної (повільнішої) пам'яті здійснюється лише тоді, коли потрібні процесору дані в кеші відсутні.

Усі сучасні процесори мають як мінімум дворівневу структуру кеш-пам'яті, а більшість процесорів Intel – трьохрівневу кеш-пам'ять. При цьому розрізняють кеш першого рівня (позначається L1), кеш другого рівня (L2) і кеш третього рівня (L3). Причому у випадку процесорів Intel кеш-пам'ять всіх рівнів розміщені на кристалі процесора.

Видалося б, навіщо потрібно робити так багато типів кеш-пам'яті? Не чи простіше створити один великий кеш? Виявляється, не простіше. Проблема полягає в тому, що чим більше розмір кеш-пам'яті, тем нижче його швидкість. Тобто можна зробити один великий, але повільний кеш, а можна – трохи маленький, але швидку кеш-пам'ять, і другий варіант виявляється більш кращим.

Крім того, кеші різних рівнів у процесорі виконують різні завдання.

Так, внутрішній кеш, інтегрований у ЦП, найшвидший і маленький кеш першого рівня L1 завжди ділиться на кеш даних (L1D) і кеш команд або інструкцій (L1I). Це так звана гарвардська архітектура процесора. Кеш L1 завжди належить тільки конкретному ядру процесора.

Кеш другого рівня L2 є вже уніфікованим (містить і дані й команди). Кеш L2 завжди більше, ніж кеш L1, але повільніше його. У випадку багатоядерних процесорів кеш L2 належить конкретному ядру процесора.

А от кеш L3 є самим більшим і повільним і розділяється між усіма ядрами процесора (в архітектурі процесорів Intel).

Зрозуміло, що у випадку, коли в процесорі є багаторівнева система кеш-пам'яті, необхідно організувати взаємодію між кешами різних рівнів.

Для початку розглянемо дворівневу систему кешу. Така кеш-пам'ять будується на базі однієї із двох архітектур, яку також називають інклюзивною (inclusive), що й виключає, іменованої ексклюзивної (exclusive). Тобто кеш L2 завжди побудований або по, що включає, або по архітектурі, що виключає, стосовно кешу L1 (відзначимо, що при наявності кеша L3 кеші L2 і L1 можуть бути, що й не включають, і не виключають по відношенню друг до друга).

Кеш L2, побудований по архітектурі, що включає, завжди дублює вміст кешу L1, а тому ефективна ємність кеш-пам'яті дорівнює ємності кеша L2.

Кеш L2, побудований по архітектурі, що виключає, ніколи не дублює вміст кеша L1, а тому ефективна ємність кеш-пам'яті дорівнює сумарної ємності кеш-пам'яті L1 і L2.

Якщо дані зберігаються на мікросхемах ОЗП з помилками, виникають помилки пам'яті. Комп'ютер використовує різні способи виявлення й виправлення помилок у пам'яті.

Різні способи виявлення помилок наведені на рис. 3.45

Без контролю парності – пам'ять без контролю парності не перевіряє помилки в пам'яті.

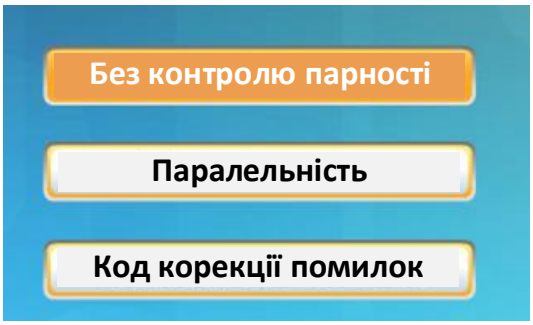


Рис. 3.45 – Помилки пам'яті

Виявлення помилок в техніці зв'язку – дія, спрямована на контроль цілісності даних при запису / відтворенні інформації або при її передачі по лініях зв'язку. Виправлення помилок (корекція помилок) – процедура відновлення інформації після читання її з пристрою зберігання або каналу зв'язку.

Для виявлення помилок використовують коди виявлення помилок, для виправлення – коригувальні коди (коди, що виправляють помилки, коди з корекцією помилок, завадостійкі коди).

Паралельність або перевірка контрольної суми (Checksum) – звично це байт, який доповнює кожні 256 байт контрольованої області. Застосовується для перевірки достовірність інформації, що зберігається у постійній (ROM BIOS) і напівпостійній (CMOS RTC, ESCD) пам’яті. Перевірка контрольної суми звичайно виконується одноразово під час включення комп’ютера.

Коди корекції помилок обо коригувальні коди – коди, які слугують для виявлення або виправлення помилок, що виникають при передачі інформації під впливом завад, а також при її зберіганні.

Для цього при запису (передачі) у корисні дані додають спеціальним чином структуровану надлишкову інформацію (контрольне число), а при читанні (прийомі) її використовують для того, щоб виявити або виправити помилки. Природно, що число помилок, яке можна виправити, обмежена і залежить від конкретного застосовуваного коду.

З кодами, які виправляють помилки, тісно пов'язані коди виявлення помилок. На відміну від перших, останні можуть тільки встановити факт наявності помилки в переданих даних, але не виправити її.

В дійсності, використовувані коди виявлення помилок належать до тих же класів кодів, що і коди, що виправляють помилки. Фактично будь-який код, що виправляє помилки, може бути також використаний для виявлення помилок (при цьому він буде здатний виявити більше число помилок, ніж був здатний виправити).

Всі завадостійкі коди можна розділити на два основних класи: блокові і неперервні (рекурентні або ланцюгові).

Як блокові, так і неперервні коди в залежності від методів внесення надмірності розділяються на роздільні і нероздільні.

Більшість відомих роздільних кодів складають систематичні коди. У цих кодів перевірні символи визначаються в результаті проведення лінійних операцій над певними інформаційними символами. Для випадку двійкових кодів кожний перевірний символ вибирається таким, щоб його сума за модулем два з певними інформаційними символами стала рівною нулю. Декодування зводиться до перевірки на парність певних груп символів. У результаті таких перевірок дається інформація про наявність помилок, а в разі потреби – про позицію символів, де є помилки.

3.2.7 Плати адаптерів і слоти розширення

Плати адаптерів підвищують функціональні можливості комп'ютера шляхом додавання контролерів певних пристроїв або заміни несправних портів.

Існує безліч різних плат адаптерів, використовуваних для розширення й індивідуального настроювання можливостей комп'ютера [5-8]:

Звуковий адаптер – відповідає за функції звуку.

Мережевий адаптер (Network Interface Card, NIC) – служить для підключення комп'ютера до мережі за допомогою мережевого кабелю.

Адаптер безпроводової мережі – служить для підключення комп'ютера до мережі по радіоканалу.

Відеоадаптер – відповідає за функції графіки.

Плата захвату – відправляє відеосигнал на комп'ютер для запису на жорсткий диск за допомогою ПО для захвату відеосигналу.

Плата ТВ-Тюнера – надає можливість перегляду й записи телевізійних сигналів на ПК за умови, що тюнер карти підключений до ефірної антени, кабельного або супутниковому ТВ.

Порт універсальної послідовної шини (Universal Serial Bus, USB) – служить для підключення периферійних пристроїв до комп'ютера.

Плата Thunderbolt – призначена для підключення до комп'ютера периферійних пристроїв.

Надлишковий масив незалежних дисків (Redundant array of independent disks, RAID) – адаптер RAID служить для підключення декількох жорстких дисків або твердотільних накопичувачів і забезпечує їхню роботу як єдиного цілого логічного сховища.

На рис. 3.46 показані деякі з перелічених плат адаптерів. Слід зазначити, що деякі з адаптерів можуть бути вбудовані в материнську плату.

Примітка. На старих комп'ютерах також могли бути модемний адаптер, прискорений графічний порт (AGP), адаптер інтерфейсу малих комп'ютерних систем (SCSI) і інші адаптери.



Рис. 3.46 – Плати адаптерів

На материнській платі комп'ютера є слоти розширення, призначені для установки плат адаптерів. Тип роз'єм використовуваної плати адаптера повинен відповідати слоту розширення. Відомості про різні слоти розширення представлені на рис. 3.47.

PCI (англ. Peripheral component interconnect, дослівно: взаємозв'язок периферійних компонентів) – шина вводу/виводу для підключення периферійних пристроїв до материнської плати комп'ютера.

Роз'єм взаємодії периферійних компонентів (PCI) – це 32– або 64-розрядний слот розширення. У цей час їм оснащується більшість материнських плат рис. 3.48а

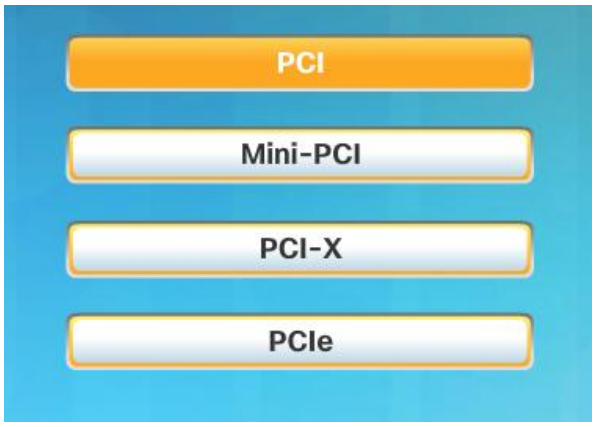
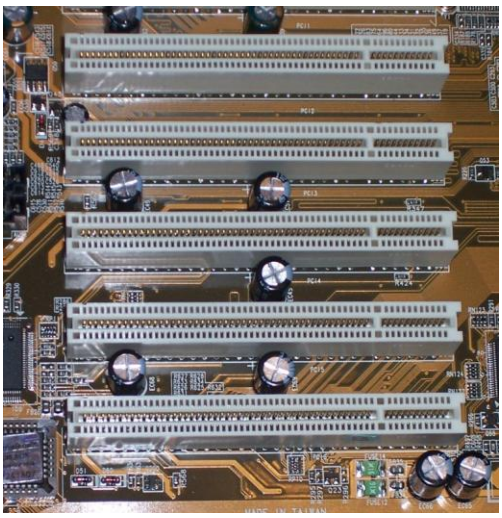


Рис. 3.47 – Слоти розширення

Mini-PCI – стандарт для підключення периферійних пристроїв до материнської плати рис. 3.48б. Це адаптація шини PCI. Він розроблений для ноутбуків і інших мініатюрних комп'ютерних пристроїв .



а



б

Рис 3.48:

а) PCI; б) Mini-PCI

PCI-X 1.0 – расширение шины PCI64 с добавлением двух новых частот работы, 100 и 133 МГц, а также механизма раздельных транзакций для улучшения производительности при одновременной работе нескольких устройств. Как правило, обратно совместима со всеми 3.3В и универсальными PCI-картами.

PCI-X 2.0 – дальнейшее расширение возможностей PCI-X 1.0; добавлены частоты 266 и 533 МГц, а также – коррекция ошибок чётности при передаче данных (ECC). Допускает расщепление на 4 независимых 16-битных шины, что применяется исключительно во встраиваемых и промышленных системах; сигнальное напряжение снижено до 1,5 В, но сохранена обратная совместимость разъёмов со всеми картами, использующими сигнальное напряжение 3,3 В.

PCIe або **PCI-E** або **PCI Express, (**також відома як **3GIO for 3rd Generation I/O;** не плутати з **PCI-X** або **PXI)** – комп'ютерна шина, що використовує програмну модель шини PCI і високопродуктивний фізичний протокол, заснований на послідовній передачі даних рис. 3.49.

На відміну від шини PCI, що використала для передачі даних спільну шину, PCI Express, в загальному випадку, є пакетною мережею з топологією типу зірка, пристрої PCI Express взаємодіють між собою через середовище, утворене комутаторами, при цьому кожен пристрій безпосередньо зв'язаний з'єднанням типу точка-точка з комутатором.

Крім того, шиною PCI Express підтримується:

гаряча заміна карт;

гарантована смуга пропускання (QoS);

управління енергоспоживанням;

контроль цілісності переданих даних.

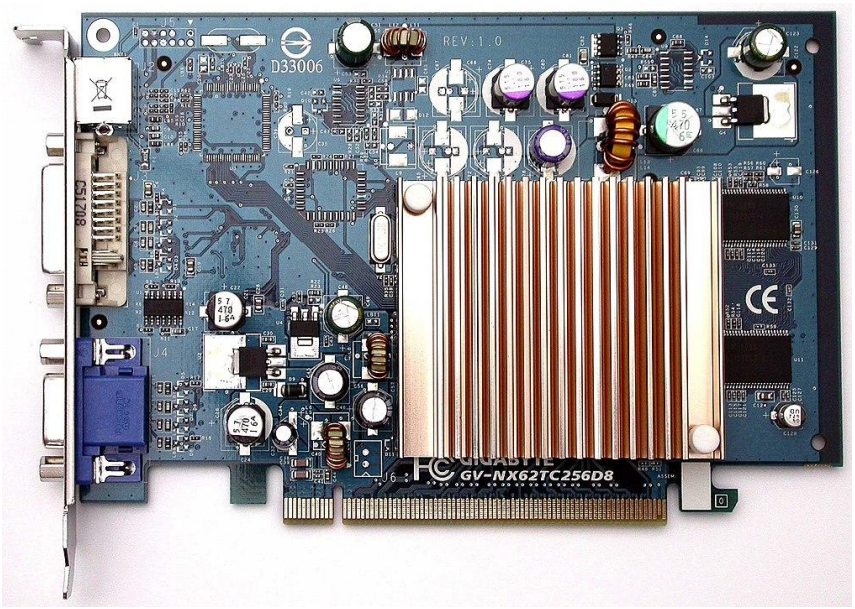


Рис. 3.49 – Відеокарта з роз'ємом PCIe

Висока пікова продуктивність шини PCI Express дозволяє використовувати її замість шин AGP і тим більше PCI і PCI-X, що призвело до заміни цих шин на PCI Express в персональних комп'ютерах.

Шина розширення – комп'ютерна шина, яка використовується на системній карті комп'ютерів або промислових контролерів, для додавання обладнань (плат) у комп'ютер. Є кілька видів:

ISA – 8 і 16 розрядна, використовувалася в перших персональних комп'ютерах;

Vl-bus – шина, розроблена на зміну шині ISA, на противагу MCA;

MCA – мікроканальна архітектура, розроблена IBM, для свого комп'ютера IBM PS/2;

PCI – шина, розроблена Intel, для процесорів Pentium;

AGP – варіант PCI, що використовувався для відеокарт;

PCI Express – сучасна шина, яка прийшла на зміну PCI;

Порівняльні характеристики сучасних шин розширення наведені в табл. 3.14.

Таблиця 3.14 – Порівняльні характеристики шин розширення

Шина	Пікова пропускна здатність Мбайт/с	Розрядність даних	Розрядність адреси	Частота МГц
PCI	133-533	32/64	32/64	33/66
PCI-X	533-4256	16/32/64	32/64	66-133
PCI Express	496-15872	1/2/4/8/12/16/32	32/64	2,5 ГГц
AGP 1x/2x/4x/8x	266/533/1066/2132	32	32/64	66

3.2.8 Пристрої зберігання даних

Пристрої зберігання даних, як показано на рис. 3.50, виконують читання інформації з магнітних, оптичних або напівпровідникових носіїв, а також здійснюють запис на них. Привод використовується для постійного зберігання даних або одержання інформації з дискового носія.



Рис. 3.50 – Пристрої зберігання даних

Нижче наведені найпоширеніші типи пристроїв зберігання.

Жорсткі диски (HDD) – традиційні магнітні дискові накопичувачі, які використовуються вже не одне десятиліття. Ємність жорстких дисків варіюється від гігабайтів (ГБ) до терабайтів (ТБ). Швидкість обертання такого диска виміряється в обертах у хвилину. Це швидкість, з якої обертається шпиндель із пластинами, на яких записані дані. Чим вище швидкість обертання шпинделя, тем швидше жорсткий диск одержує дані із пластин. Найбільш широке поширення одержали жорсткі диски зі швидкістю обертання 5400, 7200 і 10 000 обертів у хвилину.

Твердотільні накопичувачі (SSD) – енергонезалежні запам'ятовувальні пристрої для зберігання даних. Вони працюють набагато швидше магнітних жорстких дисків. Ємність таких дисків варіюється від гігабай-

тів (ГБ) до терабайтов (ТБ). У твердотільних накопичувачах відсутні рухливі деталі, тому вони абсолютно безшумні й більш енергоефективні, а також виділяють менше тепла, чім магнітні жорсткі диски. Носії SSD мають такі ж формфактори, що й магнітні жорсткі диски, і стрімко витісняють останні з ринку пристроїв зберігання даних.

Гібридні диски – також називані твердотільними гібридними накопичувачами (SSHD), являють собою компроміс між магнітними жорсткими дисками й твердотвльними накопичувачами. Вони працюють швидше, чим HDD, однак коштують менше, чим SSD. Такий накопичувач являє собою магнітний HDD із вбудованим SSD, який використовується в якості кеша. Накопичувач SSHD автоматично кешує часто використовувані дані.

Привод оптичних дисків – у приводі оптичних дисків для читання даних з носіїв використовується лазер. Існує три типи оптичних дисків: компакт-диски (CD), універсальні цифрові диски (DVD) і диски Blu-ray (BD). Компакт-диски, диски DVD і диски Blu-ray бувають тільки для читання, записувані (однократний запис) або перезаписувані (багаторазове читання й запис). У табл. 3.15 представлені відомості про різні типи оптичних носіїв і їх приблизна ємність.

Таблиця 3.15 – Відомості про різні типи оптичних носіїв

Оптичний накопичувач	Опис	Ємність накопичувача
CD-ROM	Накопичувач тільки для читання у вигляді компакт-диска, на який уже записані дані	700 МБ
CD-R	Накопичувач у вигляді компакт-диска, на який можна однократно записати дані	
CD-RW	Накопичувач у вигляді компакт-диска, на який можна багаторазово записувати дані й стирати їх	
DVD -R0M	Накопичувач тільки для читання у вигляді диска 040, на який уже записані дані (одношаровий)	4,7 ГБ (одношаровий) 8,5 ГБ (двошаровий)
DVD-RAM	Накопичувач у вигляді диска DVD, на який можна багаторазово записувати дані й стирати їх	
DVD +1/-R	Накопичувач у вигляді диска DVD, на який можна однократно записати дані	
DVD+/-RW	Накопичувач у вигляді диска DVD, на який можна багаторазово записувати дані й стирати їх	
BD– ROM	Накопичувач тільки для читання у вигляді диска Blu-ray, на який уже записані фільми, ігри або ПО	25 ГБ (одношаровий) 50 ГБ (двошаровий)
BD-R	Накопичувач у вигляді диска Blu-ray, на який можна однократно записати дані	
BD– RE	Накопичувач у вигляді диска Blu-ray, на який можна багаторазово записувати дані й стирати їх	

3.2.9 Інтерфейси пристроїв зберігання даних і RAID

Для підключення внутрішніх HDD, SSD і приводів оптичних дисків до материнської плати найчастіше використовується послідовний інтерфейс (SATA). Накопичувачі SATA підключаються до материнської плати через 7-контактне роз'єм SATA.

На одному кінці такого кабелю є роз'єм із ключем для підключення до накопичувача або привода, а на іншому – роз'єм із ключем для підключення до контролера. На рис. 3.51 показаний кабель SATA.



Рис. 3.51 – Кабель SATA



Рис. 3.52 – Підключення переносного жорсткого диску USB

Існує 3 основні версії інтерфейсу SATA: SATA 1, SATA 2 і SATA 3. Кабелі й роз'єм для них однакові, однак швидкості передачі даних різняться. Максимальна швидкість передачі даних через інтерфейс SATA 1 становить 1,5 Гбит/з, а через інтерфейс SATA 2 – до 3 Гбит/с. Інтерфейс SATA 3 забезпечує найбільшу швидкість передачі даних, яка може становити до 6 Гбит/с.

Примітка. До застарілих способів підключення зовнішніх приводів ставляться інтерфейс із інтегрованою електронікою керування диском (IDE), удосконалений інтерфейс із інтегрованою електронікою керування диском (EIDE) і паралельний інтерфейс ATA (PATA).

До комп'ютера також можна підключати зовнішні пристрої зберігання даних.

На рис. 3.52 показаний переносний жорсткий диск, підключений до ноутбука за допомогою кабелю USB. USB є найпоширенішим інтерфейсом для підключення зовнішніх пристроїв. Також для підключення зовнішніх пристроїв зберігання даних використовується інтерфейс External SATA (ESATA). Кабелі й роз'єм ESATA відрізняються від кабелів і роз'ємів SATA.

Широку популярність за високу швидкість передачі даних завоювали інтерфейси USB 3.0 і USB 3.1 з роз'ємами синього кольору. Накопичувачі USB підтримують можливість гарячої заміни, тобто для підклю-

чення або витягу такого пристрою не потрібно перезавантажувати комп'ютер.

До одному порту USB комп'ютера за допомогою концентраторів USB можна теоретично підключити до 127 окремих пристроїв. Концентратор USB використовується для підключення декількох пристроїв USB. Нарешті, багато пристроїв можуть одержувати живлення через порт USB, що усуває необхідність у зовнішньому джерелі живлення.

Існує кілька типів роз'ємів USB. На рис. 3.53 представлені найпоширеніше роз'єм USB типу A, а також три інших часто використовуваних роз'єм USB.

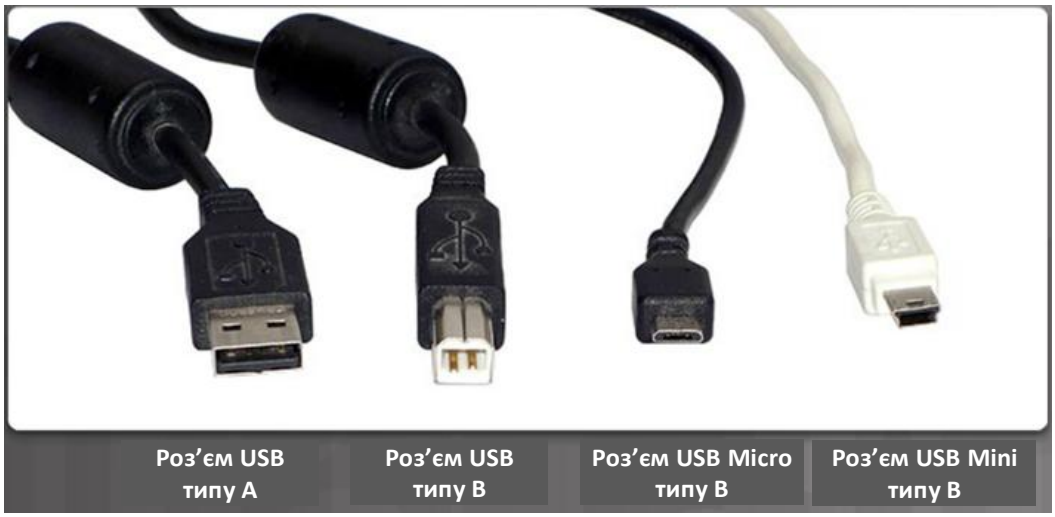


Рис. 3.53 – Типи роз'ємів USB

На рис. 3.54 представлене новітнє роз'єм USB-C (або роз'єм USB типу C).

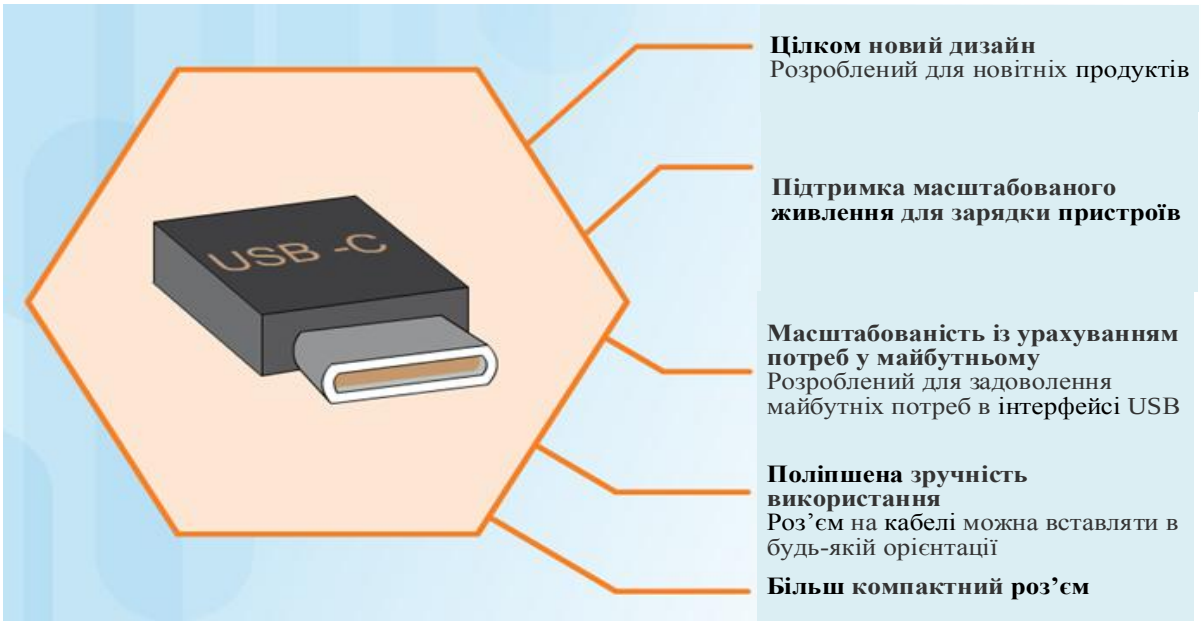


Рис. 3.54 – Роз'єм USB-C (або роз'єм USB типу C)

У табл. 3.16 представлені способи підключення зовнішніх пристроїв зберігання даних.

Таблиця 3.16 – Типи зовнішніх підключень

Тип підключення	**Опис**	**Максимальна пропускна спроможність**	**Максимальна довжина кабелю**
Firewire 400 (IEEE 1394a)	Підтримує підключення приводів з можливістю гарячої заміни До одного порту через концентратори можна підключити до 63 пристроїв Подає живлення	400 Мбіт/с	4,5 м
Firewire 800 (IEEE 1394b)	Зворотно сполучимо з Firewire 400 Для підключення також можна використовувати кабель Ethernet	800 Мбіт/с	4,5 м 100 м
ESATA	Служить для підключення зовнішніх приводів SATA Для живлення зовнішніх дисків потрібен окремий кабель живлення Несумісний з SATA	3 Гбіт/с	2 м
USB 2.0	Підтримує підключення приводів з можливістю гарячої заміни До одного порту через концентратори можна підключити до 127 пристроїв Подає живлення	480 Мбіт/с	5 м
USB 3.0	Зворотно сполучимо з USB 2.0	5 Гбіт/с	3 м
USB 3.1	Зворотно сполучимо з USB 2.0 і USB 3.0	10 Гбіт/с	3 м
Thunderbolt	Підтримує шлейфове підключення до 6 пристроїв Подає живлення В інтерфейсі Thunderbolt 3 використовується роз’єм USB-C	10 Гбіт/с 20 Гбіт/с (Thunderbolt 2) 40 Гбіт/с (Thunderbolt 3)	3 м

На рис. 3.55 показана діаграма для порівняння продуктивності різних інтерфейсів.

RAID (англ. Redundant Array of Independent Disks) – технологія віртуалізації даних, яка об'єднує кілька дисків в логічний елемент для надійності збереження інформації та підвищення продуктивності накопичувачів.

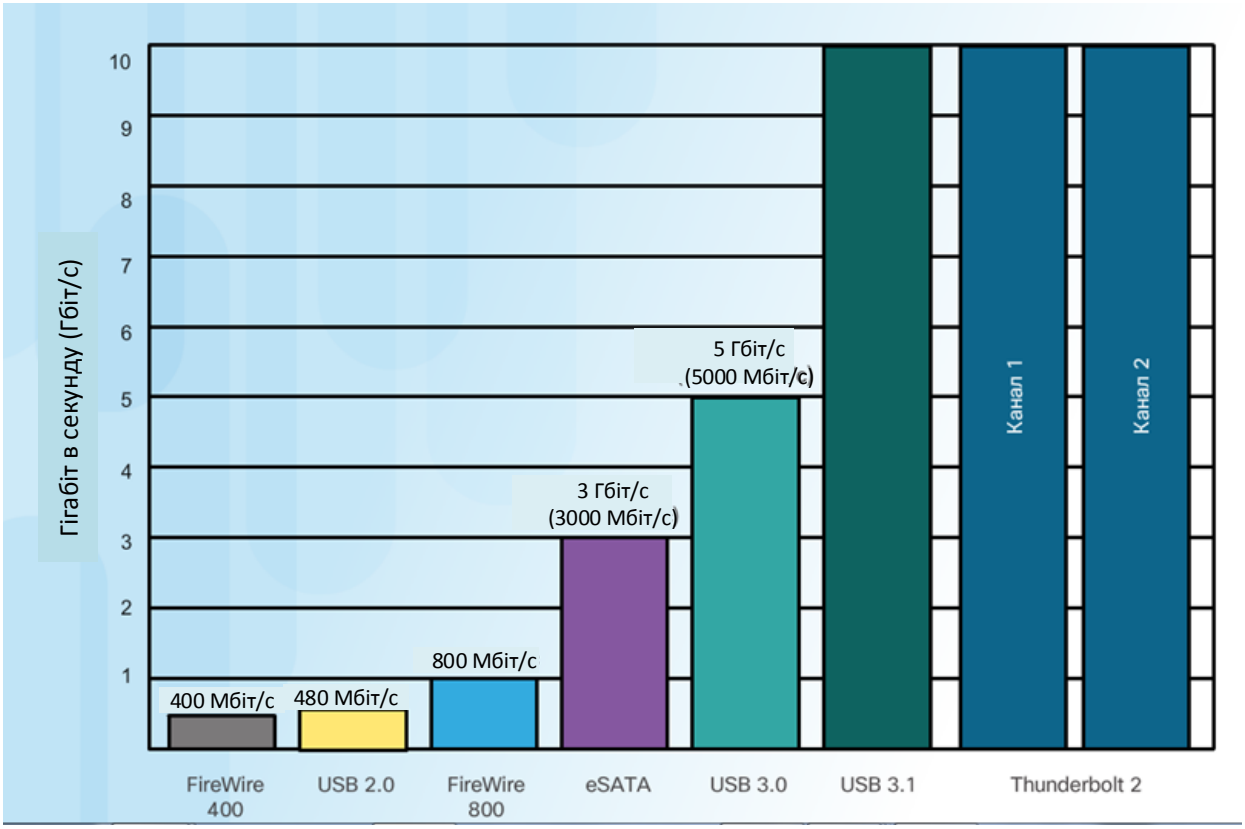


Рис. 3.55 – Максимальна пропускна спроможність зовнішніх підключень

Дисковий масив – це набір дискових пристроїв, які працюють разом, щоб підвищити швидкість і/або надійність системи вводу/виводу. Цим набором пристроїв керує особливий RAID-контролер (контролер масиву), який забезпечує функції розміщення даних масивом; а для решти усієї системи дозволяє представляти увесь масив, як один логічний пристрій вводу/виводу. За рахунок паралельного виконання операцій читання та запису на кількох дисках, масив забезпечує підвищену швидкість обміну порівняно з одним великим диском.

Масиви також можуть забезпечувати надійне зберігання даних, для того, щоб дані не були втрачені у разі виходу з ладу одного з дисків. Залежно від рівня RAID, проводиться або дублювання або рівномірний розподіл даних на дисках.

У табл.. 3.17 показане порівняння різних рівнів RAID.

Таблиця 3.17 – Порівняння рівнів RAID

Рівень RAID	**Мінім. кіл-ть дисків**	**Опис**	**Переваги**	**Недоліки**
0	2	Чергування даних без надмірності	Найкраща продуктивність	Відсутня захист даних, збій на одному диску приводить до втрати всіх даних

Рівень RAID	Мінім. кіл-ть дисків	Опис	Переваги	Недоліки
1	2	Дзеркалювання дисків	Висока продуктивність, високий рівень захисту даних завдяки їхньому дублюванню	Високі витрати на реалізацію, оскільки необхідний додатковий диск рівної або більшої ємності
2	2	Кодування з виправленням помилок	Даний рівень більше не використовується	Тієї ж продуктивності можна досягтися при менших витратах за допомогою RAID 3
3	3	Чергування даних на рівні байтів з виділеною парністю	Для більших, послідовних запитів даних	Не підтримує множинні, одночасні запити на читання й запис
4	3	Чергування даних на рівні блоків з виділеною парністю	Підтримує множинні запити на читання, при збої диска використовується виділений диск парності для створення диска на заміну	Запити на запис – вузьке місце через виділений диск парності
5	3	Комбінація чергування даних і парності	Підтримує множинні одночасні запити на читання й запис Дані записуються на всі диски з парністю Дані можна відтворити на основі інформації, знайденої на інших дисках	Продуктивність при записі нижче, чим у RAID 0 і 1
6	4	Незалежні диски для зберігання даних з подвійною парністю	Чергування даних на рівні блоків, дані парності розподілені по всіх дисках, може обробити одночасні збої двох дисків	Продуктивність нижче, чим у RAID 5; підтримується не на всіх контролерах дисків
RAID 0+1	4	Комбінація чергування даних і дзеркалювання	Висока продуктивність, найвищий рівень захисту даних	Високі витрати, оскільки для дублювання даних потрібно у два рази більше місця
10	4 (необхідно парне число)	Дзеркальований набір у наборі із чергуванням	Відмовостійкість і поліпшення продуктивності	Високі витрати, оскільки для дублювання даних потрібно у два рази більше місця

3.2.10 Відеопорти й кабелі для підключення монітора

Відеопорт використовується для підключення монітора до комп'ютера за допомогою кабелю. Відеопорти й кабелі для підключення монітора передають аналогові сигнали, цифрові сигнали або сигнали обох видів. Комп'ютери – цифрові пристрої, що створюють цифрові сигнали. Ці цифрові сигнали направляються в графічну плату, звідки передаються по кабелю на цифровий монітор. Цифрові сигнали можна також перетворити в аналогові за допомогою графічної плати, а потім передати на аналоговий монітор. Низька якість зображення – це результат перетворення цифрового сигналу в аналоговий. Монітор і кабель для його підключення цифрові сигнали, що підтримують, забезпечують більш висока якість зображення в порівнянні з підтримуючими тільки аналогові сигнали.

Існує кілька типів відеопортів і роз'ємів:

Цифровий відеоінтерфейс (DVI) (див. рис. 3.55) – роз’єм DVI білого кольору звичайно включає 24 контакту (три ряди по вісім контактів) для передачі цифрового сигналу, 4 контакту для передачі аналогового сигналу й плоский контакт, який називається шиною заземлення. Як правило, DVI-D обробляє тільки цифрові сигнали, а роз’єм DVI-A – тільки аналогові. В DVI застосовується двоканальний інтерфейс для створення двох груп каналів передачі даних, які здатні передавати цифрові відеодані зі швидкістю понад 10 Гбит/с.

Роз’єм Displayport (див. рис. 3.56) – інтерфейс, розроблений для підключення високотехнологічних комп'ютерів і моніторів для роботи із графікою, а також для підключення компонентів і екранів домашніх кінотеатрів. Це роз’єм має 20 контактів і може бути використаний для передачі аудіо, відео або обох типів даних. Displayport підтримує передачу відеоданих на швидкості до 8,64 Гбит/с.



Рис. 3.55 – Роз’єм DVI



Рис. 3.56 – Роз’єм Displayport

Mini Displayport – більш компактна версія роз’єм Displayport. Він використовується в інтерфейсах Thunderbolt 1 і Thunderbolt 2.

HDMI – мультимедійний інтерфейс високої чіткості, розроблений спеціально для телевізорів високої чіткості. Однак його характеристики передачі цифрового сигналу зробили його відмінним кандидатом для установки на комп'ютери. Існує два розповсюджені типи кабелів HDMI. Повнорозмірний кабель HDMI типу A – стандартний кабель для підключення аудіо– і відеопристроїв. Кабель minihdmi типу C використовується для підключення ноутбуків і портативних пристроїв, таких як планшети. Роз'єм типу C, зображений на рис. 3.57, менше роз'єм типу A і має 19 контактів.

Thunderbolt (див. рис. 3.58) – в інтерфейсах Thunderbolt 1 і Thunderbolt 2 використовується адаптер Mini Displayport (MDP), а в інтерфейсі Thunderbolt 3 – роз'єм USB-C.



Рис. 3.57 – Роз'єм Mini Displayport



Рис. 3.58 – Роз'єм Thunderbolt 1 і Thunderbolt 2

Роз'єм VGA (див. рис. 3.59) – роз'єм для передачі аналогового відеосигналу. У ньому є 3 ряду контактів, усього контактів 15. Іноді його називають роз'ємом DE-15 або HD-15.



Рис. 3.59 – Роз'єм VGA

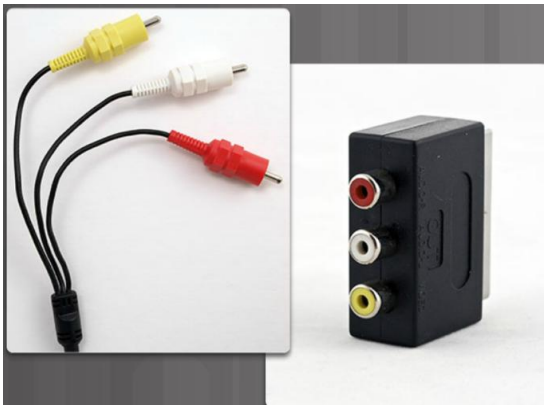


Рис. 3.60 – Роз'єм RCA

Роз'єм RCA (див. рис. 3.60) – такі роз'єм включають центральний штекер, оточений ободком, і використовуються для передачі аудіо або

відео. Часто роз'єм RCA випускаються групами по три. Жовтий роз'єм відповідає за передачу відео, а червоний і білий призначені для лівого й правого каналів аудіосигналу.

Роз'єм BNC (див. рис. 3.61) – служить для підключення коаксіального кабелю до пристроїв за допомогою чвертьобертової схеми підключення. Роз'єм BNC використовуються для передачі цифрового або аналогового аудіо або відео.

Роз'єм Din-6 – має 6 контактів і, як правило, використовується для передачі аналогового аудіо, відео й живлення для камер систем безпеки.



Рис. 3.61 – Роз'єм BNC

Безпроводовий інтерфейс – звичайно вимагає підключення додаткових передавачів до монітора або телевізора.

Примітка. До застарілих способів підключення моніторів ставляться композитний кабель/кабель RGB або S-Video.

3.2.11 Інші порти й кабелі

Через порти введення-виводу комп'ютера підключаються периферійні устрої, такі як принтери й сканери, а також знімні накопичувачі. Крім розглянутих раніше портів і інтерфейсів, комп'ютер може бути оснащений іншими портами.

Порт PS/2 (див. рис. 3.62) – використовується для підключення до комп'ютера клавіатури або миші. Порт PS/2 – 6-контактне роз'єм MINI-DIN. Роз'єм для клавіатури й миші, як правило, мають різні кольори. Якщо порти не мають колірного маркування, поруч із кожним із цих портів перебуває зображення клавіатури або миші.

Аудіопорти (див. рис. 3.63) – використовуються для підключення аудіопристроїв до комп'ютера. Аналогові роз'єм звичайно включають лінійний вхід для підключення зовнішнього джерела звуку (наприклад, стереосистеми), роз'єм для мікрофона й роз'єм лінійних виходів для підключення динаміків або навушників. Також є порти введення й виводу цифрового сигналу. Вони використовуються для підключення цифрових джерел і пристроїв виводу. Такі роз'єм й кабелі служать для передачі світлових імпульсів за допомогою оптоволоконних кабелів.

Ігровий порт/MIDI (див. рис. 3.63) – використовується для підключення джойстика або пристрою з інтерфейсом MIDI.



Рис. 3.62 – Кабель і роз'єм PS/2

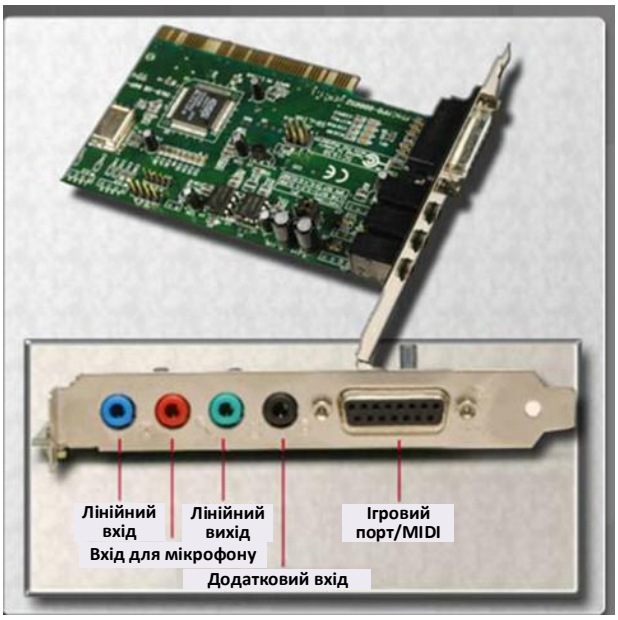


Рис. 3.63 – **Аудіопорти**

Мережевий порт Ethernet (див. рис. 3.64) – мережевий порт, який також називають роз'ємом RJ-45. Він має 8 контактів і використовується для підключення пристроїв до мережі. Швидкість підключення залежить від типу мережевого порту. Існує два розповсюджені стандарти Ethernet: Fast Ethernet (або 100BASE) для передачі даних на швидкості до 100 Мбіт/с і Gigabit Ethernet (1000BASE) для передачі даних на швидкості до 1000 Мбит/с. Максимальна довжина мережевого кабелю Ethernet становить 100 м.

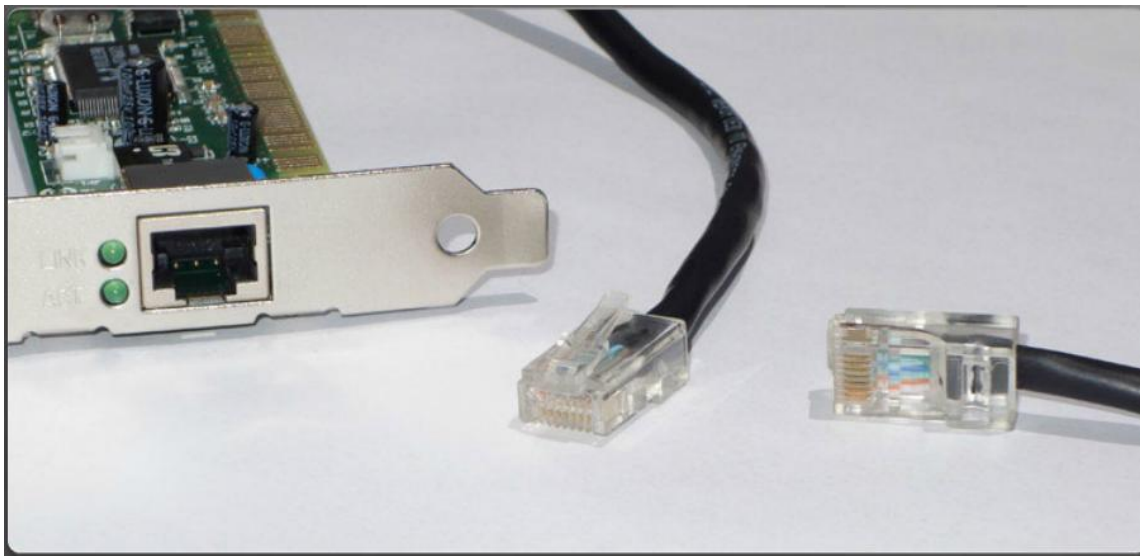


Рис. 3.64 – Мережевий порт

Порти й кабелі USB – універсальна послідовна шина (USB) являє собою стандартний інтерфейс, через який периферійні пристрої підклю-

чаються до комп'ютера. Устрою USB підтримують можливість гарячої заміни. Це означає, що користувачі можуть підключати й відключати дані пристрої, коли комп'ютер включений. Роз'ємами USB оснащені комп'ютери, фотоапарати, принтери, сканери, пристрої зберігання даних і багато інші електронні устрої. Концентратор USB використовується для підключення декількох пристроїв USB. Один порт USB комп'ютера може підтримувати до 127 окремих пристроїв за допомогою безлічі концентраторів USB. Деякі устрої можуть також одержувати живлення через порт USB, що усуває необхідність у зовнішньому джерелі живлення.

Пропускна здатність порту USB 1.1 становить 12 Мбіт/с у режимі повної швидкості й 1,5 Мбіт/с у режимі низької швидкості. Максимальна довжина кабелю USB 1.1 становить 3 м. Інтерфейс USB 2.0 забезпечує швидкість передачі даних, яка може становити до 480 Мбіт/с. Максимальна довжина кабелю USB 2.0 становить 5 м. Максимальна швидкість передачі даних пристроями USB визначається конкретним портом. Інтерфейс USB 3.0 дозволяє передавати дані зі швидкістю до 5 Гбит/с. USB 3.0 назад сполучимо з більш ранніми версіями цього інтерфейсу. Для кабелю USB 3.0 не існує певної максимальної довжини, однак загальноприйнята його довжина становить 3 м.

Порти й кабелі Firewire – Firewire являє собою високошвидкісний інтерфейс, що підтримує можливість гарячої заміни й використовуваний для підключення периферійних пристроїв до комп'ютера. Один порт Firewire підтримує до 63 пристроїв. Деякі устрої можуть також одержувати живлення через порт Firewire, що усуває необхідність у зовнішньому джерелі живлення. В Firewire використовується стандарт Інституту інженерів по електроніці й електротехніці (IEEE) 1394; цей інтерфейс також відомий як i.Link. Інститут IEEE займається випуском публікацій і створенням технологічних стандартів.

Стандарт 1394a підтримує швидкість передачі до 400 Мбіт/с для кабелю довжиною 4,5 м або менш. Для цього стандарту використовується 4-контактний або 6-контактне роз'єм. Стандарт IEEE 1394b (Firewire 800) підтримує більш широкий діапазон підключень, включаючи неекрановану кручену пару (UTP) категорії 5 і оптичне волокно. Залежно від використовуваного носія, підтримуються швидкості передачі даних до 3,2 Гбит/з на відстані 100 м або менш.

Кабелі ESATA – використовуються для підключення пристроїв SATA до інтерфейсу ESATA за допомогою 7-контактного кабелю для передачі даних. Цей кабель не забезпечує подачу живлення на пристрій SATA. Для цього використовується окремий кабель живлення.

Примітка. До інших портів ставляться послідовні порти, паралельні порти й модемні порти.

3.2.12 Адаптери й конвертери

Сьогодні у світі існує велика кількість стандартів підключення. Багато хто з них сумісні, однак для цього необхідні спеціальні компоненти, які називаються адаптерами або конвертерами.

Адаптер – компонент, що забезпечує фізичне підключення двох різних технологічних рішень. Наприклад, адаптер DVI-HDMI. Адаптер може бути виконано у вигляді одного компонента або у вигляді кабелю з різними роз'ємами на кінцях.

Конвертер – виконує ту ж функцію, що й адаптер, однак служить для перетворення сигналів з одного виду в інший. Наприклад, за допомогою конвертера USB 3.0-SATA жорсткий диск можна використовувати в якості флеш-диска.

На ринку сьогодні представлений найширший вибір різних адаптерів і конвертерів.

Адаптер DVI–HDMI – служить для підключення монітора HDMI до порту DVI.

Адаптер DVI–VGA (див. рис. 3.65) – служить для підключення кабелю VGA до порту DVI.



Рис. 3.65 – Адаптер DVI–VGA



Рис. 3.66 – Адаптер USB–Ethernet

Адаптер USB A–USB B – служить для підключення порту USB A до порту USB B.

Адаптер USB–Ethernet (див. рис. 3.66) – служить для підключення кабелю Ethernet до порту USB.

Адаптер USB–PS/2 (див. рис. 3.67) – служить для підключення клавіатури або миші USB до порту PS/2.

Конвертер HDMI–VGA – служить для перетворення вихідного сигналу VGA комп'ютера в сигнал HDMI для підключення монітора HDMI.

Конвертер Thunderbolt–DVI – служить для перетворення відеосигналу Mini Displayport у відеосигнал DVI для підключення монітора DVI.



Рис. 3.67 – Адаптер USB–PS/2

3.3 Пристрої вводу й виводу

3.3.1 Пристрої вводу

Пристрій уведення використовуються для введення даних або команд у комп'ютер.

Нижче наведені приклади пристроїв уведення.

Клавіатура й миша (див. рис. 3.68) – найпоширеніші пристрої введення. Клавіатура використовується для введення текстових команд, а миша – для взаємодії із графічним інтерфейсом користувача. На ноутбуках також є сенсорні панелі, які забезпечують вбудовані можливості миші.

Сенсорні екрани (див. рис. 3.69) – являють собою екрани, чутливі до торкання й натисканню пальцями. Комп'ютер одержує команди залежно від місця екрана, натиснутого користувачем.

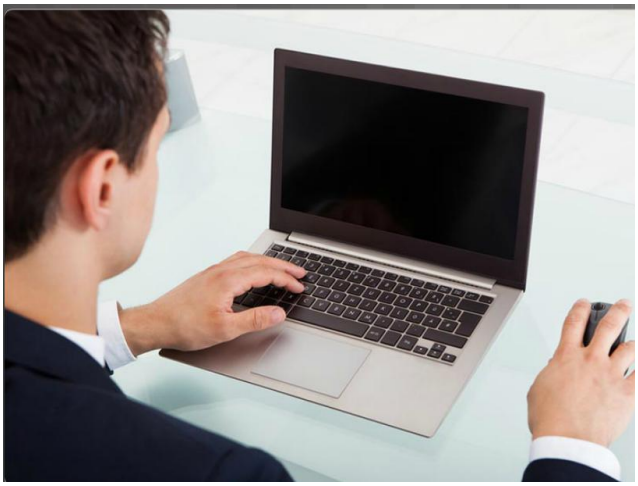


Рис. 3.68 – Клавіатура й миша

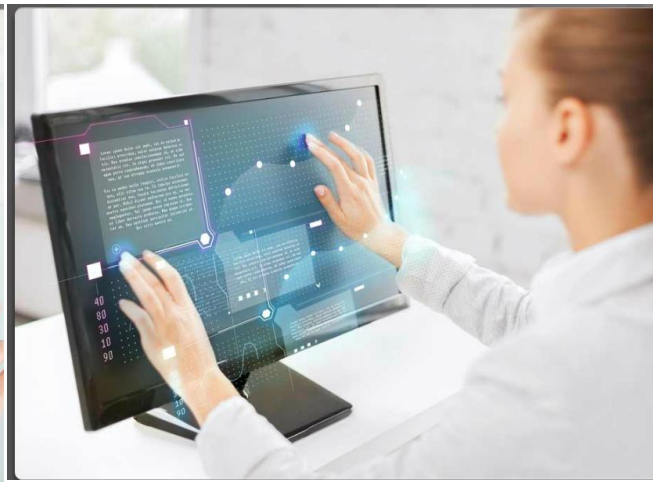


Рис. 3.69 – Сенсорні екрани

Джойстики й геймпади (див. рис. 3.70) – пристрою введення для комп'ютерних ігор. За допомогою геймпаду користувач управляє рухами в грі й змінює область огляду ігрового простору. Для цього на геймпаді є невеликі стики й кілька кнопок. На багатьох геймпадах також є тригери, що відслідковують силу натискання. Для авіасимуляторів і подібних ігор також використовуються джойстики.

Цифрові фотоапарати й відеокамери (див. рис. 3.71) – використовуються для створення зображень, які можна зберегти, відобразити, надрукувати або відредагувати. Що підключаються або вбудовані вебкамери дозволяють знімати відео в режимі реального часу.



Рис. 3.70 – Джойстики й геймпади



Рис. 3.71 – Цифрові фотоапарати й відеокамери

Сканери (див. рис. 3.72) – дозволяють переводити зображення або документи в цифровий формат. Цифроване зображення зберігається у вигляді файлу, який можна потім переглянути, роздрукувати або змінити. Пристрій для зчитування штрих-коду – це різновид сканера, що зчитує універсальний код товару. Ці пристрої широко використовуються для одержання відомостей про ціну й складських запасах.

Графічні планшети (дігітайзери) (див. рис. 3.73) – такі пристрої дозволяють конструкторові або художникові створювати креслення, зображення або інші добутки за допомогою стілуса – інструмента, що нагадує олівець, – на поверхні, яка розпізнає торкання стілуса. Деякі графічні планшети мають кілька площин або сенсорів, що дозволяє створювати тривимірні моделі, переміщаючи стілус у повітрі.



Рис. 3.72 – Сканер



Рис. 3.73 – Графічні планшети (дигитайзери)

Пристрої біометричної ідентифікації (див. рис. 3.74) – служать для ідентифікації користувача по унікальних фізичних характеристиках,

таким як відбиток пальця або голос. На багатьох ноутбуках є вбудовані сканери відбитків пальців для автоматичного входу в систему пристрою

Пристрою читання смарт-карт – такі пристрої введення звичайно використовуються на комп'ютерах для аутентіфикації користувачів. Смарт-карта може бути розміром із кредитну карту. У неї вбудований мікропроцесор, який звичайно перебуває під позолоченим контактним майданчиком на одній зі сторін карти.

KVM-перемикач (Keyboard, video, mouse switch) – це встаткування, використовуване для керування декількома комп'ютерами за допомогою одного монітора, клавіатури й миші. На підприємствах використання KVM-перемикачів дозволяє організувати економічний доступ до декільком серверам. Користувачі домашніх комп'ютерів можуть використовувати KVM-перемикачі для економії місця, як показано на рис. 3.75, підключаючи кілька комп'ютерів до одному монітору, клавіатурі й миші.



Рис. 3.74 – Сканер відбитків пальців



Рис. 3.75 – KVM-перемикач (Keyboard, video, mouse switch)

Більш нові моделі KVM-перемикачів дозволяють підключати пристрою USB і динаміки до декільком комп'ютерам. Як правило, натиснувши кнопку на KVM-перемикачі, користувач може перейти з одного підключеного комп'ютера на інший. Деякі моделі перемикачів здійснюють перехід з одного комп'ютера на інший при натисканні користувачем певного комбінації клавіш на клавіатурі, наприклад **CTRL > CTRL > A > УВЕДЕННЯ** для роботи з першим підключеним комп'ютером **і CTRL > CTRL > B > УВЕДЕННЯ** для переходу на наступний комп'ютер.

3.3.2 Пристрої виводу

DLP – цифрова обробка світла, технологія, використовувана в проекторах. У проекторах DLP використовується обертовий кольоровий диск із дзеркальною матрицею, керованої мікропроцесорами, яка називається цифровим мікродзеркальним пристроєм (DMD). Кожне дзеркало відпові-

дає певному пікселю. Кожне дзеркало відбиває світло або на лінзу, або на радіатор. У такий спосіб створюється монохромне зображення, що має до 1024 відтінків сірого між чорним і білим. Потім для створення кольорового проектованого зображення використовується кольоровий диск.

Монітор (monitor) або **дисплей** (display) – електронний пристрій для відображення інформації. Пристрій, призначений для відтворення відеосигналу і візуального відображення інформації, отриманої від комп'ютера рис. 3.76.



Рис. 3.76 – Монітор, принтер, динаміки

Додаткову інформацію, присвячену вибору монітора, див. здесь.

Примітка. До застарілих типів моніторів ставляться монітори з електронно-променевими трубками (ЕЛТ).

Принтери – це пристрої виводу, за допомогою яких можна створювати паперові копії файлів, збережених у комп'ютері. Деякі принтери використовуються тільки в певних метах, наприклад, для печатки кольорових світлин. Багатофункціональні пристрої (БФП) призначені для виконання безлічі завдань: друк, сканування, передача факсів і створення ксерокопій рис. 3.76.

Динаміки й навушники – це пристрою виводу аудіосигналів. У більшості комп'ютерів аудіо забезпечується або інтегрованим у материнську плату адаптером, або окремим адаптером – звуковою картою. Підтримка аудіо містить у собі порти введення й виводу аудіосигналів. Звукова карта оснащена підсилювачем для навушників і зовнішніх динаміків рис. 3.76.

Телевізори також ставляться до пристроїв виводу, однак вони можуть забезпечувати можливості введення. Смарт-телевізори працюють під керуванням операційної системи й можуть одержувати дані як від користувача, так і від безлічі джерел контенту в Інтернеті, від смартфонів і планшетів, а також від інших підключених до телевізора пристроїв. Смарт-телевізор практично зводить нанівець необхідність у телевізійній

приставці. Телевізійна приставка призначена для підключення звичайного телевізора до джерел контенту, таким як кабельне телебачення, супутникове телебачення або потокове віщання онлайн.

3.3.3 Характеристики моніторів

Розрізнювальна спроможність екрана монітора пов'язане з рівнем точності відтворення зображення. Більш високий дозвіл означає більш висока якість зображення.

З розрізнювальною спроможністю екрану монітора пов'язані наступні поняття:

Піксель – ця англійська абревіатура, що означає елемент зображення (picture element). Пікселі – це дрібні крапки, з яких полягає екран. Кожний піксель складається із трьох субпікселів червоного, синього й зеленого квітів (RGB).

Розмір крапки – це відстань між пікселями екрана. Чим менше розмір крапки, тем вище якість зображення.

Контрастність – коефіцієнт контрастності позначає різницю між інтенсивністю світла самої яскравої крапки (білий) і самої темної крапки (чорний). Монітор з коефіцієнтом контрастності 10 000:1 буде давати більш бляклі відтінки білого й більш світлі відтінки чорного в порівнянні з монітором, що володіє коефіцієнтом контрастності 1 000 000:1.

Частота відновлення екрана (refresh rate) – коефіцієнт, що позначає частоту відновлення зображення в секунду (виміряється в герцах [Гц]). Чим більше частота відновлення, тем вище якість зображення.

Частота кадрів (frame rate) – це частота, з якої джерело відеозображення може видавати нові кадри для їхнього відображення на екрані. Частота відновлення екрана монітора, вимірювана в герцах, прямо відповідає його максимальній частоті кадрів у секунду (FPS). Наприклад, монітор із частотою відновлення екрана 144 Гц відображає максимум 144 кадрів у секунду.

Черезрядкове/прогресивне розгорнення – на моніторах із черезрядковим розгорненням зображення створюється за два проходи. При першому проході виводяться непарні рядки екрана знизу нагору, при другому – парні рядки. У моніторах із прогресивним розгорненням зображення створюється за один прохід порядково зверху вниз.

Горизонтальна, вертикальна і колірна спроможність – число пікселів у рядку називається горизонтальним дозволом. Число рядків екрана називається вертикальним дозволом. Кількість відтворених квітів називається колірним розрізнювальням.

Співвідношення сторін – відношення розмірів видимої області монітора по горизонталі й вертикалі. Наприклад, дозвіл QSXGA становить 2560 пікселів по горизонталі й 2048 пікселів по вертикалі, у результаті чого співвідношення сторін становить 5:4. Якщо видима область має

ширину 16 дюймів і висоту 12 дюймів, то співвідношення сторін буде 4:3. У видимої області шириною 24 дюйма й висотою 18 дюймів співвідношення сторін також становить 4:3.

Власна спроможність – число пікселів у самого монітора. Монітор, що має дозвіл 1280 x 1024, має 1280 пікселів по горизонталі й 1024 пікселя по вертикалі. Власний режим – це режим, у якому зображення, що відправляється на монітор, відповідає його власному розрізнювальні.

У табл. . 3.18 представлені розповсюджені дозволи й співвідношення сторін екранів моніторів.

Таблиця 3.18 – Розрізнювальна спроможність екранів моніторів

Стандарт монітора	**Число пікселів по горизонталі й вертикалі**	**Співвідношення сторін**
VGA	640 x 480	4:3
SVGA	800 x 600	4:3
HD	1280 x 720	16:9
WXGA	1280 x 800	16:10
SXGA	1280 x 1024	5:4
QHD	1440 x 2560	16:9
UXGA	1600 x 1200	4:3
PHD	1920 x1080	16:9
UHD	3840 x 2160	16:9
WQUXGA	3840 x 2400	16:10
PUHD	7680 x 4320	16:9
QUHD	15 360 x 8640	16:9

Монітори мають засобу настроювання якості зображення. Нижче наведені розповсюджені параметри моніторів:

Яскравість – інтенсивність зображення

Контрастність – співвідношення яскравостей найяснішої й самої темної частин зображення

Місце розташування – положення зображення на екрані по горизонталі й вертикалі

Скидання – скидання параметрів монітора до заводських

Використання додаткових моніторів на робочому місці може підвищити продуктивність праці користувача. Додаткові монітори дозволяють побільшати розміри робочого стола або дублювати його й переглядати більше відкритих вікон. Багато комп'ютерів мають вбудовану підтримку декількох моніторів. Для настроювання декількох моніторів необхідне наступне обладнання:

- два відеопорти або більш;
- додаткові монітори.

3.4 Вибір компонентів для зборки комп'ютера

При складанні або модернізації комп'ютера слід ураховувати ряд важливих моментів рис. 3.77.

Перед покупкою компонентів необхідно спочатку визначити, для яких цілей він буде використовуватися. Які завдання планується виконувати на комп'ютері? Чи буде комп'ютер використовуватися всіма членами родини? Чи збираєте ви робочу станцію для замовника в архітектурному бюро, де користувачі працюють із додатками, що інтенсивне споживають ресурси відеоадаптера, такими як Autocad? Або ж ви збираєте комп'ютер для ігор, який дозволив би користувачеві обійти суперників в іграх?

Потім необхідно відповістити на запитання, що стосується кількості й типів зовнішніх пристроїв, які планується підключити до комп'ютера. чи вимагається створювати систему RAID? Чи планує замовник підключати до комп'ютера застарілі компоненти? Чи вимагається встановити високопродуктивну плату відеоадаптера?

Призначення комп'ютера й типи зовнішніх компонентів прямо впливають на вибір материнської плати. Вона повинна забезпечити можливість установки бажаного ЦП і системи його охолодження, необхідної оперативної пам'яті потрібного обсягу. Крім того, материнська плата повинна бути оснащена необхідною кількістю портів і слотів розширення потрібних типів.



Новий комп'ютер

Для яких цілей планується використовувати комп'ютер?

Які компоненти необхідно до нього підключити?

У який бюджет слід укластися?

Рис. 3.77 – Зборка комп'ютеру

3.4.1 Вибір материнської плати

Нові материнські плати часто мають нові функції або стандарти, які можуть бути несумісні з більш старими компонентами/ При виборі материнської плати на заміну перевірте, чи підтримує вона вже встановлені ЦП, ОЗП, відеоадаптер і інші плати адаптерів рис. 3.78. Процесорне роз'єм й чипсет материнської плати повинні бути сумісними зі ЦП. Материнська плата також повинна вміщати існуючий радіатор і вентилятор,

якщо використовується старий ЦП. Звернете особливу увагу на кількість і тип слотів розширення. Перевірте, чи відповідають вони вже існуючим платам адаптерів і чи допускають використання нових плат. Існуючий блок живлення повинен мати роз'єм, що відповідають новій материнській платі. І, нарешті, нова материнська плата повинна фізично міститися у вже існуючий корпус комп'ютера.

При складанні комп'ютера вибирайте чипсет, що відповідає вашим потребам. Наприклад, можна придбати материнську плату із чипсетом, який дозволяє використовувати кілька портів USB, роз'єм ESATA, об'ємний звук і відео.

Корпус ЦП повинен відповідати типу роз'єм або гнізда материнської плати. У корпус ЦП входять властиво мікросхема ЦП, точки підключення й матеріали, що оточують ЦП, що й розсіюють тепло.

Дані передаються з однієї частини комп'ютера в іншу через набір проводів, відомий як шина. Шина складається із двох частин. Частина шини, відповідальна за дані, відома як шина даних. По ній дані передаються між компонентами комп'ютера. Частина, відповідальна за адресацію, називається шиною адреси. По ній передаються адреси місць розташування пам'яті, по яких ЦП може прочитати або записати дані.



Рис. 3.78 – Материнська плата

Від розміру шини залежить кількість даних, переданих одноразово. По 32-розрядній шині одночасно передаються 32 біта даних із процесора в ОЗП або в інші компоненти материнської плати. По 64-розрядній шині одночасно передаються 64 біта даних. Швидкість, з якої дані передаються через шину, визначається тактовою частотою, яка вимірюється в мегагерцах або гігагерцах.

Слоти розширення PCI з'єднані з паралельною шиною, яка відправляє трохи біт даних по безлічі провідників одночасно. Замість слотів розширення PCI у цей час використовуються слоти PCIe, що підключаються до послідовної шини, по якій передаються незалежні дані від кожного пристрою з більш високою швидкістю.

При складанні комп'ютера слід вибирати материнську плату, яка має слоти, що відповідають поточним і прогнозованим потребам користувача.

3.4.2 Вибір корпусу й вентиляторів

Вибір материнської плати й зовнішніх компонентів прямо впливає на вибір корпусу й блоку живлення. Ці компоненти необхідно вибирати з урахуванням формфактора материнської плати. Наприклад, для материнської плати ATX потрібні корпус і блок живлення, сумісні із цим формфактором.

Часто корпуси продаються із уже встановленим блоком живлення. У цьому випадку необхідно перевірити, чи забезпечує блок живлення достатню потужність для роботи всіх компонентів, які будуть установлені в корпусі.

Можна вибрати більш об'ємний корпус, щоб у майбутньому встановити додаткові компоненти. Або можна вибрати більш компактний корпус, який займає мінімум місця. У цілому корпус повинен бути міцним, простим в обслуговуванні, а також мати досить простору для установки додаткових компонентів.

На рис. 3.79 наведені різні фактори, що визначають вибір корпусу комп'ютера.

Безліч внутрішніх компонентів комп'ютера виділяють тепло під час роботи. Для подачі охолодного повітря в корпус комп'ютера й відведення тепла повинні бути встановлені вентилятори усередині корпусу.

Тип моделі корпусу

Вибір моделі корпусу залежить від типу материнської плати.

Необхідно точна відповідність по розміру й формі.

При виборі вентиляторів для корпуса необхідно врахувати фактори, представлені

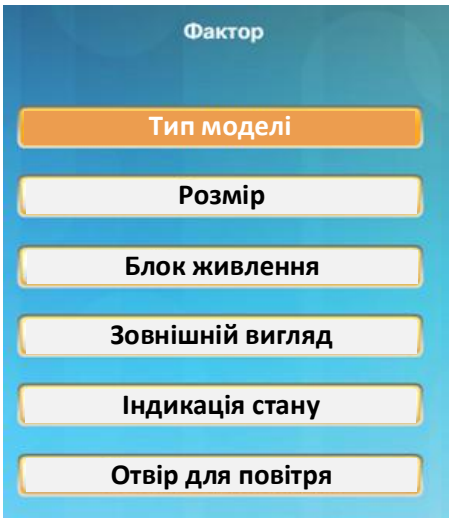


Рис. 3.79 – Вибір корпусу комп'ютера

При виборі вентиляторів для корпусу необхідно врахувати фактори, представлені в табл. 3.19.

Примітка. Напрямок потоку повітря, створюваного всіма вентиляторами в корпусі, повинне бути однаковим, щоб забезпечувати відтік нагрітого повітря й приплив холодного. Неправильна орієнтація вентилятора при установці або використання вентиляторів невідповідного розміру або швидкості може привести до створення зустрічних потоків повітря, які будуть заважати один одному.

Таблиця 3.19 – Вибір вентиляторів для корпусу

Фактори	Необхідно враховувати...|
Розмір корпусу	Для більших корпусів звичайно потрібні більші вентилятори, оскільки вентилятори невеликого розміру не можуть створити достатній потік повітря.
Швидкість роботи вентилятора	Більші вентилятори обертаються повільніше, що скорочує рівень шуму.
Число встановлених у корпусі компонентів	Безліч компонентів, установлених у корпусі комп'ютера, виділяють додаткове тепло, що вимагає установки більшої кількості вентиляторів, більших вентиляторів або вентиляторів з більш високою швидкістю обертання.
Фізичне середовище	Установлені в корпусі вентилятори повинні розсіювати достатня кількість тепла, щоб уникнути перегріву внутрішніх компонентів.
Число місць для установки вентиляторів	Різні корпуси мають різна кількість місць для установки вентиляторів.
Розташування місць для установки вентиляторів	Різні корпуси мають різні місця розташування для установки вентиляторів.
Електричні підключення	Деякі вентилятори підключаються до материнської плати прямо, інші підключаються прямо до блоку живлення.

3.4.3 Вибір блоку живлення

Блок живлення перетворить вхідний змінний струм у вихідний постійний струм. Як правило, блоки живлення дають напруга в 3,3 В, 5 В и 12 В. Їхня потужність виміряється у ватах (Вт). Блок живлення повинен надавати достатнє електроживлення для всіх установлених компонентів, а також для тих компонентів, які можуть бути додані пізніше. Якщо ви вибираєте блок живлення, виходячи тільки з існуючих потреб уже встановлених компонентів, може знадобитися його заміна при відновленні або додаванні інших компонентів.

У табл. 3.20 на малюнку представлені відомості про різних факторів, які слід ураховувати при виборі блоку живлення.

При підключенні кабелів блоку живлення до інших компонентів слід проявляти обережність. Якщо роз’єм не вставляється з невеликим зусиллям, по-перше, перевірте, не потрапили чи в роз’єм сторонні предмети, по-друге, переконаєтеся, що штирьки роз’єм не погнуті, і по-третє, спробуйте змінити положення роз’єм. Якщо при підключенні кабелю або іншої деталі доводиться прикладати помітні зусилля, щось не так. Кабелі, роз’єм й компонента спроектовані таким чином, щоб для підключення не було потрібно велике зусилля. Ніколи не застосовуйте силу при підключенні роз’єм або компонента. Невірне підключення роз’єм може ушкодити й роз’єм, і гніздо. Не квапитеся й перевірте, чи правильно ви підключаєте обладнання.

Таблиця 3.20 – Фактори при виборі блоку живлення

Фактори	Необхідно враховувати...
Тип материнської плати	Блок живлення повинен бути сполучимо з материнською платою.
Необхідна потужність	Складете значення потужності кожного компонента, щоб довідатися сумарну потужність, яка буде потрібно для роботи комп'ютера. Якщо для компонента не зазначена споживана потужність, підрахуйте її, помноживши напругу на силу струму. Якщо для компонента необхідний інший рівень потужності, виберіть більш високі вимоги.
Число встановлених у корпусі компонентів	Переконаєтеся в тому, що потужності блоку живлення досить для роботи вже встановленого встаткування із запасом не менш 25 %.
Типи компонентів	Переконаєтеся в тому, що блок живлення оснащений роз'ємами живлення підходящих типів.
Тип корпусу	Переконаєтеся, що блок живлення підходить для установки в бажаний корпус.

3.4.4 Вибір ЦП і системи охолодження процесора

Перед придбанням ЦП перевірте, чи сполучимо він із уже існуючою материнською платою. Веб-сайти виробників – гарне джерело відомостей про сумісність ЦП із іншими пристроями.

У табл. 3.21 представлені **відомості про різні сокети і процесори, які можна в них установлювати**.

Таблиця 3.21 – Відомості про різні сокети і процесори, які можна в них установлювати

Роз'єм Intel	Архітектура	Роз'єм AMD	Архітектура
775	Land Grid Array (LGA)	AMD	Pin Grid Array (PGA)
1155	LGA	AM3+	PGA
1156	LGA	FM1	PGA
1150	LGA	FM2	PGA
1366	LGA	FM2+	PGA
2011	LGA		

При модернізації ЦП переконаєтеся, що буде використовуватися правильна напруга. Модуль стабілізатора напруги інтегрована в материнську плату. Настроїти параметри напруги, що подавати на ЦП, можна в BIOS або UEFI. Швидкість роботи сучасних процесорів виміряється в гігагерцях. Номінальна частота процесора означає максимальну швидкість, на якій процесор точно працює без помилок. Нижче наведено два основні фактори, що обмежують швидкість роботи процесора.

Мікросхема процесора являє собою набір транзисторів, зв'язаних один з одним провідниками. Передача даних по транзисторах і провідникам викликає затримки.

У міру того як стан транзисторів міняється із включеного на виключене й навпаки, виробляється невелика кількість тепла. У міру росту швидкості роботи процесора обсяг вироблюваного тепла росте. Коли процесор перегрівається, він починає працювати з помилками.

Системна шина – це шлях між ЦП і північним мостом. Вона використовується для з'єднання різних компонентів, таких як чипсет і плати розширення, з ОЗУ. Дані передаються по системній шині в обох напрямках. Частота роботи шини виміряється в мегагерцах. Частота, з якої працює ЦП, визначається шляхом множення швидкості роботи системної шини на множник швидкості процесора. Наприклад, у процесорі, що працює зі швидкістю 3200 МГц, може використовуватися системна шина із частотою 400 Мгц. Якщо розділити 3200 МГц на 400 МГц, ми одержимо 8. Отже, ЦП працює у вісім раз швидше системної шини.

Процесори діляться на 32– і 64-розрядні. Основна відмінність полягає в числі команд, які процесор може обробити одноразово. 64-розрядний процесор обробляє більше команд на такт, чім 32-розрядний. 64-розрядний процесор також підтримує більше пам'яті. Щоб використовувати можливості 64-розрядного процесора, перевірте, чи підтримують установлені операційна система й додатки цей тип процесора.

Центральний процесор – один з найбільш дорогих компонентів у комп'ютері, що вимагає особливого обігу. ЦП виділяє дуже багато тепла, тому для охолодження більшості ЦП необхідні радіатор і вентилятор.

В табл. 3.22 перераховані деякі фактори, які слід ураховувати при виборі системи охолодження ЦП.

Таблиця 3.22 – Фактори вибору системи охолодження ЦП

Фактори	**Необхідно враховувати...**
Тип роз’єм	Типи радіатора й вентилятора повинні відповідати типу роз’єм на материнській платі.
Фізичні характеристики материнської плати	Радіатор і вентилятор не повинні заважати іншим компонентам, підключеним до материнської плати.
Розмір корпусу	Радіатор і вентилятор повинні міститися усередині корпусу.
Фізичне середовище	Радіатор і вентилятор повинні мати можливість розсіювати досить тепла, щоб ЦП не нагрівався в теплому середовищі.

3.4.5 Вибір ОЗП

Якщо додатки зависають або комп'ютер часто виводить повідомлення про помилки, може знадобитися нове ОЗП. Щоб визначити, чи зв'язана ця проблема з ОЗП, виконаєте тест оперативної пам'яті в BIOS. Якщо така можливість відсутня, скористайтеся спеціальною програмою для тестування ОЗП. Також можна замінити модуль ОЗП свідомо справним модулем. Перезавантажите комп'ютер, щоб перевірити, чи працює він без помилок.

При виборі нового ОЗП необхідно перевірити, чи сумісне воно із уже встановленою материнською платою. Крім того, швидкість нового ОЗП повинна підтримуватися чипсетом. При покупці нового ОЗП корисно побрати із собою вихідний модуль пам'яті рис. 3.80.



Рис. 3.80 – ОЗП

Пам'ять розділяється на небуферізуєму й буферізуєму.

Небуферізуєма пам'ять – це звичайна пам'ять для комп'ютерів. Комп'ютер зчитує дані прямо із блоку пам'яті, завдяки чому досягається швидкодія більша, ніж може забезпечити буферізуєма пам'ять. Однак існує обмеження на обсяг ОЗП, який можна встановити в комп'ютер.

Буферізуєма пам'ять – спеціальна пам'ять для серверів і високопродуктивних робочих станцій, де використовується ОЗП великого обсягу. У модулях таких схем пам'яті є вбудована схема управління. Керуючий чип допомагає контролеру пам'яті управляти більшими обсягами оперативної пам'яті. Буферізуємі ОЗП не слід установлювати на ігрові комп'ютери й робочі станції із середньою продуктивністю, оскільки наявність додаткової схеми контролера знижує швидкість обробки даних оперативною пам'яттю.

На рис. 3.81. наведені фактори, які слід ураховувати при виборі нової плати вводу-виводу.

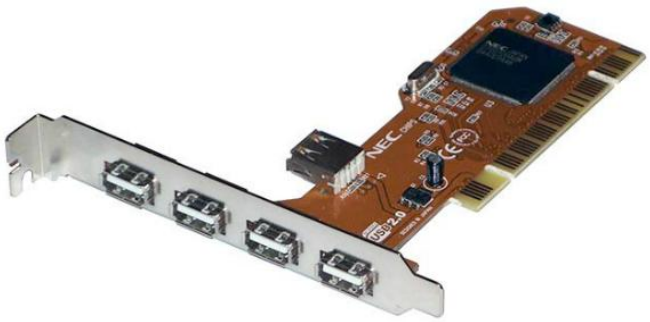


Рис. 3.81 – Фактори, які слід ураховувати при придбанні нової плати введення-виводу

- Тип роз’єм
- Тип порту введення-виводу
- Кількість портів уведення-виводу
- Додаткові вимоги до живлення

Мережеві інтерфейсні плати – замовники обновляють плати мережевих адаптерів, щоб підвищити швидкість і побільшати пропускну здатність. На рис. 3.82. наведені фактори, які слід ураховувати при виборі нової мережевої плати.

Плати захвату – такі плати необхідні для імпорту відео в комп'ютер і запису його на жорсткий диск. Додавання плати захвату із ТВ-тюнером дозволяє переглядати й записувати телевізійні програми. Система комп'ютера повинна мати досить потужний ЦП, ОЗП достатнього

обсягу й швидкодії й високошвидкісною системою зберігання для того, щоб відповідати вимогам замовника в області цифрування, записи й редагування відео. Вибирайте плату захвату на основі поточних і прогнозованих потреб замовника. Наприклад, якщо замовнику необхідний запис однієї програми під час перегляду іншої, слід установити кілька плат захвату або одну плату з декількома ТВ-тюнерами.



Рис. 3.82 – Фактори, які слід ураховувати при придбанні нового мережного адаптера

- Тип слота
- Швидкість передачі даних
- Тип роз'єм
- Підключення до провідної або безпроводової мережі
- Сумісність зі стандартами

На рис. 3.83. наведені фактори, які слід ураховувати при виборі нової плати захвату.



Рис. 3.83 – Фактори, які слід ураховувати при придбанні нової плати захвату

- Тип роз'єм
- Дозвіл і частота кадрів
- Порт уведення-виводу
- Стандарти форматів

На рис. 3.84 – 3.86 наведені фактори, які слід ураховувати при придбанні нових плат графічної карти, звукової карти, контролера пристроїв зберігання даних, відповідно.



Рис. 3.84 – Фактори, які слід ураховувати при придбанні нової графічної плати

- Тип роз'єм
- Тип порту
- Обсяг і швидкість відео ОЗП
- Графічний процесор
- Максимальна розрізнювальна спроможність



Рис. 3.85 – Фактори, які слід ураховувати при придбанні нової звукової карти

- Тип роз’єм
- Цифровий сигнальний процесор (ЦСП)
- Частота дискретизації
- Типи портів і роз'ємів
- Апаратний декодер
- Відношення сигнал/шум



Рис. 3.86 – Фактори, які слід ураховувати при придбанні нової плати контролера пристроїв зберігання даних

- Тип роз’єм
- Кількість контактів у роз’ємі
- Зовнішні або внутрішні підключення
- Розмір плати
- ОЗП плати контролера Процесор плати контролера
- Тип RAID

Питання, що стосуються придбання плати адаптера:

- Чи є на материнській платі вільний слот розширення?
- Чи сумісна плата адаптерів з вільним слотом?
- Які поточні й прогнозовані потреби замовника?
- Які можливі варіанти комплектації?

Наприклад, якщо користувачу потрібно додати внутрішній пристрій читання карт, а на материнській платі немає внутрішнього роз’єм USB, необхідна карта введення-виводу USB із внутрішнім роз’ємом USB.

3.4.6 Вибір жорстких дисків

Якщо внутрішній пристрій зберігання даних більше не відповідає вимогам замовника або відмовляє, може знадобитися його заміна. Ознаками збоїв у роботі внутрішнього пристрою зберігання даних можуть служити незвичайні звуки, видавані пристроєм під час роботи, вібрація, повідомлення про помилки, випадки ушкодження даних або неможливість завантажити додатка.

На рис. 3.87 наведені фактори, які слід ураховувати при виборі нового жорсткого диска.

Внутрішні приводи звичайно підключаються до материнської плати через інтерфейс SATA, а зовнішні пристрої зберігання даних – через інтерфейс USB, esata або Thunderbolt.

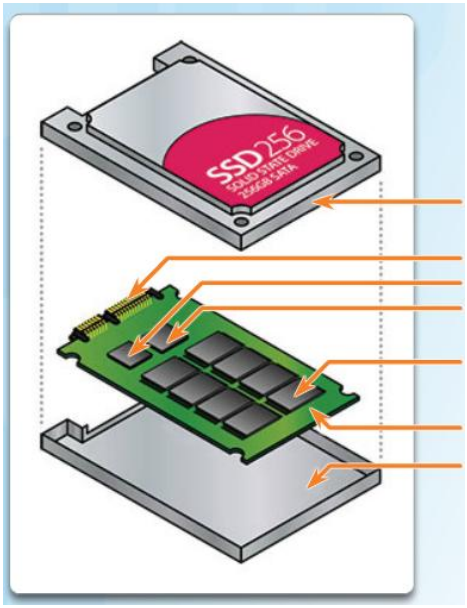
На рис. 3.88 показані компоненти твердотільного накопичувача (SSD).

Примітка. Кабелі SATA і ESATA мають схожий зовнішній вигляд, але не є взаємозамінними.



Рис. 3.87 – Фактори, які слід ураховувати при виборі жорсткого диска

- Зовнішній або внутрішній
- HDD, SSD або SSHD
- Можливість гарячої заміни
- Виділення тепла
- Вироблений шум
- Споживана потужніст



Верхня кришка

Інтерфейсний роз’єм

Мікросхема кеш-пам'яті

Мікросхема контролера

Мікросхеми NAND на обох сторонах логічної плати

Логічна плата

Нижня кришка

Рис. 3.88 – Компоненти твердотільного накопичувача

3.4.7 Вибір пристрою читання носіїв

Пристрій читання носіїв – це пристрій, який виконує зчитування й запис на різні типи карт пам'яті, які використовуються в цифрових фотоапаратах, смартфонах або MP 3-програвачах. При заміні пристрою читання носіїв перевірте, чи підтримує воно тип використовуваних пристроїв зберігання даних і їх ємність.

На рис. 3.89 наведені фактори, які слід ураховувати при виборі пристрою читання носіїв.



Рис. 3.89 – Придбання нового пристрою читання носіїв
Підтримувані карти пам'яті
Зовнішній або внутрішній
Тип роз'єму

Вибирайте такий пристрій на основі поточних і прогнозованих потреб замовника. Наприклад, якщо замовникові необхідно використовувати різні типи карт пам'яті, потрібно багатоформатний пристрій читання носіїв. Розповсюджені типи карт пам'яті показані на рис. 3.90.

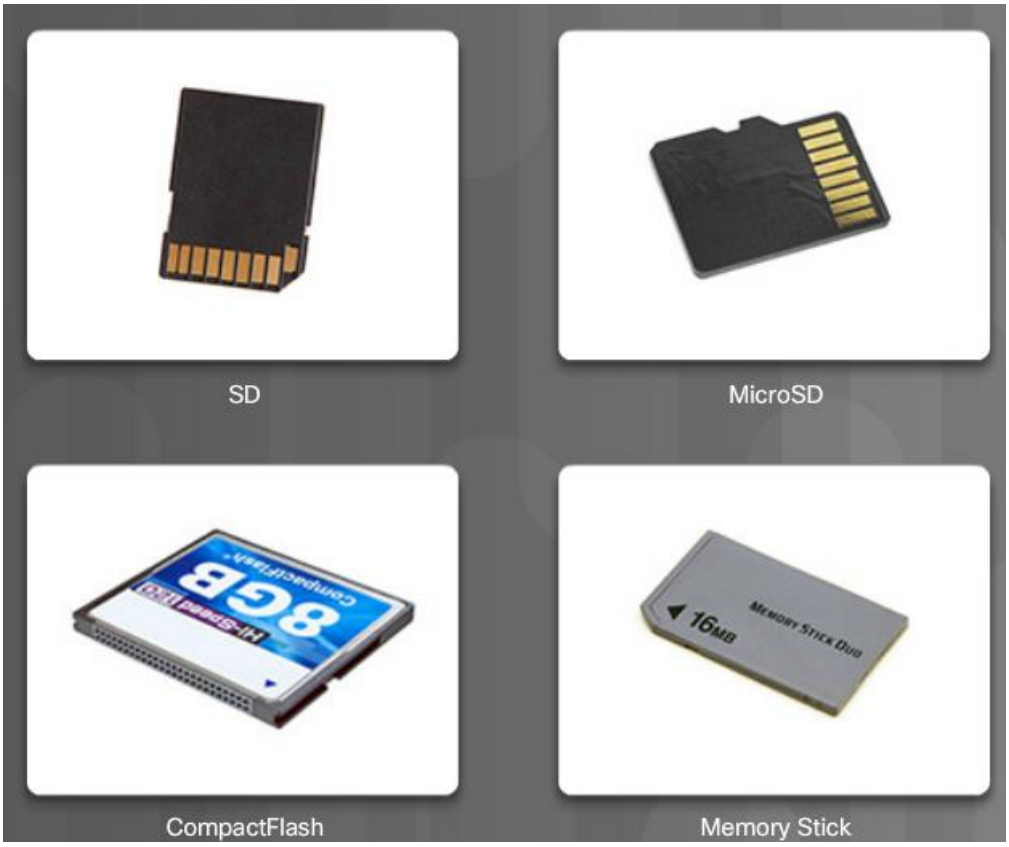


Рис. 3.90 – Розповсюджені карти пам'яті

Карта Secure Digital (SD) – карти SD призначені для використання в портативних пристроях, таких як фотоапарати, MP 3-програвачі й ноутбуки. Ємність карт SD становить до 2 ГБ. Карти SD великої ємності (SDHC) мають ємність до 32 ГБ, а карти SD розширеної ємності (SDXC) – до 2 ТБ даних.

Microsd – значно зменшена версія карти SD, широко використовувана в смартфонах і планшетах.

Minisd – карта SD, розмір якої більше карти microsd, але менше звичайної карти Secure Digital. Карти такого формату були розроблені для мобільних телефонів.

Compactflash – застарілий формат, який, проте, широко використовується завдяки своїй високій ємності (як правило, до 128 ГБ) і високої швидкості. Карти Compactflash часто використовуються у відеокамерах.

Memory Stick – карти Memory Stick, розроблені корпорацією Sony, використовуються у фотоапаратах, MP 3-програвачах, системах кишенькових відеоігор, мобільних телефонах і інших портативних електронних пристроях.

emmc – карти Embedded Multimediacard широко використовуються в смартфонах і деяких планшетах.

xd – також називані Picture Card; такі карти використовувалися в деяких цифрових фотоапаратах.

3.4.8 Вибір приводів оптичних дисків

Привод оптичних дисків використовує лазер для читання й запису даних на оптичних носіях.

На рис. 3.91 наведені фактори, які слід ураховувати при виборі привода оптичних дисків.



Рис. 3.91 – Придбання нового привода оптичних дисків

- Тип роз'єму
- Можливості зчитування
- Можливості запису

У таблиці на табл. 3.23 представлені зведені відомості про можливості привода оптичних дисків.

Таблиця 3.23 – Придбання нового привода оптичних дисків

Оптичний пристрій	Читання компакт-дисків	Запис компакт-дисків	Читання дисків DVD	Запис дисків DVD	Читання дисків Blu-ray	Запис дисків Blu-ray	Перезапис дисків Blu-ray
CD-ROM	+	-	-	-	-	-	-
CD-RW	+	+	-	-	-	-	-
DVD-ROM	+	-	+	-	-	-	-
DVD-RW	+	+	+	+	-	-	-
BD-ROM	+	-	+	-	+	-	-
BD-R	+	+	+	+	+	+	-
BD-RE	+	+	+	+	+	+	+

На диск DVD можна записати значно більше інформації, чому на компакт-диск, а диски Blu-ray дозволяють зберігати значно більше даних, чому диски DVD. Диски DVD і BD також можуть мати два шари для запису даних, завдяки чому обсяг записуваних даних можна фактично подвоїти.

3.4.9 Вибір зовнішнього накопичувача

Зовнішній накопичувач – це портативність і зручність роботи на декількох комп'ютерах. Зовнішній накопичувач підключається до зовнішнього порту, наприклад USB, ESATA або Thunderbolt. Прикладом знімного накопичувача можуть служити зовнішні флеш-диски, іноді називані флешками, що підключаються через порт USB.

На рис. 3.92 наведені фактори, які слід ураховувати при виборі зовнішнього накопичувача.



Рис. 3.92 – Фактори, які слід ураховувати при виборі зовнішнього накопичувача

- Тип порту
- Ємність накопичувача
- Швидкість
- Портативність
- Споживана потужність

Вибирайте тип зовнішнього накопичувача, що відповідає потребам замовника. Наприклад, якщо замовникові потрібно переносити невеликі обсяги даних, наприклад одну презентацію, гарним вибором стане придбання флеш-диска. Якщо замовникові потрібно виконувати резервне копіювання або перенос більших обсягів даних, виберіть зовнішній жорсткий диск.

3.4.10 Вибір обладнань вводу-виводу

Вибирайте апаратне й програмне забезпечення на основі вимог замовника. Довідавшись, які обладнання введення або висновку необхідні замовникові, необхідно визначити, як підключати їх до комп'ютера.



Рис. 3.93 – Розповсюджені роз'єми введення й виводу

На рис. 3.93 показана задня панель комп'ютера з декіль-

кома розповсюдженими роз’ємами. Інженери повинні мати чітку виставу про різні типи інтерфейсів і портів.

3.5 Товсті клієнти й тонкі клієнти

Іноді для позначення комп'ютера використовують наступні терміни:

Товсті клієнти – стандартні комп'ютери, які розглядалися раніше в цій главі. У комп'ютерів є власна операційна система, різні додатки й локальне сховище даних. Вони є автономними системами, і для їхньої роботи не потрібне підключення до мережі. Усі обчислення виконуються локально на комп'ютері.

Тонкі клієнти – звичайно це мережні комп'ютери з обмеженими можливостями, які для обробки всіх даних використовують ресурси вилученого сервера. Для роботи тонким клієнтам потрібне мережне з'єднання із сервером, а для доступу до ресурсів звичайно використовується веб-браузер. Однак у якості клієнта може виступати комп'ютер, на якому встановлено ПО тонкого клієнта, або невеликий виділений термінал, що полягає з монітора, клавіатури й миші. Звичайно в тонких клієнтах не передбачене внутрішнє сховище, а їх локальні ресурси вкрай обмежені.

У табл. 3.24 перераховані відмінності між товстими й тонкими клієнтами.

Таблиця 3.24 – Відмінності між товстими й тонкими клієнтами

Фактори	**Товсті клієнти**	**Тонкі клієнти**
Необхідні ресурси	**Монітор, миша, клавіатур вертикальний корпус (зі ЦП і ОЗП), внутрішнє сховище**	**Монітор, миша, клавіатура невеликий корпус**
Розміри	Великі	Малі
Доступ до мережі	Необов'язково	Обов'язково
Обробка даних	Локально на комп'ютері	Віддалено на серверах
Обсяг робіт по розгортанню в організації	Більше	Менше
Вартість робіт з розгортання в організації	Більше	Менше

Крім товстих і тонких клієнтів, існують комп'ютери, розроблені для виконання певних завдань. В обов'язку комп'ютерного інженера входять оцінка й вибір підходящих компонентів, а також модернізація або складання спеціалізованих комп'ютерів відповідно до вимог замовників.

У даному розділі розглядаються деякі з таких спеціалізованих комп'ютерів.

3.5.1 Робочі станції Cax

Прикладом спеціалізованого комп'ютера може служити робоча станція, використовувана для комп'ютерного проектування (CAD) або автоматизованого виробництва (CAM).

Робоча станція CAD або CAM (Cax), як показано на рис. 3.94, використовується для проектування продуктів і керування процесом виробництва. Робочі станції Cax використовуються для створення креслень, проектування житлових будинків, автомобілів, літаків, комп'ютерів і багатьох деталей товарів, що ввійшли в повсякденний побут. Комп'ютер, використовуваний для виконання ПО Cax, повинен відповідати його потребам і потребам обладнань уведення-висновку, необхідних користувачеві для проектування й виробництва продукції. ПО Cax звичайно є складним і вимагає надійного встаткування.

При необхідності в запуску ПО Cax розглянете варіанти придбання наступного встаткування:

Потужний процесор – ПО Cax повинне в дуже швидкому темпу виконувати надзвичайно великий обсяг обчислень. Він повинен швидко обробляти двох– і тривимірну графіку. Для робочих станцій CAD рекомендуються швидкі багатоядерні процесори.

Високопродуктивний відеоадаптер – такі графічні плати забезпечують швидку обробку двомірної й тривимірної графіки за допомогою спеціалізованих ГП. Бажане або навіть необхідно мати кілька моніторів, щоб користувач міг працювати із програмним кодом, двомірною візуалізацією й тривимірними моделями одночасно.

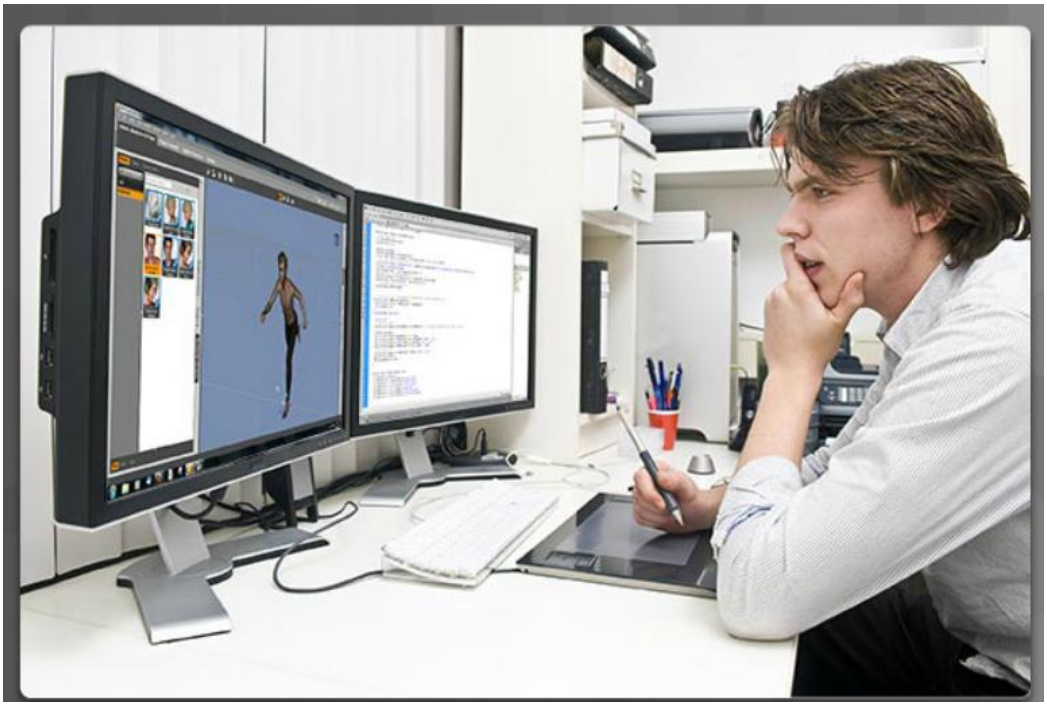


Рис. 3.94 – Робоча станція CAx

ОЗП – робоча станція Сах обробляє значні обсяги даних, тому ОЗП надто важливо. Чим більше ОЗП, тим більше даних зможе обробити процесор, перш ніж йому знадобиться зчитати дані з більш повільних жорстких дисків. Установите максимум пам'яті, підтримуваною материнською платою й операційною системою. Обсяг і швидкість роботи пам'яті повинні перевищувати мінімальні вимоги додатка Сах.

3.5.2 Робочі станції для монтажу звуку й відео

Робоча станція для монтажу звуку використовується при записі музики, створенні музичних компакт-дисків і наклейок для компакт-дисків. Робоча станція для монтажу відео може використовуватися при створенні телевізійної реклами, складанні вечірньої програми телепередач, а також при створенні фільмів для кінотеатрів або домашнього перегляду.

При складанні комп'ютера, на якому виконується монтаж звуку й відео, поєднуються спеціалізовані встаткування й програмне забезпечення. ПО для запису й монтажу звуку на робочій станції для монтажу звуку (див. рис. 3.95) використовується для запису звуку, керування звучанням за допомогою мікшування й спецефектів, а також фінальної обробки записів для публікації. ПО для запису й монтажу відео використовується для вирізання, копіювання, комбінування й редагування фрагментів відео. За допомогою цього ПО можна також додавати спецефекти у відео.

Для використання ПО для монтажу звуку й відео може знадобитися наступне встаткування.

Спеціалізована звукова плата – при записі музики на комп'ютер у студії може знадобитися передавати кілька потоків вхідних даних від мікрофонів і багато потоків вихідних даних на встаткування для спецефектів. Для цих цілей буде потрібно звукова плата, що підтримує потрібну кількість потоків вхідних і вихідних даних. Розглянете характеристики звукових плат різних виробників і ознайомтеся з конкретними вимогами замовників, щоб вибрати звукову плату, відповідну до всіх вимог сучасної студії звукозаписи або обробки звуку.

Спеціалізована відеоплата – для комбінування й монтажу різних відеопотоків і спецефектів у режимі реального часу необхідна відеоплата з підтримкою високого дозволу й декількох дисплеїв. Ознайомтеся з конкретними вимогами замовників і розглянете характеристики відеоплат, щоб установити плату, яка може обробляти більші обсяги інформації, що надходять із сучасних відеокамер і апаратури спецефектів.

Жорсткі диски з високою швидкодією й великою ємністю – сучасні відеокамери здійснюють запис у високому дозволі й з високою частотою кадрів. Це приводить до формування більших обсягів даних. Жорсткі диски маленької ємності будуть швидко заповнюватися, а жорсткі диски з низькою швидкодією не будуть задовольняти вимогам, що навіть може викликати втрату кадрів. Для запису високоякісного відео без

втрати кадрів необхідний жорсткий диск із високою швидкодією й великою ємністю, такий як SDD або SSHD. Рівні RAID, такі як 0 або 5, на яких використовується чергування, можуть підвищити швидкість читання або записи даних.

Два монітори – при роботі зі звуком або відео використання двох, трьох або більш моніторів може допомогти відслідковувати всі події, що відбуваються на декількох доріжках, кадрах, обладнаннях і програмах. Рекомендуються плати з інтерфейсами HDMI, Displayport і Thunderbolt, однак можна використовувати й плати з роз'ємом DVI. Якщо потрібно кілька моніторів, при створенні робочої станції для монтажу звуку або відео будуть потрібні спеціалізовані відеоплати.

3.5.3 Робочі станції для віртуалізації



Рис. 3.95 – Робоча станція для монтажу звуку

Вам може знадобитися зібрати комп'ютер для замовника, що використовує технології віртуалізації. Одночасний запуск двох або більш операційних систем на одному комп'ютері називається **віртуалізацією**. Часто на комп'ютері встановлюється одна операційна система, а ПО віртуалізації використовується для установки й керування додатковими установками інших операційних систем. При цьому можуть використовуватися різні операційні системи від декількох виробників ПО.

Існує ще один тип віртуалізації – інфраструктура віртуальних робітничих середовищ (Virtual Desktop Infrastructure, VDI). VDI дозволяє користувачам, увійшовши на сервер, здійснювати доступ до віртуальних комп'ютерів. Дані, що вводяться за допомогою миші й клавіатури, відправляються на сервер для керування віртуальним комп'ютером. Вихідні дані, такі як звук і відео, відправляються на динаміки й відображаються на дисплеї клієнта, з якого здійснюється доступ до віртуального комп'ютера.

Малопотужні тонкі клієнти використовують ресурси продуктивного сервера для виконання складних обчислень. Доступ до VDI для використання віртуальних комп'ютерів можна також здійснювати з ноутбуків, смартфонів і планшетів. Нижче перераховані деякі функціональні можливості віртуальних обчислень:

Тестування ПО або відновлення ПО в середовищу, яке не порушує середовище використовуваної операційної системи.

Використання на комп'ютері операційних систем відразу декількох типів, наприклад Linux або Mac OS X.

Використання мережі Інтернет без ризику ушкодити основну встановлену систему шкідливим ПО.

Запуск старих додатків, несумісних із сучасними операційними системами.

Для віртуальних обчислень потрібно могутніше встаткування, оскільки кожна установка потребує своїх власних ресурсів рис. 3.96. Одну або два віртуальні середовища можна запустити на сучасному комп'ютері із простим устаткуванням, однак для повної установки VDI може знадобитися дороге встаткування з високою швидкодією, здатне підтримувати роботу декількох користувачів у різних середовищах.

Для запуску віртуальних комп'ютерів може знадобитися наступне встаткування.

ОЗП максимальної ємності – для задоволення вимог кожного віртуального середовища й головного комп'ютера буде потрібно ОЗУ достатньої ємності. Для стандартної установки, у якій використовується тільки кілька віртуальних машин, може бути досить 1 ГБ ОЗП для підтримки сучасної операційної системи, такий як Windows 8. При наявності декількох користувачів і необхідності підтримувати багато віртуальних комп'ютерів для кожного з них може знадобитися встановити ОЗУ ємністю не менш 64 ГБ.

Ядра ЦП – незважаючи на те, що віртуальні обчислення можуть здійснюватися й на одноядерному ЦП, використання ЦП із додатковими ядрами допомагає побільшати швидкість і скоротити час відповіді при розміщенні декількох користувачів і віртуальних машин. У деяких установках VDI використовуються комп'ютери з декількома багатоядерними ЦП.



Рис. 3.96 – Робоча станція для віртуалізації

3.5.4 Ігрові ПК

Багато користувачів захоплюються комп'ютерними іграми. З кожним роком відеогри стають усе більш досконалими, і їм потрібно усе могутніше встаткування, нові типи встаткування й додаткові ресурси, щоб забезпечити плавний ігровий процес, що й приносить задоволення рис. 3.97.



Рис. 3.97 – Ігрові ПК

Вашому замовникові може знадобитися зібрати комп'ютер для відеоігор. Для складання ігрового комп'ютера може знадобитися наступне встаткування.

Потужний процесор – для підтримки відеоігор усе компоненти комп'ютера повинні взаємодіяти синхронно. Потужний процесор допомагає забезпечити своєчасну обробку всіх даних програмного забезпечення й устаткування. Такий процесор повинен підтримувати високу частоту кадрів, швидку обробку тривимірної графіки й звуку високої якості. Багатоядерні процесори допомагають скоротити час відгуку встаткування й ПО.

Високопродуктивний відеоадаптер – у сучасних відеоіграх використовуються високі дозволи й дрібна деталізація. Для забезпечення високої якості, чіткості й плавності зображень, відображуваних на моніторі, буде потрібно відеоплата зі швидким спеціалізованим графічним процесором і відеопам'яттю з високою швидкодією і ємністю. У деяких ігрових комп'ютерах використовується кілька відеоплат для забезпечення високої частоти кадрів або підтримки декількох моніторів.

Високопродуктивна звукова карта – у відеоіграх використовується трохи високоякісних аудіоканалів для занурення гравця в атмосферу гри. Високоякісна звукова карта поліпшує якість звуку в порівнянні із вбудованою звуковою картою комп'ютера. Виділена звукова карта та-

кож допомагає побільшати загальну продуктивність, розвантажуючи процесор. Аматори відеоігор найчастіше використовують спеціальні навушники й мікрофони для спілкування з іншими гравцями.

Високопродуктивна система охолодження – високорівневі компоненти часто виробляють більше тепла, чому стандартні. Для забезпечення охолодження комп'ютера під високими навантаженнями при грі в удосконалені відеоігри часто потрібно більш стабільне охолодне встаткування. Для охолодження ЦП, графічних процесорів і ОЗП часто використовуються збільшені вентилятори, радіатори й пристрою рідинного охолодження.

Велика кількість швидкої оперативної пам'яті – комп'ютерні ігри вимагають великого обсягу пам'яті. Крім того, у процесі гри постійно здійснюється доступ до відеоданих, аудіоданним і всієї необхідної для гри інформації. Чим більше ємність ОЗП комп'ютера, тем рідше доводиться звертатися до пристроїв зберігання даних. ОЗП з високою швидкодією допомагає процесору забезпечувати синхронізацію всіх даних, тому що дозволяє витягати необхідні для обчислення дані при необхідності.

Система зберігання даних з високою швидкодією – жорсткі диски 7200 і 10 000 про/хв забезпечують набагато більшу швидкість добування даних у порівнянні з дисками 5400 про/хв. Твердотільні накопичувачі й SSHD є більш дорогими, однак вони дозволяють значно побільшати продуктивність відеоігор.

Спеціалізоване ігрове встаткування – деякі ігри передбачають зв'язок з іншими гравцями. Щоб говорити з ними, необхідний мікрофон, а щоб слухати їх, необхідні динаміки або навушники. Щоб установити, чи потрібний мікрофон або головна гарнітура, з'ясуєте в замовника, у які ігри він відіграє. У деякі ігри можна відіграти в 3 D-Версії. Для використання цієї функції можуть знадобитися спеціальні окуляри й спеціальні відеоплати. Для оптимальної зручності користувача в деяких іграх краще використовувати кілька моніторів. Наприклад, авіасимулятор можна настроїти так, щоб кабіна відображалася одночасно на дві, трьох і більш моніторах.

3.5.5 Домашні кінотеатри на основі ПК

Для складання домашнього кінотеатру на основі ПК (Home Theater Personal Computer, HTPC) потрібне спеціалізоване встаткування, що забезпечує високоякісне зображення для користувача. Кожний компонент устаткування повинен підключатися й належним чином надавати необхідні сервіси й ресурси для підтримки різних вимог до системи HTPC рис. 3.98.

Корисною функцією HTPC є можливість запису відеопрограм для перегляду в майбутньому. Така функція називається зрушенням часу. Системи HTPC можуть бути розроблені для перегляду телевізійних програм у прямому ефірі, потокової передачі фільмів і вмісту Інтернету, пе-

регляду сімейних світлин і відеозаписів і навіть для роботи в Інтернеті з використанням телевізора як монітора. При складанні HTPC може знадобитися наступне встаткування.



Рис. 3.98 – Домашній кінотеатр на основі ПК

Спеціалізовані корпуси й блоки живлення – при складанні HTPC можна використовувати материнські плати меншого розміру, щоб компоненти могли поміститися в корпусі більш компактного формфактора. Цей корпус із маленьким формфактором виглядає як типовий компонент домашнього кінотеатру. Як правило, у корпусі HTPC установлюються більші вентилятори, які обертаються повільніше й створюють менше шуму в порівнянні з вентиляторами в типовій робочій станції. Щоб додатково знизити шум, створюваний системою HTPC, можна використовувати блоки живлення без вентиляторів (залежно від вимог до живлення). Деякі конструкції HTPC містять компоненти з особливо низьким енергоспоживанням і не вимагають вентиляторів для охолодження.

Аудіосистема об'ємного звуку – об'ємний звук створює ефект присутності у відеопрограмі. У системі HTPC може використовуватися функція об'ємного звуку материнської плати (якщо її підтримує чипсет), або можна встановити спеціалізовану звукову карту для передачі високоякісного об'ємного звуку на динаміки або додатковий підсилювач для оптимального звучання.

Вихідне роз'єм HDMI – стандарт HDMI дозволяє передавати відео у форматі високої чіткості, об'ємний звук і дані на телевізори, мультимедійні ресивери й проектори. Інтерфейс HDMI також можна використовувати для керування функціями різних пристроїв, що підтримують таку можливість.

ТВ-Тюнери й кабельні плати – для того, щоб система HTPC відображала телевізійні сигнали, необхідно використовувати тюнер. ТВ-Тюнер перетворить сигнали аналогового й цифрового телебачення в аудіо– і відеосигнали, які можуть використовуватися й зберігатися на комп'ютері. Кабельні плати можуть використовуватися для одержання телевізійних сигналів від компанії кабельного телебачення. Кабельна плата потрібно для доступу до кабельних каналів високоякісного віщання. Деякі кабельні плати можуть ухвалювати до шести каналів одночасно.

Спеціалізований жорсткий диск – жорсткі диски з низьким рівнем шуму й низьким енергоспоживанням звичайно називаються аудіовідеодисками (A/V). Такі диски спеціально розроблені для тривалого й надійного запису й можуть похвастати збільшеним терміном служби.

Замість складання системи HTPC деякі замовники можуть попросити виконати складання домашнього сервера на базі ПК. Домашній сервер на базі ПК можна встановити в будь-якому місці будинку й використовувати його з декількох пристроїв одночасно. Домашній сервер надає загальний доступ до файлів і принтерам, а також виконує потокову передачу аудіо-, відеофайлів і світлин на комп'ютери, ноутбуки, планшети, телевізори й інші мультимедійні пристрої по мережі. На домашньому сервері можна настроїти масив RAID для захисту коштовних даних на випадок збою жорсткого диска. Для потокової передачі даних на кілька пристроїв без затримок установите гігабітну мережеву інтерфейсну плату.

Огляд Розділу 3. Кінцеве обладнання телекомунікаційних систем

У даній главі перераховані компоненти, з яких полягає система персонального комп'ютера, а також принципи підбору компонентів для модернізації. Багато тем з даної глави ще не один раз знадобляться вам протягом усього курсу.

Сфера інформаційних технологій охоплює використання комп'ютерів, мережного встаткування й ПО для обробки, зберігання, передачі й одержання інформації.

Комп'ютерна система складається з апаратного й програмного забезпечення.

Корпус комп'ютера й блок живлення слід вибирати таким чином, щоб вони були сумісні з устаткуванням, установлюваним у корпус, і дозволяли додавати додаткові компоненти.

Внутрішні компоненти комп'ютера вибираються відповідно до конкретних можливостей і функціями. Усі внутрішні компоненти повинні бути сумісні з материнською платою.

При підключенні пристроїв слід використовувати підходящі типи портів і кабелів.

До типових пристроїв уведення ставляться клавіатура, миша, сенсорний екран, і цифрові камери.

У число типових пристроїв виводу входять монітори, принтери й динаміки.

Корпуси, блоки живлення, ЦП і система охолодження, ОЗП, жорсткі диски й плати адаптерів слід обновляти у випадку відмови пристрою або якщо пристрій більше не відповідає вимогам користувача.

Для спеціалізованих комп'ютерів потрібне встаткування, що відповідає їхнім конкретним функціям. Тип устаткування, використовуваного в спеціалізованих комп'ютерах, визначається залежно від способів роботи користувача і його цілей.

Список використаних джерел

Керівні документи

1. В. О. Собина, Д. В. Тарадуда, М. М. Піксасов, Л. В. Борисова, О. В. Закора, А. Б. Фещенко, М.В. Маляров, Д. Л. Соколов, Дослідження проблем функціонування системи зв’язку ДСНС, використання засобів телекомунікацій та інформатизації в системі ДСНС, шляхів їх розвитку із застосуванням сучасних телекомунікаційних та інформаційних технологій, Звіт про НДР: № держреєстрації 0119U001009, Х.: НУЦЗУ, 2020. – 85 с. Режим доступу: http://ndr.dsns.gov.ua/?p=7135 .

2. .Порядок організації роботи відомчої цифрової телекомунікаційної мережі ДСНС Наказ ДСНС 23.10.2019 № 608

3. Наказ МВС України 08.02.2019 № 93 Про затвердження Інструкції щодо практик чи процедур проектування, дослідження, введення в експлуатацію, експлуатації та технічного обслуговування (супроводження) автоматизованих систем централізованого оповіщення

4. Наказ МВС України 20.10.2017 № 870 Про затвердження Положення про автоматизовану інформаційну систему оперативного призначення єдиної інформаційної системи МВС

Література

5. Тарарака В. Д. Архітектура комп'ютерних систем: навчальний посібник. – Житомир : ЖДТУ, 2018. – 383 с.

6. А.О. Новацький Комп'ютерна електроніка: Мікропроцесорні системи: Програмування мікропроцесорних систем: Навчальний посібник для студентів напряму підготовки 6.050201 «Системна інженерія» кафедри Автоматики та управління у технічних системах Київ: НТУУ "КПІ", 2014– 307 с..

7. Курс lT Essentials Сетевой академии Cisco [Электронный ресурс]. Режим доступа: https://www.netacad.com/ru/courses/os-it/it-essentials

8. Сучасні телекомунікаційні мережі у цивільному захисті: Підручник. / Г.В. Щербак, Л.І. Мельникова, І.В. Рубан, К.В. Садовий, Д.В. Сумцов. – Харків, УЦЗУ, 2007. – 261 с

Контрольні питання

1. Корпуси
2. Блоки живлення, Потужність блоку живлення
3. Речі, щоб шукати при виборі блоку живлення
4. Материнські плати
5. Архітектури ЦП
6. Підвищення продуктивності ЦП, Системи охолодження ЦП
7. ПЗП, ОЗП
8. Модулі пам'яті
9. Плати адаптерів і слоти розширення
10. Обладнання зберігання даних
11. Інтерфейси обладнань зберігання даних і RAID
12. Відеопорти й кабелі для підключення монітора
13. Інші порти й кабелі
14. Адаптери й конвертери
15. Обладнання введення
16. Характеристики моніторів
17. Зборка комп'ютера
18. Вибір материнської плати
19. Вибір корпусу й вентиляторів
20. Тип моделі корпусу
21. Вибір вентиляторів для корпусу
22. Вибір блоку живлення
23. Фактори при виборі блоку живлення
24. Вибір ЦП і системи охолодження процесора
25. Відомості про різні сокети і процесорах, які можна в них встановлювати
26. Фактори Вибір системи охолодження ЦП
27. Вибір ОЗП
28. Фактори, які слід ураховувати при придбанні нової графічної плати
29. Питання, що стосуються придбання плати адаптера
30. Фактори, які слід ураховувати при придбанні нової звукової карти
31. Фактори, які слід ураховувати при придбанні нової плати контролера обладнань зберігання даних
32. Фактори, які слід ураховувати при придбанні нової плати введення-виводу

33. Фактори, які слід ураховувати при придбанні нового мережевого адаптера

34. Фактори, які слід ураховувати при придбанні нової плати захвату.

35. Вибір жорстких дисків

36. Компоненти твердотільного накопичувача

37. Вибір обладнання читання носіїв

38. Фактори, які слід ураховувати при виборі нового обладнання читання носіїв

39. Вибір приводів оптичних дисків

40. Фактори, які слід ураховувати при виборі приводу оптичних дисків

41. Тип оптичних носіїв

42. Вибір зовнішнього накопичувача

43. Фактори, які слід ураховувати при виборі зовнішнього накопичувача

Питання для тест-контролю

1. Які дві вимоги до апаратних засобів комп'ютера пред'являються якщо буде потреба запуску декількох віртуальних машин? (Виберіть два варіанти.)

Кілька моніторів

Високошвидкісний адаптер безпроводового зв'язку

Багатоядерний ЦП

Відеоадаптер високого розрізнення

Великий обсяг ОЗП

2. **Яка одиниця вимірювань використовується для позначення швидкості жорсткого диска?**

число кластерів у хвилину

число обертів у хвилину

гігабайти

число сторінок у хвилину

3. Який термін використовується для визначення провідників на материнській платі, які забезпечують перенесення даних з однієї частини комп'ютера в іншу?

Міст

Набір мікросхем

Плата введення-виводу

Шина

4. Який компонент впливає на вибір корпусу й блоку живлення при створенні нового ПК?

Звукова карта

Материнська плата

Модуль ОЗП

Тип жорсткого диска

Відеоадаптер

5. Яка величина електрики виражається у ватах?

Кількість електронів, що проходять через ланцюг за секунду

Опір протіканню струму в ланцюзі.

Робота, необхідна для переміщення електронів по ланцюгу, помножена на число електронів, що проходять через ланцюг у секунду.

Кількість роботи, необхідне для переміщення електронів по ланцюгу.

6. Який тип інтерфейсу, спочатку розроблений для телебачення високої чіткості, також використовується для приєднання до комп'ютера аудіо– і відеопристроїв?

VGA

USB

DVI

HDMI

Firewire

РОЗДІЛ 4. ЗНАЙОМСТВО З ТЕХНІКОЮ БЕЗПЕКИ ПРИ ОБСЛУГОВУВАННІ КІНЦЕВОГО ОБЛАДНАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ З ВИКОРИСТАННЯМ ІНСТРУМЕНТІВ

У цій главі розглядаються основні методики безпечної роботи на робочому місці, апаратний і програмний інструментарій, а також утилізація небезпечних матеріалів. Правила техніки безпеки допомагають захистити людей від нещасних випадків і травм. Крім того, вони допомагають захистити обладнання від ушкоджень. Деякі із цих вказівокспрямовані на захист навколишнього середовища від забруднення, до якого може привести неправильна утилізація матеріалів [1-3] рис. 4.1.



Рис.4.1– Приклад неправильної утилізація матеріалів

4.1 Загальні правила техніки безпеки

Безпечні умови роботи допомагають уникнути травм і ушкодження комп'ютерного встаткування. Безпечне робоче місце повинне втримуватися в чистоті й порядку, мати належне висвітлення. Усі повинні знати й дотримувати техніки безпеки [4-9].

Додержуйтеся вимог інструкції з безпеки, щоб уникнути порізів, опіків, ударів електричним струмом і порушення зору. Рекомендується переконатися, що під рукою є вогнегасник і набір для надання першої медичної допомоги. Неправильно розміщені або незакріплені кабелі мо-

жуть стати травмонебезпечними перешкодами при монтажімережі. Щоб уникнути ризику для кабельного розведення рекомендується використовувати кабельні канали або короби.

Нижче представлений неповний список запобіжний заходів при роботі з комп'ютером:

1. Зніміть годинник і прикраси, підтягніть вільний одяг, щоб вона не бовталася.

2. Відключитеживлення й від'єднаєте кабелі живленняобладнання з розеток перед початком ремонтних робіт.

3. Заклейте гострі краї усередині комп'ютера ізоляційною стрічкою.

4. Ніколи не розбирайте блок живлення або монітор із вбудованим блоком живлення.

5. Не доторкайтеся до гарячих частин принтера або деталям принтера, що перебувають під високою напругою.

6. Довідайтеся, де перебуває вогнегасник і як ним користуватися.

7. Не тримаєте їжу й напої на робочому місці.

8. Підтримуйте своє робоче місце в чистоті й порядку.

9. Згинайте коліна, коли піднімаєте важкі предмети, щоб не ушкодити спину.

10. Використовуйте захисні окуляри щоб уникнути ушкодження ока.

11. Перед очищенням або ремонтом устаткуванняпереконаєтеся, що інструменти перебувають у справному стані. Почистите, полагодите або замінитеті з них, які не функціонують належним чином.

4.2.Електрична безпека

Додержуйтеся інструкцій по електричній безпеці, щоб уникнути загорянь електромережі, травм і нещасних випадків зі смертельним результатом (рис. 4.2).

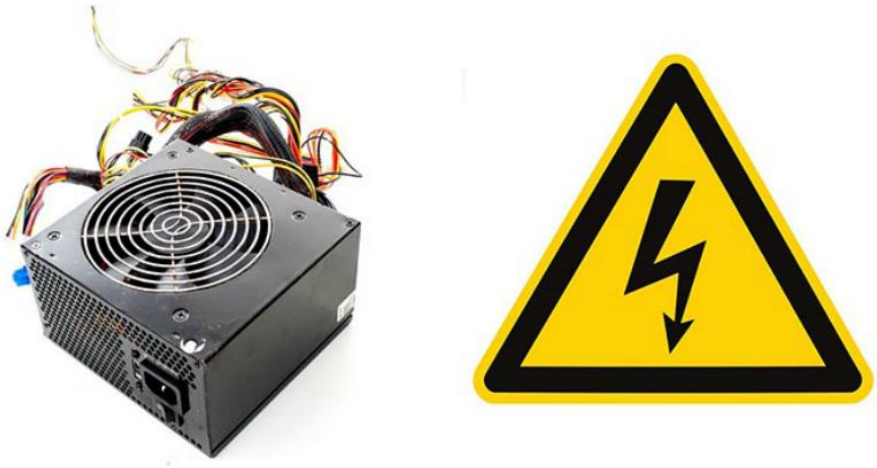


Рис. 4.2 Електрична небезпека від блоку живлення

Деякі деталі принтерів нагріваються під час використання, а інші, такі як блоки живлення, можуть перебувати під високою напругою. Вивчите інструкцію до принтера, щоб довідатисярозташування деталей під напругою. Деякі деталі зберігають високанапруга навіть після вимикання принтера. Перед початком ремонтних робіт переконаєтеся, що пройшлодоситьчасу, щоб принтер охолодів.

Електричні пристрої мають певні вимоги до електроживлення. Наприклад, для різних ноутбуків випускаються різні адаптери змінногоструму. Використання адаптера змінногоструму від іншого ноутбука або пристрою іншого типу може викликатиушкодження самого адаптера й ноутбука.

4.3 Пожежна безпека

Додержуйтеся правил безпеки для захисту життя, споруджень і встаткування. Щоб уникнути удару електричним струмом і для попередження ушкоджень комп'ютера перед початком ремонтних робіт виключите комп'ютер і відключитеживлення.

Пожежа може дуже швидко поширитися й завдати серйозної шкоди. Правильне використання вогнегасника попередить поширення й вихід з-під контролю невеликої пожежі. Користуйтеся мнемонічною підказкою В– Н-Н– О, щоб запам'ятати основні правила використання вогнегасників:

В — Висмикнути чеку.

Н — Направити на підставу вогню, а не на саме полум'я.

Н — Натиснути на важіль.

О — Описувати соплом дуги зі сторони убік.

Ознайомтеся з типами вогнегасників, які застосовуються у вашій країні й регіоні. Різні типи вогнегасників містятьрізні хімічні речовини для боротьби з різними типами пожеж, залежно від їхнього джерела:

1. Папір, дерево, пластик, картон
2. Бензин, гас, органічні розчинники
3. Електроустаткування
4. Легкозаймисті метали

При роботі з компонентами комп'ютера звертайте увагу на заходи, що виходять від комп'ютерів і електричних пристроїв. Коли відбувається коротке замикання або перегрів електричних компонентів, від них ідезахід гару. У випадку пожежі виконуйте наступні правила безпеки:

1. Ніколи не намагайтеся боротися з нелокалізованою пожежею, яка вийшла з під контролю.
2. Перед початком роботи обов'язково ознайомтеся з маршрутом евакуації у випадку пожежі.
3. Швидко покиньтебудинок.
4. Звернетеся в аварійно-рятувальні служби за допомогою.

5. Знайдіть і прочитайте інструкція для експлуатації вогнегасників на своєму робочому місці перед тем, як використовувати їхрис. 4.3.



Рис. 4.3 Використання вогнегаснику

4.4 Електростатичний розряд і Електромагнітні перешкоди

4.4.1 Електростатичний розряд

Електростатичний розряд (ECP) може виникнути при нагромадженні електричного заряду (статичної електрики), який є на поверхні, що контактує з іншою поверхнею із протилежним зарядом.

Якщо попередньо не зняти електричний заряд, то ECP може викликатиушкодженнявстаткування комп'ютера. Щоб запобігти ушкодженнювстаткування й втрату даних, випливайте відповідним керівництвам по експлуатації, беріть до уваги стан навколишнього середовища й використовуйтевстаткування для стабілізації електроживлення.

Щоб людина могла відчутиECP, повинне нагромадитися як мінімум 3000 вольтів статичної електрики. Наприклад, статичнаелектрика може накопичуватися на тілі людини, коли людейіде по килимовому покриттю. Коли людей доторкається до іншій людині, обоєвипробовують удар струмом. Якщо розряд викликав біль або супроводжувався шумом, то напругастановилабільш 10 000 вольт. Для порівняння, ушкодження компонентів комп'ютера може бути викликане статичною електрикою з напругою менш 30 вольтів.

ECP може привести до необоротногоушкодження електричних компонентів. Додержуйтеся наведеним рекомендацій, щоб запобігти ушкодженням від ECP:

1. Зберігаєтевсе компоненти в антистатичних пакетах, поки не буде потрібно їх установлювати.
2. Використовуйте заземлені килимки на робочому місці.
3. Використовуйте заземлені антистатичні килимки в робочих зонах.
4. При ремонті комп'ютера використовуйте антистатичний браслет.

4.4.2 Електромагнітні перешкоди

Електромагнітні перешкоди (ЕМП) — це втручання зовнішніх електромагнітних сигналів у середовище передачі даних, наприклад мідні кабелі.

У мережномусередовищіЕМП спотворює сигнал таким чином, що впристроїв, що ухвалюють, виникають труднощі з його інтерпретацією.

ЕМПвиходять не тільки від тих пристроїв, від яких їх прийнято очікувати, наприклад від мобільних телефонів. Інші типи електричного встаткування можуть випускати безшумне, невидиме електромагнітне поле радіусом більш кілометра.

Існує безліч джерел ЕМП:

1. Будь-яке джерело, що генерує електромагнітні хвилі
2. Антропогенні джерела, такі як лінії електропередачі і електродвигуни
3. Природні явища, такі як грози, сонячне або космічне випромінювання

Безпроводові мережічутливі до радіочастотних перешкод (РЧП).

РЧП викликаються радіопередавачами й іншими пристроями, що працюють на тій же частоті. Наприклад, безпроводової телефон може викликати проблеми з безпроводовою мережею, якщо обоєпристроювикористовують ту саму частоту. Мікрохвильові печі також можуть викликати перешкоди, якщо вони перебувають поблизу пристроїв безпроводової мережі.

4.5 Клімат

Кліматичні умови по-різному можуть впливати на комп'ютерне встаткування: рис. 4.4.



Рис. 4.4 Кліматичні умови

Якщо температура навколишнього середовища дуже висока, обладнання може перегріватися.

При дуже низькій вологості підвищується ймовірність ЕСР.

При дуже високій вологості обладнання може одержатиушкодження від вологи.

4.6 Типи коливань напруги електроживлення

Напруга – це міра енергії, яка потрібна для переміщення заряду з одного місця в інше. Рух заряджених часток (наприклад, електронів) називається електричним струмом. Комп'ютерним схемам для роботи електронних компонентів потрібне напруга й електрична струм. Якщо напруга в комп'ютері нестабільно або неправильно, компоненти комп'ютера можуть працювати некоректно. Нестабільність напруги називається коливаннями або стрибками напруги електроживлення.

Наступні типи коливань напруги живленнязмінногоструму можуть привести до втрати даних або апаратному збою:

Відключення: повна втрата живленнязмінногоструму. Причиною відключення може стати перегорілий запобіжник, поломка трансформатора або ушкодження лінії електропередачі.

Зниженанапруга (просідання напруги): зниження рівня напруги змінногоструму, що триває протягом певного періоду часу. Зниження відбувається, коли напруга на лінії електропередачі становитьменш 80% від нормального рівня напруги, а також у випадку перевантаження електричних схем.

Шум: перешкоди від генераторів і блискавок. Шум знижує якість електроживлення, що може викликати помилки в комп'ютерній системі.

Сплеск: різке підвищення напруги, якатриває протягом короткого періоду й перевищує 100% від нормальної напруги на лінії. Сплески можуть бути викликані ударами блискавки. Вони також можуть відбуватися при відновленні електричної системи після відключення.

Стрибок напруги: значне підвищення напруги щодо нормального потоку електрики. Стрибок напруги триваєтрохинаносекунд, або мільярдних часток секунди.

4.7 Пристрої для захисту електроживлення

Щоб уникнути проблем з коливаннями напруги електроживлення, використовуйтепристрої для захистуданих і комп'ютерного встаткування:

Мережний фільтр захищає від ушкоджень, вносимих стрибками й сплесками напруги. Мережний фільтр відводить зайваелектричнанапруга з лінії в заземлення.

Джерело безперебійного живлення (ДБЖ, UPS) захищає від можливих проблем з електроживленням, надаючипотрібнийрівень електро-

живлення для комп'ютера або іншого пристрою рис. 4.5. Акумулятор **ДБЖ** постійно заряджається, коли пристрійперебуває в роботі. **ДБЖ** забезпечує необхідна якість електроживлення при зниженій напрузі й відключенні електроживлення. Багато пристроїв**ДБЖ** можуть прямо взаємодіяти з операційною системою комп'ютера. Цей зв'язок дозволяє **ДБЖ** безпечно виключити комп'ютер і зберегти дані до того, як розрядиться акумулятор **ДБЖ**.

Резервне джерело живлення (РДЖ) допомагає захистити від можливих проблем з електроживленням рис. 4.6. Резервний акумулятор **РДЖ** забезпечує живлення, якщо вступник напруга падає нижче нормального рівня. У нормальномурежимі роботи акумулятор неактивний. Коли напруга падає, акумулятор подає постійний струм на інвертор живлення, який перетворить його в зміннийструм для живлення комп'ютера. Цей пристрій не так надійний, як ДБЖ, оскільки потрібен час, щоб перемкнутися на живлення від акумулятора.

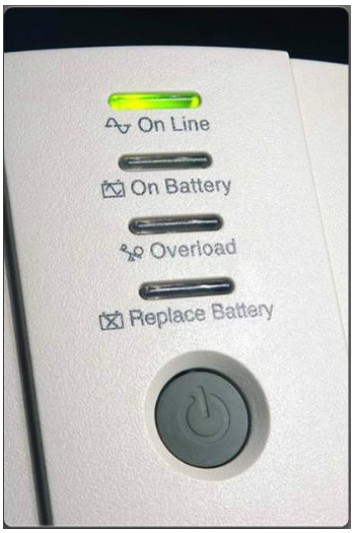


Рис. 4.5 – Панель управління ДБЖ



Рис. 4.6 – РДЖ

Якщо перемикаючий пристрій виходить із ладу, акумулятор не може подавати живлення на комп'ютер.

УВАГА! Виробники **ДБЖ** не рекомендують підключати до них лазерні принтери, тому що це може викликати перевантаження **ДБЖ**.

4.8 Паспорт безпеки

Комп'ютери й периферійні пристроїмістять матеріали, які можуть заподіяти шкоданавколишньому середовищу. Небезпечні матеріали іноді називають токсичними відходами. Вони можуть містити високу концентрацію важких металів, таких як кадмій, свинець або ртуть. Правила утилізації небезпечних матеріалів різняться в різних країнах. Зв'яжіться

з місцевими органами, відповідальними за вивіз і переробку відходів, і одержите інформацію про порядок утилізації й відповідних послугах.

Паспорт безпеки також називається паспортом безпеки матеріалу (ПБМ). Він являє собою інформаційний бюлетень зі зведеними даними по составу матеріалу, включаючи небезпечні інгредієнти, які можуть негативно впливати на здоров'я людей, пожежонебезпека й вимоги по наданню першої допомоги. ПБМмістить інформацію про хімічну реактивність і несумісності. Крім того, у ньомуприводятьсявідомості про безпечнийобіг з матеріалом і його зберіганні, дії у випадку розливу й витоку, а також інструкції з утилізації.

Щоб визначити, чи класифікується матеріал як небезпечний, ознайомтеся із ПБМ виробника. У США Управління по охороні праці й техніці безпеки (УОТ) вимагає, щоб до всіх небезпечних матеріалів додавався ПБМ при передачі їх новому власникові. Інженерам, що обслуговують технікові, може знадобитися інформація із ПБМ, прикладеного до продуктів, що здобуваються для ремонту або технічного обслуговування комп'ютера. УОТ також вимагає, щоб співробітників інформували про матеріали, з якими вони працюють, і забезпечували інструкціями з техніки безпеки рис 4.7.



Рис. 4.7 Сайт управління по охороні праці й техніці безпеки (США)

У ПБМзазначений найбільш безпечний спосіб утилізації потенційно небезпечних матеріалів. Завжди звіряйтеся з місцевими законами, що

стосуютьсядозволених методів утилізації, перш ніж приступитися до утилізації електронного встаткування.

ПБМмістить коштовну інформацію:

1. Назва матеріалу
2. Фізичні властивості матеріалу
3. Небезпечні інгредієнти, що містяться в матеріалі
4. Дані про реакційну здатність, наприклад, про пожежонебезпеку й вибухонебезпечності
5. Порядок дій при розливах і витоках
6. Особливі запобіжний заходи
7. Небезпека для здоров'я
8. Вимоги до спеціального захисту

У Євросоюзі 1 червня 2007 року в силу вступив регламент реєстрації, оцінки, дозволу й обмеження хімічних речовин (REACH), який замінив численні директиви й регламенти єдиною системою.

4.9 Утилізація обладнання

Належна утилізація або переробка небезпечних компонентів комп'ютерів є глобальною проблемою. Переконаєтеся в дотриманні регламентів по утилізації конкретних елементів. Організації, які порушують ці регламенти, можуть бути оштрафовані або залучені в дорогі судові розгляди. Регламенти по утилізації компонентів комп'ютера відрізняються в різних країнах. Для одержання актуальних відомостей по цімпитаннюзвернетеся в місцеву природоохоронну організацію.

Батареї й акумулятори

Батареї й акумулятори часто містятьрідкісноземельні метали, які можуть завдати шкоди навколишньому середовищу. В акумуляторах портативних комп'ютерів можуть утримуватися свинець, кадмій, літій, марганець і ртуть. Ці метали не розкладають і залишаються в навколишньомусередовищі на довгі роки. Ртуть повсюдно використовується у виробництві батарей і є винятково токсичної й шкідливою для людини.

Відправлення батарей і акумуляторів на переробку повинна входити в список стандартних дій. Усі батареї й акумулятори, включаючи літій-іонні, нікель-кадмієві, нікель-металогідрідні й свинцево-кислотні, підлягають процедурам утилізації, які відповідають місцевому природоохоронному законодавству.

Монітори

Дотримуйте обережності при обігу з Элт-Моніторами. В Элт-Моніторах може зберігатися високанапруга, навіть після відключення від джерела живлення.

Монітори містять скло, метал, пластик, свинець, барій і рідкісноземельні метали. Згідно з Агентством по охороні навколишнього середовища (АОНС) США, монітори можуть містити приблизно 1,8 кг свинцю.

Утилізація моніторів повинна проводитися відповідно до природоохоронного законодавства.

Комплекти тонерів, картриджі й проявники

Використані комплекти тонерів і картриджі для принтерів необхідно належним чином утилізувати відповідно до застосовного природоохоронного законодавства. Вони також підлягають переробці. Деякі постачальники й виробники тонерів і картриджів приймають порожні картриджі на повторне заправлення. Деякі компанії спеціалізуються на заправленні порожніх картриджів. Можна придбати набори для заправлення картриджів для струминних принтерів, однак це не рекомендується робити, тому що чорнило в принтері можуть протекти й привести до необоротнихушкоджень. Використання повторно заправлених картриджів для струминних принтерів може анулювати гарантію на принтер.



Рис. 4.8 – Утилізація або переробка небезпечних компонентів комп'ютерів

Хімічні розчинники й аерозольні балони

Звернетеся в місцеву компанію по вивозу відходів, щоб довідатися, як і де робити утилізацію хімікатів і розчинників, використовуваних для очищення комп'ютерів. Не виливайте хімікати й розчинники в раковину або в стоки, які з'єднані з колектором міської каналізації.

До балонів і пляшкам, що містять розчинники або інші речовини, що чистять, необхідно ставитися з обережністю. Переконаєтеся, що вони позначені як особливо небезпечні відходи, і відповідним чином звертай-

теся з ними. Наприклад, деякі аерозольні балони вибухають при нагріванні, якщо їх уміст не був використаний до кінця.

4.10 Загальне використання інструментів

Для ремонту комп'ютерів потрібен набір спеціальних інструментів рис. 4.9. Ознайомтеся звідомостями про те, як правильно використовуватикожний інструмент, а також переконаєтеся в тому, що для завдання застосовується правильний інструмент. Уміле використання інструментів і програмного забезпечення полегшує роботу й забезпечує винне й безпечне виконання поставлених завдань.



Рис. 4.9. – Набір спеціальних інструментів для ремонту комп'ютерів

У наборі повинні втримуватися всі інструменти, необхідні для проведення повного ремонту встаткування. З досвідом ви зрозумієте, які інструменти потрібно мати для різного типу робіт. Апаратний інструментарій ділиться на чотири категорії:

1. Засобу запобігання ECP
2. Ручні інструменти
3. Інструменти для очищення
4. Інструменти для діагностики

4.11 Засоби запобігання ЕСР

Існує два засоби запобігання ЕСР: антистатичний браслет і антистатичний килимок.

Антистатичний браслет захищає комп'ютерне встаткування, якщо він заземлений на корпус комп'ютера,застосовується для запобігання ушкодження комп'ютерного встаткування електростатичним розрядом- рис. 4.10.

Антистатичний килимок захищає комп'ютерне встаткування, запобігаючи нагромадження статичної електрики на встаткуванні або на інженерові, він перешкоджає нагромадженню статичної електрики, коли інженер стає на нього сам або ставить устаткування під час роботи (рис. 4.11).



Рис. 4.10 – Антистатичний браслет



Рис. 4.11 – Антистатичний килимок

4.12 Ручні інструменти

Більша частина інструментів, використовуваних при складанні комп'ютера, являє собою дрібні ручні інструменти. Їх можна придбати як окремо, так і в наборі для ремонту комп'ютерів. Набори інструментів значно різняться по розміру, якості й ціні. На рис. 4.12 а) – е)наведені додаткові відомості про найпоширеніші ручні інструменти.

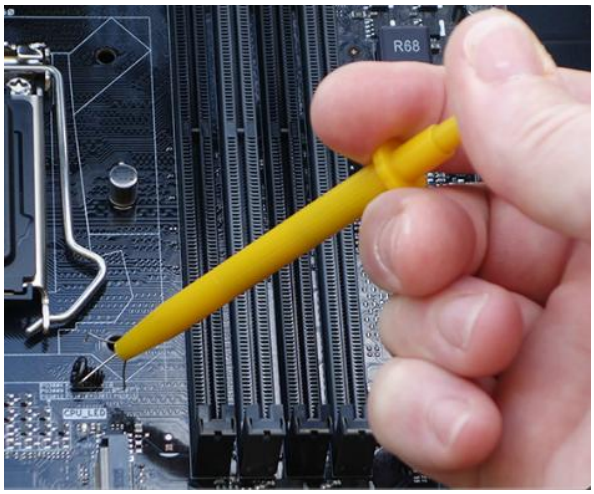
Викрутка із плоским шліцом (рис. 4.12, а) використовується, коли потрібно відкрутити або затягти гвинт із прямим шліцом.

Хрестова викрутка (рис. 4.12, б) використовується, коли потрібно відкрутити або затягти гвинт із хрестоподібним шліцом.

Викрутка з жалом зіркоподібної форми (рис. 4.12, в) використовується, щоб затягти або відкрутити гвинти, що мають зіркоподібне поглиблення на головці. Найчастіше такі гвинти можна побачити на ноутбуках.

Шестигранна викрутка (рис. 4.12, г) , також називана гайковим ключем, використовується для затягування гайок одночасно із застосуванням викрутки для затягування гвинтів.

а)  б)  в)  г) 

д) 

е) 

Рис.4.12– Додаткові відомості про найпоширеніші ручні інструменти:

Екстрактор (рис. 4.12, д) застосовується для добування деталей з тих місць, розмір яких не дозволяє дістати деталь руками.

Ліхтарик (рис. 4.12, е) потрібний для висвітлення місць, які важко розглянути без додаткового світла.

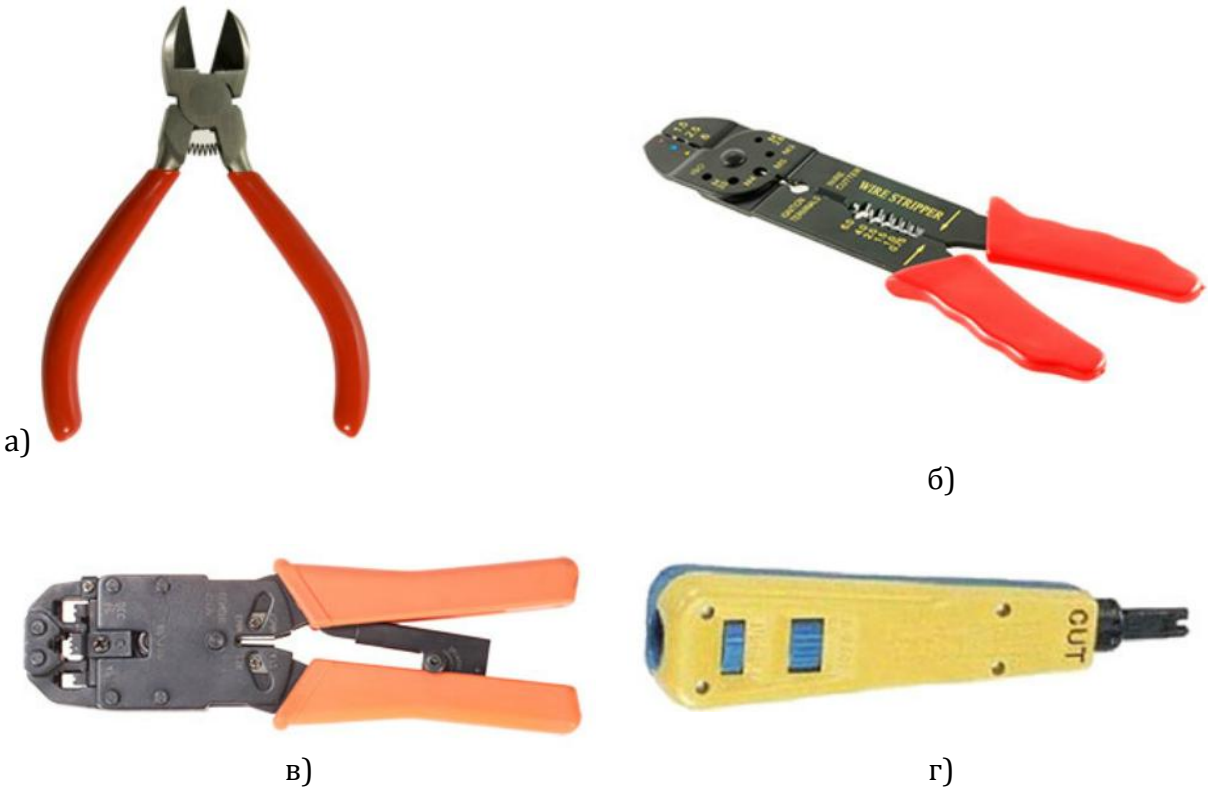
4.13 Інструменти для роботи з кабелями

У комплект інструментів для ремонту комп'ютерів також входять інструменти для ремонту й підготовки кабелів. На рис. рис. 4.13а)–б)наведені додаткові відомості про найпоширеніші інструменти для роботи з кабелями.

Гострозубці (рис. 4.13, а) використовуються для обрізки проводів.

Кліщі для зняття ізоляції (рис. 4.13, б) потрібні для видалення ізоляції із проводів. Ізоляцію слід видаляти, коли потрібно скрутити проведення з іншими проводами або прикріпити до роз’єм, щоб вийшов кабель.

Обтискної інструмент (рис. 4.13, в) використовується для з'єднання роз'ємів і проводів.



а) б)

в) г)

Рис.4.13– Додаткові відомості про найпоширеніші інструменти для роботи з кабелями

Інструмент для закладення кабелю (рис. 4.12, г) використовується для приєднання проведення до місця його кріплення на платі

4.14 Інструменти для очищення

Проводячи технічне обслуговування й ремонт комп'ютерів, необхідно мати відповідні інструменти для їхнього очищення. Використання правильних інструментів допомагає забезпечити відсутність ушкоджень комп'ютерних компонентів у процесі очищення. На рис. 4.14 а) – г) наведені додаткові відомості про найпоширеніші інструменти для очищення.

М'яка безворсова тканина (рис. 4.14, а) використовується для очищення різних комп'ютерних компонентів, не дряпаючи їх і не залишаючи сторонніх часток.

Стиснене повітря (рис. 4.14, б) використовується, щоб здувати пил і сторонній частки з різних деталей комп'ютера, не стосуючись компонентів.

Стяжки (рис. 4.14, в) використовуються, щоб акуратно поєднувати кабелі усередині й зовні комп'ютера.

Каса для деталей (рис. 4.14, г) застосовується для зберігання гвинтів, перемичок, затискачів і інших дрібних деталей, а також запобігає їхньому змішуванню



а)



б)



в)



г)

Рис. 4.14 – Додаткові відомості про найпоширеніші інструменти для очищення:

4.15 Інструменти для діагностики

Цифровиймультіметр

Цифровиймультіметр (див.рис. 4.15 а)) — це пристрій, здатне виконувати різнівиміри. З його допомогою перевіряють цілісність ланцюгів і якість електроживлення в компонентах комп'ютерів. Цифровиймультіметр виводить інформацію на Жк-Екран або світлодіодний дисплей.

Адаптер зворотної петлі (Loopback adapter)

Адаптер зворотної петлі (див.4.15 б)), також називаний петлевий заглушкою, перевіряє базову функціональність портів комп'ютера. Адаптер повинен відповідати порту, який потрібно протестувати.

Генератор тону й щуп

Генератор тону й щуп (див.4.15 в)) — це інструмент, щополягає із двох частин. Генератор тону підключається до кабелю за допомогою спеціальних адаптерів. Генератор тону створює сигнал, який проходить по всій довжині кабелю. Щуп виконує трасування кабелю. Коли щуп роз-

ташований близько до кабелю, до якого підключений генератор тону, сигнал чутний через динамік у щупі.

Аналізатор Wi-Fi

На рис. 4.15 г показаний екран аналізатора Fluke Wifi Analyzer. Аналізатор Wi-Fi являє собою мобільний засіб для перевірки безпроводових мереж, а також для пошуку й усунення неполадок у їхній роботі. Багато аналізаторів мають широкий набір інструментів, покликаних спростити планування корпоративних мереж, забезпечити їхнябезпека й відповідність нормативним вимогам, а також для обслуговування безпроводових мереж. Однак аналізатори Wi-Fi можна також використовувати й для невеликих локальних безпроводових мереж. Завдяки цьому засобу інженер може переглядати відомості про всі доступні в заданій області безпроводові мережі, визначатирівень сигналу кожної з них, а також визначати місця для установкикрапок доступу для настроювання зони покриття мережі.



а)



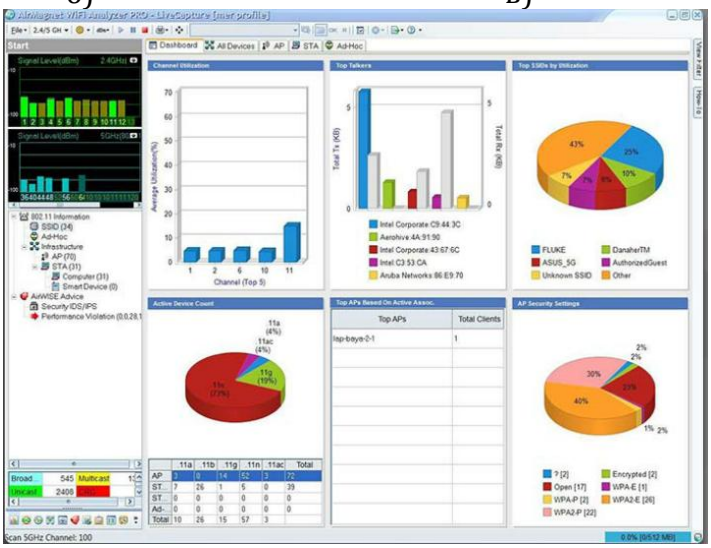
б)



в)



д)



г)

4.15 – Інструменти для діагностики

Деякі аналізатори Wi-Fi дозволяють виконувати пошук і усунення неполадок у роботі безпроводової мережі шляхом визначення неправильних конфігурацій, збоїв у роботі крапок доступу й проблем, викликаних радіоперешкодами.

Зовнішній корпус для жорсткого диска

Хоча зовнішній корпус для жорсткого диска (див. 4.15, д) не є діагностичним інструментом, його часто використовують при діагностиці й ремонті комп'ютерів. Жорсткий диск користувача міститься в зовнішній корпус для перевірки, діагностики й ремонту з використанням комп'ютера, у справності якого немає сумнівів. Також можна записувати резервні копії даних на диск, поміщений у зовнішній корпус, щоб запобігти ушкодженню даних під час ремонту комп'ютера.

За допомогою цифрового мультіметра (рис. 4.15, а) перевіряють цілісність ланцюгів і якість електроживлення в компонентах комп'ютера.

Адаптер зворотної петлі (рис. 4.15, б) застосовується для перевірки базової функціональності портів комп'ютера.

Генератор тону й щуп (рис. 4.15, в) використовуються для трасування кабелів.

Аналізатор Wi-Fi (рис. 4.15, г) являє собою мобільний засіб для перевірки безпроводових мереж, а також для пошуку й усунення неполадок у їхній роботі.

У зовнішньому корпусі (рис. 4.15, д) міститься жорсткий диск, придатний для використання з метою діагностики жорсткого диска або комп'ютера замовника, який не завантажується. Також зовнішній корпус може застосовуватися для створення резервних копій жорсткого диска замовника.

4.16 Засоби управління дисками

Програмні засоби допомагають проводити діагностику комп'ютерних і мережевих проблем і визначати, яке з комп'ютерних пристроїв працює некоректно. Інженер повинен уміти використовуватиряд програмних засобів для діагностики проблем, обслуговування обладнання й захисту даних, що зберігаються на комп'ютері.

Інженер повинен уміти визначати, які програмні засоби потрібно використовувати в різних ситуаціях. Засобикерування дисками допомагають визначити й виправити помилки диска, підготувати диск до зберігання даних і вилучити непотрібні файли.

Управління дисками ініціалізує диски, створює й форматує розділи (рис. 4.16, а).

Форматування готовить жорсткий диск до зберігання інформації (рис. 4.16, б).

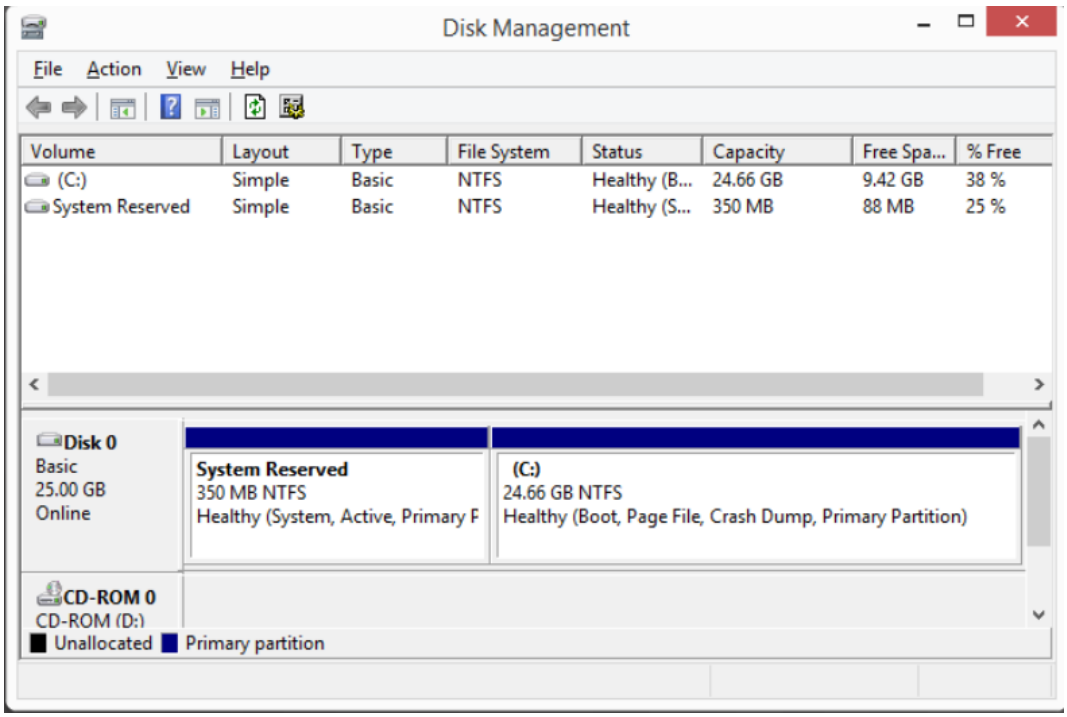


Рис.4.16 а

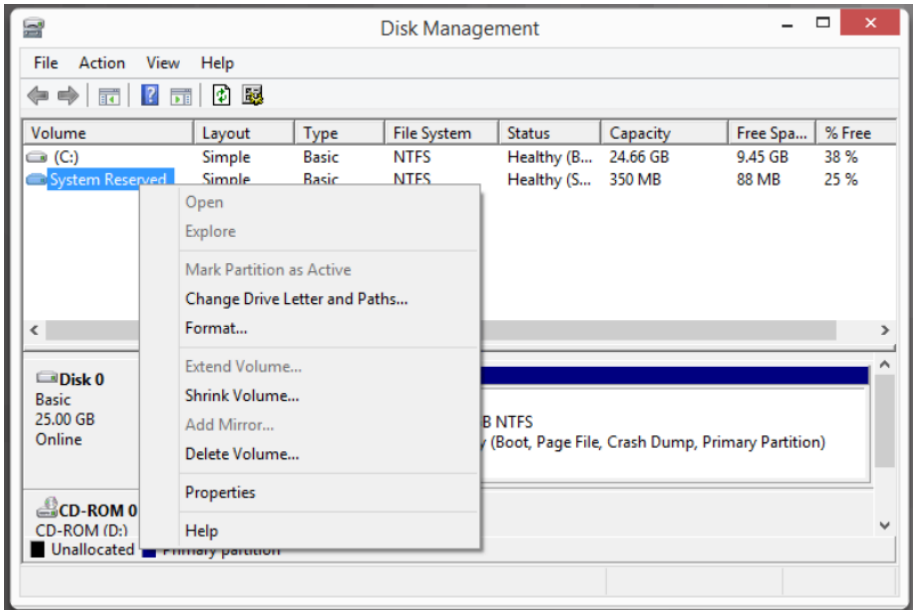


Рис.4.16 б

Scandisk або CHKDSK перевіряють цілісність файлів і папок на жорсткомудиску, скануючи файлову систему. Ці засоби також можуть перевіряти поверхня диска на наявність фізичних ушкоджень (див.рис. 4.16, в).

Оптимізація дисків (раніше називалася дефрагментацією) оптимізує простір на жорсткомудиску для забезпечення більш швидкого доступу до програм і даним (див.рис. 4.16, г).

Очищення диска очищає простір на жорсткомудиску, виконуючи пошук файлів, які можуть бути безпечно вилучені (диврис. 4.16, д).

Перевірка системних файлів (SFC)сканує критичні файли операційної системи й заміняє ушкоджені файли (див.рис. 4.16, е). Використовуйтезавантажувальний диск Windows 8 для усунення несправностей і відновлення ушкоджених файлів. Завантажувальний диск Windows 8 відновлює системні файли Windows, а також ушкоджені або загублені файли й переустановлює операційну систему. Для вирішення проблем з усуненням несправностей можна використовуватизасоби від сторонніх постачальників.

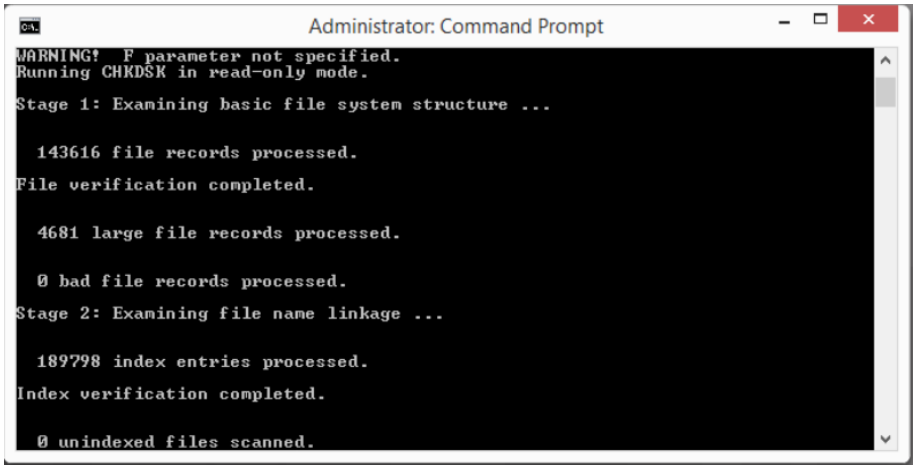
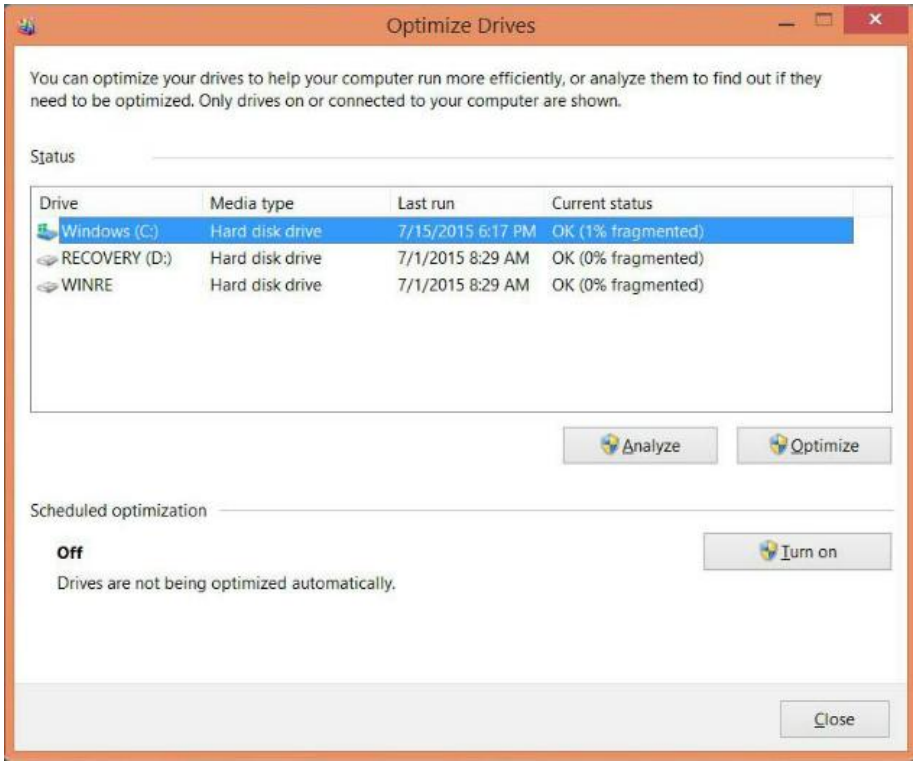


Рис.4.16 в



4.16 г)

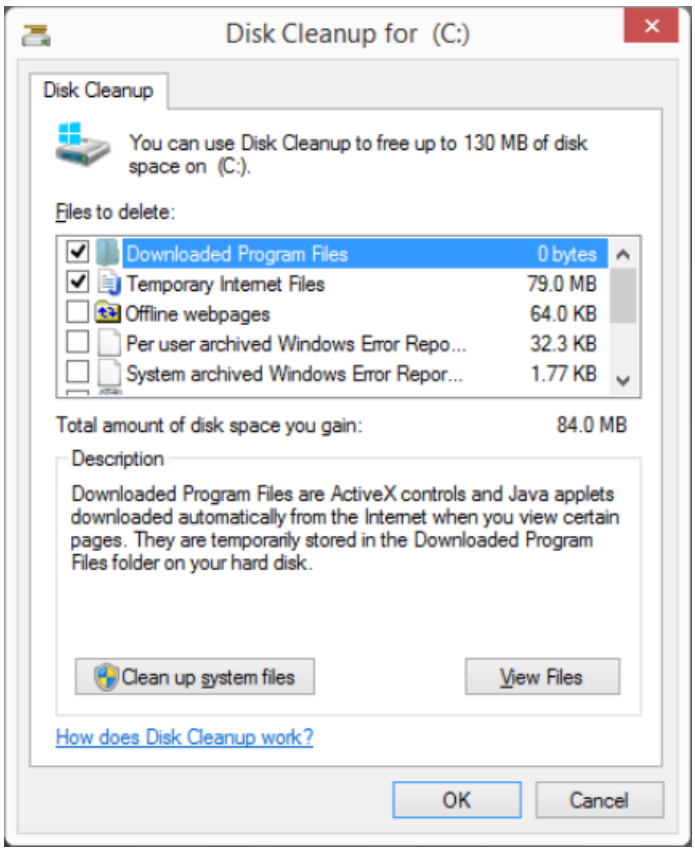


Рис.4.16 д)

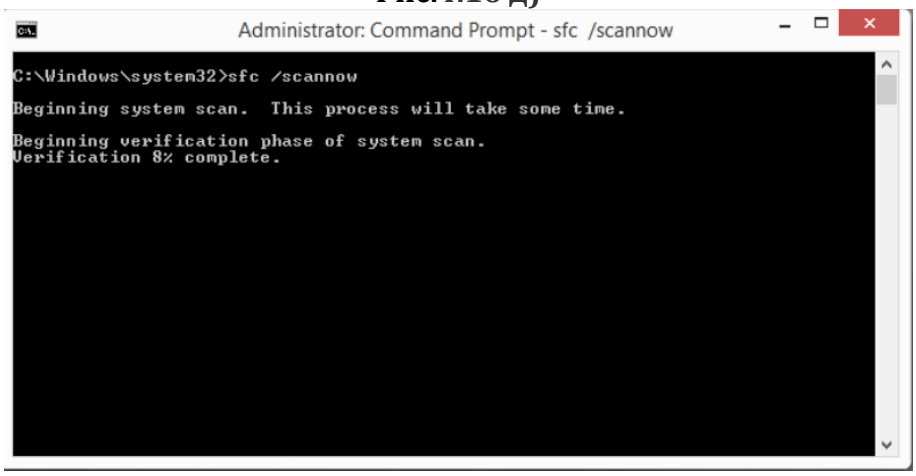


Рис.4.16 е)

4.17 Захисні програмні засоби

Щороку віруси, шпигунське ПО й інші типи атак зловмисників вражають мільйони комп'ютерів. Ці атаки можуть ушкодити операційні системи, додатки й дані. У заражених комп'ютерів можуть навіть виникати проблеми з роботою встаткування або вихід компонентів з ладу.

Для захистуданих і цілісності операційної системи й устаткування-використовуйте програмне забезпечення, розроблене для захисту від атак і видалення шкідливих програм.

Існують різні типи програмного забезпечення для захистувстаткування й даних.

Центр підтримки Windows — перевіряє стан важливих параметрів безпеки (див.рис. 4.17, а). Центр підтримки безупинно робить перевірку, щоб гарантувати, що програмний міжмережевий екран і антивірусні програми працюють. Він також забезпечує автоматичне завантаження й установкувідновлень.

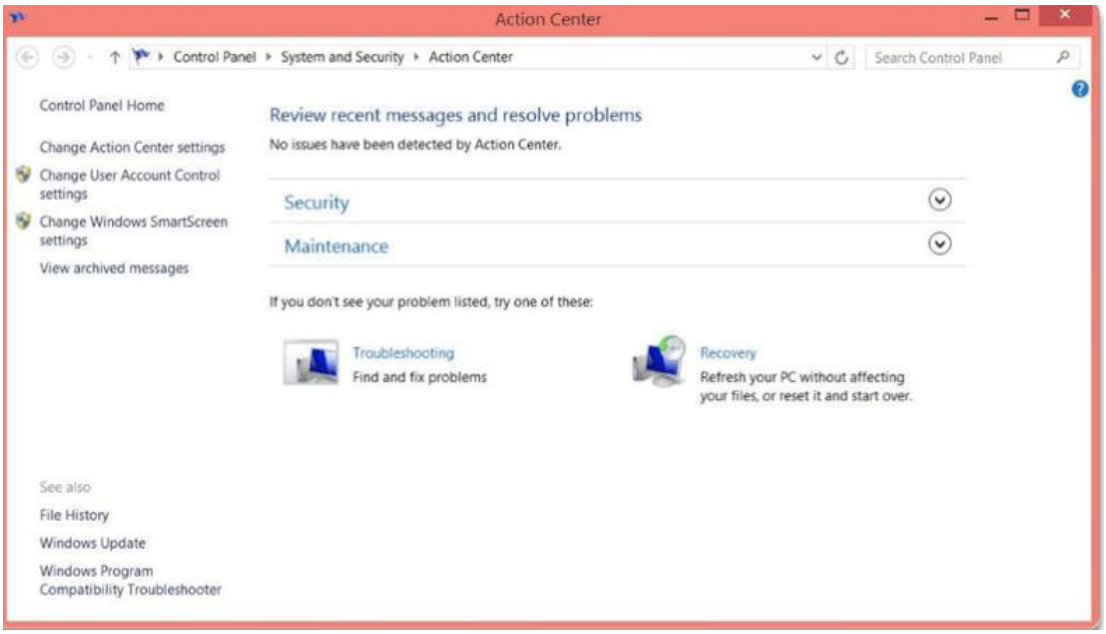


Рис.4.17 а

Windows Defender — служить для захисту комп'ютера від вірусів і шпигунського ПО (див.рис. 4.17, б).

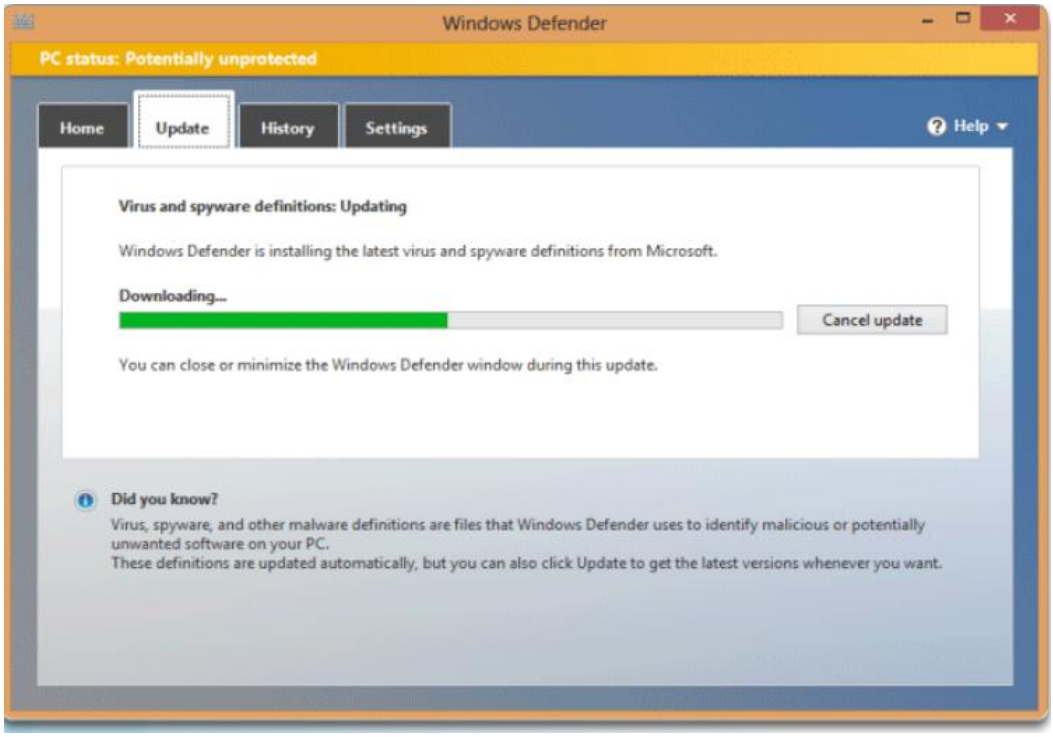


Рис.4.17 б

Міжмережевий екран Windows — безупинно працює для захисту від несанкціонованих мережних підключень до вашого комп'ютера (див.рис. 4.17, в).

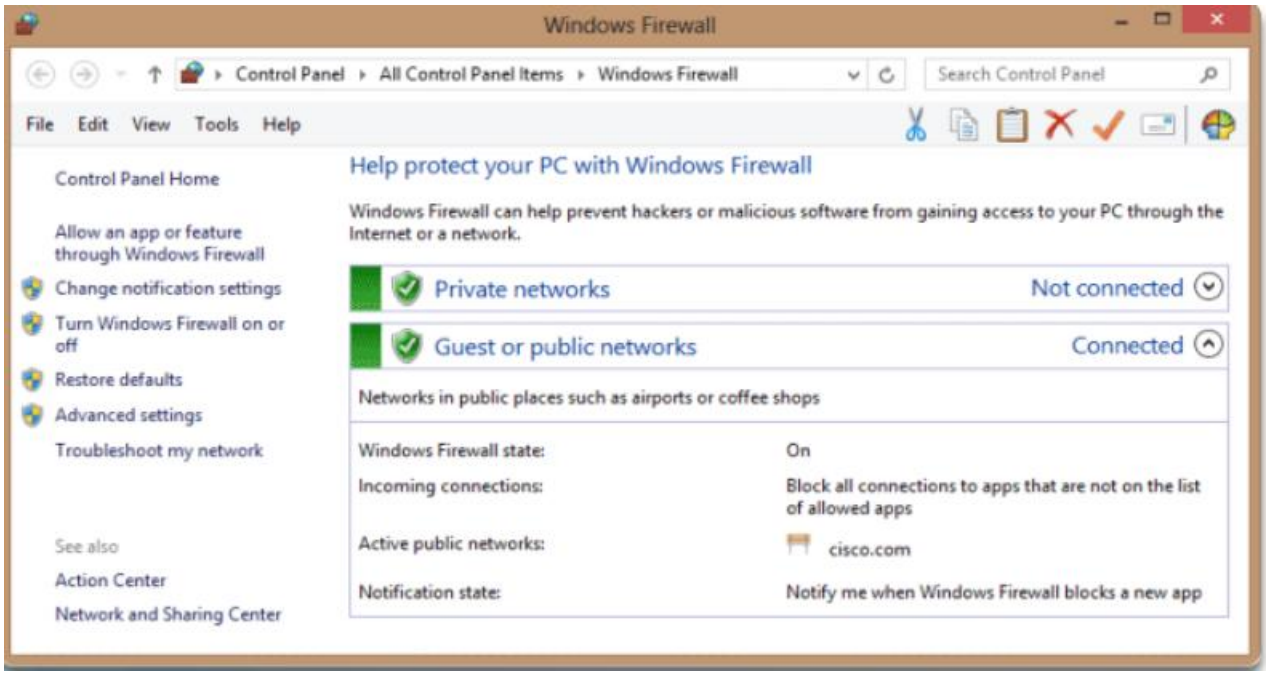


Рис.4.17 в

4.18 Довідкові засоби

Гарне обслуговування клієнтів має на увазі надання замовникові докладного опису проблеми і її розв'язку. Важливо, щоб інженер документував усі випадки обслуговування й ремонту, а також надавав таку документацію всім іншим інженерам. Такі документи можна використовувати в якості довідкового матеріалу при вирішенні схожих проблем.

Особисті довідкові засоби

До складу особистих довідкових засобів входять посібника з усунення несправностей, керівництва виробників, короткі довідкові керівництва й журнали ремонтних робіт. На додаток до накладних технічний фахівець повинен вести журнал відновлення і ремонту.

Замітки — робіть замітки в процесі усунення несправностей і ремонту. Звертайтеся до цих заміток, щоб не повторювати вже пройдених етапів і визначити, до якого етапу приступати далі.

Журнал — вносите в журнал опис проблеми, можливі розв'язки, які застосовувалися для її виправлення, і етапи усунення проблеми. Записуйте всі зміни настроювання встаткування й запасні частини, використані при ремонті. Ваш журнал разом із замітками може принести користь при дозволі схожих ситуацій у майбутньому.

Історія ремонту — складіть докладний список проблем і випадків ремонту, включаючи дату, замінені деталі й інформацію про замовника.

Історія ремонту дозволяє технічному фахівцевівизначити, які роботи проводилися з конкретним комп'ютером у минулому.

Довідкові засоби з Інтернету

Інтернет є прекрасним джерелом інформації про конкретні проблеми програмного забезпечення і їх можливих розв'язках:

Пошукові системи Інтернету

Новинні групи

Збірникипитань, що часто задаються, виробникам

Комп'ютерні керівництва в Інтернеті

Форуми й чати в Інтернеті

Технічні веб-сайти

На рис. 4.18 приводиться приклад технічного веб-сайту.

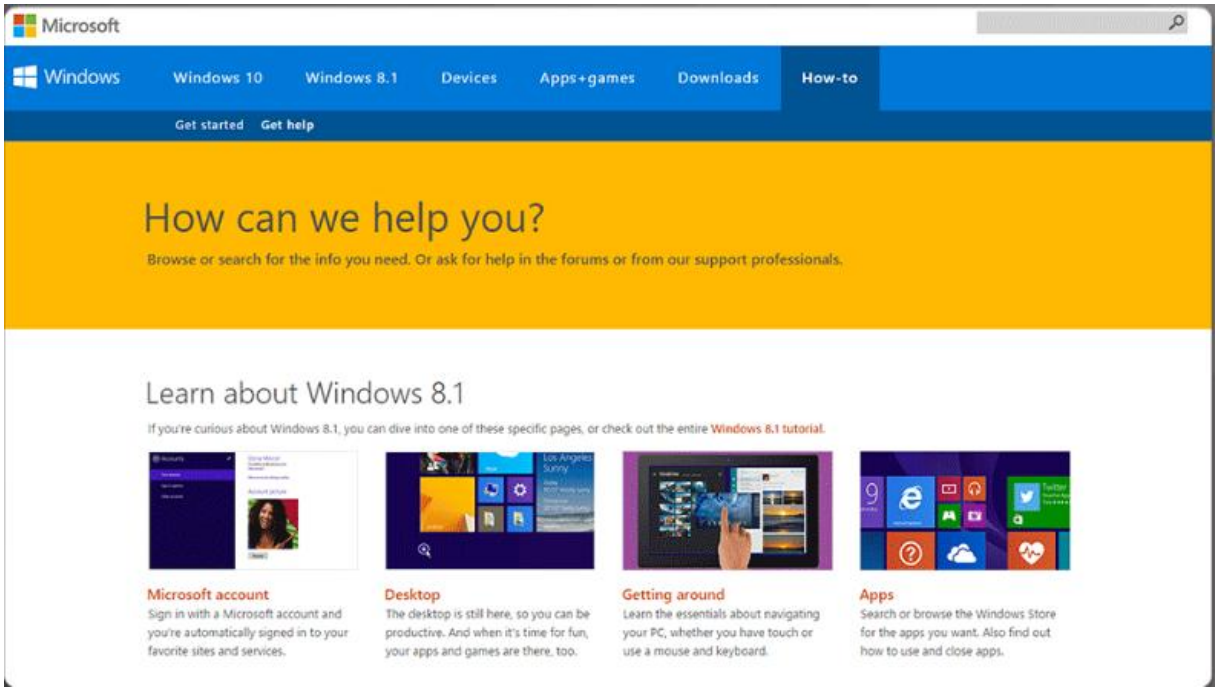


Рис.4.18. – Приклад технічного веб-сайту

4.19 Інші інструменти

З досвідом роботи ви знайдете безліч доповнень для свого набору інструментів. На рис. 4.19 а) показане, як можна використовувати паперовий скотч для того, щоб позначати витягнуті з комп'ютера деталі, коли каса для деталей недоступна.

Робочий комп'ютер також є важливим ресурсом, який потрібно брати собою при виїзді на ремонт комп'ютерів. Робочий комп'ютер можна використовувати для пошуку інформації, завантаження програм і драйверів, для зв'язку з іншими технічними фахівцями.

На рис. 4.19 б) показані типи запасних частин для комп'ютерів, які слід додати в набір інструментів. Переконаєтеся, що запчастини перебувають у справному стані, перш ніж використовувати їх. Заміна можливо

несправних комп'ютерних компонентів свідомо справними допоможе швидко визначити, який саме компонент не працює належним чином.



а)



б)

Рис.4.19

4.20 Антистатичний браслет

Антистатичний браслет — це провідник, що з'єднує тіло інженера з устаткуванням, з яким ведеться робота. Коли на тілінакопичується статична електрика, воно йде по приєднаному до браслета проведенні, зрівнюючи тим самим заряди між інженером і встаткуванням.

Прикладом статичної електрики служитьслабкий удар струмом, який ви одержуєте, коли йдете по кімнаті з килимовим покриттям і доторкаєтеся до дверної ручки. Цей слабкий удар не приносить шкоди людині, але якщо такий же електричний заряд перейде з людину на комп'ютер, то компоненти комп'ютера можуть бути ушкоджені. Носіння антистатичного браслета може захистити від ушкоджень комп'ютерних компонентів через електростатичний розряд.

Як показано на рис. 4.20, браслет складається із двох частин і достатньо зручний:

Крок 1. Оберніть браслет навколо зап'ястя й закріпите його за допомогою застібки або липучки. Метал на звороті браслета повинен перебувати в постійномуконтакті зі шкірою.



Рис.4.20 – Антистатичний браслет

Крок 2. Пристебніть роз'єм на кінціпроведення до браслета й приєднаєте другий кінець проведення або до встаткування, або до тієї ж крапки заземлення, до якої приєднаний антистатичний килимок. Металевий каркас корпусає гарним місцем для приєднання проведення. З'єднуючи проведення з устаткуванням, з яким ведеться робота, виберіть незабарвлену металеву поверхню. Пофарбовані поверхні не так добре проводятьелектрика, як незабарвлений метал.

Примітка. Підключайте проведення від браслета до встаткування з боку тієї руки, на яку надет антистатичний браслет. Так проведення не буде заважати під час роботи.

Хоча носіння антистатичного браслета й допомагає запобігти ЕСР, можна додатково знизити ризик, якщо не надягати одяг із шовку, поліестера й вовни. Ці тканини найбільше сприяють нагромадженню статичної електрики.

Примітка. Слід закочувати рукава, знімати шарфи або краватки й заправляти сорочку для того, щоб одяг не заважав при роботі. Переконаєтеся, що серги, намиста та інші нещільно сидячі прикраси належним чином закріплені.

УВАГА! Не надягайте антистатичний браслет при ремонті блоку живлення. Не приступайте до роботи із внутрішніми компонентами блоку живлення, поки не пройдете відповідне навчання.

4.21 Антистатичний килимок

Антистатичний килимок слабко проводить електрика. Він знімає статичну електрику з компонентів комп'ютера й безпечно переводить його від устаткування до крапки заземлення, як це показане на рис. 4.21.

Крок 1. На робочому місці килимок слід помістити під корпус комп'ютера або покласти поруч із ним.

Крок 2. Прикріпите килимок до корпуса за допомогою затискача, щоб забезпечити заземлюючу поверхню, на яку можна покласти запчастини після їхнього добування із системи.

Якщо робота виконується на спеціальному робочому місці, заземлите його й антистатичний підложний килимок. Коли ноги перебувають на килимку, а антистатичний браслет — на руці, тіло має однаковий заряд з устаткуванням, і це зменшує ймовірність ЕСР.

Чим нижче ймовірність ЕСР, тем менше можливість ушкодження чутливих ланцюгів і компонентів.

Примітка. Завжди тримаєте компоненти за краї.

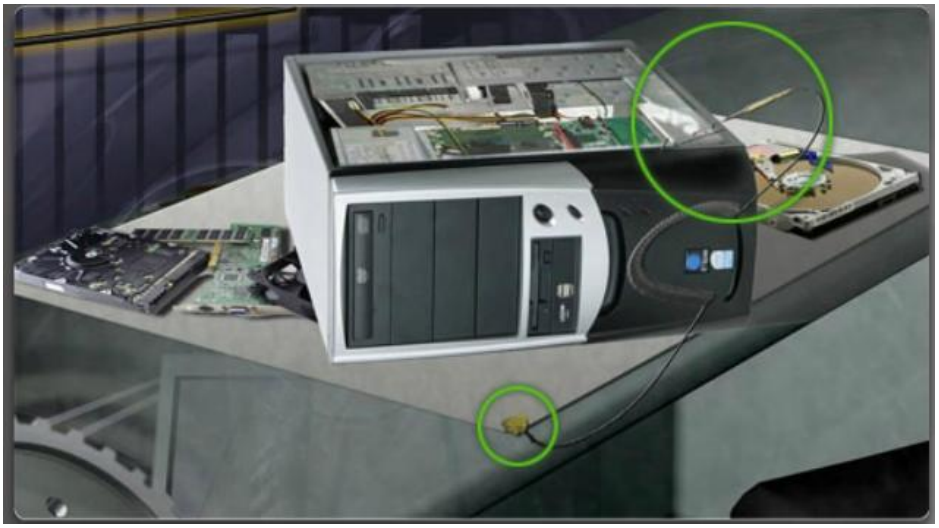


Рис.4.21 – Антистатичний килимок

4.22 Ручні інструменти

Інженер повинен уміти правильно використовуватикожний інструмент із набору. На цій сторінці розповідається про різні ручні інструменти, які використовуються для ремонту комп'ютерів.

Гвинти

Підберіть для кожного гвинта відповідну викрутку. Приставте кінчик викрутки до головки гвинта. Повертайте викрутку за годинниковою

стрілкою, щоб затягти гвинт, і проти годинникової стрілки, щоб послабити його, як показано на рис. 4.22 а).

Завжди використовуйте викрутку підходящого типу й розміру, оскільки а якщо ні, то гвинт можна зірвати. Зірваний гвинт, можливо, не вдасться затягти щільно, а також його може бути непросто відкрутити. Викиньте гвинти із зірваними капелюшками.

Викрутка із плоским шліцом

Використовуйте викрутку із плоским шліцом при роботі із гвинтами із прямим шліцом, як це показане на рис. 4.22 б). Не користуйтеся викруткою із прямим шліцом, щоб викрутити гвинт із хрестоподібним шліцом. Ніколи не використовуйте викрутку як важіль. Якщо не вдаєтьсявилучити компонент, перевірте, не втримує чи його на місці затискач або засувка.

УВАГА! Якщо потрібно прикласти велике зусилля, щоб вилучити або приєднати компонент, можливо, щось робиться неправильно. Ще раз перевірте, не чи пропущений який-небудь гвинт або затискач, який утримує компонент на місці. Скористайтеся посібником з роботи із пристроєм або кресленням, щоб одержати додаткову інформацію.

Хрестова викрутка (Philips)

Як показано на рис. 4.22 в), використовуйте хрестову викрутку для гвинтів із хрестоподібним шліцом. Не використовуйте такі викрутки в якості шила, тому що подібні дії приведуть до ушкодження кінчика викрутки.

Шестигранна викрутка

Використовуйте шестигранну викрутку, щоб закручувати й відкручувати болти із шестигранною головкою. Шестигранні болти не можна затягувати занадто сильно, тому що так можна ушкодити болт. Користуйтеся шестигранною викруткою, яка занадто велика для даного болта.

УВАГА! Деякі інструменти намагнічені. Працюючи з електронними пристроями, переконаєтеся, що використовувані інструменти не намагнічені. Магнітні поля можуть ушкодити дані, що зберігаються на магнітних носіях. Також намагнічені інструменти можуть індуціюватиструм, здатнийушкодити внутрішні компоненти комп'ютера. Перевірте свій інструмент, доторкнувшись до нього гвинтом. Якщо гвинт притягається, не використовуйте цей інструмент.

Інструменти для добування компонентів

Як показано на рис. 4.22 г), для установки й добування частин, до яких важко добратися пальцями, можна використовувати екстрактор. При використанні цих інструментів стежите за тим, щоб не дряпати компоненти й не піддавати їхнім ударам.

УВАГА! Не можнавикористовувати олівці, щоб міняти настроювання перемикачів усередині корпусу комп'ютера. Олівцевий грифель може

спрацювати як провідник і привести до ушкодження компонентів ком-п'ютера.



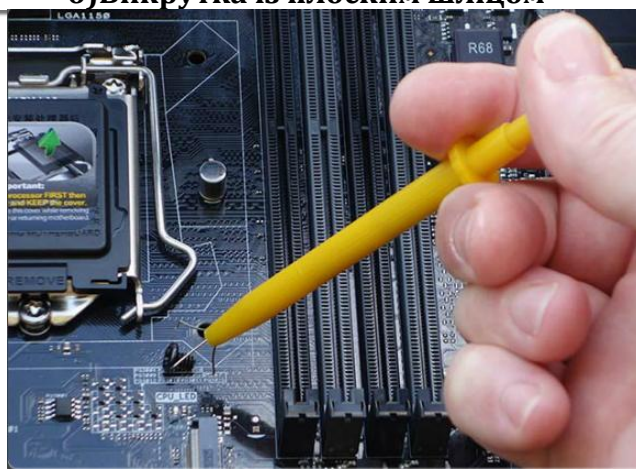
а)Гвинти



б)Викрутка із плоским шліцом



в)Хрестова викрутка



г)Інструменти для добування компонентів



Мультіметр Fluke Networks 110 являє приклад устаткування, яке застосовується для перевірки напруги. Щоб вивчити різні функції мультіметра, спробуйте натискати різні кнопки, використовувати різні режими.

Щоб вивчити різні функції мультіметра, спробуйте натискати його кнопки, вивчите шкалу й щупи.

д)

Рис. 4.22 – Ручні інструменти

Для технічного обслуговування й ремонту комп'ютерів можуть використовуватисячисленні спеціальні інструменти, такі як зіркоподібні насадки, антистатичні сумки й рукавички й екстрактори інтегральних схем. Уникайте намагнічених інструментів, таких як викрутки з магнітними наконечниками, або інструментів, у яких використовується магніт для добування маленьких важкодоступних металевих предметів. Додатково існують ще спеціальні пристрої для тестування, застосовувані для діагностики проблем з комп'ютерами й кабелями.

Мультіметр — пристрій, що вимірює напруга постійного й змінного струму, електричний струм і інші електричні характеристики, як показано на рис. 4.22 д).

Тестер для блоку живлення — пристрій, який перевіряє, чи правильно подається електроживлення комп'ютера. Простий тестер блоку живлення може мати тільки світлові індикатори, а більш досконалі версії показують напруга й силуструму.

Кабельний тестер — пристрій, який перевіряє замикання й несправності проводки, наприклад приєднання проведення до неправильного контакту.

Адаптер зворотної петлі — пристрій, який приєднує до порту комп'ютера, концентратора, комутатора або маршрутизатора для виконання діагностичної процедури, називаною перевіркою зворотної петлі. При перевірці зворотної петлі сигнал передається по каналу й вертається до его пристрою, що відправив. У такий спосіб перевіряється цілісність передачі даних.

4.23 Матеріали, що чистять

Підтримка чистоти комп'ютерів усередині й зовні є важливою частиною технічного обслуговування. Бруд може перешкоджати роботі вентиляторів, кнопок і інших механічних компонентів. На рис. 4.23 показані більші скупчення пили на комп'ютерних компонентах.

Занадто більші скупчення пили на електричних компонентах діють як теплоізолятор і втримують тепло. Теплоізоляція знижує здатність радіаторів і вентиляторів охолодження підтримувати потрібну температуру компонентів, що приводить до перегріву й поломкам мікросхем і ланцюгів.

Примітка. Очищаючи комп'ютер зсередини за допомогою стисненого повітря, направляйте сопло на компоненти з відстані не менш 10 див. Блок живлення й вентилятор потрібно очищати із задньої сторони корпуса.

УВАГА! Перш ніж чистити будь-який пристрій, виключите його й відключите від джерела живлення.



Рис. 4.23– Скупчення пили на вентиляторі відеокарти.

Корпуси комп'ютерів і монітори

Для чищення комп'ютерних корпусів і зовнішніх поверхонь моніторів використовуйте розчин м'якого засобу, що чистить, і вологу безворсову тканину. Змішайте краплю рідини для миття посуду й 120 мол води для одержання розчину, що чистить. Якщо вода просочилася усередину корпуса, дайте їй досить часу, щоб висохнути, перш ніж включати комп'ютер.

Якщо комп'ютер установлений у місці, де він підданий надмірному забрудненню або запиленню, слід використовувати корпус, що дозволяє запобігти влученню великої кількості пили, щоб уникнути ушкодження компонентів комп'ютера. Такий корпус повинен бути оснащений фільтрами для запобігання влучення пили усередину корпуса. Регулярно очищайте або заміняйте такі фільтри.

ЖК-дисплеї

Не використовуйте, що чистять засоби для стекол або будь-які інші засоби, що містять аміак, для ЖК-дисплеїв, крім тих випадків, коли очисник спеціально розроблений для цієї мети. Агресивні хімічні речовини ушкоджують покриття дисплея. Найчастіше такі дисплеї не мають захисного скла, тому протирайте їх з особливою обережністю й не давите на дисплей занадто сильно.

Очищайте, що запилилися компоненти за допомогою стисненого повітря. Стиснене повітря не викликає нагромадження електростатичного заряду на компонентах. Переконаєтеся, що приміщення вентилюється належним чином, перш ніж видувати пил з комп'ютера. Рекомендується надягати респіратор, щоб не вдихати частки пилу.

Здувайте пил переривчастими струменями повітря з балончика. Ніколи не нахиляйте балончик і не перевертайте його під час застосування. Не допускайте, щоб лопати вентилятора оберталися від потоку стисненого повітря. Утримуйте вентилятор нерухомо. Мотор вентилято-

ра може зламатися, якщо лопати будуть обертатися при виключеному моторі.

Контакти компонентів

Використовуючи безворсову тканину, злегка змочену в ізопропіловом спирті, обережно протріть контакти на компонентах. Не використовуйте медичний спирт. Медичний спирт містить домішки, які можуть ушкодити контакти. Перед повторною установкою використовуйте стиснене повітря, щоб здути волокна з контактів.

Клавіатури

Чистите настільну клавіатуру за допомогою стисненого повітря, а потім використовуйте ручний пилосос із насадкою-щіткою, щоб вилучити пил, що залишився.

УВАГА! Ніколи не використовуйте стандартний пилосос для видалення пили з комп'ютера. Пластмасові деталі пилососа можуть накопичувати статична електрика й розряджатися про компоненти. Використовуйте тільки пилососи, призначені для електронних компонентів.

Миші

Для очищення зовнішньої поверхні миші використовуйте, засіб що чистить для скла і м'яку тканину. Не розпорошуйте, що чистить засіб безпосередньо на мишу. При очищенні кулькової миші можна вийняти кульку й почистити її, засобом що чистить для скла і м'якою тканиною. Начисто протріть ролики усередині миші за допомогою тієї ж тканини. Не розпорошуйте ніяких рідин усередину миші.

У Табл.4.1 показані комп'ютерні компоненти, які потрібно чистити й відповідні їм матеріали, що чистять.

Таблиця 4.1 – Комп'ютерні компоненти, які потрібно чистити й відповідні їм матеріали, що чистять

Корпус комп'ютера й зовнішня поверхня монітора	**Матеріали, що чистять**
ЖК-Дисплей	Розчин, що чистить, для ЖК-дисплеїв або дистильована вода й безворсова тканина
ЭЛТ-Монітор	Дистильована вода й безворсова тканина
Радіатор	Стиснене повітря
ОЗП	Ізопропиловий спирт і безворсова щітка
Клавіатура	Ручний пилосос із насадкою-щіткою
Миша	М'яка безворсова тканина і засіб що чистить

Висновки

В Розділі 4. розглянуті загальні правила технікою безпеки при обслуговуванні кінцевого обладнання телекомунікаційних систем з використанням інструментів, електрична безпека і пожежна безпека під час експлуатації і профілактичних робіт кінцевого обладнання телекомунікаційних мереж

Проаналізований впливелектростатичних розрядів,електромагнітних перешкод, клімату на працездатністькінцевого обладнання телекомунікаційних систем.Обґрунтовані вимоги допараметрів коливань напруги електроживлення, які контролюються пристроями для захисту електроживлення.

Розглянуті паспорт безпеки і заходи утилізації обладнання.Наданий загальні правила використання інструментів їх перелік за призначенням: засоби запобігання ЕСР (Антистатичний браслет і килимок), ручні інструменти,інструменти для роботи з кабелями, для очищення, для діагностики. Пояснені особливості застосування засобів управління дисками, захисних програмних засобів іматеріалів, що чистять від пилу.

Список використаних джерел

Керівні документи

1. Закон України «Про охорону праці». В редакції Закону N229-IV (229-15) від 21.11.2002, Відомості Верховної Ради, 2003, N 2, ст.10. https://zakon.rada.gov.ua/laws/show/2694-12#Text

2. Постанова Верховної Ради №188/98 від 5 березня 1998р. «Про Основні напрями державної політики України у галузі охорони довкілля, використання природних ресурсів та забезпечення екологічної безпеки» https://zakon.rada.gov.ua/laws/show/188/98-%D0%B2%D1%80#Text

3. Наказ МНС України від 7.05.2007 року № 312 Про затвердження Правил безпеки праці в органах і підрозділах МНС України. https://www.dsns.gov.ua/files/2019/2/14/321/PRAVIL_Ohor-Pr_MNS.pdf

Література

4. В. О. Собина, Д. В. Тарадуда, М. М. Піксасов, Л. В. Борисова, О. В. Закора, А. Б. Фещенко, М.В. Маляров, Д. Л. Соколов, Дослідження проблем функціонування системи зв’язку ДСНС, використання засобів телекомунікацій та інформатизації в системі ДСНС, шляхів їх розвитку із застосуванням сучасних телекомунікаційних та інформаційних технологій, Звіт про НДР: № держреєстрації 0119U001009, Х.: НУЦЗУ, 2020. – 85 с. Режим доступу: http://ndr.dsns.gov.ua/?p=7135.

5. Тararака В. Д. Архітектура комп'ютерних систем: навчальний посібник. – Житомир : ЖДТУ, 2018. – 383 с.

6. Воробієнко П. П., Захарченко М. В., Орел Л. В. Безпека життєдіяльності: навчальний посібник – Одеса: ОНАЗ ім. О. С. Попова – 2013. –76 с.

7. Курс IT Essentials Мережевої академії Cisco [Електронний ресурс]. Режим доступу: https://www.netacad.com/ru/courses/os-it/it-essentials

8. Сучасні телекомунікаційні мережі у цивільному захисті: Підручник. / Г.В. Щербак, Л.І. Мельникова, І.В. Рубан, К.В. Садовий, Д.В. Сумцов. – Харків, УЦЗУ, 2007. – 261 с

9. Чуб І.А. та ін. Автоматизовані системи управління та зв`язок у цивільному захисті. – Харків: УЦЗУ, 2005.-240 с.

Питання та завдання для самостійного контролю знань

Контрольні питання

5. Загальні правила техніки безпеки.
6. Електрична безпека і пожежна безпека.
7. Електростатичний розряд і електромагнітні перешкоди.
8. Вплив клімату на роботу телекомунікаційного обладнання.
9. Типи коливань напруги електроживлення.
10. Пристрої для захисту електроживлення.
11. Паспорт безпеки, утилізація обладнання.
12. Засоби запобігання ЕСР.
13. Ручні інструменти.
14. Інструменти для роботи з кабелями.
15. Інструменти для очищення.
16. Інструменти для діагностики.
17. Засоби управління дисками.
18. Захисні програмні засоби.
19. Антистатичний браслет.
20. Антистатичний килимок.
21. Матеріали, що чистять.

Питання для тест-контролю

1. Чому слід носити антистатичний браслет при роботі з електронним обладнанням?

Для відводу статичної електрики від компонента і його безпечногопереносу від обладнання до точки заземлення.

Для виключенняутворення зарядів статичної електрики, викликаного контактом з одягом із шовку, поліестру або вовни.

Для вирівнювання електричного заряду між тілом людини й обладнанням.

Для запобігання перешкод від одягу й незакріплених прикрас.

2. Яким способом лінійно-інтерактивний ДБЖ захищає обладнання комп'ютера від тривалого зниження напруги й аварійних перерв в енергопостачанні?

шляхом перемикання з основного на резервне джерело живлення

шляхом зупинки потоку напруги, що надходить на комп'ютер

шляхом використання акумулятора для подачі постійного рівня

напруги

шляхом заземлення надлишкової електричної напруги

3. Яку небезпеку представляє утилізація ЕПТ-монітора для технічного фахівця, що здійснює таку утилізацію?

Збереження залишкової високої напруги.

Небезпека для органів подиху.

Наявність вибухових матеріалів.

Наявність шкідливих хімічних речовин.

4. Чому олівець не можна використовувати усередині комп'ютера?

Графить в олівці може індуціюватиструм.

Графить є струмопровідним матеріалом.

Графить викликає корозію.

Олівець може втримувати статичний заряд.

5. Який інструмент слід використовувати, якщо користувачу потрібно оптимізувати простір на жорсткомудиску?

Format

Fdisk

Управління дисками

Оптимізація дисків

6. Укажіть порядок дій при роботі з вогнегасником. (Використовуються не всі варіанти.)

Направити на підставу вогню, а не на саме полум'я

Описувати соплом дуги зі сторони убік

Оцінити площу, охоплену вогнем

Натиснути на важіль

Висмикнути чеку

1-й

2-й

3-й

4-й

Не використовується

7. Інженер припускає, що блок живлення несправний. Як це можна перевірити?

перевіривши температуру блоку живлення

від'єднуючи по черзі всі роз'єми й включаючи живлення комп'ютера

розібравши блок живлення

за допомогою мультіметра

8. Інженер витягає новий відеоадаптер PCIe з антистатичного пакета, щоб установити плату в настільний комп'ютер. Які двазаходи потрібно прийняти інженеру для захисту плати й інших компонентів комп'ютера? (Виберіть два варіанти.)

Екранувати плату й комп'ютер від джерел ЕМВ.

Підключити комп'ютер до ІБЖ під час установки плати.

Забезпечити низьку вологість на робочому місці.

Використовувати правильно підключений антистатичний браслет.

9. Якаобставина збільшує ймовірність ушкодження комп'ютера від ЕСР?

заземлення на корпус комп'ютера з метою зняття статичного заряду із себе

робота при низькомурівні вологості

підключення принтера до ІБЖ

використання викрутки з магнітною головкою при роботі з жорстким диском

10. Який засіб, що чистить, рекомендується використовувати для очищення контактів компонентів комп'ютера?

воду, змішану з невеликою кількістю засобу для миття посуду

склоочисник з нашатирним спиртом

ізопропіловий спирт

медичний спирт

РОЗДІЛ 5. ЗБОРКА КІНЦЕВОГО ОБЛАДНАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ І ОСНОВНІ ЗАХОДИ ЙОГО ПРОФІЛАКТИЧНОГО ОБСЛУГОВУВАННЯ

5.1 Зборка кінцевого обладнання телекомунікаційних систем

Основним елементом кінцевого обладнання телекомунікаційних систем є ПК, тому зборка комп'ютерів є важливою частиною роботи персоналу. Інженерному складу слід використовувати логічний і методичний підхід до роботи з компонентами комп'ютера. Іноді буде потрібно визначити, чи бідує комп'ютер замовника у відновленні або заміні. Важливо розвивати навички по установці компонентів, діагностиці несправностей і їх усуненню. У цій главі обговорюється важливість сумісності компонентів. Крім того, у ній розглядаються відповідні системні ресурси для роботи з устаткуванням і програмним забезпеченням засобів інформаційних технологій [1-3].

5.1.1 Відкриття корпусу персонального комп'ютера

При зборці або ремонті комп'ютера важливо підготувати робочий простір, перш ніж відкривати корпус комп'ютера. Вам буде потрібно відповідне висвітлення, гарна вентиляція й комфортна температура в приміщенні. До робочого місця або стола повинен бути забезпечений доступ з будь-якого боку. Не захаращуйте робочу поверхню інструментами й комп'ютерними компонентами. Покладіть на стіл антистатичний килимок, це допоможе захистити електронне обладнання від ЕСР. Корисно використовувати невеликі контейнери для зберігання гвинтів і інших деталей, які ви знімаєте [4-8].

Комп'ютерні корпуси випускаються в різних формфакторах. Нагадаємо, що формфактор корпусу — це його розмір і форма. Також існують різні методи відкривання корпусів. Щоб впізнати, як відкривається конкретний комп'ютерний корпус, звіритеся з посібником користувача або зверніться на сайт виробника.



Рис.5.0 – Новий порожній корпус комп'ютера

Більшість комп'ютерних корпусів відкриваються одним з наступних способів:

Кожух комп'ютерного корпусузнімається як єдине ціле.

Знімаються верхня й бічні панелі корпусу.

Верхня панель корпусназнімається раніше бічних.

Щоб відкрити бічну панель, яка відкривається як стулка, потрібно відкритизасувку.

На рис. 5.0 показаний новий порожній корпус формфактора ATX. Корпус (або шасі) являє собою порожній каркас із попередньо встановленими вентиляторами й кабелями для підключення останніх, а також із кнопками на передній панелі, світлодіодними індикаторами, портами USB, аудіо-роз'ємами й іншими гніздами.

5.1.2 Установка компонентів ПК

5.1.2.1 Установка блоку живлення

Від інженера може знадобитися замінити або встановити блок живлення, як показано на рис. 5.1. Більшість блоків живлення можна встановити в корпус комп'ютера тільки одним способом. Завжди додержуйтеся інструкцій по установці, зазначених у керівництві до корпусу комп'ютера й блоку живлення.



а) **б)**

Рис. 5.1 – Блок живлення а) та готова розводкакабелів б)

Нижче представлений основний порядок установки блоку живлення.

Крок 1. Вставте блок живлення в корпус.

Крок 2. Сполучить отвори на блоці живлення з відповідними отворами в корпусі.

Крок 3. Зафіксуйте блок живлення в корпусі, використовуючи підходящі гвинти.

Порада по установці. Спочатку закрутите гвинти рукою, а потім затягніть їхньою викруткою. Це дозволить більш щільно затягти два останні гвинти.

Блоки живлення мають вентилятори, від вібрації яких недостатньо затягнуті гвинти послабляються. Установлюючи блок живлення, переконайтеся, що ви використовуєте всі гвинти й досить затягуєте їх.

Розмістить всі невикористовувані кабелі в корпусі так, щоб вони не заважали роботі інших компонентів або вентиляторів. Для організації кабелів рекомендується використовувати кабельні стяжки, гумки або застібки «липучки». Щоб уникнути накопичення кабелів у корпусі, деякі блоки живлення мають модульну конструкцію. Це означає, що до блоку живлення підключені тільки необхідні кабелі. У міру установки додаткових компонентів у майбутньому підключаються додаткові кабелі живлення. Приклад блоку живлення з готовим розведенням кабелів показаний на рис. 5.2.



Рис. 5.2. – Перевіртесумісність роз’ємів ЦП і сокету МП

Порада по установці. Використовуйте стяжки тільки після підключення кабелів живлення до потрібного компонента.

5.1.2.2Установка ЦП, блоку радіатора й вентилятора

ЦП, радіатор і вентилятор (кулер) слід установлювати на материнську плату перед її установкою в корпус комп'ютера. Це дозволяє краще бачити й переміщати компоненти під час їх установки.

Перш ніж установлюватиЦП на материнську плату, переконайтеся в тому, що він сумісний з роз’ємомЦП, як показано на рис. 5.2. Материнські плати призначені для роботи з певними типами ЦП, і не всі процесори можна встановити в роз’єм, наявний на материнській платі.

У табл. 5.1 представлений опис найпоширеніших типів роз’ємів і примітки по установці процесорів у кожний з них.

Примітка. Роз’єм SEC і LIF є застарілими.

Таблиця5.1 – Архітектури з'єднувачів ЦП

Архітектури ЦП	Примітки по установці |
Single-Edge Connector (SEC)	Сполучить вилучення на ЦП із ключами на рознімані SEC.
Low-Insertion Force (LIF) Zero-Insertion Force (ZIF) Pin Grid Array (PGA)	РозміститьЦП так, щоб індикатор контакту 1 збігався з контактом 1 на розніманіЦП.
Land Grid Array (LGA)	РозміститьЦП так, щоб два вилучення на ньому збігалися із двома виступами на рознімані.

ЦП і материнська плата дуже чутливі до електростатичних розрядів. Неправильний обіг із цими компонентами може привести до ушкодженняобладнання внаслідок ЭСР. Тому при установці або добуванніЦП завжди поміщайте компоненти на антистатичний килимок і надягайте антистатичний браслет (або антистатичні рукавички).

УВАГА! При роботі зі ЦП ніколи не торкайте його контакти. ТримаєтеЦП на антистатичномукилимку доти, поки він вам не знадобиться. ЗберігаєтеЦП в антистатичномувпакуванні.

Нижче представлений порядок установкиЦП і кулера.

Крок 1. Сполучите контакт 1 на ЦП із контактом 1 на рознімані, як показано на табл. 5.2 (1). На ЦП такий контакт позначений крапкою, а на рознімані — трикутником. Звернетеся до документації до ЦП і материнській платі, щоб ознайомитися звідомостями про те, як слід сполучати ці компоненти. Акуратно поміститеЦП у роз'єм. Ніколи не вставляйте ЦП у роз'єм із зусиллям, оскільки можна ушкодити сам ЦП і роз'єм. Якщо відчувається опір, припинитеустановку й переконаєтеся, що ЦП орієнтований правильно.

Крок 2. ЦП фіксується в рознімані материнської плати за допомогою фіксуючої пластини. Вилучите фіксуючу пластину на ЦП, як показано на табл. 5.2 (2).

Крок 3. Вилучитепритискної важіль, щоб зафіксувати пластину, як показано на табл. 5.2 (3).

Крок 4. Зафіксуйте притискної важіль, завивши його за фіксуючий виступ, як показано на табл. 5.2 (4)..

Крок 5. Нанесіть термопасту на ЦП, як показано на табл. 5.2 (5)Для відводу тепла від ЦП застосовується термопаста. У більшості випадків потрібне невелика кількість термопасти. Термопаста рівномірно розподіляється під вагою й тиском блоку радіатора й вентилятора. Випливайте інструкції з нанесення, наданої виробником термопасти.

Крок 6. Сполучите фіксатори кулера з отворами в материнській платі навколо роз'ємЦП, як показано на табл. 5.2 (6).. Будьте обережні, щоб не защемити проведення вентилятора ЦП.

Крок 7. Затягніть фіксатори кулера, щоб закріпити його на місці. Уважно додержуйтеся інструкцій виробника кулератабл. 5.2 (7).

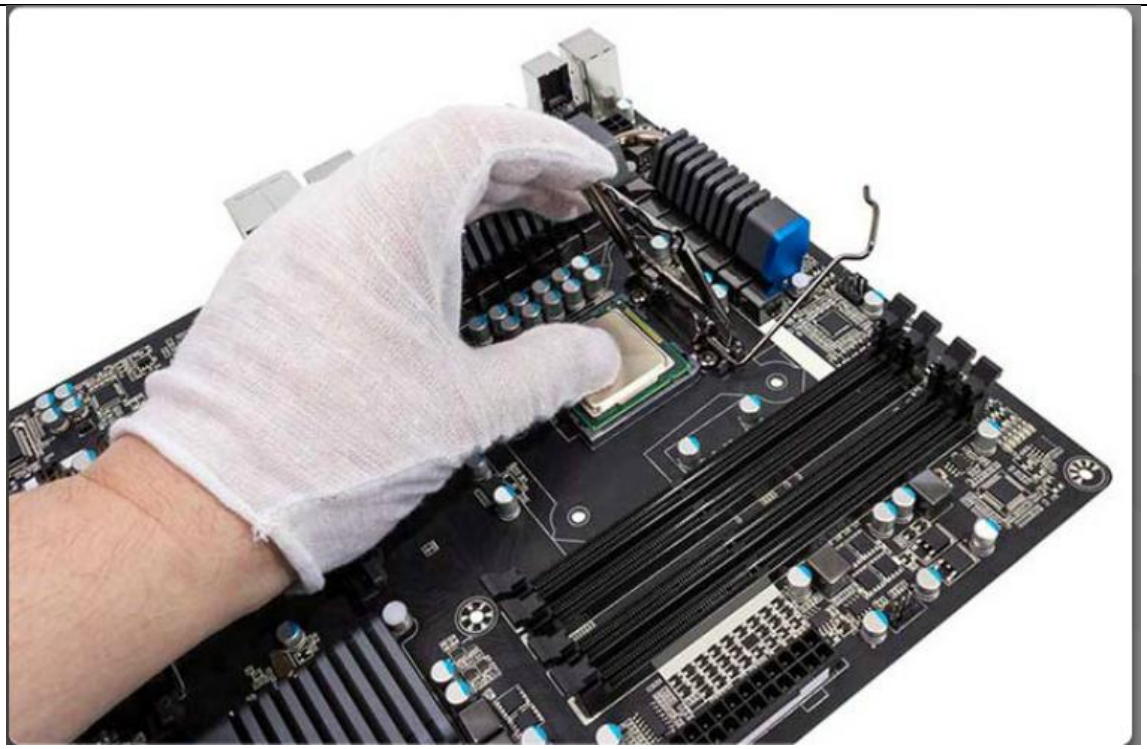
При установцістарогоЦПочистите верх ЦП і нижню частину радіатора безворсовою тканиною, змоченоїізопропіловим спиртом. У такий спосіб ви вилучите стару термопасту й забруднення. Якщо між ЦП і радіатором залишиться бруд, це значно знижує здатністьтермопасти відводити тепло від ЦП. Додержуйтеся рекомендацій виробника по нанесенню термопасти.

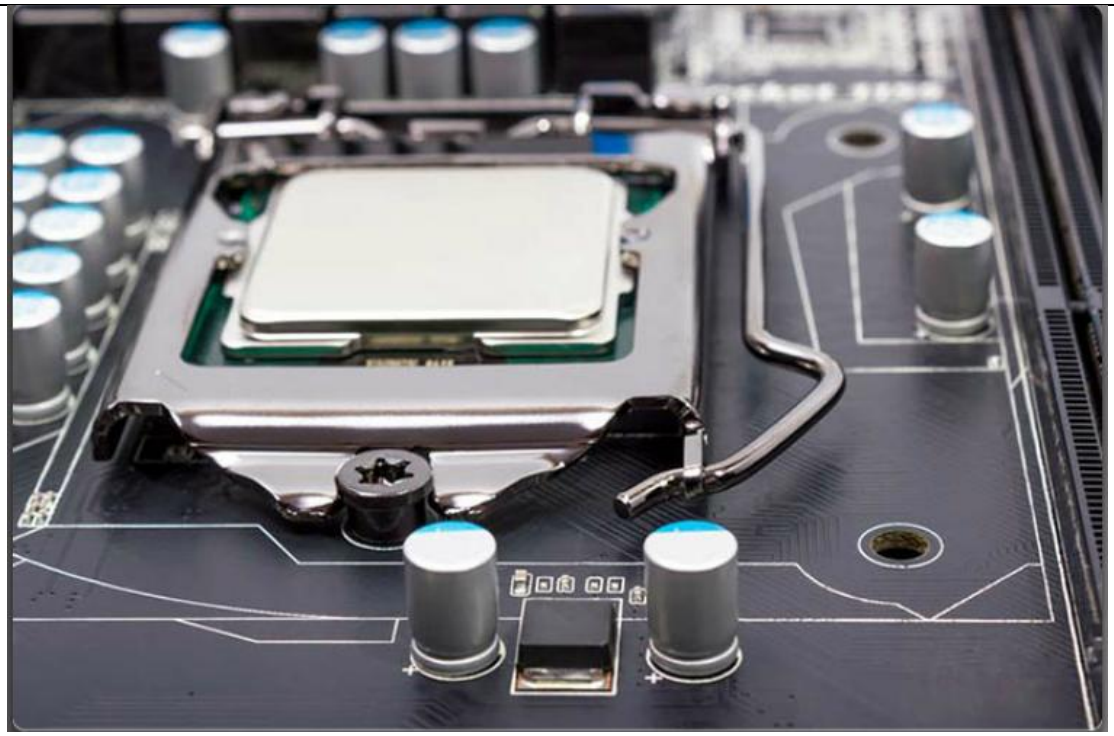
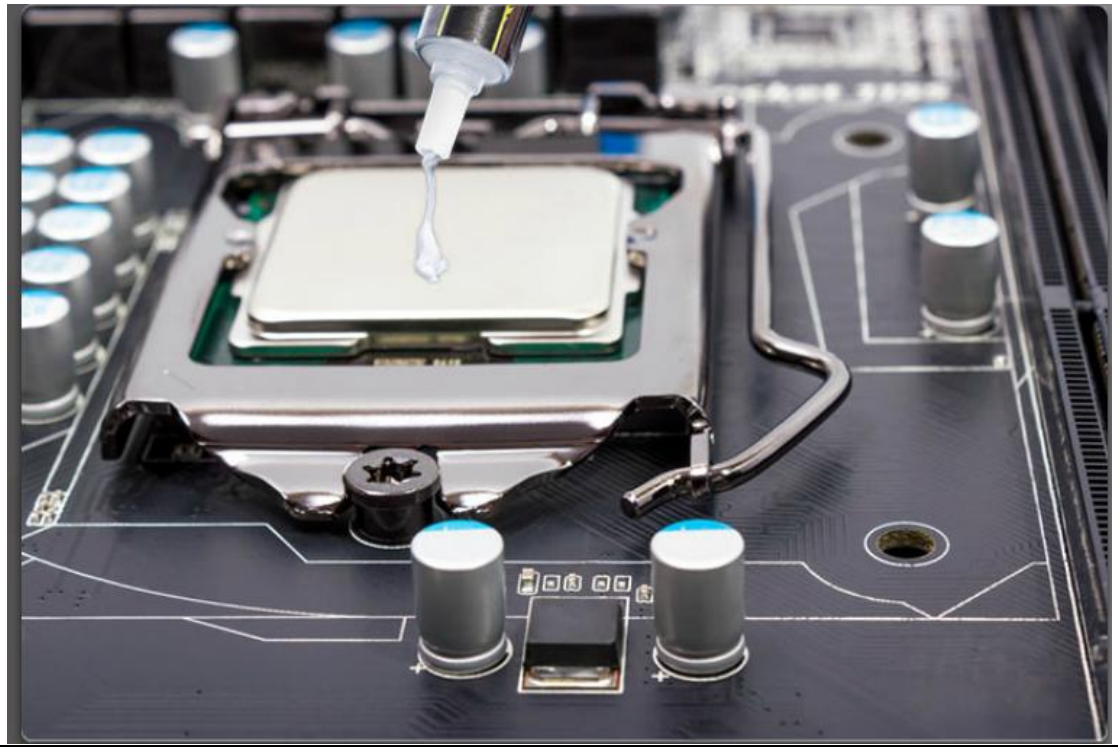
Порада по установці. Замість безворсової тканини можна використовувати паперовий кавовий фільтр.

Примітка.При установціЦП завжди додержуйтеся інструкцій, зазначеним у керівництві до материнської плати. Приклад такого керівництваперебуваєв табл. 5.2

Таблиця5.2 – Установка ЦП

Дії	Опис
1.	**Сполучите ЦП із роз'ємом і акуратно вставте його в роз'єм.** 
2.	**Зафіксуйте ЦП у роз'ємі материнської плати за допомогою фіксуючої пластини.Опустіть фіксуючу пластину.**

	
3.	**Вилучите притискної важіль, щоб зафіксувати пластину.** **Опустіть притискної важіль.** 
4.	**Зафіксуйте притискної важіль, завівши його за фіксуючий виступ.**

	
5.	**Нанесіть термопасту на ЦП.** 
6.	**Сполучите тримачі блоку радіатора й вентилятора з отворами в материнській платі навколо роз'єму ЦП. Встановіть блок радіатора і вентилятора**

		
7.	**Затягніть фіксатори кулеру, щоб закріпити його на місці.**	

5.1.2.3 Установка ОЗП

ОЗП забезпечує тимчасове сховище даних для ЦП і швидкий доступ до них під час роботи комп'ютера. ОЗП — енергозалежна пам'ять. Це значить, що її вміст втрачається при кожномувідключенніживлення комп'ютера.

ОЗП можна встановлювати на материнську плату до її закріплення в корпусікомп'ютера. Переконаєтеся, що ОЗП сумісне з материнською платою, переглянувши документацію до неї або відвідавши веб-сайт виготовлювача.

Так само як ЦП і материнська плата, оперативна пам'ять дуже чутлива до електростатичних розрядів. Тому при установці або витяговіОЗП завжди поміщайте компоненти на антистатичний килимок і надягайте антистатичний браслет (або антистатичні рукавички).

Нижче наведений порядок установкиОЗП на материнську плату.

Крок 1. Відкрийте замки в слоті DIMM (див.табл. 5.3 (1).).

Крок 2. Сполучите вилучення на ОЗП із ключами в розніманні й надавите на модуль (див.табл. 5.3 (2)).

Крок 3. Переконаєтеся в тому, що замки встали на місце (див.табл. 5.3 (3)).

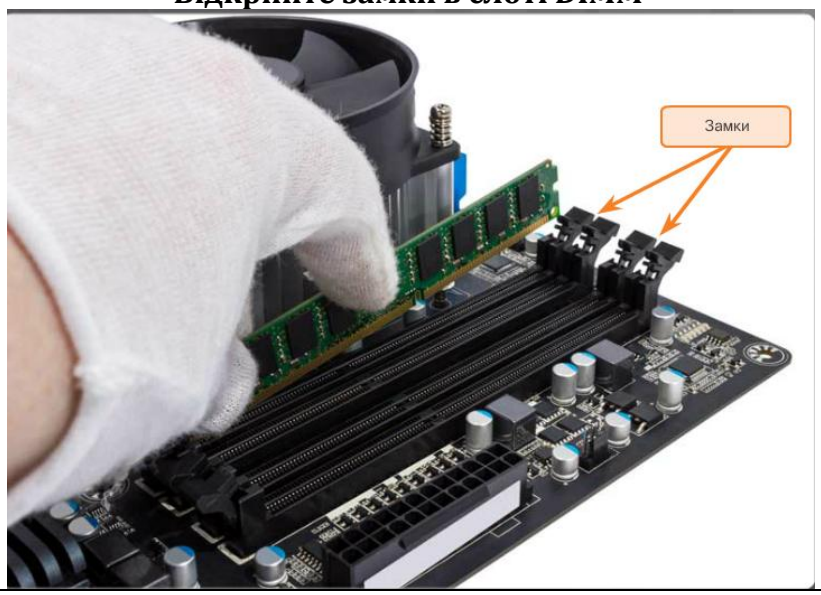
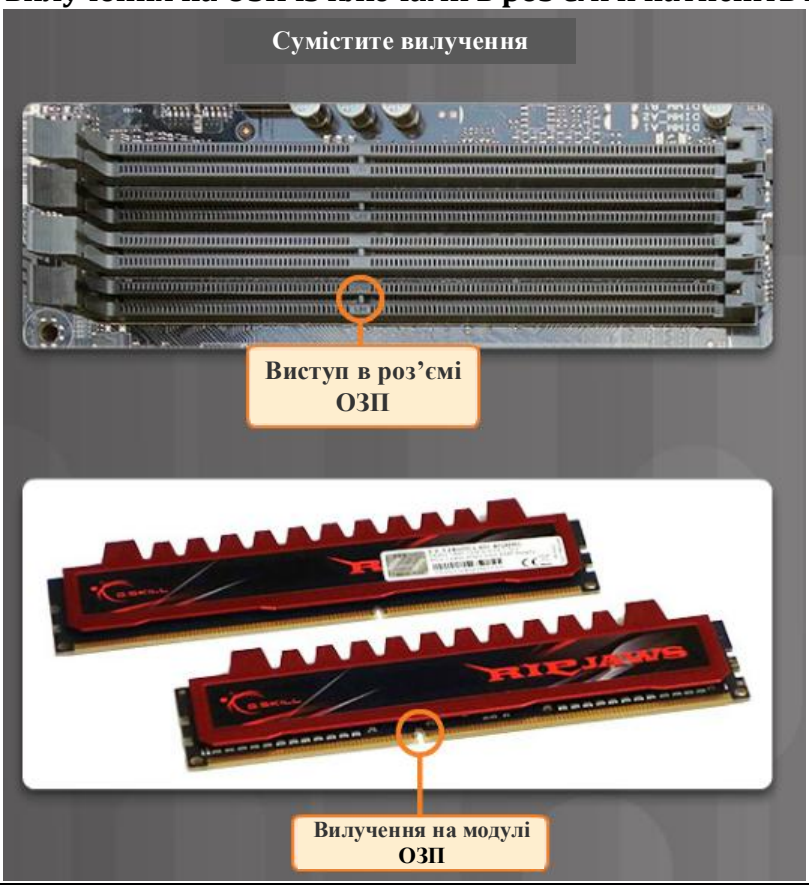
УВАГА! Якщо модуль ОЗП вставлений неправильно, то при включенніживлення комп'ютера він може бути ушкоджений сам і нанести серйозні ушкодження материнській платі.

Крок 5. Переконаєтеся, що кожний модуль пам'яті вставлений у роз’ємповністю й замки надійно фіксують їх на материнській платі (див. табл. 5.3 (3)).

Крок 5. Візуально оцініте, що всі контакти повністю ввійшли вроз’єм(див. табл. 5.3(3)).

Рада по установці. У випадку правильної установки модуля ОЗП в з'єднувачі буде чутне характерне клацання, і ви відчуєте, що замокустав на місце.

Таблиця5.3 – становка ЦП

Дії	Опис
1.	**Відкрийте замки в слоті DIMM** 
2.	**Сумістите вилучення на ОЗП із ключами в роз’ємі й натисніть на модуль** 

3.	**Переконаєтеся в тому, що замки встали на місце** **Встановлені модулі ОЗП** 

5.1.2.4 Установка материнської плати

Тепер материнську плату можна встановити в корпус комп'ютера.

Для установки материнської плати виконаєте наступні дії.

Крок 1. Виберіть підходящі ізоляційні стойки для установки материнської плати в корпус. Слід уникати зіткнення друкованої материнської плати з металевими частинами корпусу. Для цього материнська плата встановлюється в корпус на спеціальні пластикові або металеві стойки, такі, як показано на табл. 5.4 (1).

Крок 2. Установите в комп'ютерний корпус ізоляційні стойки так, щоб вони збігалися з розташуванням кріпильних отворів у материнській платі. Використовуйте тільки ті стойки, які підходять під отвори в материнській платі. На табл. 5.4 (2). показані стойки для материнської плати формфактора ATX. Установка додаткових ізоляційних стойок може перешкодити правильному розташуванню материнської плати в корпусі комп'ютера або навіть ушкодити її.

Крок 3. Установите рамку для інтерфейсів уведення-виводу в задню частину корпусу комп'ютера, як показано на табл. 5.4 (3). Рамкавведення-виводу має вирізи, призначені для роз’ємів на материнській платі.

Крок 5. Сполучитероз’єм введення-виводу в задній частині материнської плати з отворами в рамці вводу-виводу.

Крок 5. Сполучите отвори для гвинтів у материнській платі з ізолюючими стойками.

Крок 6. Спочатку вставте всі гвинти й закрутите їх від руки, перш ніж затягувати їхньою викруткою. Не затягуйте гвинти занадто сильно.

Поради по установці. Вставте з'єднувачі в задній частині материнської плати в отвори в рамці вводу-виводу, щоб сполучити отвори на материнській платі, а потім вставте перший гвинт. Крім того, для вставки гвинтів в отвори і їх закручування від руки корисно використовувати екстрактор.

Таблиця 5.4 – Установка материнської плати

Дії	Опис
1.	Виберіть відповідні ізоляційні стойки для установки материнської плати в корпус. 
2.	Установіте в комп'ютерний корпус ізоляційні стойки так, щоб вони збігалися з розташуванням кріпильних отворів у материнській платі. 
3.	Установіть рамку для інтерфейсів уведення-виводу в задню частину комп'ютерного корпусу.

	
4.	Сполучите роз’єми введення-виводу в задній частині материнської плати з отворами в рамці вводу-виводу.
5.	Сполучите отвори для гвинтів у материнській платі з ізолюючими стійками.
6.	Спочатку вставте всі гвинти й закрутите їх від руки, перш ніж затягувати їхньою викруткою.

5.1.2.5 Установка жорсткого диска

Для розміщення приводів у корпусікомп'ютера є спеціальні відсіки. У табл. 5.5 представлений опис трьох найпоширеніші типів відсіків для приводів.

Щоб установити жорсткий диск, виберіть вільний відсік для приводів, відповідний до ширини диска. Для установки невеликих приводів у широкі відсіки використовуються спеціальні лотки або адаптери.

Нижче представлений порядок установки 3, 5-дюймового жорсткого диска (шириною 8,9 див) в 3, 5-дюймовий відсік для привода табл. 5.6.

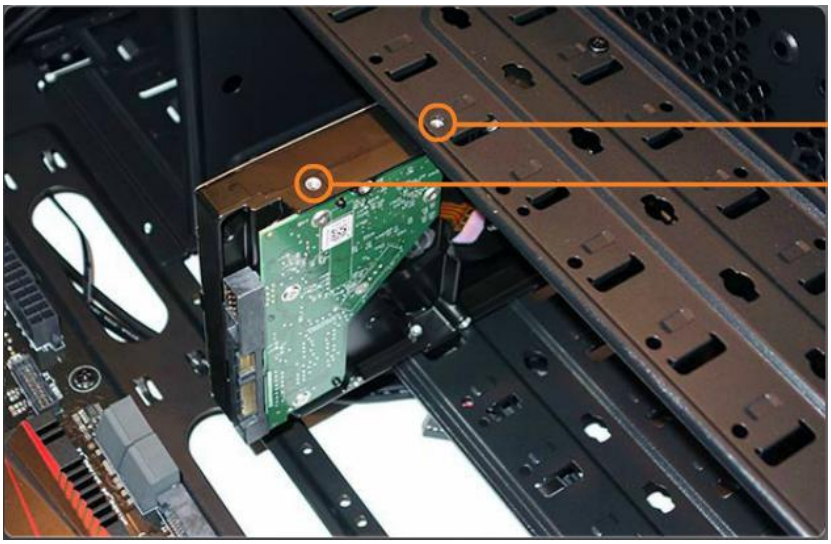
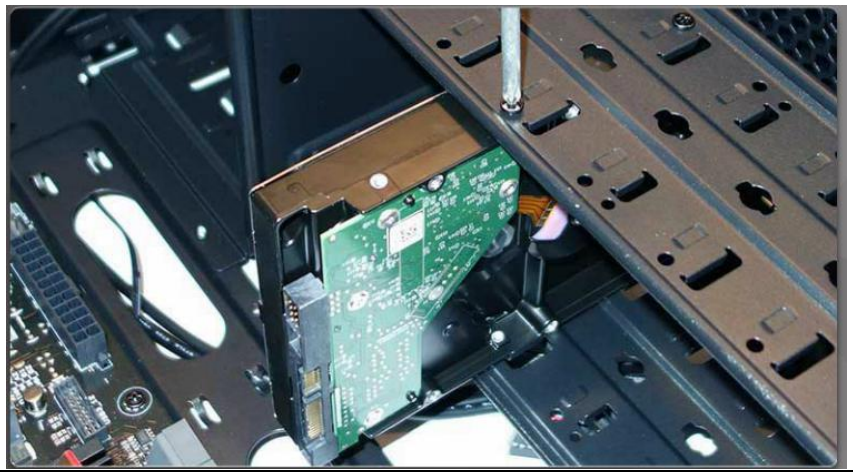
Таблиця 5.5 – Типи відсіків для приводів

Ширинавідсікудляприводів	**Опис**
5,25 дюйма (13,34 см)	• Звичайно використовується для установки приводів оптичних дисків. • У більшості повнорозмірних вертикальних корпусів є два відсіки або більш.
3,5 дюйма (8,9 см)	• Звичайно використовується для установки 3, 5-дюймових жорстких дисків. • Служить для установки додаткових портів USB або пристроїв читання смарт-карт. • У більшості повнорозмірних вертикальних корпусів є два внутрішні відсіки або більш.
2,5 дюйма (6,35 см)	• Призначений для невеликих 2, 5-дюймових жорстких дисків і твердотільних накопичувачів. • Самий вузький відсік. • Стає популярним у нових моделях корпусів.

При установці в корпус декількох дисків рекомендується забезпечити достатній зазор між ними, необхідний для ефективного охолодження компонентів. Крім того, диск слід установлювати металевою стороною нагору. Вона призначена для розсіювання тепла, виділюваного жорстким диском.

Порада по установці. Спочатку закрутите гвинти від руки, перш ніж затягувати їхньою викруткою. Це дозволить більш щільно затягти два останні гвинти.

Таблиця 5.6 – Порядок установки материнської плати жорсткого диска

Дії	Опис
1.	**Крок 1.** Розмістите жорсткий диск так, щоб він був на одномурівні із прорізом відсіку для привода.
2.	**Крок 2.** Вставте жорсткий диск у відсік таким чином, щоб отвору для гвинтів привода збіглися з отворами в корпусі. 
3.	**Крок 3.** Закріпите жорсткий диск усередині корпусупідходящими гвинтами 

5.1.2.6 Установка привода оптичних дисків

Оптичні приводи встановлюються в 5, 25-дюймові відсіки (шириною 13,34 див), до яких є доступ з передньої панелі корпусу. Такі відсіки забезпечують доступ до носіїв даних без відкриття корпусу.



Рис. 5.3 – Установка привода оптичних дисків

Нижче представлений порядок установки оптичного привода.

Крок 1. Розміститепривод оптичних дисків так, щоб він був на одномурівні із прорізом 5, 25-дюймового відсіку на лицьовійсторонікорпусу, як показано на рис. 5..

Крок 2. Вставте привод оптичних дисків у відсік таким чином, щоб отвору для гвинтів у приводі збігалися з отворами в корпусі.

Крок 3. Зафіксуйте привод оптичних дисків у корпусі, використовуючи підходящі гвинти.

Порада по установці. Спочатку закрутите гвинти від руки, перш ніж затягувати їхньою викруткою. Це дозволить більш щільно затягти два останні гвинти.

5.1.2.7 Типи плат адаптерів

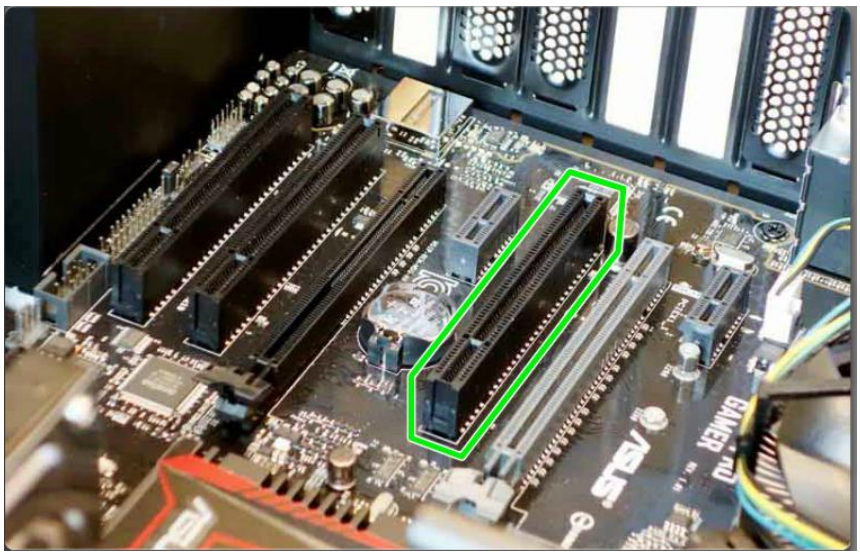
Плати адаптерів розширюють можливості комп'ютера. Існує безліч різних плат адаптерів, включаючи відеоадаптери, плати адаптерів Ethernet і безпроводовоїмережі, звукові карти, ТВ-Тюнери, плати для захоплення відео, плати для підключення зовнішніх портів, таких як USB, Firewire, Thunderbolt, і багато інші.

Плати адаптерів установлюються в перераховані нижче слоти розширення на материнській платі.

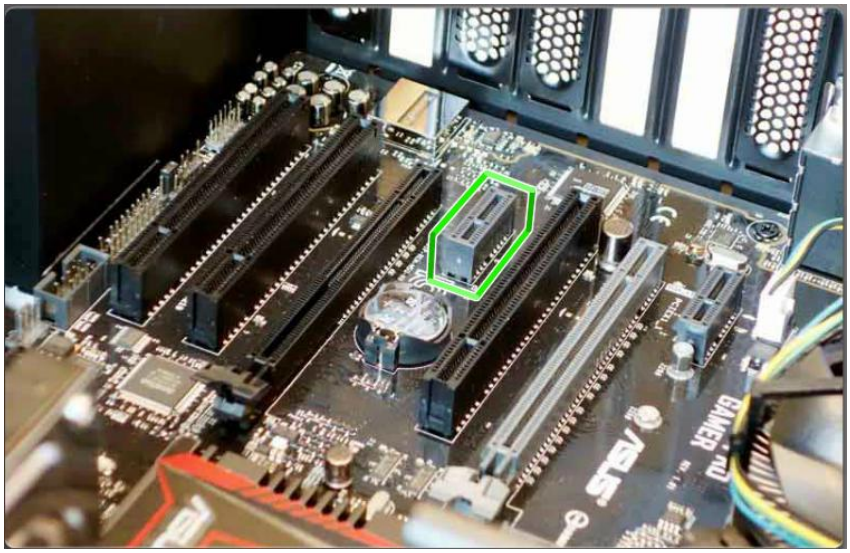
PCI — (див.рис. 5.4. а)) роз’ємвзаємодії периферійних компонентів (PCI) одержав широке поширення й використовується для підключення застарілих плат розширення.

PCIe — роз’ємPCI Express, який представлено чотирма типами слотів: x1 (див.рис. 5.5. б)), x4, x8 і x16 (див.рис. 5.5. в)). Слоти PCIe бувають різної довжини, від самого короткого (x1) до самого довгого (x16).

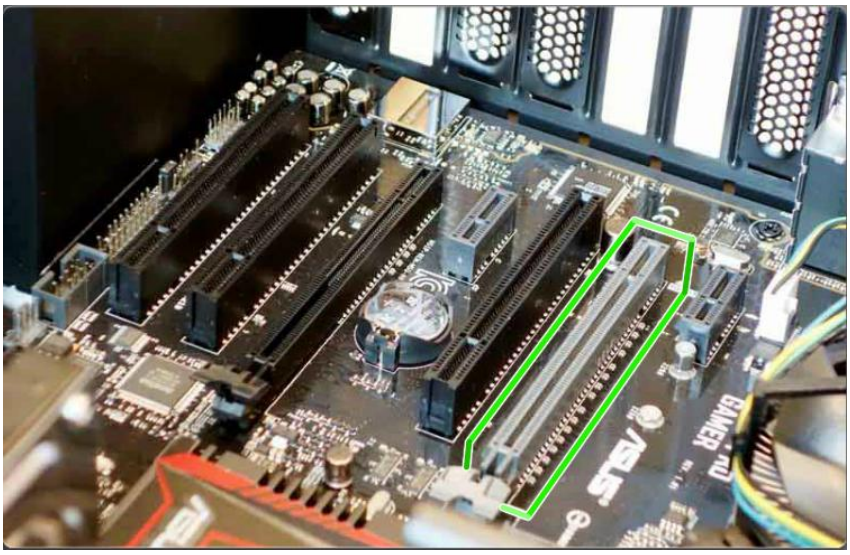
Плати адаптерів, представлені на рис. 5.5., повинні бути сумісні зі слотами розширення на материнській платі.



а)



б)



в)

Рис. 5.4– Роз’єми адаптерів



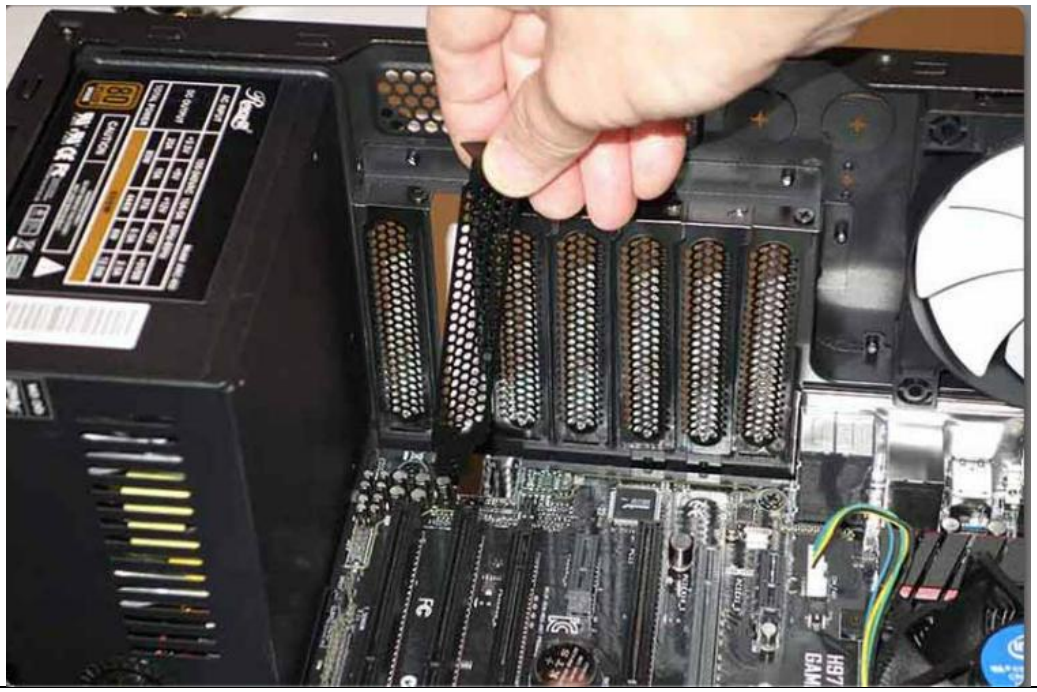
Рис. 5.5 – Плати адаптерів

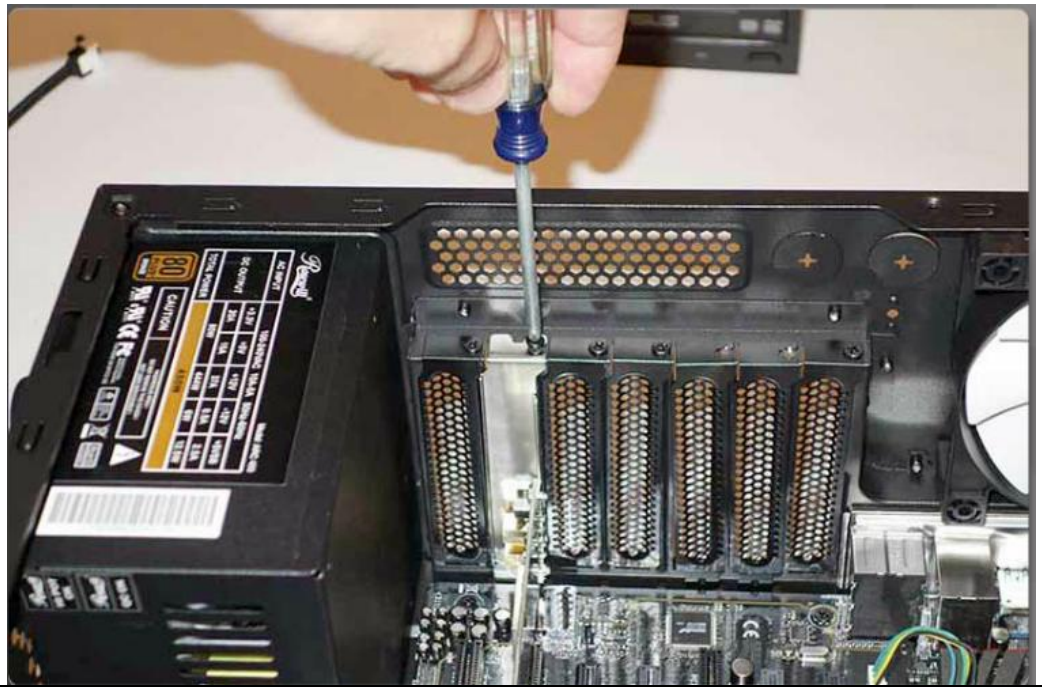
5.1.2.8. Установка адаптера безпроводової мережі

Адаптер безпроводової мережі дозволяє комп'ютеру підключатися до безпроводових мереж (Wi-Fi). Для адаптерів безпроводової мережівикористовуються слоти розширенняPCI або PCIe на материнських платах. Багато адаптерів безпроводової мережі встановлюються в роз'ємUSB.

Нижче представлений порядок установки адаптера табл.5.7.

Таблиця 5.7 – Порядок установки адаптера безпроводової мережі

Дії	Опис
	Крок 1. Знайдіть порожній слот PCI у корпусі й вилучите невелику металеву заглушку 

	Крок 2. Сполучите плату з відповідним слотом розширення на материнській платі.
	Крок 3. Вставте адаптер безпроводової мережі в слот PCI**.** Акуратно надавите на плату, щоб вона повністювстала на місце. 
	Крок 5. Зафіксуйте адаптер безпроводової мережі.Закріпите монтажну скобу адаптера на корпусі комп'ютера підходящим гвинтом. 

5.1.2.9 Установка плати відеоадаптера

Плати відеоадаптерів установлюються в слотірозширенняPCI, AGP і PCIe на материнській платі.

Для установки плати відеоадаптера виконаєтезазначені нижче дії.

Крок 1. Знайдіть порожній слот PCIe x16 у корпусі й вилучите невелику металеву заглушку.

Крок 2. Сполучите плату відеоадаптера з підходящим слотом розширення на материнській платі.

Крок 3. Акуратно надавите на адаптер, щоб він повністювстав на місце.

Крок 5. Закріпите монтажну скобу плати відеоадаптера на корпусі комп'ютера за допомогою підходящого гвинта.

Для роботи багатьох плат відеоадаптера потрібне окреме живлення, яке подається від блоку живлення по кабелю живлення. Цей кабель підключається до 6– або 8-контактному розніманню на відеоадаптері. На деяких платах є два такі роз’єм. По можливості забезпечте зазор між платою відеоадаптера й іншими платами розширення, оскільки перша виділяє досить багато тепла, для відводу якого застосовується вентилятор, установлюваний на плату.

Порада по установці. Перед придбанням відеоадаптера довідайтеся його довжину (і довжини інших плат адаптерів). Довгі плати можуть виявитися несумісні з певними материнськими платами. На материнській платі можуть бути мікросхеми й інші електронні компоненти, які не дозволяють правильно встановити плату адаптера в слот розширення. Крім того, розміри самого корпуса можуть обмежити вибір плат адаптерів, які можна в нього встановити. У комплекті з деякими платами адаптерів можуть іти монтажні скоби різної висоти, щоб їх можна було встановити в корпус відповідного формфактора.



Рис. 5.6. – Установка плати відеоадаптера

5.1.3 Установка блоку живлення

5.1.3.1 Підключення живлення материнської плати

Для роботи материнської плати потрібне електроживлення. Крім того, материнська плата передає частину одержуваного живлення на різні підключені до неї компоненти. Кількість і тип необхідних роз'ємів, які повинні бути на блоці живлення, залежить від материнської плати й установленого на ній процесора. У табл.5.8представлені відомості про різні типи роз'ємів, якими може бути оснащена материнська плата. Зверніть увагу, що для живлення материнської плати звичайно використовується два силові роз'єм.

УВАГА! При підключенні кабелів блоку живлення до інших компонентів слід проявляти обережність. Кабелі, роз'єм й компонента спроектовані таким чином, щоб для підключення не було потрібно велике зусилля. Якщо при підключенні кабелю або іншої деталі доводитьсяприкладати помітні зусилля, щось не так. Ніколи не застосовуйте силу при підключеннироз'єм або компонента. А якщо ні, то можна ушкодити й роз'єм, і гніздо. Якщо при підключеннироз'єм доводиться прикладат ипомітні зусилля, перевірте, чи правильно орієнтоване роз'єм й не чи погнуте контакти.

Таблиця 5.7 – Типи роз'ємів живлення на материнської платі

Стандарт ATX	Опис роз'ємів живлення на материнській платі
ATX	• Основний 20-контактний роз'єм материнської плати • Додатковий 6-контактний роз'єм
ATX12V версії 2.x	• Основний 24-контактний роз'єм материнської плати • Додатковий 4-контактний роз'єм
AMD GES	• Основний 24-контактний роз'єм материнської плати • Додатковий 8-контактний роз'єм
EPS12V	• Основний 24-контактний роз'єм материнської плати • Додатковий 8-контактний роз'єм (звичайно розділений навпіл на два роз'єми по 4 контакта)

Нижче представлений порядок підключення роз'ємівживлення до материнської плати.

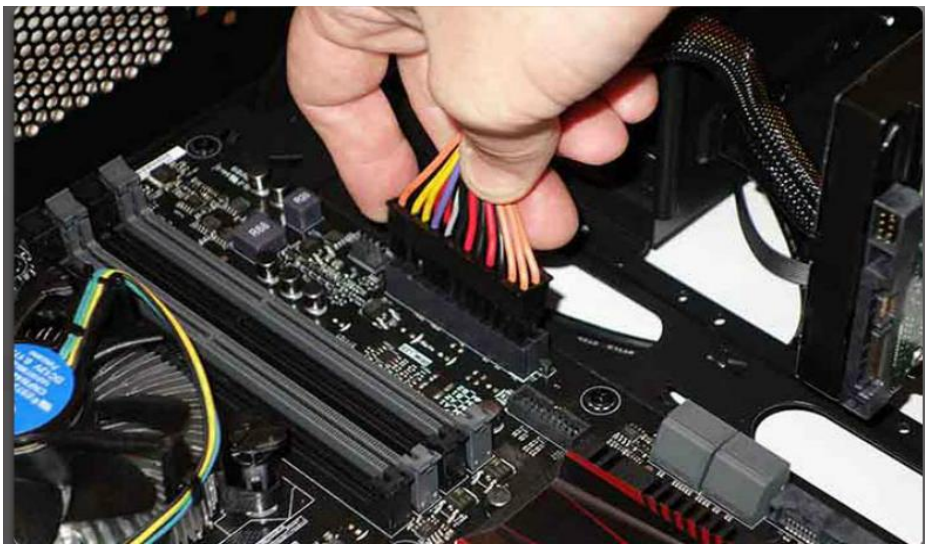
Крок 1. Сполучите 24-контактний (або 20-контактний) роз'ємживлення ATX із гніздом на материнській платі.

Крок 2. Акуратно надавите на роз'єм, поки засувка не встане на місце (див.рис. 5.7 а)).

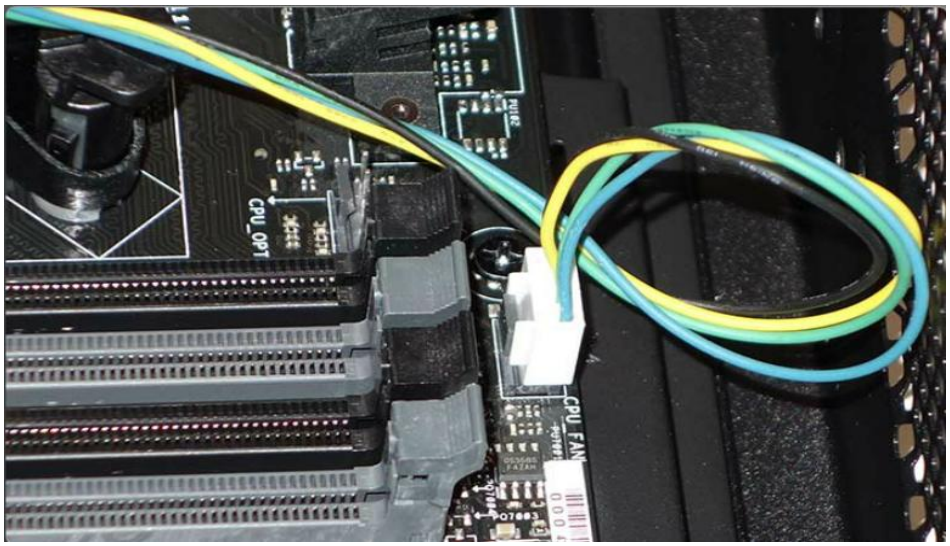
Крок 3. Сполучите 4-контактний (або 8-контактний) додаткове роз'ємживлення із гніздом на материнській платі.

Крок 5. Акуратно надавите на роз'єм, поки засувка не встане на місце (див.рис. 5.7 б)).

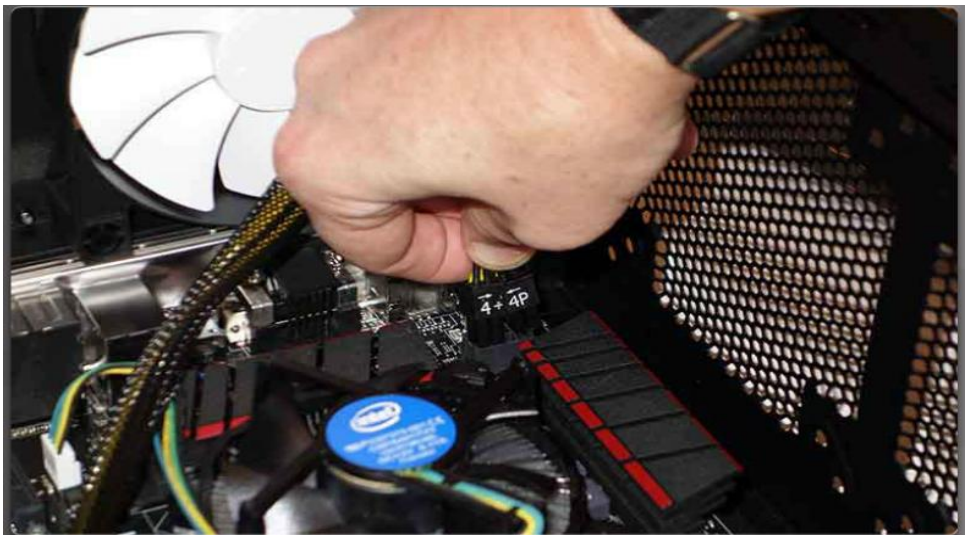
Крок 5. Сполучитероз'ємживлення вентилятора ЦП із роз'ємом на материнській платі (див.рис. 5.7 в)).



а) **Підключення основного 24-контактного роз’єму живлення**



б) **Підключення додаткового 4-контактного роз’єму живлення**



в) **Підключення 4-контактного роз’єму вентилятора ЦП**

Рис. 5.7 – Підключення роз’ємів живлення материнської плати стандарту ATX12V версії 2.x

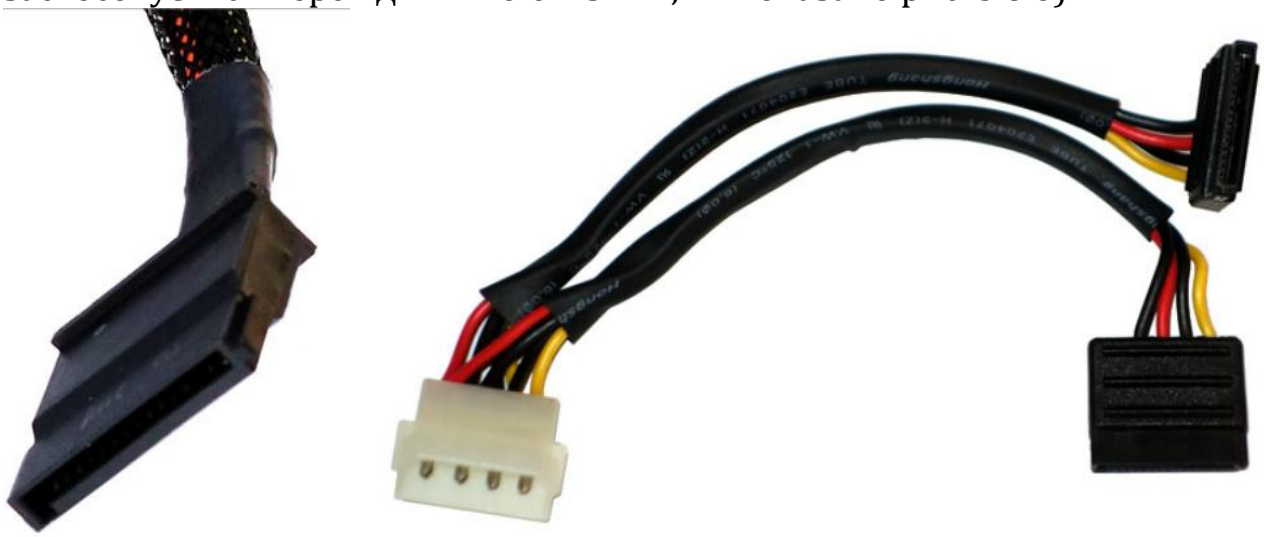
Крок 6. Акуратнонадавите на роз’єм, поки він не буде вставлений повністю.

Порада по установці. Роз’ємживлення спроектовані таким чином, що вставити їх у гніздо можна тільки одним способом. Деякі частини роз’єм мають квадратну форму, а інші небагато округлені. Якщо по зовнішньому вигляду роз’єм можна визначити, що він не встане в гніздо, пам'ятайте, що округлені частини роз’єм можна вставити у квадратні отвори, однак квадратні частини не вдасться вставити в округлені отвори. Роз’ємживлення спеціально розроблені такої форми.

5.1.3.2Підключенняживлення до внутрішніх приводів і вентиляторам у корпусі

Традиційно для живлення жорстких дисків і приводів оптичних дисків використовувалися 4-контактні роз’ємживлення Molex. Тепер для підключення живлення до таких приводів звичайно застосовуються 15-контактні роз’єм SATA, як показано на рис. 5.8 а).

Для зручності використання деякі приводи оснащуються як 15-контактним роз’ємом SATA, так і 4-контактним роз’ємом Molex. На таких приводах слід використовувати тільки одинроз’ємживлення, ніколи не використовуютьсяобоєроз’єм. На багатьох застарілих блоках живлення можуть відсутніроз’єм SATA. Для підключення живлення до таких дисків застосовується перехідник Molex–SATA, як показано рис. 5.8 б).



а) Живлення SATA **б) Адаптер живлення Molex–SATA**

Рис. 5.8 – Роз’єми живлення жорстких дисків і приводів оптичних дисків

Нижче представлений порядок підключення кабелю SATA до диска.

Крок 1. Сполучите 15-контактне роз’ємживлення з портом на диску.

Крок 2. Акуратно надавите на роз’єм, щоб він повністювстав на місце (див.рис. 5.9).

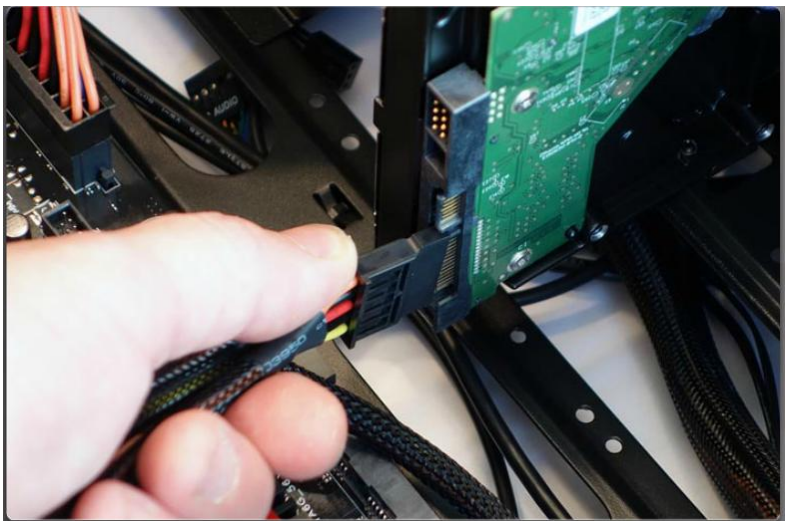


Рис. 5.9 – Підключення роз'єму живлення SATA до внутрішнього накопичувача

Порада по установці. При підключенні кабелів SATA дотримуйте особливої обережності. Якщо спробувати вставити їх із зусиллям під кутом, можна відламати роз'єм на диску.

Для роботи інших периферійних обладнань (наприклад, для вентиляторів у корпусі) також потрібне живлення. На більшості материнських плат для цього передбачені 3– або 4-контактні роз'єм. Нижче представлений основний порядок підключення живлення вентиляторів у корпусі.

Крок 1. Сполучите 3– або 4-контактне роз'ємживлення вентилятора з портом на материнській платі.

Крок 2. Акуратно надавите на роз'єм, щоб він повністювстав на місце (див.рис. 5.10).

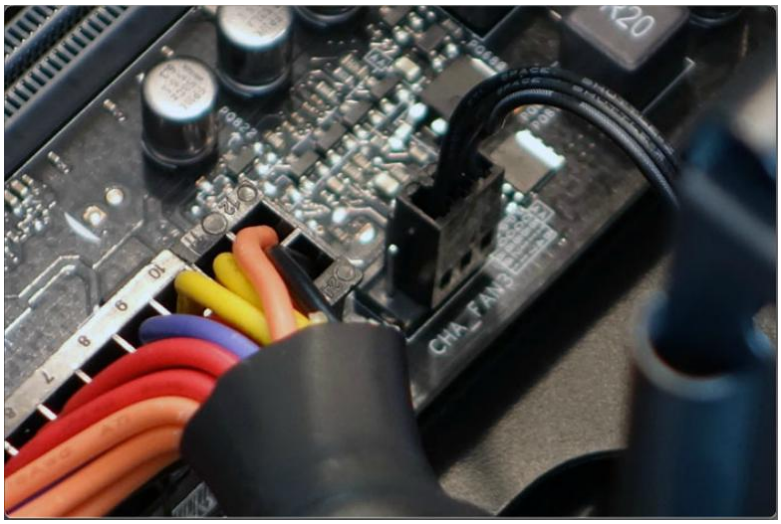


Рис. 5.10 – Підключення роз'єму живлення вентилятора

Підключите інші кабелі корпусу у відповідні роз'єм, керуючись інструкціями до материнської плати й корпусу.

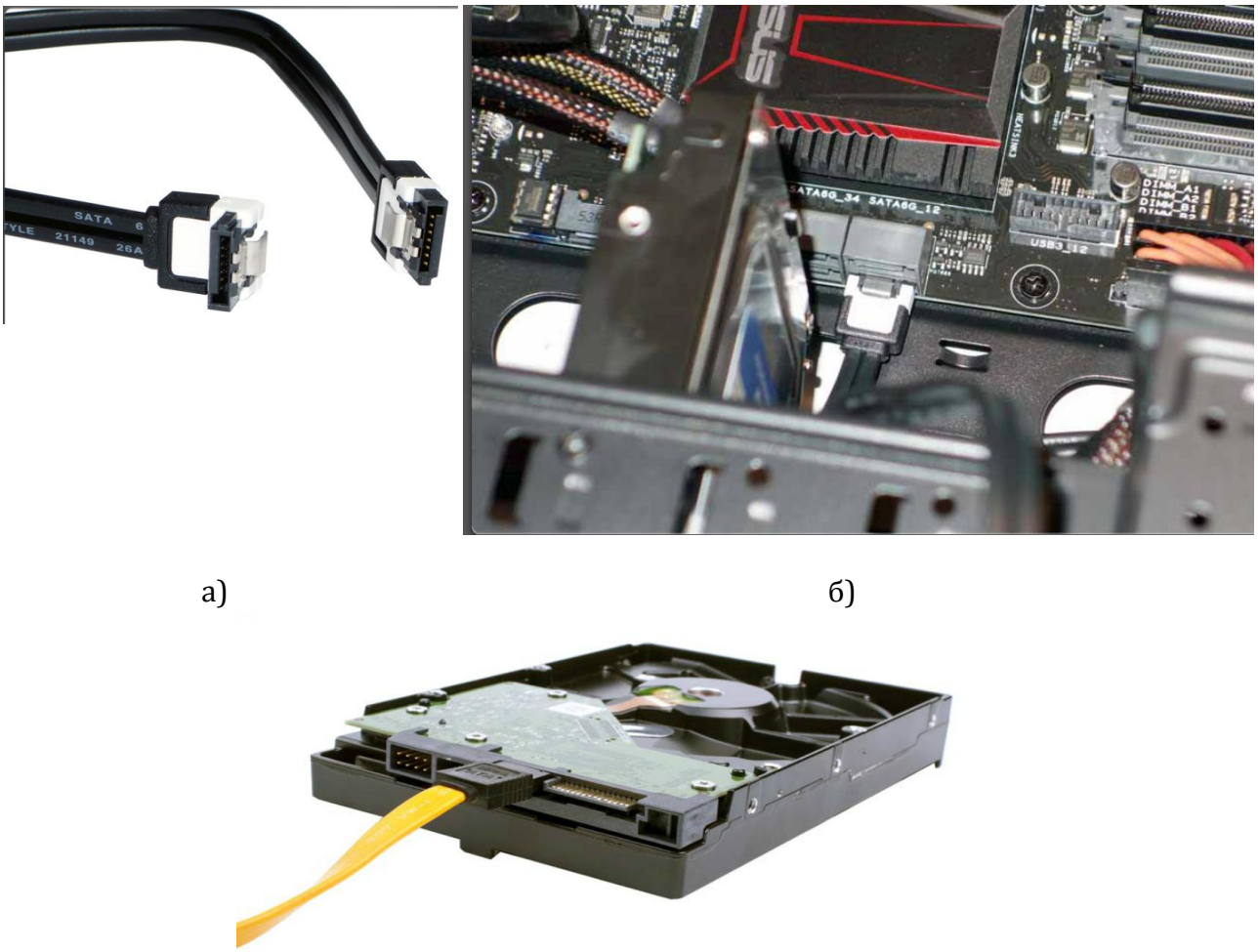
Порада по установці.3-контактні роз’ємживлення вентилятора можна підключати до 4-контактним портам. Роз’єм й гніздо спроектовані таким чином, що їх можна з'єднати, навіть якщо один контакт залишиться незадіяним.

5.1.3.3 Підключення внутрішніх кабелів для передачі даних

Для підключення внутрішніх жорстких дисків і приводів оптичних дисків до материнської плати використовуються кабелі SATA.

Кабель SATA для передачі даних оснащений 7-контактним роз’ємом, як показано на рис. 5. 11 а). Кабелі SATA мають спеціальні ключі, що дозволяють підключити їх тільки в одній орієнтації. На багатьох кабелях SATA також є фіксатори, що дозволяють уникнути від'єднання кабелю. Щоб витягти такий кабель, необхідно затиснути металеву пластину на розніманні й потягнути роз’єм на себе.

Нижче представлений порядок підключення привода до материнської плати за допомогою кабелю SATA для передачі даних.



а) б)

Рис. 5. 11 – Підключення внутрішніх жорстких дисків і приводів оптичних дисків до материнської плати

а) роз’єм кабелюSATA; б) підключення кабелюSATA до материнської плати; в) підключення кабелюSATA до жорсткого диску

Крок 1. Підключитеодин кінець кабелю SATA у гніздо на материнській платі (див.рис. 5. 11 б)). Зверніть увагу, що на материнській платі є кілька гнізд SATA.

Крок 2. Підключите другий кінець кабелю SATA до порту SATA меншого розміру на приводі (див.рис. 5. 11 в)).

Порада по установці. При підключенні кабелів SATA для передачі даних дотримуйте тих же запобіжного заходів, чого й при підключенні силових кабелів SATA. Також не згинайте й не складайте кабель під гострими кутами, оскільки це може негативно позначитися на швидкості передачі даних.

5.1.3.4 Установка кабелів передньої панелі

На корпусі комп'ютера є кнопки управліннямживленням материнської плати й світлові індикатори активності обладнання. За допомогою кабелів, щойдуть із передньої частини корпусу, підключите ці кнопки й індикатори до материнської плати. На рис. 5.12 показані кабелі передньої панелі, які найчастіше зустрічаються в комп'ютерних корпусах. На рис. 5.13 показанерозповсюдженероз'єм системної панелі на материнській платі, до якого підключаються кабелі. На материнській платі біля роз'єм системної панелі є написи, що вказують, куди підключати кожний з кабелів.



Рис. 5.12 – Роз'єми передньої панелі

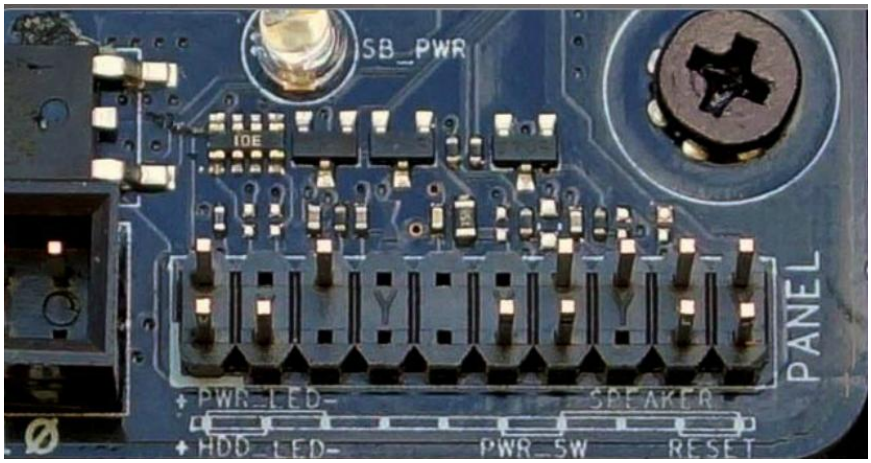


Рис. 5.13 – Роз'єм системної панелі

Роз'єм системної панелі не мають ключів. Наведені нижче інструкції з підключення кабелів до з'єднувачів на системній панелі єзагальними, тому що не існує єдиних стандартів маркування кабелів корпусу й роз'ємівсистемної панелі. Однак на кожномукабелі передньої панелі звичайно є невелика стрілка, що вказує на контакт номер 1, як показано на рис. 5.15.

Примітка. Маркування на ваших кабелях передньої панелі й роз'ємахсистемної панелі можуть відрізнятися від тих, що показані на

рис. 5.15. Завжди звіряйтеся з керівництвом до материнської плати. Там ви знайдете діаграми й додаткову інформацію про підключення кабелів передньої панелі.

Роз’єм системної панелі включають наступні:

Кнопка живлення — служить для включення й вимикання комп'ютера. Якщо не вдається виключити комп'ютер за допомогою кнопки живлення, натисніть і втримуйте її протягом 5 секунд.

Кнопка скидання (Reset) — служить для перезапуску комп'ютера без відключення живлення.

Індикатор живлення — світиться, коли комп'ютер включений, і часто мигає, коли комп'ютер перебуває в сплячомурежимі. Кожна пара контактів індикатору на з'єднувачеві системної панелі материнської плати має контакт номер 1, позначений знайомий «+», як показано на рис. 5.15.

Індикатори активності дисків — світяться або мигають, коли комп'ютер виконує читання даних з жорстких дисків або запис на них.

Системний динамік — материнська плата використовує динамік у корпусі (якщо він є) для оповіщення про стан комп'ютера. Наприклад, одиночний сигнал виходить, що при початку роботи комп'ютера не виникало проблем. Якщо є проблема з устаткуванням, для оповіщення про тип цієї проблеми видається ряд діагностичних звукових сигналів. Важливо відзначити, що системний динамік відрізняється від динаміків комп'ютера, які використовуються для відтворення музики або інших звуків. Для кабелю системного динаміка звичайно використовується чотири контакти на рознімані системної панелі.

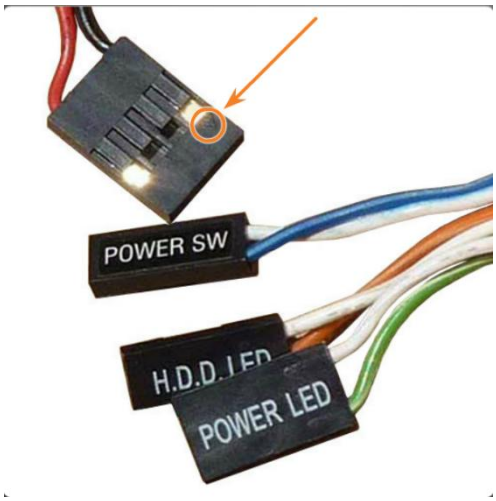


Рис. 5.14– Стрілка індикатор контакту

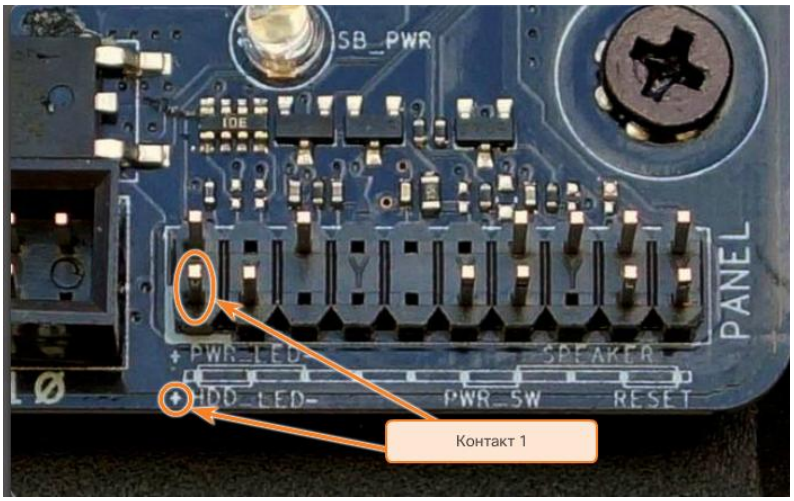


Рис. 5.15– Індикатор контакту 1 роз’єму системної панелі

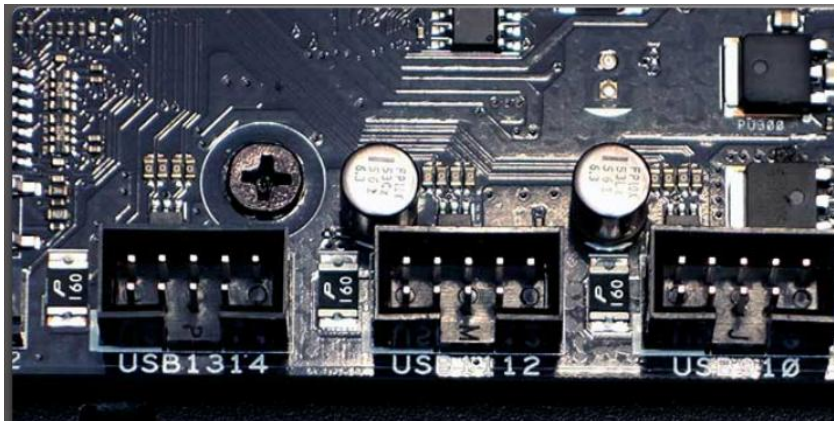
Роз’ємаудіо — на деяких корпусах є зовнішні аудіопорти й роз’єм для підключення мікрофонів, зовнішнього звукового обладнання, такого

як сигнальні процесори, мікшерні пульти й інструменти. Також можна придбати спеціальні аудіопанелі й підключити їх прямо до материнської плати. Ці панелі можна або встановлювати у відсіки для зовнішніх приводів, або робити їх автономними.

Порти USB — розташовані зовні більшості комп'ютерних корпусів. Роз’ємUSB на материнській платі найчастіше складаються з 9 або 10 контактів, об'єднаних у дваряди, як показано на рис. 5.16. Це об'єднання уможливлює два підключення USB, тому гніздоUSB часто єпарними. Іноді дваз'єднувача являють собою єдине ціле, як показано на рис. 5.17, і тоді їх можна підключити до цілого гніздаUSB материнської плати. Роз’ємUSB також можуть мати по чотири або п'ять контактів або окремі групи із чотирьох або п'яти контактів. Більшості обладнаньUSB потрібне підключення тільки чотирьох контактів. П'ятий контакт використовується для заземлення екрана деяких кабелів USB.

УВАГА! Переконаєтеся, що на рознімanні материнської плати є оцінка USB. Роз’єм Firewire дуже схожі на них. Не підключайте кабель USB до роз’єм Firewire, оскільки а якщо ні, то можна ушкодити материнську плату.

Нові корпуси й материнські плати мають підтримку стандарту USB 3.0 і навіть можуть підтримувати стандарт USB 3.1. Роз’єм USB 3.0 і USB 3.1 на материнській платі зовні схожі на роз’єм USB, але мають додаткові контакти.



5.16 – Роз’єми USB материнської плати



5.17 Внутрішній роз’єм материнської плати

У табл.5.8 представлені примітки відносно різних індикаторів на передній панелі.

Основний порядок підключення кабелів передньої панелі м представлений в табл.5.9.

У більшості випадків, якщо кнопка або індикатор не працює, причиною є неправильна орієнтація роз’єму. Щоб виправити це, виключите комп'ютер і відключитеживлення, відкрийте корпус і переверніть з'єд-

нувач для непрацюючої кнопки або індикатору. Щоб уникнути неправильного підключення деякі виробники поєднують кілька кабелів передньої панелі (наприклад, кабелі індикаторів живлення, кнопок включення й скидання) в одинроз'єм з «ключем».

Таблиця 5.8– Примітки відносно різних індикаторів на передній панелі

Індикаторів	Сигнали індикаторів
Системний-динамік	Служитьдлязвуковогооповіщенняпростанкомп'ютера. Якщоєпроблемазобладнанням, дляоповіщенняпротипцієїпроблемивидаєтьсяряддіагностичнихзвукових сигналів.
USB	Найчастішескладаютьсяз 9 або10контактів, об'єднанихудваряди, абомаютьокремігрупиізчотирьохабоп'ятиконтактів.
Кнопкаживлення	Служитьдлявключенняабовимиканнякомп'ютера.
Індикаториактивне	Світитьсяабомигає, коликомп'ютерробитьзчитуванняабозаписданих.
Індикаторживлення	Світиться, коликомп'ютервключений, імигає, коликомп'ютерперебуває в сплячомурежимі.
Кнопкаскидання	Служитьдляперезапускукомп'ютерабезвідключенняживлення.
Роз'єм аудіо	Служитьдляз'єднанняпортівроз'ємівдляпідключеннямікрофонівабозовнішньогообладнання – наприклад, сигнальнихпроцесорів, мікшерних пультівіінструментів.

Порада по установці. Роз'єм й кінцівки кабелів передньої панелі дуже маленькі. Сфотографуйте їх, щоб знайти контакт номер 1. Оскільки до моменту закінчення зборки комп'ютера простір у корпусі обмежене, скористайтеся екстрактором, щоб підключити кабелі до з'єднувачів.

Таблиця 5.9– Особливості підключення кабелів передньої панелі

Крок	Передняпанель	Особливостіпідключення
1.	**Кнопкаживлення**	• Сполучите роз'єм 1 двухпроводного кабелю кнопки живлення з відповідними контактами на материнській платі та підключите кабель живлення до роз'єму системної панелі в місці, позначеному PWR_SW.
2.	**Кнопкаскидання**	• Сполучите роз'єм 1 двухпроводного кабелю кнопки скидання з відповідними контактами на материнській платі та підключите кабель кнопки скидання до роз'єму системної панелі в місці, позначеному RESET..
3.	**Індикаторживлення**	• Сполучите роз'єм 1 кабелю індикатору живлення на передній панелі з відповідними контактами на материнській платі та підключите кабель ін-

Крок	Передняпанель	Особливостіпідключення
		дикатору живлення до роз’єму системної панелі в місці, позначеному PWR_LED..
4.	**Індикаторактивностінакопичувача**	• Сполучите роз’єм 1 кабелю індикатору активності накопичувача на передній панелі з відповідними контактами на материнській платі та підключите кабель індикатору активності жорсткого диска до роз’єму системної панелі в місці, позначеному HDD_LED..
5.	**Системнийдинамік**	• Сполучите роз’єм 1 кабелю системного динаміка з відповідними контактами на материнській платі та підключите кабель динаміка до роз’єму системної панелі в місці, позначеному SPEAKER..
6.	**USB**	• Сполучите роз’єм 1 кабелю USBз відповідними контактами на материнській платі та підключите кабель USB до роз’єму USB..
7.	**Звуковікабелі**	• Оскільки існує безліч спеціальних функцій і різного обладнання, звіряйтеся з документацією до материнської плати, корпусу й аудіопанелі. Там є всі необхідні вказівки. Підключите звуковий кабель до звукового роз’єму.

5.1.3.5 Зворотназборкакорпусу

Перш ніж установлювати на місце бічні панелі корпусу комп'ютера, переконаєтеся, що все компоненти належним чином вирівняні й закріплені. До них ставляться ЦП, ОЗП, плати адаптерів, кабелі даних, кабелі передньої панелі й кабелі живлення.

Після установки кришки переконаєтеся, що вона закріплена гвинтами у всіх передбачених місцях. У деяких корпусах використовуються гвинти, які вставляються за допомогою викрутки. В інших корпусах застосовуються гвинти з маховичками, які можна затягти вручну.

Якщо ви не певен, як саме слід знімати або заміняти корпус комп'ютера, звіритеся з документацією або відвідаєте веб-сайт виробника.

УВАГА! Звертайтеся з деталями корпусу акуратно. На деяких кожухах комп'ютерних корпусів зустрічаються гострі або зазубрені грані.

Порада по установці. Оглянетеобласті, де панелі стикаються з рамою корпусу. При необхідності заберіть кабелі усередину корпусу, щоб випадково не затиснути й не ушкодити їх рис. 5.18.

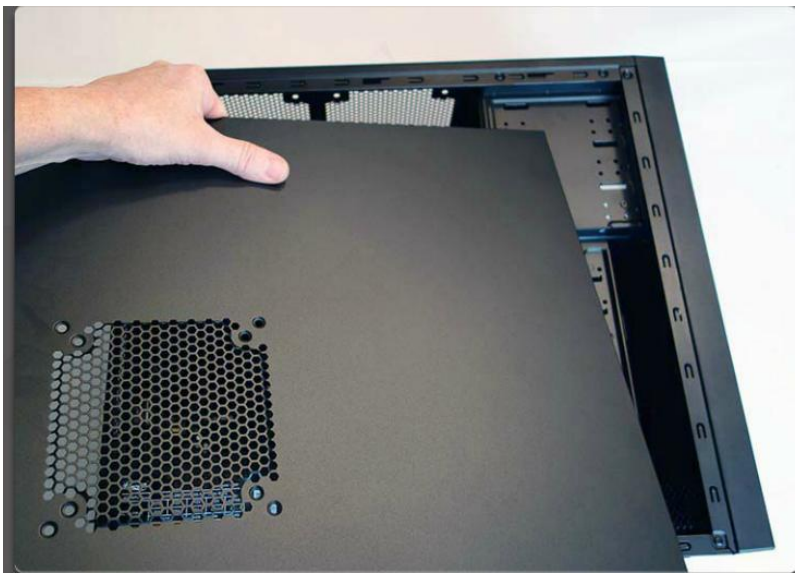


Рис. 5.18. – Зборка корпусу

5.1.3.6 Установка зовнішніх кабелів

Установивши на місце кришки корпусу, підключите кабелі до задньої сторони комп'ютера.

Примітка. Кабель живлення потрібно підключати після всіх інших кабелів.

Приєднуючи кабелі, стежите за їхньою відповідністю з'єднувачам на комп'ютері. Наприклад, у старих системах для кабелів миші й клавіатури використовуються однакові з'єднувачі PS/2, але щоб уникнути неправильного підключення, вони позначені різним квітами. Часто на з'єднувачі можна побачити зображення обладнання, для якого він призначений, наприклад символ клавіатури, миші, монітора або USB.

УВАГА! Ніколи не давите на з'єднувачі занадто сильно, коли підключаєте кабелі.

Для установки різних зовнішніх кабелів виконаєтезазначені нижче дії.

Крок 1. Підключите кабель монітора до відеопорту (див.рис. 5.19а)). Зафіксуйте кабель на з'єднувачі за допомогою гвинтів. Якщо в зібраному вами комп'ютері є відеоадаптер, підключите кабель монітора до відеопорту адаптера, а не до порту на материнській платі.

Крок 2. Підключите кабель клавіатури до відповідного до порту PS/2 (див.рис. 5.19б)).

Крок 3. Підключите кабель миші до відповідного до порту PS/2 (див.рис. 5.19в)).

Крок 5. Підключите кабель USB до з'єднувачіUSB (див.рис. 5.19г)).

Крок 5. Підключите кабель живлення до блоку живлення (див.рис. 5.19д)).

Примітка. На деяких материнських платах є тільки один порт PS/2. На деяких материнських платах можуть бути відсутні порти PS/2 для пі-

дключення клавіатури й миші. До таких материнських плат слід підключати USB-Клавіатури й USB-Миші.

Порада по установці. Для підключення застарілого периферійного обладнання до материнських плат, на яких відсутні з'єднувачі, можна використовувати перехідник PS/2–USB.



а) Підключення кабелю монітора



б) Підключення кабелю клавіатури



в) Підключення кабелю миші



г) Підключення кабелю USB



д) Підключення кабелю живлення

Рис 5.19 Установка зовнішніх кабелів

5.1.3.7 Завершення зборки комп'ютера

Крок 1: Установка бічних панелей
a. Установите бічні панелі в корпус комп'ютера.
b. Зафіксуйте їх за допомогою гвинтів для панелей.
Крок 2: Підключення монітора
a. Підключите кабель монітора до відеопорту.
b. Зафіксуйте кабель на з'єднувачі за допомогою гвинтів.
Крок 3: Підключення клавіатури
Підключите кабель клавіатури до порту USB або PS/2 для клавіатури.
Крок 4: Підключення миші
Підключите кабель миші до порту USB або PS/2 для миші.
Крок 5: Підключення кабелю Ethernet
Підключите кабель Ethernet до порту Ethernet.
Крок 6: Підключення антени безпроводової мережі
Підключите антену до роз’єм для антени безпроводової мережі.
Крок 7: Підключення кабелю живлення
Підключите кабель живлення до роз’єм на блоці живлення.
Крок 8: Перевірка підключень

5.1.4 Коди звукових сигналів і настройки BIOS

Під час завантаження (запуску) комп'ютера базова система введення-висновку (BIOS) виконує перевірку основних компонентів комп'ютера. Ця перевірка називається самотестуванням при включенніживлення (Power-On Self Test, POST).

Як показано на рис. 5.20, під час POST перевіряється, чи правильно працює обладнання комп'ютера. При виявленні неправильної роботи якого-небудь обладнання інженер довідається про проблему, одержуючи повідомлення про помилку або звуковий сигнал. Як правило, одиночний звуковий сигнал означає, що комп'ютер працює нормально. У випадку виявлення проблем з устаткуванням комп'ютер може вивести чистий екран при завантаженні й подати серію звукових сигналів. Кожний виробник BIOS використовує власні коди для позначення проблем з устаткуванням. В табл. 5.10наведені кодів звукових сигналів. Коди звукових сигналів для конкретного комп'ютера наведені в документації до материнської плати.

Проблема POST може виникнути до ініціалізації відеоадаптера. Під час пошуку й усунення неполадок комп'ютера в умовах, коли неможливо вивести зображення на екран, можна використовувати плату POST. Плата POST, яку іноді називають діагностичною платою, вставляється в слот на материнській платі, наприклад у слот PCI, PCIe або в порт USB.

При запуску комп'ютера на платі POST відображається серія із двох– або чотиризначнихшістнадцятирічних кодів. У випадкувиникнення проблем цей код можна використовувати для діагностики неполадки

за допомогою даних від виробника материнської плати, BIOS або плати POST.

Порада по установці. Щоб визначити, виконується чи POST належним чином, витягніть із комп'ютера всі модулі ОЗП й включите його. Комп'ютер повинен видати звуковий сигнал, що вказує на відсутність оперативної пам'яті. Цядія не нашкодить комп'ютеру.

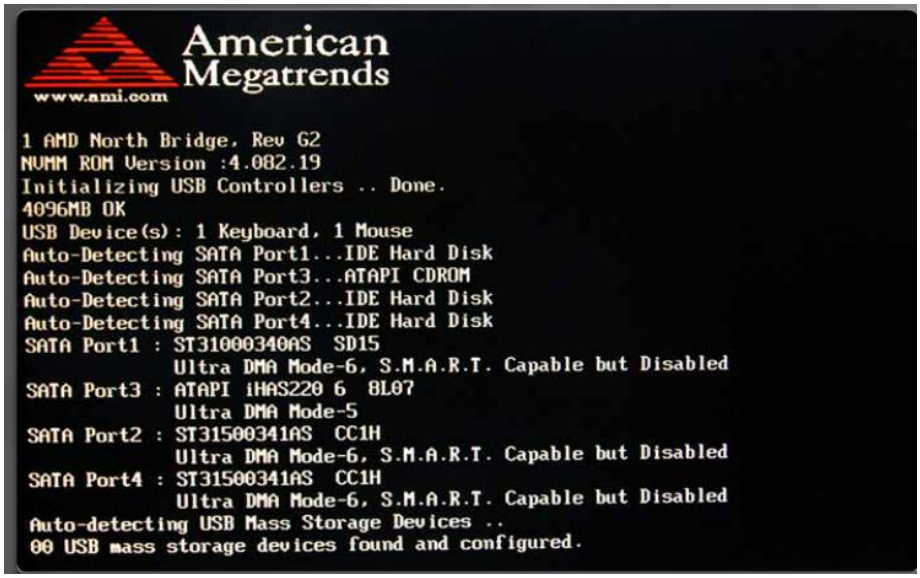


Рис. 5.20 – Процедура POST – перевірка основних компонентів комп'ютера

Таблиця 5.10 Загальні коди звукових сигналів

Код звукового сигналу	Значення	Причина
1 сигнал (немає відео)	Помилка відновлення пам'яті	Несправна пам'ять
2 сигнали	Помилка контролю по парності при звертанні до пам'яті	Несправна пам'ять
3 сигнали	Помилка пам'яті в перших 64 КБ	Несправна пам'ять
4 сигнали	Не працює таймер	Несправна материнська плата
5 сигналів	Помилка процесора	Несправний процесор
6 сигналів	Помилка A20 порту 8042	Несправні ЦП або материнська плата
7 сигналів	Виключення процесора	Несправний процесор
8 сигналів	Помилка відеопам'яті	Несправна відеокарта або пам'ять
9 сигналів	Помилка контрольних сум ПЗП	Несправний BIOS
10 сигналів	Помилка контрольних сум CMOS	Несправна материнська плата
11 сигналів	Несправна кеш-пам'ять	Несправні ЦП або материнська плата

5.1.4.1 BIOS і CMOS

Для роботи будь-якої материнської плати потрібна базова система введення-висновку (BIOS). BIOS являє собою мікросхему ПЗП на материнській платі, на якій перебуває невелика програма. Ця програма призначена для управліннявзаємодією операційної системи з устаткуванням комп'ютера.

Крім POST, BIOS також визначає:

доступні диски;

завантажувальні носії;

параметри настройки пам'яті й спосіб її використання;

параметри настройки слотів розширенняPCIe і PCI;

параметри настройки портів SATA і USB;

параметри управлінняживленням материнської плати.

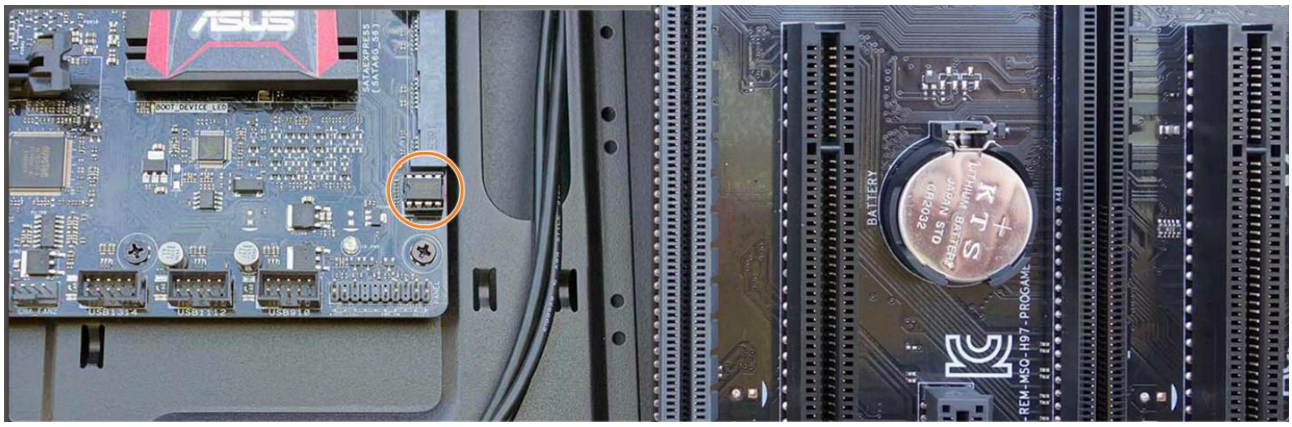
Настройка BIOS материнської плати зберігаються в мікросхемі, яка називається комплементарним метало-оксидним напівпровідником (CMOS). Вона аналогічна показаної на рис. 5.21 а).

Під час завантаження комп'ютера програма BIOS зчитує збережені в CMOS настройка, що визначають порядок настройкаобладнання.

Для живлення CMOS, у якій перебуваютьнастройка BIOS, використовується батарея, як показано на рис. 5.21 б). Якщо батарея розряджається, важливі настройка можуть бути загублені. Тому рекомендується завжди документувати настройка BIOS.

Примітка. Простий спосіб задокументувати настройка — сфотографувати різні екрани меню BIOS.

Порада по установці. Якщо дата й час на комп'ютерізазначені неправильно, це може вказувати на проблеми з батареєю CMOS.



а) **б)**

Рис. 5.21 – CMOS:

а) Мікросхема CMOS; б) Батарея CMOS

5.1.4.2 Програманастройки BIOS

Після заміни або установкидеякогообладнання, такого як модулі пам'яті, обладнаннязберіганняданих і плати адаптерів, може знадобитися змінити настройку BIOS, використовувані за замовчуванням. Для зміни відповідних параметрів необхідно скористатися програмою настройки BIOS.

Для входу в програму настройки BIOS необхідно натиснути відповідну клавішу або комбінацію клавіш під час процедури POST. Для різних материнських плат використовуються різні комбінації клавіш, однак у більшості комп'ютерів для входу в програму настройки BIOS потрібно натиснути клавішу DEL або функціональну клавішу. Наприклад, якщо встановлена материнська плата ASUS, для входу в програму настройки BIOS необхідно під час POST натиснути клавішу DEL або функціональну клавішу F2.

Примітка. Клавішу або комбінацію клавіш для конкретного комп'ютера можна знайти в документації до материнської плати.

Багато материнських плат під час виконання процедури POST виводять зображення, називане вікно-заставка. У вікні-заставці іноді вказується комбінація клавіш для входу в BIOS.

Хоча кожний виробник використовує свою власну програму настройки BIOS, усі програми мають схожі пункти меню, як ті, які показані на рис. 5.22.

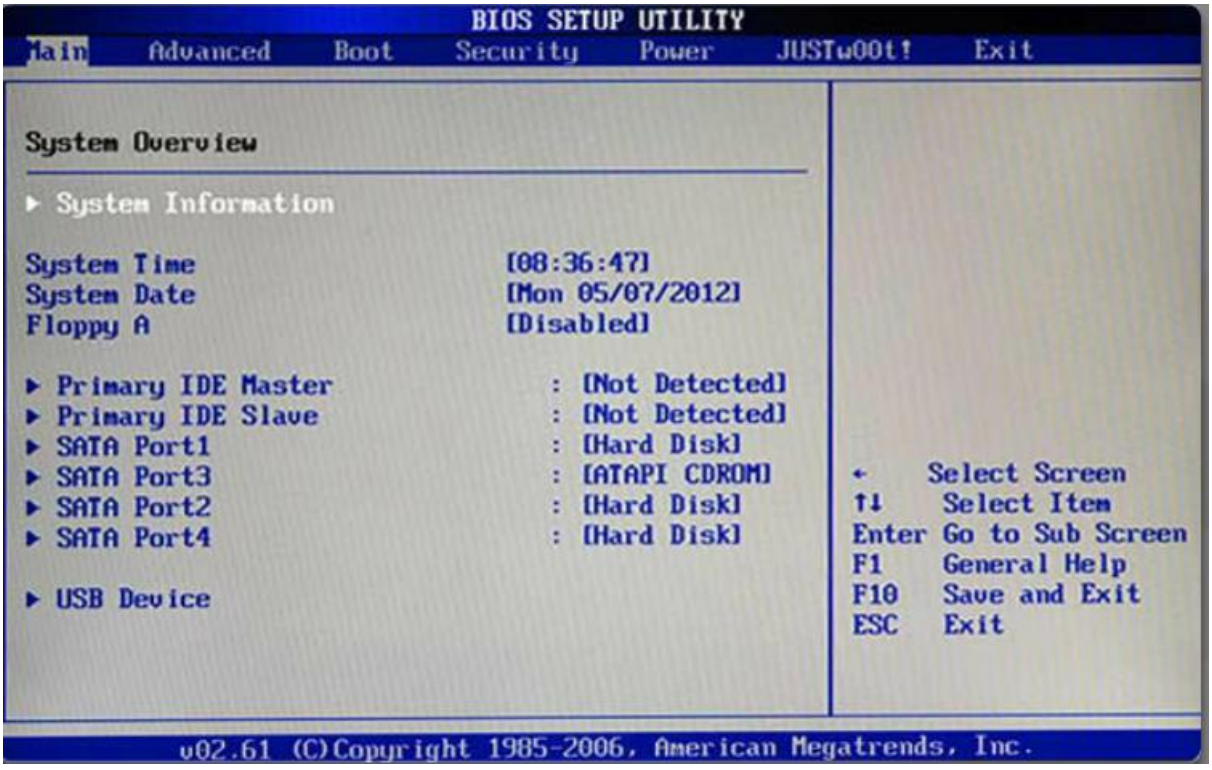


Рис. 5.22 – Сервісна програма настройки BIOS

Main — базове настройки системи

Advanced — додаткові параметри системи

Boot — варіанти завантажувальних пристроїв і порядок завантаження

Security — параметри безпеки

Power — додаткові параметри управлінняживленням

Justw00t! — додаткові параметри напруги й годин

Exit — варіанти виходу з BIOS і завантаження значень за замовчуванням

Примітка. Знімки екранів програми настройки BIOS у цьомурозділінаведені винятково для довідки. Зовнішній вигляд меню вашого екрана може відрізнятися від представленого тут. Додержуйтеся інструкцій на екрані й звернетеся до документації виробника до встановленої материнської плати.

5.1.4.3 Програма настройки UEFI

На деяких комп'ютерах використовується єдиний розширюваний мікропрограмний інтерфейс (Unified Extensible Firmware Interface, **UEFI**) рис. 5.23.

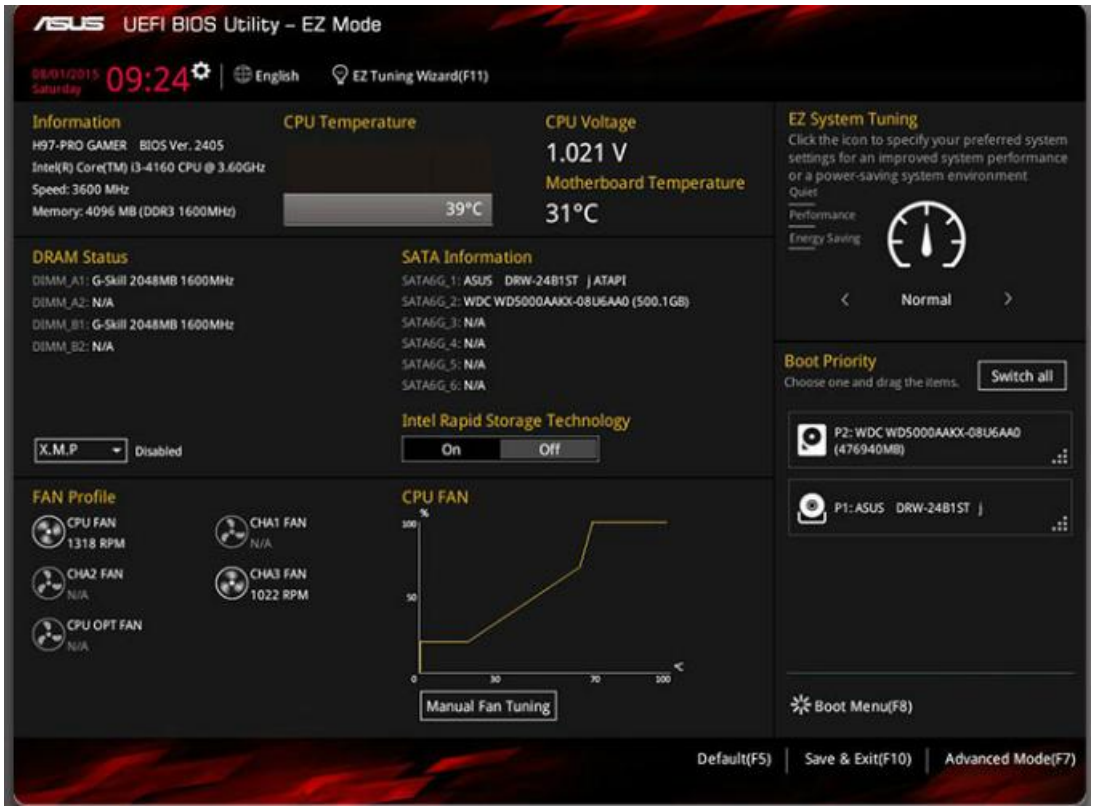


Рис. 5.23– Сервісна програма UEFI BIOS

UEFI служить для настройки тих же параметрів, що й традиційна програма настройки BIOS, однак у ній є додаткові параметри. Наприклад,

інтерфейс UEFI підтримує використання миші, на відміну від традиційного BIOS.

Примітка. Знімки екранів програми настройки UEFI у цьомурозділінаведені винятково для довідки. Зовнішній вигляд меню вашого UEFI може відрізнятися від представленого тут. Додержуйтеся інструкцій на екрані й звернетеся до документації виробника до встановленої материнської плати.

5.1.4.4 Інформація BIOS про компоненти

За допомогою інформації BIOS інженер може довідатися, які компоненти встановлені на даномукомп'ютері, а також деякі їхні характеристики рис. 5.24. Ця інформація може використовуватися при діагностиці неправильно працюючого обладнання й для визначення можливостей відновлення. Нижче приводитьсядеяка інформація про загальні компоненти, яку виводить BIOS.

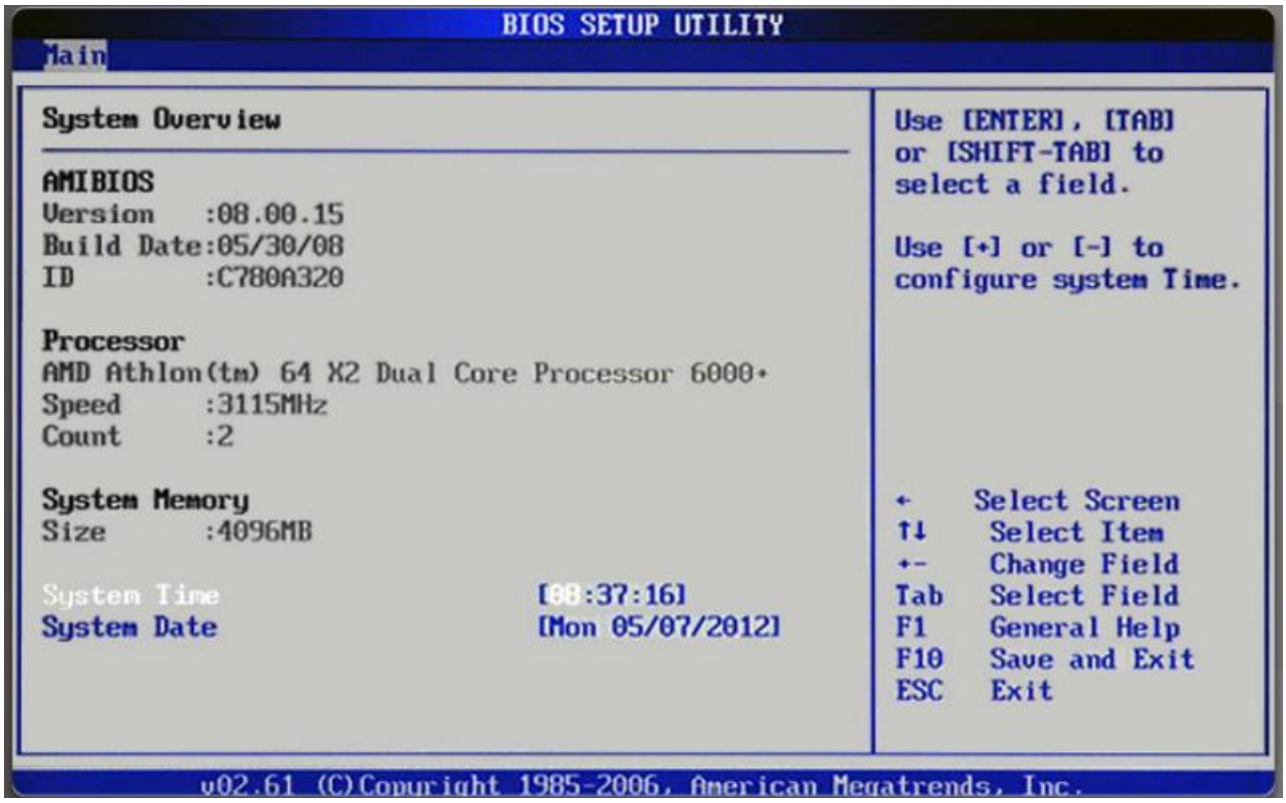


Рис. 5.24– Програма настройки BIOS

CPU — у цьомурозділі відображаються відомості про виробника ЦП і швидкості роботи процесора. Крім того, виводиться інформація про кількість установлених процесорів.

RAM — у цьомурозділі відображається інформація про виробника ОЗП й швидкості роботи оперативної пам'яті. Також може виводитися інформація про кількість роз’ємів і про те, у які роз’єм встановлені модулі ОЗП.

Hard Drive — у цьомурозділі представлена інформація про виробника, розмір і типі жорстких дисків. Також може виводитися інформація про тип і кількість контролерів жорстких дисків.

Optical Drive — тут відображається інформація про виробника й тип приводів оптичних дисків.

5.1.4.5 Параметриконфігурації BIOS

Ще одна функція програми настройки BIOS — вибір спеціальних параметрів устаткування комп'ютера для задоволення потреб окремого користувача. Функції, що допускають індивідуальну настройку, визначаються виробником і версією BIOS. Перш ніж вносити зміни в BIOS, необхідно чітко зрозуміти, як ці зміни можуть вплинути на комп'ютер. Неправильні настройки можуть зробити несприятливий ефект.

Основні параметри конфігурації BIOS включають наступні:

Дата й час — на головній сторінці BIOS є поля System Time (Системний час) і System Date (Системна дата) для настройки системних годин, як показано на рис. 5.25а).

Відключення обладнань — можна скористатися розширеними настройками BIOS і відключити обладнання, які не потрібні або які не використовуються, як показано на рис. 5.25 б).

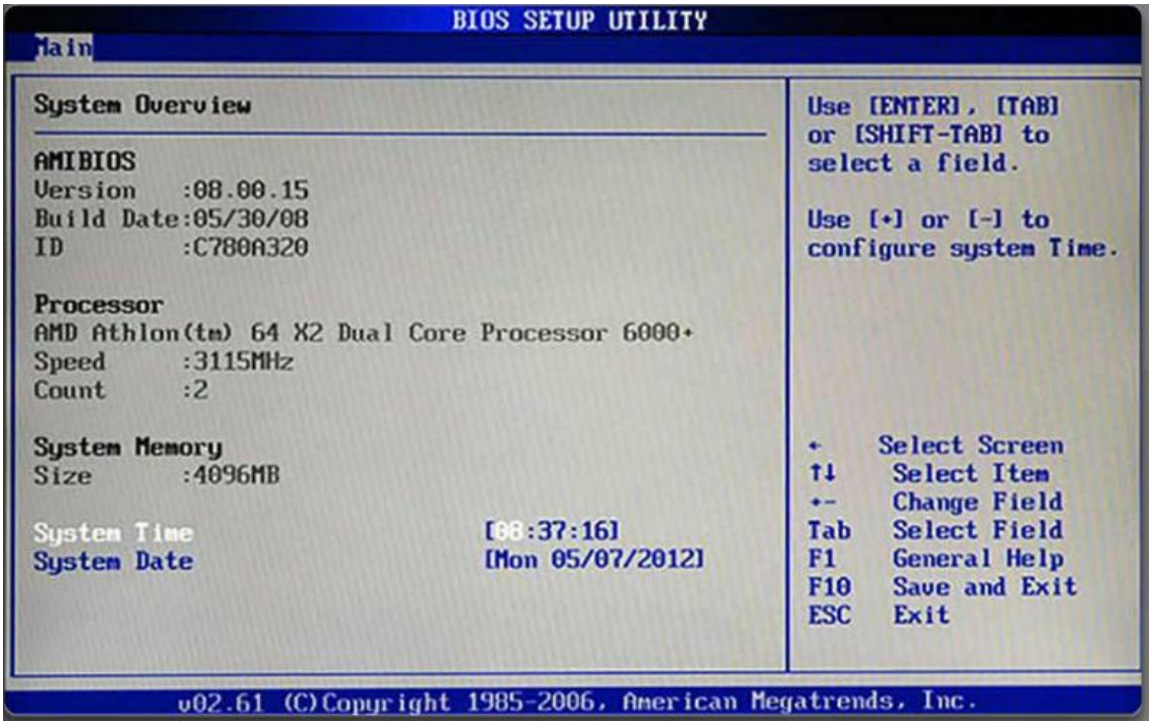
Порядок завантаження — після виконання процедури POST комп'ютер спробує завантажити операційну систему. BIOS шукає розділ, що завантажується, на першому в списку порядку завантаження обладнанні. Список порядку завантаження — це впорядкований список обладнань комп'ютера, з яких можна виконувати завантаження. Якщо це обладнання не має розділу, що завантажується, комп'ютер переходить до перевірки наступного обладнання зісписку. Коли обладнання з, що завантажується розділом знайдене, BIOS перевіряє його на наявність установленої операційної системи. Цей список звичайно перебуває в BIOS на вкладці Boot (Завантаження), як показано на рис. 5.25 в). Можна вказати порядок завантаження комп'ютера з жорстких дисків, привода оптичних дисків, завантаження по мережі, завантаження з носіївUSB і обладнаньфлеш-пам`ять.

Тактова частота ЦП — деякі програми настройки BIOS дозволяють змінювати тактову частоту ЦП, як показано на рис. 5.25 г). Зменшення тактової частоти ЦП приводить до того, що комп'ютер працює повільніше й робить менше тепла. Це називається вповільненням процесора. Це може зменшити шум від роботи вентиляторів і буває корисно, якщо потрібний меншгучний комп'ютер, наприклад для домашнього кінотеатру або спальні. При збільшенні тактової частоти ЦП комп'ютер починає працювати швидше, але робить більше тепла, що може зробити його більшгучним через більш високу швидкість обертання лопат вентилятора. Така настройка називається розгоном процесора.

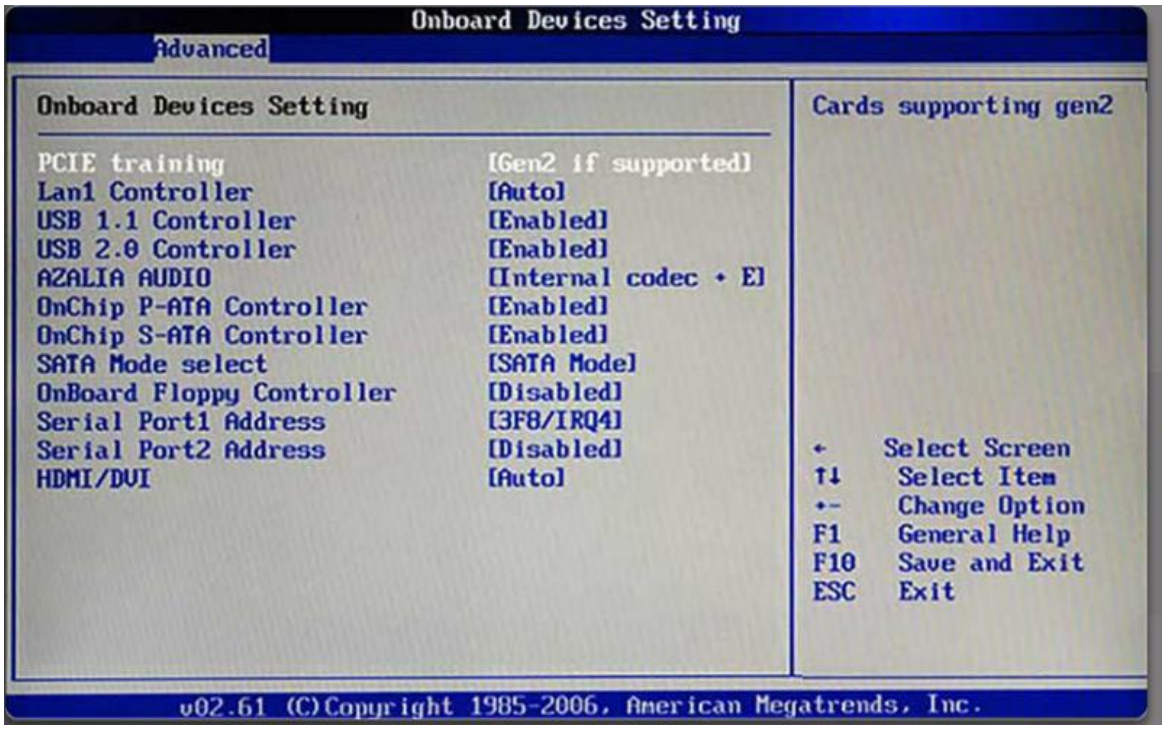
Віртуалізація — технологія віртуалізації уможливлює одночасну роботу декількох операційних систем у різних файлах або розділах. Вона

забезпечує імітацію характеристик комп'ютера в цілому, включаючи обладнання, BIOS, операційну систему й програми. Включите в BIOS функцію віртуалізації для комп'ютера, на якому буде використовуватися технологія віртуалізації, як показано на рис. 5.25 д).

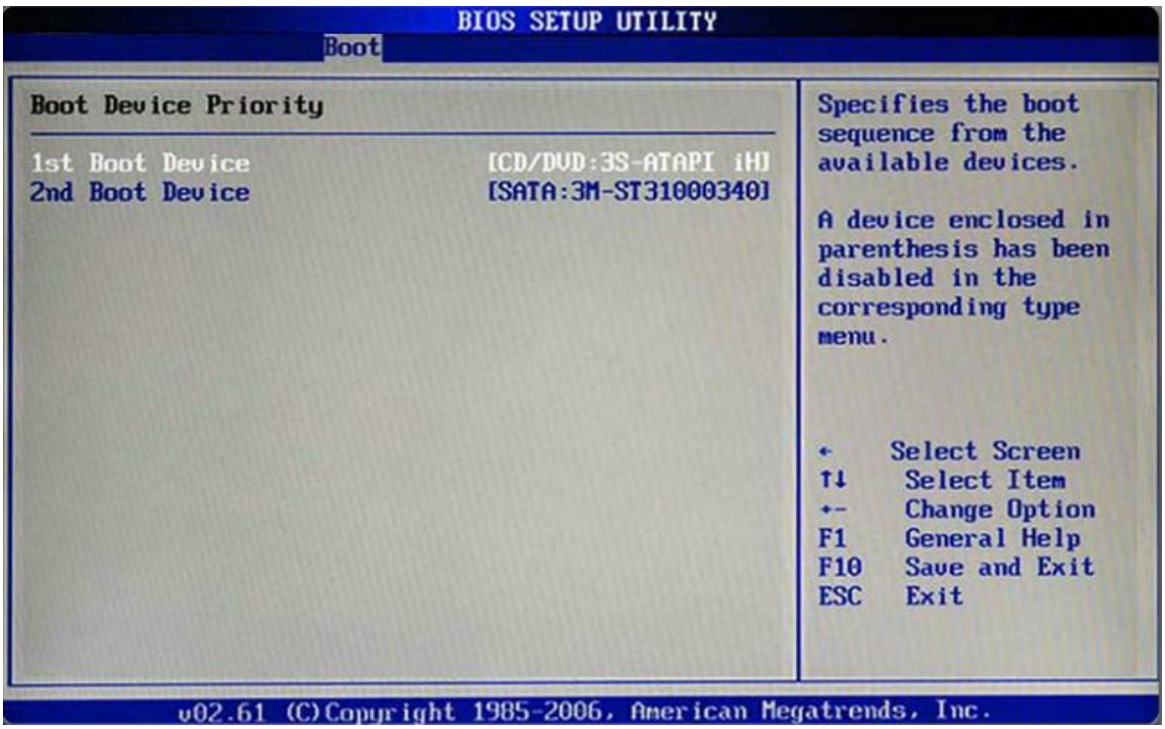
У табл.5.11 представлені рекомендації з настройки параметрів BIOS.



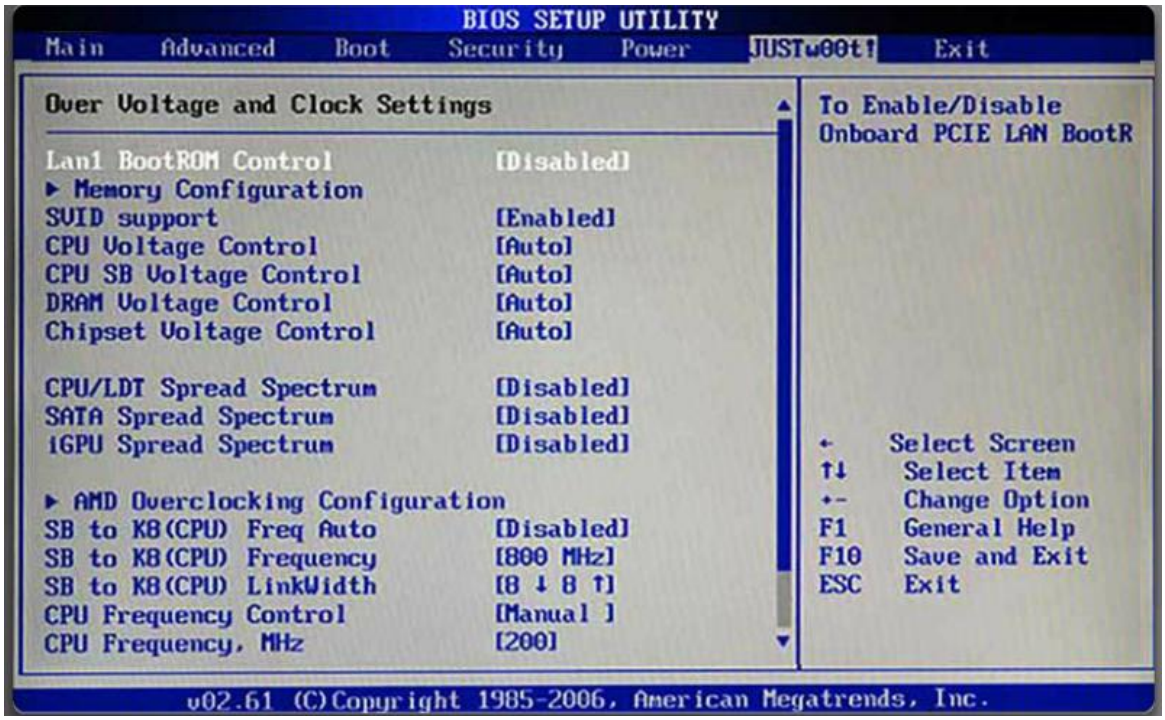
а) Системний час ідата BIOS



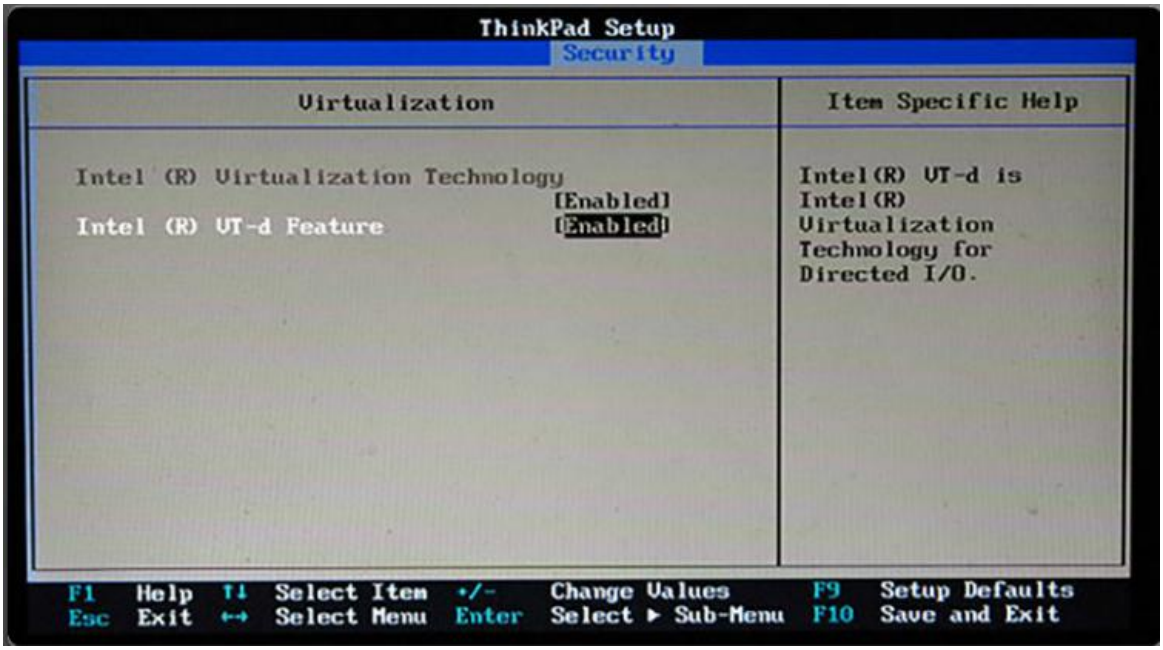
б) Параметри пристроїв BIOS



в) Порядок загрузкиBIOS



г)Тактова частота ЦПBIOS



д) Параметри віртуалізаціїBIOS

Рис.5.25 – Параметри конфігурації BIOS

Таблиця 5.11 – Настройка параметрів BIOS

Параметр BIOS	Особливості настроювання
Час і дата	• У цих полях завжди слід указувати правильні час і дату, оскільки на них орієнтується як операційна система, так і інші програми. • Неправильна установка дати й часу може привести до непередбачених проблем.
Відключення пристроїв	• При установці виділених відеоадаптера, звукової карти або мережевого адаптера слід відключити відповідний пристрій, вбудоване в материнську плату. • Якщо пристрій не працює, перевірте додаткові параметри BIOS, щоб довідатися, чи не відключений пристрій випадково.
Порядок завантаження	• Укажіть порядок завантаження відповідно до вимог користувача. • Вилучите зі списку порядку завантаження непотрібні пристрої.
Тактова частота	• Будь-які дії по розгону ЦП приводять до анулювання гарантії на нього. Розгін процесора може привести до скорочення його терміну служби або завдати шкоди ЦП. • Завжди слід установлювати систему охолодження, здатну без шкоди для ЦП справлятися з підвищенням температури, викликаним розгоном.
Віртуалізація	• Відключите цей параметр, якщо віртуалізація працює неправильно або цю технологію не планується використовувати.

5.1.4.6 Настройка безпеки BIOS

BIOS найчастіше підтримує безліч різних функцій безпеки для захисту настроювань BIOS і даних на жорсткомудиску, а також для того, щоб допомогти відновити комп'ютер у випадку крадіжки.

Нижче перераховані деякі найпоширеніші функції безпеки BIOS.

Паролі BIOS — як показано на рис. 5.26, паролі забезпечують різні рівні доступу до настроювань BIOS. Зверніть увагу, що можна змінити два параметри настройки паролів. Supervisor Password (Пароль адміністратора) — цей пароль надає доступ до всіх користувацьких паролів і всім екранам і настройкам BIOS. User Password (Пароль користувача) — дозволяє одержати доступ до настроювань BIOS на основі заданого рівня-дозволів. У табл.5.12 показані найпоширеніші рівнідозволів для користувачів. Перш ніж задавати пароль користувача, необхідно спочатку настроїти пароль адміністратора.

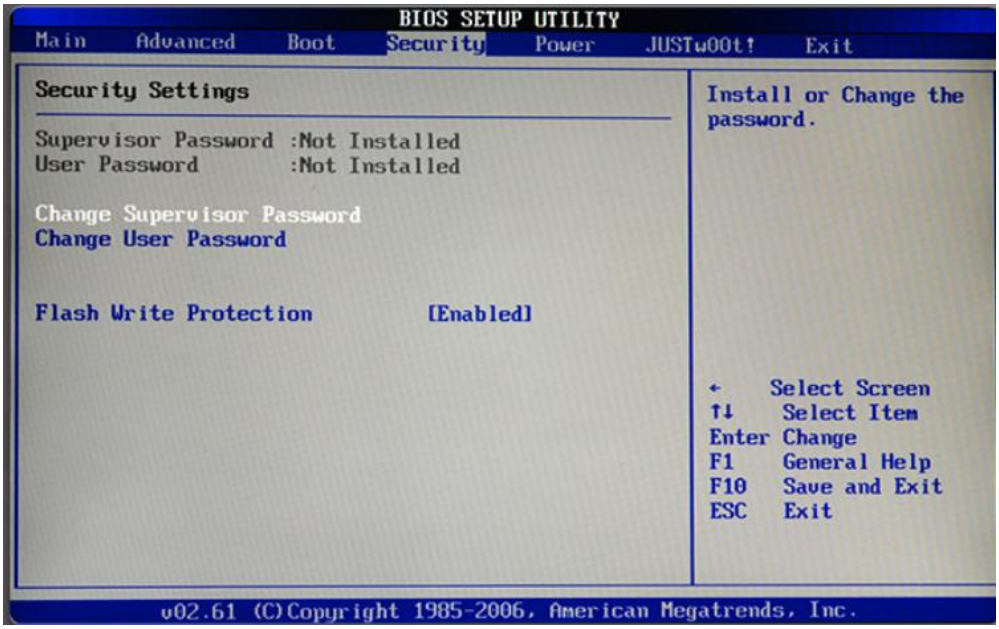


Рис. 5.26 – ПароліBIOS

Таблиця 5.12 – Рівні доступу

Рівеньдоступу	Описрівня
Full Access (Повний доступ)	• Доступнівсіекранийпараметри, крімпараметрапароляадміністратора.
LimitedAccess(Обмеженийдоступ)	• Надаєправоназмінутількидеякихпараметрів, наприкладчасуйдати.
LimitedAccess(Тількиперегляд)	• Доступнівсіекрани, алевідсутніправаназмінупараметрів.
No Access (Немає доступу)	• ДоступдопрограминастроюванняBIOSвідсутній.

Шифрування вмісту дисків — для запобігання крадіжки дані на жорсткомудиску можна зашифрувати. У результаті цієї операції дані на диску перетворяться в код. Без правильного пароля комп'ютер не вдасться завантажити, а дані, лічені з жорсткого диска, не вдасться розшифрувати. Навіть якщо встановити такий жорсткий диск в інший комп'ютер, дані залишаться зашифрованими.

Lojack — дана функція безпеки включає дві програми: модуль тривалого зберігання даних, який вбудований в BIOS, і агент додатка, установлюваний користувачем. Після установки в BIOS активується модуль тривалого зберігання даних. Відключити його не вдасться. Агент додатків періодично відправляє через Інтернет інформацію про обладнання і його місцезнаходженні в Центр моніторингу. Власник такого комп'ютера може виконувати дії, перераховані на рис. 5.27.

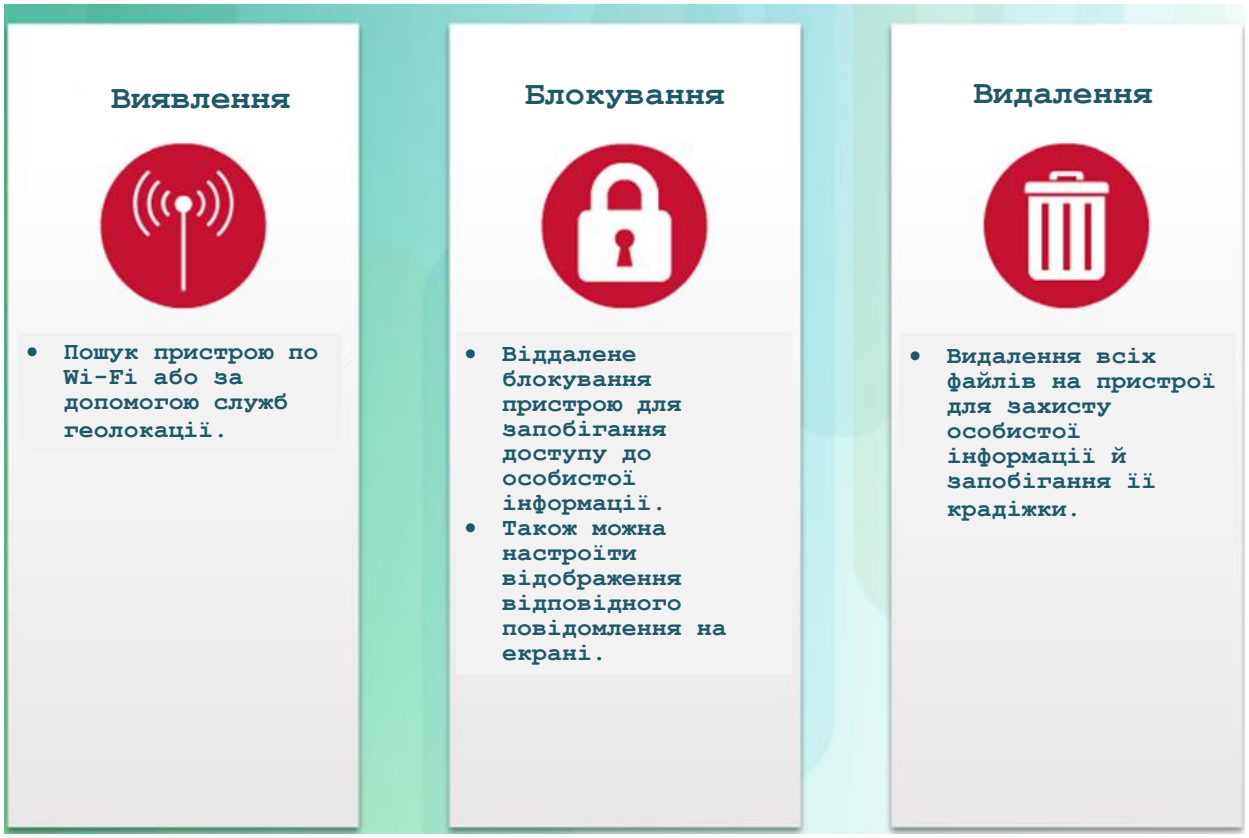


Рис. 5.27 – Функції LoJack

Довірений платформний модуль (TPM) — це мікросхема, призначена для захистуобладнання шляхом шифрування ключів, цифрових сертифікатів, паролів і даних. TPM використовується в ОС Windows для підтримки повного шифрування диска за допомогою Bitlocker.

Безпечне завантаження — це стандарт безпеки UEFI, що гарантує, що комп'ютер буде завантажувати тільки ті операційні системи, яким

довіряє виготовлювач материнської плати. Ця функція дозволяє запобігти завантаженню несанкціонованоїОС під час запуску комп'ютера.

5.1.4.7 Діагностика й моніторинг обладнання в BIOS

Функції BIOS для моніторингу обладнаннякорисні для збору інформації й відстеження активності материнської плати й підключеного до неї обладнання. Тип і кількість функцій моніторингу різниться залежно від моделі материнської плати. Використовуйте сторінку моніторингу обладнання для перегляду інформації про температуру, швидкість обертання вентиляторів, напрузі й про інших параметрах. Крім того, на цій сторінці може втримуватися інформація про обладнання для виявлення вторгнень.

Нижче перераховані деякі найпоширеніші функції BIOS для діагностики й моніторингу обладнання.

Температура — материнські плати оснащені тепловими датчиками для моніторингу термочутливогообладнання. Наприклад, тепловий датчик, розташований під роз'ємомЦП, дозволяє відслідковувати температуру процесора. При підвищенні температури ЦП BIOS може побільшати швидкість обертання вентилятора процесора, щоб остудити його, зменшити тактову частоту ЦП або навіть виключити комп'ютер, щоб запобігти ушкодженню процесора. Інші теплові датчики відслідковують температуру усередині корпусу або блоку живлення. Крім того, комп'ютер може бути оснащений тепловими датчиками для відстеження температури модулів ОЗП або чипсетів.

Швидкість обертання вентиляторів — у деяких BIOS можна набудовувати профілі й змінювати швидкість обертання вентиляторів для досягнення певногорезультату. У табл.5.13 представлені часто використовувані профілі настроювань швидкості обертання вентилятора ЦП.

Таблиця 5.13 – Профілі настройки швидкості обертання вентилятора

Профіль	Опис
Standard(Стандартний)	• Вентиляторавтоматичнопідбудовуєтьсяпідтемпературу ЦП, корпусу, блокуживленняабоіншогообладнання.
Turbo (Турборежим)	• Вентиляторпостійнопрацюєнамаксимальнійшвидкості.
Silent (Тихий)	• Вентиляторобертаєтьсязмінімальноюшвидкістю, щодозволяєзнизитирівеньшуму.
Manual (Ручна настройка)	• Користувачможесамостійнозмінюватипараметри, щоналежатьдоконтролюшвидкостіобертаннявентилятора.

Напруга — можна відслідковувати напруга на ЦП або регулятори напруги на материнській платі, як показано на рис. 5.28. Якщонапруга занадто висока або занадто низьке, компоненти комп'ютера можуть бути ушкоджені. Якщо напруга сильна відрізняється від номіналу, переко-

нається, що блок живлення справний. Якщо блок живлення не забезпечує правильні напруги, то справа може бути в ушкоджених регуляторах напруги на материнській платі. У цьомувипадку може знадобитися ремонт або заміна материнської плати.

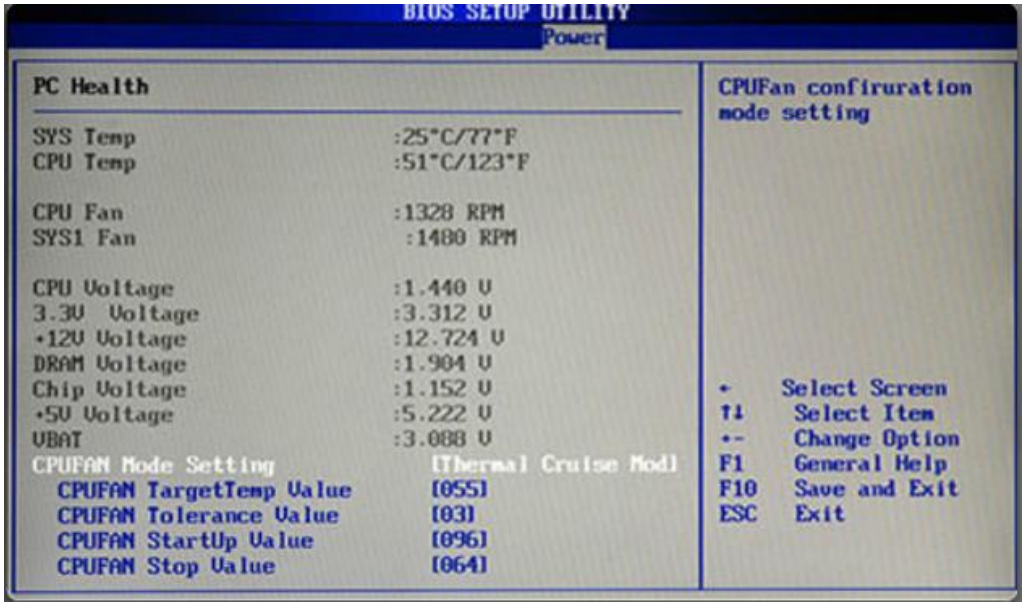


Рис. 5.28 – Напруги

Тактова частота ЦП і швидкість передачі даних по шині — деякі програми настройки BIOS дозволяють відслідковувати тактову частоту ЦП, як показано на рис. 5.29.

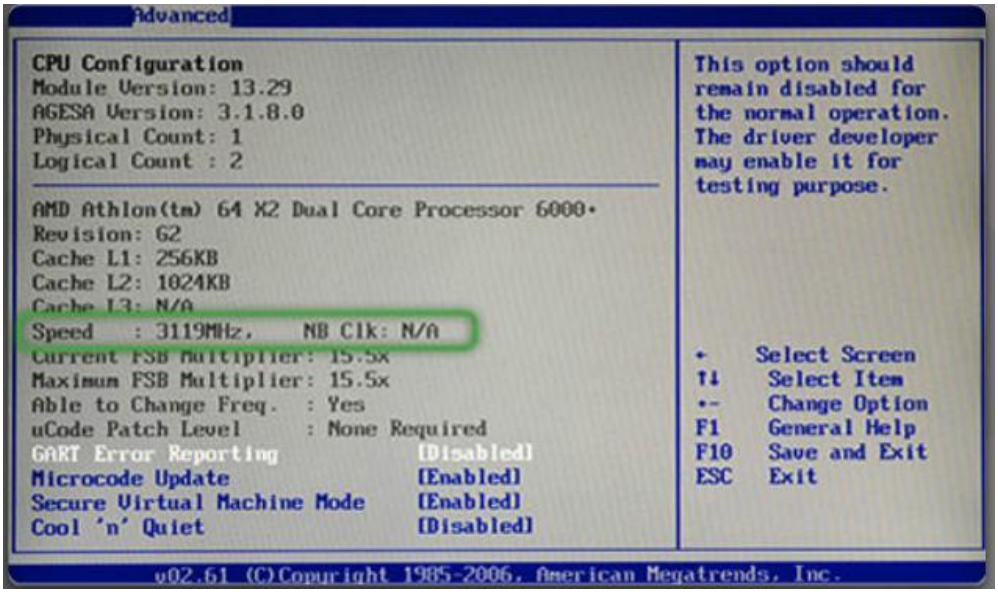


Рис. 5.29– Тактова частота і швидкість шини

У деяких BIOS також може бути можливість відслідковувати швидкість передачі даних по одній або декільком шинам. Може знадобитися відстежи-

ти один із цих параметрів, щоб визначити, чи правильні параметри ЦП були автоматично обрані BIOS або задані вручну замовником або збирачем комп'ютера. Неправильна настройка значення швидкості передачі даних може викликати підвищення температури ЦП і підключеного до нього обладнання або привести до неправильної роботи плат адаптерів і ОЗП.

Виявлення вторгнення — на деяких комп'ютерних корпусах є перемикач, який спрацьовує при відкриттікорпусу. Можна настроїти BIOS на запис тих моментів, коли перемикач активується, щоб власник знав про випадки несанкціонованого відкриття корпусу. Цей перемикач підключається до материнської плати.

Вбудовані функції діагностики — якщо замічена проблема з яким-небудь обладнанням, підключеним до комп'ютера, або базовою функцією, наприклад з вентилятором або контролем температури й напруги, можна скористатися вбудованими функціями діагностики, щоб визначити, у чому саме полягає ця проблема. Найчастіше програма надає опис проблеми або код помилки, які далі будуть використовуватися для її усунення. У таблиці 5.14 представлені часто використовувані засоби діагностики. Багато вбудованих програм діагностики створюють журнал, у якому фіксуються записи про всі виявлені проблеми.

Таблиця 5.14 – Вбудована діагностика

Діагностична перевірка	**Опис**
Starttest(Перевіркапризапуску)	• Перевірка основних компонентів на правильність їх роботи. • Використовуйте цю перевірку, якщо комп'ютер не завантажується належним чином.
Harddrivetest(Перевіркажорсткогодиска)	• Перевірка жорсткого диска на наявність ушкоджених секторів. • Якщо виявляється ушкоджена область, програма намагається знайти дані й перенести їх в інше місце, а також позначає ушкоджену область, щоб вона не використовувалася в майбутньому. • Використовуйте цю перевірку, якщо є підозра, що жорсткий диск працює неправильно, якщо комп'ютер не завантажується або якщо жорсткий диск робить незвичайний шум.
Memorytest(Перевіркапам'яті)	• Перевірка модулів пам'яті на правильність їх роботи. • Використовуйте цю перевірку, якщо комп'ютер працює з помилками або не завантажується. • Якщо ця перевірка видає повідомлення про помилки, негайно замініте пам'ять.
Batterytest(Перевіркаакумулятора)	• Перевірка правильності роботи акумулятора. • Використовуйте цю перевірку, якщо акумулятор працює неправильно, не тримає заряд або видає неправильні повідомлення про рівень заряду.

Цю інформацію можна використовувати для вирішення проблем і розшифрування кодів помилок. Якщо обладнанняперебуває на гарантії, цю інформацію можна використовувати, щоб розповісти про проблему службі підтримки.

5.1.4.8 Режим EZ в UEFI

На нових комп'ютерах BIOS замінена інтерфейсом UEFI. Незважаючи на те що екрани UEFI для кожної материнської плати різні, у всіх цих інтерфейсах представлені ті самі функції.

На рис. 5.30 показаний знімок екрана сервісної програми ASUS UEFI BIOS Utility, запущеної в режимі EZ. При вході в інтерфейс UEFI за замовчуванням відображається екран EZ Mode (Режим EZ). На цьомуекрані представлена основна інформація про систему, відомості про температуру ЦП і материнської плати, вихідній напрузі ЦП, швидкостях обертання вентиляторів, інформація про пам'ять і інтерфейс SATA.

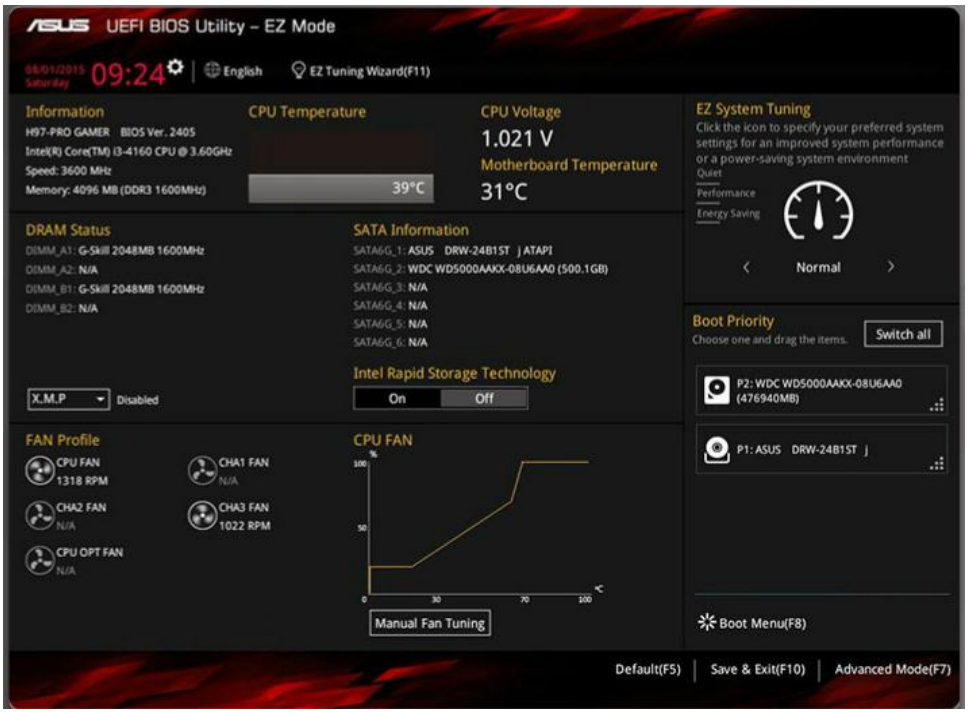


Рис. 5.30 – Сервісна програма ASUS UEFI BIOS Utility – режим EZ

На сторінці EZ Mode (Режим EZ) можна виконувати зазначені нижче дії:

Змінювати дату й час.

Вибирати мова інтерфейсу програми.

Використовувати майстер настройки EZ Tuning Wizard для автоматизації процесу створення сховища на основі дисків RAID, а також для розгону системи.

Використовувати інструменти EZ System Tuning для настройки режиму продуктивності системи.

Включати або відключати SATA RAID.

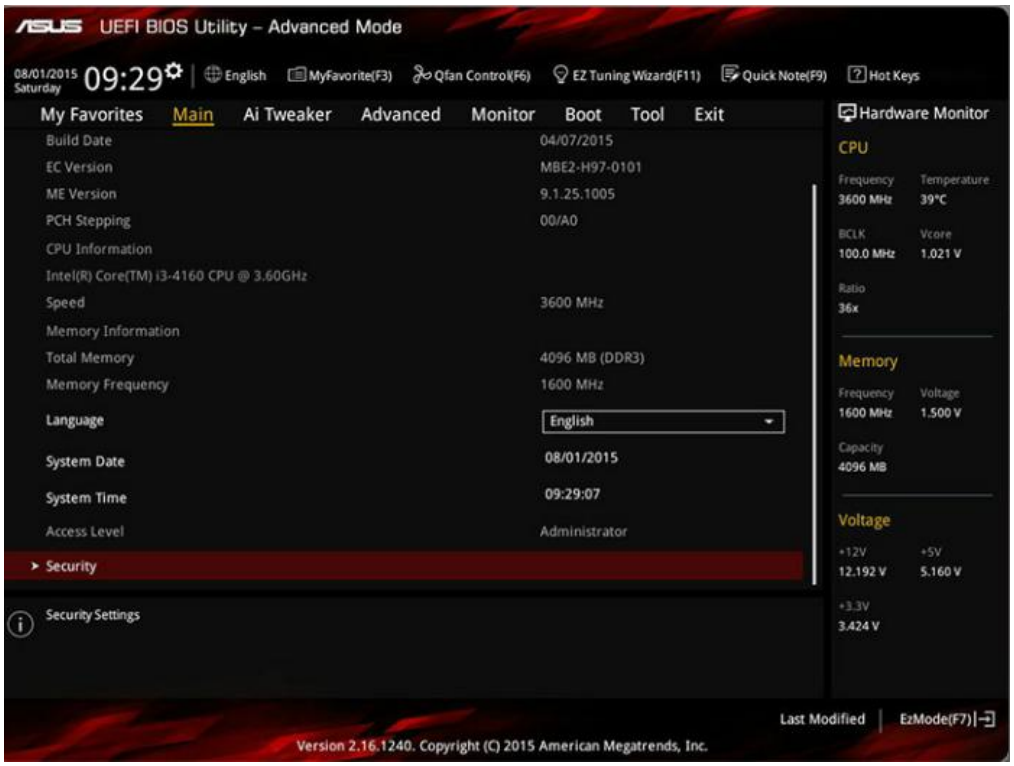
Вибирати пріоритет завантажувальних пристроїв.

Крім того, є розширений режим, у якому можна настроїти додаткові параметри й управляти їхніми значеннями. Для перемикання між режимами використовується клавіша F7.

5.1.4.9 Розширений режим в UEFI

При вході в режим Advanced Mode (Розширений режим) з'являється екран Main для настройки материнської плати ASUS. Як показано на рис. 5.31 а), цей режим служить для розширеноїнастройки параметрів UEFI.

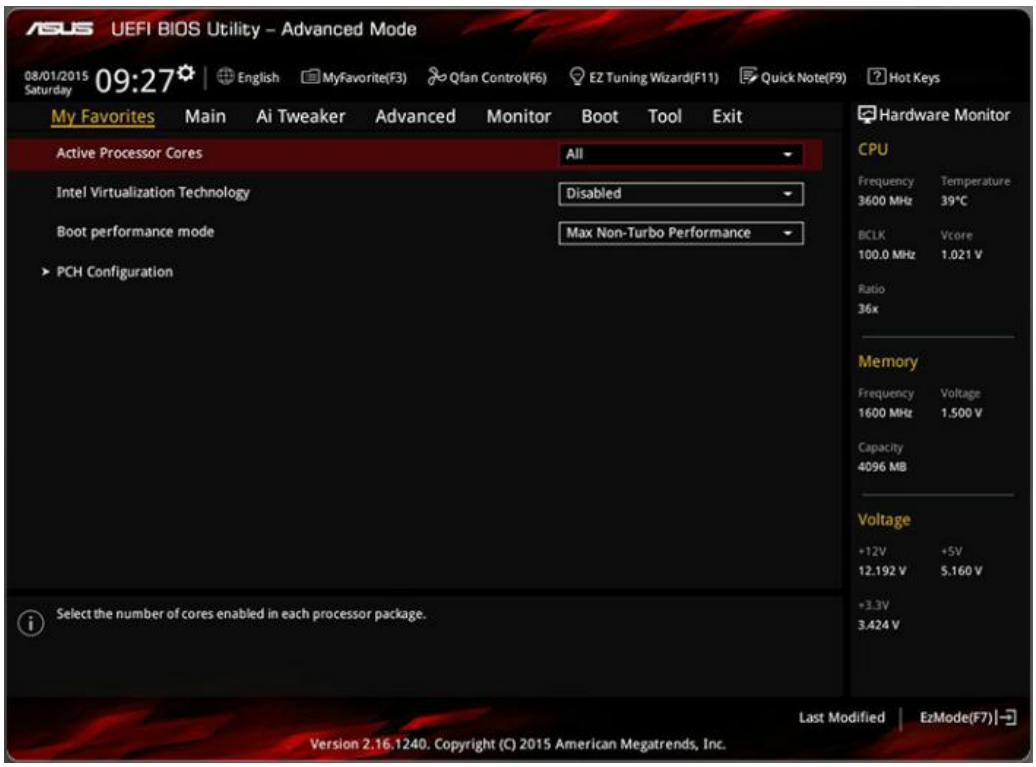
Примітка. Для повернення в режим EZ натисніть клавішу F7.



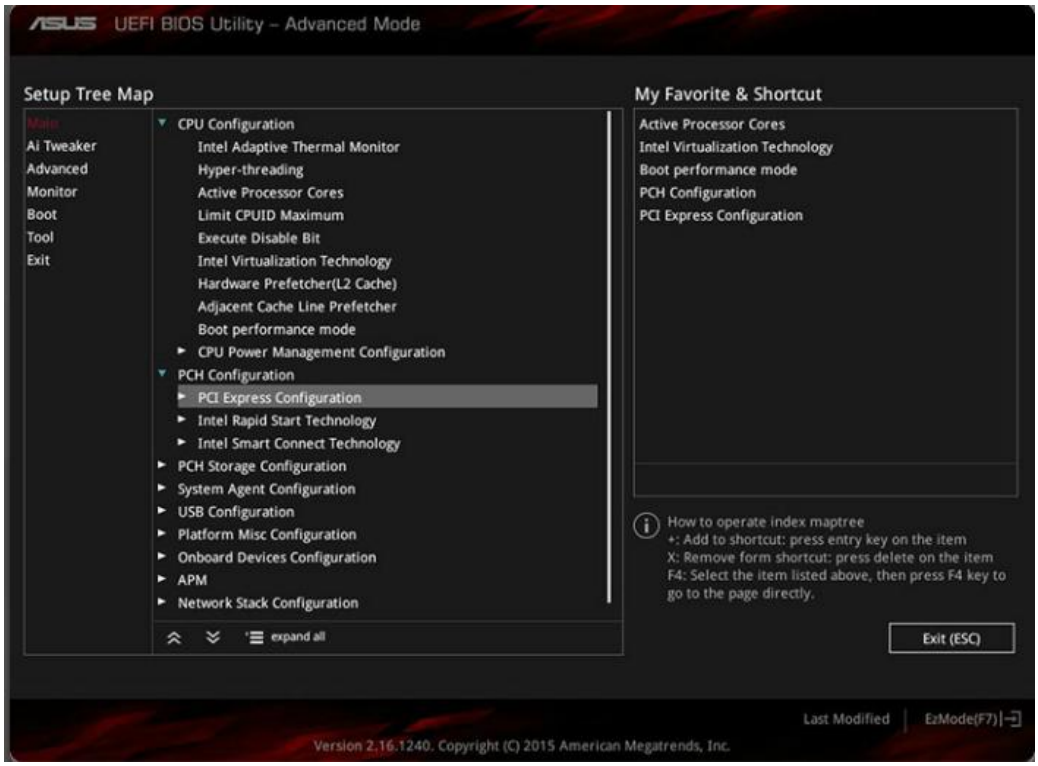
а) Розширений режим настройки ASUS UEFI

У верхній частині меню відображаються наступні розділи:

My Favorites — (див.5.31 б)) використовується для швидкого доступу до часто використовуваних параметрів. Щоб перейти до екрана Setup Tree Map, показаному на рис. 5. 31 в), натисніть клавішу **F3** або клацніть елемент **My Favorites (F3)**.



б)Розширений режим – екран My Favorites



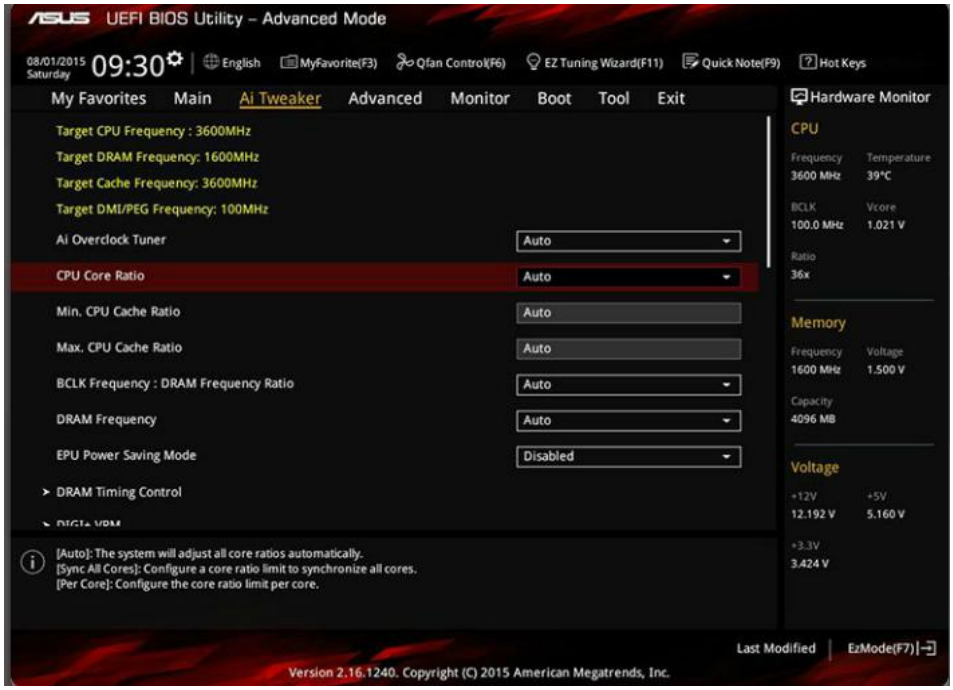
в) Настройка обраного– екран Setup Tree Map

Main — (див.5.31 г)) служить для відображення відомості про комп'ютер і зміни базової конфігурації. Тут можна задати дату, час, язик і параметри безпеки.



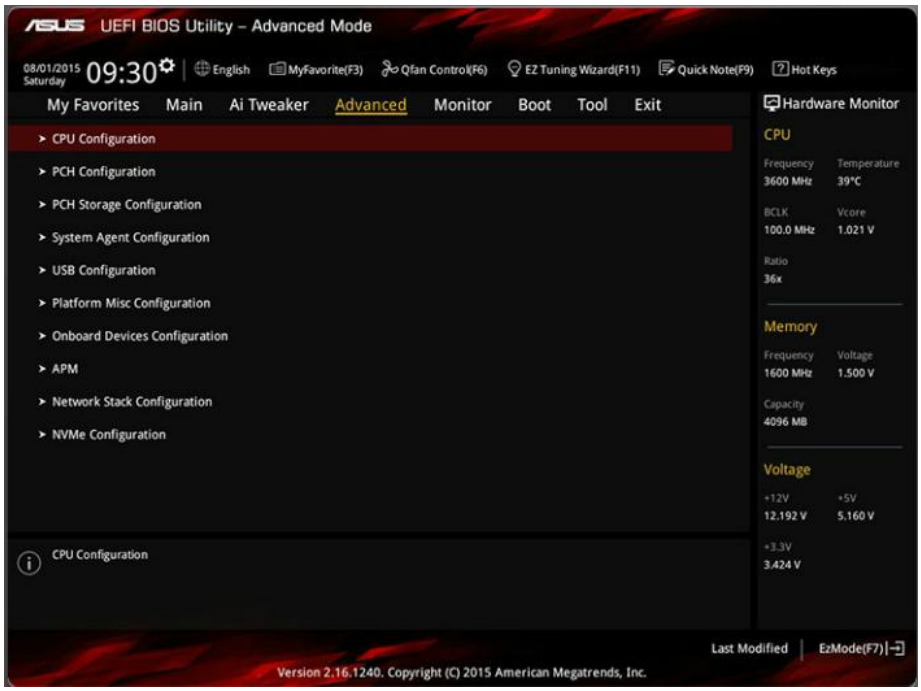
г)Розширений режим – екран Main

Ai Tweaker — (див.5.31 д)) використовується для зміни параметрів розгону ЦП і оперативної пам'яті. При зміні значень параметрів у цьому розділі завжди слід проявляти обережність. Неправильна настройка цих параметрів може привести до несправностей у роботі системи.



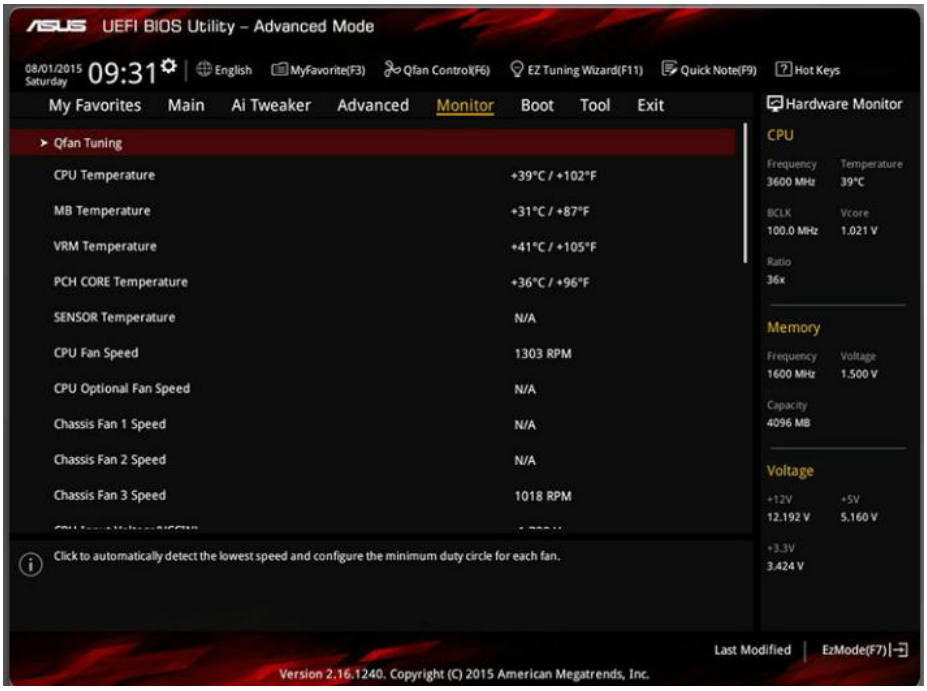
Розширений режим – екран Ai Tweaker

Advanced — (див.5.31 е)) служить для настройки параметрів ЦП і інших обладнань. При зміні значень параметрів у цьомурозділі завжди слід проявляти обережність. Неправильна настройка цих параметрів може привести до несправностей у роботі системи.



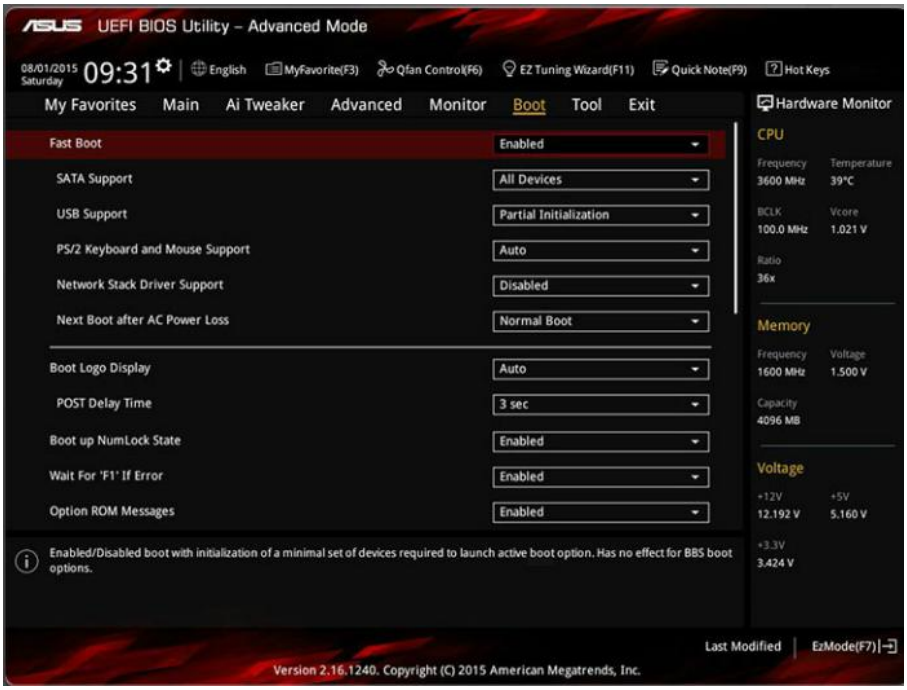
е) Розширений режим – екран Advanced

Monitor — (див.5.31 ж)) у цьомурозділі представлені відомості про температуру, станживлення й роботі вентиляторів. Також тут можна змінити швидкість обертання вентиляторів.



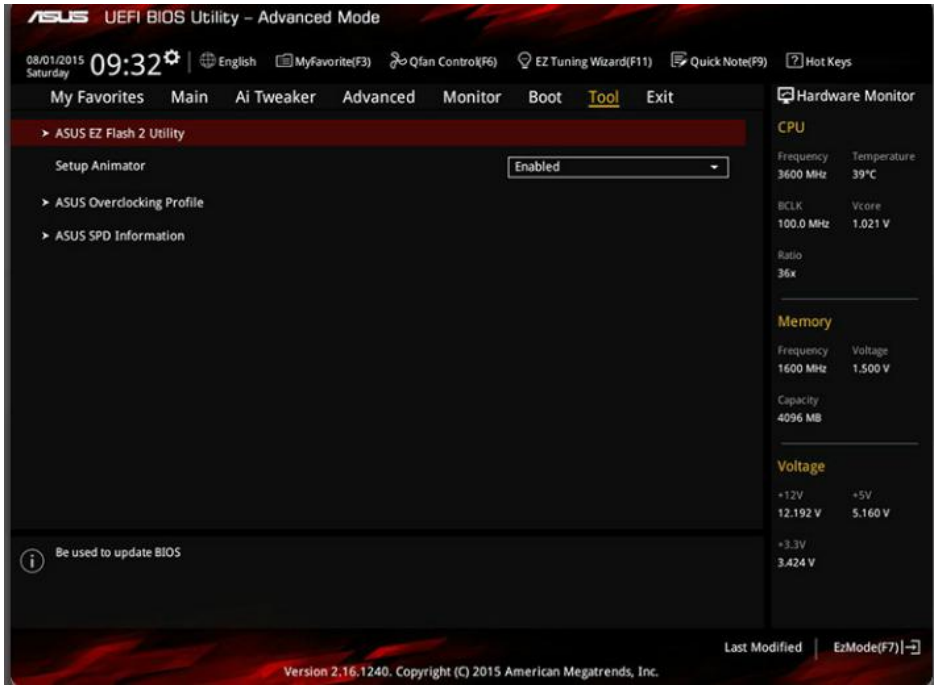
ж)Розширений режим – Monitor

Boot — (див.5.31 з)) служить для виміру варіантів завантаження комп'ютера.



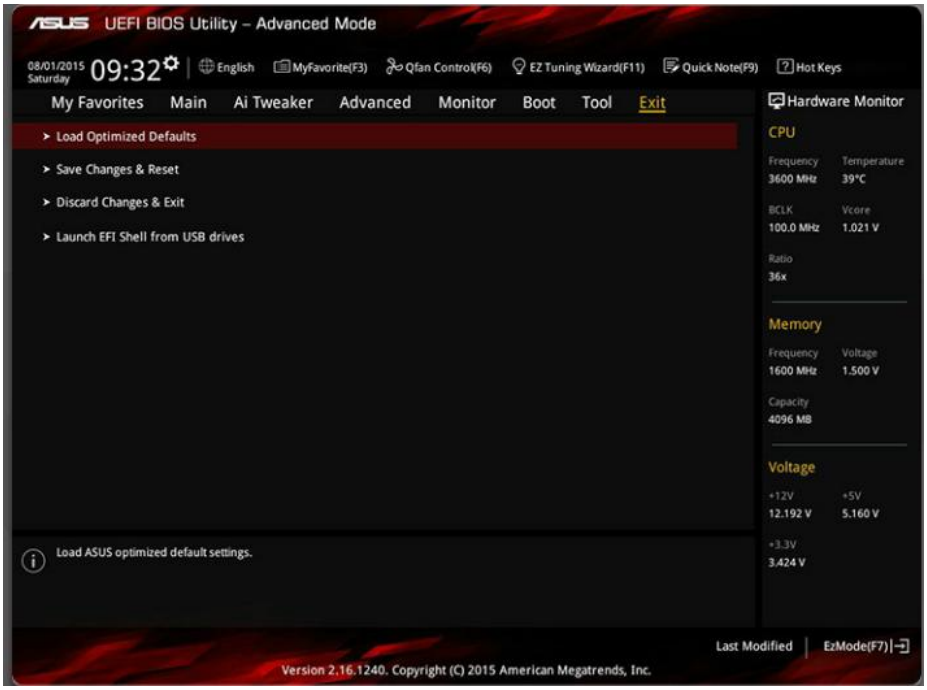
з)Розширений режим – Boot

Tool — (див.5.31 і)) служить для настройки параметрів спеціальних функцій.



і) Розширений режим – Tool

Exit — (див.5.31 к)) служить для вибору параметрів виходу з інтерфейсу й завантаження параметрів за замовчуванням.



к)Розширений режим – екран Exit

Рис. 5.31 – Режими UEFI BIOS Utility ПК ASUS

Підсумкові відомості про сервісні програми ПК наведені у табл. 5.15.

Таблиця 5.15 – Сервісні програми ПК

Термін	Опис
CMOS	Служить для зберігання настроювань BIOS.
UEFI	Підтримує використання миші замість традиційних екранів BIOS.
BIOS	Проста програма, яка зчитує збережені в CMOS настроювання, щовизначають порядок настроювання встаткування.
Lojack	Функція безпеки, що дозволяє одержативідомості про пристрій і його місці розташування.
POST	Апаратна перевірка основних компонентів комп'ютера.
TPM	Мікросхема, призначена для захистуобладнання шляхом шифрування ключів цифрових сертифікатів, паролів і даних.

5.1.5Модернізація ПК

5.1.5.1 Модернізація компонентів материнської плати

Комп'ютери потребують періодичної модернізації в силу різних причин:

Міняються вимоги користувачів.

Для роботи оновленого ПО потрібне нове обладнання.

Нове обладнання забезпечує більшу продуктивність.

Зміни в комп'ютері можуть привести до необхідності модернізації або заміни деяких компонентів або периферійних пристроїв. Оцініте ефективність і вартість модернізації й заміни.

При модернізації або заміні материнської плати, можливо, прийдеться замінити інші компоненти, включаючи ЦП, блок радіатора й вентилятора й ОЗП рис. 5.32. Нова материнська плата повинна підходити до старого корпусу комп'ютера. Крім того, наявний блок живлення повинен повною мірою задовольняти вимогам нової материнської плати в електроживленні.



Рис.5.32 Модернізація компонентів материнської плати

Модернізацію материнської плати слід починати з переносуЦП, блоку радіатора й вентилятора на нову материнську плату. Із цими компонентами набагато легше працювати, коли вони перебувають поза корпусом. Працюйте на антистатичномукилимку й надягайте антистатичні рукавички або антистатичний браслет, щоб уникнути ушкодженняЦП. Якщо для нової материнської плати потрібно інші ЦП і ОЗП, установите їх на цьомуетапі. ОчиститеЦП і радіатор від староїтермопасти. Не забудьте нанести свіжий шартермопасти між ЦП і радіатором.

На багатьох застарілих материнських платах були перемички, змінивши положення яких можна було настроювати параметри різних компонентів плати. Однак на сучасних материнських платах перемички зу-

стрічаються досить рідко. Удосконалена електроніка дозволяє настроювати відповідні параметри із програми настроювання BIOS або за допомогою інтерфейсу UEFI.

Термін служби батареї CMOS становить кілька років. Однак якщо на комп'ютері не підтримуються правильні час і дата або втрачаються параметри настройки між вимиканнями, швидше за все, батарея вирядженa й вимагає заміни. Переконаєтеся, що нова батарея відповідає моделі, необхідної для материнської плати.

Для установки батареї CMOS виконаєте наступні дії:

Крок 1. Акуратно зруште убік або піднімите тонкі металеві затискачі, щоб зняти стару батарею.

Крок 2. Правильно розташуйтепозитивний і негативний полюси батареї.

5.1.5.2 Модернізація материнської плати

Перш ніж приступитися до модернізації, вивчите необхідні відомості про підключення компонентів до відповідних до роз’ємів на новій материнській платі. Завжди записуйте в журнал усі дії по настроюванню поточного комп'ютера. Щоб швидко запам'ятати розташування компонентів і спосіб їх підключення до материнської плати, їх можна сфотографувати за допомогою камери мобільного телефону. Ці знімки можуть виявитися надзвичайно корисними при повторномускладанні компонентів системи рис.5.33.



Рис.5.33 – Модернізація материнської плати

Нижче представлений порядок модернізації материнської плати в корпусі комп'ютера.

Крок 1. Запишіть відомості про те, як блок живлення, вентилятори в корпусі й кабелі від кнопок у корпусі підключені до старої материнської плати.

Крок 2. Від'єднаєте кабелі від старої материнської плати.

Крок 3. Від'єднаєте плати розширення від корпусу. Витягніть плати розширення й помістите кожну плату в антистатичний пакет або на антистатичний килимок.

Крок 5. Ретельно запишіть, як стара материнська плата кріпиться до корпусу. Деякі монтажні гвинти потрібні для підтримки деталей, а деякі забезпечують важливе заземлююче з'єднання материнської плати й корпусу. Звернете особливу увагу на неметалічні гвинти й стойки, тому що вони можуть виступати в ролі ізоляторів. Заміна ізоляційних гвинтів і опор на металеве обладнання, що проводить електрику, може викликатиушкодження електричних компонентів.

Крок 5. Витягніть стару материнську плату з корпусу.

Крок 6. Оглянете нову материнську плату й визначите на ній роз’єм для підключення живлення, кабелів SATA, вентиляторів, портів USB, аудіоз'єднувачів, з'єднувачів передньої панелі й іншого обладнання.

Крок 7. Оглянете рамку для інтерфейсів уведення-висновку, яка перебуває в задній частині корпусу. Замініте стару рамку нової, яка йде в комплекті з новою материнською платою.

Крок 8. Вставте материнську плату в корпус і зафіксуйте її. Звернетеся до посібника користувача материнської плати й корпусу, щоб ознайомитися з відповідними інструкціями. Використовуйте гвинти підходящого типу. Не заміняйте гвинти з різьбленням на саморізьблені металеві гвинти, тому що вони ушкодять отвори для гвинтів з різьбленням і можуть бути ненадійні. Переконаєтеся, що гвинти з різьбленням мають правильну довжину й крок різьблення. Якщо різьблення правильне, вони будуть легко вставлятися. Якщо доводиться додавати зусилля, щоб вставити гвинт, можна ушкодити отвір з різьбленням. Крім того, такий гвинт не зможе надійно фіксувати материнську плату. Також при використанні неправильних гвинтів може утворюватися металева стружка, що може привести до короткого замикання.

Крок 9. Потім підключите блок живлення, вентилятори в корпусі, світлодіодні індикатори, передню панель і інші необхідні кабелі. Якщо роз’ємживленняATX мають інший розмір (у них може бути різна кількість контактів), може знадобитися адаптер. Схема цих підключень є в документації до материнської плати.

Крок 10. Установивши нову материнську плату й підключивши кабелі, установите й закріпите всі плати розширення.

Тепер потрібно перевірити виконану роботу. Переконаєтеся, що всі деталі підключені й немає непідключених проводів. Підключите клавіатуру, мишу, монітор і живлення. Якщо буде виявлена проблема, негайно відключите блок живлення.

5.1.5.3 Відновлення BIOS

Виробники материнських плат можуть публікувати на своїх вебсайтах оновлені версії BIOS, що забезпечують більш стабільну роботу системи, що поліпшують її сумісність і продуктивність. Однак обновляти мікропрограмне забезпечення може бути ризиковано. Як показано на рис. 5.34, у примітках до випуску описуються відновленняпродукту, поліпшення сумісності й виправлені помилки. Деякі нові обладнання можуть працювати правильно тільки із установленими оновленнями BIOS. Щоб довідатися, яка версія BIOS установлена на комп'ютері, перевірте відомості в меню настройки BIOS (див.рис. 5.25 а)) або в сервісній програмі UEFI BIOS (див.рис. 5.31 г)).



```
*****************************************************************************
                              FEATURES ADDED
*****************************************************************************
Build 0027:
- Add 'Power On' option into BIOS 'Power Loss Control'.

Build 0026:
- None.

Build 0025:
- Add the function "CPU Swapping".
- Remove the function "Fan Control".
- Add the customer's feature "EtherBoot".
  Note: Reserve two blocks "FFF00000h - FFF0FFFFh" and "FFF10000h - FFF1FFFF"
        in the flash ROM to support the feature "EtherBoot".
        The special OPROM of NIC 82540 should be only placed in the block
        "FFF00000h - FFF0FFFFh".
        The special OPROM of NIC 82550 should be only placed in the block
        "FFF10000h - FFF1FFFFh".

*****************************************************************************
                               ISSUES FIXED
*****************************************************************************
Build 0027:
- System hangs at POST code 67 sometimes during Windows* 2000 continuous
  reboot test (With new 2.4G/533FSB CPU, 80532KE056iM).
- Upgrade the micro code for D-1 and M-0 stepping CPU.
        a. D-1 stepping CPU
           Patch ID: 018h => 02Dh
        b. M-0 stepping CPU
           Patch ID: 014h => 029h

Build 0026:
- Defect ID 65139, [XX] - SR1350-E Mitsumi Slimline CD-ROM fails on with
  certain multi-adapter backplane (Note two types exist) - one works, the
  other is not recognized.
- Upgrade the micro code for D-1 and M-0 stepping CPU to support Intel(r) Xeon(tm)
  3.2 Ghz 2M L3 cache based processors.
        a. D-1 stepping CPU
```

Рис.5.34 – Примітки до випуску BIOS

Перед відновленням мікропрограми материнської плати запишіть відомості про виробника BIOS і моделі материнської плати. Ця інформація необхідна для визначення потрібних файлів для завантаження з вебсайту виробника материнської плати. Обновляйте мікропрограму тільки в тих випадках, коли виникають проблеми із системним Обладнанням або коли потрібно розширити функціональність системи.

Раніше інформація BIOS комп'ютера зберігалася в мікросхемах ПЗП. Щоб обновити інформацію в BIOS, потрібно було замінити мікросхему ПЗП, що не завжди представлялося можливим. Тепер для BIOS використовуються мікросхеми EEPROM (ЕППЗУ), які можуть обновлятися користувачем без відкриття корпуса комп'ютера. Цей процес називається перезаписом BIOS.

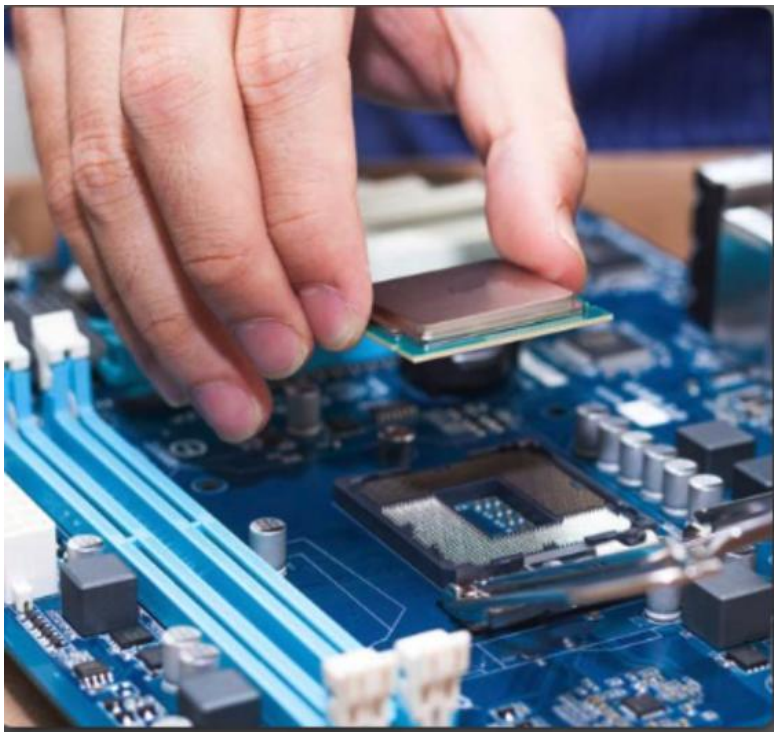
Щоб завантажити новий BIOS, зайдіть на веб-сайт виробника й виконаєте рекомендовані процедури по установці. Установка ПО для BIOS може містити в собі завантаження нового файлу BIOS, копіювання або витяг файлів на знімний носій і подальше завантаження із цього знімногоносія. Програма установки видає користувачеві запити для успішного завершення процесу.

Сьогодні багато виробників материнських плат пропонують програмне забезпечення для перезапису BIOS прямо з операційної системи. Наприклад, сервісна програма ASUS EZ Update дозволяє автоматично обновляти ПО материнській плати, необхідні драйвери й версію BIOS. Крім того, за допомогою цієї сервісної програми користувач може вручну обновити збережену версію BIOS і вибрати зображення, яке відображається на екрані під час виконання процедури POST. Така сервісна програма входить у комплект поставки материнської плати. Також її можна завантажити з веб-сайту ASUS.

УВАГА! Неправильна або перервана установка BIOS може викликати вихід комп'ютера з ладу.

5.1.5.4 Модернізація ЦП, блоку радіатора й вентилятора

Один зі способів підвищити потужність комп'ютера — побільшати швидкість обробки даних. Цього можна добитися шляхом модернізації ЦП. Однак ЦП повинен відповідати вимогам, перерахованим на рис. 5.35.



Вимоги до ЦП:
Новий ЦП повинен підходити під уже наявний роз'єм ЦП.
Новий ЦП повинен бути сполучимо із чипсетом наявної материнської плати.
Новий ЦП повинен працювати з існуючими материнською платою й блоком живлення.

Рис.5.35 – Вимоги до ЦП

Для нового ЦП може знадобитися іншийкулер. Кулер повинен фізично підходити під ЦП і бути сумісним з його роз’ємом. Також він повинен бути здатний ефективно відводити тепло від більш швидкого ЦП.

УВАГА! Між новим ЦП і кулером потрібно нанести термопасту.

Переглянете параметри температури в BIOS, щоб визначити, чи є які-небудь проблеми зі ЦП або кулером. Додатка від сторонніх постачальників також можуть надавати інформацію про температуру ЦП у зручному для читання форматі. Переглянете користувацьку документацію до материнської плати або ЦП, щоб визначити, чи працює мікросхема в припустимомутемпературномудіапазоні.

Щоб установити в корпус додаткові вентилятори для охолодження компонентів комп'ютера, виконаєтезазначені нижче дії.

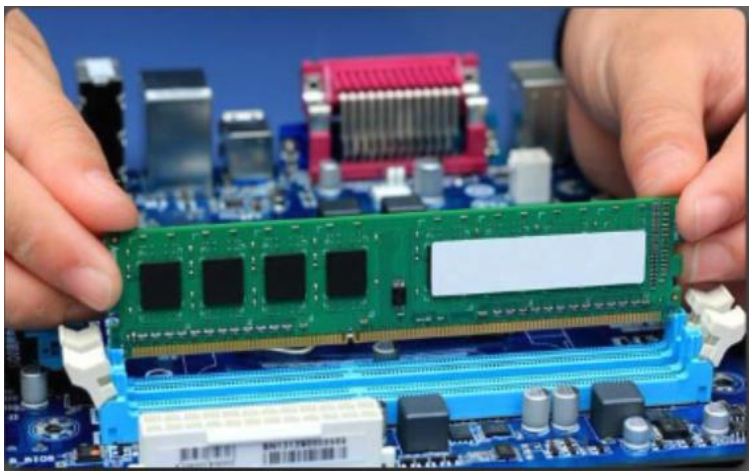
Крок 1. Установите вентилятор так, щоб він був спрямований у потрібномунапрямку — або для забору повітря, або для відводу тепла з корпусу.

Крок 2. Закріпите вентилятор, використовуючи попередньо просвердлені в корпусі отвори. Звичайно вентилятори встановлюються у верхній частині корпусу для відводу гарячого повітря, а також у нижній частині — для подачі охолодженого повітря в корпус. Не слід установлюватидва вентилятори, які відводять повітря в протилежних напрямках, занадто близько друг до друга.

Крок 3. Підключите вентилятор до блоку живлення або материнській платі, залежно від типу роз’єм вентилятора.

5.1.5.5 Модернізація оперативної пам'яті

Збільшення обсягуОЗП практично завжди приводить до підвищення продуктивності системи. Перш ніж модернізувати або заміняти ОЗП, відповідайте на запитання, перераховані на рис. 5.36.



Питання, що стосуються придбання нового ОЗП:

- Який тип ОЗП використовується материнською платою в даний момент?
- Чи є вільні роз'єми для ОЗП?
- Чи можна встановлювати ОЗП по одному модулю, або їх потрібно поєднувати в підходящі банки?
- Чи відповідає нове ОЗП характеристикам існуючої пам'яті – наприклад, швидкості обробки даних, затримці, типу й напрузі?

Рис. 5.36 – Питання, які стосуються модернізації ОЗП

Примітка. Модулі пам'яті звичайно слід установлювати в материнську плату в певномупорядку. Звернетеся до посібника користувача материнської плати, щоб ознайомитися з відповідними відомостями.

Нижче наведений порядок модернізації ОЗП на материнській платі.

Крок 1. Щоб витягти встановлений модуль ОЗП, відкрийте фіксуючі його засувки.

Крок 2. Витягніть модуль із роз’єм.

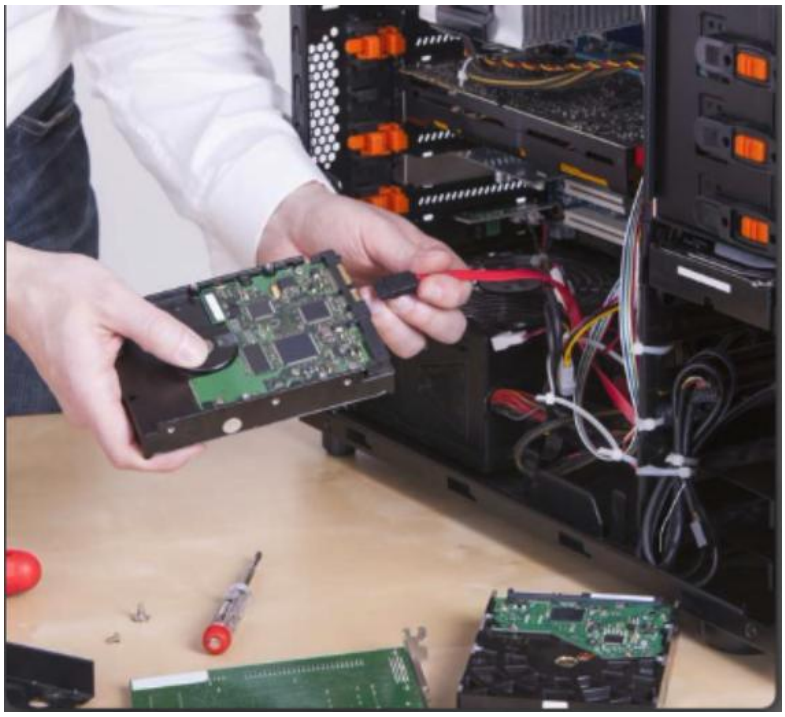
Крок 3. Вставте новий модуль у роз’єм, з якого ви тільки що витягли старий модуль ОЗП.

Крок 5. Закрийте фіксуючі засувки.

Система визначить новий модуль ОЗП, якщо він сумісний з нею й установлений правильно. Якщо BIOS не відображає наявність вірного обсягуОЗП, переконаєтеся, що модулі ОЗП сумісні з материнською платою й установлені правильно.

5.1.5.7 Модернізація жорстких дисків

Замість придбання нового комп'ютера для одержання більш високої швидкості доступу до даних і збільшення ємності системи зберігання можна додати ще один жорсткий диск. На рис. 5.37перерахованийряд причин для установки додаткового диска.



Причини для установки нового диска

- Збільшення дискового простору
- Збільшення швидкості жорсткого диска
- Установка другої ОС
- Зберігання системного файлу підкачування
- Забезпечення відмовостійкості
- Резервне копіювання вихідного жорсткого диска

Рис. 5.37 – Причини для установки додаткового диска

Вибравши підходящий для конкретного комп'ютера жорсткий диск, випливайтенаведеним нижче вказівкам по установці.

Крок 1. Помістите жорсткий диск у порожній відсік для приводів і затягніть гвинти, щоб зафіксувати диск.

Крок 2. Підключите диск до материнської плати за допомогою відповідного кабелю.

Крок 3. Приєднаєте кабель живлення до диска.

5.1.5.8 Модернізація пристроївввводу-виводу

Периферійні обладнання слід періодично модернізувати. Наприклад, якщо обладнання вийшло з ладу або ви прагнете швидше й продуктивніше працювати, то, можливо, слід вибрати нове обладнання.

Існує кілька причин для модернізації клавіатури й/або миші:

Заміна клавіатури й миші на більш ергономічні моделі, такі як на рис. 5.38 а). Ергономічні обладнаннябільш зручні у використанні й дозволяють запобігти тунельному синдрому.



а) **б)**

в)

Рис. 5.38 – Модернізація пристроїв вводу-виводу:

а) ергономічні пристрої вводу; б) декілька моніторів; в) концентратор USB

Зміна розкладки клавіатури під певнізавдання, такі як печатка на другомуязиці з додатковими символами.

Використання комп'ютера людьми з обмеженими можливостями.

Нижче перераховані різні способи модернізації моніторів.

Установка захисного фільтра, який не дає людям з боку читати інформацію з екрана. Це зможуть робити тільки сам користувач і люди, що коштують безпосередньо за ним.

Установкапротибликового фільтра, який допомагає усунути відблиски від сонця й джерел яскравого світла. Протибликовий фільтр значно полегшує читання з екрана при денномувисвітленні або коли джерело світла перебуває прямо за користувачем.

Підключення декількох моніторів, як показано на рис. 5.38 б), щоб побільшати продуктивність роботи, тому що це дозволяє користувачеві виводити на екран більше інформації й робить перенесення даних між відкритими програмами більш простим і швидким. Звичайно для роботи з декількома моніторами потрібна потужна відеокарта або установка ще однієї відеокарти.

Іноді неможливо виконати відновлення при наявних гніздах розширення або роз'ємх. У такомувипадку можна зробити відновлення за допомогою підключення по USB. Якщо комп'ютер не має вільного порту USB, потрібно встановити плату адаптера USB або придбати концентратор USB, як показано на рис. 5.38 в).

Може знадобитися установка драйверів для нового обладнання. Звичайно це можна зробити за допомогою настановного носія. Якщо настановний носій відсутній, оновлені драйвери можна завантажити з вебсайту виробника.

Примітка. Драйвер із цифровим підписом пройшов лабораторне тестування Windows на перевірку якості обладнання, по закінченню якого йому привласнюється цифровий підпис Microsoft. Установка драйвера без цифрового підпису може привести до нестабільності системи, появі повідомлень про помилки й проблемам із завантаженням. Якщо в процесі установкиобладнання система виявить драйвер без цифрового підпису, відобразиться запит на припинення або продовження установки. Установлюйте драйвери без цифрового підпису, тільки якщо певен у їхнімджерелі. У деяких операційних системах Windows заборонена установка драйверів без цифрового підпису.

5.2 Основні заходипрофілактичного обслуговування ПК

5.2.1 Профілактичне обслуговування

Профілактичне обслуговування містить у собі регулярне й систематичне виконання огляду, очищення й заміну зношених деталей, матеріалів і систем. Ефективне профілактичне обслуговування підвищує відмовостійкість деталей, матеріалів і систем і дозволяє підтримувати обладнання й програмне забезпечення в гарному робочому стані.

Пошук і усунення несправностей — це систематичний процес, використовуваний для виявлення причини збою в комп'ютерній системі й

виправлення відповідних проблем з Обладнанням і програмним забезпеченням.

У цій главі представлені загальні рекомендації із процедур пошуку й усунення несправностей і по створенню програм профілактичного обслуговування. Ці рекомендації є відправною крапкою для розвитку ваших власних навичок профілактичного обслуговування, а також пошуку й усунення неполадок.

5.2.2 Огляд профілактичного обслуговування ПК

5.2.2.1 Переваги профілактичногообслуговування

Є трохи факторів, що мають найбільше значення для планів профілактичного обслуговування. Плани профілактичного обслуговування розробляються на базі як мінімум 2 факторів:

- **Місце розташування комп'ютера й навколишнє середовище** — комп'ютери, які перебувають у курних середовищах, наприклад використовувані на будівельнихмайданчиках, як показано на рис. 5.39, вимагають більшої уваги, чім комп'ютери, використовувані в офісах.



Рис. 5.39 Використання ПК на будівельних майданчиках

- **Використання комп'ютера** — при обслуговуванні мереж з дуже інтенсивним трафіком, наприклад, мереж навчальних закладів, може знадобитися додаткове сканування й видалення шкідливого ПО, а також небажаних файлів.

Задокументуйте завдання по регулярному обслуговуванню компонентів комп'ютера, а також частоту виконання кожної з них. Потім вико-

ристовуйте цей список завдань для створення програми профілактичного обслуговування.

В обслуговуванні комп'ютерів і захисту даних необхідно використовувати профілактичний підхід. Регулярне обслуговування дозволяє зменшити число потенційних проблем з Обладнанням і програмним забезпеченням. Регулярне обслуговування зменшує час простою комп'ютера й витрати на ремонт.

Нижче перераховані переваги профілактичного обслуговування.

1. Поліпшення захисту даних
2. Збільшення терміну служби компонентів
3. Поліпшення стабільності роботи обладнання
4. Скорочення числа збоїв обладнання

5.2.2.2.Завдання профілактичного обслуговування

Обладнання

Перевірте стан кабелів, компонентів і периферійних обладнань. Очистите компоненти, щоб знизити ймовірність перегріву. Полагодите або замініте все компоненти зі слідами ушкоджень або надмірного зношування.

У програму обслуговування обладнання рекомендується включити наступні завдання:

1. Видалення пили з вентиляторів.
2. Видалення пили із блоку живлення.
3. Видалення пили з компонентів усередині комп'ютера й периферійного обладнання, такого як принтери.
4. Очищення миші, клавіатури й екрана монітора.
5. Пошук і закріплення погане підключених кабелів.

Програмне забезпечення

Переконаєтеся, що встановлені останні версії використовуваного програмного забезпечення. Додержуйтеся політиків, прийнятим в організації, відносно установки оновлень безпеки, операційних систем і програм. Багато організацій не дозволяють виконувати відновлення без всебічного попереднього тестування. Це тестування виконується для підтвердження того, що відновлення не спричинить проблем з ОС і ПО.

На рис. 5.40 показаний екран відновлення Windows 8.1.

Використовуйте ці завдання як керівництво по формуванню графіка профілактичного обслуговування програмного забезпечення, відповідного до ваших потреб:

1. Перегляд і установка відповідних оновлень безпеки.
2. Перегляд і установка відповідних оновлень ПО.
3. Перегляд і установка відповідних оновлень драйверів.
4. Відновлення файлів визначень вірусів.
5. Сканування на наявність вірусів і шпигунського ПО.
6. Видалення невикористовуваних або непотрібних програм.

7. Сканування жорстких дисків на наявність помилок.
8. Оптимізація (дефрагментація) жорстких дисків.

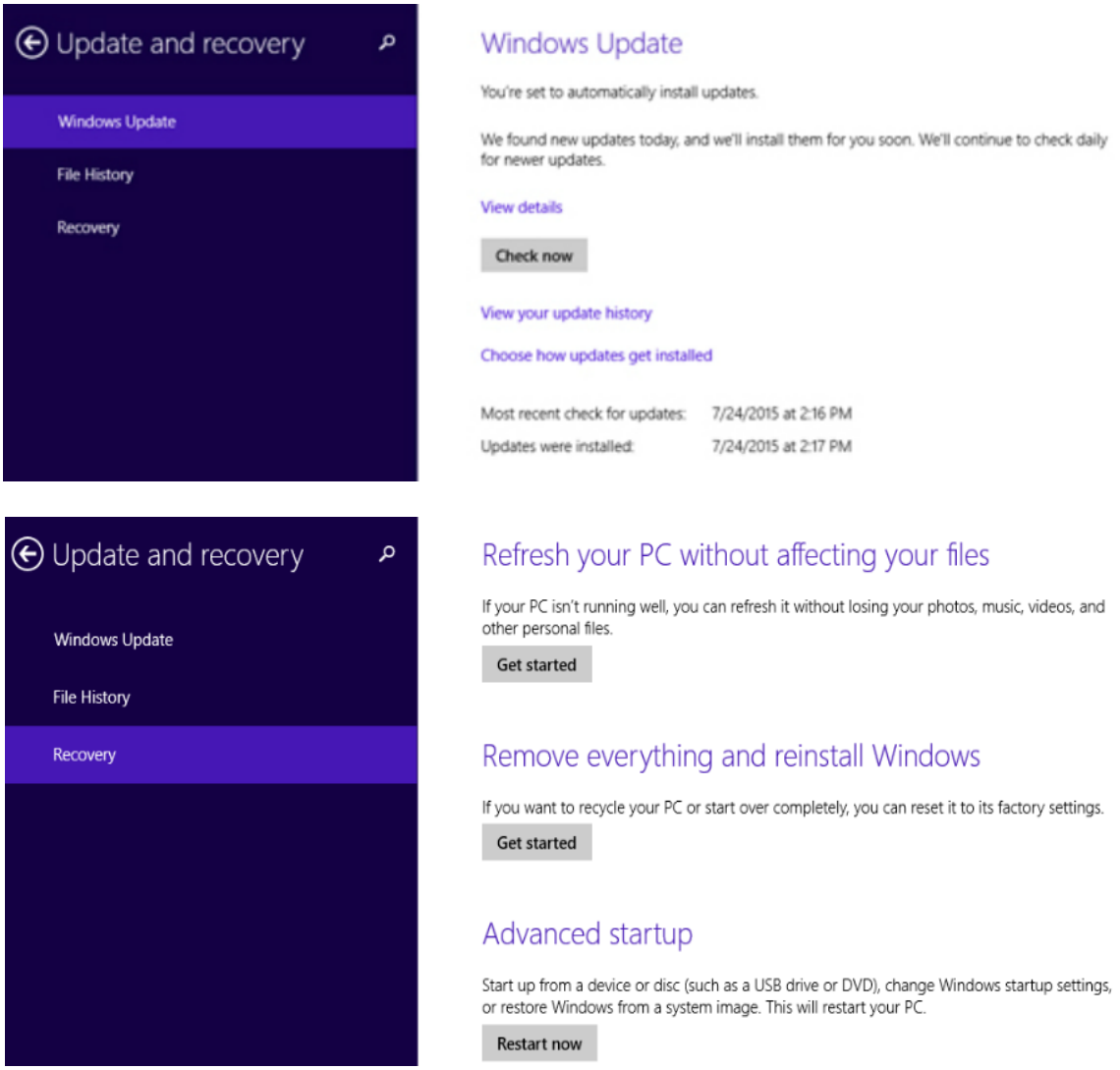


Рис. 5.40 – Екран відновлення Windows 8.1

5.2.2.3Очищеннякорпусу й внутрішніх компонентів

Важливо підтримувати корпус комп'ютера й внутрішні компоненти в чистому стані. Частота проведення процедури очищення компонентів комп'ютера залежить від кількості пили й інших стерпних повітрям часток, а також від звичок користувача. Регулярне чищення або заміна повітряних фільтрів у приміщенні, у якому використовується комп'ютер, значно скоротить обсяг пилу в повітрі.

Пил і бруд ззовні комп'ютера можуть проникати усередину через вентилятори охолодження. Накопичуючись усередині комп'ютера, пил заважає циркуляції повітря й охолодженню компонентів. компоненти, що надмірно нагріваються, комп'ютера частіше виходять із ладу. Основною метою очищення є запобігання нагромадження пили. На рис. 5.41

показаний вентилятор охолодження, на якому нагромадилася надмірна кількість пили.

Для видалення пили з корпусу комп'ютера використовуйте стиснене повітря, пилосос зі слабким потоком повітря й захистом від електростатичних розрядів і невеликий шматок безворсової тканини. Потік повітря, створюваний деякими інструментами для очищення, здатний ушкодити компоненти й перемички або послабити їхнє кріплення. Також він може приводити до утвору статичного розряду. Важливо підтримувати ці компоненти в чистому стані:

1. Блок радіатора й вентилятор
2. ОЗП
3. Плати адаптерів
4. Материнська плата
5. Вентилятори
6. Блок живлення
7. Внутрішні диски

Пилосос зі слабким потоком повітря й захистом від електростатичних розрядів можна використовувати для видалення пили й інших речовин, які перебувають усередині корпусу. Пилосос також можна використовувати для втягування пили, піднятої стисненим повітрям. При використанні стисненого повітря з балончика, як показано на рис. 5.42, тримаєте його вертикально, щоб рідина не витекла на компоненти комп'ютера.

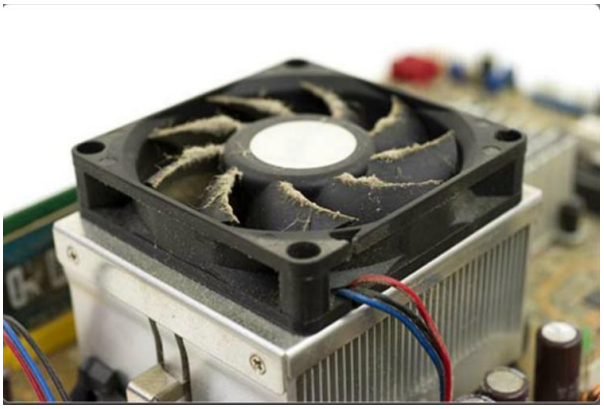


Рис. 5.41 – Вентилятор охолодження з пилом



Рис. 5.42 – Використанні стисненого повітря з балончика

Завжди додержуйтеся інструкцій і попередженням на балончиках зі стисненим повітрям. Розташовуйте балончик на безпечній відстані від чутливих обладнань і компонентів.

Використовуйте безворсову тканину для видалення пили, який залишається за компонентами.

Увага! При очищенні вентилятора за допомогою стисненого повітря притримуйте його лопати. Це запобіжить обертанню ротора з надмірно високою швидкістю й переміщення вентилятора в небажаному напрямку.

Регулярне очищення також дає можливість перевірити компоненти на предмет ослаблених гвинтів і роз'ємів.

1. Відсутні кришки гнізд розширення, через які в комп'ютер можуть проникати пил, бруд або живі комахи
2. Відсутні або погано затягнуті гвинти кріплення плат адаптерів
3. Нещільно приєднані або переплутані кабелі, які можуть вивалюватися з корпуса й компонентів

Використовуйте тканину або щітку, щоб очистити корпус комп'ютера зовні. Якщо ви використовуєте засіб, що чистить, не наносите його безпосередньо на корпус. Замість цього нанесіть невелику кількість засобу, що чистить, на тканину й протріть зовнішню поверхню корпусу.

5.2.2.4Огляд внутрішніх компонентів

Кращим способом підтримки комп'ютера в гарному стані є профілактична перевірка його стану. От основний контрольний перелік компонентів, що підлягають огляду.

- **Блок радіатора й вентилятора ЦП** — перевірте, не чи нагромадився пил на радіаторі й вентиляторі ЦП. Перевірте, чи вільно обертається вентилятор. Перевірте надійність приєднання кабелю живлення вентилятора. Перевірте роботу вентилятора, включивши живлення й переконавшись у тому, що він обертається.
- **Модулі ОЗП** — модулі ОЗП повинні бути надійно закріплені в гніздах ОЗП. Іноді фіксатори можуть слабшати. При необхідності відкріпите й знову закріпите їх. Використовуйте стиснене повітря для видалення пили.
- **Обладнання зберігання даних** — перевірте всі обладнання зберігання даних. Усі кабелі повинні бути надійно приєднані до роз'ємів. Упевніться, що всі перемички на місці, добре закріплені й правильно встановлені. Від приводів не повинні виходити стукіт, деренчання або скрегіт.
- **Плати адаптерів** — плати адаптерів повинні бути надійно закріплені у своїх гніздах. Якщо плата закріплена нещільно, це може привести до короткого замикання. Закріплюйте плати адаптерів за допомогою стопорних гвинтів або фіксаторів, щоб вони не розбовталися у

своїх гніздах. Використовуйте стиснене повітря для видалення пили й бруди із плат адаптерів і із гнізд.

- **Гвинти** —, що відгвинтилися гвинти можуть привести до проблем, якщо їх відразу ж не затягти або не вигвинтити. Гвинт, що відгвинтився усередині корпуса, може привести до короткого замикання або може закотитися в таке місце, звідки його буде складно витягти.
- **Кабелі** — оглянете всі кабельні з'єднання. Перевірте, чи немає зламаних і погнутих штирків. Переконаєтеся, що всі фіксуючі гвинти роз'ємів затягнуті настільки, наскільки їх можна затягти вручну. Переконаєтеся, що кабелі ніде не перекручені, не перегнуті й не затиснені.
- **Обладнання живлення** — оглянете подовжувачів, мережні фільтри (обмежники напруги) і обладнання ІБЖ. Переконаєтеся в тому, що вентиляція обладнань живлення виконується належним чином, і ніщо не перешкоджає потоку повітря. Замініте обладнання живлення, якщо вони працюють не так, як повинні.
- **Клавіатура й мишу** — використовуйте стиснене повітря для очищення клавіатури, миші й сенсора миші.

5.2.2.5Турбота про навколишнє середовище

Оптимальні умови експлуатації:

- Відносна вологість від 10% до 80%
- Температура від 7,2 до 32,2 °C

5.2.3Процедура пошуку й усунення неполадок

5.2.3.1 Уведення в пошук і усунення неполадок

Для здійснення пошуку й усунення неполадок потрібне наявність організованого й продуманого підходу для вирішення проблем, пов'язаних з комп'ютерами й іншими компонентами. Часом проблеми виявляються в ході профілактичного обслуговування. В інших випадках замовник може звернутися до вас зі своєю проблемою. Логічний підхід до пошуку й усуненню неполадок дозволяє відсівати змінні фактори й визначати причини проблем у систематичному порядку. Постановка правильних питань, перевірка потрібного обладнання й вивчення потрібних даних допомагають зрозуміти проблему й запропонувати потенційний розв'язок.

Навички пошуку й усунення неполадок вигострюються згодом. З кожною вирішеною проблемою ви здобуваєте новий досвід і поліпшуєте свої навички пошуку й усунення неполадок. Ви довідаєтеся, як і де варто поєднувати або пропускати етапи для швидкого пошуку розв'язку проблеми. Процедура пошуку й усунення неполадок — це набір рекомендацій, який міняється відповідно до ситуації.

У даному розділі представлений підхід до вирішення проблем, застосовний як до обладнання, так і програмного забезпечення.

Примітка. Термін «замовник» у тому розумінні, як він використовується в цьому курсі, позначає будь-якого користувача, якому потрібна технічна підтримка при роботі з комп'ютерами.

Перед початком пошуку й усунення неполадок завжди дотримуйте необхідних обережностей для захисту даних на комп'ютері. Деякі втручання, такі як заміна жорсткого диска або переустановленняОС, можуть привести до втрати даних на комп'ютері. Робіть усе можливе для запобігання втрати даних у ході ремонту.

Увага! Завжди виконуйте резервне копіювання перед початком пошуку й усунення неполадок. Перед початком будь-якої роботи на комп'ютері замовника необхідно захистити дані. У випадку втрати даних замовника в результаті проведених вами операцій відповідальність за це може бути покладена на вас або вашу компанію.

Резервне копіювання даних

Резервна копія даних — це копія даних з жорсткого диска комп'ютера, збережена на іншому обладнанні зберігання або в хмарі.

Хмарне сховище даних — це мережне сховище даних, доступ до якого здійснюється через Інтернет.

Організація може виконувати резервне копіювання **щодня, щотижня або щомісяця.**

Якщо ви не певен у тому, що резервне копіювання виконане, не намагайтеся вживати ніяких дій по пошукові й усуненню неполадок, поки не уточните цей момент із замовником. Нижче приводиться список елементів для перевірки за допомогою замовника того факту, що було виконано резервне копіювання.

1. Дата останнього резервного копіювання
2. Уміст резервної копії
3. Цілісність резервної копії
4. Доступність усіх носіїв резервної копії для відновлення даних

Якщо в замовника немає поточної резервної копії, а у вас немає можливості створити її, попросите замовника підписати заява про звільнення від відповідальності. Ця заява повинна містити як мінімум наступну інформацію:

1. Дозвіл працювати над усуненням неполадок комп'ютера, незважаючи на відсутність поточної резервної копії.
2. Звільнення від відповідальності у випадку втрати або ушкодження даних.
3. Опис роботи, яка буде виконана.

5.2.3.2.Визначення проблеми

Першим етапом процедури пошуку й усунення неполадок є визначення проблеми. На цьому етапі необхідно одержати якнайбільше інформації від замовника, а потім провести діагностику комп'ютера табл. 5.16.

Таблиця 5.16 – Етап 1. Визначення проблеми

Інформаціяпрозамовника	• Назва компанії • Ім'я контактної особи • Адреса • Номер телефону
Комплектаціякомп'ютера	• Виробник і модель • Операційна система • Мережеве оточення • Тип підключення
Описнеполадки	• Відкриті питання • Закриті питання
Повідомленняпропомилки	
Послідовностізвуковихсигналів	
Індикатори	
POST	

Етикет при бесіді

У ході розмови із замовником випливайте наведеним нижче рекомендаціям:

1. Для одержання інформації ставте прямі запитання.
2. Не використовуйте галузевий жаргон.
3. Не говорите із замовником з висока.
4. Не ображайте замовника.
5. Не обвинувачуйте замовника в тому, що він сам створив цю проблему.

Втабл. 5.17 перераховані деякі найбільш важливі відомості, які слід одержати в замовника.

Таблиця 5.17 – Виявлення проблеми

Тип питання	Технічне питання
Закритий	Чи використовувався ваш комп'ютер ким-небудь ще останнім часом?
Закритий	Чи Видавав комп'ютер які-небудь повідомлення про помилки?
Відкритий	Які у вас проблеми з комп'ютером або мережею?
Закритий	Чи Можете ви відтворити проблему?
Відкритий	Яке програмне забезпечення було недавно встановлене на ваш комп'ютер?
Відкритий	Що ви робили, коли виявилася неполадка?
Закритий	Чи міняли ви свій пароль останнім часом?
Відкритий	Які зміни в обладнання вашого комп'ютера були внесені останнім часом?
Закритий	Ви зараз у мережі?

Відкриті й закриті питання

Відкриті питання дозволяють замовникам описати проблему своїми словами. Використовуйте відкриті питання для одержання загальної інформації.

Ґрунтуючись на інформації, отриманої від замовника, можна перейти до закритих питань. Закриті питання звичайно припускають відповідь «так» або «ні».

Документування відповідей

Задокументуйте інформацію, отриману від замовника, у замовленні на виконання роботи й у журналі обліку ремонтних робіт. Записуйте все, що, на вашу думку, може бути важливо для вас або іншого технічного фахівця. Незначні деталі часто допомагають розв'язати складну або заплутану проблему.

Звукові коди

Кожний виробник BIOS використовує унікальну послідовність звукових сигналів (комбінація довгих і коротких звукових сигналів), що вказує на ту або іншу помилку в роботі обладнання. При пошуку й усуненні неполадок включите комп'ютер і слухайте. Коли система виконує процедуру POST, більшість комп'ютерів видають один звуковий сигнал, який означає коректне завантаження операційної системи комп'ютера. У випадку помилки ви можете почути кілька звукових сигналів. Задокументуйте послідовність звукових кодів і досліджуйте код з метою визначення причини конкретної проблеми.

Відомості BIOS

Якщо комп'ютер завантажується, але зупиняється після виконання процедури POST, вивчите параметри BIOS. Обладнання може бути не виявлене або не настроєне належним чином. Ознайомтеся з документацією до материнської плати й переконаєтеся в правильності параметрів BIOS.

Додаток Event Viewer (Перегляд подій)

У випадках, коли комп'ютер піддається системним, користувацьким або програмним помилкам, додаток Event Viewer (Перегляд подій) відображає оновлену інформацію про помилки. Додаток Event Viewer (Перегляд подій), показане на рис.5.43, записує наступну інформацію про неполадку:

1. Тип виниклої неполадки
2. Дата й час неполадки
3. Рівень серйозності неполадки
4. Джерело неполадки
5. Ідентифікаційний номер події
6. Користувач, який перебував у системі, коли виникла неполадка

Хоча в Перегляді подій відображаються відомості про помилку, для визначення розв'язку може знадобитися додаткове вивчення проблеми.

Device Manager (Диспетчер обладнань)

Додаток Device Manager (Диспетчер обладнань), показане на рис. 5.44, відображає всі обладнання, настроєні на комп'ютері. Операційна система позначає обладнання, що не працюють належним чином, значком помилки.

1. Жовтий кружок зі знак оклику (!) указує на те, що обладнання не працює належним чином.

2. Червоний кружок зі значком **X** означає, що обладнання відключене.

3. Жовтий знак питання (?) указує на те, що система не може визначити, який драйвер слід установити для обладнання.

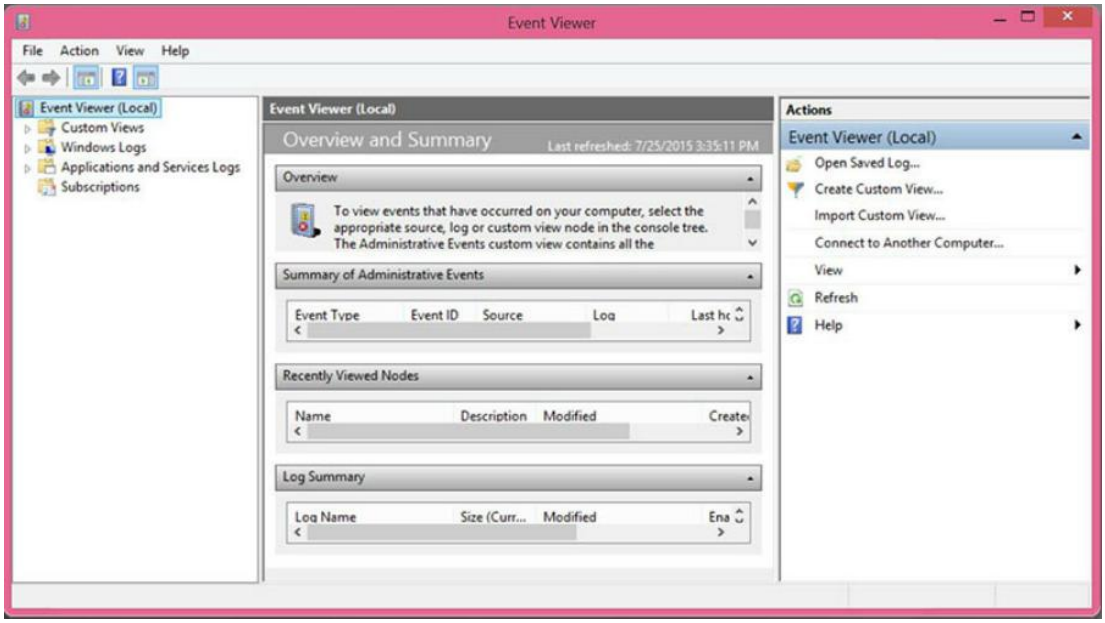


Рис. 5.43 – Додаток Event Viewer

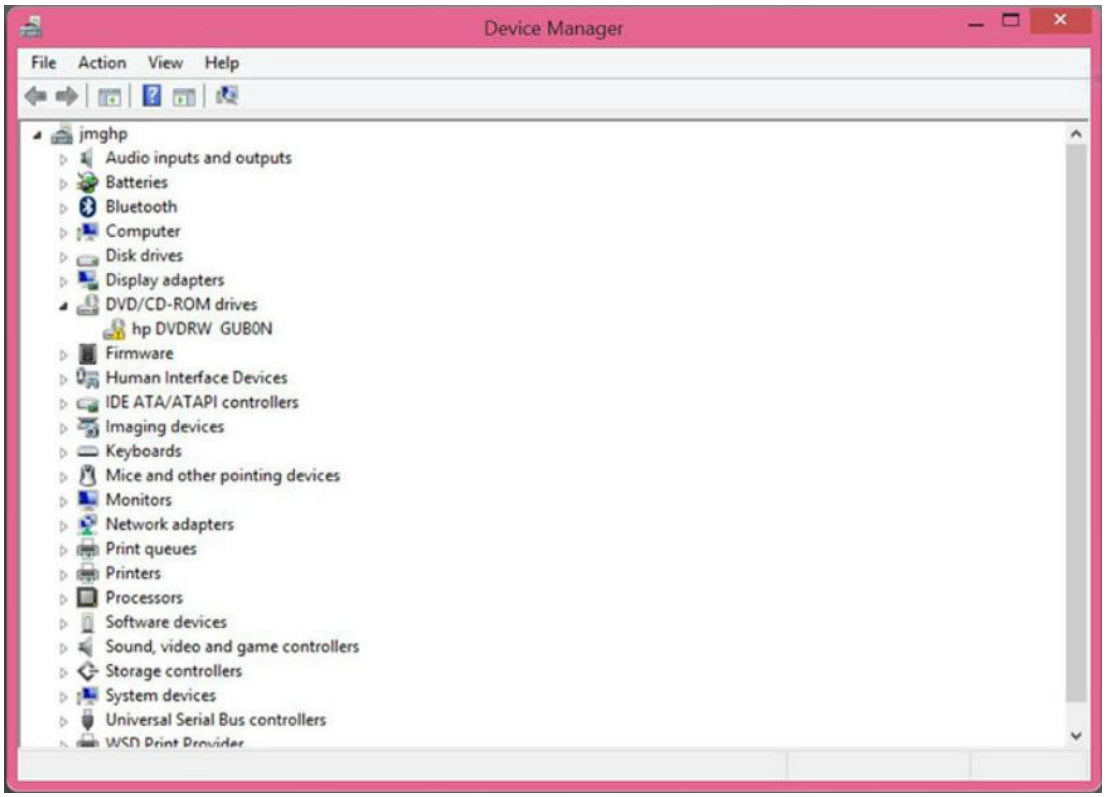


Рис. 5.44 – Додаток Device Manager (Диспетчер обладнань)

Task Manager (Диспетчер завдань)

Додаток Task Manager (Диспетчер завдань), показане на рис. 5.45, відображає додатка й фонові процеси, що працюють у даний момент на комп'ютері. За допомогою Диспетчера завдань можна завершувати роботу додатків, які перестали відповідати.

Також можна відслідковувати продуктивність ЦП і віртуальної пам'яті, переглядати як усі процеси, що виконуються в даний момент, так і інформацію про мережні підключення.

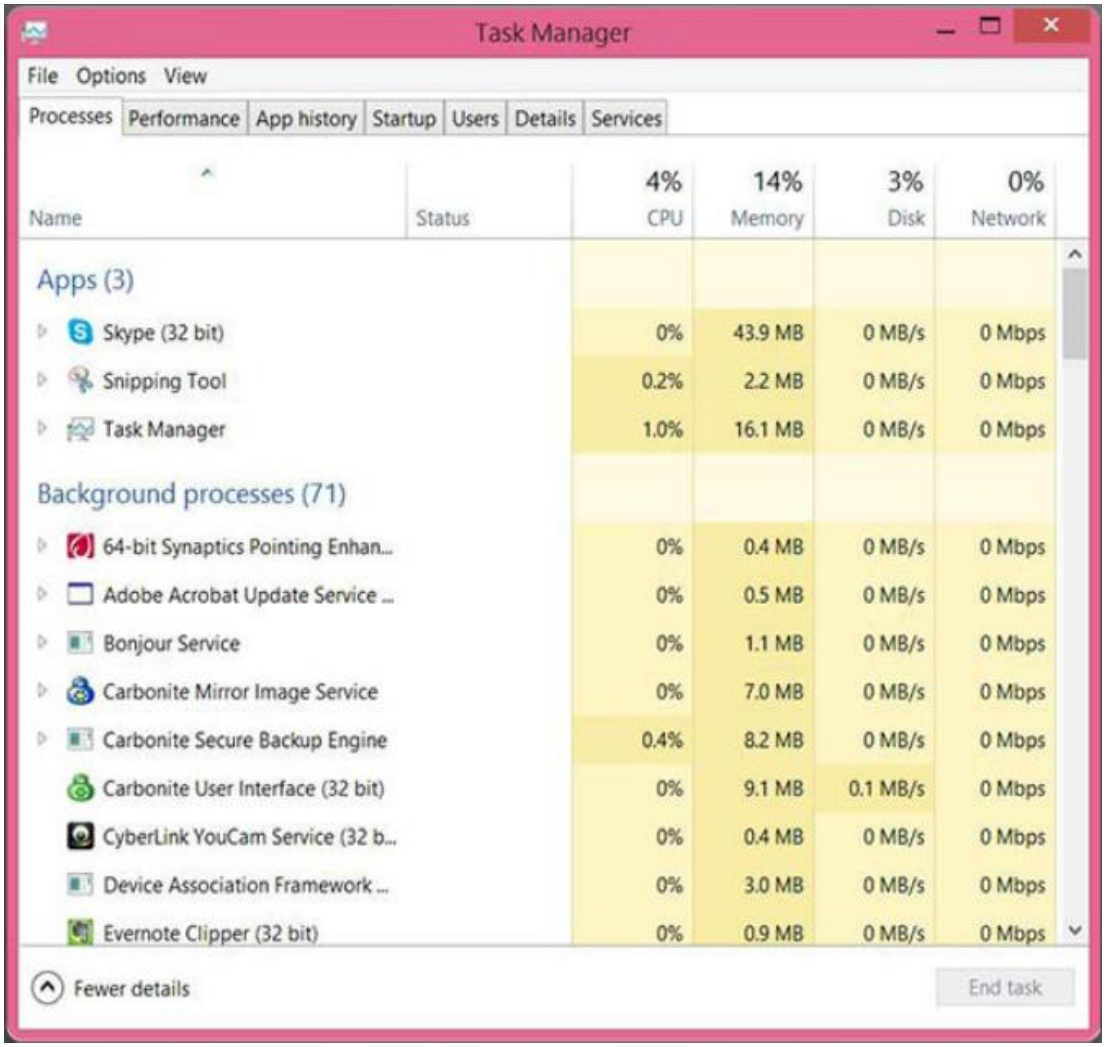


Рис. 5.45 – Додаток Task Manager (Диспетчер завдань)

Інструменти для діагностики

З'ясуєте, яке ПО доступно для допомоги в діагностиці й усуненні неполадок. Є безліч програм, які допомагають усувати неполадки обладнання. Виробники системного обладнання звичайно надають власні кошти для діагностики. Наприклад, виробник жорстких дисків може надати засіб для завантаження комп'ютера й діагностики причин відсутності завантаження операційної системи з жорсткого диска.

5.2.3.3 Формування припущень про можливу причину

Другий етап процедури пошуку й усунення несправностей — формування припущень про їхню можливу причину табл. 5.18.

Таблиця 5.18 – Етап 2.Формування припущень про можливу причину

Пристрій відключений
Перемикач живлення для розетки перебуває в положенні «виключене»
Мережевий фільтр відключений
Ослабнули роз'єми зовнішніх кабелів
Диск у призначеномузавантажувальномуприводі не є завантажувальним
Невірний порядок завантаження в параметрах BIOS,

У першу чергу створіть список найпоширеніших причин виникнення неполадки. Навіть якщо замовник уважає, що неполадка викликана серйозною проблемою, почніть із розгляду самих очевидних причин, перш ніж переходити до більш складної діагностики.

Самі очевидні або прості причини слід розташувати на початку списку. Більш складні причини розмістите наприкінці.

При необхідності виконаєте внутрішнє (по журналах) або зовнішнє (використовуючи Інтернет) дослідження відповідно до симптомів.

Подальші етапи процедури пошуку й усунення неполадок містять у собі перевірку кожної з можливих причин.

5.2.3.4 Перевірка припущень із метою визначення причини

Точна причина неполадки визначається шляхом перевірки припущень одного за іншим, починаючи з найбільш простих. Втабл. 5.19 наведені деякі типові дії по визначенню причини неполадки.

Таблиця 5.19 – Етап 3. Перевіркаприпущеньізметоювизначенняпричини

Стандартні дії для визначення причини	• Переконаєтеся в тому, щопристрійвключений. • Переконаєтеся, щоперемикачживленнядлярозеткиперебуває в положенні «включене». • Переконаєтеся, щомережевийфільтрвключений. • Переконаєтеся, щозовнішнікабеліприєднанінадійно. • Переконаєтеся, щопризначенийдискєзавантажувальним. • Перевіртепорядокзавантаження в параметрахBIOS.

Після виявлення точної причини неполадки визначите дії по її усуненню. У міру нагромадження досвіду в області пошуку й усунення неполадок комп'ютерів ви будете швидше виконувати ці етапи. Попрактикуйтеся в кожному з них, щоб краще ознайомитися із процесом пошуку й усунення неполадок.

Якщо не вдається визначити точну причину неполадки після перевірки всіх припущень, сформулюйте нове припущення про можливі причини й перевірте його. При необхідності передайте проблему більш дос-

відченому технічному фахівцеві. Перед передачею задокументуйте кожну виконану перевірку, як показано на рис. 5.46.

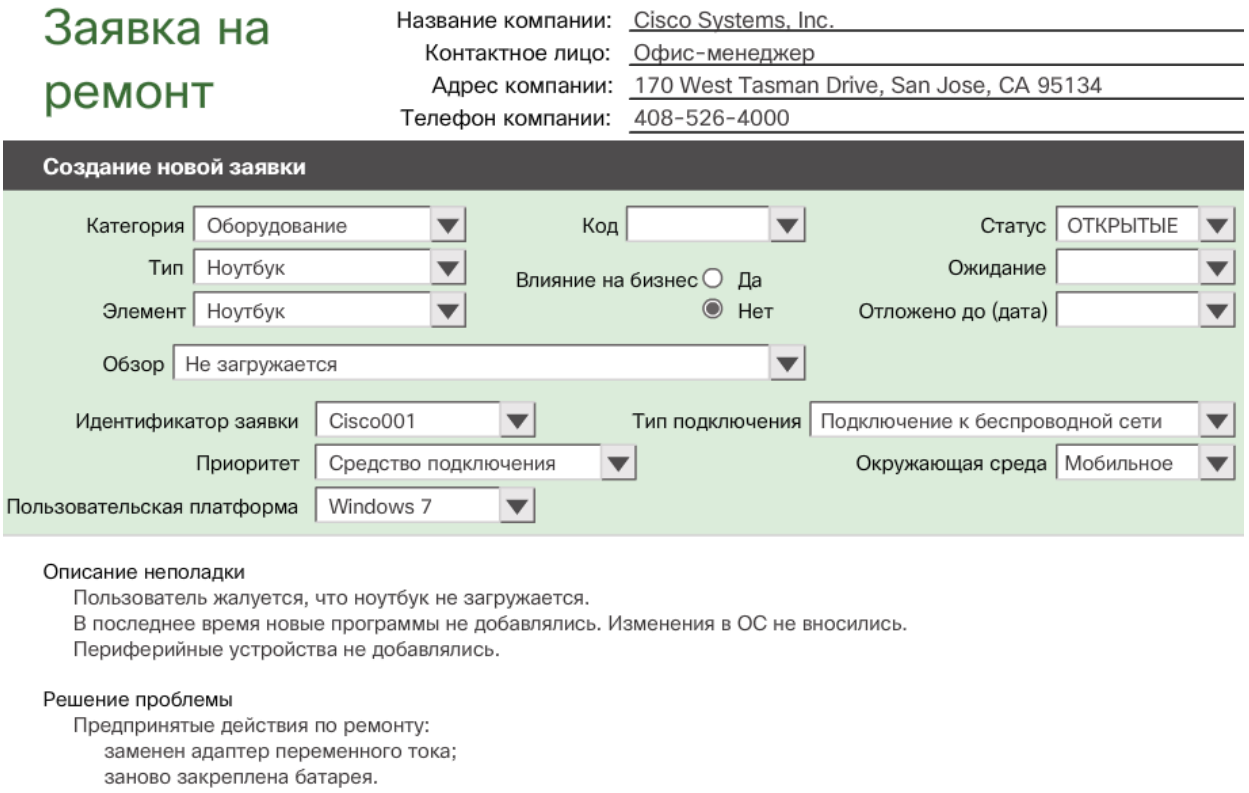


Рис. 5.46– Документування кожної виконаної перевірці

5.2.3.5 Розробка плану дій по усуненню неполадки і його виконання

Установивши точну причину неполадки, розробіть план дій для її усунення й виконаєте його. Часом неполадку можна усунути за допомогою швидких процедур. Якщо швидка процедура привела до усунення неполадки, виконаєте повну перевірку функціонального стану системи й при необхідності вживіть профілактичних заходів. Якщо швидка процедура не привела до усунення неполадки, продовжите вивчення проблеми й поверніться до етапу 3, щоб сформулювати нове припущення про її можливі причини.

Після розробки плану дій слід перейти до пошуку можливих розв'язків. В табл.5.20 перераховані області, у яких можна вести пошук

Розділите більші проблеми на дрібні, які можна аналізувати й вирішувати окремо. Розставитевирішення по пріоритету, починаючи з найпростіших і швидких у реалізації. Створіть список можливих вирішень і застосовуйте їх по одному.

Якщо використання якого-небудь розв'язку не допомогло усунути проблему, поверніть усе у вихідний стан і спробуйте інший варіант.

Таблиця 5.20 – Етап 5. Розробка плану дій по усуненню неполадки і його-виконання

Якщонапопередньо-муетапіпроблеманебулаусунута, тодляїївирішеннянеобхідний подальшийаналізситуації.	• Журнали обліку ремонтних робіт служби підтримки • Інші технічні фахівці • Веб-сайти виробників: розділ питань, що часто задаються • Технічні веб-сайти • Новинні групи • Керівництва до комп'ютера • Керівництва до пристроїв • Форуми в Інтернеті • Пошук в Інтернеті

Продовжуйте виконувати цю процедуру, поки не буде знайдений підходящий розв'язок.

5.2.3.6 Повна перевірка функціонального стану системи й вживання профілактичних заходів якщо буде потреба

Після усунення неполадки продовжуйте процес пошуку й усунення несправностей, провівши повну перевірку функціонального стану системи й прийнявши всі необхідні профілактичні заходи (табл. 5.21). Повна перевірка функціонального стану системи допомагає переконатися в тому, що вихідна проблема вирішена й що в ході ремонту не виникли нові неполадки. Завжди, якщо є така можливість, пропонуйте замовникові перевірити, що проблема вирішена й система функціонує справно.

Таблиця 5.21 – Етап 5.Перевірка всіх функцій системи й (при необхідності) вживання профілактичних заходів

• Перезавантажитекомп'ютер.
• Перевірте, чиправильнопрацюютьдодатки.
• ПеревіртемережуйпідключеннядоІнтернету.
• Роздрукуйтедокументізбудь-якогододатка.
• Переконаєтеся, щовсіпідключеніпристроїпрацюютьправильно.
• Переконаєтеся у відсутності повідомлень про помилки.

5.2.3.7 Документування отриманих даних, вжитих заходів і результатів

По закінченню ремонту комп'ютера завершите процес усунення неполадок разом із замовником. В усному й письмовому виді опишіть замовнику неполадку й вирішення, які допомогли її усунути. У табл. 5.22 показані дії, які слід почати по закінченню ремонту.

Перевірте вирішення разом із замовником. Якщо замовник доступний, продемонструйте, як вирішення усунуло проблему з комп'ютером. Нехай замовник протестує вирішення і спробує відтворити неполадку. Коли замовник переконається, що проблема усунута, ви можете запов-

нити документацію для ремонту в замовленні на обслуговування й у своєму журналі. Включите в документацію наступну інформацію:

Опис неполадки.

Дії, початі для усунення неполадки.

Компоненти, використані при ремонті.

Таблиця 5.22 – Етап 6. Документування отриманих даних, вжитих заходів і результатів

• Обговоритезастосованийвирішенняіззамовником.
• Нехайзамовникупевниться, щопроблемаусунута.
Надайте замовнику всі папери.
• Задокументуйтедії, початідляусуненнянеполадки, узамовленнінаобслуговуванняйужурналітехнічногофахівця.
• Задокументуйтекомпоненти, використаніприремонті.
• Задокументуйтечас, витрачененавирішенняпроблеми.

5.2.3.8 Розповсюджені неполадки ПК і способи їх усунення

Розповсюджені неполадки ПК і способи їх усунення зведені до табл.5.23 -5.27

Таблиця 5.23 – Розповсюджені неполадки пристроїв зберігання даних і способи їх усунення

Визначення проблеми	Можливі причини	Можливі розв'язки
Комп'ютер не розпізнає пристрій зберігання даних.	• Кабель живлення нещільно підключений. • Кабель для передачі даних нещільно підключений. • Перемички встановлені неправильно. • Відмова пристрою зберігання даних. • Некоректні параметри пристрою зберігання даних в BIOS.	• Щільно підключите кабель живлення. • Щільно підключите кабель для передачі даних. • Переустановите перемички. • Замініте пристрій зберігання даних. • Скиньте параметри пристрою зберігання даних в BIOS.
Комп'ютер не розпізнає оптичний диск.	• Диск вставлений у перевернеyому положенні. • У привод вставлені кілька дисків. • Диск ушкоджений. • Неправильний формат диска. • Привод оптичних дисків несправний.	• Вставте диск правильно. • Переконаєтеся, що в привод вставлений тільки один диск. • Замініте диск. • Установите диск підходящого типу. • Замініте привод оптичних дисків.
Комп'ютер не витягає оптичний	• Заїдання приводу оптичних дисків. • Привод оптичних дисків	• Вставте штир у маленький отвір поруч із кнопкою витягу на приводі, щоб відкрити лоток.

Визначення проблеми	Можливі причини	Можливі розв'язки
диск.	був заблокований програмним забезпеченням. • Привод оптичних дисків несправний.	• Перезавантажите комп'ютер. • Замініть привод оптичних дисків.
Комп'ютер не розпізнає знімний зовнішній привод.	Знімний зовнішній привод не встановлений належним чином. • Зовнішні порти відключені в параметрах BIOS. • Знімний зовнішній привод несправний.	• Витягніть і знову установите привод. • Включите порти в параметрах BIOS. • Замініть знімний зовнішній привод.
Пристрій читання носіїв не зчитує дані з карти пам'яті, яка працює в камері.	• Пристрій читання носіїв не підтримує цей тип карти пам'яті. • Пристрій читання носіїв підключене неправильно. • Пристрій читання носіїв не налаштований належним чином у параметрах BIOS. • Пристрій читання носіїв несправний.	• Використовуйте карту пам'яті іншого типу. • Переконаєтеся, що пристрій читання носіїв підключене належним чином до комп'ютера. • Переконфігуруйте пристрій читання носіїв у параметрах BIOS. • Установите перевірений пристрій читання носіїв.
Добування даних із флеш-накопичувача USB або збереження їх на ньому виконується повільно.	• Материнська плата не підтримує USB 3.0. • Порт настроєний на максимальну швидкість у параметрах BIOS.	• Обновите материнську плату або USB-Флеш накопичувач для підтримки USB 3.0. • Настроїте високу швидкість порту в параметрах BIOS.

Таблиця 5.24 – Розповсюджені неполадки материнських плат і внутрішніх компонентів і способи їх усунення

Визначення проблеми	Можливі причини	Можливі розв'язки
Годинник на комп'ютері показують неправильний час, або параметри BIOS міняються при перезавантаженні комп'ютера.	• Можливо, батарея CMOS погано закріплена. • Можливо, батарея CMOS несправна.	• Закріпите батарею. • Заміните батарею.
Комп'ютер не запускається після відновлення прошивання BIOS.	• Відновлення прошивання BIOS установлене неправильно.	• Зверніться до виробника материнської плати для одержання нової мікросхеми BIOS.(Якщо на материнській платі є дві мікросхеми BIOS, можна використовувати другу).

Визначення проблеми	Можливі причини	Можливі розв'язки
Комп'ютер відображає невірну інформацію про ЦП при завантаженні.	• Параметри ЦП некоректні в розширених параметрах BIOS. • BIOS не розпізнає ЦП належним чином.	• Задайте коректні розширені параметри BIOS для ЦП. • Обновите BIOS.
Світлодіодний індикатор жорсткого диска на передній панелі комп'ютера не загоряється.	• Провід індикатору жорсткого диска не приєднаний або приєднаний нещільно. • Провід індикатору жорсткого диска неправильно приєднаний до роз'єму на передній панелі корпусу	• Повторно підключите провід індикатору жорсткого диска до материнської плати. • Правильно підключите провід індикатору жорсткого диска до рознімання на передній панелі корпусу
Вбудована мережева плата на материнській платі перестала працювати.	• Апаратний збій мережевої плати.	• Установите нову мережеву плату у відкрите гніздо.
Комп'ютер не показує відео після установки нового відеоадаптера PCIe.	• Параметри BIOS настроєні на використання вбудованого відео. • Кабель усе ще підключений до вбудованого відеоадаптера. • Новий відеоадаптер несправний.	• Відключите вбудований відеоадаптер у параметрах BIOS. • Підключите кабель до нового відеоадаптера. • Для нового відеоадаптера необхідно додаткове живлення. • Підключите всі необхідні роз'єми живлення до відеоадаптера. • Установите перевірений відеоадаптер.
Нова звукова плата не працює.	• Динаміки не підключені до відповідного роз'єму. • Виключений звук. • Звукова плата несправна. • Параметри BIOS настроєні на використання вбудованого звукового пристрою.	• Підключите динаміки до відповідного роз'єму. • Включите звук. • Установите перевірену звукову плату. • Відключите вбудований звуковий пристрій у параметрах BIOS.

Таблиця 5.25 – Розповсюджені неполадки блоків живлення й способи їх усунення

Визначення проблеми	Можливі причини	Можливі розв'язки
Комп'ютер не включається.	• Комп'ютер не підключений до розетки змінного струму. • Розетка змінного струму несправна. • Кабель живлення несправний. • Перемикач блоку живлення не включений. • Перемикач блоку живлення настроєний на неправильну напругу. • Кнопка живлення не підключена належним чином до рознімання на передній панелі. • Відмова блоку живлення.	• Підключите комп'ютер до перевіреної розетки змінного струму. • Використовуйте перевірений кабель живлення. • Включите перемикач блоку живлення. • Настроїте перемикач блоку живлення на правильну напругу. • Правильно підключите кнопку живлення до роз'єму на передній панелі корпусу. • Установите перевірений блок живлення.
Комп'ютер перезавантажується, неочікуване відключається, або відчувається захід диму або згорілих електронних компонентів.	• Блок живлення починає відмовляти.	• Замініте блок живлення.

Таблиця 5.26 – Розповсюджені неполадки ЦП і пам'яті й способи їх усунення

Визначення проблеми	Можливі причини	Можливі вирішення
Комп'ютер не завантажується або зависає.	• Перегрів ЦП. • Відмовляє вентилятор ЦП. • Відмова ЦП.	• Переустановите ЦП. Замініте вентилятор ЦП. • Додайте вентилятор(и) у корпус. • Замініте ЦП.
Вентилятор ЦП видає незвичайний шум.	Відмовляє вентилятор ЦП.	Замініте вентилятор ЦП.
Комп'ютер перезавантажується без попередження, зависає або відображає повідомлення про помилки.	• Установлена занадто висока частота системної шини. • Установлений занадто високий множник частоти ЦП. • Установлена занадто висока напруга живлення ЦП.	Відновите заводські параметри материнської плати за замовчуванням. • Понизите параметри системної шини. • понизите множник частоти ЦП. • понизите параметри напруги живлення ЦП.

Визначення проблеми	Можливі причини	Можливі вирішення
Після відновлення з одноядерного ЦП на двоядерний ЦП комп'ютер працює повільніше й показує графік лише для одного ЦП у диспетчері завдань.	BIOS не розпізнає двоядерний ЦП.	Обновите прошивання BIOS для підтримки двоядерного ЦП.
ЦП не встановлюється на материнську плату.	Невірний тип ЦП.	Замініте ЦП на ЦП, відповідний до типу роз'єму материнської плати.
Комп'ютер не розпізнає доданий модуль ОЗП.	Новій модуль ОЗП несправний. • Установлений модуль ОЗП невідповідного типу. Тип доданого модуля ОЗП відрізняється від типу вже встановленого модуля ОЗП. • Новий модуль ОЗП не закріплений у гнізді пам'яті.	• Замініте модуль ОЗП. • Установите модуль ОЗП підходящого типу. • Закріпите модуль ОЗП в гнізді пам'яті.
Після відновлення Windows комп'ютер працює дуже повільно.	• Недостатній обсяг ОЗП на комп'ютері. • Не вистачає пам'яті відеоадаптера.	• Установите додатковий модуль ОЗП. • Установите відеоадаптер з більшим обсягом пам'яті.

Таблиця 5.27 – Розповсюджені неполадки дисплеїв і способи їх усунення

Визначення проблеми	Можливі причини	Можливі вирішення
Живлення на дисплей подається, але зображення на екрані відсутнє.	• Відеокабель підключений нещільно або ушкоджений. • Комп'ютер не подає відеосигнал на зовнішній дисплей.	• Повторно підключите або заміните відеокабель. • Підключите зовнішній дисплей, використовуючи комбінацію клавіші Fn і багатофункціональної клавіші.
Дисплей мигає.	• Зображення на екрані обновляються недостатньо швидко. • Інвертор екрана ушкоджений або працює несправне.	• Настроїте частоту відновлення екрана. • Розберіть дисплей і заміните інвертор.
Зображення на дисплеївиводиться затемненим.	• Заднє підсвічування ЖК-екрана неправильно настроєне.	• Ознайомтеся в посібнику з ремонту з інструкціями з калібрування заднього підсвічування ЖК– екрана. Належним чином настроїте заднє підсвічування ЖК– екрана.
Пікселі на екрані згаслі	• Живлення не подається на пікселі.	• Звернетеся до виготовлювача.

Визначення проблеми	Можливі причини	Можливі вирішення
або не передають колір.		
У зображенні на екрані присутні миготливі лінії або малюнки різних квітів і різного розміру (артефакти).	• Дисплей неправильно підключений. • Графічний процесор перегрівається. • Графічний процесор несправний або працює неправильно.	• Розберіть дисплей і перевірте роз'єм. • Розберіть і очистите комп'ютер, прибравши пил і сміття. • Замініте графічний процесор.
Кольорові зображення неправильно відображаються на екрані.	• Дисплей неправильно підключений. • Графічний процесор перегрівається. • Графічний процесор несправний або працює неправильно.	• Розберіть дисплей і перевірте роз'єм. • Розберіть і очистите комп'ютер, прибравши пил і сміття. • Замініте графічний процесор.
Зображення на екрані дисплея перекручені.	• Змінені параметри дисплея. • Дисплей неправильно підключений. Графічний процесор перегрівається. • Графічний процесор несправний або працює неправильно.	• Змініте параметри дисплея на заводські. • Розберіть комп'ютер і перевірте підключення дисплея. • Розберіть і очистите комп'ютер, прибравши пил і сміття. • Замініте графічний процесор.
На екрані відображається побічне зображення.	Пляма на дисплеї.	• Виключите дисплей і від'єднайте його від джерела живлення на кілька годин. • Використовуйте функцію розмагнічування, якщо вона доступна. • Замініте дисплей.
Зображення на екрані перекручені по геометрії.	• Драйвер ушкоджений. • Некоректні параметри дисплея.	• Обновите або переустановите драйвер у безпечному режимі. • Скорегуйте геометрію, використовуйте параметри дисплея
На екрані виводяться занадто більші зображення й значки.	• Драйвер ушкоджений. • Некоректні параметри дисплея.	• Обновите або переустановите драйвер у безпечному режимі. • Скорегуйте геометрію, використовуйте параметри дисплея.
Проектор перегрівається й вимикається.	• Вентилятор несправний. • Вентиляційні отвори закупорені. • Проектор перебуває в	• Замініте вентилятор. • Очистите вентиляційні отвори. • Демонтуйте корпус або забезпечте належну вентиля-

Визначення проблеми	Можливі причини	Можливі вирішення
	корпусі.	цію.
Дисплеї не вирівняні або неправильне орієнтовані в параметрах для декількох дисплеїв.	• Параметри для декількох дисплеїв некоректні. • Драйвер ушкоджений.	• Використовуючи панель управління дисплеєм, ідентифікуйте кожний дисплей і настроїте вирівнювання й орієнтацію. • Обновите або переустановите драйвер у безпечному режимі.
Дисплей перебуває в режимі VGA.•	• Комп'ютер перебуває в безпечному режимі. • Драйвер ушкоджений.	• Перезавантажите комп'ютер. • Обновите або переустановите драйвер у безпечному режимі.

Висновкиз розділу 5. Зборка кінцевого обладнання телекомунікаційних систем

У цій главі докладно розглядаються етапи зборки персонального комп'ютера, першого завантаження системи а також принципи профілактичного обслуговування й процедури пошуку й усунення неполадок.

Важливо завжди пам'ятати перелічене нижче:

1. Корпуси комп'ютерів випускаються в безлічі розмірів і комплектацій.
2. Багато компонентів комп'ютера повинні підходити під формфактор корпусу.
3. ЦП установлюється на материнську плату разом із блоком радіатора й вентилятора. Перед установкою останнього необхідно обов'язково нанести на ЦП термопасту.
4. Модулі ОЗП встановлюються в гнізда ОЗП на материнській платі.
5. Карти розширень установлюються в слоти PCI і PCIe на материнській платі. Жорсткі диски встановлюються в 3, 5-дюймові відсіки усередині корпусу.
6. Приводи оптичних дисків установлюються в 5, 25-дюймові відсіки, до яких є доступ зовні корпусу.
7. Кабелі блоку живлення підключаються до всіх приводів і материнській платі.
8. Внутрішні кабелі для передачі даних служать для обміну даними з усіма приводами.
9. Зовнішні кабелі служать для підключення периферійних пристроїв до комп'ютера.
10. Неправильна робота встаткування позначається кодами звукових сигналів.

11. Програма настроювання BIOS виводить інформацію про компоненти комп'ютера й дозволяє користувачеві міняти параметри системи.

12. Компоненти комп'ютера потребують періодичного відновлення й заміні деталей.

13. Додаткові жорсткі диски підвищують відмовостійкість і дають можливість установлювати додаткові операційні системи.

Принципи профілактичного обслуговування й сутність процедур пошуку й усунення неполадок пояснюється нижче:

1. Регулярне профілактичне обслуговування скорочує число проблем з обладнанням і програмним забезпеченням.

2. Перед початком якого-небудь ремонту створіть резервну копію даних з комп'ютера.

3. Процедура пошуку й усунення неполадок — це набір рекомендацій, що допомагає ефективно вирішувати проблеми, пов'язані з комп'ютером.

4. Документуйте всі свої дії, навіть якщо вони не дають результатів. Створювана вами документація буде корисним ресурсом для вас і інших технічних фахівців.

Список використаних джерел

Керівні документи

1. Порядок організації роботи відомчої цифрової телекомунікаційної мережі ДСНС Наказ ДСНС 23.10.2019 № 608

2. Наказ МВС України 08.02.2019 № 93 Про затвердження Інструкції щодо практик чи процедур проектування, дослідження, введення в експлуатацію, експлуатації та технічного обслуговування (супроводження) автоматизованих систем централізованого оповіщення

3. Наказ МВС України 20.10.2017 № 870 Про затвердження Положення про автоматизовану інформаційну систему оперативного призначення єдиної інформаційної системи МВС

Література

4. Тарарака В. Д. Архітектура комп'ютерних систем: навчальний посібник. – Житомир : ЖДТУ, 2018. – 383 с..

5. Сєрих С.О.Вибір на налаштування кінцевого обладнання інформаційних систем. Керівництво до проведення і виконання практичних занять з дисципліни «Кінцеві пристрої інформаційних», Київ: ДУТ, 2020. – 93 с.

6. А.О. Новацький Комп'ютерна електроніка: Мікропроцесорні системи: Програмування мікропроцесорних систем: Навчальний посібник для студентів напряму підготовки 6.050201 «Системна інженерія» кафедри Автоматики та управління у технічних системах Київ: НТУУ "КПІ", 2014– 307с.

7. Зозуля Ю. BIOS на 100 %. — СПб.: Питер, 2009. — 336 с.: ил. — (Серия «На 100%»).

8. Курс lT Essentials Сетевой академии Cisco [Электронный ресурс]. Режим доступа: https://www.netacad.com/ru/courses/os-it/it-essentials

Відео-контент

1. Сборка компьютера! (для новичков) [Електронний ресурс]. Режим доступу:https://www.youtube.com/watch?v=gsGfbDiR4MM

2. Как собрать компьютер. Подробная инструкция по сборке ПК v2.0 [Електронний ресурс]. Режим доступу:
https://www.youtube.com/watch?v=R48bRlPNwJQ

3. Как собрать компьютер самому? / гайд по сборке игрового ПК с нуля для начинающих новичков. [Електронний ресурс]. Режим доступу: https://www.youtube.com/watch?v=hr-siRhvApM

4. Профилактика компьютера или ноутбука, когда делать, как делать? [Електронний ресурс]. Режим доступу:
https://www.youtube.com/watch?v=BU32NdOU6ZU

5. Как правильно почистить компьютер от пыли и профилактика [Електронний ресурс]. Режим доступу:
https://www.youtube.com/watch?v=WwZWA9cauyU

Питання та завдання для самостійного контролю знань

Контрольні питання:

1. Відкриття корпусу комп'ютера
2. Установка блоку живлення
3. Установка ЦП, блоку радіатора й вентилятора
4. Установка ОЗП
5. Установка материнської плати
6. Установка жорсткого диска
7. Установка привода оптичних дисків
8. Типи плат адаптерів
9. Установка адаптера безпроводової мережі
10. Установка плати відеоадаптера
11. Підключення живлення материнської плати
12. Підключення живлення до внутрішніх приводів і вентиляторам у корпусі
13. Підключення внутрішніх кабелів для передачі даних
14. Установка внутрішніх кабелів
15. Установка кабелів передньої панелі
16. Зворотне складання корпуса
17. Завершення складання комп'ютера
18. Коди звукових сигналів і настроювання BIOS
19. BIOS і CMOS

20. Програма настроювання BIOS
21. Програма настроювання UEFI
22. Інформація BIOS про компоненти
23. Параметри конфігурації BIOS
24. Настроювання безпеки BIOS
25. Діагностика й моніторинг устаткування в BIOS
26. Режим EZ в UEFI
27. Розширений режим в UEFI
28. Завантаження комп'ютера
29. Модернізація компонентів материнської плати
30. Модернізація материнської плати
31. Оновлення BIOS
32. Модернізація ЦП, блоку радіатора й вентилятора
33. Модернізація оперативної пам'яті
34. Пошук файлу BIOS
35. Модернізація жорстких дисків
36. Модернізація пристроїв вводу-виводу
37. Огляд профілактичного обслуговування ПК
38. Переваги профілактичного обслуговування
39. Задачі профілактичного обслуговування
40. Очистка корпусу й внутрішніх компонентів
41. Огляд внутрішніх компонентів
42. Турбота про навколишнє середовище
43. Процедура пошуку й усунення неполадок
44. Етапи процедури пошуку й усунення неполадок
45. Вступ в пошук і усунення неполадок
46. Визначення проблеми
47. Інтерактивне завдання — визначення проблеми
48. Формування припущень про можливу причину
49. Перевірка припущень із метою визначення причини
50. Розробка плану дій по усуненню неполадки і його виконання
51. Повна перевірка функціонального стану системи й вживання профілактичних заходів якщо буде потреба
52. Документування отриманих даних, вжитих заходів і результатів
53. Розповсюджені неполадки й способи їх усунення
54. Розповсюджені неполадки ПК і способи їх усунення

Питання для тест-контролю

Користувач повідомляє, що ранками при включенніодного з комп'ютерів параметри конфігурації на цьомукомп'ютері скидаються. Що можна зробити для виправлення цієї ситуації?

Замінити материнську плату.

Перемістити перемички.

Обновити прошивання BIOS.

Замінити батарею CMOS.

У чомуполягає одна із цілей регулювання тактової частоти в настроюваннях BIOS?

Зниження швидкості роботи й температури ЦП.

Запуск декількох операційних систем у файлах або розділах.

Зміна порядку завантажувальних розділів.

Відключення пристроїв, які не потрібні або не використовуються комп'ютером.

Технічний фахівець зауважує, що на материнській платі половина рознімань для оперативної пам'яті пофарбована в одинколір, а друга половина – в іншій. Яка технологія, швидше за все, реалізована в цій системі?

Код корекції помилок

Віртуалізація

Двосторонні модулі пам'яті

Двоканальний режим

Яка дія слід почати при складанні комп'ютера, щоб уникнути плутанини з кабелями усередині корпусу комп'ютера?

Установити модульний блок живлення.

Установити жорсткий диск розміром 2,5" замість 3,5".

Установити ЦП без використання радіатора й вентилятора.

Установити материнську плату в корпус без використання стійок.

Інженер установлює додаткову пам'ять на комп'ютер. Як йому забезпечити правильне розміщення пам'яті?

Мітка на модулі пам'яті завжди повинна бути спрямована убік ЦП

Ключ у модулі пам'яті повинен бути сполучений із ключем у гнізді для модуля пам'яті,

Стрілки на модулі пам'яті повинні бути сполучені зі стрілками на гнізді для материнської плати.

Гнізда для модуля пам'яті мають колірне маркування: один край позначений червоним кольором, а іншої — синім

Як ідентифікувати контакт № 1 на кабелях передньої панелі при складанніПК, щоб забезпечити правильність їх приєднання до з'єднувачів на материнській платі?

По червоному проведенню

За знаком плюс

По наявності маленької стрілки або вилучення

По P1

Інженер зібрав новий комп'ютер і тепер повинен настроїти BIOS. У який момент слід натиснути клавішу для запуску програми настроювання BIOS?

у процесі завантаження Windows

після процедури POST, але перед початком завантаження Windows

перед включенням комп'ютера

під час процедури POST

Для чого призначена функція Lojack?

Допомагає власниковіпристрою дистанційно визначити місце розташування пристрою, заблокувати його або вилучити всі файли на пристрої.

Надає паролі для різних рівнів доступу до BIOS.

Дозволяєкомп'ютеру завантажувати тільки ту операційну систему, якої довіряє виробник материнської плати.

Шифрує дані на жорстких дисках для запобігання доступу до даних без правильного пароля.

Коли технічному фахівцеві слід використовувати непідписаний драйвер для знову встановлюваного комп'ютерного встаткування?

Якщо на настановномуносії Windows відсутній підписаний драйвер.

Якщо недоступний вихідний настановний носій драйвера.

Якщо це непідписаний драйвер самої нової версії.

Якщо фахівець довіряє джерелу, що надало драйвер.

Яке твердження описує призначення рамки розніманьуведення-виводу?

Вона забезпечує можливість підключення до портів уведення-виводу материнської плати в різних корпусах комп'ютера.

Вона вставляється в материнську плату, збільшуючи число доступних гнізд для адаптерних плат.

Вона підключає гнізда адаптера PCIe, використовувані для відео, безпосередньо до ЦП для збільшення швидкості обробки.

Вона надає кілька гнізд для підключення жорстких дисків SATA до материнської плати.

Для якого слота розширення материнської плати передбачено чотири варіанти різної довжини: від x1 до x16?

PCIe SATA PCI AGP

Що використовується для запобігання контакту материнської плати з металевими ділянкамикорпусу комп'ютера?

рознімання з нульовим зусиллям вставки

ізолюючі муфти

термопаста

заглушка тилових портів корпусу

РОЗДІЛ6.ПРИНЦИПИ ОРГАНІЗАЦІЇ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Вступ

У даній главі наведенізагальнівідомості про принципи, стандарти й призначеннімереж.Щоб відповідати очікуванням і вимогам замовників і користувачів мережі, ви повинні добре розбиратися в принципах роботи мереж.Ви познайомитеся з основами проектування мереж і довідаєтеся, як деякі компоненти впливають на потоки даних у мережі.Ці знання допоможуть вам успішно проектувати й розгортати мережі, а також знаходити й усувати неполадки.

6.1 Принципи організації мереж

6.1.1Комп'ютерні мережі

6.1.1.1 Визначення мережі

Мережі – це системи, формовані з'єднаннями.Наприклад, дороги, що з'єднують групи людей, формують фізичну мережу. Зв'язки між вами й вашими друзями формують вашу особистумережу.Веб-сайти, що дозволяють окремим користувачам зв'язуватися зі сторінками один одного, називаються соціальними мережами. Існують також мережі за призначенням:

- Система доставки пошти;
- Телефонна система;
- Система суспільного транспорту;
- Корпоративна комп'ютерна мережа;
- Інтернет.

Система автомобільних доріг, показана на малюнку, аналогічна комп'ютерноїмережі. Автомобілі, вантажівки й інші транспортні засоби «подорожують» по мережі так само, як повідомлення. Кожний водій визначає початкову крапку (комп'ютер-джерело) і кінцеву крапку (комп'ютер-адресат).У цій системі діють правила, аналогічні знакам «Стоп» і світлофорам.Вони управляють переміщенням транспортного потоку від джерела до призначення.

6.1.1.2 Вузли

Комп'ютерні мережі складаютьсязрізних пристроїв. Деякі пристрої можуть служити або в якостівузлів, або в якостіпериферійних пристроїв.

Вузол (хост) – цебудь-який пристрій, щовідправляє, щой одержує інформаціюз мережі. Принтер, підключений до ноутбука, є периферійним пристроєм.Якщо ж принтер підключений до мережінапряму, він функціонує як вузол [1-6].

До мережі можна підключити вузли різних типів: Найпоширеніші показані на рис. 6.1.



Рис.6.1 – Позначення кінцевих пристроїв

Примітка. Телефон, що використовує для роботи протокол IP, називається IP-телефоном.Він підключається до комп'ютерної мережі, а не до звичайної телефонної мережі.

Комп'ютерні мережівикористовуються в організаціях, школах, державних установах і дому.Багато мереж підключені друг до друга через Інтернет.У мережі можна спільно користуватися ресурсами різних типів.

Приклади загальних ресурсів у комп'ютерній мережі:

- Служби, наприклад служби друку або сканування;
- Простір зберігання на таких пристроях як жорсткі диски або оптичні диски;
- Додатки, наприклад, бази даних;
- Інформація, що зберігається на інших комп'ютерах, наприклад, документи й фотографії;
- Календарі, синхронізовані між комп'ютером і смартфоном.

6.1.1.3 Проміжні пристрої

Комп'ютерні мережімістятьбезлічпристроїв, що перебувають між вузлами.Ці проміжні пристрої забезпечують передачу даних з одного вузла на іншій.Найпоширеніші проміжні пристрої представлені на рис. 6.2.

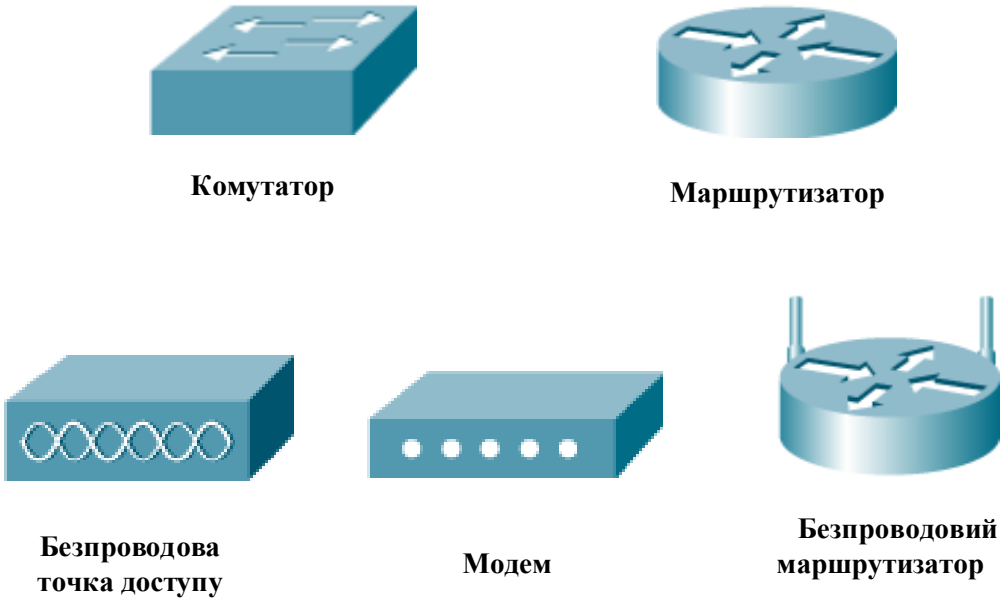


Рис.6.2 – Позначення проміжних пристроїв

Комутатор використовується для підключення декількох пристроїв до мережі. **Маршрутизатор** використовується для передачі трафіка між різними мережами. **Безпроводовий маршрутизатор** підключає до мережі кілька безпроводових пристроїв. Крім того, безпроводовий маршрутизатор часто містить комутатор, щоб провідні пристрої могли підключитися до мережі.

Точка доступу (AP)забезпечуєбезпроводове з'єднання, алемаєменшефункцій, чому безпроводовий маршрутизатор.

Модем використовується для підключення невеликого або домашнього офісу до Інтернету. Ці пристрої будуть розглянуті більш докладно далі в цій главі.

6.1.1.4 Середовища передачі даних

Зв'язок у мережі здійснюється через середовища передачі данихСередовище передачі даних уявляє собою канал, по якому повідомлення передається від джерела до адресата. По-англійському термін «середовище передачі даних» – media (не плутайте з «ЗМІ»).

Мережеві пристрої можутьбутиз'єднанізадопомогоюрізних середовищ передачіданих рис. 6.3.

Як показано на рис. 6.3, вони містять у собі:

- **Міднікабелі** – дляпередачіданихміж пристроями використовуються електричнісигнали.

- **Волоконне-оптичнікабелі** – дляпередачіінформаціїувигляді світловихімпульсів використовується скловолокноабопластмасовеволокно.
- **Безпроводовіпідключення** – дляпередачіданих використовуються радіосигнали, інфрачервонатехнологіяабосупутниковийзв'язок.



Рис.6.3 – Середовища передачі даних

Позначення, показані на рис. 6.4, використовуються в цьомукурсі для представлення різних типів середовищ передачі даних.

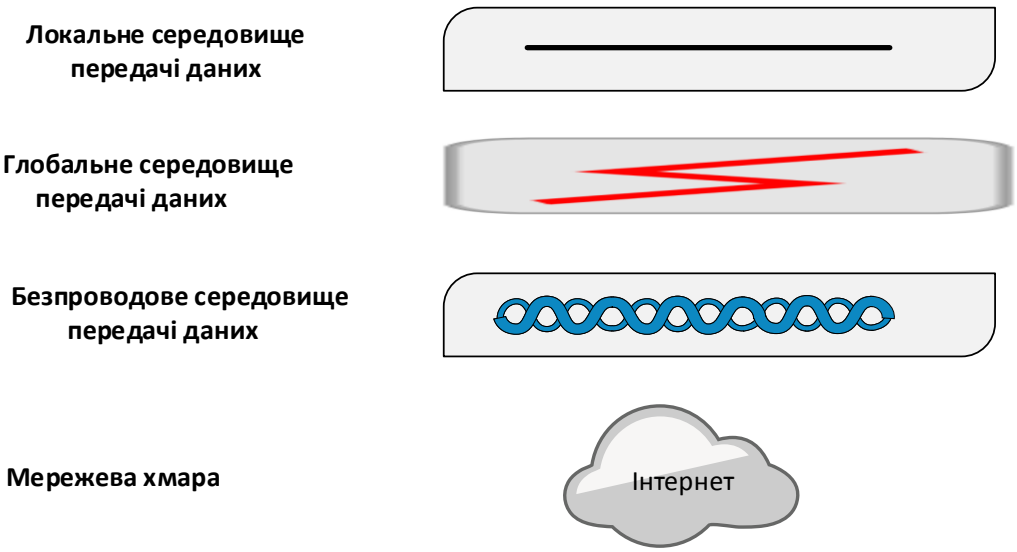


Рис.6.4– Позначення середовищ передачі даних

Локальні мережі (LAN), глобальні мережі (WAN) і безпроводові мережі описані в наступному розділі. Зображення хмари буде використовуватися в цьому курсі для позначення підключення до Інтернету. Інтернет часто є середовищем для зв'язку однієї мережі з іншою мережею.

6.1.1.5.Визначення позначень мережевих пристроїв і середовищ передачі даних

Позначення мережевих пристроїв і середовищ передачі даних зведені до табл. 6.1.

Таблиця 6.1 – Визначення позначень мережевихпристроїв і середовищ передачі даних

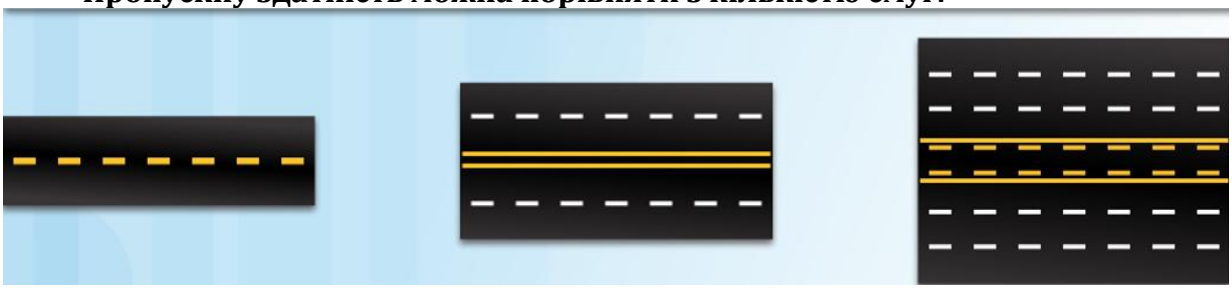
Позначення	Кінцевий пристрій	Проміжний пристрій	Середовище передачі даних
		✓	
	✓		
			✓
		✓	
	✓		
	✓		
			✓
		✓	
	✓		
			✓
		✓	
		✓	

6.1.1.6 Пропускна спроможність і затримка

Пропускна спроможністьмережі аналогічна кількості смуг автотраси рис. 6.5. Кількість смуг автотраси – це кількість автомобілів, які мо-

жуть одночасно їхати по трасі.Траса з вісьма смугами може пропустити в чотири рази більше автомобілів, чомудвохсмугова.У цьомуприкладіавтомобілі й вантажівки являють собою дані.

Пропускну здатність можна порівняти з кількістю смуг.



Мережевіпристрої можна порівняти з виїздами на головну дорогу, сигналами світлофора, дорожніми знаками й картами.



Передані дані можна порівняти з автомобілями, що рухаються.

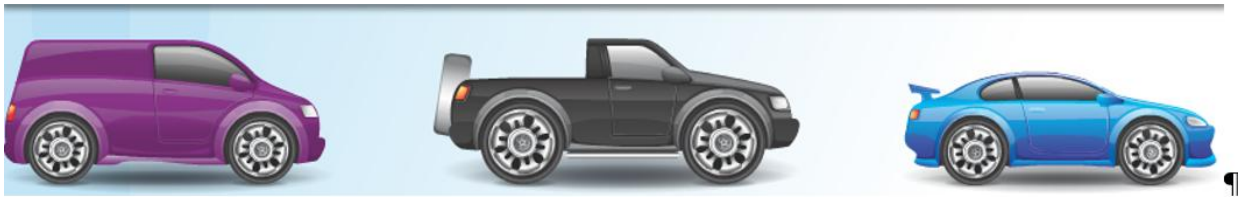


Рис.6.5 – Пропускна спроможність мережі

При передачі даних по комп'ютерній мережі вони розбиваються на невеликі фрагменти, які називаються пакетами. Кожний пакет містить інформацію про адресу джерела й призначення.Пакети відправляються по мережі біт за бітом.Пропускна спроможністьмережі виміряється кількістю біт, яке можна передати за одну секунду.Нижче наведені одиниці вимірупропускноїспроможності:

- біт/с – біт у секунду
- Кбіт/с – кілобіт у секунду
- Мбіт/с – мегабіт у секунду
- Гбіт/с – гігабіт у секунду

Примітка. 1 байтрівний 8 бітаміпозначаєтьсязаголовною буквою Б.Цепозначеннязвичайне використовується при описі розміруфайлуабо ємності сховища, наприклад: файлрозміром 2,5 МБ абодиск ємністю 2 ТБ.

Кількість часу, яка витрачається на передачу даних від джерела одержувачеві, називається затримкою.На шляхуавтомобіля по місту зустрічаються червоні сигнали світлофора або об'їзди.Передача даних уповільнюється залежно від мережевихпристроїв і довжини кабелів. Мережевіпристрої збільшують затримку при обробці й пересиланню даних.При пошуку в Інтернеті або завантаженні файлу затримка, як правило, не викликає яких-небудь проблем. Додатки, для яких важлива швидкодія, наприклад додатки для телефонних і відео-дзвінків через Інтернет, а також відеогри, можуть сильно страждати від затримок.

6.1.1.7Передача даних

Дані можуть передаватися по мережі в одному із трьох режимів: симплексному (однобічному), напівдуплексному або повнодуплексному (дуплексний – двосторонній) рис. 6.6.

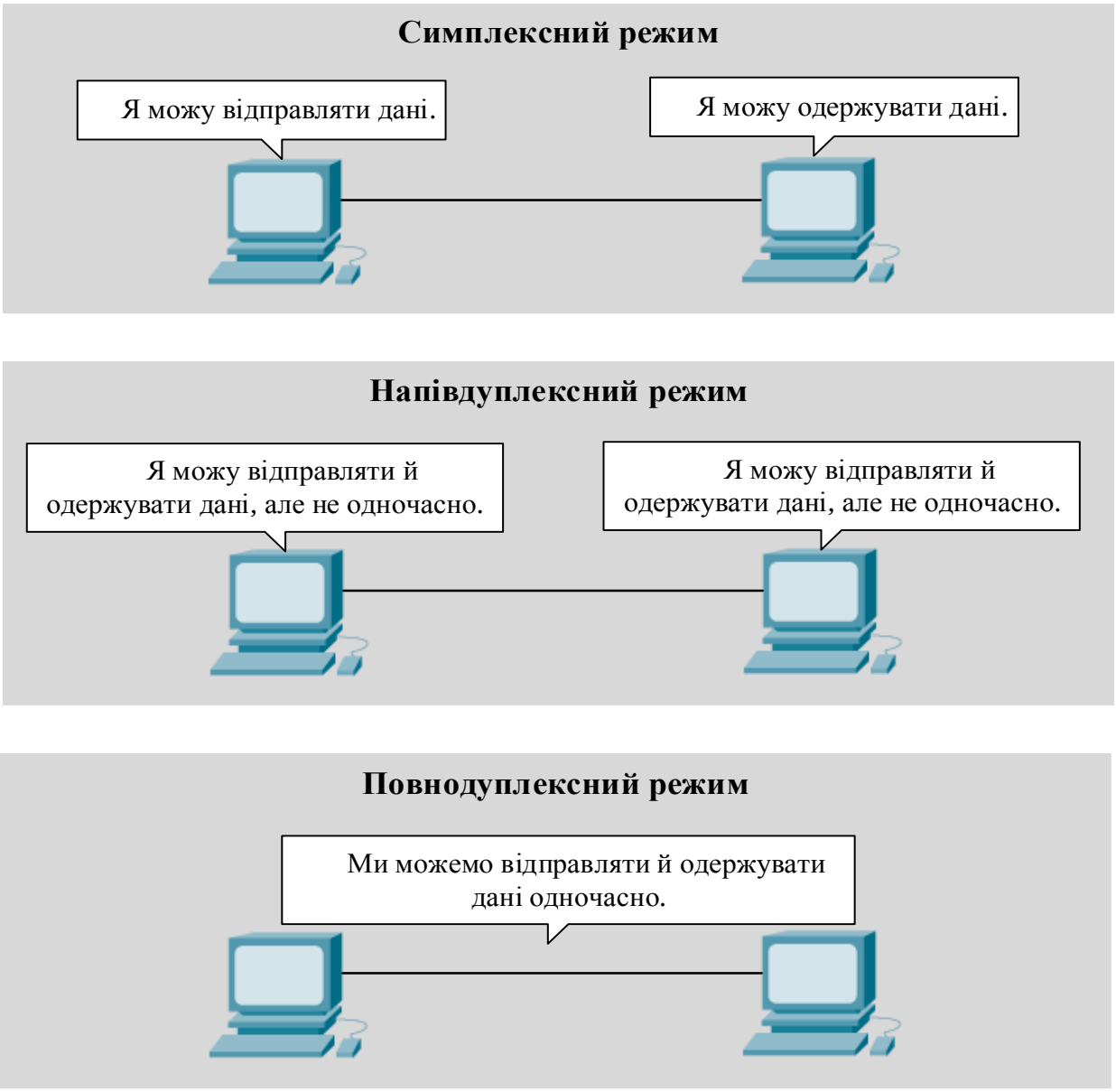


Рис.6.6 – Режими передачі даних

Симплексний режим являє собою передачу даних єдиним потоком в одному напрямку. Прикладом симплексної передачі є сигнал, що відправляється з телевізійної станції на домашній телевізор.

Напівдуплексний режим – це передача даних, при якій у кожний момент часу можна відправляти повідомлення тільки в одному напрямку, називається напівдуплексної, як показано на рис. 6.6. При напівдуплексній передачі канал зв'язку дозволяє виконувати передачу в обох напрямках, але не одночасно. Двосторонні радіоканали, наприклад поліцейський або аварійний мобільний радіозв'язок, працюють у напівдуплексному режимі. Якщо натиснута кнопка на мікрофоні для передачі даних, неможливо почути співрозмовника на іншому кінці. Якщо користувачі на обох кінцях спробують говорити одночасно, передати дані не вдасться.

Повнодуплексний режиміснує колипередача даних в обох напрямках одночасно називається повнодуплексной, як показано на рис. 6.6. Прикладом повнодуплексного зв'язку є телефонний зв'язок. Обидва співрозмовника можуть говорити й слухати одночасно.

Повнодуплексна мережева технологія підвищує продуктивність мережі, оскільки дозволяє одержувати й відправляти дані одночасно. Широкосмугові технології, такі як цифрова абонентська лінія (DSL) і кабельне підключення, функціонують у повнодуплексному режимі. Широкосмугові технології дозволяють одночасно передавати кілька сигналів по одному проводу. Наприклад, при використанні підключення DSL користувачі можуть одночасно завантажувати дані на комп'ютер і говорити по телефону.

6.1.2 Типи мереж

6.1.2.1 Локальні мережі

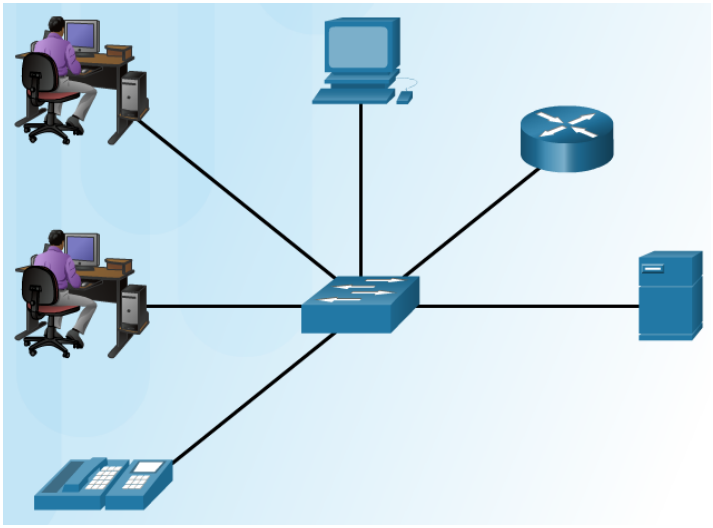


Рис.6.7 – Локальна мережа (LAN)

Комп'ютерні мережівідрізняються наступними специфічними характеристиками:

- Площа покриття
- Кількість підключених користувачів
- Кількість і типи доступних служб
- Область відповідальності

Локальна мережа (LAN) представлена на рис. 6.7

Традиційно**локальна мережа (LAN)** визначається

як мережа, що охоплює невеликугеографічну область. Однак характерною рисою сучасної локальної мережіє те, що вона звичайно належить одній людині, наприклад хазяїнові вдома або малого підприємства, або управляється ІТ-відділом, наприклад у школі або компанії.Ця людина або група застосовують до мережі політики безпеки й контролю доступу.

6.1.2.2Безпроводові локальні мережі

Бепроводова локальна мережа (WLAN) – це локальна мережа, у якій для передачі даних між безпроводовими пристроями використовуються радіохвилі. У традиційній локальній мережі (LAN) пристрої підключені друг до друга за допомогою мідних кабелів. У деяких середовищах прокладка мідних кабелів може бути недоцільна, небажана й навіть неможлива. У цих ситуаціях використовуються безпроводові пристрої для передачі й приймання даних за допомогою радіохвиль. Як і локальні мережі, безпроводові локальні мережі надають загальний доступ до ресурсів, таким як файли й принтери, а також доступ до Інтернету.

Безпроводові локальні мережі можуть працювати у двох режимах. В інфраструктурному режимі (Infrastructure) безпроводові клієнти підключаються до безпроводового маршрутизатора або точки доступу (AP). Точка доступу, показана на рис. 6.8, підключена до комутатора, який забезпечує доступ до іншої частини мережі й Інтернету.

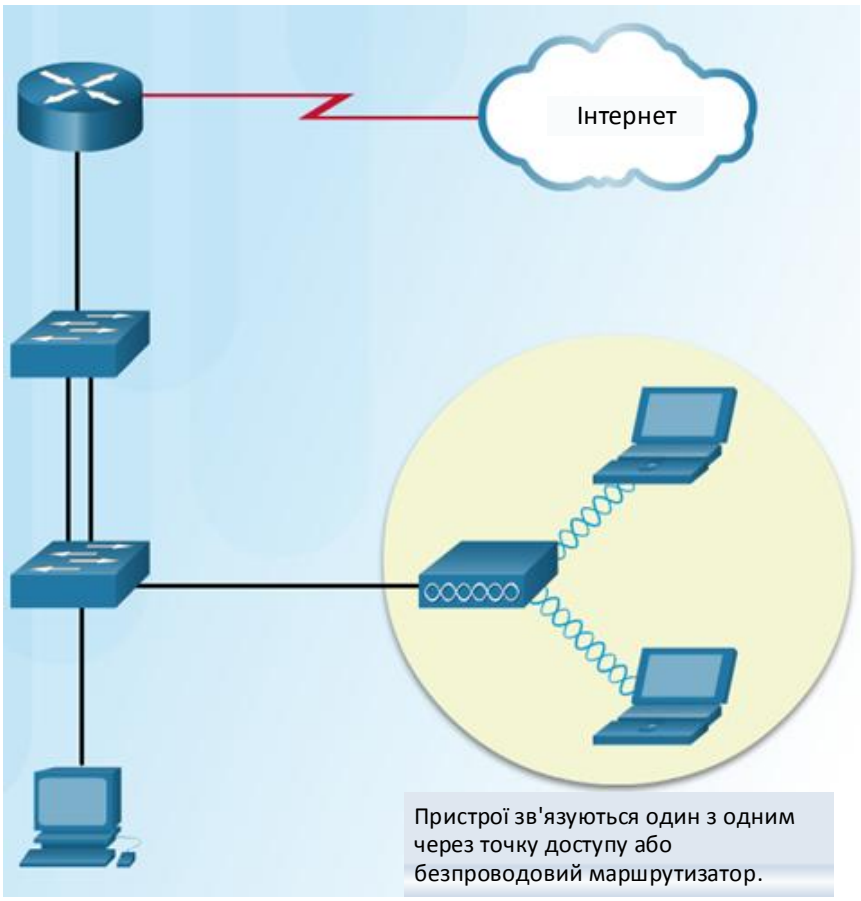


Рис.6.8 – Інфраструктурний режим

Точки доступу, як правило, підключаються до мережі за допомогою мідних кабелів. За допомогою мідного кабелю підключається тільки точка доступу, а не всі клієнти мережі. Дальність дії (радіус покриття) типових систем WLAN варіюється від 30 м у приміщенні до набагато більшої відстані при розгортанні поза приміщеннями, залежно від використовуваної технології.

Режим Ad Hoc (прямого подключения) означает, что сеть WLAN создается по мере необходимости. Обычно сети Ad Hoc создаются на некоторое время. На рис. 6.9 показан пример режима Ad Hoc. Ноутбук подключен по беспроводной сети к смартфону, имеющему доступ к Интернету через поставщика сотовой связи.



Рис.6.9 – Режим AdHoc

6.1.2.3Персональні мережі

Персональна мережа (PAN) підключає пристрої, такі як миші, клавіатури, принтери, смартфони й планшетні ПК, що перебувають у межах досяжності окремого користувача рис. 6.10. Усі ці пристрої підключаються до одного вузла, найчастіше за допомогою технології Bluetooth.



Рис.6.10 – Персональна мережа (PAM)

Bluetooth – це технологія безпроводового зв'язку, що дозволяє пристроям обмінюватися даними на невеликих відстанях. До одному пристрою з підтримкою Bluetooth можна підключити до семи інших пристроїв з підтримкою Bluetooth. Пристрої Bluetooth, описані в стандарті IEEE 802.15.1, здатні обробляти голос і дані. Пристрої з підтримкою Bluetooth працюють у радіочастотному діапазоні від 2,4 до 2,485 ГГц, тобто в так званому діапазоні для використання в промислових, наукових і медичних цілях (Industrial, Scientific, and Medical – ISM). Стандарт Bluetooth містить у собі технологію адаптивної перебудови частоти (Adaptive Frequency Hopping – AFH). Технологія AFH дозволяє «перекидати» сигнали на різні частоти в діапазоні Bluetooth, знижуючи в такий спосіб можливість виникнення перешкод при використанні декількох пристроїв Bluetooth.

6.1.2.4Муніципальні мережі (MAN)

Муніципальна мережа (MetropolitanAreaNetwork – MAN) – це мережа, щорозгортаєтьсяу великому комплексі будинків абонатериторіїцілогомістарис. 6.11.

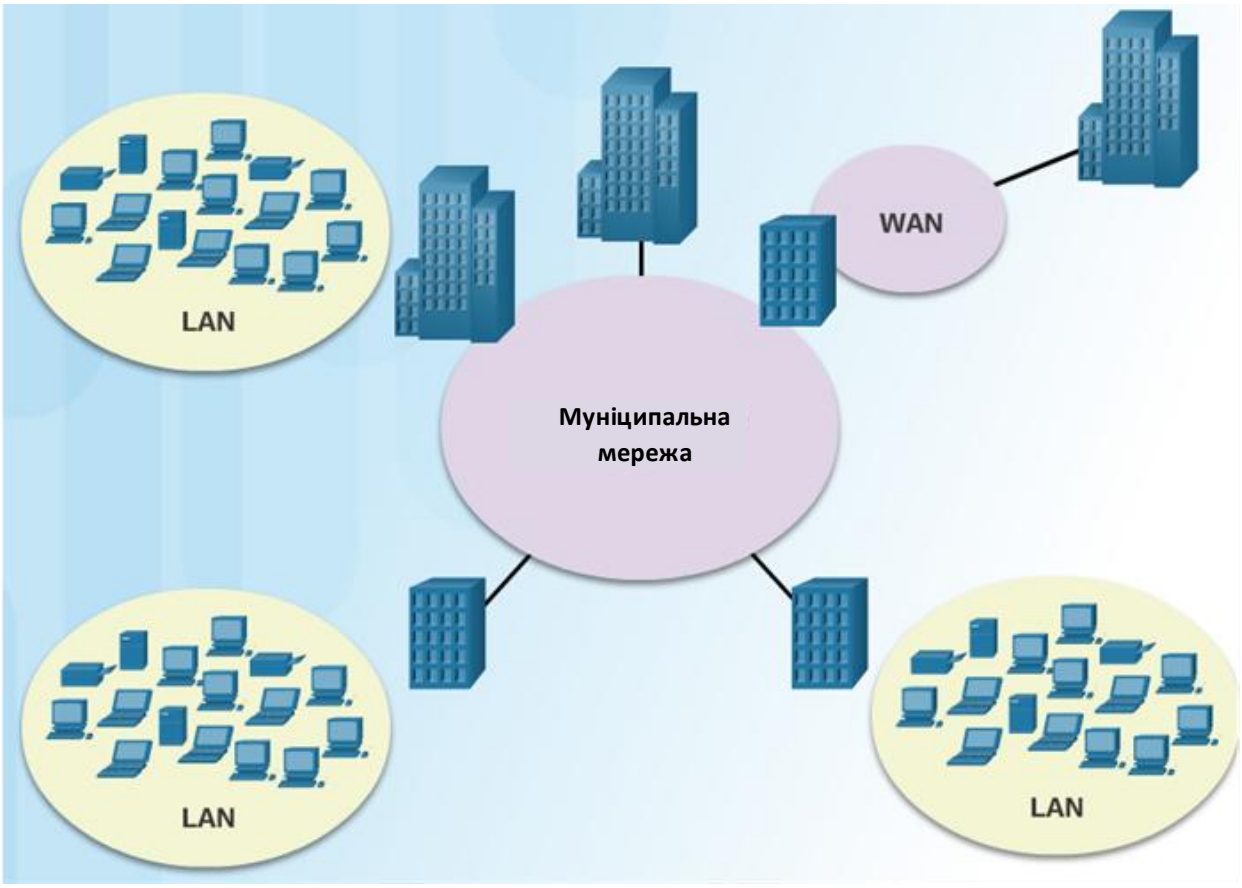


Рис.6.11 – Муніципальна мережа (MAN)

Мережа цього типу складається з різних будинків, підключених друг до друга за допомогою безпроводових або волоконне-оптичних магістральних каналів.Канали зв'язку й устаткування, як правило, є власні-

стю об'єднання користувачів або постачальника мережевих послуг (провайдера), який продає послуги користувачам.Муніципальна мережа може функціонувати в якості високошвидкісної мережі, що надаєзагальний доступ до регіональних ресурсів.

6.1.2.5 Глобальні мережі

Глобальна мережа (WAN)з'єднуєкількалокальних мереж, розташованих у різних географічнихмісцях розташування. Характерною рисою глобальної мережіє те, що вона належить операторові зв'язку рис. 6.12. Окремі особи й організації містять контракти на використання сервісів WAN.Найпоширенішим прикладом мережі WAN є Інтернет.Інтернет – це велика мережа WAN, що полягає з мільйонів взаємно підключених мереж.На рис. 6.12 зображені мережі Лондон й Харків, підключені друг до друга через Інтернет.

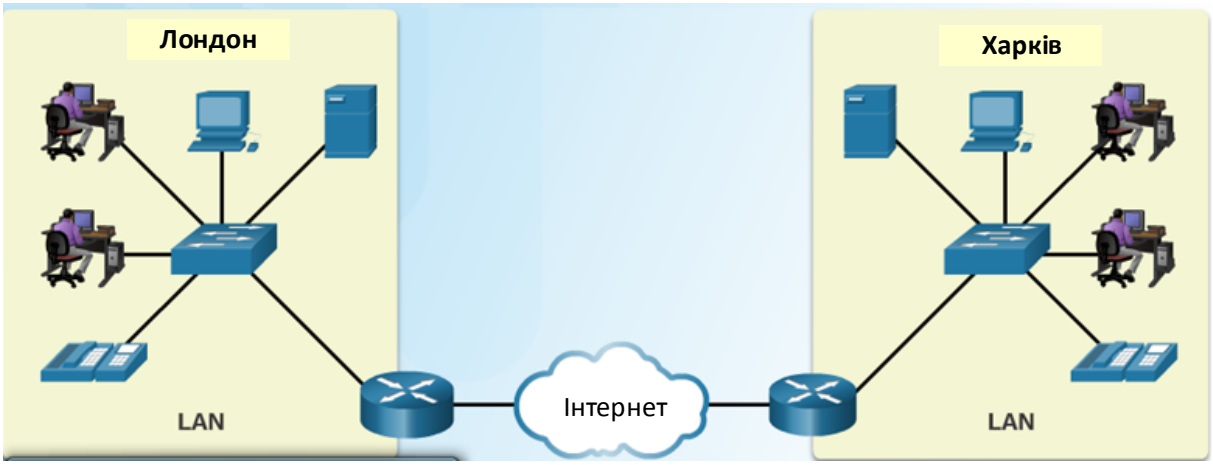


Рис.6.12– Глобальна мережа (WAN)

6.1.2.6 Одноранговімережі

В одноранговій мережі (peer-to-peer network) відсутня ієрархія комп'ютерів і немає виділених серверів рис. 6.13.

Усіпристрої, які також називаються клієнтами, мають рівні можливості й обов'язки.Окремі користувачі відповідають за свої ресурси й можуть самостійно вирішувати, які дані й пристрої встановлювати й до яких даних і пристроївнадаватизагальний доступ.Оскільки окремі користувачі відповідають за ресурси на своїх комп'ютерах, у мережі відсутня центральна точкауправління або адміністрування.

Одноранговімережі є оптимальним варіантом для середовищ, що нараховують не більш десяти комп'ютерів. Одноранговімережі також можуть існувати усередині більших мереж. Навіть у більших клієнтських мережах користувачі можуть обмінюватися ресурсами прямо з іншими користувачами без допомоги мережного сервера. Якщо в домашній мережі кілька комп'ютерів, можна настроїти одноранговумережу. Як показано на малюнку, користувачі цих комп'ютерів зможуть спільно викори-

стовувати файли, відправляти й одержувати повідомлення, а також друкувати документи за допомогою загального принтера.

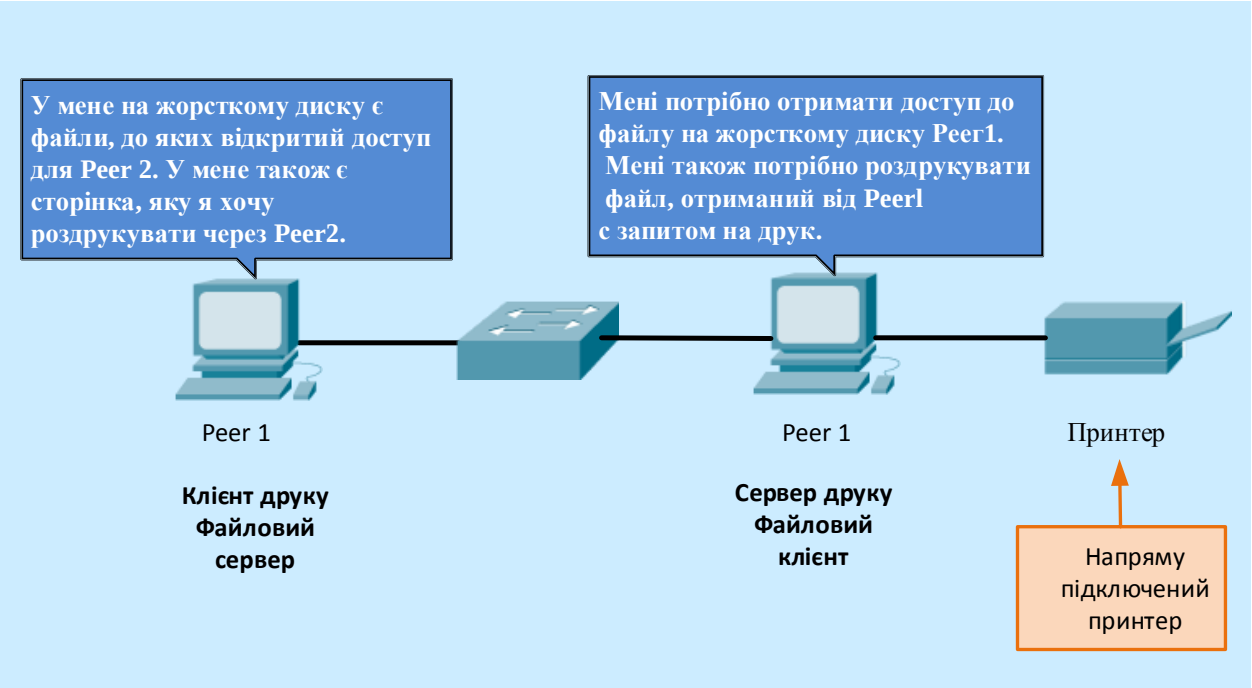


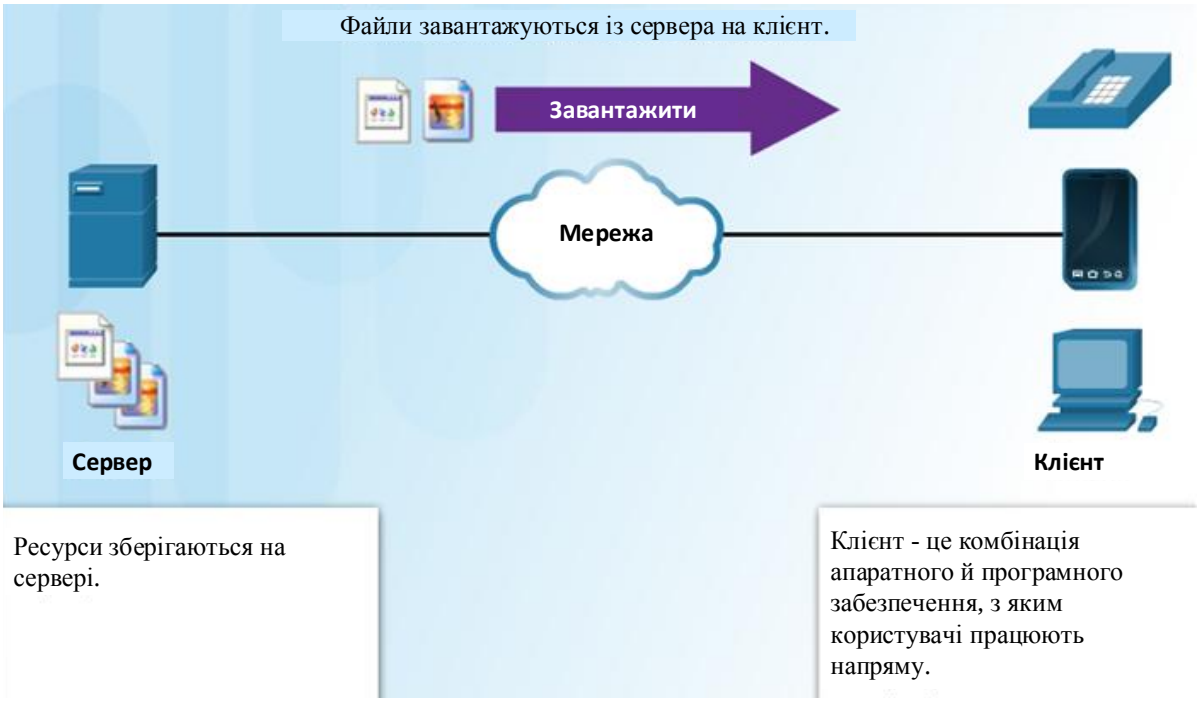
Рис.6.13 – Приклад однорангової мережі

Одноранговi мережі мають ряд недоліків.

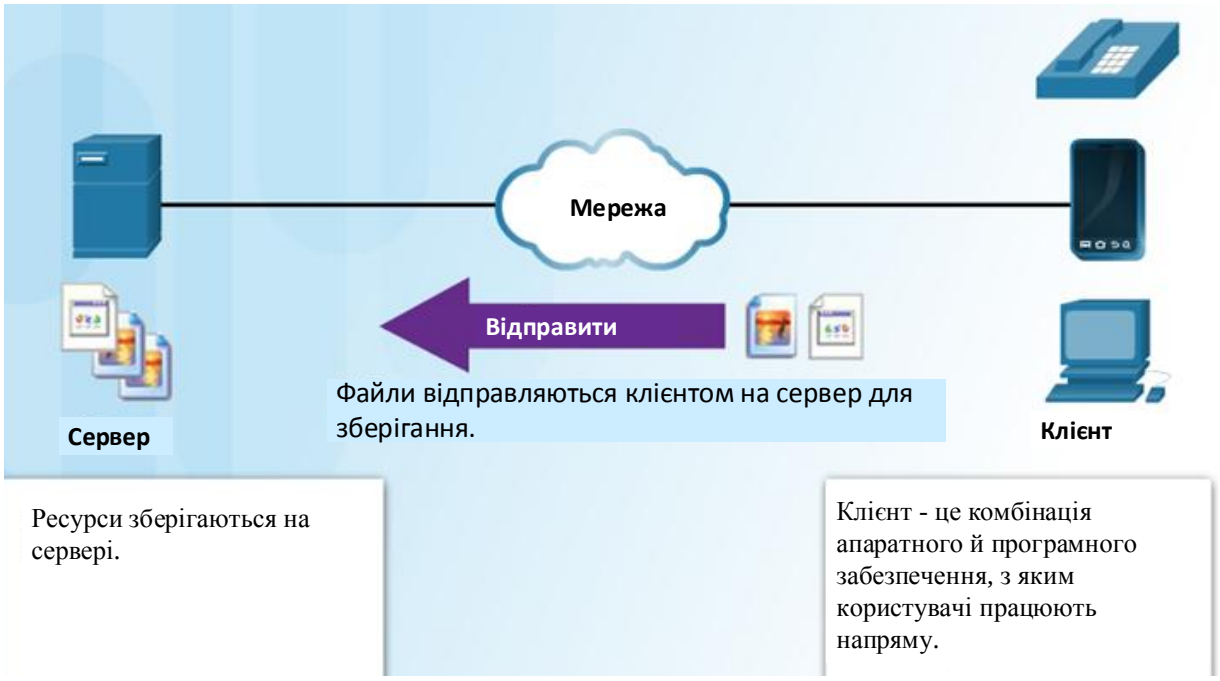
- Відсутнє централізоване адміністрування мережі. Це утруднює визначення користувачів, що контролюють ресурси в цій мережі.
- Відсутня централізована система забезпечення безпеки. Кожний комп'ютер використовує окремі засоби забезпечення безпеки для захисту даних.
- Мережа стає усе більш складною й важкоупрваляємою в міру збільшення числа підключених до неї комп'ютерів.
- Швидше за все, у такій мережі не буде централізованої системи зберігання даних. Операції резервного копіювання прийдеться виконувати окремо для кожного комп'ютера. Відповідальність за це буде нести кожний окремий користувач.

6.1.2.7 Клієнт-серверні мережі

На сервери встановлюється програмне забезпечення, що дозволяє їм надавати клієнтам служби, такі як управління файлами, електронна пошта або веб-сторінки. Для роботи кожної служби необхідно окреме серверне програмне забезпечення. Наприклад, серверу на рис. 6.14 а), б) потрібно ПО файлового сервера, щоб надавати клієнтам можливість одержувати й зберігати файли.



а)



б)

Рис.6.14:

а) Приклад. Відправка файлу клієнту з файлового сервера; б)– Приклад. Відправка файлу клієнтом на файловий сервер

У клієнт-серверної мережі клієнт запитує інформацію або служби від сервера. Сервер надає запитану інформацію або служби клієнтові.

Сервери в клієнт– серверної мережі звичайно виконують певні завдання обробки даних для клієнтських комп'ютерів. Наприклад, сервер може здійснювати пошук по базі даних, а потім відправляти клієнтові запитані записи.

На одному сервері можна одночасно встановити кілька типів серверного ПО. У домашні або невеликих корпоративних мережах одному комп'ютеру доводиться виступати в якості файлового сервера, веб-сервера й сервера електронної пошти. Крім того, на клієнтському комп'ютері можна запускати кілька типів клієнтського програмного забезпечення. Необхідно встановити клієнтське ПО для кожної служби. При установці декількох клієнтських програм клієнт зможе одночасно підключатися до декільком серверам. Наприклад, у користувача є можливість перевіряти електронну пошту, переглядати веб-сторінки, обмінюватися миттєвими повідомленнями й слухати інтернет-радіо.

У клієнт-серверної мережі ресурси контролюються шляхом централізованого мережного адміністрування. Адміністратор мережі виконує резервне копіювання даних і застосовує заходу забезпечення безпеки. Адміністратор мережі також контролює доступ користувачів до ресурсів сервера.

6.1.2.8 Зіставлення типів мереж

Зіставлення типів мереж наведене до табл. 6.2

Таблиця 6.2 – Зіставлення типів мереж

Тип мережі	Опис
Персональна мережа (PAN)	Мережі цього типу підключають пристрої в межах досяжності окремого користувача. Усі ці пристрої підключаються до одному вузлу.
Однорангова мережа	У цій мережі відсутня ієрархія комп'ютерів і немає виділених серверів. Усі клієнти мають рівні можливості й обов'язками.
Локальна мережа (LAN)	Ця мережа охоплює невелику географічну область, і, як правило, належить одній людині або управляється IT-Відділом.
Муніципальна мережа (MAN)	Мережа цього типу охоплює великий комплекс будинків або ціле місто й складається з різних будинків, підключених друг до друга за допомогою безпроводових або волоконне-оптичних магістральних каналів.
Безпроводова локальна мережа (WLAN)	Мережа, у якій для передачі даних між безпроводовими пристроями використовуються радіохвилі. Ця мережа може працювати в інфраструктурному режимі або режимі AD hoc.
Глобальна мережа (WAN)	Мережа, що з'єднує кілька локальних мереж, розташованих у різних географічних місцях розташування.
Клієнт-Серверна мережа	Мережа, у якій вузли запитують інформацію або службу в сервера. Сервер надає вузлам запитану інформацію або службу.

6.2 Мережеві стандарти

6.2.1 Еталонні моделі

6.2.1.1 Відкриті стандарти

Відкриті стандарти сприяють сумісності, конкуренції й інноваціям. Крім того, вони гарантують, що продукт окремої компанії не зможе монополізувати ринок або одержати несправедливу перевагу в порівнянні з конкурентами.

Гарний приклад – покупка безпроводового маршрутизатора для будинку. Існує безліч варіантів маршрутизаторів від різних виробників. Усі вони підтримують стандартні протоколи, такі як протокол Інтернет версії 4 (Ipv4), протокол динамічного настроювання вузла (DHCP), 802.3 (Ethernet) і 802.11 (безпроводові локальні мережі). Ці відкриті стандарти й протоколи розглядатися далі в цій главі. Вони дозволяють клієнтові з операційною системою Apple X від компанії Apple завантажувати веб-сторінки з веб-сервера, що працює під управлінням операційної системи Linux. Це пов'язане з тим, що обидві операційні системи використовують відкриті стандартні протоколи.



Рис.6.15 – Логотипи веб-сайтів організацій по стандартизації

Кілька міжнародних організацій по стандартах відповідальні за розробку мережевих стандартів. На рис. 6.15 представлені логотипи веб-сайтів організацій по стандартизації.

6.2.1.2 Протоколи

Протокол являє собою набір правил. Протоколи Інтернету – це набори правил, що регулюють обмін даними між комп'ютерами в мережі. Специфікації протоколу визначають формат повідомлень, що брав участь в обміні.

Для надійної доставки пакетів важливі строки. Згідно із протоколами, повідомлення повинні надходити протягом певних проміжків часу, щоб комп'ютерам не доводилося чекати повідомлення нескінченно, наприклад якщо повідомлення згубилися. При передачі даних системи використовують один або кілька таймерів.

Протоколи також ініціюють додаткові дії, якщо мережа не вкладається в час, визначений правилами.

Основні функції протоколів:

- Ідентифікація й обробка помилок;
- Стиск даних;
- Визначення порядку поділуданих і формування пакетів;
- Призначення адрес пакетам даних;
- Визначення порядку оголошення відправлення й одержання пакетів даних.

6.2.1.3 Еталонна модель OSI

На початку 80-х років Міжнародна організація по стандартах (ISO) розробила еталонну модель взаємодії відкритих систем (OSI) для стандартизації способу зв'язку пристроїв у мережі. Ця модель була важливим кроком до забезпечення взаємодії між мережевими пристроями.

Модель OSI ділить зв'язок у мережі на сім рівнів, як показано в табл. 6.3. Хоча існують і інші моделі, сьогодні більшість постачальників мереж створюють свої продукти з використанням цієї платформи.

Таблиця 6.3 – Модель OSI

Модель OSI	Рівень	Опис
Рівень додатків	7	Відповідає за надання мережевих служб додаткам
Рівень вистави	6	Перетворює формати даних, щоб забезпечити рівню додатків стандартний інтерфейс
Сеансовий рівень	5	Установлює й завершує підключення між локальними й вилученими додатками, а також управляє ними
Транспортний рівень	4	Надає надійний транспорт і управління потоком при передачі даних по мережі
Мережевий рівень	3	Відповідає за логічну адресацію й маршрутизацію
Канальний рівень	2	Забезпечує фізичну адресацію й управляє доступом до середовища передачі даних
Фізичний рівень	1	Визначає всі електричні й фізичні вимоги до пристроїв

Примітка. Мнемоніка допомагає запам'ятати сім шарів моделі OSI. От два приклади: All People Seem To Need Data Processing і Please Do Not Throw Sausage Pizza Away. Існують і російськомовні варіанти: «Футбольний Клуб Спартак? Тільки Слабких Звикли Перемагати!» і «Прикладом представник сеансу транспортував мережу по каналу фізично».

6.2.1.4 Модель TCP/IP

Модель TCP/IP була створена дослідниками Міністерства оборони США. Вона складається з рівнів, що виконують необхідні функції по підготовці даних для передачі по мережі. У табл. 6.4 показано чотири рівні моделі TCP/IP.

Таблиця 6.4 – Модель TCP/IP

Рівень TCP/IP	Опис
Рівень додатків	На ньому працюють високорівневі протоколи, такі як SMTP і FTP
Транспортний рівень	Указує, який додаток запросив або одержує дані через зазначені порти
Рівень Інтернет (міжмережевий рівень)	На ньому відбувається IP-Адресація й маршрутизація
Рівень доступу до мережі	На ньому існують MAC-Адресація й фізичні компоненти мережі

Назва моделі TCP/IP містить назви двох важливих протоколів транспортного рівня – TCP (протокол керування передачею) і IP (протокол міжмережевого обміну). Протокол TCP відповідає за надійну доставку пакетів. Протокол IP забезпечує додавання адрес джерела й призначення до даних. Однак модель TCP/IP містить у собі безліч інших протоколів, крім TCP і IP. Ці протоколи утворюютьпровідний стандарт передачі даних по мережах і через Інтернет.

У табл. 6.5 показані деякі з найбільш популярних протоколів моделі TCP/IP. Клацніть кожний з них для одержання більш докладної інформації.

Таблиця 6.5 – Протоколимоделі TCP/IP

<table>
<tr><td rowspan="2">Рівень додатків</td><td>Система імен</td><td>Конфігурація вузла</td><td>Эл. Пошта</td><td>Передача файлів</td><td>Веб</td></tr>
<tr><td>DNS</td><td>BOOTP
DHCP</td><td>SMTP
POP
IMAP</td><td>FTP
TFTP</td><td>HTTP</td></tr>
<tr><td>Транспортний рівень</td><td colspan="2">UDP</td><td colspan="3">TCP</td></tr>
<tr><td>Міжмережевий рівень</td><td>IP
NAT</td><td>Підтримка IP
ICMP</td><td colspan="3">Протоколи маршрутизації
OSPF EIGRP</td></tr>
<tr><td>Рівень доступу до мережі</td><td colspan="5">ARP PPP Ethernet Драйвери інтерфейсів</td></tr>
<tr><td colspan="6">Система (або служба) доменних імен (Domain Name System або Service, DNS)
Перетворить імена доменів, наприклад cisco.com, в IP-Адреси.</td></tr>
</table>

6.2.1.5 Протокольний блок даних (PDU)

Дані – загальний термін для позначення PDU, використовуваної на прикладному рівні

Сегмент – PDU транспортного рівня

Пакет – PDU мережного рівня

Кадр – PDU рівня каналу даних (залежить від засобу підключення)

Біти – PDU фізичного рівня, використовувана при фізичній передачі даних по засобу підключення

Повідомлення починається з верхнього прикладного рівня й переходить по рівнях TCP/IP до нижнього рівня мережного доступу. У міру того як дані додатків передаються вниз із одного рівня на інший, на кожному з рівнів до них додається інформація відповідно до протоколів. Це називається процесом інкапсуляції (рис. 6.16).

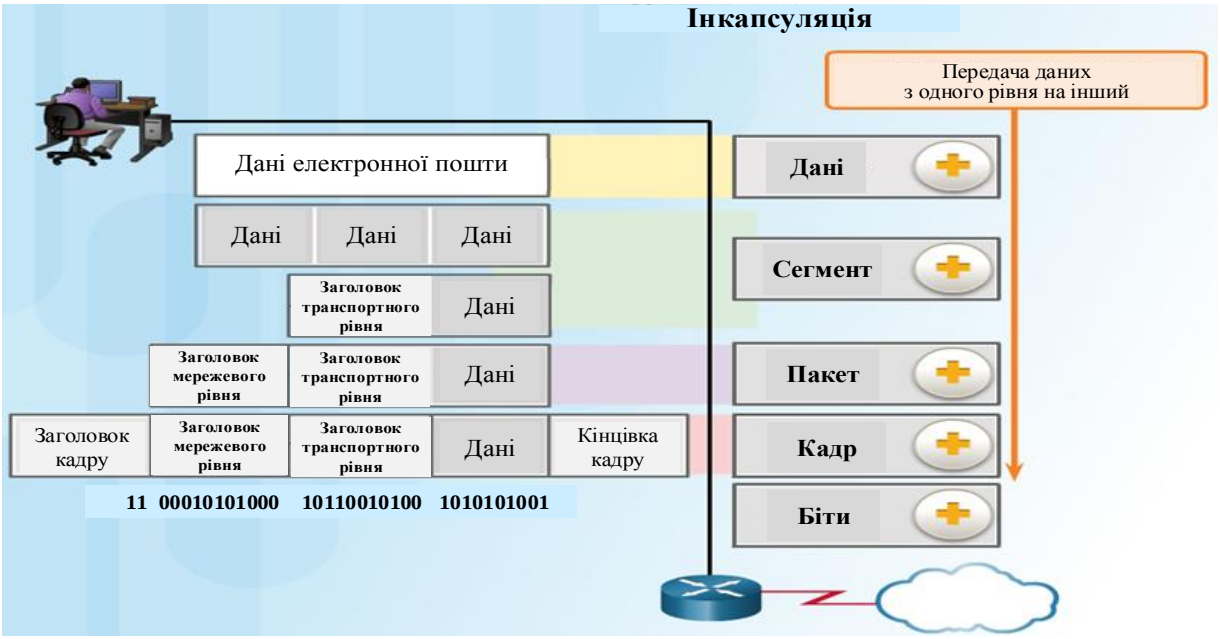


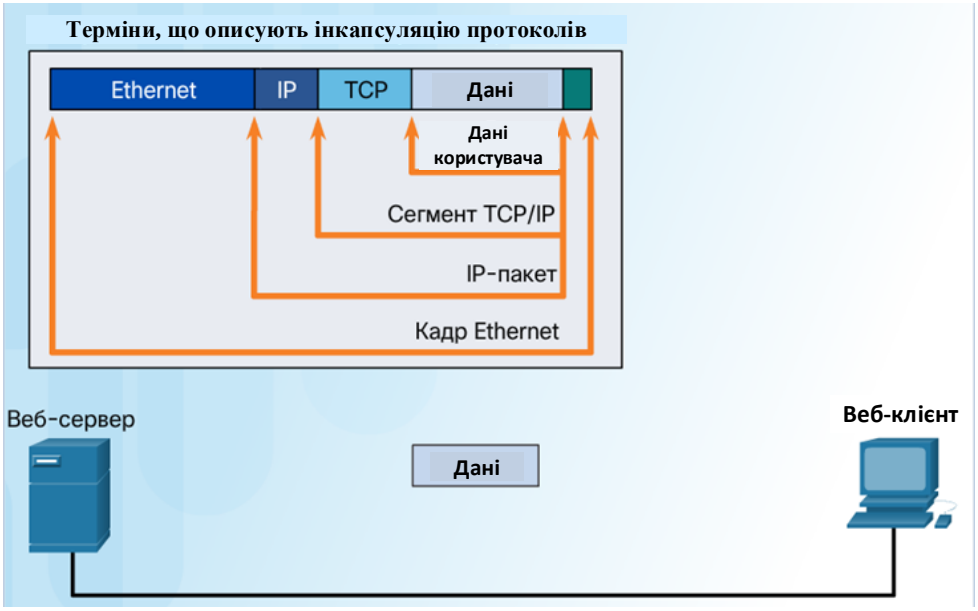
Рис.6.16 – Процес інкапсуляції

Форма, яку ухвалює масив даних на кожному з рівнів, називається протокольним блоком даних (PDU). У ході інкапсуляції кожний наступний рівень інкапсулює PDU, отриману від вищого рівня відповідно до використовуваного протоколу. На кожному етапі процесу PDU одержує інше ім'я, що відбиває нові функції. Універсальної схеми іменування для PDU не має, і в цьому курсі PDU називаються відповідно до термінології набору протоколів TCP/IP, як показано на рис. 6.16.

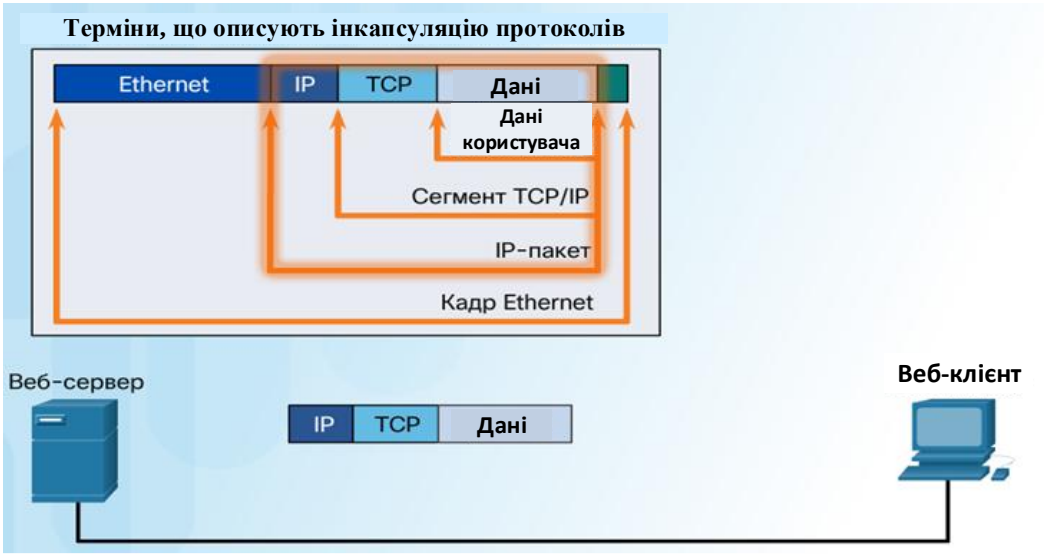
6.2.1.6Приклад інкапсуляції

При відправленні повідомлення по мережі процес інкапсуляції йде від верхнього рівня до нижньогорис. (рис. 6.17, а). Дані на кожному рівні виявляються вкладеними усередину інкапсульованого протоколу. Наприклад, сегмент TCP є частиною даних усередині IP-пакетарис. (рис. 6.17, б). На рис. 6.17, в продемонстроване, як іде процес інкапсуляції, коли веб-сервер відправляє веб-сторінку веб-клієнту.

а)



б)



в)

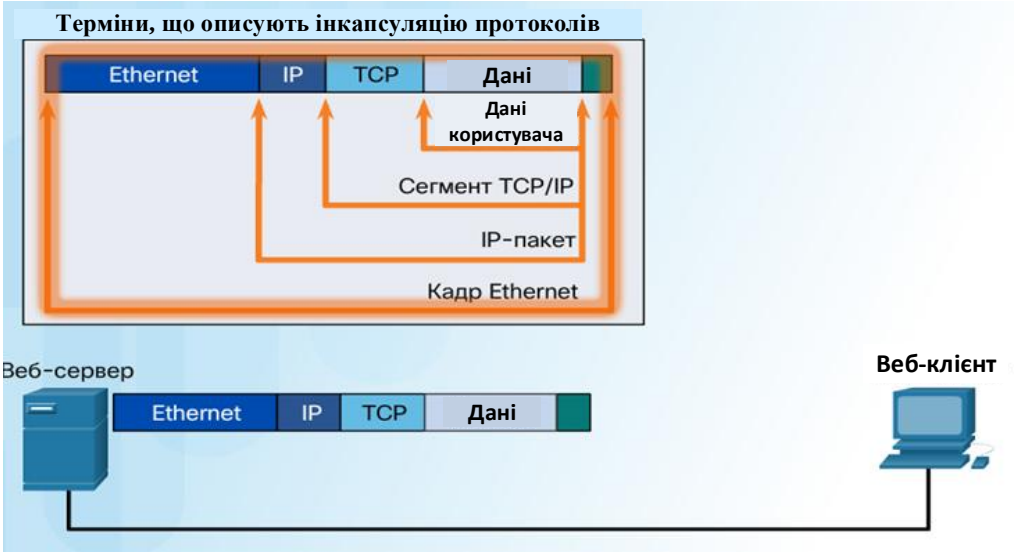


Рис.6.17 – Взаємодія протоколів при відправленні повідомлення

6.2.1.7 Приклад декапсуляції

Зворотний процес на вузлі, що приймає, називається декапсуляцією. Декапсуляція – це процес видалення одного або декількох заголовків пристроєм, що приймає. У міру просування даних нагору з одного рівня на іншій до додатків для кінцевих користувачів вони декапсулюються.

На рис. 6.18 показаний процес декапсуляції.

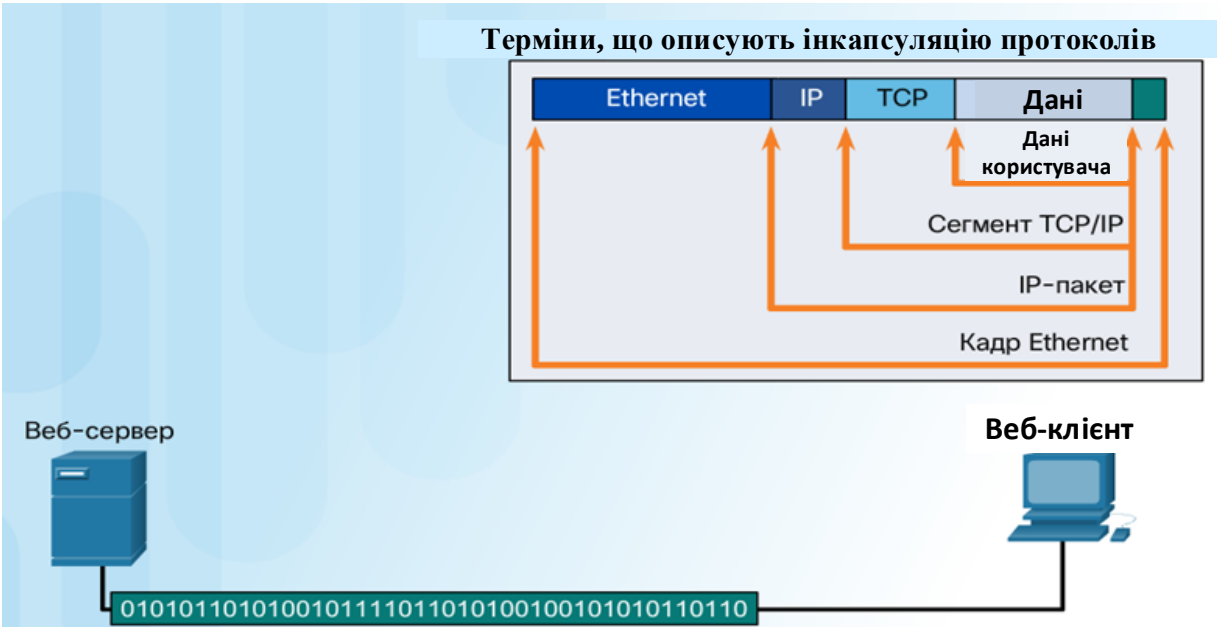


Рис.6.18– Взаємодія протоколів при отриманні повідомлення

6.2.1.8 Порівняння моделей OSI і TCP/IP

Моделі OSI і TCP/IP є еталонними моделями, використовуваними для опису процесу передачі даних. Модель TCP/IP використовується спеціально для набору протоколів TCP/IP, а модель OSI – для розробки стандартів зв'язку для обладнання й додатків різних постачальників.

Модель TCP/IP виконує ту ж процедуру, що й модель OSI, але використовує чотири рівні замість семи. У табл. 6.6 показане порівняння рівнів двох моделей.

Таблиця 6.6 – Порівняння моделей OSI і TCP/IP

Модель OSI		**Модель TCP/IP**
7	Рівень додатків	Рівень додатків
6	Рівень вистави	
5	Сеансовий рівень	
4	Транспортний рівень	Транспортний рівень |
3	Мережний рівень	Міжмережевий рівень |
2	Канальний рівень	Рівень доступу до мережі
1	Фізичний рівень	
Основні подібності стосуються транспортного й мережевого рівнів; однак ці дві моделі по різному працюють із вищими й нижчестоящими рівнями.		

6.2.2 Стандарти Ethernet для проводових і безпроводових мереж

6.2.2.1 CSMA/CD

Протокол Ethernet описує правила управління передачею даних у мережі Ethernet. Щоб забезпечити сумісність усіх пристроїв Ethernet один з одним, IEEE розробила стандарти для виробників і програмістів по розробці пристроїв Ethernet рис. 6.19.



Рис.6.19 – Прослуховування проводу пристроями

Архітектура Ethernet заснована на стандарті IEEE 802.3.Стандарт IEEE 802.3 визначає, що в мережі реалізується спосіб контролю доступу «множинний доступ з контролем несучої й виявленням конфліктів (CSMA/CD)».

- **Несуча** – провідник, використовуванийдляпередачіданих.
- **Контроль** – кожний пристрій прослуховує провідник, щоб визначити, чивільнийвіндляпередачіданих, якпоказанонарис. 6.19.
- **Множиннийдоступ** – у мережі можутьодночаснобути присутнімкілька пристроїв.
- **Виявленняконфліктів** – конфлікт викликає подвоєннянапругина проводі, розпізнаване мережевими платами пристроїв.

В CSMA/CD усіпристроїпрослуховуютьмережевий провідник і чекають, коли він буде вільний для відправлення даних.Цей процес схожий на очікування сигналу готовності лінії на телефоні перед набором номера.Коли пристрійвизначає, що ніякі інші пристрої не передають дані, він намагається відправити дані.Якщо ніякий інший пристрій не відправляє дані в це ж час, передача на комп'ютер призначення відбувається без

проблем.Якщо в цей час інший пристрій виконає передачу, у провіднику виникне конфлікт.

Перша станція, яка виявляє конфлікт, відправляє сигнал наявності конфлікту (jam signal), якийговорить усім вузлам зупинити передачу й запустити алгоритм відновлення після конфлікту.Алгоритм відновлення після конфлікту обчислює випадковий час, після закінчення якого кінцева станція намагається повторити передачу.Звичайно цей випадковий часрівняється 1 або 2 міллісекундам (мс).Ця послідовність відбувається щораз при наявності конфлікту в мережі й може знизити швидкість передачі Ethernet на 40 відсотків.

Примітка. Більшість мереж Ethernet працює в цей час у повнодуплексномурежимі.У такомурежимі Ethernet конфлікти виникають рідко, оскільки пристрої можуть виконувати відправлення й прийманняданих одночасно.

6.2.2.2 Стандарти кабелів Ethernet

Стандарт**IEEE802.3** визначає кількафізичнихреалізацій, щопідтримуютьEthernet. У табл. 6.7 наведене зведення стандартів різних типів кабелів Ethernet.

Таблиця 6.7 – Стандарти Ethernet

Стандарти Ethernet	Середовища передачі даних	Швидкості передачі
10BASE-T	Категорія 3	Передача даних зі швидкістю 10 Мбіт/с.
100BASE-TX	Категорія 5	На швидкості 100 Мбіт/зі швидкості передачі 100BASE-TX вдесятеро вище швидкостей 10BASE-T.
1000BASE-T	Категорія 5е, 6	Архітектура 1000BASE-T підтримує швидкості передачі даних до 1 Гбіт/с.
10GBASE-T	Категорія 6а, 7	Архітектура 10GBASE-T підтримує швидкості передачі даних до 10 Гбіт/с.

1000BASE-T — у цей час найбільш часте реалізована архітектура Ethernet. Її назва містить у собі характеристики стандарту:

- 1000 означає швидкість роботи порту: 1000 Мбіт/с або 1 Гбіт/с.
- BASE означає передачу в основній смузі частот. При передачі в основній смузі частот уся пропускна спроможність кабелю використовується для одного типу сигналу.
- T означає мідний кабель (Twisted pair).

6.2.2.3 CSMA/CA

IEEE802.11 – це стандарт, що визначає зв'язок для безпроводових мереж. У безпроводових мережах застосовується множинний доступ з контролем використання несучої й запобіганням конфліктів (CSMA/CA). CMSA/CA не виявляє конфлікти, а намагається уникнути їх, очікуючи

своєї черги для передачі. Кожний передавальний пристрій включає в кадра відомості про час, необхідний йому для передачі. Усі інші безпроводові пристрої ухвалюють цю інформацію й знають, як довго середовище передачі даних буде зайнято (див.рис. 6.20).Це означає, що безпроводові пристрої працюють у напівдуплексномурежимі. Уточки доступу або безпроводового маршрутизатора ефективність передачі зменшується в міру підключення все більшої кількості пристроїв.



Рис.6.20 – Множинний доступ CSMA/CA

6.2.2.4 Стандарти безпроводової передачі даних

IEEE 802.11, або Wi-Fi, являє собою групу стандартів, які визначають характеристики радіочастотного випромінювання, швидкість передачі й інші параметри безпроводових локальних мереж. За останні роки розроблений ряд реалізацій стандарту IEEE 802.11, показаних у табл. 6.8.

Таблиця 6.8 – Порівняння стандартів 802.11

Стандарт IEEE	Максимальна швидкість	Максимальний радіус дії усередині приміщень	Частота	Зворотна сумісність
802.11a	54 Мбіт/с	35 м	5 ГГц	-
802.11b	11 Мбіт/с	35 м	2,4 ГГц	-
802.11g	54 Мбіт/с	38 м	2,4 ГГц	802.11b
802.11n	600 Мбіт/с	70 м	2,4 ГГц і 5 ГГц	802.11 a/b/g
802.11ac	1,3 Гбіт/с (1300 Мбіт/с)	35 м	5 ГГц	802.11a/n

Канальні параметри прийомного пристрою, малого радіуса дії стандартів IEEE 802.11b/g/n, у тому числі вбудованого або вхідного до складу інших пристроїв наступні:

смуга радіочастот –2400-2483,5 Мгц;

припустима потужність випромінювання передавача не більш – 100 мВт;

кількість каналів – 14;

центральная несуча частота 1 каналу– 2,412 (ГГц);

інтервал частот між каналами – 5 МГц.

Канальні параметри стандартів 802.11a/n/ac наступні:

кількість каналів з 34-го по 180 – 147;

смуга радіочастот – 5170 – 5905 МГц;

центральная несуча частота 34 каналу – 5,170 (ГГц);

інтервал частот між каналами: – 5 МГц.

Стандарти 802.11a, 802.11b і 802.11g слід вважати застарілими.

Нові мережі WLAN повинні містити в собі пристрою, що задовольняють стандарту 802.11ac. В існуючих реалізаціях мереж WLAN рекомендується при придбанні нових пристроїв виконати відновлення до 802.11ac.

6.2.2.5 Безпека безпроводової мережі

Кращий спосіб захисту безпроводових мереж – використання автентифікації й шифрування.У початковомустандарті 802.11 минулого визначено два типи автентифікації, показані на рис. 6.21.

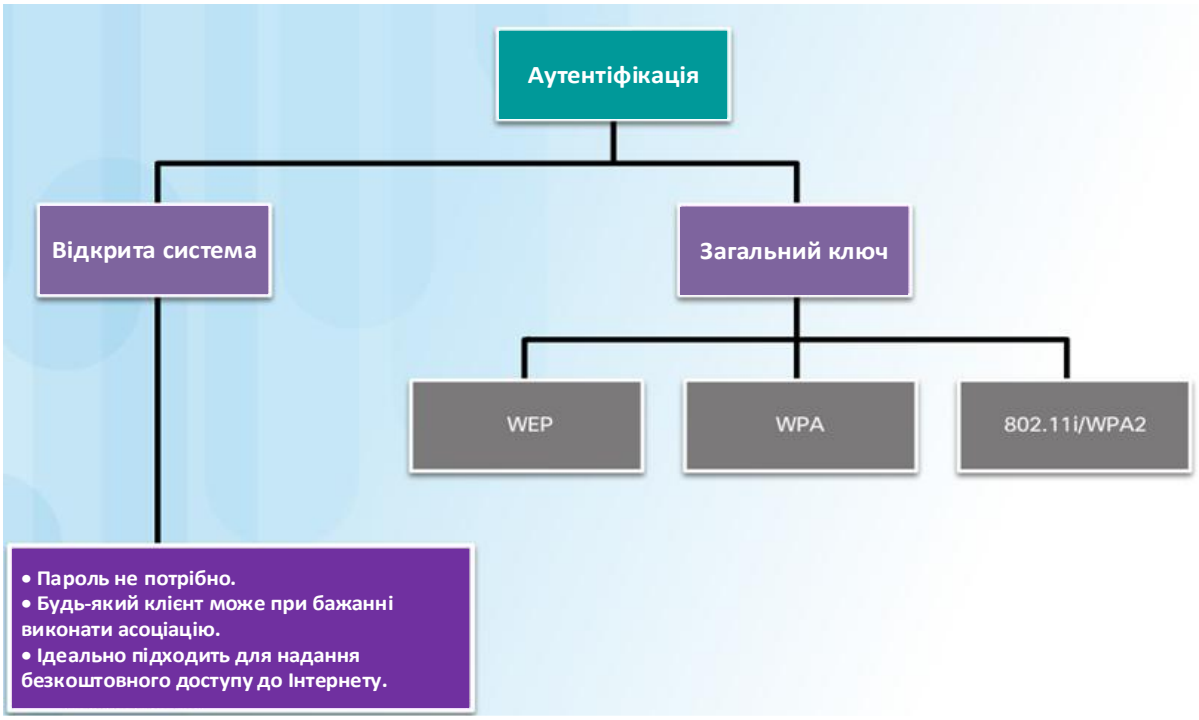


Рис.6.21– Методи автентифікації

- **Автентифікація відкритої системи** — будь-який безпроводовий пристрій може підключитися до безпроводової мережі. Цей тип автентифікації слід використовувати тільки в тих випадках, коли безпека не має значення.
- **Автентифікація за допомогою загального ключа** — надає механізми автентифікації й шифрування даних, переданих між безпроводовим клієнтом і точкою доступу.

У мережах WLAN доступні три варіанти автентифікації за допомогою загальногоключа.

- **Еквівалент таємності проводової мережі (Wired Equivalent Privacy, WEP)** – специфікація забезпечення безпеки WLAN, визначена в
- початковому стандарті 802.11. Однак при передачі пакетів ключ не змінюється, тому його досить легко зламати.
- **Захищений доступ до Wi-Fi (Wi-Fi Protected Access, WPA)** — цей стандарт використовує WEP, але забезпечує захист даних за допомогою набагато більш надійного протоколу шифрування з використанням тимчасових ключів (TKIP). Алгоритм TKIP міняє ключ для кожного пакета, тому його набагато складніше зламати.
- **IEEE802.11i/WPA2** – стандартIEEE 802.11i є в цей час галузевим стандартом безпеки безпроводових мереж.Версія Wi-Fi Alliance називається WPA2.802.11i і WPA2 використовують для шифрування вдосконалений стандарт шифрування (Advanced Encryption Standard, AES).У цей час AES уважається самим надійним протоколом шифрування.

З 2006 року всі пристрої, на які нанесений логотип Wi-Fi Certified, сертифіковані для використання WPA2.Тому сучасні безпроводові мережі завжди повинні використовувати стандарт 802.11i/WPA2.

6.3 Фізичні компонентимережі

6.3.1 Мережеві пристрої

6.3.1.1 Модеми

IT-інженери повинні розуміти призначення й характеристики базових мережевих пристроїв. У цьому розділі розглядаються різні пристрої (рис. 6.22).

Модем підключається до Інтернету через інтернет-провайдера (ISP). Існують три основні типи модемів. Модеми перетворять цифрові комп'ютерні дані у формат, який можна передавати в мережу інтернет-провайдера. Аналоговий модем перетворить цифрові дані в аналогові сигнали й передає їх по телефонній лінії. Модем цифрової абонентської лінії (DSL) з'єднує мережу користувача безпосередньо з інфраструктурою цифрової мережі телефонної компанії. Кабельний модем з'єднує мережу користувача з постачальником послуг кабельного ТВ, який звичай-

но має гібридну мережу (HFC) з волоконне-оптичними й коаксіальними кабелями [7, 8].

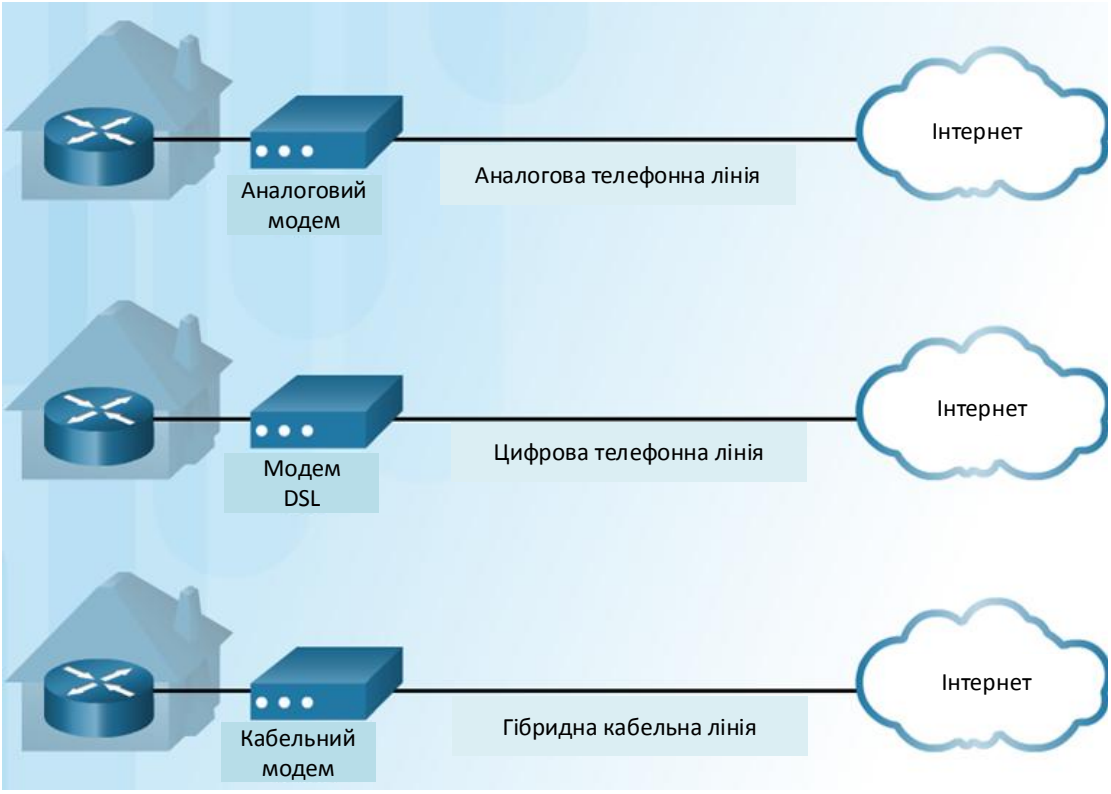


Рис.6.22 – Приклади модемів

6.3.1.2 Концентратори, мости й комутатори

Обладнання, використовуване для підключення пристроїв у локальній мережі, пройшло шлях розвитку від концентраторів до мостів і комутаторів.

Концентратори

Концентратори (hub), показані на рис. 6.23, приймають дані на одному порту, потім відправляють їх на всі інші порти. Концентратор розширює дальність дії мережі, оскільки регенерує (відновлює) електричні сигнали. Крім того, можна підключати концентратори до іншого мережного пристрою, наприклад до комутатора або маршрутизатора, який, у свою чергу, підключений до інших сегментів мережі.

Сьогодні концентратори використовуються рідше, оскільки комутатори є більш ефективними й менш дорогими. Концентратори не виконують сегментацію (поділ) мережевого трафіка. Коли один пристрій відправляє трафік, концентратор передає цей трафік на всі підключені до нього пристрою. Смуга пропущення ділиться між усіма пристроями.

Мости

Мости (bridge) були винайдені для поділу локальних мереж на сегменти. Мости запам'ятовують, які пристрої перебувають у кожному сег-

менті. Тому міст може виконувати фільтрацію мережевого трафіка між сегментами локальної мережі. Це дозволяє зменшити обсяг трафіка між пристроями. Розглянемо приклад на рис. 6.23. Якщо комп'ютеру «PC-A» потрібно відправити завдання на принтер, трафік не буде передано в сегмент 2. Однак сервер теж одержить копію трафіка із завданням для друку.

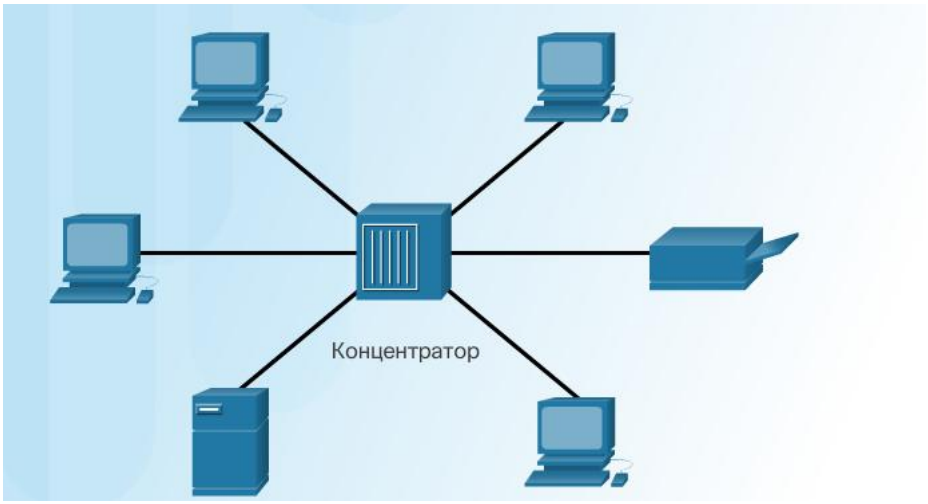


Рис.6.23 – Підключення пристроїв до локальної мережі через концентратори

Комутатори

Мости й концентратори тепер уважаються застарілими пристроями, оскільки комутатори (switch) ефективніше й дешевше рис. 6.24.

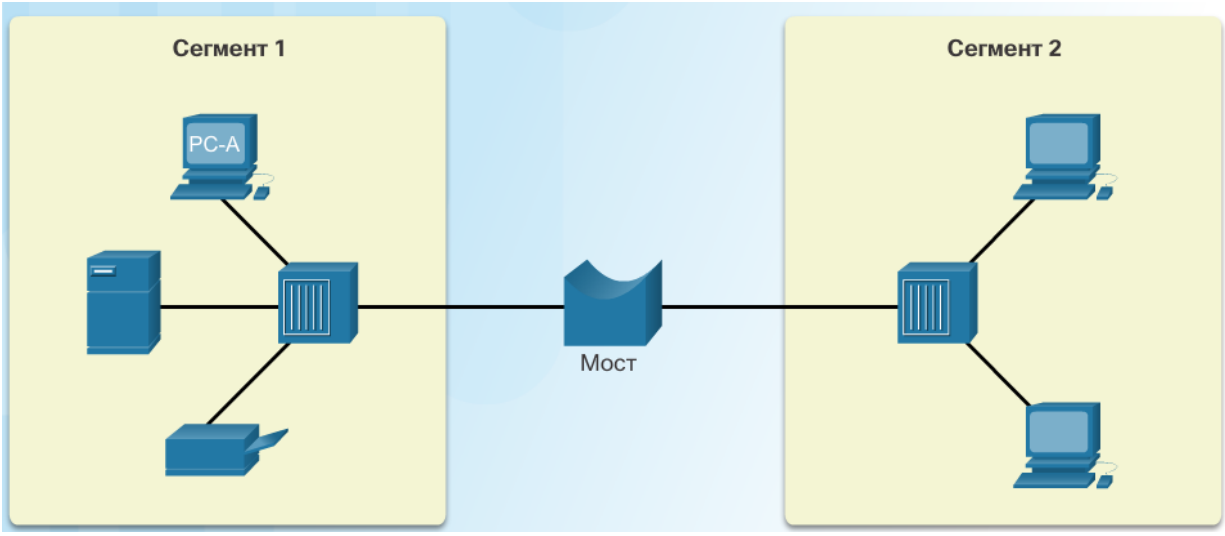


Рис.6.24 – Мости розділяють LANна сегменти

Як показано на рис. 6.25, комутатор виконує мікросегментацію локальної мережі. Мікросегментація означає, що комутатори здійснюють фільтрацію й сегментацію мережевого трафіка, відправляючи дані тіль-

ки на пристрій, якому цей трафік адресований. Такий підхід забезпечує підвищення пропускної спроможності, виділеної для кожного пристрою в мережі. Якщо до кожного порту комутатора підключений тільки один пристрій, він працює в повнодуплексному режимі. У концентраторів такої можливості просто немає. Коли комп'ютер «PC-A» відправляє завдання на принтер, тільки принтер одержить цей трафік.

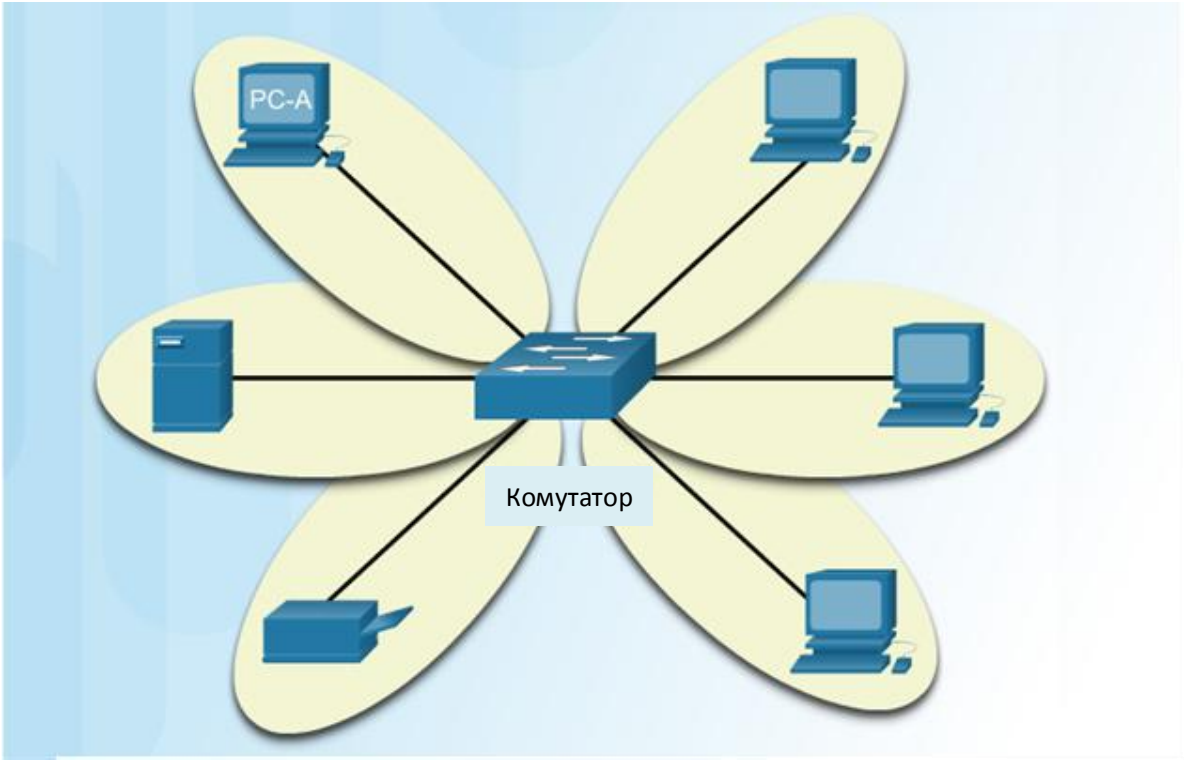


Рис.6.25 – Комутатори здійснюють мікросегментацію мережі LAN

Комутатори ведуть таблицю комутації. Таблиця комутації містить список усіх MAC-адрес мережі, а також список портів комутатора, через які доступні пристрої з певними MAC-адресами. Таблиця комутації запам'ятовує MAC-адреси, записуючи для кожного вхідного кадра MAC-адреси джерела й порт, на який цей кадр прийшов. Після цього комутатор створює таблицю комутації, у якій MAC-адреси зіставляються з вихідними портами. При одержанні трафіка, призначеного для певного MAC-адреси, комутатор за допомогою таблиці комутації визначає, який порт слід використовувати для відправлення повідомлення на цей MAC-адресу. Трафік пересилається одержувачу через цей порт. Відправлення трафіка тільки через один конкретний порт безпосередньо одержувачу дозволяє не впливати на інші порти.

6.3.1.3Точки безпроводового доступу й маршрутизатори

Точки безпроводового доступу, зображені на рис. 6.26, надають доступ до мережі для безпроводових пристроїв, таких як ноутбуки й планшетні ПК.



Точки безпроводового доступу використовують радіохвилі для зв'язку з безпроводовими мережними платами в пристроях і з іншими безпроводовими крапками доступу. Точка безпроводового доступу має обмежену зону покриття. Для забезпечення адекватної зони покриття великомасштабних безпроводових мереж потрібно кілька крапок доступу. Точки безпроводового доступу забезпечують тільки підключення до мережі, у той час як безпроводовий маршрутизатор надає додаткові можливості.

Рис.6.26– Точки безпроводового доступу

Маршрутизатори

Маршрутизатори з'єднують мережі, як показано на рис. 6.27. Комутатори використовують MAC-адреси для пересилання трафіка в рамках однієї мережі. Маршрутизатори використовують IP-адреси для пересилання трафіка в інші мережі. Маршрутизатором може бути комп'ютер зі спеціальним мережевим програмним забезпеченням або пристрій, зібраний виробником обладнання. У великих мережах маршрутизатори підключаються до комутаторів, які підключаються до локальних мереж. Так підключений маршрутизатор праворуч на рис. 6.27. Маршрутизатор виконує функції шлюзу в зовнішні мережі.

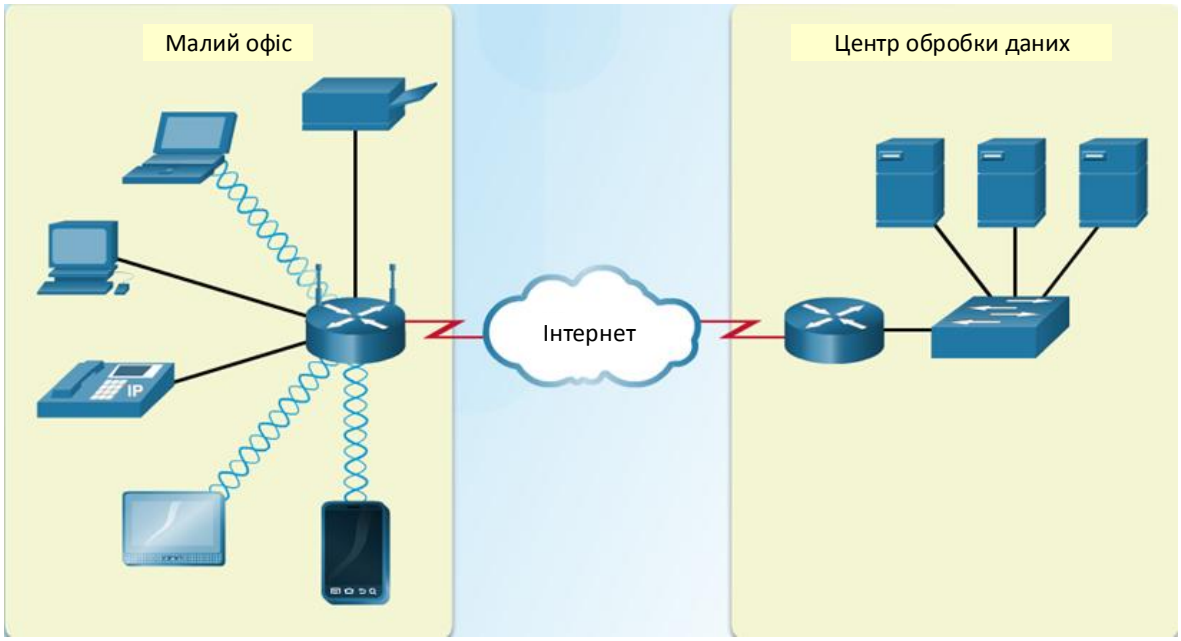


Рис.6.27 – З'єднання мереж маршрутизаторами

Маршрутизатор, зображений ліворуч на рис. 6.27, інакше називається багатофункціональним пристроєм або інтегрованим маршрутизатором. Він поєднує в собі комутатор і точку безпроводового доступу. У деяких випадках зручніше купити й настроїти один пристрій, що відповідає всім потребам, чим купувати окремий пристрій для кожної функції. Це особливо справедливо для невеликого або домашнього офісу. Багатофункціональні пристрої можуть також мати функції модему.

6.3.1.4 Апаратні міжмережеві екрани

Інтегрований маршрутизатор може також служити апаратним міжмережевим екраном. Апаратні міжмережеві екрани захищають дані й обладнання в мережі від несанкціонованого доступу. Апаратний міжмережевий екран розташовується між двома або більш мережами, як показано на рис. 6.28. Він не використовує ресурси комп'ютерів, які захищає, отже, не впливає на продуктивність обробки даних.

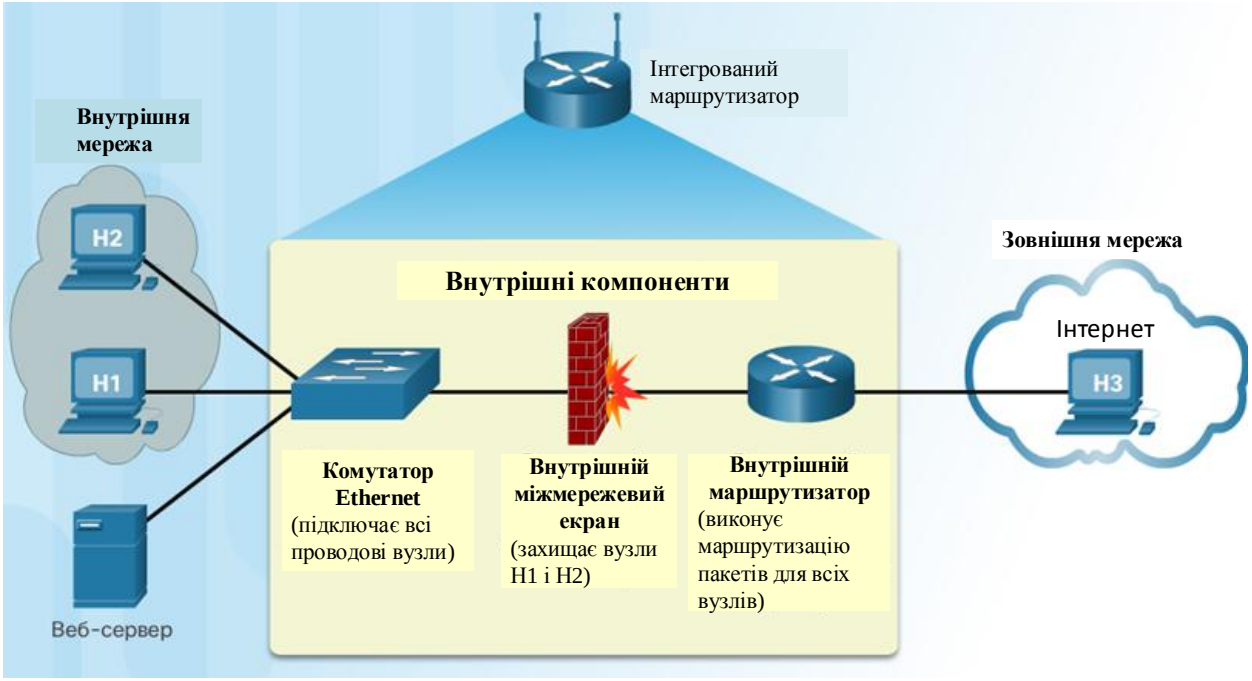


Рис.6.28 – Апаратний міжмережевий екран

У міжмережевих екранах застосовуються різні методи визначення дозволеного й забороненого доступу до сегментів мережі, наприклад список контролю доступу (ACL). Цей список являє собою файл, використовуваний маршрутизатором і утримуючий правила щодо трафіка між мережами. При виборі апаратного міжмережевого екрана слід урахувати наступні аспекти.

- **Займане місце** – пристрій установлюється окремо й використовує спеціалізоване обладнання.
- **Вартість** – початкова вартість оновлення обладнання й ПО може бути досить високої.

- **Число комп'ютерів** – пристрій забезпечує захист декількох комп'ютерів.
- **Вимоги до продуктивності** – незначний вплив на продуктивність комп'ютерів.

Примітка. У захищеній мережі, якщо продуктивність комп'ютерів не є проблемою, включите вбудований міжмережевий екран операційної системи, щоб забезпечити додаткову безпеку. Деякі додатки можуть працювати неправильно, поки для них відповідним чином не буде настроєний міжмережевий екран.

6.3.1.5 Інші пристрої

Комутаційні панелі



Рис.– 6.29 Патч – панель

Комутаційна панель (або патч-панель), показана на рис. 6.29, звичайно використовується, щоб зібрати в одному місці вхідні кабелі від різних мережевих пристроїв. Вона забезпечує точку з'єднання комп'ютерів з комутаторами або маршрутизаторами. Комутаційна панель може мати або не мати живлення. Комутаційна панель із живленням може регенерувати слабкі сигнали перед відправленням їх на наступний пристрій.

Повторювачі

Регенерація слабких сигналів, показана на рис. 6.30, є основною функцією повторювачів (repeater).

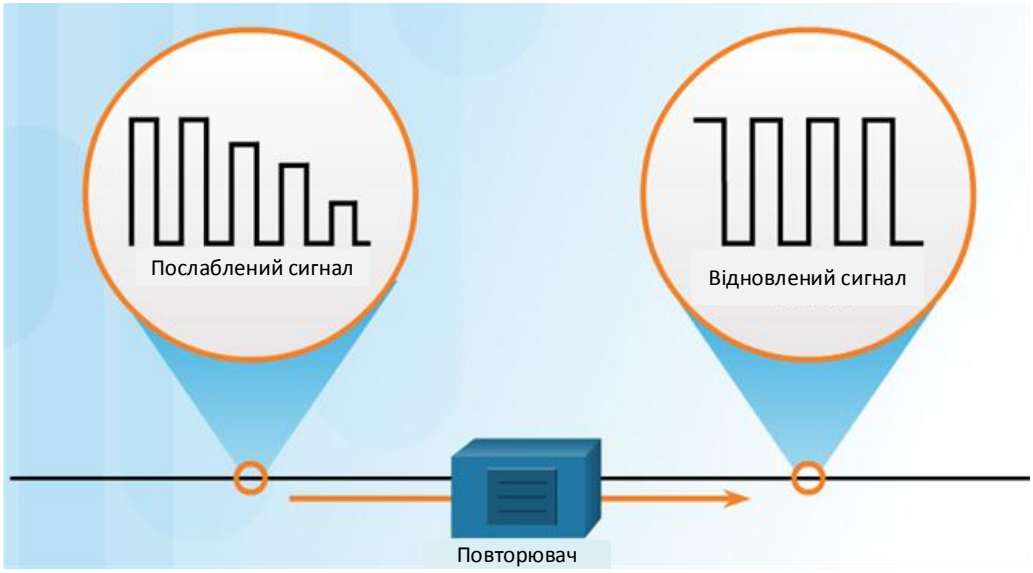


Рис.6.30 – Повторювач

Повторювачі також називаються розширниками, оскільки вони збільшують відстань, на яку можна передавати сигнал. У сучасних мережах повторювачі найбільше часто використовуються для регенерації сигналів в оптоволоконних кабелях.

Живлення через Ethernet (Poe)

Комутатор з PoE (Power over Ethernet) передає по кабелю Ethernet разом з даними постійний струм невеликої потужності для живлення пристроїв, що підтримують PoE. На низьковольтні пристрої, що підтримують технологію PoE, такі як точки доступу Wi-Fi, пристрої відеоспостереження й IP-Телефони, живлення можна подавати з віддалених місць розташування. Пристрою з підтримкою технології PoE можуть одержувати живлення по підключеннях Ethernet на відстані до 100 м. Можна також подавати живлення через кабель Ethernet за допомогою проміжного PoE-Інжектора, показаного на рис. 6.31.



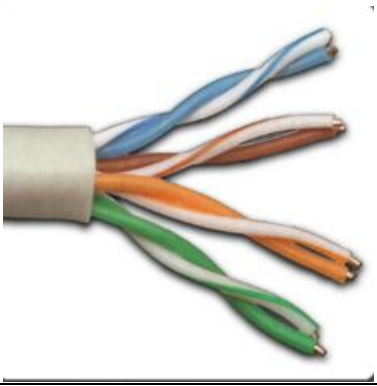
Рис. 6.31– PoE-інжектор

6.3.2 Кабелі й роз'єми

6.3.2.1 Коаксіальні кабелі

Існує безліч мережевих кабелів, як показано в табл. 6.9. У коаксіальних кабелях і кручений парі для передачі даних використовуються електричні сигнали. В оптоволоконних кабелях для передачі даних використовуються світлові сигнали. Ці кабелі різняться пропускною спроможністю, розміром і вартістю.

Таблиця 6.9– Мережеві кабелі

Кабель «витапара»	Коаксіальний кабель	Оптоволоконний кабель
		

Коаксіальний кабель, показаний у табл. 6.9, звичайно виготовлений з міді або алюмінію. Він використовується в кабельному телебаченні й у системах супутникового зв'язку.

По коаксіальному кабелю проходять дані у формі електричних сигналів. Екранування в нього краще, чим у неекранованої витої парі (UTP), відношення сигналу до шуму вище, і даних передається більше. Однак кручена пара замінила коаксіальний кабель у локальних мережах, оскільки в порівнянні з неекранованою крученому парою коаксіальний кабель складніше в установці, дорожче й гірше піддається ремонту.

Коаксіальний кабель укладений в оболонку й може мати різні роз'єми, як показано на рис. 6.32. Існує кілька типів коаксіальних кабелів.

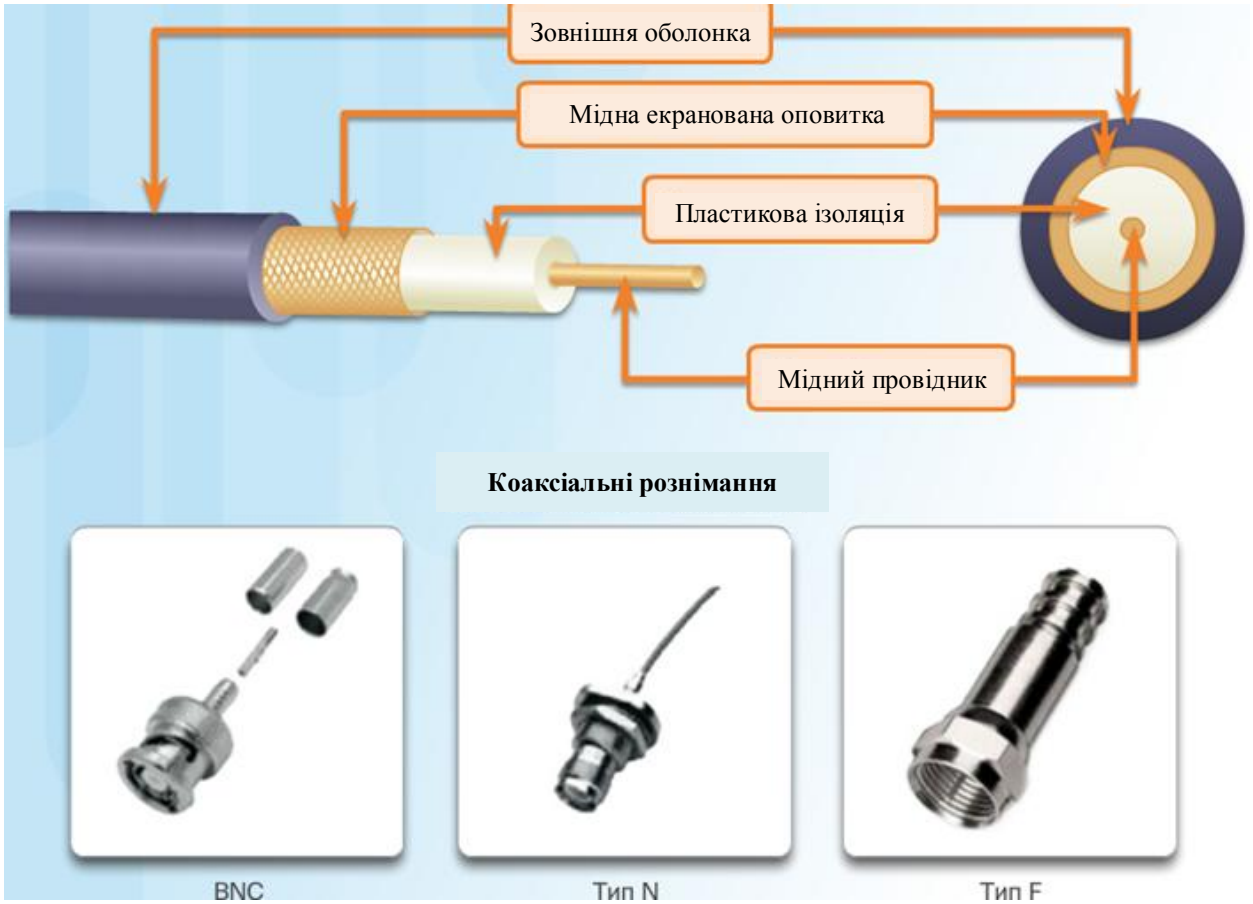


Рис. 6.32 – Конструкція коаксіального кабелю

- **Thicknet або 10BASE5** – використовується в мережах і працює на швидкості 10 Мбіт/с із максимальною довжиною 500 м.
- **Thinnet 10BASE2** – використовується в мережах і працює на швидкості 10 Мбіт/с із максимальною довжиною 185 м.
- **RG-59** – найчастіше використовується для кабельного телебачення в США.
- **RG-6** – кабель більш високої якості, чім RG-59, з великою пропускною здатністю й менш підданий перешкодам.

Коаксіальний кабель не має конкретної максимальної пропускної спроможності. Швидкість передачі й обмежуючі фактори визначаються використовуваною технологією передачі сигналу.

6.3.2.2 Кабелі «вита пара»

Вита пара – це тип мідного кабелю, використовуваний для телефонного зв'язку й більшості мереж Ethernet. Вита пара забезпечує захист від взаємних або перехресних наведень, тобто від шуму, створюваного сусідніми парами проводів у кабелі. Серед кабелів цього типу найбільше широко поширені кабелі на основі неекранованої крученої пари (UTP).

Як показано на рис. 6.33, кабель UTP складається із чотирьох навитих один на одного пар провідників з колірним маркуванням, які укладені в загальну гнучку пластикову оболонку, що захищає кабель від незначних ушкоджень. Навивка провідників один на одного допомагає захиститися від перехресних наведень. Однак неекранована вита пара не захищає від електромагнітних і радіочастотних перешкод. Електромагнітні й радіочастотні перешкоди можуть бути викликані самими різними джерелами, включаючи електромотори й флуоресцентні лампи.

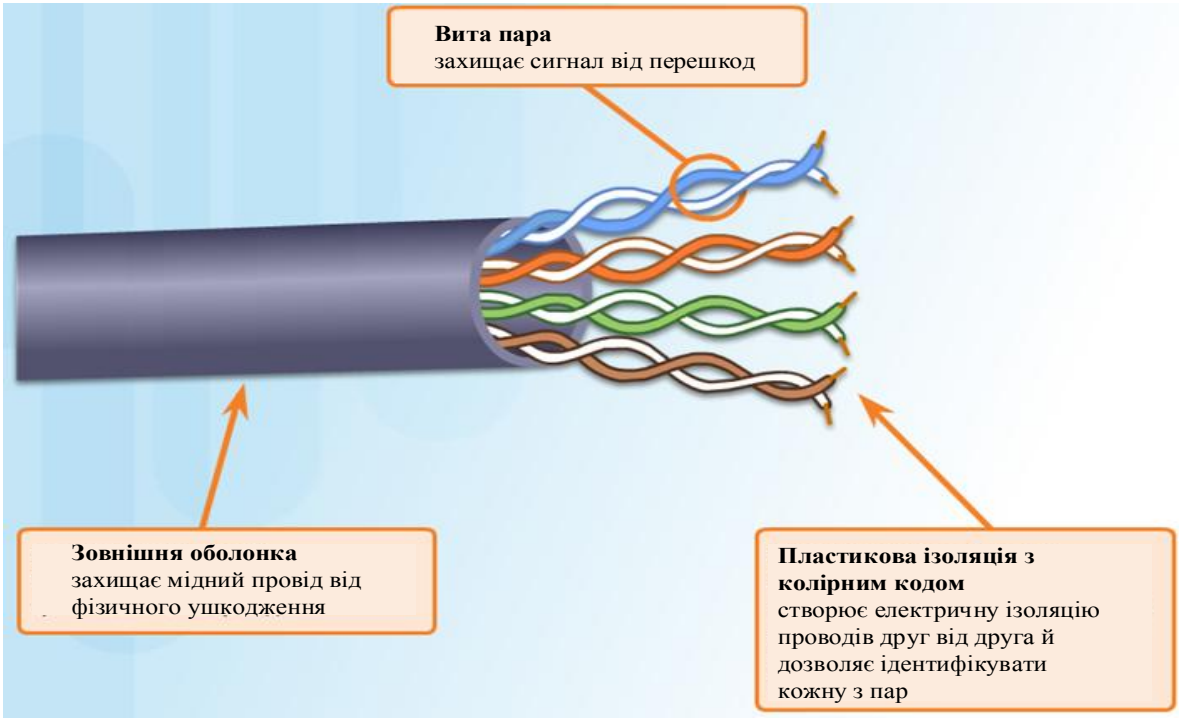


Рис. 6.33 – Склад кабелю UTP

Усередині кабелю може перебувати тонка нейлонова нитка. При витягуванні вона робить на оболонці поздовжній розріз. Це зручний спосіб одержати доступ до пар провідників. Він дозволяє уникнути ушкодження або розрізування проводів у кабелі.

Екранована витапара (STP) була розроблена для забезпечення ефективного захисту від електромагнітних і радіочастотних перешкод.

Як показано на рис. 6.34, кожна пара обгорнена в екран з фольги. Чотири пари обгорнені в металеве обплетення або фольгу.

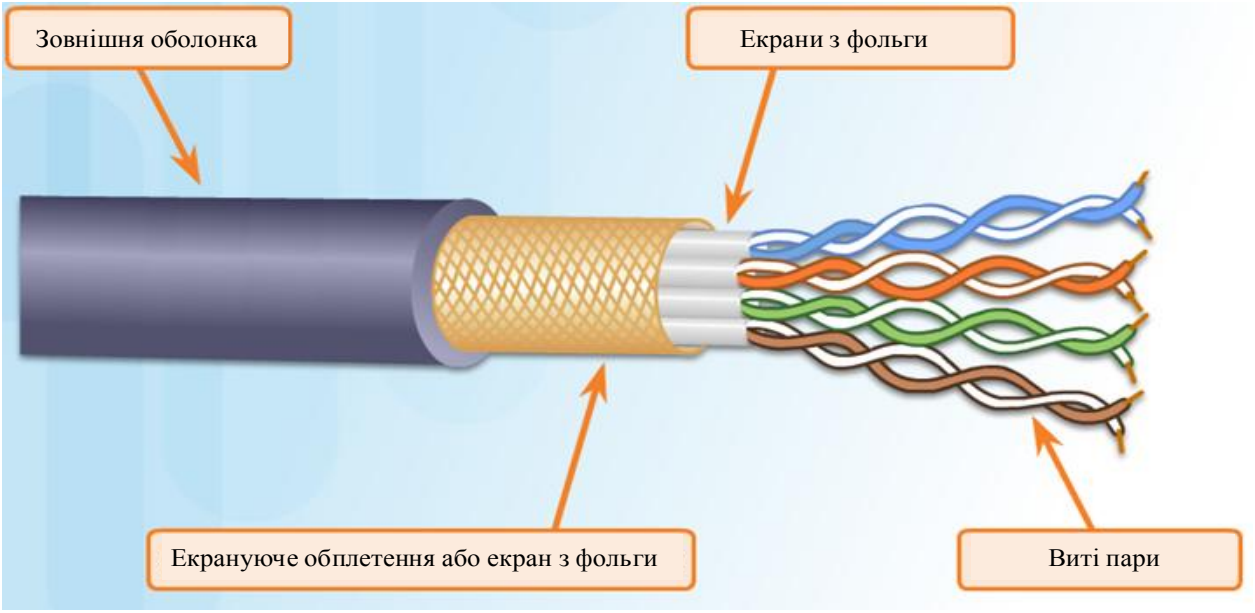
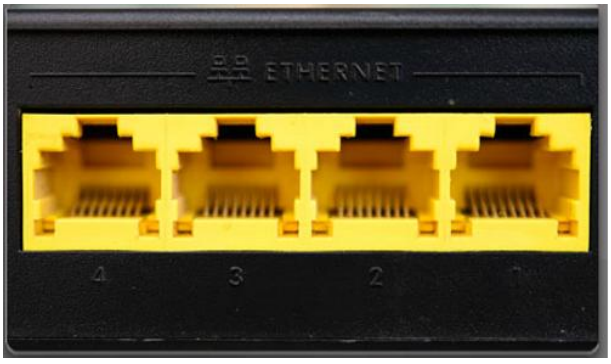


Рис. 6.34 Захисне екранування кабелю UTP

Кабелі UTP і STP мають роз’єми RJ-45 і вставляються в гнізда RJ-45, як показано в рис. 6.35. У порівнянні з кабелем UTP кабель STP помітно дорожче, і його складніше монтувати. Для одержання найбільш повного ефекту від екранування кабелі STP оснащуються спеціальними екранованими роз’ємами RJ-45 для кабелів STP (не показані). Якщо такий кабель не заземлити належним чином, то екран може діяти як антена й приймати небажані сигнали.



Штекерначастинароз'єму RJ-45 UTP (Конектор)



Гніздова частина роз'єму RJ-45 UTP (Розетка)

Рис. 6.35 – Роз'єми та гніздакабелів UTP в STP

6.3.2.3Характеристики категорій витих пар

Кабелі «вита пара» мають кілька категорій. Ці категорії засновані на числі проводів у кабелі й числі витків на одиницю довжини. Сьогодні

в більшості мереж використовується кабель «вита пара». Характеристики кабелю «вита пара» показані на табл. 6.10.

Таблиця 6.10 – Характеристики кабелю «вита пара»

Категорія	Швидкість	Функції
UTPкатегорії 3	10 Мбіт/спричастоті16 МГц	• Підходить для локальної мережі Ethernet. • Найбільше часто використовується для телефонних ліній.
UTPкатегорії 5	100 Мбіт/спричастоті100 МГц	• Виготовляється по більш строгих стандартах, чім категорія 3, для забезпечення більш високих швидкостей передачі даних.
UTP категорії 5е	1000 Мбіт/спричастоті100 МГц	• Виготовляєтьсяпобільшстрогих-стандартах, чімкатегорія 5, длязабезпеченнябільшвисокихшвидкостейпередачіданих. • Меншечисловитківнаодиницюдовжини, чімвкатегорії 5. Це забезпечує більш ефективний захист від електромагнітних і радіочастотних перешкод від зовнішніх джерел.
UTPкатегорії 6	1000 Мбіт/спричастоті250 МГц	• Виготовляється по ще більш строгих стандартах, чім категорія 5е.
Неекранована вита паракатегорії 6а	1000 Мбіт/с при частоті 500 Мгц	• Менше число витків на одиницю довжини, чому категорія 5е. Це забезпечує більш ефективний захист від електромагнітних і радіочастотних перешкод від зовнішніх джерел. • Кабель категорії 6а має кращу ізоляцію й продуктивність, чім кабель категорії 6. • Може мати пластиковий роздільник для поділу пар проводів усередині кабелю, що забезпечує більш ефективний захист від електромагнітних і радіочастотних перешкод. • Гарний вибір для клієнтів, що використовують додатки, для яких потрібно більша пропускна спроможність, такі як відеоконференції або ігри. • Кабель ScTP (екранована вита пара) дуже дорогий і суттєво менш гнучкий, чім UTP.
Екрануванавитапара-категорії 7	10 Мбіт/спричастоті600 МГц	

Примітка. Для кабелю категорії 3 використовується 6-контактний роз'єм RJ-11, тоді як для інших кабелів «вита пара» використовується 8-контактний роз'єм RJ-45, як показано на рис. 6.35.

У нових або реконструйованих офісних будівлях часто використовується певний тип кабелю UTP, що з'єднує всі офіси із центральним місцем,

яке називається головним розподільним вузлом (Main distribution facility, MDF). Максимальна довжина кабелю UTP, використовуваного для передачі даних, – 100 м. Для підключення до головного розподільного вузла кабелів, довжина яких перевищує максимальну межу, потрібно комутатор, повторювач або концентратор. Ці комутатори, повторювачі й концентратори повинні перебувати в незалежному комутаційному вузлу (IDF).

Кабелі, що прокладаються в пленум-порожнинах, повинні бути спеціально призначені для цієї мети. Пленум-порожнина – це простір у будівлі, використовуване для вентиляції, наприклад простір над підвісною стелею. Кабель для пленум-порожнин виготовлений зі спеціального вогнетривкого пластику, що виділяє менше диму, чім інші типи кабелю.

6.3.2.4 Схеми з'єднання провідників витої пари

Існують дві різні послідовності контактів (схеми проводки, розпіновки), які називаються T568A і T568B. Кожна така схема задає певний порядок підключення провідників (окремих жил) на кінці кабелю. Ці дві схеми схожі, але дві із чотирьох пар міняються місцями, як показано на рис. 6.36.

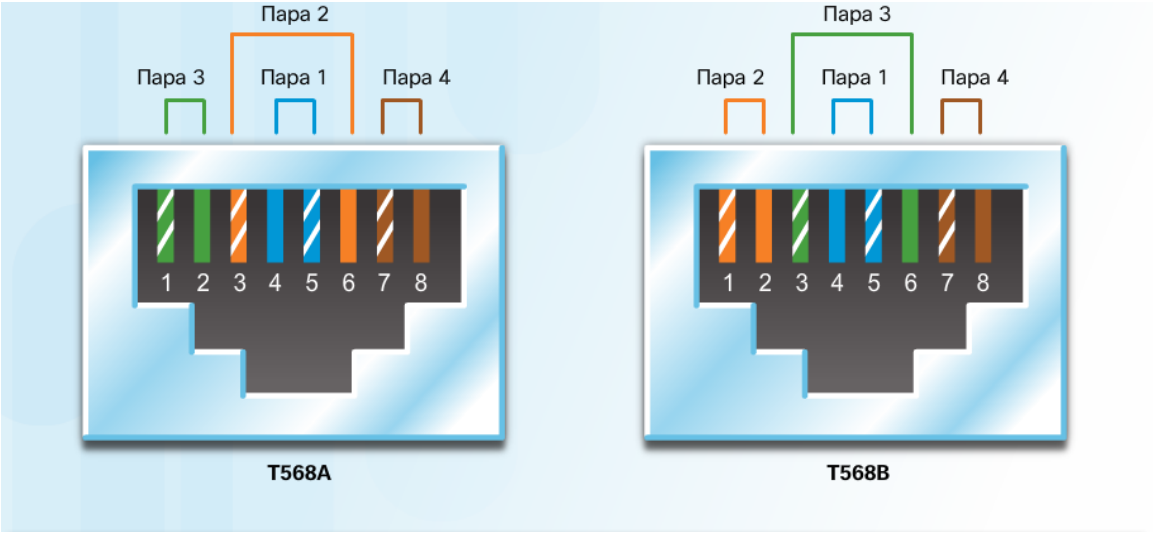


Рис. 6.36 – Схеми проводки, розпіновки

При монтажімережі необхідно вибрати й дотримувати однієї із двох схем проводки (T568A або T568B) рис. 6.37. Важливо, щоб усі підключення в рамках проекту виконувалися по одній і тій же схемі. Працюючи в існуючій мережі, використовуйте наявну схему проводки.

По схемах T568A і T568B можна створити два типи кабелів – прямій і кроссовий (перехресний) табл. 6.11. Прямий кабель зустрічається найчастіше. Контакти на обох кінцях кабелю розташовані в однаковому порядку, використовуючи ту саму схему. Порядок підключення (розпіновка) провідників кожного кольору по обидва боки збігається.

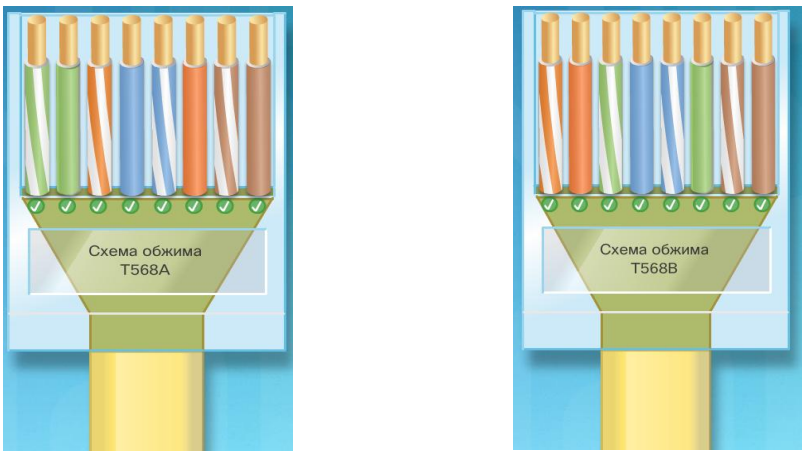


Рис. 6.37– Розведення виводів (розпіновка) кабелів. Вид роз'єму RJ-45 знизу

Таблиця 6.11 – Типи з'єднання кабелів

Типкабелю	Стандарт	Застосування
ПрямийкабельEthernet	Обидвакінця T568A або T568B	• Підключає мережевий вузол до мережевого пристрою, наприклад до комутатора або концентратора.
КросовийкабельEthernet	Одинкінець T568A, іншийкінець T568B	• З'єднує два вузли мережі • З'єднує два мережеві проміжні пристрої (комутатор до комутатора або маршрутизатор до маршрутизатора)

Два безпосередньо підключені пристрої, що використовують для передачі й приймання різні контакти, називаються різнорідними. Для обміну даними між ними потрібний прямий кабель. Наприклад, для підключення комп'ютера до комутатора потрібен прямий кабель.

У кросовому кабелі використовуються обидві схеми проводки. На одному кінці кабелю перебуває роз'єм, обтиснутий за схемою T568A, на іншому – за схемою T568B. Безпосередньо підключені пристрої, що використовують для передачі й приймання ті самі контакти, називаються однорідними. У цьому випадку для обміну даними потрібний кросовій кабель. Наприклад, для підключення комп'ютера до іншого комп'ютера потрібен кросовій кабель.

Примітка. При використанні невідповідного кабелю підключення між пристроями не буде. Однак багато сучасних пристроїв автоматично визначають передавальні, що й ухвалюють контакти й відповідно міняють внутрішні підключення.

6.3.2.5 Волоконне-оптичні кабелі

Конструкція волоконне-оптичного кабелю представлена на рис. 6.38

Зовнішня оболонка звичайно це ПВХ-оболонка для захисту волокна від стирання, вологи й забруднень. Состав зовнішньої оболонки залежить від області застосування кабелю.

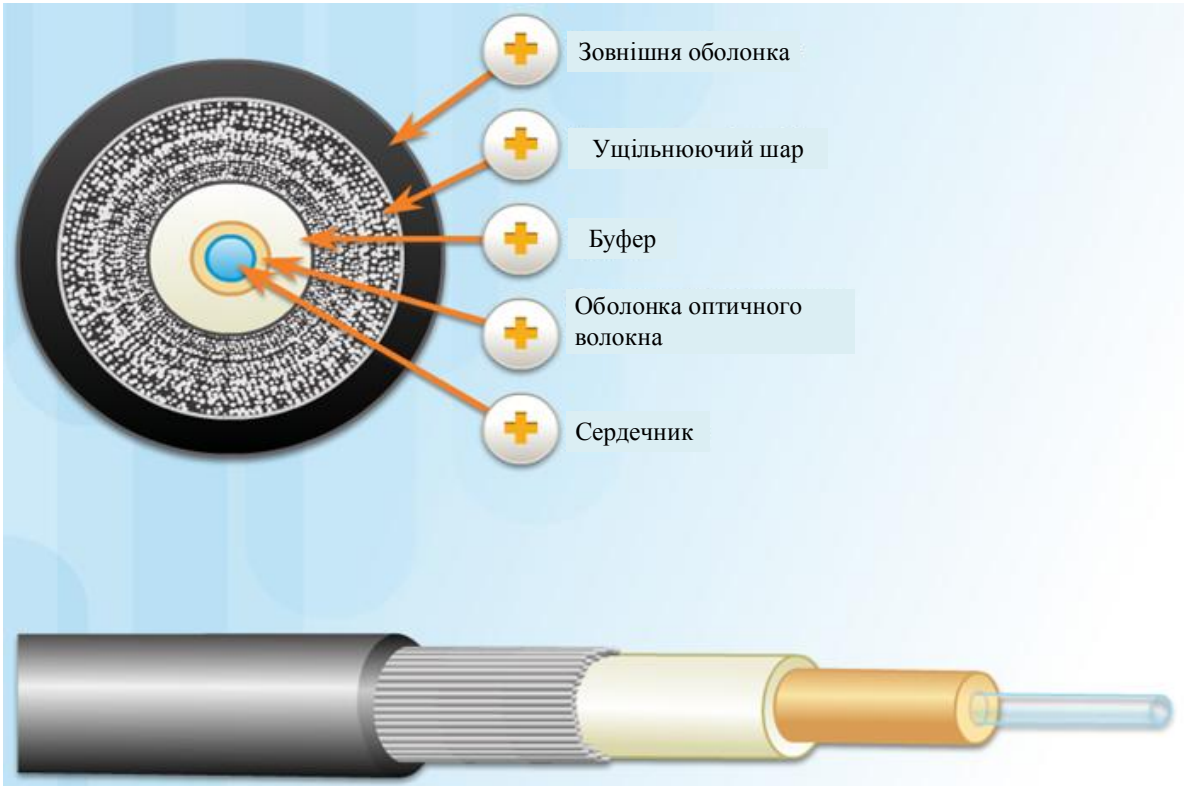


Рис.6.38 – Конструкція волоконне-оптичного кабелю

Ущільнюючий шар оточує буфер і захищає оптоволоконний кабель від розтягання при витаскуванні. У якості матеріалу для ущільнюючого шару часто використовується матеріал для виготовлення бронежилетів.

Буфер використовується для захисту сердечника кабелю й оболонки оптичного волокна від ушкоджень.

Оболонка оптичного волокна виготовляється з матеріалів, що злегка відрізняються від тих, з яких виготовлений сердечник. Відіграє роль свого роду дзеркала, яке відбиває світло в сердечник оптоволоконного кабелю. Це запобігає розсіюванню світла при проходженні його по кабелю.

Сердечник і є світлопередаюче середовище в центрі оптоволоконного кабелю. Як правило, він виконується із кварцу або скла. По сердечникові передаються світлові імпульси.

Оптоволокно складається із двох видів скляних компонентів (сердечника й внутрішньої оболонки) і захисної зовнішньої оболонки. Оскільки для передачі сигналів використовується світло, оптоволоконний кабель не підданий впливу електромагнітних або РЧ-перешкод. При вході в кабель усі сигнали перетворяться у світлові імпульси, а при виході з кабелю вони перетворяться назад в електричні сигнали. Це означає, що оптоволоконний кабель може передавати більш чіткі сигнали, на більшу відстань і з більшою пропускною спроможністю, чім кабель, виготовле-

ний з міді або інших металів. Хоча оптоволокно дуже тонке й може легко гнутися, завдяки властивостям сердечника й оболонки воно дуже міцне. Завдяки своїй міцності оптичне волокно може використовуватися в найважчих умовах експлуатації.

6.3.2.6Типи оптоволоконних кабелів

Оптоволоконні кабелі підрозділяються на два основні типи.

- **Одномодовий оптоволоконний кабель (single-mode fiber, SMF).** Має сердечник дуже малого діаметра. Для передачі променю світла потрібна лазерна технологія (див. рис. 6.39). Широко використовується для організації ліній зв'язку довжиною кілька сотень кілометрів, наприклад для дальньої телефонії й кабельного телебачення.

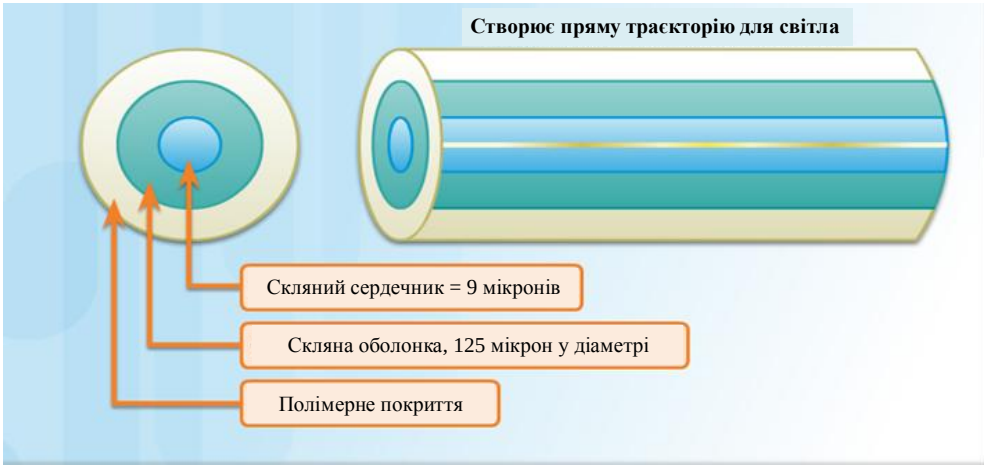


Рис.6.39 – Одномодовий кабель

- **Багатомодовий оптоволоконний кабель (Multi-mode fiber, MMF)**. Має сердечник більшого діаметра. Для передачі світлових імпульсів використовуються світлодіодні випромінювачі. Як показано на рис. 6.40, світло, випромінюване світлодіодом, входить у багатомодовое волокно під різними кутами.



Рис.6.40 – Багатомодовий кабель

Такі кабелі популярні в локальних мережах, оскільки дозволяють використовувати для роботи недорогі світлодіоди. Багатомодовий кабель забезпечує пропускну спроможність до 10 Гбіт/с на відстані до 550 метрів.

Порівняльна характеристика одномодового й багатомодового оптоволоконних кабелів міститься в табл. 6.12.

Таблиця 6.12 Порівняльна характеристика оптоволоконних кабелів

Одномодовий оптоволоконнийкабель	**Багатомодовый оптоволоконнийкабель**
Невеликий сердечник	Розмір сердечника більше, чим в одномодовому кабелі
Менше дисперсії	Виникає більше дисперсії й, отже, більше втрат сигналу
Підходить для більших відстаней	Підходить для більших відстаней, але не таких більших, як у випадку одномодового кабелю
Використовує лазери як джерело оптичного випромінювання	Використовує світлодіоди як джерело світла
Звичайно використовується в магістральних сполученнях комплексу будівель з відстанню в кілька тисяч метрів	Звичайно використовується з локальними мережами або на відстані в межах 200 м для мережі комплексу будівель

6.3.2.7 Оптоволоконні роз'єми

Основні типи оптоволоконних роз'ємів представлені на рис. 6.41



Роз'єми ST



Роз'єми SC



Роз'єми LC



Дуплексні багатомодові роз'єми LC

Рис.6.41 – Оптоволоконні роз'єми

Роз’єми ST (Straight-Tip, байонетного типу)

Один з перших типів конекторів. Роз’єм надійно фіксується механізмом, що закручується, байонетного типу.

Роз’єм SC (Subscriber Connector)

Іноді називають квадратним або стандартним роз’ємом. Цей тип роз’ємів, широко використовуваний у локальних і глобальних мережах, оснащений механізмом із засувкою push-pull для забезпечення надійного монтажу. Цей тип роз’ємівикористовується із багатомодовими й одномодовими оптоволоконними кабелями.

Симплексні роз’єм LC (Lucent Connector)

Менший по розміру варіант оптоволоконного роз’ємSC. Іноді називається малим або локальним роз’ємом, швидко набирає популярність через малий розмір.

Дуплексні багатомодовіроз’ємиLC

Аналогічні симплексним LC, але з використанням дуплексного роз’єму.

Оптоволоконний роз’єм монтується на кінці оптичного волокна. Існують різні типи оптоволоконних роз’ємів. Основні відмінності між цими типами полягають у розмірах і методах механічних з'єднань. Тип застосовуваних у мережі рознімань визначається видом обладнання, що підключається.

Оскільки світло по оптоволокну передається тільки в одному направленні, для роботи в повнодуплексномц режимі потрібні два оптоволокна. Тому в оптичних сполучних кабелях є два волокна, на кінцях кожного з яких змонтовані стандартні одноволоконні роз’єми. Деякі оптоволоконні роз’єми допускають підключення до них як передавальні, так і приймальні волокна. Такі роз’єми називаються дуплексними. Прикладом є дуплексний багатомодовий роз’єм типу LC, показаний на рис. 6.41.

6.4 Основні принципи організації мереж і мережеві технології

6.4.1 Адресація обладнання в мережі

6.4.1.1 Мережева адресація

На рис. 6.42 показано два способи ідентифікації особистості – відбиток пальця й листа з адресом. Як правило, відбитки пальців людини не міняються. Вони дозволяють фізично ідентифікувати людей. Поштова адреса людини може змінитися, оскільки залежить від його місця проживання або від того, де він забирає пошту.

Пристрої, підключені до мережі, мають дві адреси, які аналогічні відбиткам пальців людини і його поштовій адресі. Ці два типи адрес – MAC-адреса (скорочення від Media Access Control – управління доступом до середовища передачі) і IP-адреса.MAC-адреса прошита на мережевій інтерфейсної платі (NIC) виробником. Вона належить до пристрою неза-

лежно від того, до якої мережі воно підключене. MAC-адреса має довжину 48 біт і може бути представлена в одному із трьох шістнадцяткових форматів, показаних у табл. 6.13.



Відбиток пальця аналогічний М-Адресі



Поштова адреса аналогічна IP-Адресі.

Рис. 6.42– Способи ідентифікації особистості

Таблиця 6.13 – Формат MAC-адреси

Форматадреси:	Опис
00-50-56-BE-D7-87	Двішістнадцятковіцифри, розділенітире
00:50:56:BE:D7:87	Двішістнадцятковіцифри, розділенідвокрапками
0050.56BE.D787	Чотиришістнадцятковіцифри, розділенікрапками

Примітка. Двійкові й шістнадцяткові системи числення досить часто зустрічаються в мережевих технологіях. Перетворення чисел з однієї системи числення в іншу виходить за рамки даного курсу. Щоб більше довідатися про ці системи числення, пошукайте інформацію про них в Інтернеті.

6.4.1.2 IP-адреси

Сучасний комп'ютер, як правило, може працювати із двома версіями IP-адрес. На початку 1990-х років виникла стурбованість із приводу нестачі мережевих адрес IPv4. Інженерна група по розвиткові Інтернету (IETF) почала пошуки альтернативних рішень. Це привело до розробки рішення, який зараз відомо як протокол IP версії 6 (IPv6). У цей час адреси IPv6 використовуються паралельно з адресами IPv4 і вже починають їх витісняти. Адреса IPv4 складається з 32 біт і представляється в десятковому форматі з поділом крапкою. Довжина адреси IPv6 становить 128 біт, і він представляється в шістнадцятковому форматі. У табл. 6.14 показані приклади адрес IPv4 і IPv6.

IP-адреси привласнюються мережевими адміністраторами на основі місцезнаходження пристрою в мережі. Коли пристрій переміщається з однієї мережі в іншу, досить імовірно, що його IP-адреса зміниться. На рис. 6.43 показана топологія із двома локальними мережами.

Таблиця 6.1 –4 Адреси IPv4 і IPv6

Формат адреси IPv4 32 біта в десятковомуформаті з поділомкрапкою **192.166.200.8**
Формат адреси IPv6 128 біт у шістнадцятковому форматі **2001:0DB8:CAFE:0200:0000:0000:0000:0008** 128 біт у стисломуформаті **2001 :DB8:CAFE:200::8**

Ця топологія демонструє, що MAC-адреси не міняються при переміщенні пристроїв. Однак IP-адреси міняються. Ноутбук був переміщений у локальну мережу LAN 2. Зверніть увагу, що MAC-адреса ноутбука не змінилася, а помінялися тільки IP-адреси.

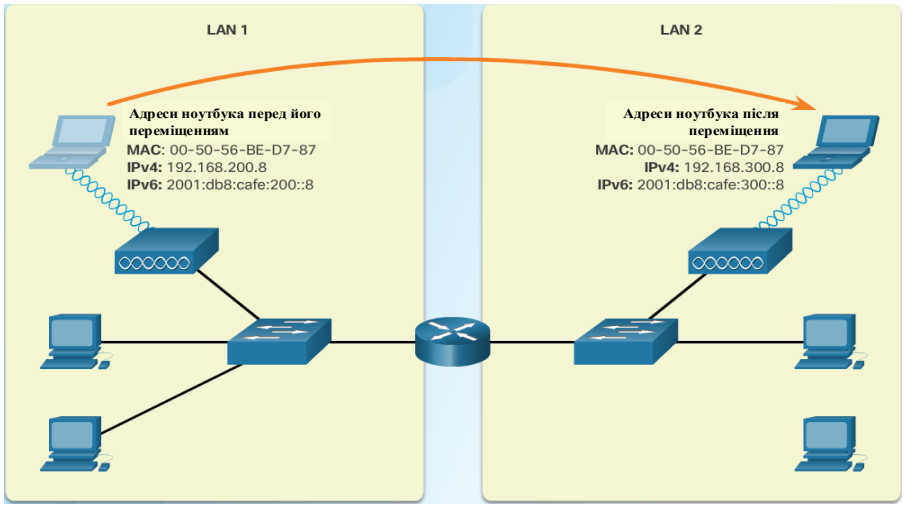


Рис.6.43– Топологія із двома локальними мережами.

На рис. 6.44 показаний вивід команди **ipconfig /all** на ноутбуку. Відображаються MAC-адреса й дві IP-адреси.

```
C:\> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : ITEuser
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . . . . . : 00-50-56-BE-D7-87
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:db8:cafe:200::8(Preferred)
   Link-local IPv6 Address . . . . . : fe80::8cbf:a682:d2e0:98a%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.200.8(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 2001:db8:cafe:200::1
                                       192.168.200.1

<выходные данные опущены>

C:\>
```

Рис.6.44– Дані про адресацію ноутбука

Примітка. В операційній системі Windows мережевий адаптер називається Ethernet-Адаптером, а MAC-адреса – фізичною адресою.

6.4.1.3 Формат адреси IPv4

При настроюванні вузла адреса IPv4 уводиться в десятковому форматі з поділом крапкою, як показано на рис. 6.45. Припустимо, вам буде потрібно ввести 32-бітовий двійковий еквівалент цього значення. Адреса 192.166.200.8 буде представлено у вигляді 11000000101010001100100000001000. Якщо помилитися хоча б в одному біті, адреса буде іншою, і пристрій не зможе обмінюватися даними по мережі.

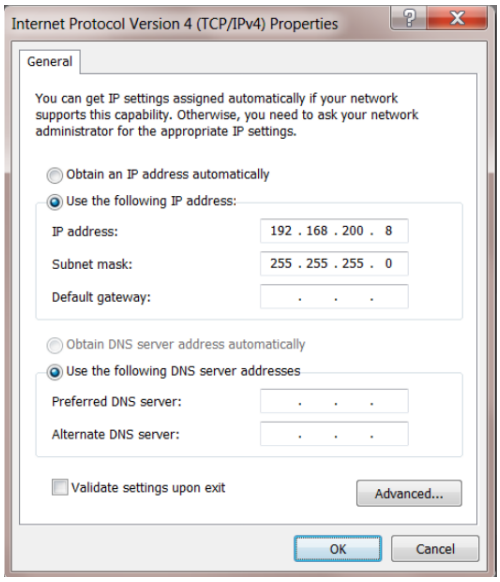


Рис.6.45– Адреса IPv4

Кожне число, розділене крапкою, називається октетом («окто» – вісім), тому що представляє 8 біт. Таким чином, адреса 192.166.200.8 складається із чотирьох октетів. Кожний біт в октеті може бути або 1 (вкл.), або 0 (відкл.). Крім того, кожному біту в октеті відповідає деяке значення. Крайній правий біт представляє значення 1. У кожного біта сусід ліворуч відповідає вдвічі більшому значенню, так що крайній лівий біт представляє значення 126. Для перетворення двійкової адреси необхідно в кожному октеті складати значення всіх бітів, рівних 1, як показано на рис. 6.46.

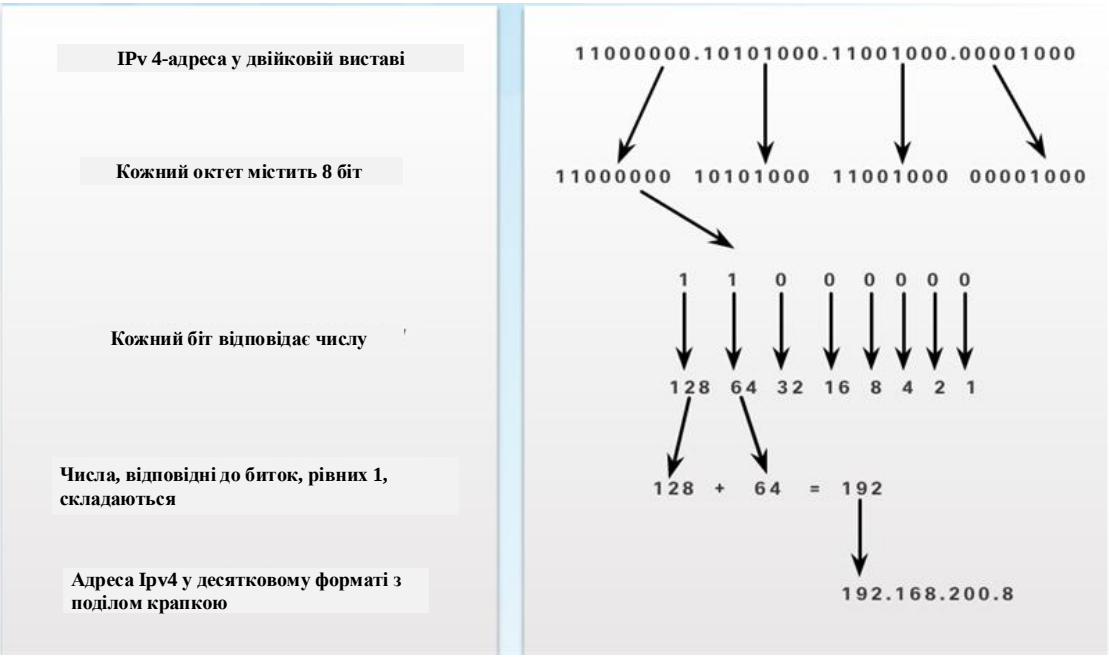


Рис.6.46– Перетворення двійкових чисел у десяткові

Крім того, IPv 4-адреса складається з 2 частин. Перша ідентифікує мережу. Друга – вузол у цій мережі. Обидві частини є обов'язковими.

Коли комп'ютер підготовляє дані до відправлення по мережі, він повинен визначити, чи потрібно відправляти дані безпосередньо одержувачеві, якому вони призначені, або на маршрутизатор. Він відправить дані безпосередньо одержувачеві, якщо одержувач перебуває в одній мережі з ним. А якщо ні, то він відправить дані на маршрутизатор. Маршрутизатор використовує мережеву частину IP-адреси для маршрутизації трафіка між різними мережами.

Комп'ютери й маршрутизатори використовують маску підмережі для визначення мережевої частини IPv 4-адреси призначення. Як і адреса IPv4, маска підмережі представлена в десятковому форматі з поділом крапкою. Наприклад, маска підмережі для адреси Ipv4 192.166.200.8 може бути такий: 255.255.255.0, як показано на рис. 6.46. Для визначення мережевої частини адреси комп'ютер використовує й адресу, і маску підмережі. Він виконує це на двійковому рівні.

На рис. 6.47 показане, як адреса 192.166.200.8 і маска підмережі255.255.255.0 перетворяться в їхні двійкові еквіваленти. Октет з десятковим значенням 255 містить вісім одиниць у двійковому форматі. Біт маски підмережі, дорівнює одиниці, означає, що відповідний йому біт входить у мережеву частину адреси. Тому перші 24 біта адреси 192.166.200.8 належать мережевій частині. Останні 8 біт – біти вузлової частини.

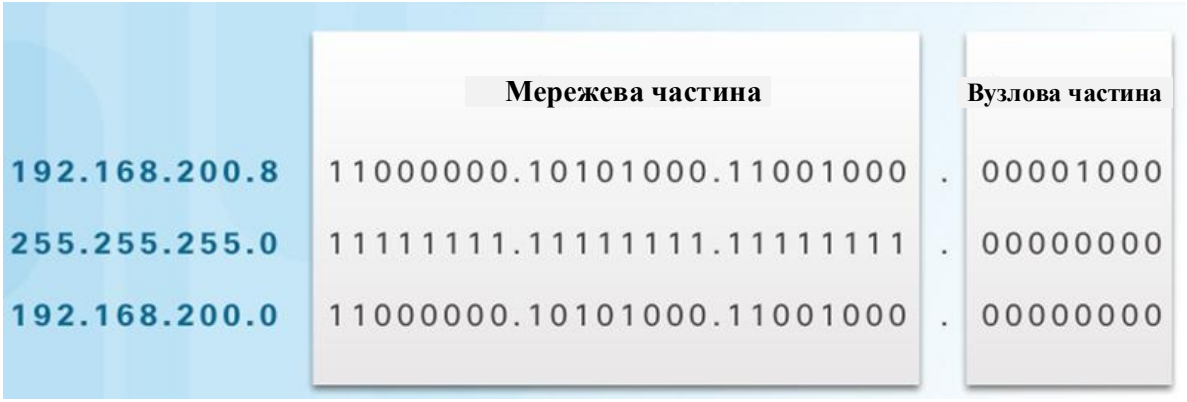


Рис. 6.47– Роль маски підмережі

6.4.1.4 Класова й безкласова адресація IPv4

Коли адресація IPv4 була вперше визначена в 1981 році, адреси були розділена на три класи, як показано в табл. 6.15. Значення першого октету в адресі IPv4 відображає, до якого класу він належить. Кожному класу була призначена маска підмережі за замовчуванням.

Маски підмережі часто представляються в префіксної нотації, як показано в табл. 6.16. Число, що стоїть після косої риси, означає, скільки бітов у масці підмережі рівні 1. Наприклад, мережа класу B 172.16.0.0 з

маскою підмережі 255.255.0.0 буде представлено у вигляді 172.16.0.0/16. Тут «/16» означає, що всі перші 16 біт у масці підмережі дорівнюють одиниці.

Таблиця 6.15 – Класи адреси Ipv4

Клас	Першийоктет	Маскапідмережі	Мережа/Вузол (З = мережу; В = вузол)	Числовузлівдлямережі
A	0-127	255.0.0.0	С.У.У.У	16777214
B	128-191	255.255.0.0	С.С.У.У	65534
C	192-223	255.255.255.0	С.С.С.У	254

Таблиця 6.16 – Маски підмережі в префіксної нотації

Маскапідмережі	Двійковавистава	Префікс
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24

На початку 1990-х років мережевим інженерам стало очевидно, що система адресації IPv4 з використанням класів зрештою вичерпає себе. Багато компаній були занадто більшими для мережевої адреси класу С, який допускає тільки 254 адреси вузлів. Але вони були недостатньо великі для мережевої адреси класу В, що допускає 65 534 адреси вузлів. Тому Інженерна група по розвиткові Інтернету розробила стратегію призначення адрес за назвою «безкласова міждоменна маршрутизація» (Classless Inter-Domain Router, скорочено CIDR, вимовляється як «сайдер»). Стратегія CIDR була тимчасовим заходом, який дозволив організаціям використовувати схеми адресації з урахуванням конкретної ситуації. Організація могла одержати чотири мережеві адреси класу С з маскою, що настроюється, підмережі, як показано на рис. 6.48. Така мережева адреса називається супермережею або надмережею (supernet), оскільки вона складається з декількох класових мережних адрес.

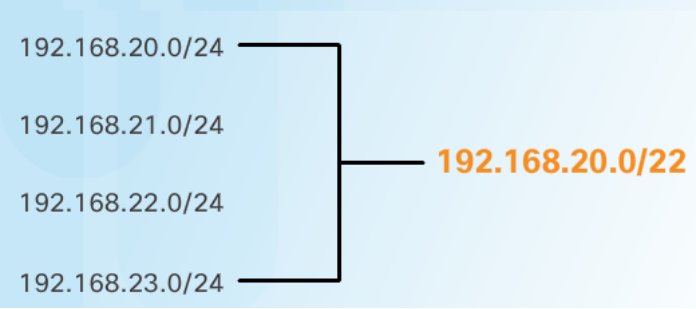


Рис. 6.48 – Приклад супермережі CIDR

6.4.1.5 Кількість IPv 6-адрес

Адресація IPv6 в остаточному підсумку замінить адресацію IPv4. IPv6 допомагає подолати обмеження протоколу IPv4 і значно розширює доступні можливості, пропонуючи функції, які оптимально відповідають поточним і прогнозованим мережевим вимогам. 32-бітний адресний простір IPv4 передбачає приблизно 4 294 967 296 унікальних адрес. Адресний простір протоколу Ipv6 підтримує 340 282 366 920 938 463 463 374 607 431 768 211 456, або 340 ундецильйонів адрес, що приблизно дорівнює кількості піщинок на Землі. У табл. 6.17 представлене візуальне порівняння адресного простору протоколів IPv4 і IPv6.

Таблиця 6.17 – Кількість адрес доступних в IPv4 і IPv6

Назвачисла	Наукова вистава	Кількістьнулів
1 тисяча	103	1 000
1 млн	106	1 000000
1 млрд	109	1 000000000
1 трильйон	1012	1 000000000000
1 квадрильйон	1015	1 000000000000000
1 квінтильйон	1018	1 000000000000000000
1 секстильйон	1021	1 000000000000000000000
1 септильйон	1024	1 000000000000000000000000
1 октильйон	1027	1 000000000000000000000000000
1 нонильйон	1030	1 000000000000000000000000000000
1 децильйон	1033	1 000000000000000000000000000000000
1 ундецильйон	1036	1 000000000000000000000000000000000 000000
	Існує 4 мільярдиадрес IPv4	
	Існує340 ундецильйонів адрес IPv6	

6.4.1.6 Формати адрес IPv6

Довжина IPv6-адрес становить 128 біт, написаних у вигляді рядка шістнадцяткових значень. Кожні 4 біта представляються однієї шістнадцятковою цифрою, утворюючи 32 шістнадцяткових значення. На рис. 6.49 показані повністю розгорнуті адреси Ipv6.

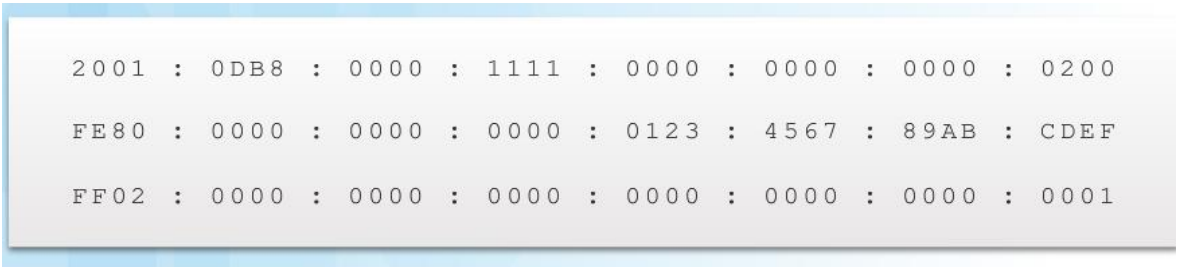


Рис. 6.49Приклади повністю розгорнутих IPv 6-адрес

Існують два правила, які допомагають скоротити кількість цифр, необхідних для представлення IPv 6-адреси.

Правило 1. Пропуск початкових нулів

Перше правило для скорочення запису IPv6-адрес – пропуск усіх початкових нулів у кожній четвірці шістнадцяткових цифр. Наприклад:

- 01AB можна представити, як 1AB
- 09F0 можна представити, як 9F0
- 0A00 можна представити, як A00
- 00AB можна представити, як AB

Правило 2. Пропуск усіх нульових сегментів

Друге правило для скорочення запису адрес IPv6 полягає в тому, що подвійна двокрапка (::) може замінити будь-яку групу нулів, що послідовно йдуть. Подвійна двокрапка (::) може використовуватися в адресі тільки один раз, інакше виникне двозначність і даного запису будуть відповідати кілька можливих адрес.

У табл. 6.18 показані приклади того, як використовувати ці два правила для стиснення адрес IPv6.

Таблиця 6.18 – Приклади скорочення адрес IPv6

Приклад 1	Повністюрозгорнутий	**2001:0DB8:0000:1111:0000:0000:0000:0200**
	Безпочатковихнулів	**2001: DB8:0:1111: 0:0:0: 200**
	Скорочений	**2001:DB8:0:1111::200**
Приклад 2	Повністюрозгорнутий	**FE80:0000:0000:0000:0123:4567:89AB:CDEF**
	Безпочатковихнулів	**FE80:0:0: 0: 123:4567:89AB:CDEF**
	Скорочений	**FE80::123:4567:89AB:CDEF**
Приклад 3	Повністюрозгорнутий	**FF02:0000:0000:0000:0000:0000:0000:0001**
	Безпочатковихнулів	**FF02:0:0: 0:0:0: 0:1**
	Скорочений	**FF02::1**

6.4.1.7 Порівняння адрес Ipv4 і IPv6

Що це таке IPv4 – це абревіатура Інтернет-протоколу четвертої версії. Це четверте видання Інтернет-Протоколу, розробленого для визначення пристроїв у мережі через систему адресації. Дана версія створена

для використання у взаємозалежних мережах з комутацією пакетів. Такий протокол використовується в основному для підключення пристроїв до Інтернету. Дана версія протоколу використовується на 32-бітних адресних схемах, які підтримують 232 адрес. У теперішня час ця версія використовується для розподілу IP-Адрес. Але через її обмеження, виникла необхідність у поліпшеній версії, яка могла б виконувати без проблем ті ж функції. Це привело до розвитку IPv6 [9-12].

Давайте розберемося в чому різниця між IPv4 і IPv6. Що це таке IPv6 – це Інтернет-Протокол шостої версії, також відомий як IPng. Що таке IPng – це абревіатура, яка розшифровується як Інтернет-протокол наступного покоління. Він є спадкоємцем Ipv4 і призначений для того, щоб Інтернет значно розширився відносно обсягу переданих даних і кількості підключених хостингов. Розвиток IPv6 почалося після побоювань, що попит на IP-адреси буде перевищувати можливості IPv4. Ця версія містить у собі 128 біт, що рівно $2^{*126.}$ Це означає, що він може підтримувати більше пристроїв. IPv6-адреси записуються в шістнадцятковому коді й розділяються двокрапками, щоб зробити їх більш читаємими для людей.

Щоб пояснити різницю між IPv4 і IPv6, потрібно порівняти їхні різниці. В IPv4 адресах – 32 біта, це значить, що вони всього 4 біта в довжину. У цій версії використовується адреса (A) записи ресурсів в DNS для зіставлення хостінгових імен з адресами IPv4. Він також використовує покажчик (PTR) в IN-ADDR. ARPA DNS використовує домени для зіставлення адрес IPv4 і хостингових імен. Ця версія Інтернет-Протоколу також створює додатково IPsec, який підтримується ззовні. Заголовок в IPv4 – це не ідентифікатор потоку пакетів для Qos обробки роутерами. Роутери й хостинг-відправники можуть вставляти пакети в цю версію Інтернет-протоколу.

З іншого боку, IPv6 зовсім інший. Ця версія надає певний формат для зменшення обробки заголовка пакета роутерами. Відмінності заголовків пакетів IPv4 і IPv6 унеможливлює взаємодію двох протоколів. Ще одна риса, що робить IPv6 більш кращим, це здатність виконувати передачі одного пакета більш, ніж в один пункт призначення в рамках однієї операції по відправленню. У хостингов IPv6 є транскордонна адреса з автоматичною конфігурацією, що дозволяє їм автоматично настроюватися при підключенні до мережі IPv6 роутера через Інтернет контроль повідомлень версії протоколу. Це робиться через відправлення ланцюжка локальних багатоадресних запитів роутера для розгляду конфігурації. Якщо конфігурація пройшла успішно, роутери відповідають на запит з оголошенням роутером пакета, що містить мережевий шар настроювання конфігурації. В IPv6 процес передачі пакетів і заголовків пакетів був спрощений, щоб зробити його більш ефективним для роутеров. Це безперервним ланцюгом розширює підґрунтя Інтернет-моделі.

Коли цей день настане й IPv4 стануть бути пошуками, то не буде іншого вибору, крім як перехід на IPv6. Є проблеми в такому переході, але

коли він, зрештою, відбудеться, його переваги й багато чого іншого прийде всім по смакові. От у чому полягає відмінність між IPv4 і IPv6.

Протоколи IPv4 і IPv6. У чому різниця й що краще?

Джерело: https://bezopasnik.info

Що таке IP адреса? Інтернет-Протокол або IP-Адреса є основним протоколом зв'язку для передачі датаграмм і дозволяє з'єднувати різні пристрої по усьому світу й ефективно створювати мережу, яку ми називаємо інтернетом. IP-адреса відповідає за адресацію вузлів, інкапсуляцію даних у датаграмми й шляхдатаграмм від вузла-джерела до вузла призначення в одній або декількох IP-Мережах. IP містить набір правил і рекомендацій, яким необхідно випливати при передачі будь-яких даних по будь-якому спектру мережірис. 6.50



Рис.6.50 – Схема розподілу адрес IP-провайдерами Інтернет

IPv4 і IPv6: що вони означають? IPv4 є 4-й версією IP. IPv4 – це протокол без установлення з'єднання, який реалізується в мережах з використанням комутації пакетів. Він працює на основі кращої моделі доставки даних, що означає, що вони одержать невизначену змінну пропускну здатність і час доставки, залежно від поточного навантаження трафіка. Це не гарантує саму доставку, не забезпечує адекватної послідовності й не дозволяє уникнути повторної доставки. IPv6 є останньою версією IP і являє собою поступове відновлення протоколу IPv4. По суті, IPv6 забезпечує повну передачу даних по декільком IP-мережам, дотримуючисьпринципів проектування, розроблених у попередній версії протоколу.

Навіщо нам IPv6? IPv4 використовує тільки 32 біта для своїх інтернет-адрес. В основному це означає, що IPv4 може обробляти до 32 IP-

Адрес, що становить 4 294 967 296 (4,29 мільярда). Хоча це число видаєтьсябільшим, оцінне число пристроїв, підключених до інтернету, перевищує 20 мільярдів, і це число росте з кожним днем. Отже, IP-Адреса будь-якого пристрою повинен бути конкретним і унікальним, і в міру росту числа користувачів адреси IPv4 закінчуються. IPv6 використовує 128-бітні інтернет-адреси. Це означає, що протокол може обробляти в цілому до 2^{128} IP-Адрес, які будуть приблизно становити 340 282 366 920 938 000 000 000 000 000 000 000 000. По суті, стандарту IPv6 досить, щоб інтернет працював дуже й дуже довго. Переваги IPv6 IPv6, поряд зі збільшенням кількості доступних адрес, приносить додаткові переваги. За допомогою протоколу IPv6 була усунута необхідність зміни мережевих адрес – NAT, яка раніше використовувалася для збереження глобального адресного простору через відсутність адрес IPv4. Крім того, протокол IPv6 також виключає можливість конфліктів приватних адрес, а також оптимізує адресну маршрутизацію. У порівнянні зі стандартами IPv4, IPv6 має більш простий формат заголовків, що дозволяє спростити й підвищити ефективність маршрутизації. Це також підвищує якість послуг (Qos), також відоме як «маркування потоку». Не забувайте, що IPv6 має вбудовану автентифікацію й захист конфіденційності, а також гнучкі опції з підтримкою розширень. У цілому, IPv6 спрощує адміністрування за допомогою протоколу DHCP. Чому повсюдний перехід на IPv6 ще не швидко відбудеться? Виснаження IPv4 було передвіщено багато років тому. Уже досить давно була введена CIDR, яка згодом була замінена широко розповсюдженим транслятором – NAT. Хоча обидва методи працюють, але вони єлишетимчасовим способом зупинити вмираючу IPv4. У принципі, уже давно необхідно перейти на IPv6, але прогрес іде дуже повільно. Щоб ввести зміни, програмне забезпечення й маршрутизатори вимагають колосальних змін для підтримки більш просунутої мережі, а це вимагає часу й грошей. Збільшення кількості пристроїв, що ухвалюють стандарти IPv6 IPv4 продовжує забезпечувати більш 99% світового інтернет-трафіка. Незважаючи на десятилітню історію розробки й впровадження стандартів, глобальне впровадження IPv6 відбувається повільно. З 2017 року, частка користувачів із протоколом IPv6 уперше досягла 20,1%, збільшуючись приблизно на 7,2% у рік. Хоча обладнаннямістять стандарти IPv6, кількість мережевих провайдерів, що переходять на IPv6, усе ще досить мало. Тим часом, IPv4 і IPv6 ефективно працюють як паралельнімережі, хоча обмін даними між цими протоколами вимагає спеціальних шлюзів. IPv4 vs IPv6: неминучі зміни Перехід на IPv6 є необхідним і неминучим, і незабаром усі будуть змушені перейти на нього, враховуючи, що пристроїв навколо нас стає більше й потреба в цій мережі також зростає.

6.4.1.8 Статична адресація

У мережі з невеликим числом вузлів можна легко настроїти потрібні IP-адреси для кожного пристрою вручну. Адреси повинен призначати мережний адміністратор, що розбирається в методах IP-адресації, що й уміє вибирати коректна адреса для кожної мережі. Призначуваний IP-адреса повинен бути унікальний для кожного вузла в одній мережі або підмережі. Цей метод називається статичною IP-адресацією.

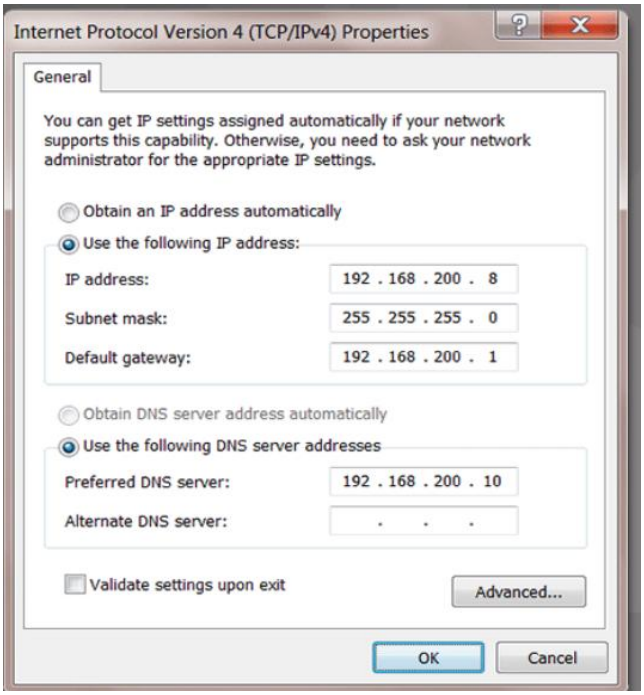


Рис.6.51 – Настроювання статичному IPv4-адресації

Для настроювання статичного IP-адреси на вузлу перейдіть у вікно властивостей TCP/IPv4 мережевого адаптера, як показано на рис. 6.51

Вузлу можна призначити наступні настроювання IP-адресації:

- **IP-адреса** – ідентифікує комп'ютер у глобальній мережі.
- **Маскапідмережі** – параметр, що дозволяє визначити мережу, до якої він підключений.
- **Шлюз за замовчуванням** – пристрій, через який комп'ютер підключається до Інтернету або до інших мереж.
- **Необов'язкові параметри** – наприклад, адреса сервера, що воліється, DNS і адреса додаткового сервера DNS.

В ОС Windows 7 перейдіть по наступних пунктах:

Пуск > Панель керування > Центр керування мережами й загальним доступом > Зміна параметрів адаптера > клацніть правою кнопкою миші **Підключення по локальній мережі > Властивості > Протокол Інтернету версії 4 (TCP/IPv4)** або **Протокол Інтернету версії 6 TCP/IPv6 > Властивості > Використовувати наступний IP-Адресу > Використовувати наступні адреси Dns-Серверів > ОК > ОК**

В Windows 6.0 і 6.1 перейдіть по наступних пунктах:

Параметри комп'ютера > Панель керування > Мережа й Інтернет > Центр керування мережами й загальним доступом > Зміна параметрів адаптера > клацніть правою кнопкою миші **Ethernet > Властивості > Протокол Інтернету версії 4 (TCP/IPv4)** або **Протокол Інтернету версії 6 (TCP/IPv6) > Властивості > Використовувати наступний IP-Адресу > Використовувати наступні адреси Dns-Серверів > ОК > ОК**

6.4.1.9 Динамічна адресація

Якщо до локальної мережі підключена велика кількість комп'ютерів, настроювання IP-Адрес для кожного вузла вручну може займати багато часу й часто пов'язана з помилками. Сервер DHCP автоматично призначає IP-адреси, що спрощує процес адресації. Автоматичне настроювання деяких параметрів TCP/IP також знижує ризик призначення дубльованих або неприпустимих IP-адрес.

Щоб комп'ютер у мережі міг скористатися службами DHCP, він повинен бути здатний виявити цей сервер у локальній мережі. Комп'ютер можна настроїти так, щоб він приймав IP-адреси від сервера DHCP, вибравши варіант **Одержувати IP-адресу автоматично** у вікні настроювання мережевого адаптера, як показано на рис. 6.52.

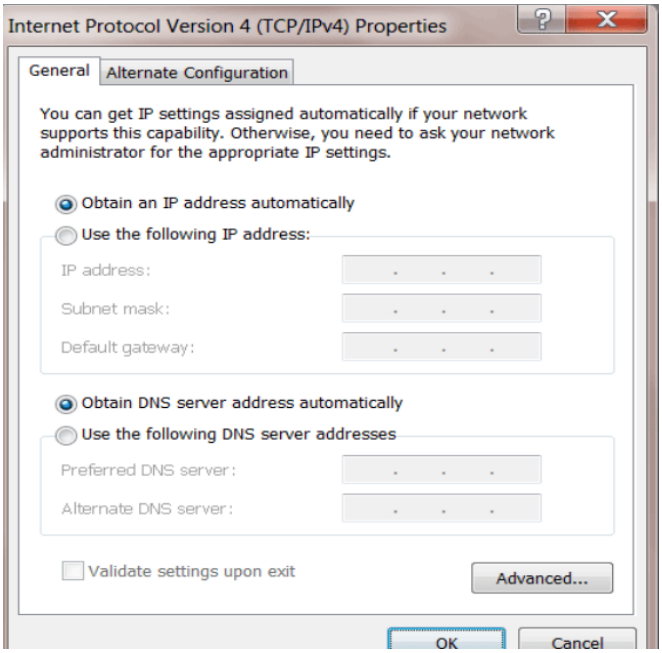


Рис. 6.52 – Настройка DNCP – адресации

Після того як комп'ютер буде настроєний для автоматичного одержання IP-адрес, усі інші поля настроювання IP-адресації стануть недоступні. Параметри DHCP настроюються однаково для провідної й безпроводової мережевої плати.

Після завантаження комп'ютер безупинно запитує IP-адресу від сервера DHCP, поки не одержить його. Якщо комп'ютеру не вдається зв'язатися із сервером DHCP для одержання IP-адреси, ОС Windows призначає автоматичний приватний IP-адресу (APIPA). Це адреса типу link-local (адреса для використання в межах локального сегмента мережі), він перебуває в діапазоні від 169.254.0.0 до 169.254.255.255. Термін link-local означає, що комп'ютер може обмінюватися даними тільки з комп'ютерами, підключеними до тієї ж мережі в тому ж діапазоні IP-адрес.

Сервер DHCP може автоматично призначити вузлу наступні відомості про настроювання IP-Адреси:

- IP-адреса
- Маска підмережі
- Шлюз за замовчуванням
- Додаткові значення, наприклад адреса сервера DNS

В ОС Windows 7 перейдіть по наступних пунктах:

Пуск > Панель керування > Центр керування мережами й загальним доступом > Зміна параметрів адаптера > клацніть правою кно-

пкою миші **Підключення по локальній мережі > Властивості > Протокол Інтернету версії 4 (TCP/IPv4)** або **Протокол Інтернету версії 6 (TCP/IPv6) > Властивості >** виберіть положення перемикача **Одержувати IP-Адресу автоматично > ОК > ОК**

В Windows 6.0 і 6.1 перейдіть по наступних пунктах:

Параметри комп'ютера > Панель керування > Мережа й Інтернет > Центр керування мережами й загальним доступом > Зміна параметрів адаптера > клацніть правою кнопкою миші **Ethernet > Властивості > Протокол Інтернету версії 4 (TCP/IPv4)** або **Протокол Інтернету версії 6 (TCP/IPv6) > Властивості >** виберіть положення перемикача **Одержувати IP-Адресу автоматично > ОК > ОК**

DNS

Для одержання доступу до сервера DNS комп'ютер використовує IP-Адресу, настроєний у параметрах DNS мережевої плати комп'ютера. Сервер DNS дозволяє або зіставляє імена й Url-Адреси вузлів і IP-адреси.

Усі комп'ютери Windows містять кеш DNS, у якому зберігаються недавно дозволені імена вузлів. Кеш є першим місцем, у якому клієнт DNS шукає зіставлення імені вузла. Оскільки кеш розміщений у пам'яті, уже дозволені IP-адреси витягуються швидше, чим при використанні сервера DNS, і при цьому не створюється мережевий трафік.

Настроювання альтернативних параметрів IP

Установка альтернативного настроювання IP в ОС Windows спрощує переміщення між мережами, що вимагають використання сервера DHCP, і мережами, у яких використовуються статичні параметри IP. Якщо комп'ютеру не вдається зв'язатися із сервером DHCP у мережі, ОС Windows використовує альтернативне настроювання IP, призначену мережевий інтерфейсної платі. Альтернативне настроювання IP також заміняє адреса APIPA, призначуваний ОС Windows у випадках, коли не вдається зв'язатися із сервером DHCP.

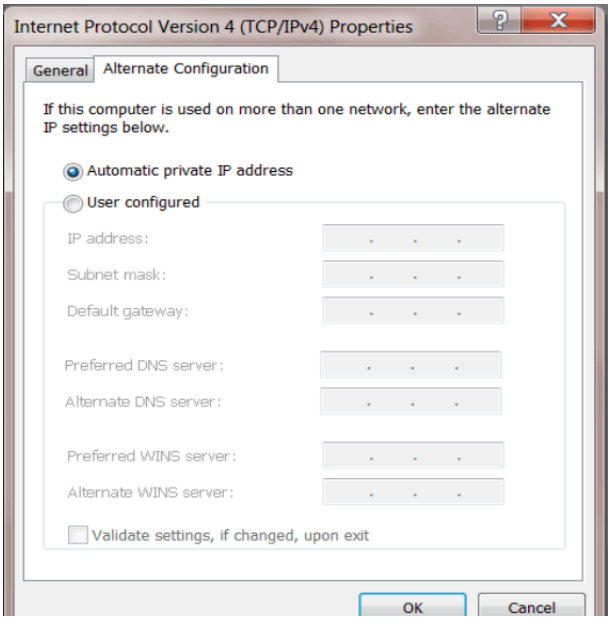


Рис. 6.53 – Настройка альтернативної адресації

Для створення альтернативного настроювання IP, як показано на рис. 6.53, перейдіть на вкладку «Альтернативна конфігурація» у вікні властивостей мережевої плати. Вкладка «Альтернативна конфігурація» відображається тільки тоді, коли обраний перемикач **Одержувати IP-адресу автоматично**.

6.4.1.10 ICMP

Протокол ICMP використовується пристроями в мережі для відправлення на комп'ютери й сервери керуючих повідомлень і повідомлень про помилки. Існує кілька способів використання ICMP, наприклад: оголошення про помилки мережі, оголошення про перевантаження мережі й усунення несправностей.

Для перевірки підключень між комп'ютерами звичайно використовується команда ping. Ping – це проста, але дуже корисна службова програма командного рядка, використовувана для визначення доступності окремих IP-адрес. Для перегляду списку параметрів, які можна використовувати з командою ping, уведіть **ping /?** у вікні командного рядка, як показано на рис. 6.54.

```
C:\> ping /?

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
    -S srcaddr     Source address to use.
    -4             Force using IPv4.
    -6             Force using IPv6.


C:\>
```

Рис.6.54 – Перевірка підключення за допомогою команди Ping

Ping відправляє луна-запит по протоколу ICMP на цільовий комп'ютер або інший мережевийпристрій. Після цього пристрій, щоодержує, відправляє луна-відповідь на запит по ICMP для підтвердження наявності зв'язку. Луна-запити й відповіді на них є тестовими повідомленнями, щовизначають, чи можуть пристрою обмінюватися пакетами. В ОС Windows на комп'ютер призначення відправляються чотири луна-запити по протоколу ICMP, як показано на рис. 6.55.

Якщо комп'ютер призначення доступний, він відправляє чотири луна-відповіді по протоколу ICMP. Відсоток успішних відповідей допомагає визначити надійність і доступність комп'ютера призначення. Інші повідомлення ICMP містять відомості про недоставлені пакети, а також про те, що пристрій занадто зайнятий для обробки пакета.

```
C:\> ping www.cisco.com

Pinging e144.dscb.akamaiedge.net [23.200.16.170] with 32 bytes of data:
Reply from 23.200.16.170: bytes=32 time=25ms TTL=54
Reply from 23.200.16.170: bytes=32 time=26ms TTL=54
Reply from 23.200.16.170: bytes=32 time=25ms TTL=54
Reply from 23.200.16.170: bytes=32 time=25ms TTL=54

Ping statistics for 23.200.16.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 25ms, Maximum = 26ms, Average = 25ms

C:\>
```

Рис. 6.55– Перевірка підключення за допомогою команди Ping

Можна також використовувати команду ping для пошуку IP-адреси вузла, якщо відоме ім'я цього вузла. Якщо видати команду ping з іменем веб-сайту, наприклад, cisco.com, як показано на рис. 6.55, відобразиться IP-адреса відповідного сервера.

6.4.2 Протоколи транспортного рівня

6.4.2.1 Роль транспортного рівня

Транспортний рівень відповідає за встановлення тимчасового сеансу зв'язку й передачу даних між двома додатками. Як показано на рис. 6.56, транспортний рівень – це канал між рівнем додатків і нижніми рівнями, які відповідають за передачу даних по мережі.

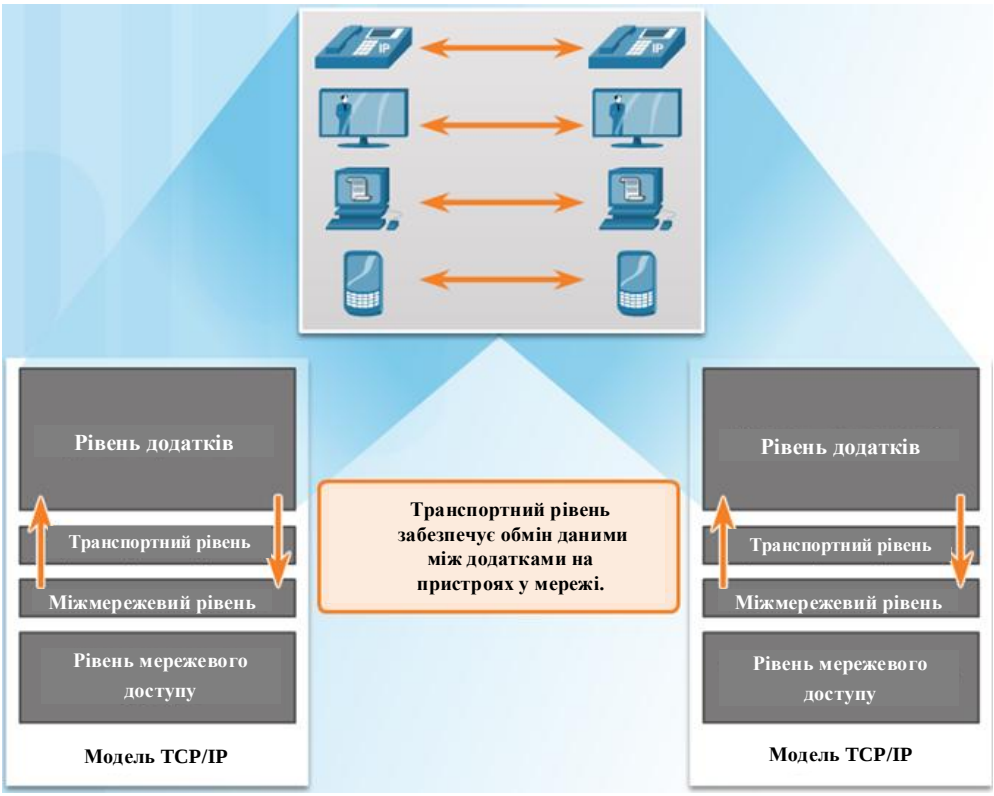
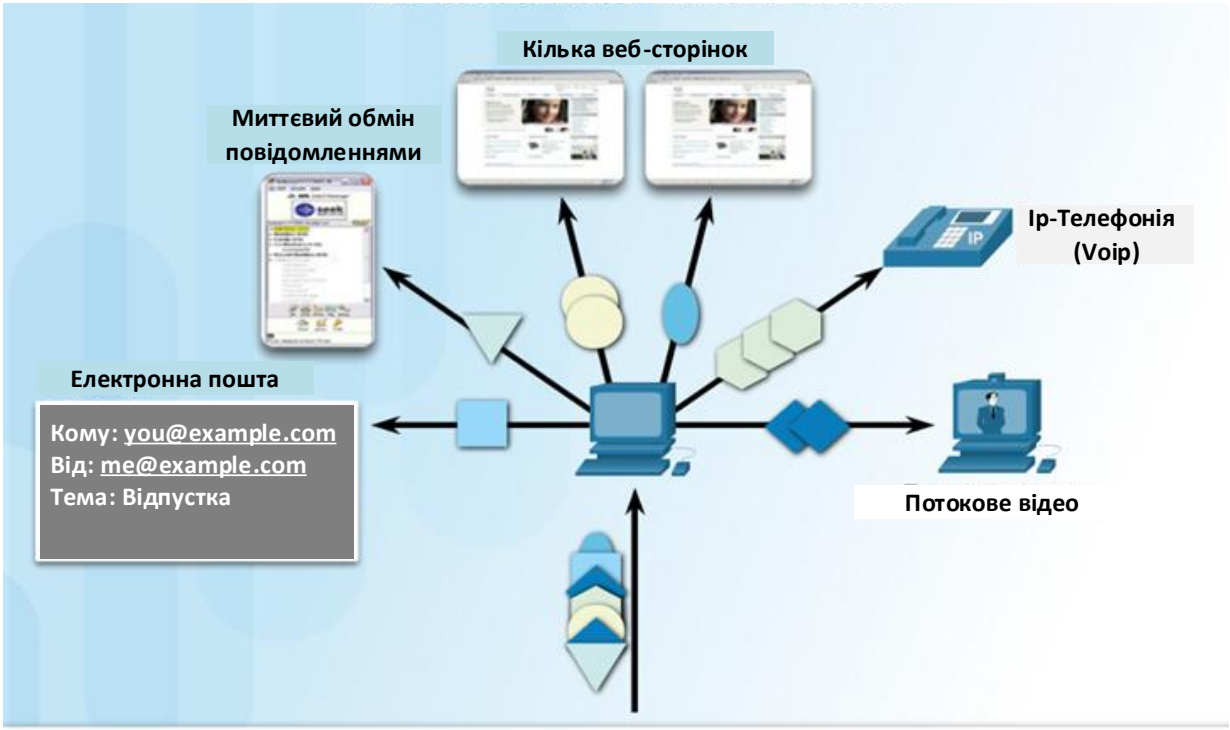


Рис.6.56 – Транспортний рівень

6.4.2.2 Функції транспортного рівня

Набір даних, переданих між додатком джерела й додатком призначення, називається сеансом зв'язку. Комп'ютер може підтримувати кілька сеансів зв'язку між декількома додатками одночасно, як показано на рис. 6.57. Це можливо завдяки трьом основним функціям транспортного рівня.

- **Відстеження сеансів зв'язку між додатками**. Пристрій може відслідковувати кілька додатків, що використовують мережу одночасно.
- **Сегментування даних і їх наступне складання**. пристрій, що відправляє, розділяє дані додатків на блоки підходящого розміру. пристрій, що приймає, збирає сегменти в дані додатки.
- **Ідентифікація додатків**. Щоб переслати потоки даних відповідним до додатків, транспортного рівня необхідно визначити цільовий додаток. Для цього транспортний рівень привласнює кожному додатку окремий ідентифікатор – номер порту.



Транспортний рівень гарантує, що навіть якщо на пристрої запущено кілька додатків, усі вони одержать правильні дані.

Рис.6.57 – Відстеження сеансів зв'язку

6.4.2.3 Протоколи транспортного рівня

Як показано на рис. 6.58, на транспортному рівні діють два протоколи: TCP (протокол управління передачею даних, transmission control protocol) і UDP (протокол передачі датаграмм користувача, user datagram protocol). TCP уважається надійним і повнофункціональним протоколом транспортного рівня, який забезпечує передачу всіх даних на вузол приз-

начення. UDP, на відміну від нього, – дуже простий протокол транспортного рівня, що не гарантує надійність. Протокол IP використовує ці транспортні протоколи для забезпечення зв'язку й передачі даних між вузлами.

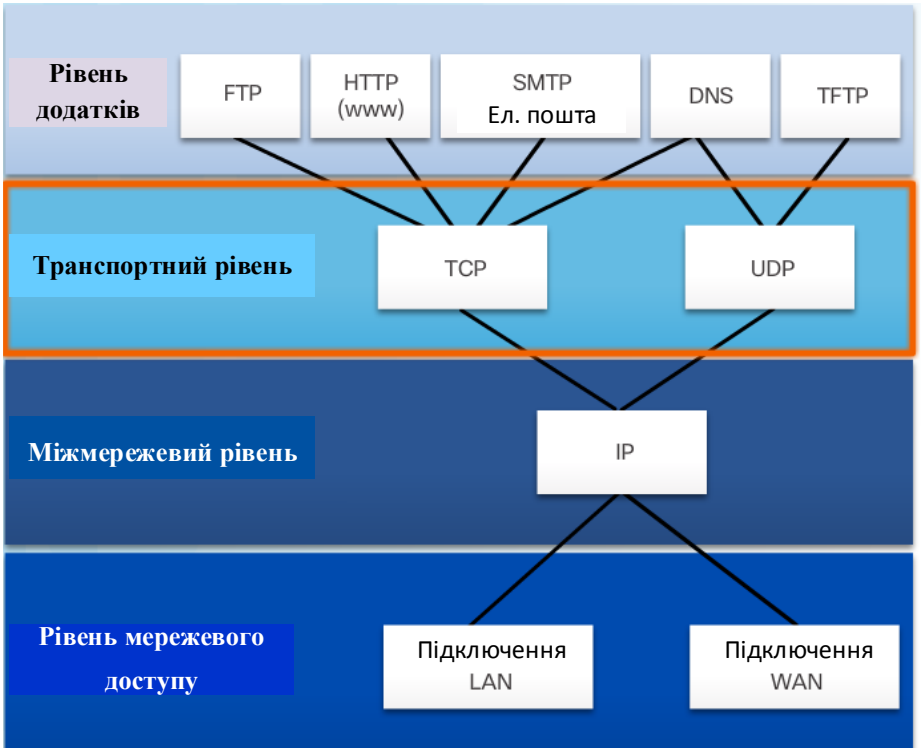


Рис.6.58 – Два протоколи транспортного рівня

На рис. 6.59 показані властивості протоколів TCP і UDP.

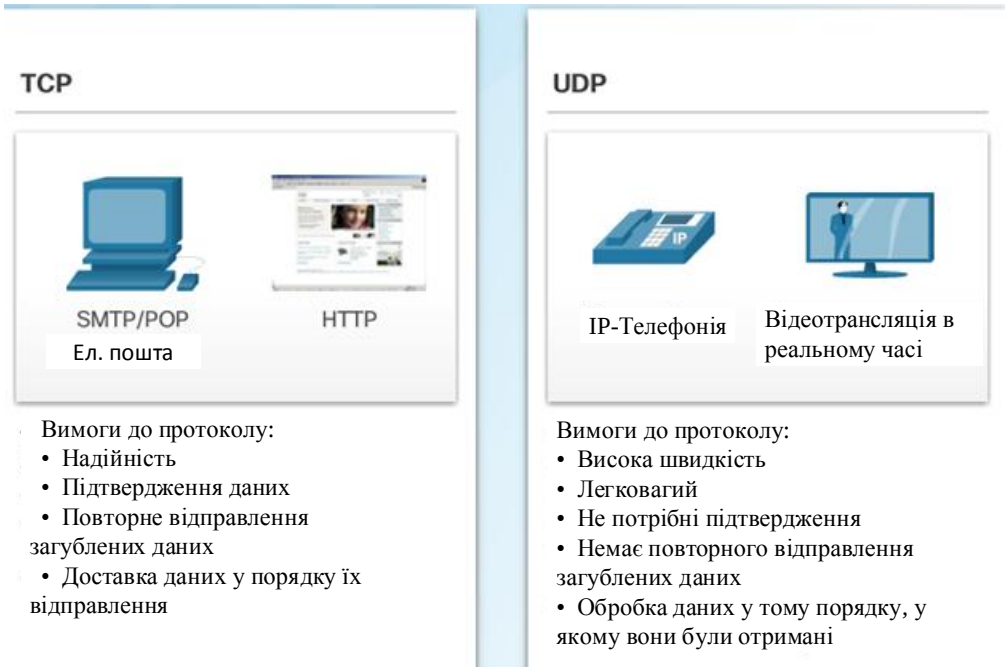


Рис. 6.59 – Властивості протоколів TCP і UDP

6.4.2.4 TCP

Передача з використанням TCP аналогічна відправленню пакетів із трекінгом, шлях яких відслідковується від відправника до одержувача. Якщо замовлення розбите на кілька частин, замовник може зайти на вебсайт транспортної компанії й подивитися порядок доставки.

TCP використовує наступні три основні операції для забезпечення надійності:

- Відстеження кількості сегментів, відправлених на те або інший пристрій тем або іншим додатком.
- Підтвердження отриманих даних.
- Повторна передача сегментів з непідтвердженими даними після закінчення певного часу очікування.

На рис. 6.60 показаний процес обміну сегментами TCP і підтвердженнями між відправником і одержувачем.

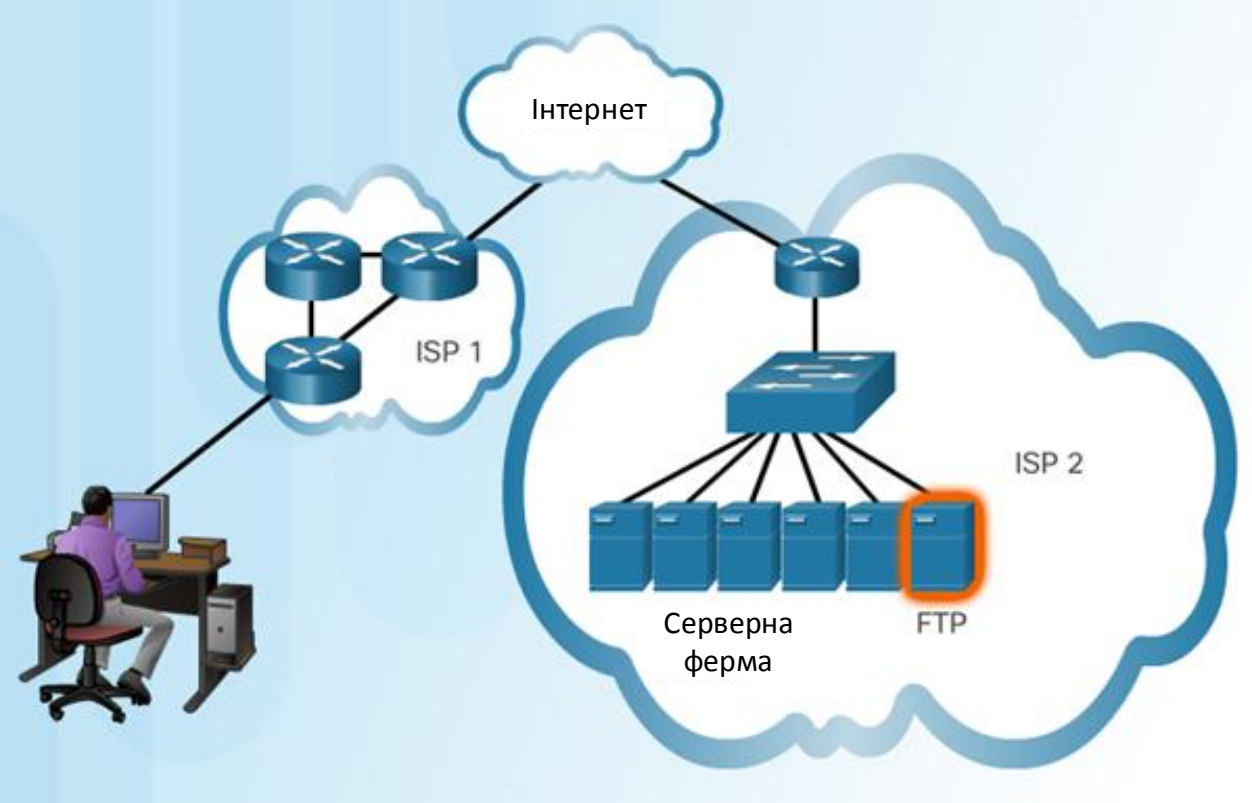


Рис.6.60– Процес обміну сегментами TCP і підтвердженнями між відправником і одержувачем

6.4.2.5 UDP

Роботу протоколу UDP можна зрівняти з відправленням поштою звичайного, не замовленого, листа. Відправник не знає, чи зможе адресат одержати листа, а поштова відділення не відповідає за відстеження листа або інформування відправника про те, чи доставлений лист за адресом.

Він забезпечує тільки основні функції для обміну сегментами даних між додатками. При цьому даний протокол відрізняється незначними

накладними витратами й практично відсутністю перевірки даних. UDP відомий як протокол негарантованої доставки даних. Стосовно до комп'ютерних мереж негарантована доставка вважається ненадійною, оскільки при цьому відсутнє підтвердження про одержання відправлених даних на вузлу призначення.

На Рис 6.61, показано представлення передачі сегментів UDP від відправника одержувачеві.

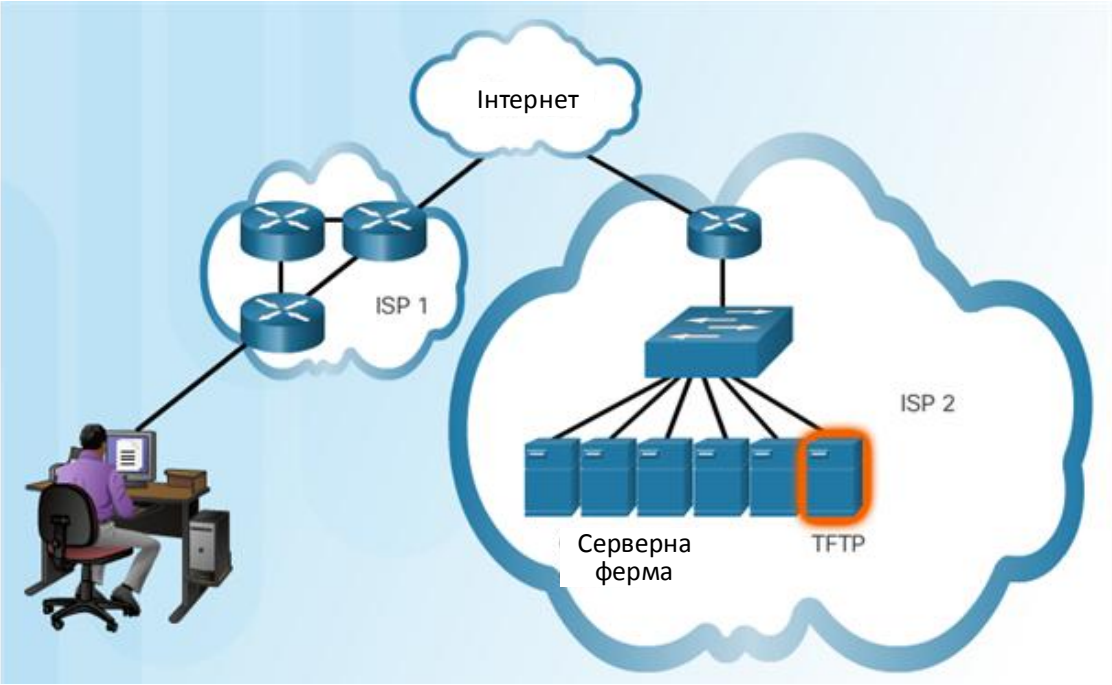


Рис 6.61– Передача сегментів UDP від відправника одержувачеві

6.4.2.6 Номера портів

У протоколах TCP і UDP використовуються номери портів джерела й призначення для відстеження сеансів зв'язку між додатками. Номер порту джерела пов'язаний з, що відправляє додатком на локальному пристрої. Номер порту призначення пов'язаний з додатком призначення на вилученому пристрої.

Номер порту джерела генерується пристроєм, що динамічне відправляє. Цей процес дозволяє одночасно встановити кілька сеансів зв'язку для одного додатка. Наприклад, при використанні веб-браузера, можна відкрити кілька вкладок одночасно. Номера портів призначення – 80 для звичайного веб-трафіка й 443 для захищеного веб-трафіка. Однак порти джерела будуть різними для кожної відкритої вкладки. Завдяки цьому комп'ютер дізнається, на яку вкладку браузера доставляти веб-вміст. Аналогічно, інші мережеві додатки, такі як електронна пошта й передача файлів, мають власні номери портів. Список загальновідомих номерів портів показаний у табл. 6.19 [7, 8].

Таблиця 6.19 – Номера портів

Загальновідомінномерипортів			
Номер-порту	**Прото-кол**	**Застосування**	**Скоро-чення**
20	TCP	FileTransferProtocol(Протоколпередачіфайлів) (дані)	FTP
21	TCP	FileTransferProtocol(Протоколпередачіфайлів) (управ-ління)	FTP
22	TCP	ПротоколSecureShell	SSH
23	TCP	ПрограмаTelnet	–
25	TCP	SimpleMailTransferProtocol(Протоколпростогообмінуелектронноюпоштою)	SMTP
53	UDP, TCP	DomainNameService(Службадоменнихімен) (DNS)	DNS
67	UDP	DynamicHostConfigurationProtocol(Протоколдинамічного настроюваннявузла) (сервер)	DHCP
68	UDP	DynamicHostConfigurationProtocol(Протоколдинамічного настроюваннявузла) (клієнт)	DHCP
69	UDP	TrivialFileTransferProtocol(Найпростішийпротоколпередачіфайлів)	TFTP
80	TCP	HypertextTransferProtocol(Протоколпередачігіпертексту)	HTTP
110	TCP	PostOfficeProtocol(Протоколпоштовоївідділення) (версія 3)	POP3
137-139	UDP, TCP	Netbios/Netbt	-
143	TCP	InternetMessageAccessProtocol(Протоколдоступудоповідомлень в Інтернеті)	IMAP
161	UDP	SimpleNetworkManagementProtocol(Простийпротоколуправліннямережею)	SNMP
427	UDP, TCP	Протоколпошукуслужби	SLP
443	TCP	HypertextTransferProtocolSecure(Протоколзахищеноїпередачігіпертексту)	HTTPS
445	TCP	Протоколобмінублокамисервер-нихповідомлень/ЗагальнафайловасистемаІнтернет	SMB/CIFS
548	Протокол TCP	AppleFilingProtocol	AFP
3389	UDP, TCP	RemoteDesktopProtocol(Протоколвилученогоробочогостола)	RDP

6.4.2.7 Порівняння TCP з UDP

Таблиця 6.20 – Порівняння TCP з UDP

Характеристика	**TCP**	**UDP**
Непотрібніпідтвердження		**+**
Обробкаданихутомупорядку, уякомувонибулиотримані		**+**
Надійність	**+**	
Високашвидкість		**+**
Повторневідправленнязагубленихданих	**+**	
Доставкаданихупорядкуїхвідправлення	**+**	
Легковагий		**+**
Немаєповторноговідправленнязагубленихданих		**+**
Підтверджуєодержанняданих	**+**	

6.4.2.8.Визначення протоколів і їх порти

Визначення протоколів і їх порти за замовчуванням наведене у табл. 6.21.

Таблиця 6.21 – Визначення протоколів і їх порти за замовчуванням

Протокол	Портизазамовчуванням
80	Протоколпередачігіпертексту(HTTP)
53	Службадоменнихімен(DNS)
21	Протоколпередачіфайлів(FTP)
548або427	AppleFilingProtocol (AFP)
110	Поштовийпротоколверсії 3 (POP3)
22	ПротоколSecureShell (SSH)
25	Протоколпростоїпередачіелектронноїпошти(SMTP)
143	Протоколдоступудоповідомлень в Інтернеті(IMAP)
443	Захищенийпротоколпередачігіпертексту(HTTPS)
445	Протоколобмінублокамисерверних повідомлень(SMB)

Список використаних джерел

1. Гніденко М.П., Гайдур Г.І., Сєрих С.О. Перспективні компоненти та засоби інфокомунікаційних технологій. – Навчальний посібник. – Київ: ДУТ, 2017. – 168 с.
2. О.Л. Недашківський Технології та протоколи Інфокомунікаційних мереж (частина перша) ДУТ К. – 2017. 67 с.
3. О.Л. Недашківський Технології та протоколи Інфокомунікаційних мереж (частина друга) ДУТ К. – 2018. 77 с.
4. Воробієнко П.П., Каразей В.М., Скопа 0.0. Протоколи міжмережної взаємодії. – Одеса, УДАЗ ім. О С. Попова, 1999. – 50 с.
5. Воробиенко П.П., Нечипорук О.Л., Струкало М.И. Принципы организации сетей с коммутацией пакетов: Учебное пособие. – Изд. 2-е пер. - Одесса: ОНАС им. А.С. Попова, 2001. – 100 с.; пл.
6. Е.В. Добровольский, А.Ю. Бессчётнов, А.А. Легунов, Д.С. Гуринович Принципы конфигурирования маршрутизаторов Cisco в сетях TCP/IP и Frame Relay: Методическое руководство к лабораторным работам № 1-6 / Под редакцией О.Л Нечипорука, М.И. Струкало. – Одесса: ОНАС им. А.С. Попова, 2001. – 63с.
7. .Курс IT Essentials Мережевої академії Cisco [Електронний ресурс]. Режим доступу: https://www.netacad.com/ru/courses/os-it/it-essentials.
8. Введение в программу CiscoPacketTracer [Электронный ресурс]. Режим доступа: https://www.intuit.ru/studies/courses/3549/791/lecture/29211.
9. Джерело: https://bezopasnik.info
10. Джерело: (http://www.todbot.ru/2012/03/ipv4-vs-ipv6.html)
11. Джерело: https://www.youtube.com/watch?v=jVjEHZc5fzw&feature=emb logo
12. Джерело: https://bezopasnik.info

Огляд Глави6. Принципи організації телекомунікаційних мереж

До сучасних мереж можна підключити безліч різних пристроїв, таких як комп'ютери, ноутбуки, планшетні комп'ютери, смартфони, телевізори, годинник і побутовий електроприлади. Ці пристрої використовують для підключення до мережі різні середовища передачі даних, у тому числі мідні й оптоволоконні кабелі, а також безпроводові підключення. Проміжні пристрої, такі як комутатори й маршрутизатори, забезпечують передачу даних між джерелом і одержувачем. Існує кілька типів мереж, до яких підключаються ці пристрої. Це локальні мережі, безпроводові мережі, персональні мережі, муніципальні мережі й глобальні мережі.

Щоб ефективно взаємодіяти один з одним, пристрою повинні дотримувати певних правил. Ці правила називаються стандартами й протоколами. Еталонна модель OSI і набір протоколів TCP/IP дозволяють мережним адміністраторам і інженерам зрозуміти взаємозв'язок цих різних стандартів і протоколів.

Існують стандарти Ethernet для провідних і безпроводових мереж. Стандарт для провідних мереж називається IEEE 802.3, а для безпроводових – IEEE 802.11.

Щоб дані гарантовано були отримані адресатом, існують кілька типів адрес, а також номера портів. MAC-адреси використовуються комутаторами для пересилання трафіка в рамках локальної мережі. IP-адреси використовуються маршрутизаторами для визначення оптимального шляху до мережі призначення. Номера портів використовуються комп'ютерами для визначення, який додатокповиннийухвалювати дані.

Питання та завдання для самостійного контролю знань

Контрольні питання:

1) Принципи організації мереж
2) Мережні стандарти
3) Фізичні компоненти мережі
4) Основні принципи організації мереж і мережні технології

Питання для тест-контролю

1. Який термін описує тип коаксіального кабелю?

568A
RG-6
UTP
Cat 5e

2. Яка технологія частіше використовується для підключення пристроїв до персональної мережі?

Bluetooth
оптоволоконні кабелі

коаксіальні кабелі
безпроводовий зв'язок стандарту IEEE 802.11 n

3. Перешкоди яких двох типів краще пригнічуються при використанні кабелю STP у порівнянні з UTP?(Виберіть два варіанти.)

MDF
Радіочастотні перешкоди
Електромагнітні перешкоди
Дисперсія
Білий шум

4. Що характерно для протоколу UDP?

низькі накладні витрати
наскрізне встановлення каналів перед передачею
виправлення помилок
гарантована передача

5. Скільки адрес вузлів доступно в мережі з маскою підмережі 255.255.0.0?

1024
254
65 534
16 777 214

6. Що позначає число 100 у стандарті 100BASE-TX?

максимальну пропускну здатність у Мбіт/з
серійний номер стандарту
максимальне число мережних вузлів
максимальну довжину кабелю 8 метрах

7. Коли принтер уважається вузлом мережі?

коли він підключений до ноутбука
коли він підключений до персонального комп'ютера
коли він підключений до робочої станції
коли він підключений до комутатора

8. Скільки пристроїв можна одночасно підключити до інтерфейсу Bluetooth?

5
127
24
7
10

9. Який стандарт IEEE передбачає використання частот обох діапазонів безпроводовому зв'язку: 2,4 ГГц і 5 ГГц?

802 11g
802 11b
802 11a
802 11п

РОЗДІЛ 7. ПРИКЛАДНА МЕРЕЖЕВА ВЗАЄМОДІЯ

Даний розділ присвячений прикладній мережевій взаємодії. Ви навчитеся встановлювати й набудовувати мережеві інтерфейсні плати (NIC), підключати пристрої до безпроводового маршрутизатора й набудовувати безпроводової маршрутизатор для забезпечення зв'язку по мережі. Ви також навчитеся настроювати членство в домені в системі Windows і обмінюватися файлами за допомогою мережевих папок і підключення дисків. Важливою частиною ваших навичок в області мережевих технологій буде вміння визначити, якого постачальника послуг Інтернету слід вибрати для домашніх мереж або мереж невеликих офісів.

Мережі й Інтернет надають безліч важливих функцій і служб. Ви довідаєтеся про центри обробки даних і перевагах хмарних обчислень. Ви також вивчите деякі з найбільш важливих мережних додатків, у тому числі Веб, електронну пошту, обмін файлами, проксі-сервери й служби безпеки. Нарешті, ви навчитеся застосовувати системний метод для пошуку й усунення неполадок.

7.1 Контрольний список монтажу мережі

Технічні фахівці з комп'ютерів повинні вміти забезпечувати вимоги своїх замовників до мережі. Тому ви повинні бути знайомі з такими аспектами, як:

Компоненти мережі — включаючи провідні й безпроводові мережеві інтерфейсні плати (мережні адаптери, мережні плати, NIC) і мережеві пристрої, такі як комутатори, безпроводові точки доступу (access point, AP), маршрутизатори, багатофункціональні пристрої і т. п [4-9].

Проектування мережі — включаючи знання того, як мережі з'єднуються один з одним для задоволення потреб підприємства. Наприклад, потреби малого підприємства значно відрізняються від потреб великого підприємства.

Розглянемо мале підприємство з 10 співробітниками (рис. 7.1).

Підприємство уклало контракт із вами на підключення своїх користувачів. Як показано на рис. 7.1, при такому невеликому числі користувачів може використовуватися невеликий багатофункціональний пристрій. Багатофункціональний пристрій надає можливості маршрутизатора, комутатора, брандмауера й точки доступу. Такий багатофункціональний пристрій звичайний називається безпроводовим маршрутизатором.

Якщо підприємство набагато крупніше, звичайний безпроводовий маршрутизатор може не підійти. Організації можуть вимагатися окремі комутатори, точки доступу, міжмережеві екрани й маршрутизатори.

Незалежно від проекту мережі ви повинні вміти встановлювати мережеві плати, підключати провідні й безпроводові пристрої, а також настроювати базове мережеве обладнання.

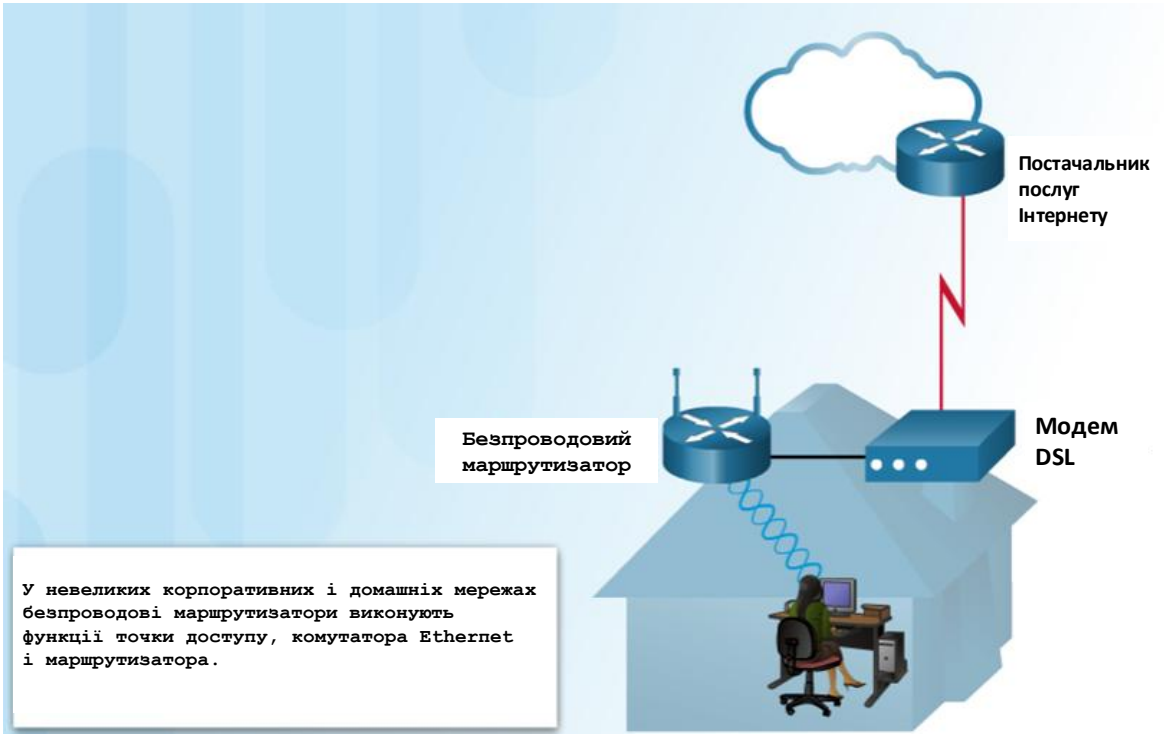


Рис. 7.1 – Невелика корпоративна або стандартна домашня мережа

Примітка. Ця глава зорієнтована на підключення й настроювання домашнього безпроводового маршрутизатора або безпроводового маршрутизатора невеликого офісу. Настроювання показуються за допомогою програми Packet Tracer [10, 11]. Разом з тим у всіх безпроводових маршрутизаторах є ті самі функції й схожий графічний користувацький інтерфейс. Ви можете придбати безліч недорогих бездпроводових маршрутизаторів як в інтернет-магазинах, так і у звичайних магазинах, комп'ютерних магазинах і магазинах побутової електроніки. Є безліч виробників, у тому числі Asus, Cisco, D-Link, Linksys, Netgear і Trendnet.

7.1.1 Компоненти мережі

7.1.1.1 Вибір мережевої плати

Для підключення до мережі потрібна мережева плата. Як показано на рис. 7.2, є різні типи мережевих плат: Мережеві плати Ethernet використовуються для підключення до мереж Ethernet, а безпроводові мережеві плати використовуються для підключення до безпроводових мереж 802.11. Більшість мережевих плат у настільних комп'ютерах інтегроване в материнську плату або підключається до слотів розширення. Мережеві плати також доступні у форм-факторі USB [4-9].

Питання, які треба враховувати при придбанні нової мережевої плати.

Тип мережної плати:

- Провідна (Fast Ethernet або Gigabit Ethernet)?

- Безпроводова 802.11n або 802.11 ac?
- Тип підключення:
- Роз’єм (PCI або PCIe)?
- USB?

Додаткові властивості мережевої плати:

- Пробудження по локальній мережі (WOL)?
- Якість обслуговування (Qos)?
- Ціна?

Якщо замовник попросить забезпечити більш високу швидкість або нові функції мережі, інженер повинен уміти обновити, установити й настроїти компоненти. Якщо замовник додає додаткові комп'ютери або безпроводові функції, інженер повинен бути здатний порекомендувати встаткування, відповідне до потреб, наприклад, безпроводові точки доступу або безпроводові мережеві плати. Пропоноване обладнання повинне працювати з наявним обладнанням і прокладеними кабелями. В іншому випадку необхідно обновити існуючу інфраструктуру. Іноді може знадобитися обновити драйвер.



Рис. 7.2 – Типи мережевих плат

7.1.1.2 Установка й оновлення мережевої плати

Для установки мережної плати в настільний комп'ютер необхідно зняти кришку корпусу. Потім зніміть кришку з доступного роз’єму. Після надійної установки мережевої плати встановите кришку на місце.

У безпроводової мережевої плати є антена, підключена до задньої частини плати або підключена кабелем, що дозволяє відрегулювати її положення для найкращого прийому сигналу. Необхідно підключити й розташувати антену.

Іноді виготовлювач публікує нове програмне забезпечення драйвера для мережевої плати. Новий драйвер може поліпшувати функції мережевої плати. Він також може вимагатися для забезпечення сумісності з операційною системою. Новітні драйвери для всіх підтримуваних операційних систем доступні для завантаження з веб-сайту виробника.

Щоб гарантувати коректну установку драйвера, може знадобитися відключення антивірусного ПЗ. Деяке антивірусне ПЗ визначає оновлення драйвера як можливу вірусну атаку. Не встановлюйте кілька драйверів одночасно; а якщо ні, то може відбутися конфлікт деяких процесів оновлення. Рекомендується закрити працюючі додатки, щоб вони не використовували файли, пов'язані з оновленням драйвера.

Також можна обновити драйвер мережної плати вручну.

В Windows 8 і Windows 8.1 виберіть:

Control Panel > Hardware and Sound > Device Manager (Панель управління > Обладнання й звук > Диспетчер пристроїв)

В Windows 7 і Windows Vista виберіть:

Start > Control Panel > Device Manager (Пуск > Панель управління > Диспетчер пристроїв)

В Windows 7 для перегляду встановлених мережевих адаптерів клацніть стрільцю поруч із категорією. Двічі клацніть по адаптеру, щоб переглянути й змінити його властивості. У вікні Adapter Properties (Властивості адаптера) перейдіть на вкладку Driver (Драйвер).

Примітка. Іноді при установці драйвера може з'явитися запит на перезавантаження комп'ютера.

Якщо після установки нового драйвера мережевої плати вона не працює належним чином, можна видалити драйвер і відкотити драйвер до попередньої версії. Двічі клацніть адаптер у вікні **Device Manager** (Диспетчер пристроїв). У вікні Adapter Properties (Властивості адаптера) перейдіть на вкладку **Driver** (Драйвер) і натисніть **Roll Back Driver** (Відкотити). Якщо перед оновленням драйвер не був установлений, цей пункт недоступний, як показано на рис. 7.3.

У цьому випадку необхідно знайти драйвер для пристрою й установити його вручну, якщо операційна система не може знайти підходящий драйвер для мережевої плати.

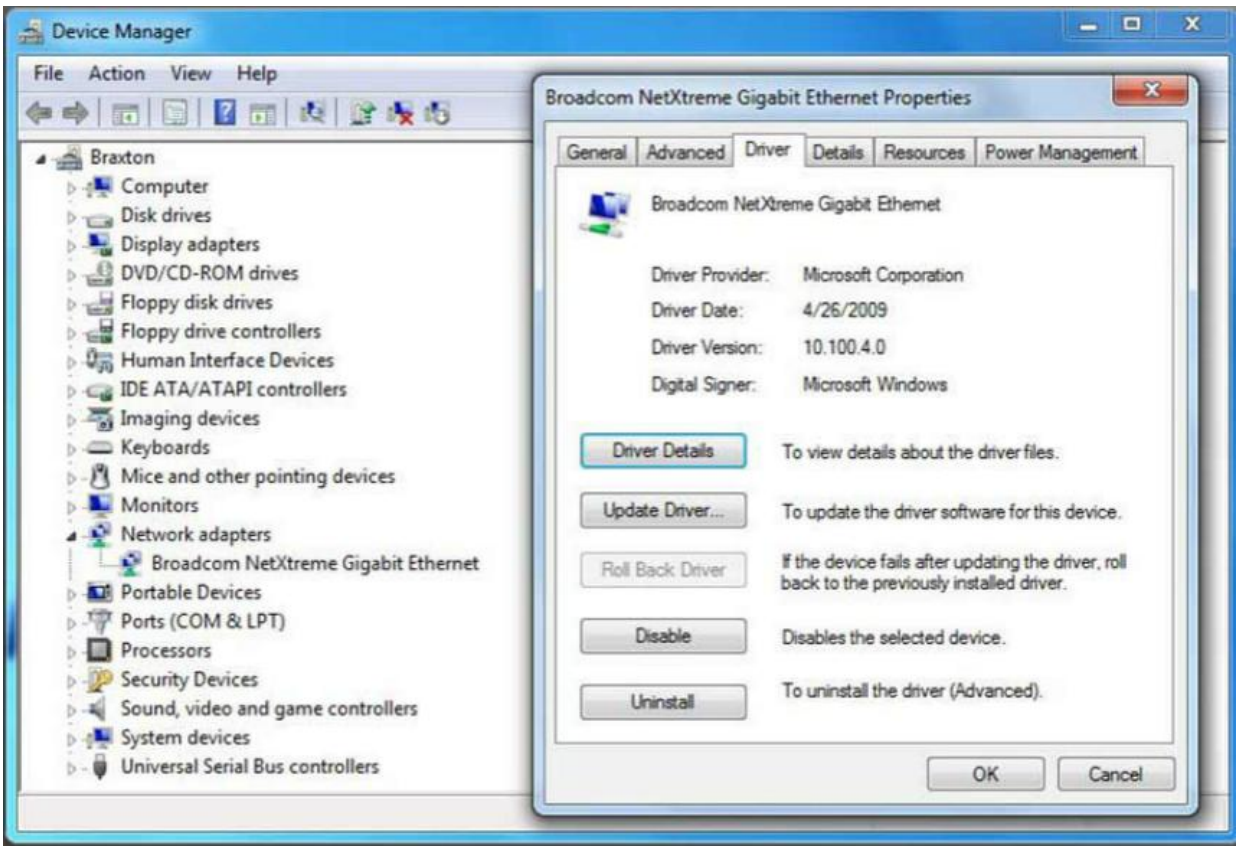


Рис. 7.3 – Управління драйвером мережевої плати

7.1.1.3 Настройка мережевої плати

Після установки драйвера мережевої плати необхідно настроїти параметри IP-адресації. Комп'ютеру можна призначити настроювання IP одним із двох способів:

Вручну — вузлу статично призначаються певні настроювання IP.

Динамічно — вузол запитує настроювання IP-Адресації в DHCP-Сервера.

Для ручного настроювання IP-параметрів в Windows 8 і 8.1 використовуйте наступний спосіб:

виберіть **Control Panel > Network and Internet > Network and Sharing Center > Change adapter settings** (Панель управління > Мережа й Інтернет > Центр управління мережами й загальним доступом > Зміна параметрів адаптера) і натисніть праву кнопку миші на **Ethernet**. Відкриється вікно Ethernet Properties (Властивості Ethernet).

В Windows 7 і Windows Vista виберіть:

Start > Control Panel > Network and Sharing Center > Change adapter settings (Мережа > Панель управління > Центр управління мережами й загальним доступом > Зміна параметрів адаптера) і натисніть праву кнопку миші на **Local Area Connection** (Підключення по локальній мережі). Це приводить до відкриття вікна Local Area Connection Properties (Властивості підключення по локальній мережі), показаного на рис. 7.4.

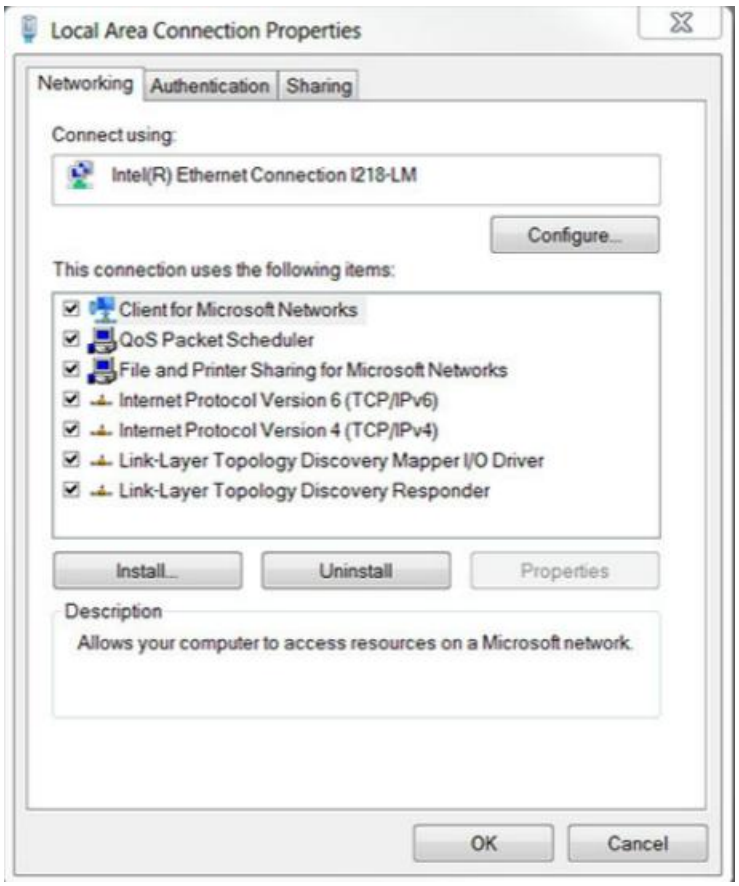


Рис. 7.4 – Вікно Local Area Connection Properties (Властивості підключення по локальній мережі)

Щоб настроїти параметри IPv4, натисніть **Internet Protocol Version 4 (TCP/IPv4) > Properties** (Протокол Інтернету версії 4 (TCP/IPv4) > Властивості). Це приводить до відкриття вікна Internet Protocol Version 4 (TCP/IPv4) Properties (Властивості протоколу Інтернету версії 4 (TCP/IPv4)), показаного на рис. 7.5. Зверніть увагу, що настроювання за замовчуванням полягає в автоматичному одержанні IP-параметрів за допомогою DHCP.

Щоб змінити настроювання вручну, натисніть **Use the following IP address** (Використовувати наступний IP-адресу), як показано на рис. 7.6. Потім уведіть відповідну адресу IPv4, маску підмережі й шлюз за замовчуванням і натисніть **OK > OK**.

Щоб настроїти параметри IPv6, натисніть **Internet Protocol Version 6 (TCP/IPv6) > Properties** (Протокол Інтернету версії 4 (TCP/IPv4) > Властивості). Це приводить до відкриття вікна Internet Protocol Version 6 (TCP/IPv6) Properties (Властивості протоколу Інтернету версії 6 (TCP/IPv6)), показаного на рис. 7.7

Натисніть **Use the following IPv6 address** (Використовувати наступний IPv6-адресу), як показано на рис. 7.8. Потім уведіть відповідний IPv6-адресу, довжину префіксу й шлюз за замовчуванням і натисніть **OK > OK**.



Рис. 7.5 – Динамічне настроювання IPv4

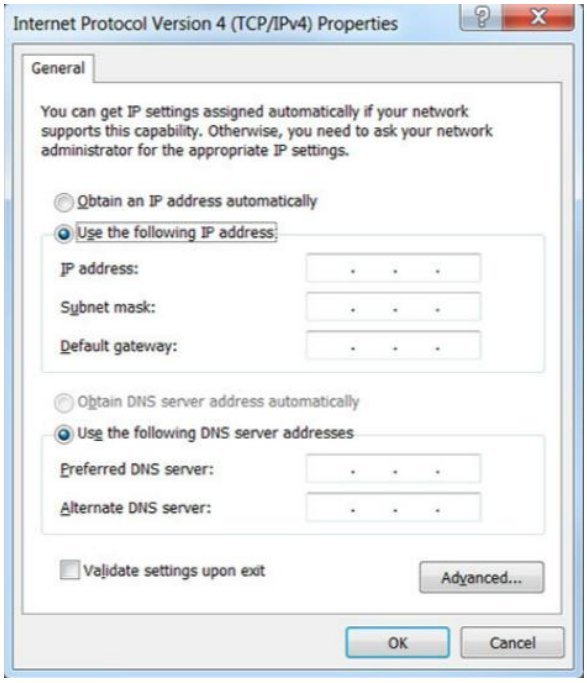


Рис. 7.6.Статичне настроювання IPv4

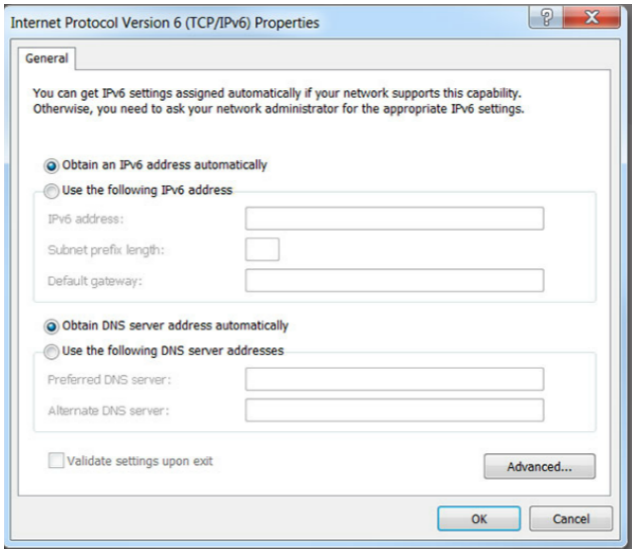


Рис. 7.7 – Динамічне настроювання IPv6

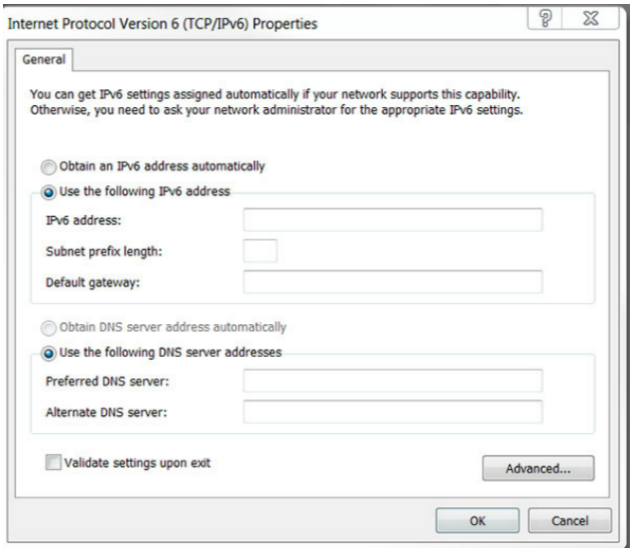


Рис. 7.8 – Статичне настроювання IPv6

Примітка. Більшість комп'ютерів сьогодні поставляються із вбудованою мережевою платою. При установці нової мережевої плати рекомендується відключити вбудовану мережеву плату в параметрах BIOS.

7.1.1.4 Додаткові параметри мережної плати

Деякі адаптери надають додаткові функції. У більшості мережевих середовищ для мережевої плати необхідно настроїти тільки IP-адресу. Для додаткових параметрів мережевої плати можна залишити значення

за замовчуванням. Однак при підключенні комп'ютера до мережі, яка не підтримує деякі або всі параметри за замовчуванням, необхідно ввести зміни. Настроювання додаткових параметрів може вимагатися для підключення комп'ютера до мережі, включення функцій, необхідних мережі, або поліпшення мережевого підключення.

Примітка. Неправильне настроювання додаткових функцій може привести до збою підключення або зниженню продуктивності.

Додаткові функції перебувають на вкладці **Advanced** (Додатково) у вікні настроювання мережевої плати. На вкладці **Advanced** (Додатково) утримуються всі параметри, надані виробником мережевої плати.

Примітка. Доступні додаткові функції й специфікація функцій на вкладці залежать від ОС, конкретного адаптера мережної плати й установленого драйвера.

До деяких додаткових функцій на вкладці ставляться наступні:

Швидкість і дуплексний режим — ці параметри повинні збігатися з настроюваннями пристрою, до якого підключена мережева плата. За замовчуванням параметри узгоджуються автоматично. Невідповідність по швидкості або дуплексному режиму може привести до зниження швидкості передачі даних. Якщо так і відбувається, може виникнути необхідність зміни швидкості й/або дуплексного режиму. На рис. 7.9 показані параметри швидкості й дуплексного режиму.

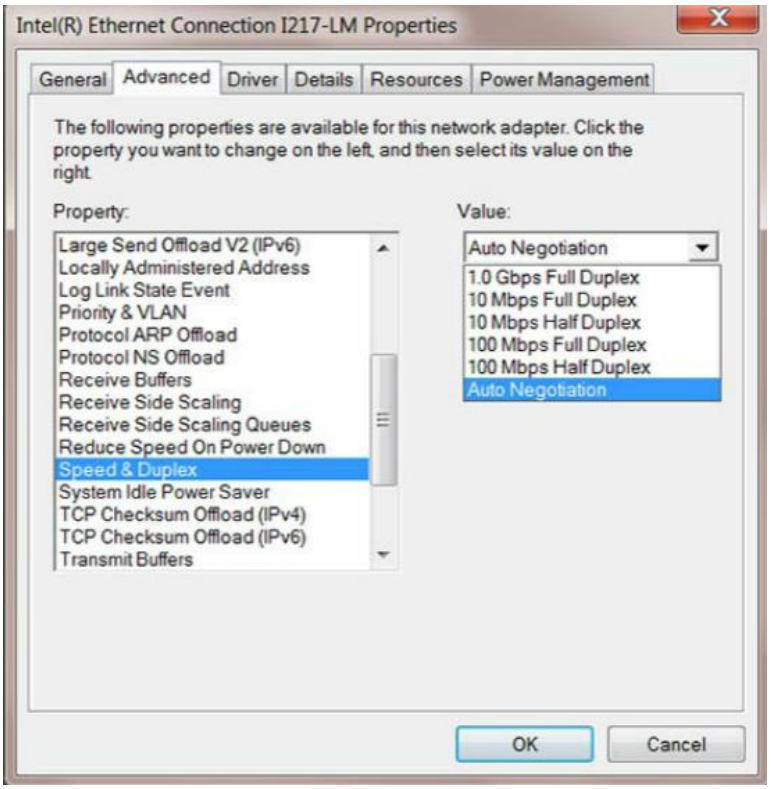


Рис. 7.9 – Параметри швидкості й дуплексного режиму

Wake on LAN (Пробудження по локальній мережі) — параметри WOL використовуються для пробудження мережевого комп'ютера з режиму низького енергоспоживання. Режим низького енергоспоживання означає, що комп'ютер виключений, але як і раніше підключений до джерела живлення. Для підтримки WOL комп'ютер повинен мати джерело живлення, сумісний з ATX, і мережеву плату, сумісну з WOL. Повідомлення пробудження, називане магічним або чарівним пакетом (magic packet), відправляється на мережеву плату комп'ютера. Цей пакет містить MAC-адресу мережної плати комп'ютера. При одержанні мережевою платою магічного пакета комп'ютер виходить зі сплячого режиму. Параметри WOL настроюються в BIOS материнської плати або в прошиванні мережевої плати. На рис. 7.10 показане настроювання в прошиванні драйвера.

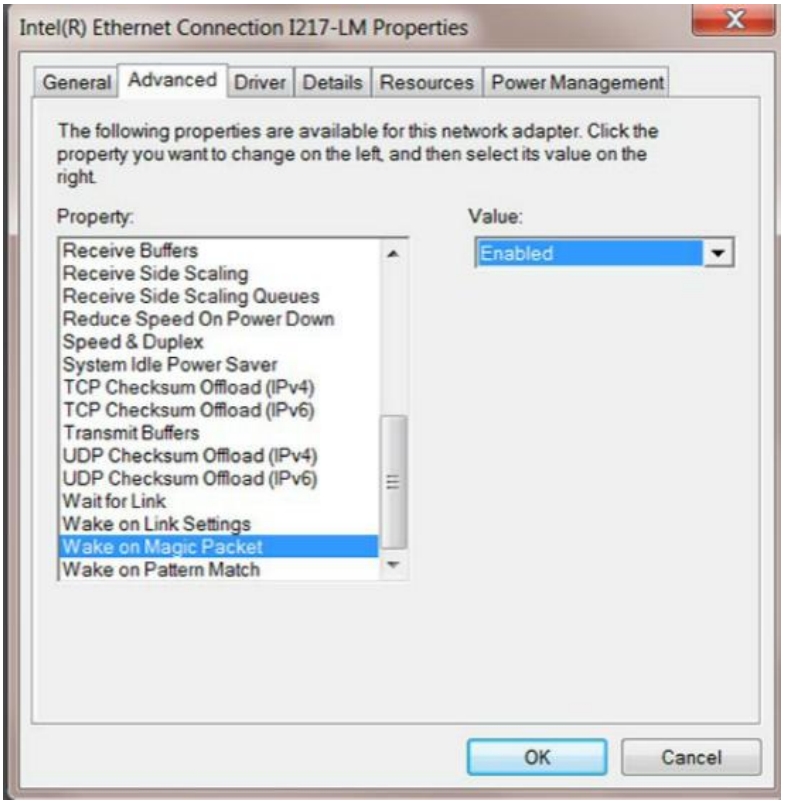


Рис. 7.10 – Параметр WOL

Якість обслуговування — Qos (Quality of Service, також називається 802.1q Qos) складається з безлічі методів, які управляють потоком мережевого трафіка, підвищують швидкість передачі даних і поліпшують передачу трафіка комунікацій у реальному часі. Qos повинне бути включене й на комп'ютері, і мережевому пристрої, щоб служба працювала. Якщо Qos установлене й включене на комп'ютері, Windows може обмежити доступну пропускну спроможність із обліком високо пріоритетного трафіка. Якщо Qos відключене, увесь трафік обробляється однаково. Qos включене за замовчуванням, як показано на рис. 7.11.

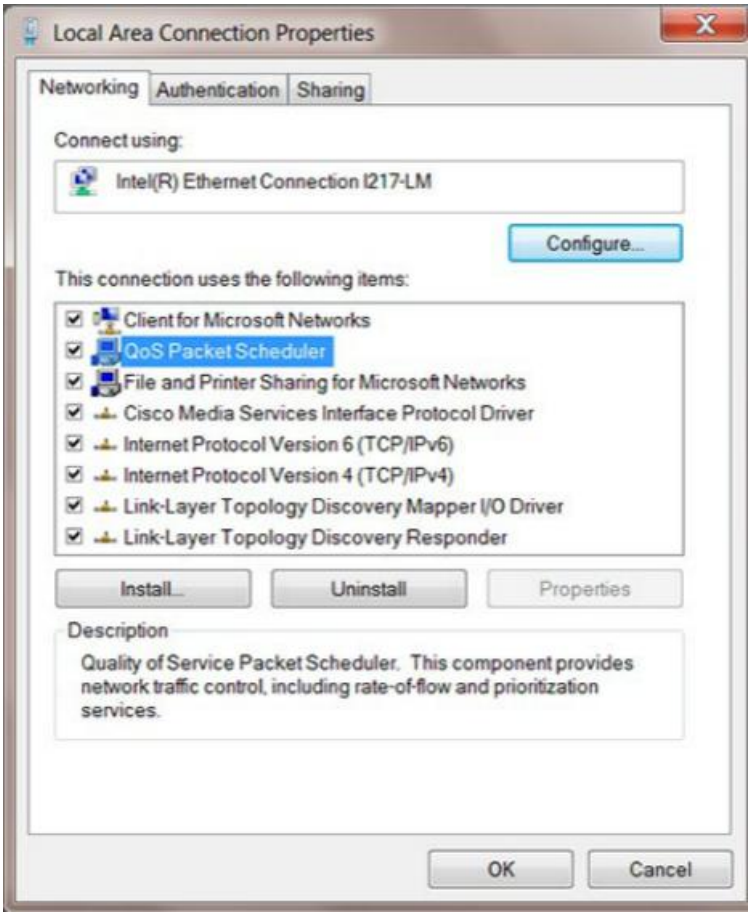


Рис. 7.11 – Механізм Qos включений по умовчанню

7.1.1.5 Підключення мережевої плати

Щоб підключитися до мережі, приєднаєте прямий кабель Ethernet до порту мережної плати, як показано на рис. 7.12. У домашній мережі або мережі невеликого офісу інший кінець кабелю часто підключається до порту Ethernet на безпроводовому маршрутизаторі. У корпоративній мережі комп'ютер найчастіше підключається до настінної розетки, яка, у свою чергу, підключається до мережевого комутатора.

Мережеві плати звичайно мають один або трохи зелених або жовтих світлодіодів або індикаторів зв'язку, як показано на рис. 7.12. Ці індикатори використовуються для позначення наявності канального підключення і його активності. Зелені світлодіоди часто використовуються для позначення наявності активного канального підключення, тоді як жовті світлодіоди часто використовуються для позначення мережевої активності.

Примітка. Призначення світлодіодних індикаторів залежить від конкретного виробника мережевої плати. Для одержання додаткової інформації див. документацію по материнській або мережевій платі.

Якщо світлодіоди не горять, це вказує на проблему. Відсутність активності може означати неправильне настроювання мережевої плати,

несправний кабель, несправний порт комутатора або навіть несправну мережеву плату. Для усунення неполадки може знадобитися замінити одне або кілька цих пристроїв.

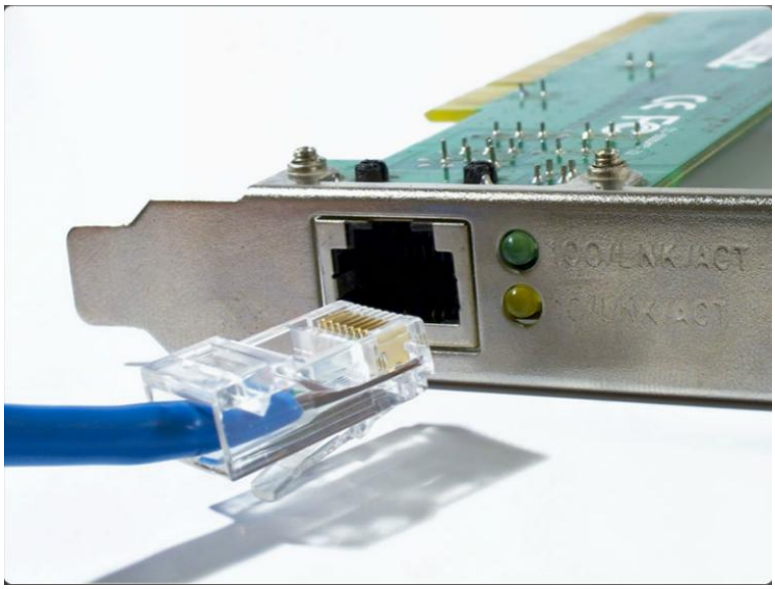


Рис. 7.12 – Індикатори зв'язку мережевої плати

7.1.1.6 Підключення маршрутизатора до Інтернету

Безпроводової маршрутизатор має кілька портів для підключення провідних пристроїв. Наприклад, безпроводової маршрутизатор на рис. 7.13 має USB-порт, порт Інтернет і чотири порти локальної мережі (LAN). Порт **Internet** (Інтернет) є Ethernet -портом, який використовується для підключення маршрутизатора до пристрою провайдера, наприклад широкосмуговому DSL– модему або кабельному модему.



Рис. 7.13 – Порти безпроводового маршрутизатора

Топологія для підключення до пристроїв показана на рис. 7.14.

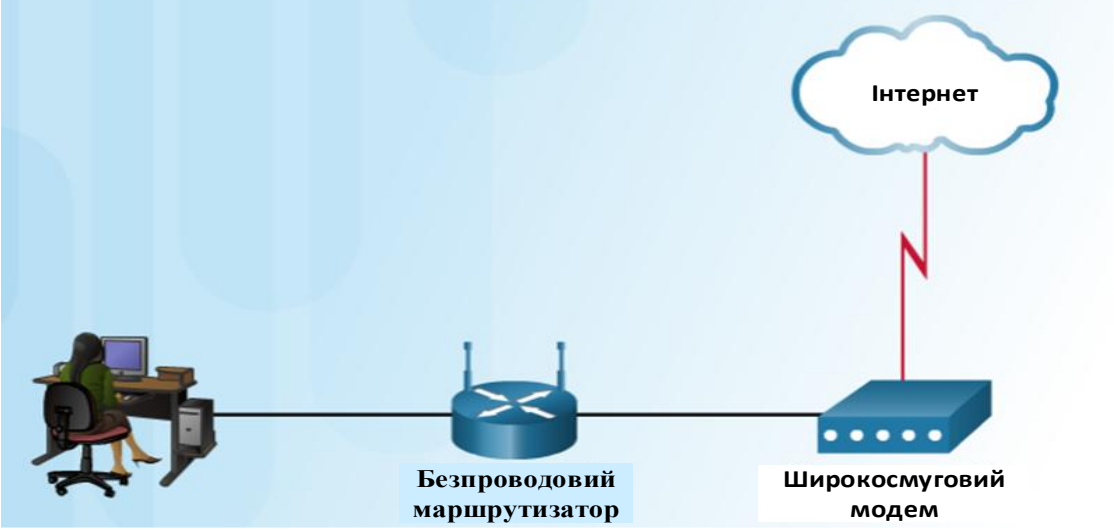


Рис. 7.14 – Підключення маршрутизатора для доступу в Інтернет

Дії для підключення безпроводового маршрутизатора до порту широкосмугового модему такі:

Крок 1. На маршрутизаторі підключите прямій Ethernet-Кабель до порту **Internet** (Інтернет). Цей порт також може називатися **WAN**. Комутуюча логіка пристрою пересилає всі пакети через цей порт при передачі даних між Інтернетом і підключеними комп'ютерами.

Крок 2. На широкосмуговому модемі постачальника послуг підключите інший кінець кабелю до відповідного до порту. Типові позначення цього порту — **Ethernet**, **Internet** і **WAN**.

Крок 3. Включите широкосмуговий модем і підключите кабель живлення до маршрутизатора. Після того як модем установлює з'єднання з постачальником послуг Інтернету, він починає обмінюватися даними з маршрутизатором. Індикатори Інтернету на маршрутизаторі загоряються, указуючи на наявність зв'язку. Модем дозволяє маршрутизатору одержувати необхідну мережеву інформацію, необхідну для одержання доступу до Інтернету від інтернет-провайдера. Ця інформація містить у собі публічні IP-адреси, маску підмережі й адреси DNS-серверів.

7.1.2 Проектування мережі

7.1.2.1 Настройка мережевого розташування

При першому підключенні системи Windows до мережі необхідно вибрати профіль мережевого розташування. Кожний профіль мережевого розташування має різні параметри за замовчуванням. Залежно від обраного профілю загальний доступ до файлів і принтерам або виявлення мережі можуть бути включені або виключені. Крім того, можуть бути застосовані різні параметри брандмауера.

Система Windows містить три профілі мережевого розташування (рис. 7.15):

Home Network (Домашня мережа) — виберіть це мережеве розташування для домашніх мереж або якщо ви довіряєте користувачам і пристроям у мережі. Мережеве виявлення включене, що дозволяє переглядати інші комп'ютери й пристрою в мережі, а інші користувачі мережі можуть бачити ваш комп'ютер.

Work Network (Робоча мережа) — виберіть це мережеве розташування для мережі невеликого офісу або мережі на іншому робочому місці. Мережне виявлення включене. Не можна створити домашню групу або приєднатися до неї.

Public Network (Суспільна мережа) — виберіть це мережеве розташування для аеропортів, кафе й інших громадських місць. Мережеве виявлення виключене. Це мережеве розташування надає найкращий захист. Також виберіть це мережеве розташування при підключенні до Інтернету прямо без використання маршрутизатора або при використанні широкосмугового мобільного зв'язку. Домашня група недоступна.

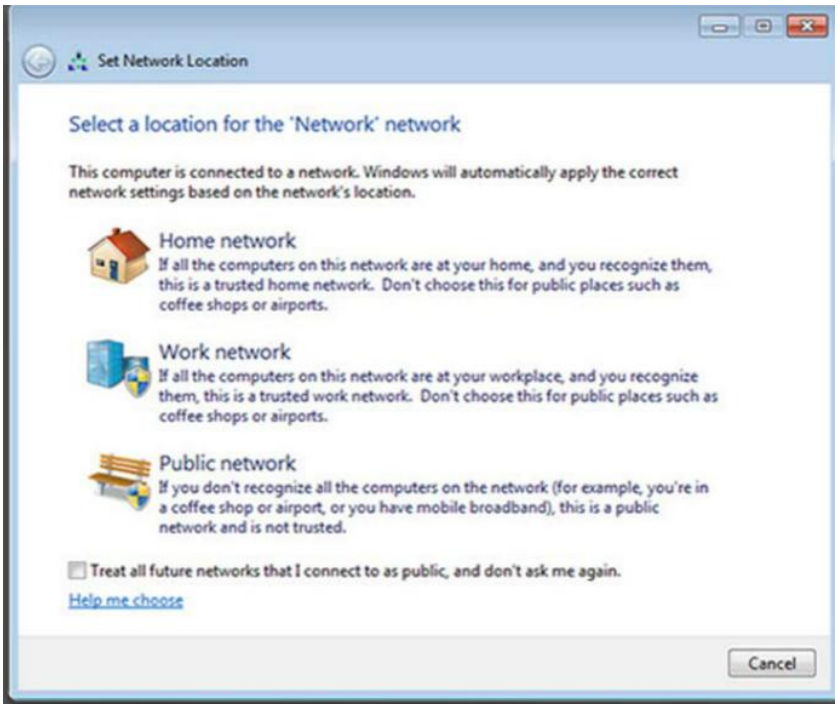


Рис. 7.15 – Вікно Set Network Location (Настроювання мережевого розміщення)

Комп'ютери, які належать суспільній, робочій або домашній мережі й мають доступ до загальних ресурсів, повинні бути членами однієї робочої групи. Комп'ютери в домашній мережі також можуть належати до домашньої групи. Домашня група надає простий спосіб загального доступу до файлів і принтерам. Windows Vista не підтримує функцію домашньої групи.

Існує й четвертий профіль мережевого розташування за назвою **Domain Network** (Доменна мережа), який звичайно використовується для корпоративних робочих місць. Цей профіль управляється адміністратором мережі й не може бути обраний або змінений користувачами, підключеними до мережі підприємства.

Примітка. При наявності в мережі тільки одного комп'ютера, якщо загальний доступ до файлів або принтерів не потрібно, найбільш безпечним вибором є варіант Public (Суспільна).

Можна змінити параметри за замовчуванням для всіх профілів мережевого розташування, як показано на рис. 7.16. Зміни в профілі за замовчуванням застосовуються для всіх мереж, які використовують цей профіль мережевого розташування.

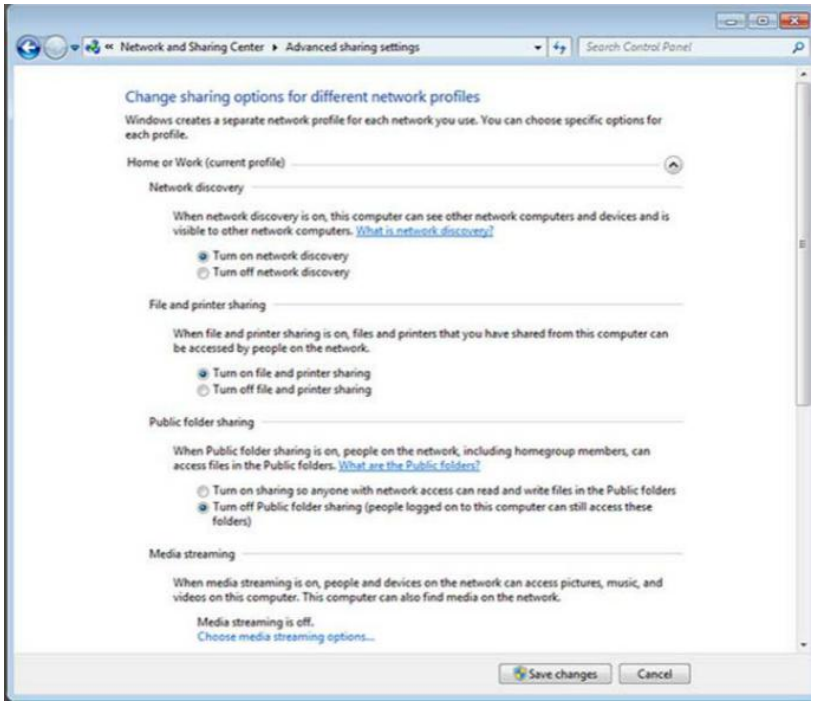


Рис. 7.16 – Параметри загального доступу за замовчуванням

Якщо вікно Set Network Location (Настроювання мережевого розміщення) не відображається при першому підключенні до мережі, може знадобитися звільнити (release) і обновити (renew) IP-адреса комп'ютера. Відкрийте командний рядок на комп'ютері, уведіть **ipconfig /release**, а потім **ipconfig /renew** для одержання IP-адреси від маршрутизатора.

7.1.2.2 Вхід на маршрутизатор

Більшість домашніх безпроводових маршрутизаторів і безпроводових маршрутизаторів для невеликих офісів готові до роботи відразу « з коробки». Вони не вимагають ніякого додаткового настроювання. Разом з тим в Інтернеті легко перебувають IP-адреси за замовчуванням для безпроводових маршрутизаторів, імена користувачів і паролі. Просто

введіть таку фразу для пошуку, як default wireless router ip address (IP-адреса за замовчуванням для безпроводового маршрутизатора) або default wireless router passwords (паролі за замовчуванням для безпроводових маршрутизаторів), для відображення списку багатьох веб-сайтів, які надають цю інформацію. Таким чином, першочерговим завданням є зміна цих параметрів за замовчуванням з метою забезпечення безпеки.

Для доступу до графічного користувацького інтерфейсу настроювання безпроводового маршрутизатора відкрийте веб-браузер. У поле Address (Адресу) уведіть приватну IP-Адресу за замовчуванням для безпроводового маршрутизатора. IP-адреса за замовчуванням можна знайти або в документації, яка поставляється з безпроводовим маршрутизатором, або в Інтернеті. На рис. 7.17 показані IP-Адреса 192.168.0.1, яка є загальним стандартним IP-адресом для деяких виробників. Вікно Security (Безпека) запитує авторизацію для одержання доступу до графічного користувацького інтерфейсу маршрутизатора. Слово **admin** звичайно використовується в якості імені користувача й пароля за замовчуванням.

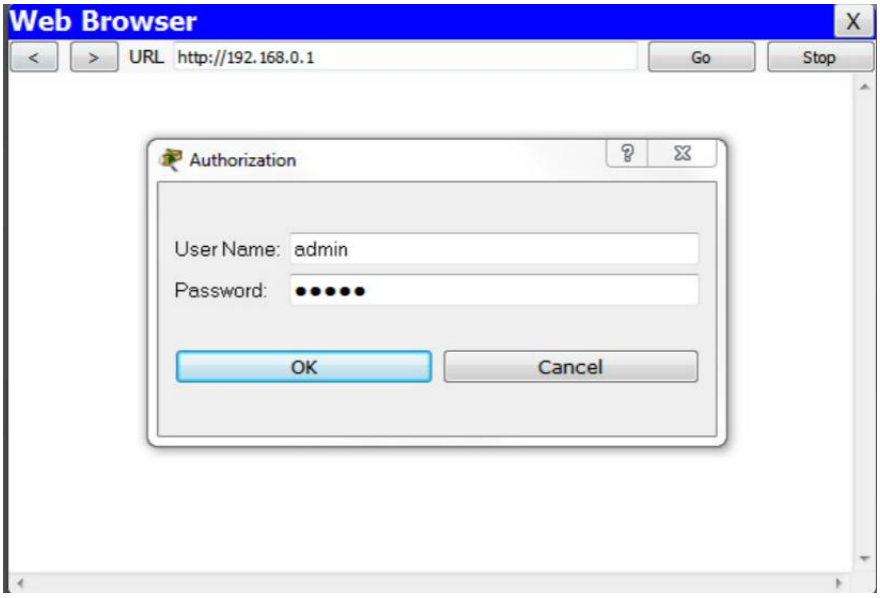


Рис. 7.17 – Вхід на маршрутизатор

Як і минулого разу, звіритеся з документацією до вашого безпроводового маршрутизатора або виконаєте пошук в Інтернеті.

7.1.2.3 Базове настроювання мережі

Після входу в систему з'явиться екран настроювань, як показано на рис. 7.18, а). На екрані настроювання буде присутній вкладки або меню, які допоможуть переключатися на різні завдання настроювання маршрутизатора. Часто необхідно зберігати параметри, змінені в одному вікні, перед переходом в інше вікно.

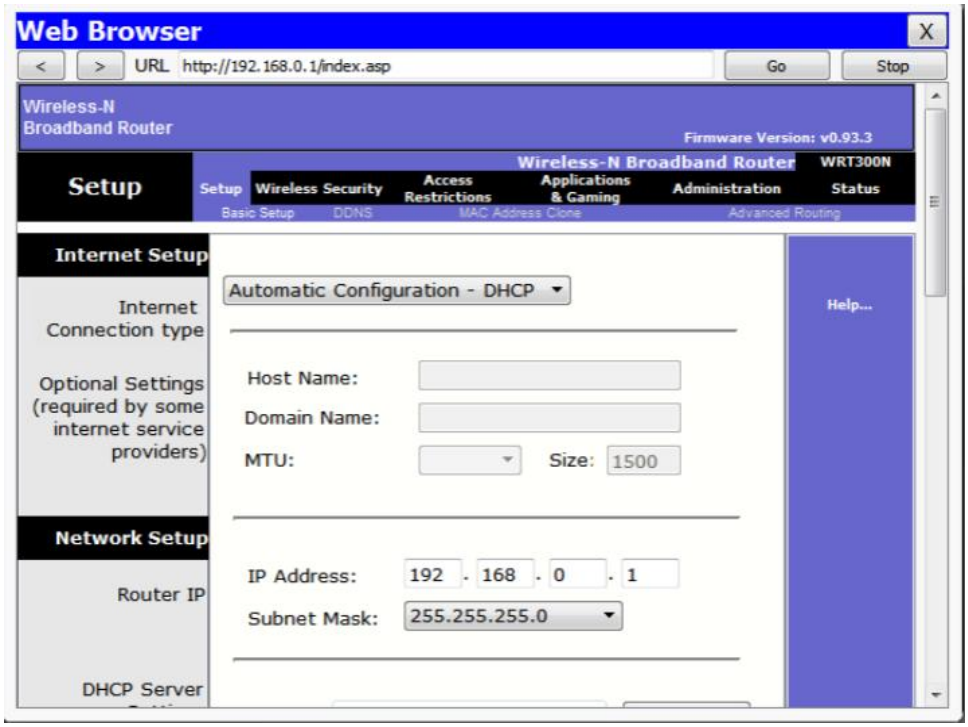


Рис. 7.18, а – Базове настроювання мережі

У такій ситуації рекомендується вносити зміни в параметри за замовчуванням.

Network Device Access Permissions (Дозволу на доступ до мережевого обладнання) — змініте ім'я користувача й пароль за замовчуванням. На деяких обладнаннях можна тільки скинути пароль, як показано на рис. 7.18, б).

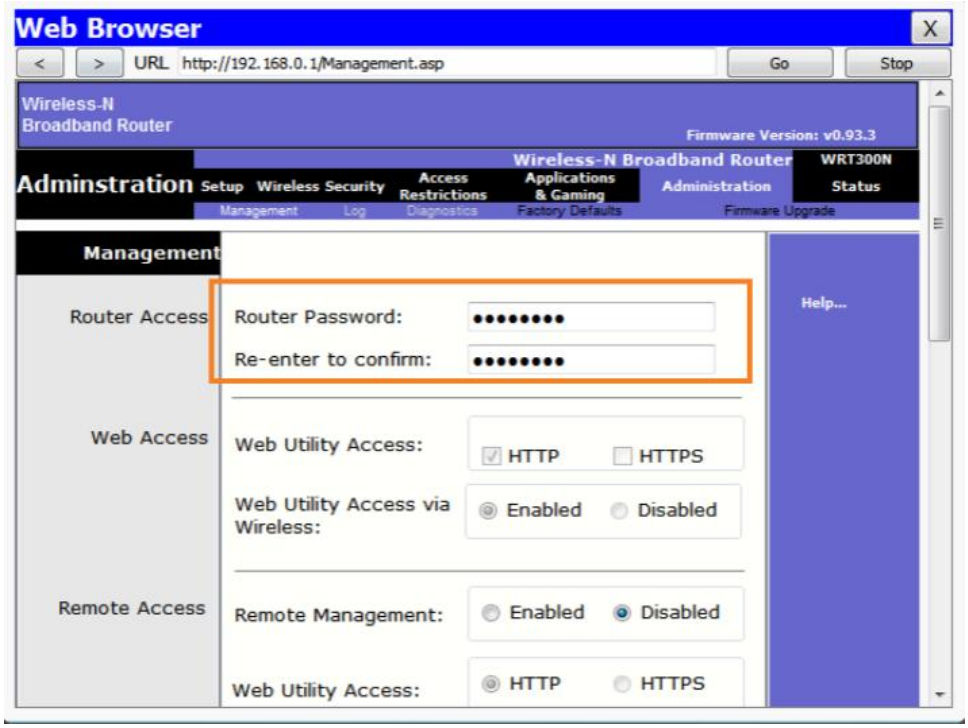


Рис. 7.18, б – Базове настроювання мережі

Після зміни пароля безпроводовий маршрутизатор знову запросить авторизацію, як показано на рис. 7.18, в).

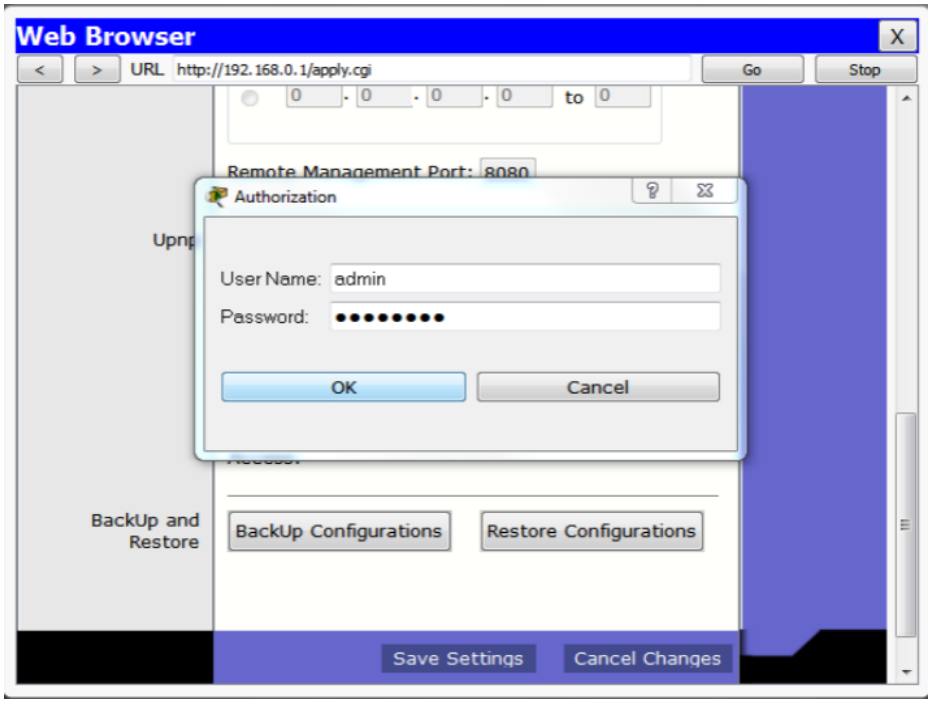


Рис. 7.18, в – Базове настроювання мережі

Router IP Address (IP-адреса маршрутизатора) — зміните IP-адресу за замовчуванням для маршрутизатора. Рекомендується використовувати приватну IP-адресацію усередині своєї мережі. IP-адреса 10.10.10.1 використовується як приклад на рис. 7.18, г).

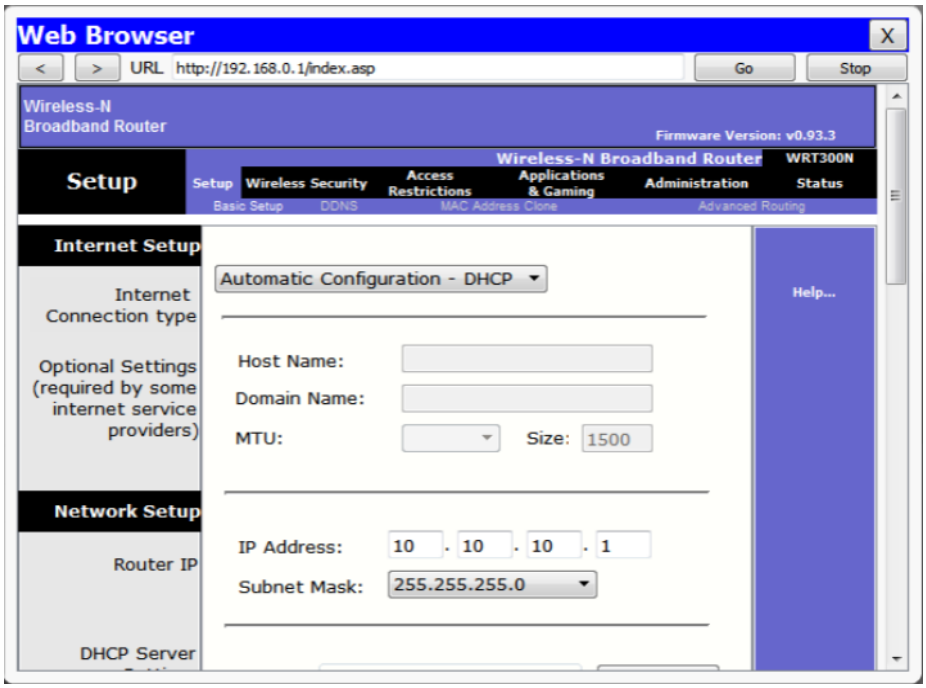


Рис. 7.18, г – Базове настроювання мережі

- Разом з тим це може бути будь-який приватний IP-адреса, обраний вами. Натискання кнопки Save (Зберегти) приведе до тимчасової втрати доступу до безпроводового маршрутизатора. Для повторного одержання доступу обновите свої IP-параметри, як показано на рис. 7.18, д). Потім уведіть нову IP-адресу маршрутизатора у веб-браузері й пройдіть автентіфікацію з новим паролем, як показано на рис. 7.18, е).

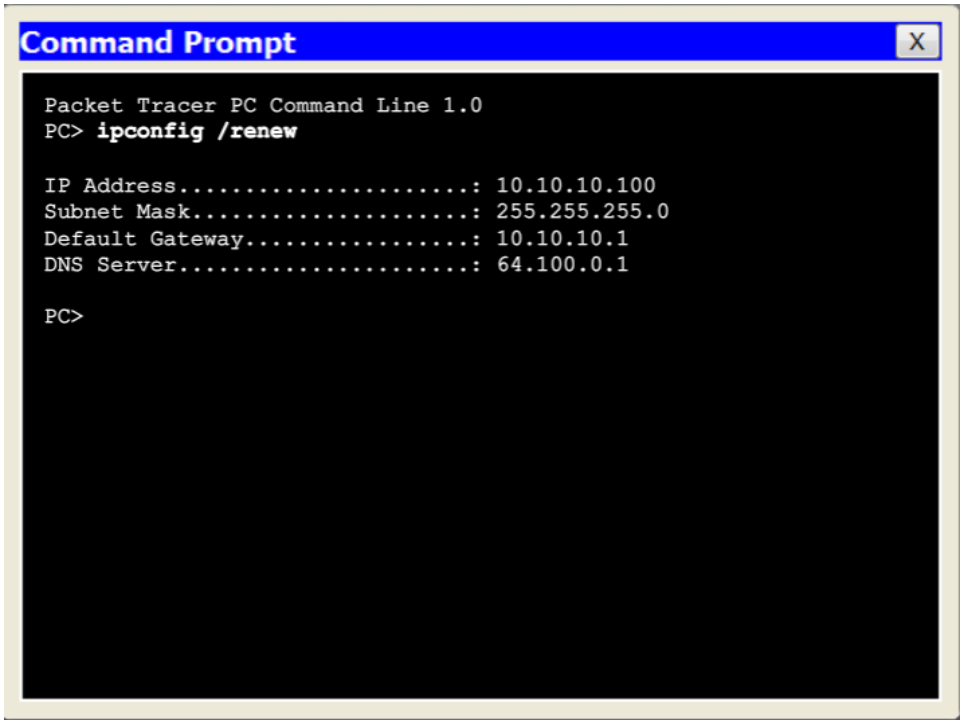


Рис. 7.18, д – Базове настроювання мережі

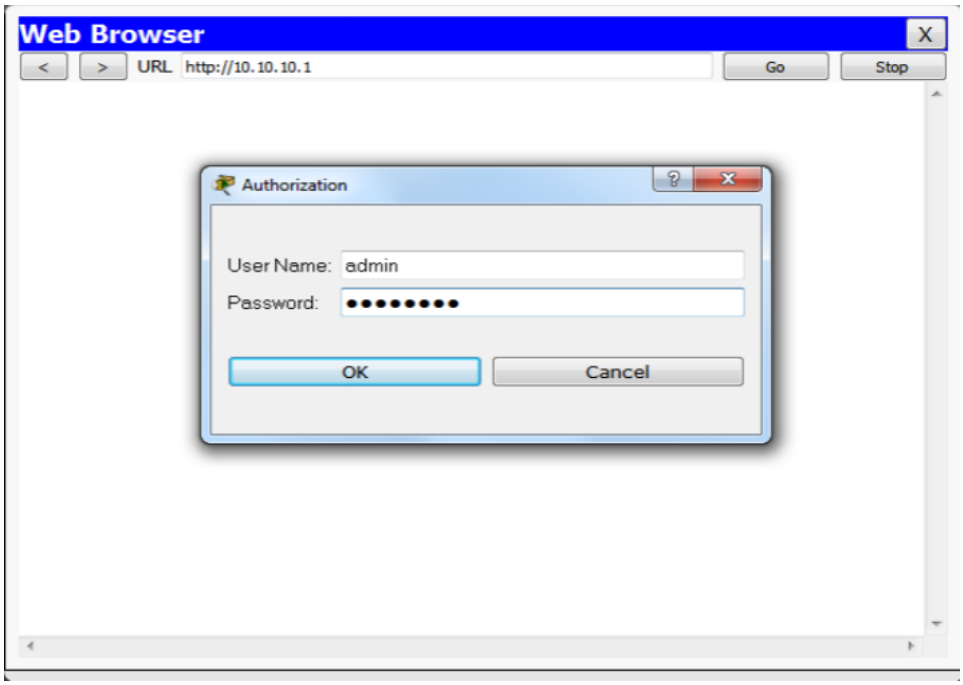


Рис. 7.18, е – Базове настроювання мережі

Деякі параметри за замовчуванням слід змінити, інші рекомендується залишити незмінними. У більшості домашніх мереж і мереж невеликих офісів використовується одне підключення до Інтернету, надане постачальником послуг доступу до Інтернету. Маршрутизатори в мережах цього типу одержують публічні адреси від постачальника послуг Інтернету, що дозволяє маршрутизатору відправляти й одержувати пакети з Інтернету. Маршрутизатор надає приватні адреси локальним мережевим вузлам. Оскільки приватні адреси не можуть використовуватися в Інтернеті, використовується процес їх перетворення в унікальні публічні адреси. Це дозволяє локальним вузлам обмінюватися даними через Інтернет.

Процес перетворення приватних адрес у маршрутизовані в Інтернеті адреси називається перетворенням мережевих адрес (NAT). За допомогою NAT приватний (локальний) IP-адреса джерела перетворюється в публічну (глобальну) адресу. Вхідні пакети проходять зворотний процес. Використовуючи NAT, маршрутизатор може перетворити відразу безліч внутрішніх IP-адрес у публічні.

Перетворювати потрібно тільки адреси пакетів, які йдуть в інші мережі. Ці пакети повинні пройти через шлюз, де маршрутизатор заміняє частки IP-адреси вихідних вузлів на загальні IP-адреси маршрутизатора.

Кожний вузол у внутрішній мережі має унікальну приватну IP-адресу, однак вузли спільно використовують маршрутизовані в Інтернеті адреси, призначені маршрутизатору постачальником послуг Інтернету.

7.1.2.4 Основні параметри безпроводової мережі

Установивши підключення до маршрутизатора, рекомендується настроїти деякі основні параметри для захисту безпроводової мережі.

Network Mode (Режим мережі) — деякі безпроводові маршрутизатори дозволяють вибирати, який стандарт 802.11 слід підтримувати. На рис. 7.19 показаний варіант Wireless-N Only (Тільки Wireless-N). Це означає, що у всіх безпроводових обладнаннях, які підключаються до безпроводового маршрутизатора, повинні бути встановлені мережні плати 802.11n. У табл 7.1 представлені інші режими мережі.

Network Name (SSID) (Ім'я мережі (SSID)) — призначте ім'я або ідентифікатор (SSID) безпроводової мережі. Безпроводовий маршрутизатор повідомляє про свою присутність за допомогою виконання широкомовного розсилання його SSID. Це дозволяє безпроводовим вузлам автоматично виявляти ім'я безпроводової мережі. Якщо широкомовне розсилання SSID відключена, на безпроводових обладнаннях необхідно вводити SSID вручну.

Channel (Канал) — безпроводові обладнання взаємодіють у певних діапазонах частот. Перешкоди можуть бути викликані, що перебувають поблизу безпроводовими маршрутизаторами або домашніми електронними обладнаннями, такими як безпроводові телефони й радіо-няні, які використовують той же діапазон частот. Ці обладнання можуть знизити

продуктивність безпроводової мережі або навіть викликати розрив мережевих підключень. Установка номера каналу може допомогти уникнути перешкод безпроводового зв'язку. Для стандартів 802.11b і 802.11g найчастіше використовуються канали 1, 6 і 11 для запобігання перешкод.

Wireless Security (Безпека безпроводової мережі) — більшість безпроводових маршрутизаторів підтримують кілька різних режимів безпеки.



Рис. 7.19 – Варіант Wireless-N Only (Тільки Wireless-N).

Таблиця 7.1 – Типові режими мережі

Режими мережі	Опис
Mixed (Змішаний)	• Режим за замовчуванням. • Виберіть при наявності обладнань 802.11n (2,4 Ггц), 802.11 g, і 802.11b.
Wireless-B/G Only (Тільки Wireless-B/G)	Виберіть при наявності обладнань 802.11b і 802.11g (2,4 ГГц).
Wireless-B Only (Тільки Wireless-B)	Виберіть при наявності тільки обладнань 802.11b.
Wireless-G Only (Тільки Wireless-G)	Виберіть при наявності тільки обладнань 802.11g.
Wireless-N	Виберіть при наявності тільки обладнань 802.11n.
Disabled (Відключене)	Виберіть для відключення безпроводового радіозв'язку.

У цей час найбільш безпечним режимом є режим WPA2 із шифруванням AES, як показано на рис. 7.20. Усі режими безпеки, описані в табл. 7.2.

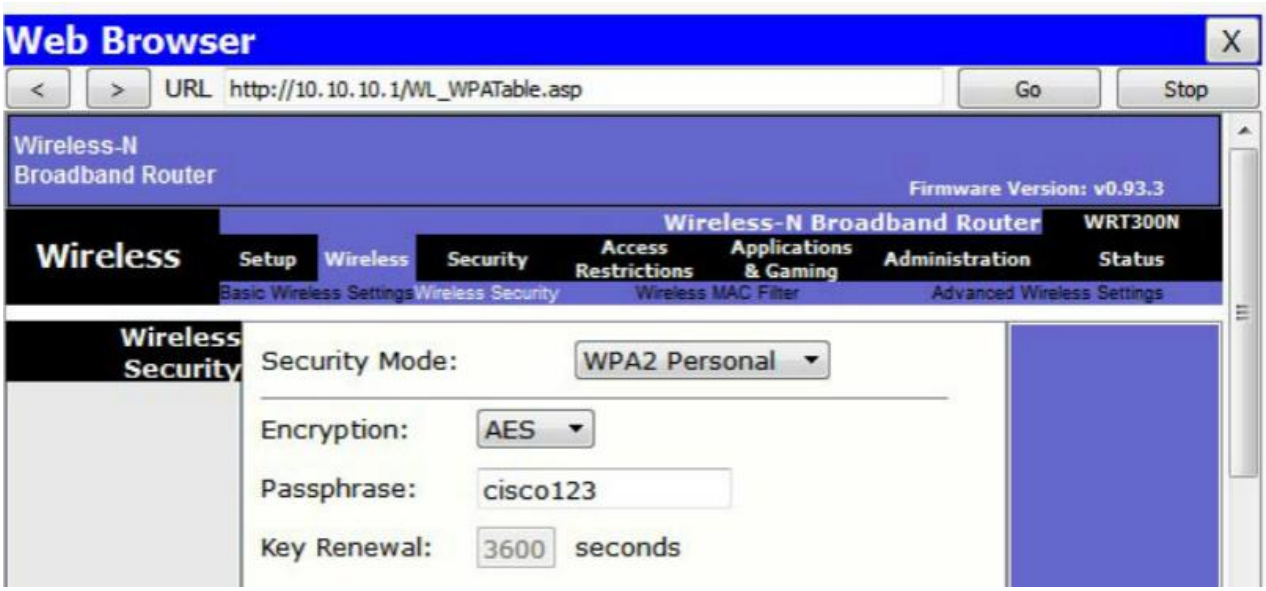


Рис. 7.20 – Режим WPA2 із шифруванням AES

Таблиця 7.2 – Режими безпеки безпроводового зв'язку

Режими безпеки	**Опис**
Протокол безпеки, аналогічному захисту провідних мереж (WEP)	Шифрування даних, переданих між безпроводовою крапкою доступу й клієнтом з використанням 64– або 128-розрядного ключа шифрування.
Протокол цілісності тимчасового ключа (TKIP)	• Це поліпшення WEP автоматично погоджує новий ключ кожні кілька хвилин. • TKIP допомагає запобігти одержанню зловмисниками достатнього обсягу даних для злому ключа шифрування.
Удосконалений стандарт шифрування (AES)	• Більш безпечна система шифрування, чому TKIP. • Для більш стійкого шифрування AES також потрібно більша обчислювальна потужність.
Захищений доступ Wi-Fi (WPA)	• Поліпшена версія WEP, створена як тимчасовий розв'язок до ратифікації 802.11i. • Тепер, після ратифікації 802.11i, випущений режим WPA2. Він охоплює весь стандарт 802.11i. • В WPA використовується набагато більш стійке шифрування, чім в WEP.
Захищений доступ Wi-Fi 2 (WPA2)	• Поліпшена версія WPA, що підтримує надійне шифрування, яке забезпечує безпека державного рівня. • Версія WPA2 може бути настроєна з перевіркою дійсності за допомогою пароля (персональна) або перевіркою дійсності на спеціальному сервері (корпоративна).

Додаткова безпека, наприклад, батьківський контроль або фільтрація контенту, є послугами, які можуть бути доступні в безпроводовому маршрутизаторі. Час доступу в Інтернет може бути обмежене певним годинником або днями, і певні IP-адреси й ключова слова можуть бути заблоковані. Місце розташування й глибина цих функцій різниться залежно від виробника й моделі маршрутизатора.

Як і Ethernet-обладнанням, безпроводовим обладнанням необхідні IP-адреси. Цей IP-адреса може призначатися через DHCP або статично. Безпроводовий маршрутизатор можна настроїти на надання адрес через DHCP, або кожному обладнанню можна призначити унікальну адресу. Часто необхідно ввести MAC-адресу обладнання для призначення IP-адреси вузлу вручну.

7.1.2.5 Перевірка зв'язку за допомогою графічного користувацького інтерфейсу Windows

Після підключення всіх обладнань, переконавшись, що горять усі індикатори зв'язку, перевірте підключення мережі. Найпростіший спосіб перевірити підключення до Інтернету — відкрити веб-браузер і перевірити доступність Інтернету. Для усунення неполадок безпроводового підключення можна використовувати графічний режим або командний рядок Windows.

Для перевірки безпроводового підключення в Windows Vista перейдіть по наступних пунктах.

Start > Control Panel > Network and Internet > Network and Sharing Center > Manage Network Connections (Пуск > Панель керування > Мережа й Інтернет > Центр управління мережами й загальним доступом > Управління мережевими підключеннями).

Для перевірки провідного або безпроводового підключення в Windows 7, 8 або 8.1 виберіть:

Start > Control Panel > Network and Internet > Network and Sharing Center > Change adapter settings (Пуск > Панель керування > Мережа й Інтернет > Центр керування мережами й загальним доступом > Зміна параметрів адаптера).

В Windows 7 і Vista провідні мережні підключення до мережі звичайно називаються Local Area Connection (Підключення по локальній мережі), як показано на рис. 7.21.

В Windows 8 і 8.1 провідні мережні підключення називаються Ethernet, як показано на рис. 7.22.

Двічі клацніть по мережному підключенню для відображення екрана стану, як показано для Windows 7 на рис. 7.23. На екрані стану відображається, чи підключений комп'ютер до Інтернету, а також тривалість підключення. У ньому також відображається число відправлених і прийнятих байтів.

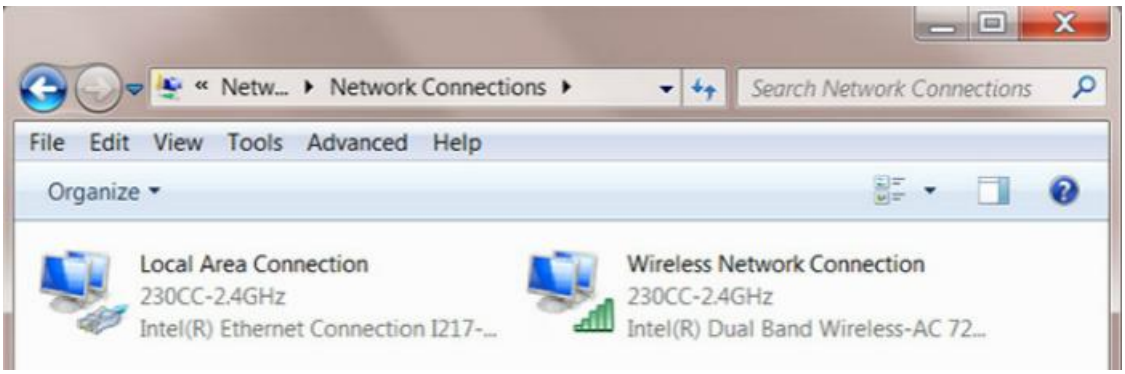


Рис. 7.21 – Local Area Connection (Підключення по локальної мережі)

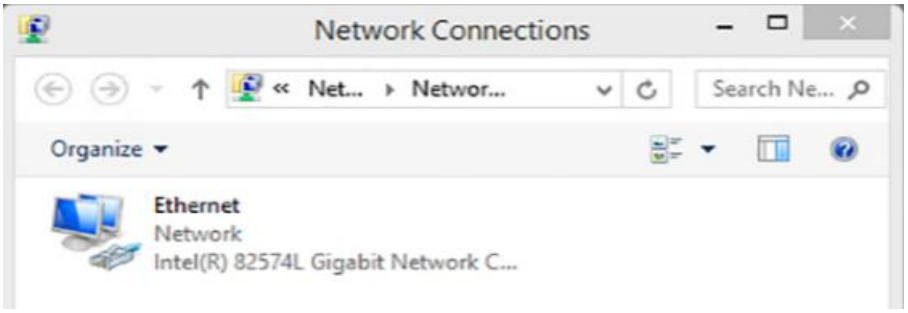


Рис. 7.22 – Проводові мережеві підключення Ethernet

У всіх версіях Windows натисніть кнопку **Details** (Відомості) для перегляду інформації про IP-Адресації, маски підмережі, шлюзу за замовчуванням, Mac-Адреси й іншої інформації, як показано на рис. 7.24.

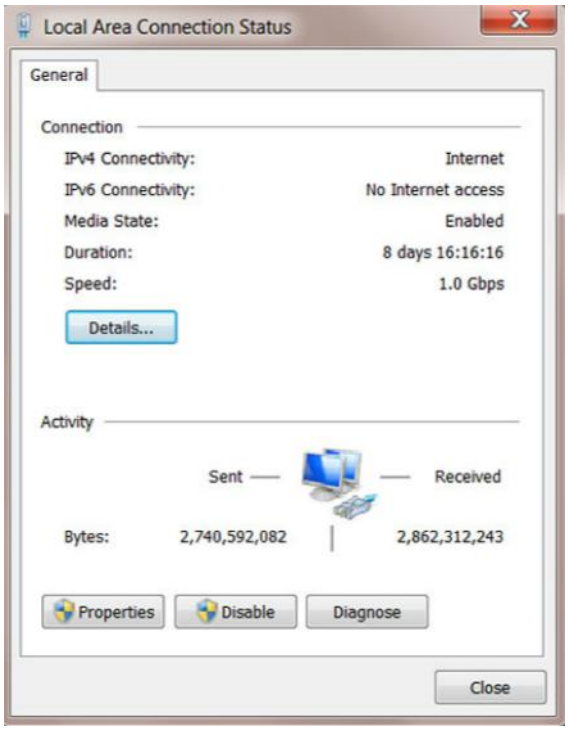


Рис. 7.23 – Екран стану

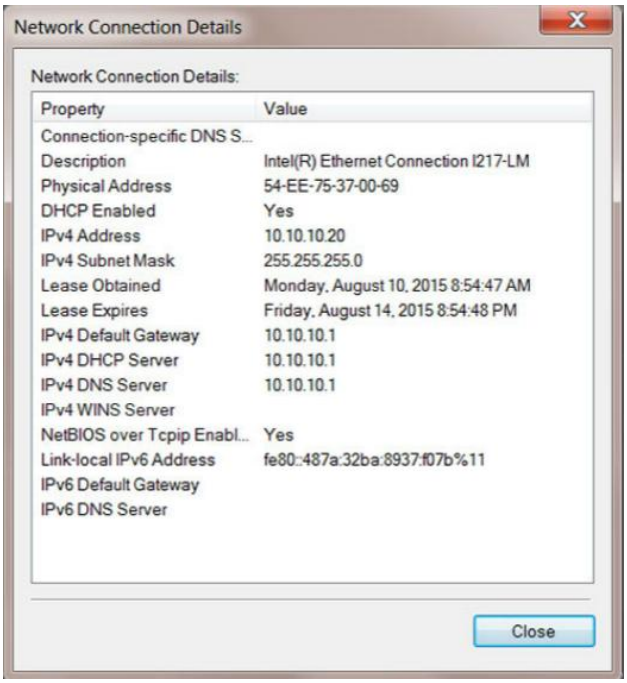


Рис. 7.24 – Вікно перегляду інформації про IP-адресації

Якщо підключення не функціонує належним чином, закрийте вікно Details (Відомості) і натисніть **Diagnose** (Діагностика) щоб скинути інформацію про це підключення й спробувати встановити нове.

7.1.2.6 Перевірка зв'язку за допомогою інтерфейсу командного рядка Windows

Для перевірки мережевого зв'язку можна використовувати інтерфейс командного рядка. Команди інтерфейсу командного рядка можна виконувати з вікна командного рядка.

Щоб відкрити вікно Command Prompt (Командний рядок) в Windows 8.x, відкрийте екран Start (Пуск), уведіть **command** і виберіть **Command Prompt** (Командний рядок).

Щоб відкрити вікно Command Prompt (Командний рядок) в Windows 7 і Windows Vista, виберіть **Start** (Пуск) і введіть **command**.

Технічному фахівцеві необхідно ознайомитися з наступними командами:

ipconfig — команда виводить на екран основну інформацію про параметри всіх мережевих адаптерів. У табл 7.3 показані доступні командні параметри. Щоб використовувати певний командний параметр, уведіть **ipconfig/***параметр* (наприклад, ipconfig/all).

ping — команда перевіряє базовий зв'язок між обладнаннями. При налагодженні проблем зі зв'язком виконайте ping до свого комп'ютера, шлюзу за замовчуванням і IP-адреси в Інтернеті. Відправивши луну-запит на популярний веб-сайт, можна перевірити наявність зв'язку з Інтернетом і серверами DNS. У командному рядку введіть **ping** *ім'я_адресата* (наприклад, ping www.cisco.com). Для виконання інших конкретних завдань можна додати параметри до команди ping.

Таблиця 7.3 – Параметри команди ipconfig

Параметри команди ipconfig	Призначення
/all	Відображає повну інформацію про настроювання всіх мережевих плат.
/release	Звільняє IP-адресу мережевої плати.
/renew	Обновляє IP-адреса мережевої плати.
/flushdns	Очищає кеш, який зберігає інформацію служби доменних імен (DNS).
/registerdns	Обновляє оренду адреси в сервера DHCP і повторно реєструє плату в службі доменних імен (DNS).
/displaydns	Відображає кешовану інформацію про DNS.

net — команда використовується для керування мережними комп'ютерами, серверами й ресурсами, такими як диски й принтери. Коман-

ди групи net використовують протокол Netbios, реалізований в операційній системі Windows. Ці команди дозволяють запускати, зупиняти й настроювати мережні служби.

netdom — команда використовується для управління обліковими записами комп'ютерів, приєднання комп'ютерів до домену й виконання інших завдань, пов'язаних з доменами.

nbtstat — команда використовується для відображення статистики підключень, що течуть, і служб, що працюють на локальних і вилучених комп'ютерах.

tracert — команда відслідковує маршрут доставки пакетів з вашого комп'ютера до вузла призначення. У командному рядку введіть **tracert** *ім'я вузла*. Першим рядком у висновку буде шлюз за замовчуванням. Кожний наступний рядок — маршрутизатор, через який проходить пакет на шляху до місця призначення. За допомогою команди tracert можна довідатися, де зупиняються пакети, і визначити місце виникнення проблеми. Якщо висновок команди дозволяє говорити про те, що місце виникнення проблеми перебуває за шлюзом за замовчуванням, це може вказувати на несправності в інтернет-провайдері (ISP), мережі Інтернет або сервері призначення.

nslookup — команда перевіряє й усуває неполадки серверів DNS. Вона відправляє серверу DNS запит для дозволу IP-адреси або імені вузла. У командному рядку введіть **nslookup** *ім'я вузла*. Команда nslookup повертає IP-вдресу, яка відповідає імені введеного вузла. Така реверсивна команда nslookup, як **nslookup IP-***адреса*, повертає ім'я вузла, яке відповідає введеному IP-адресі.

Примітка. Кожна із цих команд має багато додаткових параметрів. Для відображення додаткових параметрів використовуйте параметр виклику довідки (/?).

7.1.2.7 Домен і робоча група

Домени й робочі групи — способи впорядкування комп'ютерів у мережі й управління ними. Вони визначаються в такий спосіб:

- **Домен** — домен являє собою групу комп'ютерів і електронних обладнань як єдину адміністративну одиницю із загальним набором правил і процедур. Комп'ютери домена можуть розташовуватися в самих різних місцях у світі. Спеціалізований сервер, який називається контролером домена, управляє всім, що стосується безпеки користувачів і мережних ресурсів, централізованої безпеки й адміністрування. Наприклад, полегшений протокол доступу до каталогів (LDAP) у межах домена — це протокол, використовуваний для надання можливості доступу комп'ютерів до каталогів даних, які розподілені по всій мережі.
- **Робоча група** — робоча група являє собою набір робочих станцій і серверів локальної мережі й призначена для забезпечення зв'язку й обміну даних між ними. Кожна окрема робоча станція контролює

свої облікові записи користувачів, безпека інформації й доступ до даних і ресурсів.

Усі комп'ютери в мережі повинні бути частиною або домена, або робочої групи. Якщо операційна система Windows уперше встановлена на комп'ютері, вона автоматично привласнює йому робочу групу, як показано на рис. 7.25.

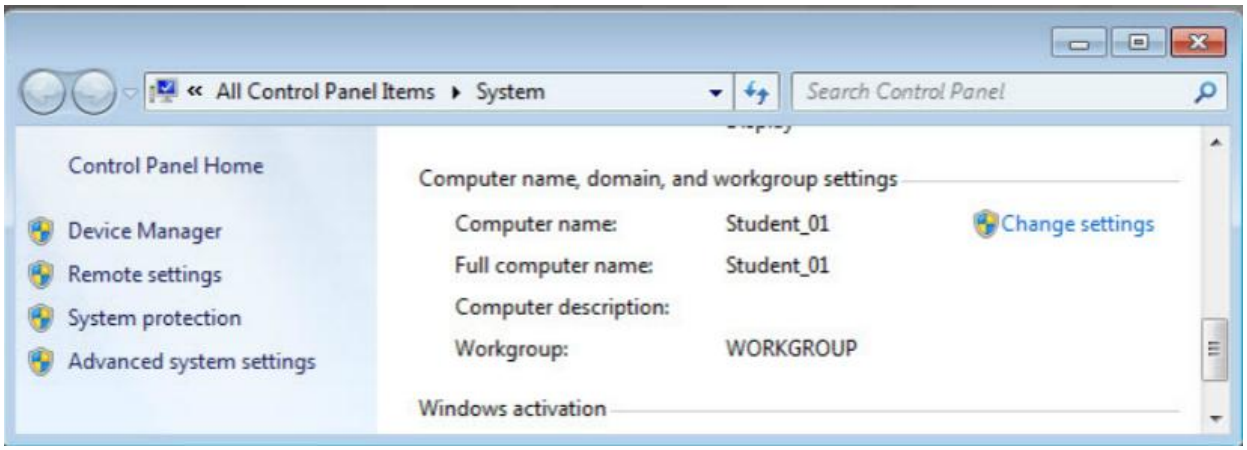


Рис. 7.25 – Ім'я домену або робочої групи

7.1.2.8 Підключення до робочої групи або домену

Щоб комп'ютери могли спільно використовувати ресурси, вони повинні входити в один домен або одну робочу групу. Старі операційні системи мають обмеження на імена, які можна давати робочим групам. Якщо в робочу групу входять як нові, так і старі операційні системи, слід використовувати ім'я робочої групи комп'ютера з найбільш старою операційною системою.

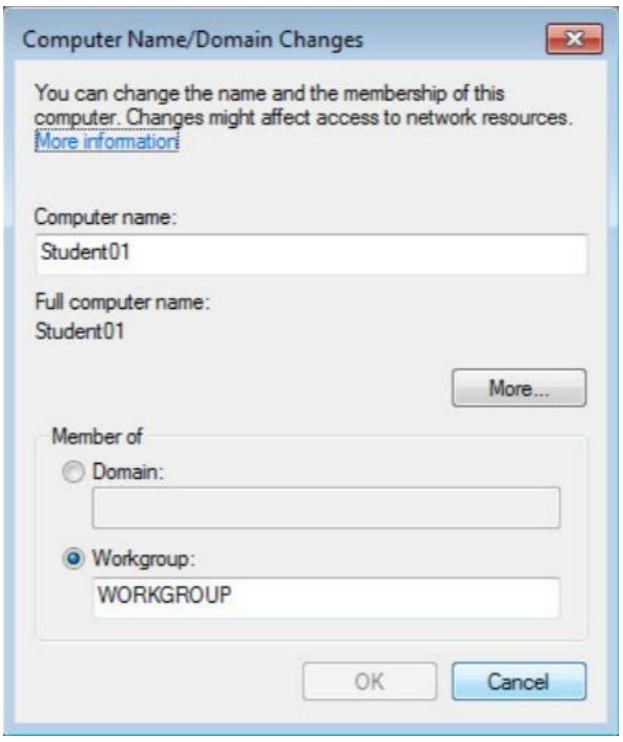


Рис. 7.26 – Зміна ім'я домена або робочої групи

Примітка. Щоб перевести комп'ютер з домена в робочу групу, необхідно знати ім'я користувача й пароль обліковому запису, який входить у групу локальних адміністраторів.

Щоб змінити ім'я робочої групи, як показано на рис. 7.26, у будь-якій версії Windows виберіть:

Control Panel > System and Security > System > Change

settings > Change (Панель управління > Система й безпека > Система > Змінити параметри > Змінити)

Для одержання доступу до майстра, показаного на рис. 7.27, виберіть **Network ID** (Ідентифікатор мережі) замість **Change** (Змінити). Майстер допоможе приєднатися до домену або робочій групі. Щоб зміни імені домена або робочої групи набули чинності, необхідно запустити знову комп'ютер.

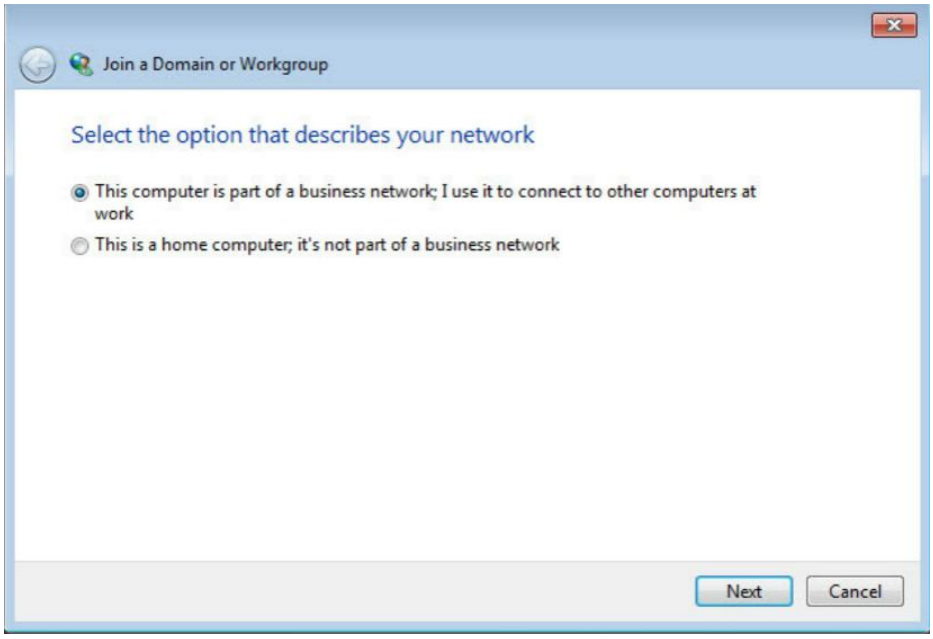


Рис. 7.27 – Майстер доменів и робочих груп

7.1.2.9 Домашня група Windows

Усі комп'ютери під управлінням Windows, які належать однієї робочій групі, також можуть бути включені в домашню групу. У мережі на кожну робочу групу може приходитися тільки одна домашня група. Один комп'ютер може бути членом тільки однієї домашньої групи. Операційна система Windows Vista не підтримує домашні групи.

Домашню групу в робочій групі може створити тільки один користувач. Інші користувачі можуть приєднатися до домашньої групи за умови, що вони знають пароль домашньої групи. Можливість використання домашньої групи залежить від профілю мережевого розташування:

Home Network (Домашня мережа) — дозволені створення домашньої групи й приєднання до неї

Work Network (Робоча мережа) — не дозволені створення домашньої групи й приєднання до неї, але можливі перегляд ресурсів і загальний доступ до них разом з іншими комп'ютерами

Public Network (Суспільна мережа) — домашня група недоступна

Щоб змінити профіль мережевого розташування комп'ютера на профіль Home Network (Домашня мережа), виконаєте наступні дії:

Крок 1. Виберіть **Start > Control Panel > Network and Sharing Center** (Пуск > Панель управління > Центр управління мережами й загальним доступом).

Крок 2. Виберіть профіль мережевого розташування зі списку в розділі View your active networks (Перегляд активних мереж), як показано на рис. 7.28.

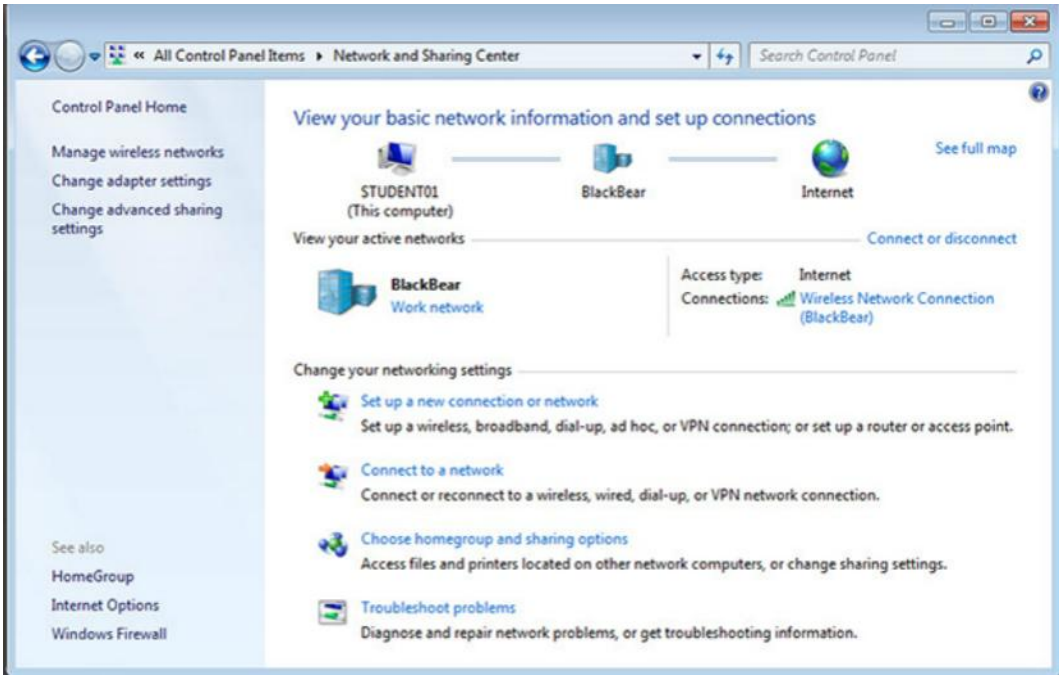


Рис. 7.28 – Поточний профіль мережевого розташування

Крок 3. Виберіть **Home network** (Домашня мережа).

Крок 4. Виберіть об'єкти для спільного користування (наприклад, зображення, музику, відео, документи й принтери), потім натисніть **Next** (Далі).

Крок 5. Приєднаєтеся до домашньої групи або створіть свою.

Для створення домашньої групи необхідно виконати наступні дії:

Крок 1. Виберіть **Start > Control Panel > Homegroup** (Пуск > Панель управління > Домашня група).

Крок 2. Виберіть **Create a homegroup** (Створити домашню групу), як показано на рис. 7.29.

Крок 3. Виберіть файли для спільного користування й натисніть **Next** (Далі).

Крок 4. Установите пароль домашньої групи.

Крок 5. Клацніть **Finish (Готове)**.

Коли комп'ютер приєднується до домашньої групи, усі облікові записи на ньому, за винятком облікового запису гостюючи, стають членами домашньої групи. Члени однієї домашньої групи можуть спільно користуватися фотографіями, музикою, відео, документами, бібліотеками й

принтерами. Користувачі контролюють доступ до своїх ресурсів. Користувачі також можуть створювати домашню групу або приєднуватися до неї, використовуючи віртуальну машину Windows Virtual PC.



Рис. 7.29 – Create a Homegroup (Створення домашньої групи)

Щоб включити комп'ютер у домашню групу, необхідно виконати наступні дії:

Крок 1. Виберіть **Start > Control Panel > Homegroup** (Пуск > Панель управління > Домашня група).

Крок 2. Натисніть **Join now** (Приєднатися), як показано на рис. 7.30.

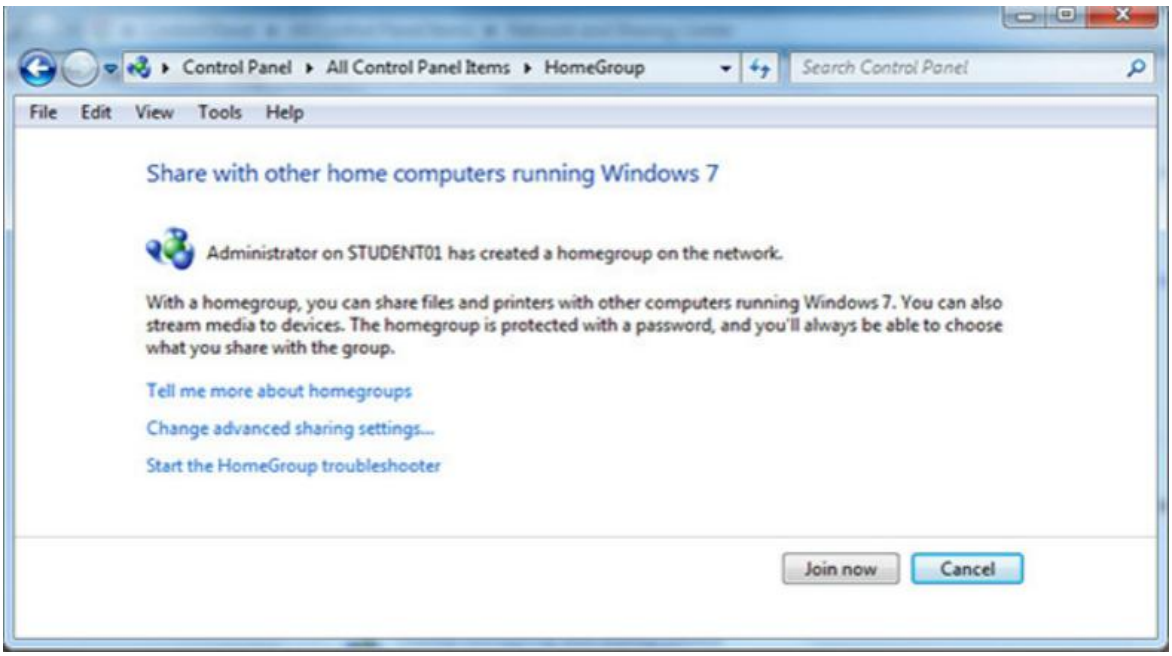


Рис. 7.30 – Join a Homegroup (Приєднання до домашньої групи)

Крок 3. Виберіть файли для спільного користування й натисніть **Next** (Далі).

Крок 4. Уведіть пароль домашньої групи й натисніть **Next** (Далі).

Крок 5. Клацніть **Finish (Готове)**.

Щоб змінити спільно використовувані файли на комп'ютері, виберіть **Start > Control Panel > Homegroup** (Пуск > Панель управління > Домашня група). Після внесення змін натисніть **Save change** (Зберегти зміни).

Примітка. Якщо комп'ютер входить у домен, можна приєднатися до домашньої групи й одержати доступ до файлів і ресурсам, які перебувають на інших комп'ютерах домашньої групи. Однак у цьому випадку немає можливості створювати домашню групу або надавати власні файли або ресурси в спільне використання домашньою групою.

7.1.2.10 Загальні мережеві папки й підключення дисків

Загальний доступ до файлів по мережі й підключення мережевих дисків – безпечний і зручний спосіб забезпечення простого доступу до мережевих ресурсів. Це особливо справедливо у випадку, коли необхідно надати доступ до мережевих ресурсів комп'ютерам під управлінням різних версій Windows. Підключення локального диска — зручний спосіб доступу з різних операційних систем до файлу, певних папок або всьому диска через мережу. При підключенні диска ресурсу на віддаленому диску привласнюється буква (від A до Z), що дозволяє використовувати віддалений диск так, ніби це був локальний диск.

Загальний доступ до файлів по мережі

Спочатку слід визначити, які ресурси будуть спільно використовуватися по мережі і які дозволи на доступ до цих ресурсів будуть у користувачів. Дозволу визначають тип доступу користувачів до файлу або папки.

Read (Читання) — користувач може переглядати файли й вкладені папки, відкривати вкладені папки, переглядати дані у файлах і запускати програмні файли.

Change (Зміна) — на додаток до дозволу на читання користувач зможе додавати файли й папки, змінювати дані у файлах і видаляти вкладені папки й файли.

Full Control (Повний доступ) — на додаток до дозволів на зміну й читання користувач може змінювати дозволи файлів і папок у розділі з файловою системою NTFS і стати власником файлів і папок.

Для загального доступу до папки використовуйте зазначений нижче спосіб.

Натисніть праву кнопку на папці, виберіть **Properties > Sharing > Advanced Sharing >Share this folder > Permissions** (Властивості > Загальний доступ > Розширене настроювання загального доступу > Відкрити загальний доступ до цієї папки > Дозволу). Визначите, які користувачі будуть мати доступ до папки, і вкажіть їхній дозволу. На рис. 7.31 показане вікно дозволів для загальної папки.

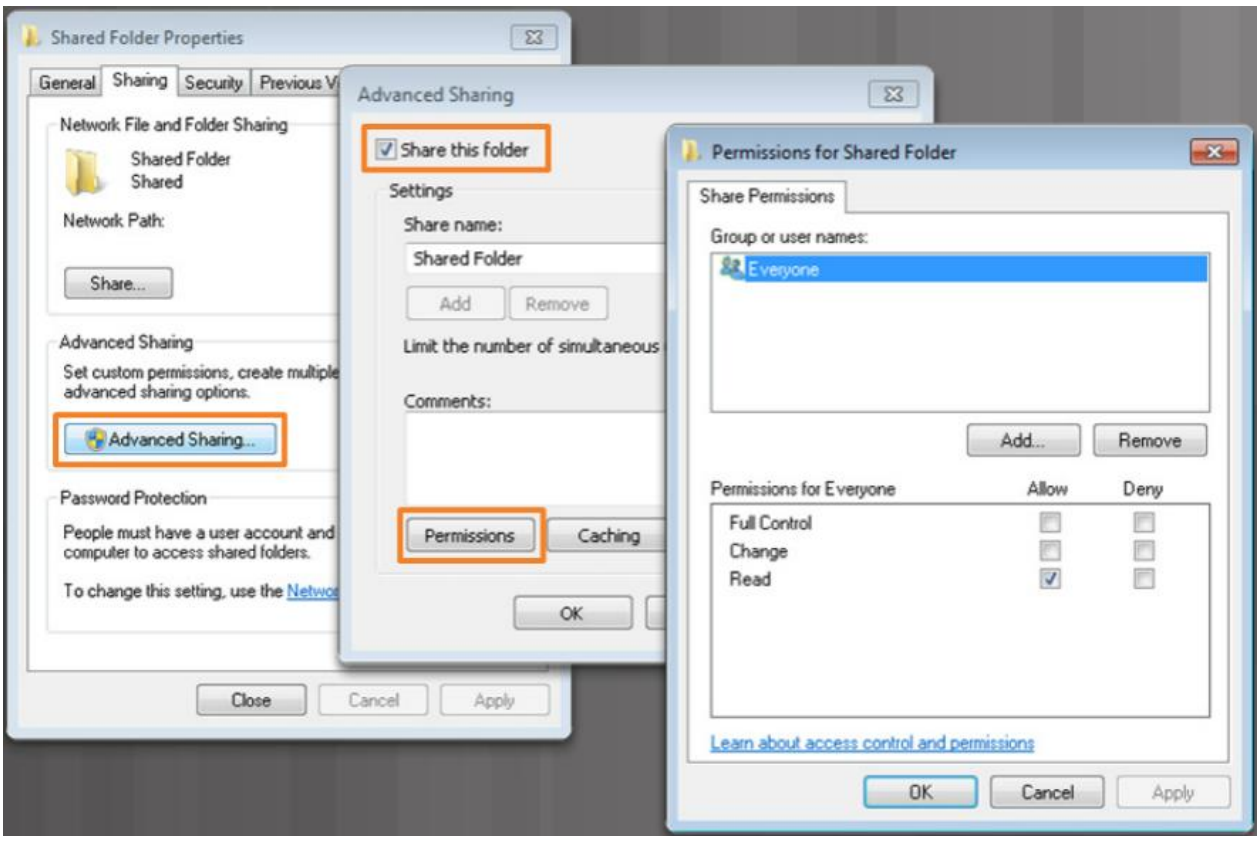


Рис. 7.31 – Установка дозволів для загальної папки

7.1.2.11 Адміністративні загальні ресурси

Адміністративні загальні ресурси, також називані схованими загальними ресурсами, позначаються знаком долара ($) наприкінці імені кожного такого ресурсу. За замовчуванням система Windows може включати сховані адміністративні загальні ресурси:

- Кореневі розділи або томи
- Коренева папка системи
- Загальний ресурс FAX$
- Загальний ресурс IPC$
- Загальний ресурс PRINT$

Для створення власного адміністративного загального ресурсу виконаєте наступні дії в будь-якій версії Windows.

Крок 1. Виберіть **Control Panel > Administrative Tools** (Панель управління > Адміністрування) і двічі клацніть **Computer Management** (Управління комп'ютером), як показано на рис. 7.32, а.

Крок 2. Розгорніть **Shared Folders** (Загальні папки), натисніть праву кнопку миші на **Shares** (Загальні ресурси) і виберіть **New Share...** (Новий загальний ресурс...), щоб відкрити **Create A Shared Folder Wizard** (Майстер створення загальної папки). Натисніть **Next** (Далі); з'явиться екран, показаний на рис. 7.32, б.

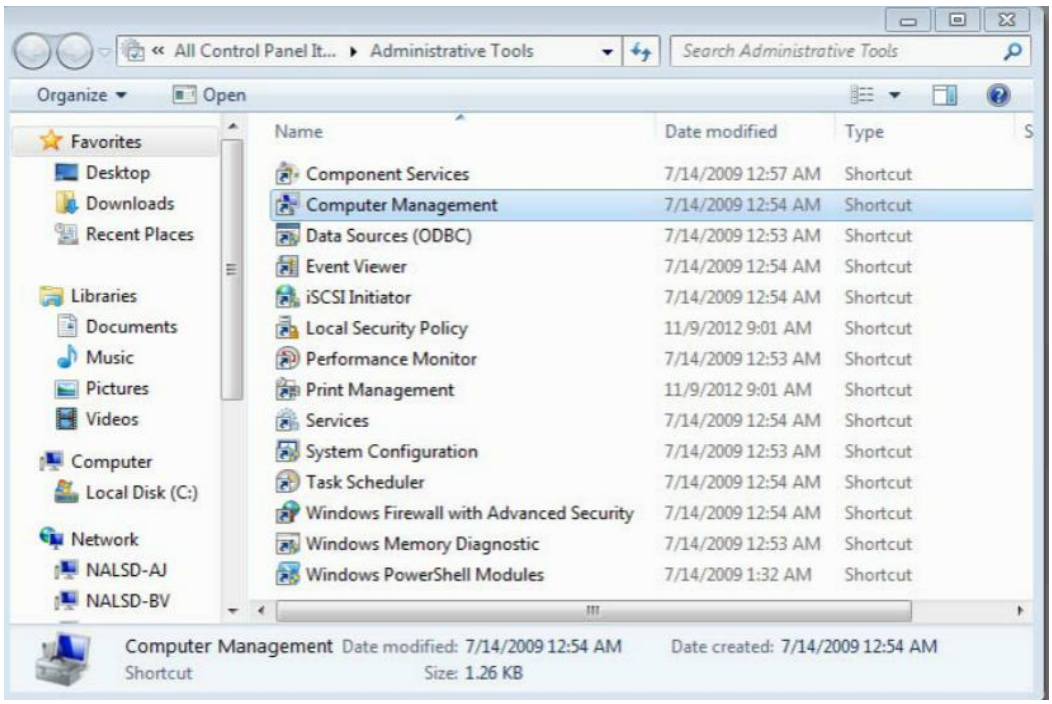


Рис. 7.32, а – Створення адміністративного загального ресурсу

Крок 3. Уведіть шлях до папки, який буде використовуватися для адміністративного загального ресурсу (наприклад, **C:\Adminonly$** на рис. 7.32, б. Папка, яка повинна ідентифікуватися як адміністративний загальний ресурс, зобов'язано мати знак долара ($) наприкінці імені. Клацніть **Next (Далі)**. Якщо папка ще не існує, система Windows видасть запит створення цієї папки.

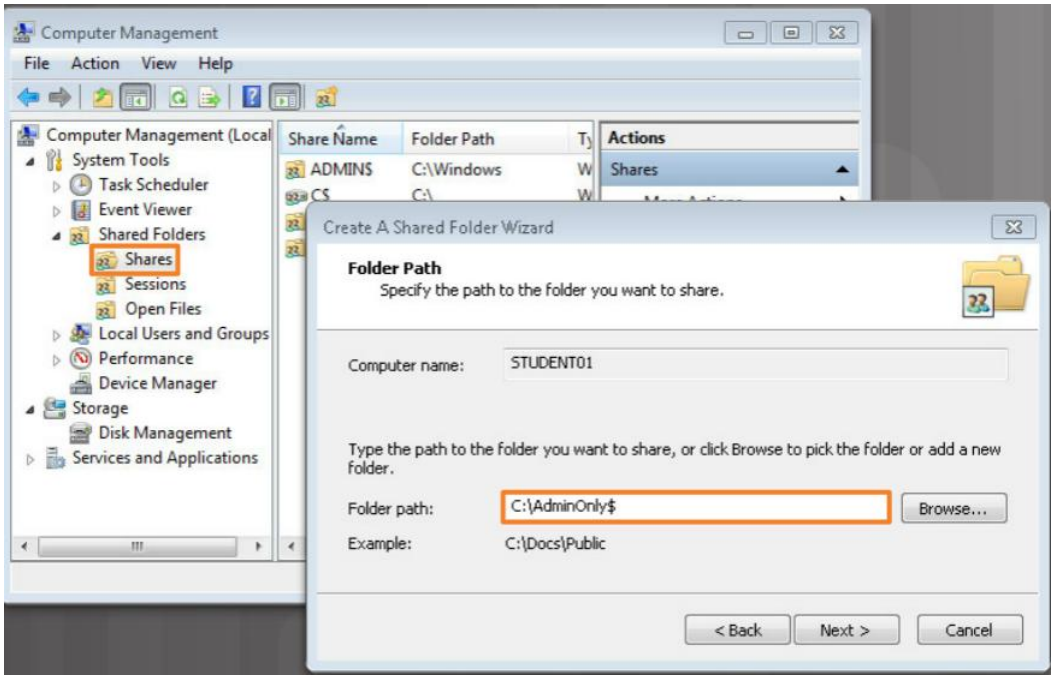


Рис. 7.32, б – Створення адміністративного загального ресурсу

Крок 4. На наступному екрані можна змінити ім'я загального ресурсу, додати додатковий опис і змінити параметри автономного режиму. Клацніть **Next (Далі)**.

Крок 5. У вікні **Shared Folder Permissions** (Дозволу для загальної папки), як показано на рис. 7.32, в), виберіть **Administrators have full access; other users have no access** (Адміністратори мають повний доступ, інші не мають доступу), а потім натисніть **Finish** (Готове).

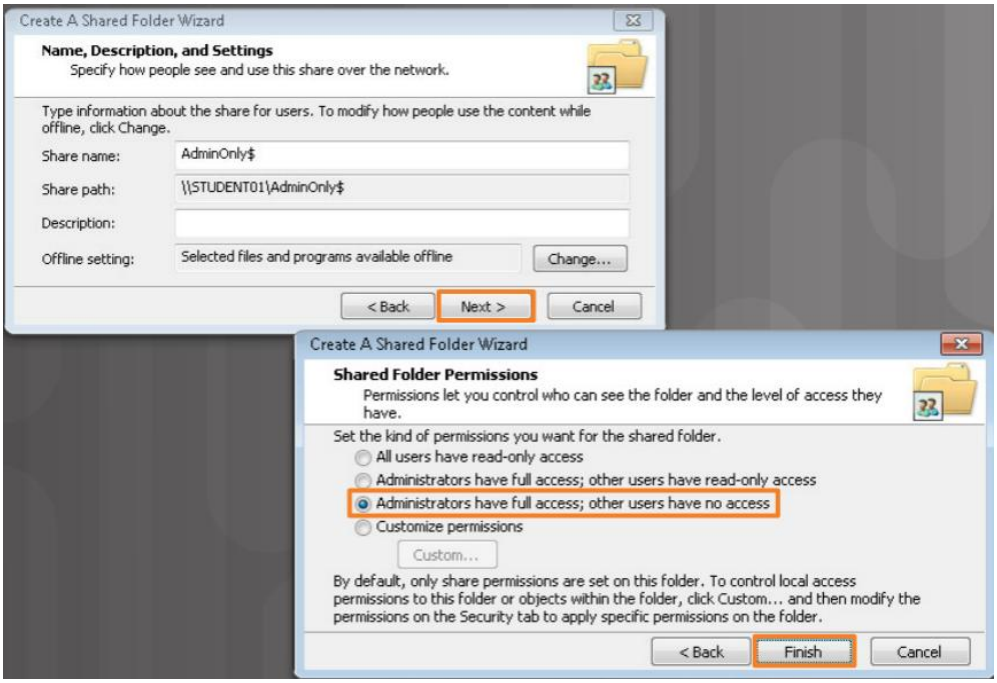


Рис. 7.32, в – Створення адміністративного загального ресурсу

7.1.2.12 Підключення мережевого диска

Щоб підключити мережевий диск до загальної папки в Windows 7 і Vista, виберіть

Start (Пуск) і клацніть правою кнопкою миші **Computer > Map network drive** (Комп'ютер > Підключити мережевий диск).

В Windows 8.0 виконаєте наступні дії:

Крок 1. У вікні Start (Пуск) уведіть **провідник** і натисніть **Провідник**, щоб його відкрити.

Крок 2. Клацніть правою кнопкою миші **Computer > Map network drive** (Комп'ютер > Підключити мережевий диск), як показано на рис. 7.33, а).

В Windows 8.1 виконаєте наступні дії:

Крок 1. У вікні Start (Пуск) уведіть **провідник** і натисніть **Провідник**, щоб його відкрити.

Крок 2. Клацніть правою кнопкою миші **This PC > Map network drive** (Цей комп'ютер > Підключити мережевий диск), як показано на рис. 7.33, б).

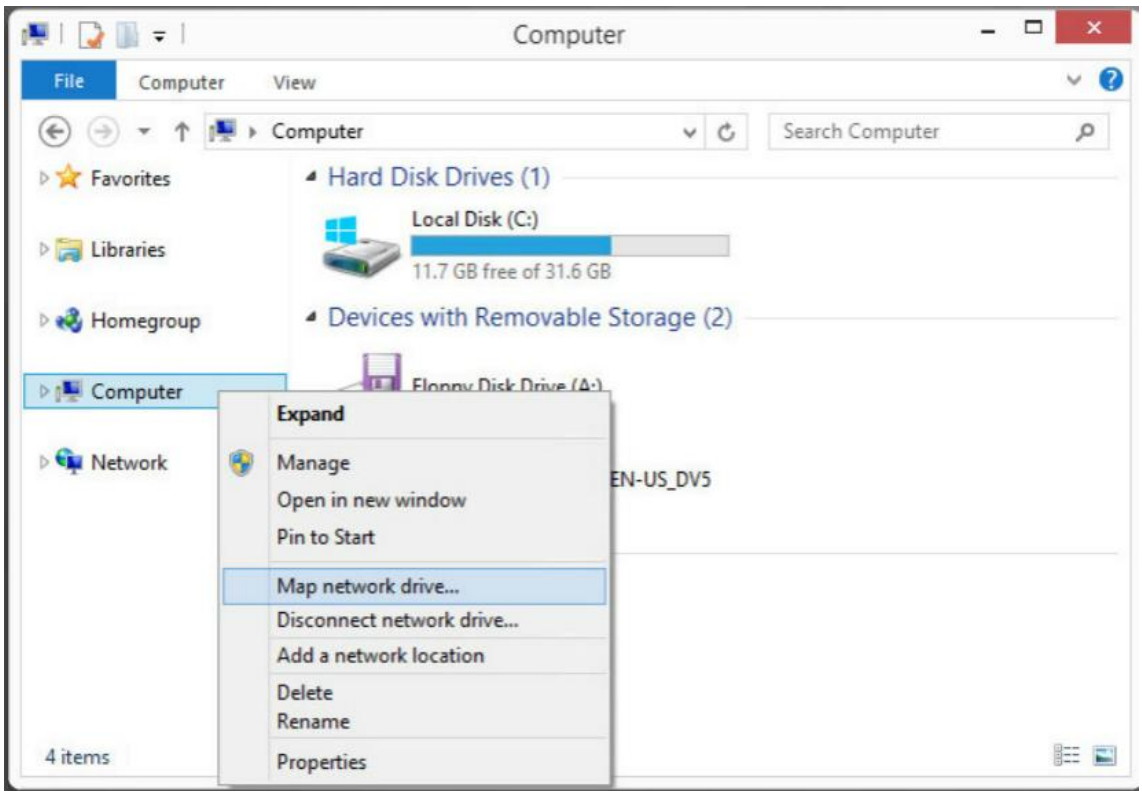


Рис. 7.33, а – Підключення мережевого диска

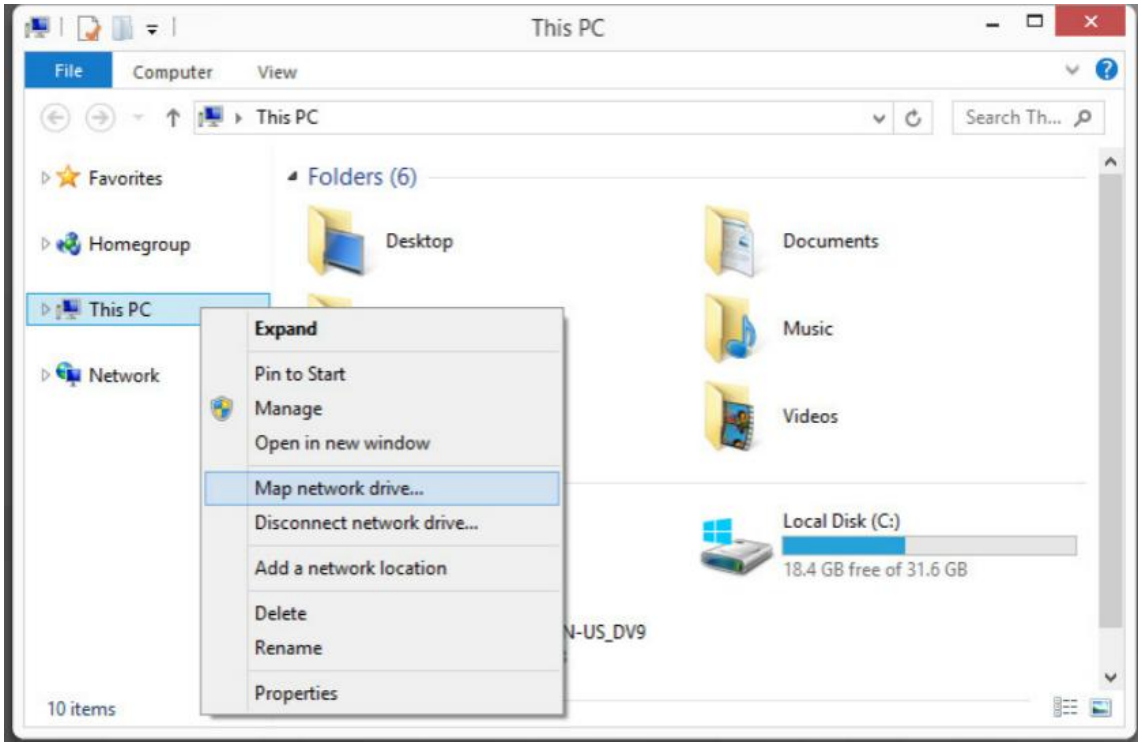


Рис. 7.33, б – Підключення мережевого диска

Знайдіть у мережі папку загального доступу й призначте їй букву диска, як показано на рис. 7.33, в) .

В операційній системі Windows 7 можна використовувати до 20 підключень загального доступу до файлів одночасно. В операційній системі Windows Vista Business можна використовувати до 10 підключень загального доступу до файлів одночасно.

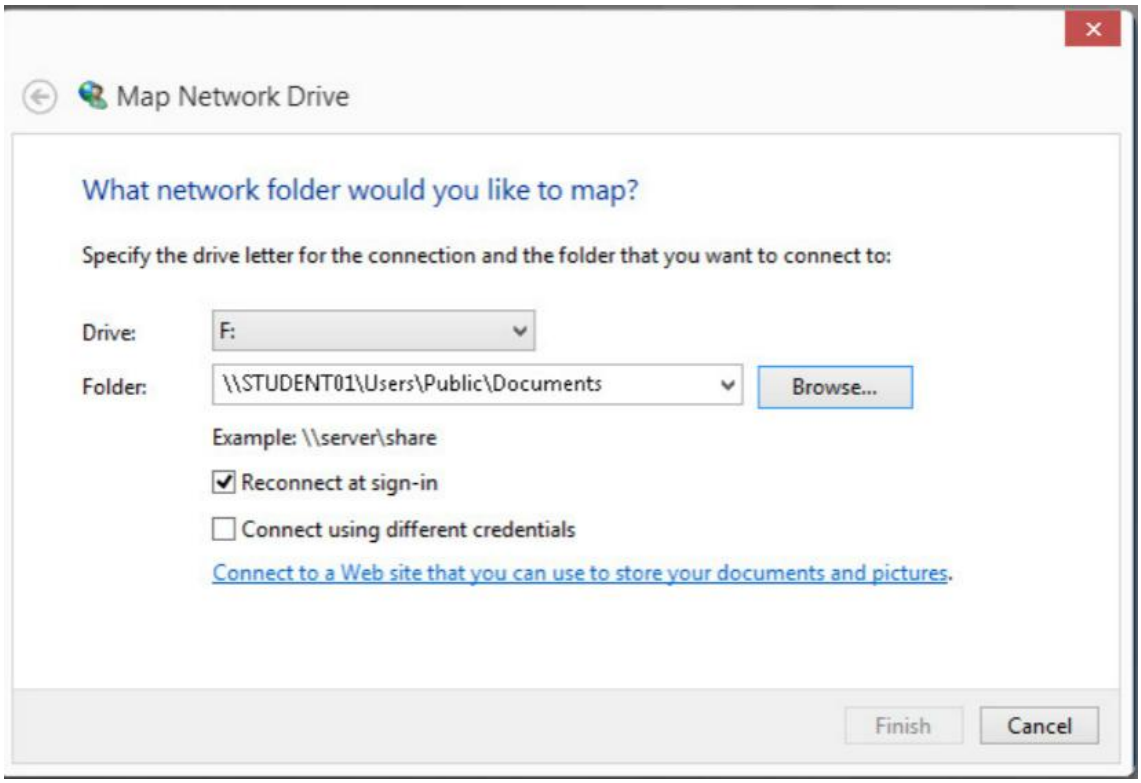


Рис. 7.33, в – Підключення мережевого диска

7.1.2.13 VPN

При підключенні до локальної мережі й загальному доступі до файлів зв'язок між комп'ютерами не виходить за рамки цієї мережі. Дані залишаються захищеними, тому що залишаються усередині мережі, за маршрутизатором, не потрапляючи в інші мережі й Інтернет. Для обміну даними й загального доступу до ресурсів через небезпечні мережі використовується віртуальна приватна мережа (VPN).

Віртуальна приватна мережа (VPN) являє собою приватну мережу, яка забезпечує підключення вилучених вузлів або користувачів друг до друга через суспільну мережу, таку як Інтернет. Найпоширеніша мета використання VPN — доступ до внутрішньої корпоративної мережі. Мережа VPN використовує виділені безпечні підключення, маршрутизовані через Інтернет між внутрішньою корпоративною мережею й вилученими користувачами. При підключенні до внутрішньої корпоративної мережі користувачі стають частиною цієї мережі й мають доступ до всіх сервісів і ресурсам, як якби вони фізично підключилися до корпоративної локальної мережі.

Для одержання дистанційного доступу користувачі повинні встановити на свої комп'ютери клієнт VPN, щоб створити безпечне підключення до внутрішньої корпоративної мережі. Програма-Клієнт VPN шифрує дані перед відправленням їх через Інтернет на шлюз VPN корпоративної приватної мережі. Шлюзи VPN створюють підключення VPN, управляють ними й контролюють їх. Підключення VPN називаються також VPN-Тунелями.

Щоб установити й настроїти підключення VPN у будь-якій версії Windows, виконаєте наступні дії:

Крок 1. Виберіть **Start > Control Panel > Network and Sharing Center** (Пуск > Панель управління > Центр управління мережами й загальним доступом) в Windows.

Крок 2. Виберіть **Set up a new connection or network** (Створення й настроювання нового підключення або мережі).

Крок 3. Після того як відкриється вікно New Connection Wizard (Майстер нових підключень), виберіть **Connect to a workplace** (Підключення до робочого місця) і натисніть **Next** (Далі).

Крок 4. Виберіть **Use my Internet connection (VPN)** (Використовувати моє підключення до Інтернету (VPN)) і введіть Інтернет-адресу й ім'я адресата, як показано на рис. 7.34, а).

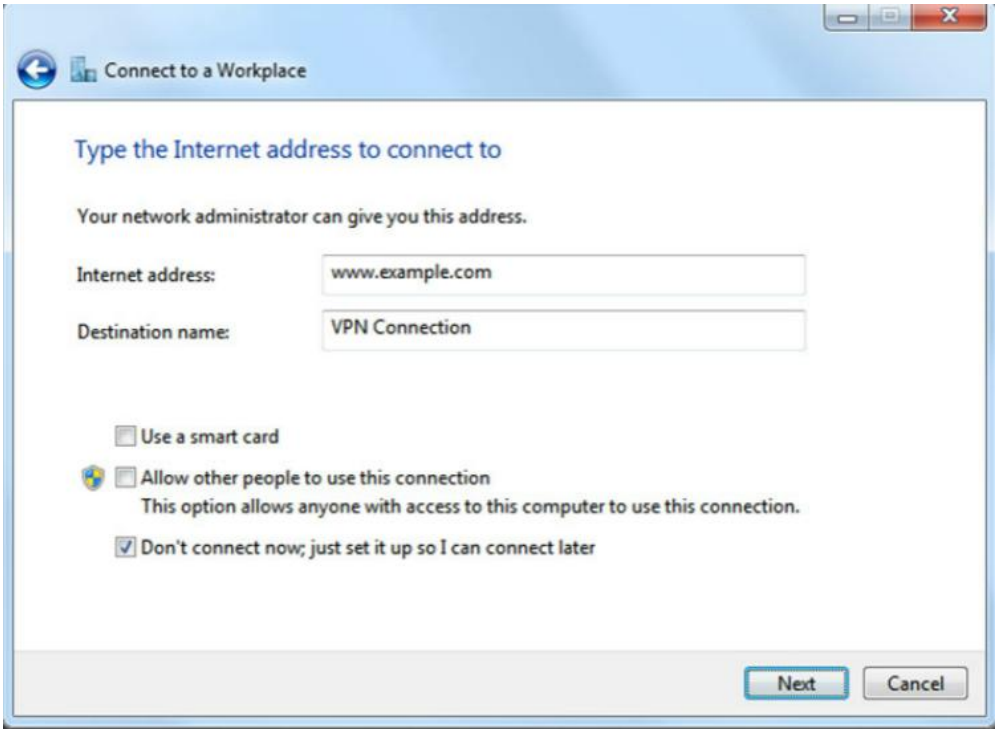
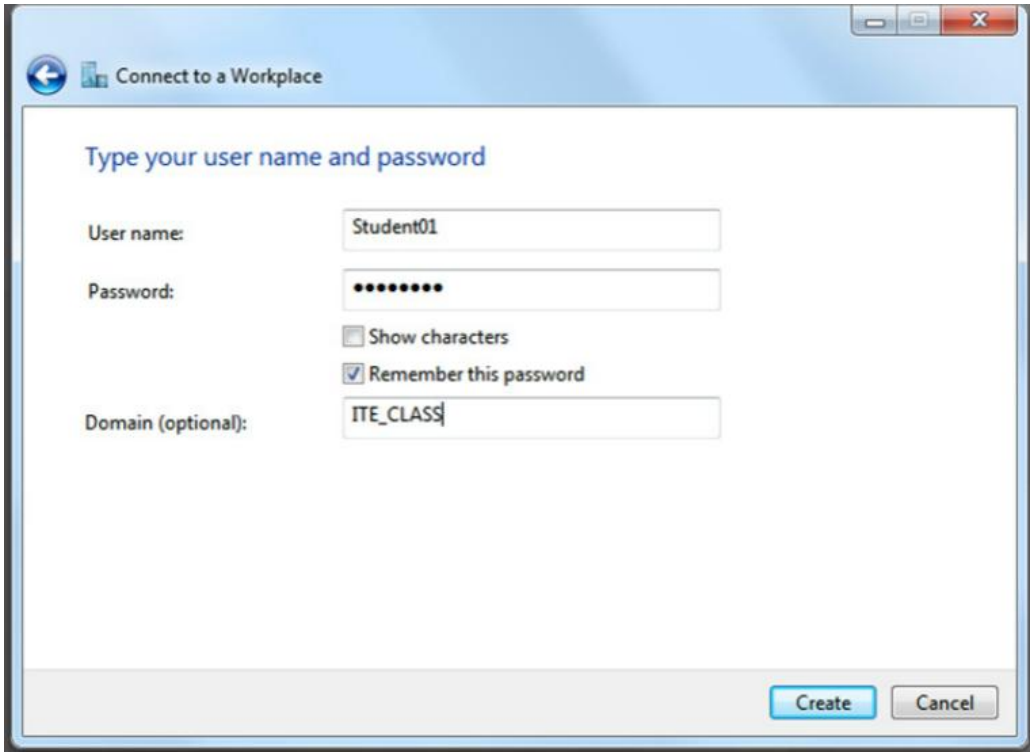


Рис. 7.34, а – Настроювання підключення VPN

Крок 5. Установите прапорець **Don't connect now; just set it up so I can connect later** (Відкласти настроювання підключення до Інтернету) і натисніть **Next** (Далі).

Крок 6. Уведіть ім'я користувача, пароль і домен (необов'язково), як показано на рис. 7.34 б). Потім натисніть **Create** (Створити).



б)

Рис. 7.34 – Настроювання підключення VPN

Крок 7. У вікні входу в систему введіть ім'я користувача й пароль і натисніть **Connect** (Підключитися).

7.1.2.14 Віддалений робочий стіл і віддалений помічник

Для усунення неполадок і відновлення комп'ютерів інженери можуть використовувати функції віддаленого помічника й віддаленого робочого стола. Як показано на рис. 7.35, віддалений робочий стіл дозволяє переглядати й контролювати комп'ютер з віддаленого місця розташування.



Рис. 7.35 – Клієнт віддаленого робочого стола Windows

Віддалений помічник, як показано на рис 7.36, дозволяє інженерам розв'язувати проблеми з комп'ютером замовника з віддаленого місця розташування.

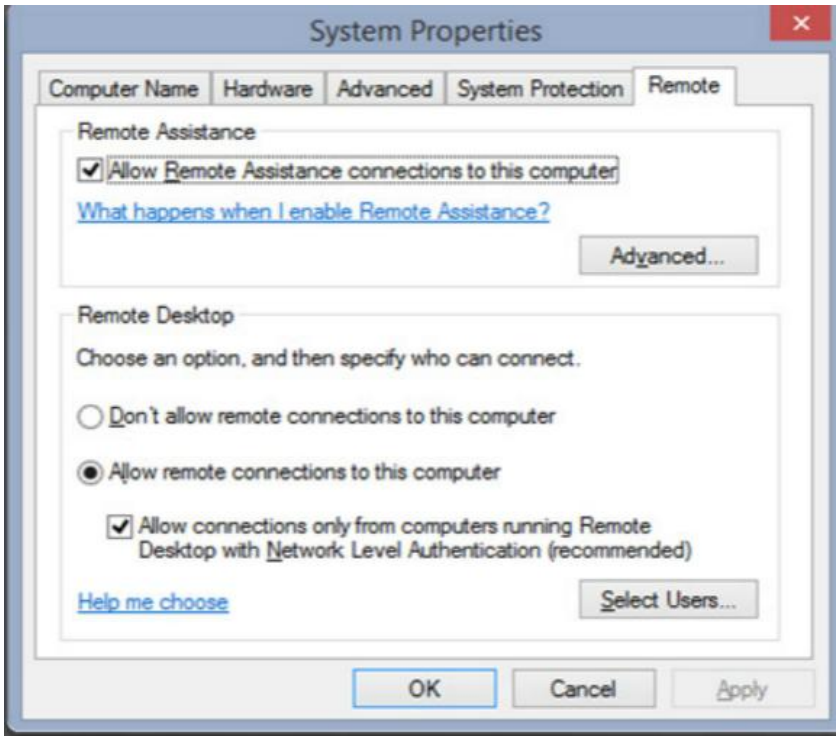


Рис. 7.36 – Windows Remote Assistance (Віддалений помічник Windows)

Віддалений помічник також дозволяє замовникові в режимі реального часу переглядати на екрані виправлення й відновлення, установлювані на комп'ютері.

Щоб одержати доступ до віддаленого робочого стола в Windows 8, відкрийте екран **Start** (Пуск), уведіть **Remote Desktop Connection** (Підключення до віддаленого робочого стола) і клацніть по значкові **Remote Desktop Connection** (Підключення до віддаленого робочого стола).

Для одержання доступу до віддаленого робочого стола в Windows 7 або Windows Vista виберіть:

Start > All Programs > Accessories > Remote Desktop Connection (Пуск > Усі програми > Стандартні > Підключення до віддаленого робочого стола)

Перш ніж використовувати віддаленого помічника в ОС Windows, його необхідно включити. Для включення й виклику віддаленого помічника, як показано на рис. 7.37, виконаєте наступні дії:

В Windows 8:

Крок 1. Натисніть праву кнопку миші **This PC** (Цей комп'ютер) (в Windows 8.1) або **Computer** (Комп'ютер) (в Windows 8.0) і виберіть **Properties** (Властивості).

Крок 2. Натисніть **Remote Settings** (Настроювання дистанційного доступу) у вікні System (Система) і перейдіть на вкладку **Remote** (Дистанційний доступ).

Крок 3. Установите прапорець **Allow Remote Assistance Connections to This Computer** (Дозволити підключення віддаленого помічника до цього комп'ютера).

Крок 4. Клацніть **OK.**

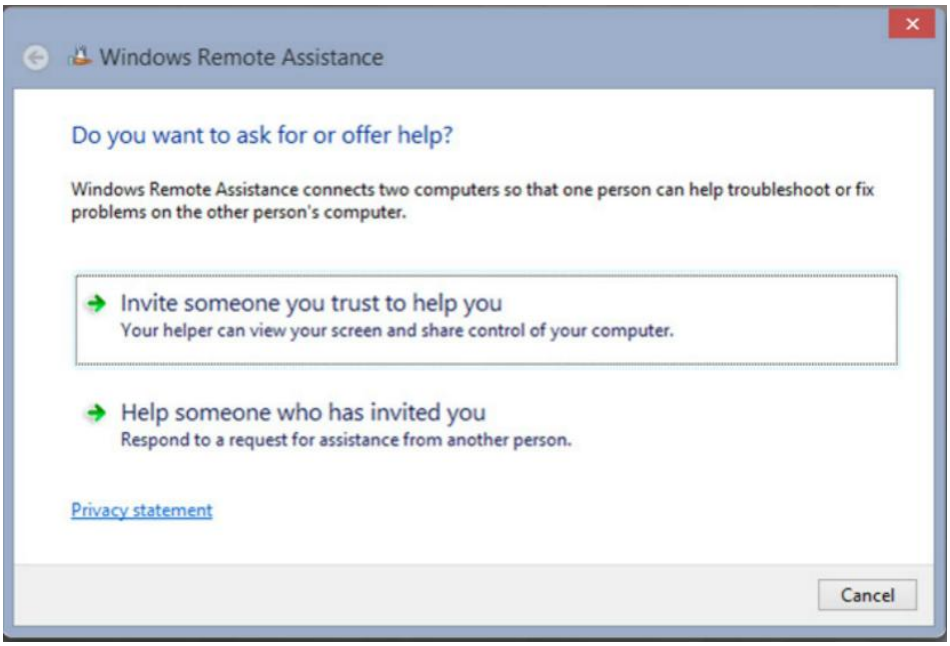


Рис. 7.37– Включення Windows Remote Assistance (Віддалений помічник Windows)

Для одержання доступу до віддаленого помічника в Windows 8 відкрийте екран **Start** (Пуск), уведіть **Invite someone to connect to your PC** (Запрошення підключитися до вашого комп'ютера) і натисніть **Enter**. Клацніть **Invite someone you trust to help you** (Запросити того, кому ви довіряєте, для надання допомоги), щоб дозволити помічникові загальний доступ до управління комп'ютером.

Примітка. Може знадобитися змінити фокус пошуку на Settings (Параметри).

Для одержання доступу до віддаленого помічника в Windows 7 або Windows Vista виберіть:

Start > All Programs > Maintenance > Windows Remote Assistance (Пуск > Усі програми > Обслуговування > Віддалений помічник Windows)

7.3 Коротка історія технологій підключення

В 90-х рр. Інтернет, як правило, використовувався для передачі даних. У порівнянні з високошвидкісними підключеннями, доступними сьогодні, швидкість передачі була низкою.

Додаткова пропускна спроможність дозволяє передавати голос і відео, а також дані. Сьогодні існує безліч способів підключення до Інтернету. Телефонне, кабельне, супутникове підключення, приватні телекомунікації пропонують широкосмуговий доступ до Інтернету для підприємств і домашнього використання.



Супутниковий приймач



Модем DSL



Кабельний модем

Рис. 7.38 – Технології широкосмугової передачі

Аналогова телефонія

В аналоговій телефонії, яку також називають звичайним телефонним зв'язком (plain old telephone service, POTS), дані передаються через стандартні голосові телефонні лінії. У цьому випадку використовується аналоговий модем, який дзвонить по телефонній лінії на інший модем, розташований на віддаленій стороні (наприклад, в інтернет-провайдера). Модем використовує телефонну лінію для передачі й приймання даних. Такий метод підключення називається, що комутируються.

Цифрова мережа з інтегрованими послугами (ISDN)

ISDN використовує кілька каналів і може надавати різні види послуг, тому вона вважається одним з видів широкосмугового доступу. ISDN є стандартним каналом для передачі голосу, відео й даних по звичайних телефонних проводах. Технологія ISDN використовує телефонні проведення як аналогову телефонну службу.

Широкосмугова передача

Широкосмугова передача — технологія, яка використовується для передачі й приймання по одному кабелю безлічі сигналів з використанням різних частот. Наприклад, кабель, використовуваний у кабельному телебаченні, може здійснювати передачу даних комп'ютерної мережі одночасно з телевізій-

ним сигналом. Оскільки у двох типах передач використовуються різні частоти, вони не заважають один одному.

Для широкосмугової передачі використовується широкий спектр частот, який може бути додатково розділений на канали. У мережевих технологіях термін «широкосмугова передача» позначає способи зв'язку, при яких передаються два або більш сигналу одночасно. Передача двох або більш сигналів одночасно збільшує швидкість передачі. Звичайно до широкосмугових мережевих підключень відносять широкосмуговий кабельний модем, DSL, ISDN і супутниковий зв'язок. На рис. 7.38 показане обладнання, використовуване для підключення до широкосмугових мереж або для передачі широкосмугових сигналів.

7.3.1 DSL і ADSL. Цифрова абонентська лінія (DSL)

DSL (Digital Subscriber Line) відноситься до служб постійного підключення, що рятує користувачів від необхідності набирати номер щораз, коли вони хочуть підключитися до Інтернету. В DSL використовуються існуючі мідні телефонні лінії для забезпечення високошвидкісної цифрової передачі даних між кінцевими користувачами й телефонними компаніями. На відміну від ISDN, де цифрова передача даних заміняє аналоговий голосовий зв'язок, DSL використовує телефонні проводи одночасно з переданими аналоговими сигналами.

У технології DSL сигнали голосу й даних передаються по мідних телефонних проводах на різних несучих частотах. Фільтр запобігає впливу сигналу DSL на телефонний сигнал. Фільтр DSL включається між кожним телефоном і телефонною розеткою.

DSL-модему фільтр не потрібно. Роботі DSL-модему частоти, використовувані телефоном, не заважають. DSL-модем може підключатися безпосередньо до комп'ютера, як показано на рис. 7.39.

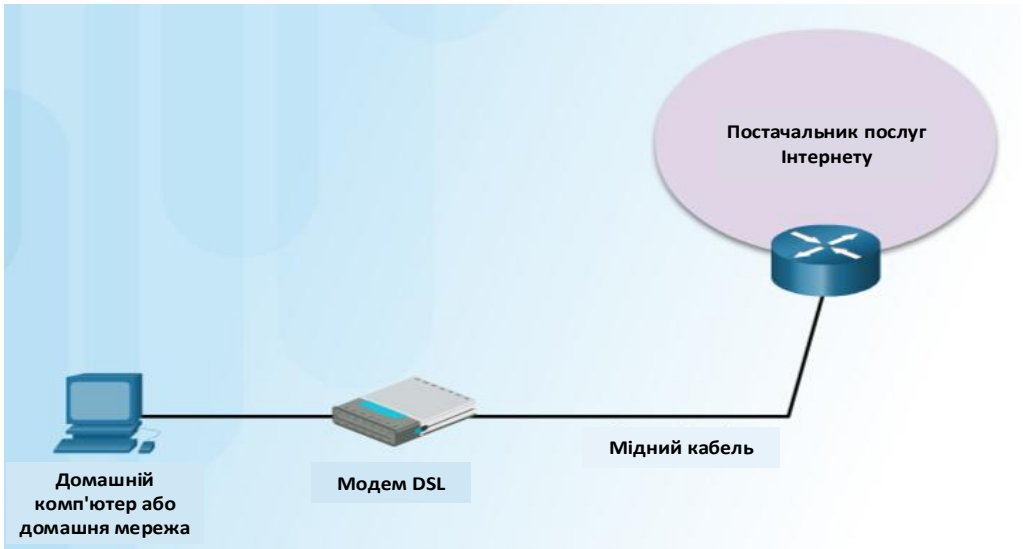


Рис. 7.39 – Підключення по DSL

Він також може підключатися до мережевого обладнання для загального доступу до підключення до Інтернету з декількома комп'ютерами.

7.3.2 Асиметрична цифрова абонентська лінія (ADSL)

Технологія ADSL відрізняється тим, що в ній пропускні спроможності в кожному з напрямків різні. Завантаженням (скачуванням, download) називається приймання даних від сервера кінцевим користувачем. Відправленням (заливанням, завантаженням на сервер, upload) називається пересилання даних від кінцевого користувача на сервер. Технологія ADSL забезпечує високу швидкість завантаження, що зручно користувачам, які завантажують більші обсяги даних. Швидкість відправлення при використанні ADSL менше, чим швидкість завантаження. ADSL не слід використовувати для розміщення веб-сервера або сервера FTP, оскільки вони передбачають інтенсивне відправлення даних в Інтернет.

7.3.3 Безпроводовий доступ до Інтернету в зоні прямої видимості

Безпроводовий доступ до Інтернету в зоні прямої видимості є постійно надаваною послугою, яка використовує радіосигнали для передачі доступу до Інтернету, як показано на рис. 7.40. Радіосигнали передаються від вишки до приймача, який користувач підключає до комп'ютера або мережевого обладнання. У цьому випадку необхідно, щоб між вишкою й приймачем не було перешкод. Вишка може бути підключена до інших вишок або мати безпосереднє підключення до магістрального каналу Інтернету.



Рис. 7.40. – Безпроводовий доступ до Інтернету в зоні прямої видимості

Відстань, на яку може передаватися радіосигнал, залишаючись досить потужним, щоб забезпечити стійке приймання, залежить від частоти сигналу. Сигнал низької частоти (900 МГц) може передаватися на відстань до 65 км, у той час як сигнал більш високої частоти (5,7 ГГц) може

подолати тільки 3 км. Погані погодні умови, дерева й високі будинки можуть вплинути на інтенсивність і якість сигналу.

7.3.4 WiMAX

Технологія широкосмугового доступу в мікрохвильовому діапазоні (Wimax) є технологією широкосмугового безпроводового зв'язку 4G на базі IP, яка забезпечує мобільним обладнанням високошвидкісний мобільний доступ до Інтернету рис. 7.41. Стандарт WiMAX зветься IEEE 802.16e. Він підтримує великі муніципальні мережі й швидкість завантаження до 70 Мбіт/с на відстанях до 50 км. Безпека і якість обслуговування (Qos) при використанні WiMAX такі ж, як і в стільникових мережах.

WiMAX використовує передачу по УКВ (ультракоротким хвилям), звичайно на частотах від 2 до 11 ГГц. Хвилі цих частот, на відміну від хвиль більш високих частот, краще долають фізичні перешкоди, оскільки вони можуть краще їх обгинати. Підтримується технологія множинних входів і виходів (Multiple Input Multiple Output, MIMO), що дозволяє встановлювати додаткові антени для збільшення пропускної спроможності.

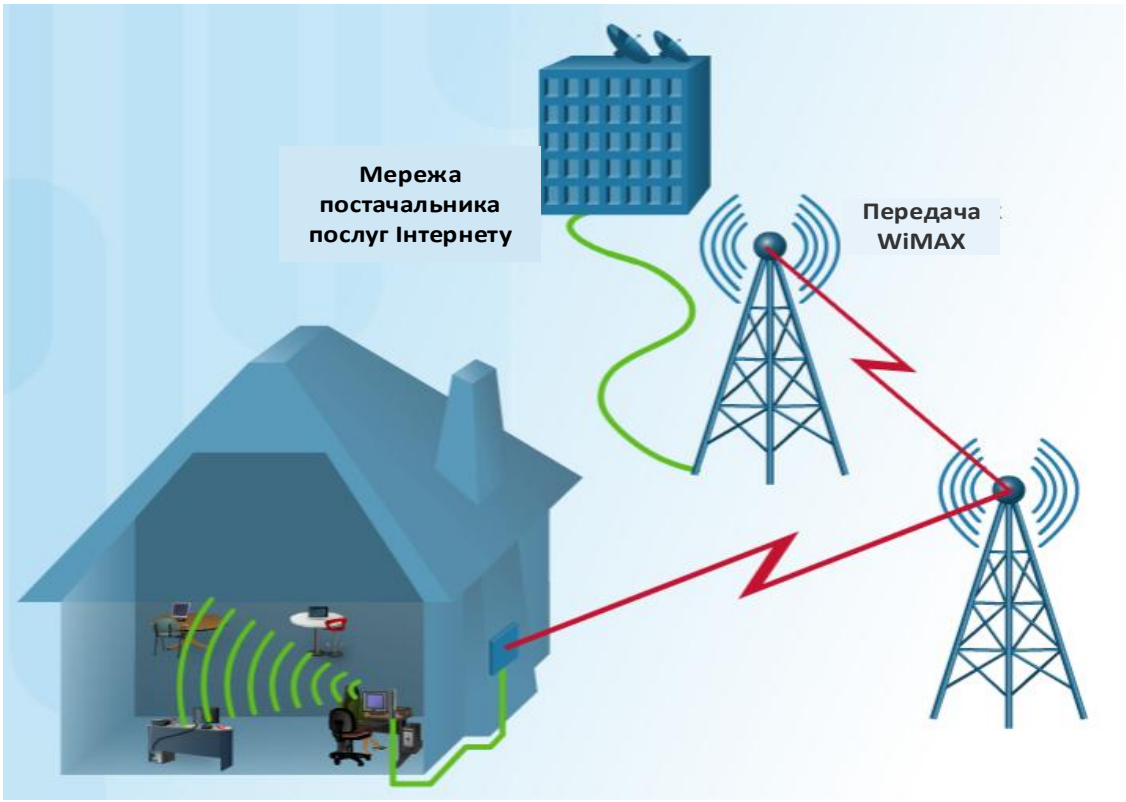


Рис. 7.41 – Передача WiMAX

Існують два способи передачі сигналу в мережах Wimax:

Fixed Wimax (Фіксований Wimax) — мережа « точка-точка» або « точка-багатоточка» зі швидкістю до 72 Мбіт/з на відстані до 50 км.

Mobile Wimax (Мобільний Wimax) — мобільна служба, схожа на Wi-Fi, але з більш високими швидкостями й більшою дальністю передачі.

7.3.5 Інші широкосмугові технології

Широкосмугові технології надають різні способи зв'язку між людьми й обладнаннями з метою спілкування й обміну інформацією. Деякі із цих способів багатофункціональні, інші призначені для забезпечення конкретних потреб. Важливо мати чітке уявлення про декілька широкосмугових технологіях і про те, як вони можуть щонайкраще допомогти замовникові.

7.3.5.1 Стільниковий зв'язок

Стільникові технології дозволяє передавати голос, відео й дані. Установивши стільниковий адаптер WAN, користувач зможе одержати доступ до Інтернету через стільникову мережу. Існують різні способи стільникового доступу в глобальну мережу:

1G — тільки аналоговий голосовий зв'язок

2G — цифровий голосовий зв'язок, конференц-зв'язок і ідентифікація зухвалого абонента; швидкість передачі даних нижче 9,6 кбіт/с

2.5G — швидкість передачі даних від 30 кбіт/с до 90 кбіт/с; підтримує перегляд веб-сторінок, коротких аудіозаписів і відео кліпів, завантаження ігор, додатка й мелодій виклику

3G — швидкість передачі даних від 144 кбіт/с до 2 Мбіт/с; підтримує повноцінний перегляд відео, потокову музику, 3 D-Гри й прискорений перегляд веб-сторінок

3.5G — швидкість передачі даних від 384 кбіт/с до 14,4 Мбіт/с; підтримує високоякісне потокове відео, високоякісну відеоконференц-зв'язок і IP-телефонію

4G — швидкість передачі даних від 5,8 Мбіт/с до 672 Мбіт/с (мобільний зв'язок) або до 1 Гбіт/с (стаціонарний зв'язок); підтримує передачу голосу по IP, ігрові послуги, високоякісне потокове мультімедіа й IPv6

5G — максимальна досяжна швидкість передачі даних при ідеальних умовах 10 – 20 Гбіт/с. Стандарт зв'язку нового покоління повинен забезпечувати пряме з'єднання між абонентами, наднадійні масштабні системи комунікації між обладнаннями, а також менший час затримки, швидкість інтернету 1-2 Гбіт/с

Стільникові мережі використовують принаймні одну з наступних технологій:

Глобальна система мобільного зв'язку (GSM) — стандарт, використовуваний для стільникового зв'язку по усьому світу.

Система пакетного радіозв'язку загального призначення (GPRS) — служба передачі даних для користувачів GSM.

Чотирьохдіапазонний зв'язок — дозволяє стільниковому телефону працювати на всіх чотирьох частотах GSM: 850 МГц, 900 МГц, 1800 МГц і 1900 МГц.

Служба коротких повідомлень (SMS) — служба передачі даних, використовувана для відправлення й одержання текстових повідомлень.

Служба мультимедійних повідомлень (MMS) — служба передачі даних, використовувана для відправлення й одержання текстових повідомлень, які можуть містити в собі мультимедійний уміст.

Enhanced Data Rates for GSM Evolution (EDGE) — підвищення швидкості передачі даних і їх надійності.

Evolution-Data Optimized (EV-DO) — підвищення швидкості завантаження і якості обслуговування (Qos).

High Speed Downlink Packet Access (HSDPA) — доступ по 3G з підвищеною швидкістю.

7.3.5.2 Кабельне підключення

Кабельне підключення до Інтернету не використовує телефонні лінії. У цьому випадку використовуються лінії коаксіального кабелю, спочатку призначені для кабельного телебачення. Для підключення комп'ютера до компанії послуги, що надає, кабельного доступу, служить кабельний модем. Комп'ютер можна підключити безпосередньо до кабельного модему. Крім того, можна підключити модем до маршрутизатора, комутатора, концентратора або багатофункціонального мережного обладнання, що дозволить декільком комп'ютерам мати доступ до Інтернету. Як і DSL, кабель забезпечує високу швидкість і постійне підключення, а це значить, що підключення до Інтернету доступно навіть тоді, коли воно не використовується.

7.3.5.3 Супутникова передача

Широкосмугова супутникова передача — альтернатива для користувачів, які не можуть використовувати кабельне підключення або DSL. Для супутникового зв'язку не потрібна телефонна лінія або кабель, оскільки для двостороннього зв'язку використовується супутникова антена. Супутникова антена передає й ухвалює сигнали від супутника, який пересилає ці сигнали постачальникові послуг, як показано на рис. 7.42.

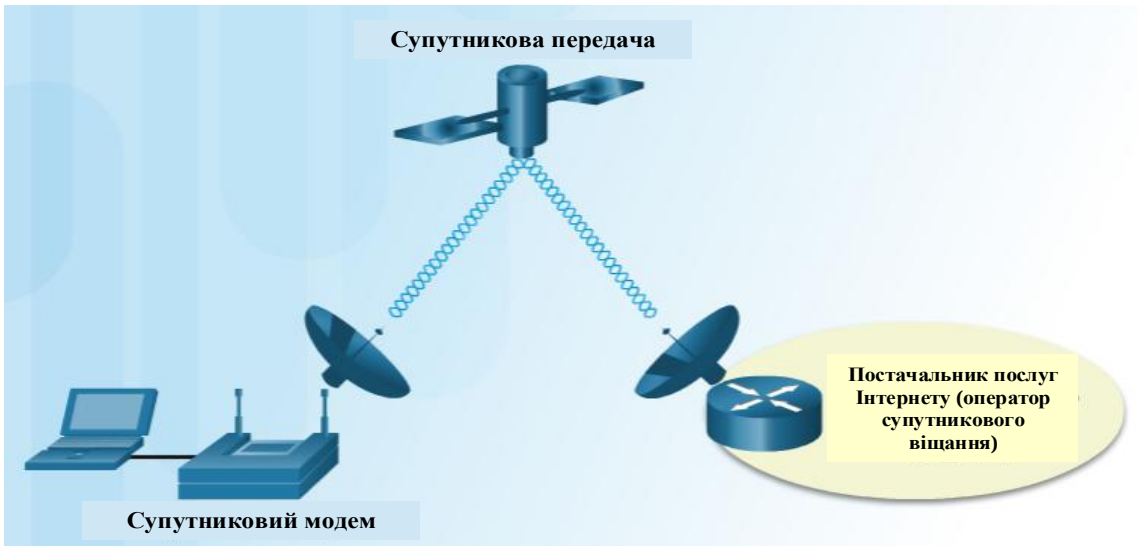


Рис 7.42 – Супутниковий зв'язок

Швидкість завантаження може досягати як мінімум 10 Мбіт/с, тоді як швидкість відправлення становить приблизно 1/10 від швидкості завантаження. Для передачі сигналу від супутникової антени до постачальника послуг Інтернету через супутник на орбіті Землі необхідно певний час. Ця затримка ускладнює використання чутливих до затримок додатків, наприклад, відеоігор, IP-телефонії й відеоконференцзв'язку.

7.3.5.4 Оптоволоконний широкосмуговий зв'язок

Оптоволоконний широкосмуговий зв'язок забезпечує більш високі швидкість з'єднання й пропускну спроможність, чому кабельні модеми, ISDN і DSL. Цей вид зв'язку дозволяє одночасно використовувати безліч цифрових послуг, таких як телефонія, відео, передача даних і відеоконференцзв'язок (табл7.4, 7.5).

Таблиця 7.4 – Докладніше про підключення постачальника послуг Інтернету

Тип	Переваги	Недоліки	Швидкість
POTS	Широка поширеність	Дуже низька швидкість Неможливо приймати телефонні дзвінки при підключенні до Інтернету	Макс. 56 Кбіт/с
ISDN	Швидкість вище, чим в POTS	Проте, ця технологія працює набагато повільніше, чим інші технології широкосмугового зв'язку	Інтерфейс базового доступу (BRI) – до 128 Кбіт/с Інтерфейс первинного доступу (PRI) – до 2,048 Мбіт/с
DSL	Низька вартість	На швидкість впливає відстань до АТС	24 Кбіт/з – 100 Мбіт/с
Кабельне підключення	Дуже висока швидкість	Низька швидкість відправлення	27 Кбіт/з – 160 Мбіт/с
Супутникова передача	Доступна там, де недоступні DSL і кабельні мережі	Дорожче, чим інші технології широкосмугового зв'язку, залежить від погодних умов	До 10 Мбіт/с або вище
Стільниковий зв'язок	Доступні для мобільних користувачів	Доступні не скрізь	20 Кбіт/с і вище залежно від використовуваної технології

Таблиця 7.5 – Визначення типів підключень постачальника послуг Інтернету

Термін	Опис
Стільниковий зв'язок	Замовник є торговельним представником і багато часу проводить у поїздках. Підключення до головного офісу необхідно майже цілодобово.
Супутникова передача	Замовник працює в будинку, йому потрібні максимально можливі швидкості висхідної й спадної передачі даних для доступу до сервера FTP компанії. Він живе в дуже вилученому районі, де недоступні DSL і кабельне підключення.

Термін	Опис
WiMAX	Замовник працює в діловому районі великого міста, і йому потрібно швидке надійне підключення, стійке до перешкод через більші будинки.
DSL	Замовник може приймати телевізійний сигнал тільки через супутник, але живе в районі, де є високошвидкісний доступ до Інтернету.
Доступ, що комутується	Замовник живе у віддаленому районі в глибокій долині й не може дозволити собі широкосмуговий зв'язок.
Кабельне підключення	Замовник хоче користуватися послугами одного постачальника для телебачення, доступу до Інтернету й телефонного зв'язку, але місцева телефонна компанія не надає всі ці послуги.

7.4 Центр обробки даних

У міру еволюції організацій для них потрібне збільшення обчислювальної потужності й простору для зберігання на жорсткому диску. Якщо ці вимоги залишити невиконаними, це вплине на можливість організації надавати необхідні послуги. Неможливість надання необхідних послуг приводить до меншої задоволеності замовників, більш низькому прибутку й, у деяких ситуаціях, втраті власності або способу життя.

Велике підприємство звичайне має власний центр обробки даних для управління сховищем і задоволення потреб організації в доступі до даних. У цих користувацьких центрах обробки даних підприємство є єдиним замовником або користувачем, що використовують послуги центру обробки даних. Разом з тим, оскільки обсяг даних продовжує рости, навіть великі підприємства збільшують ємність сховищ даних, використовуючи послуги сторонніх центрів обробки даних.

На сьогоднішній момент у світі існують більш 3000 центрів обробки даних, які пропонують організаціям загальні послуги з розміщення інформації. І набагато більше центрів обробки даних належать приватним корпораціям для їхнього власного використання.

7.4.1 Хмарні обчислення й центр обробки даних

Такі терміни, як центр обробки даних і хмарні обчислення, часто використовуються неправильно. Відповідні визначення центру обробки даних і хмарних обчислень (рис. 7.43) [1-3].

Центр обробки даних — звичайне сховище даних і система обробки, використовувані внутрішнім відділом IT або орендарем.

Хмарні обчислення — звичайно дистанційна послуга, яка забезпечує доступ по запиту до загального пулу, що настроюються обчислювальних ресурсів. Ці ресурси можна швидко виділяти й звільняти з мінімальними зусиллями по управлінню.

Постачальники хмарних послуг використовують центри обробки даних для надання хмарних послуг і хмарних ресурсів. Для забезпечення

доступності ресурсів і послуг передачі даних постачальники часто виділяють певний простір у декількох віддалених центрах обробки даних.



Рис. 7.43 – Центр обробки даних

Національний інститут стандартів і технологій (NIST) у спеціальній публікації 800-145 визначає модель хмари, яка містить у собі п'ять характеристик, три моделі обслуговування й чотири моделі розгортання.

Хмарні обчислення – це модель для забезпечення повсюдного, зручного мережевого доступу на вимогу до спільно використовуваного пулу конфігуруємих обчислювальних ресурсів (наприклад, мереж, серверів, сховищ, додатків і сервісів), які можуть бути швидко підготовлені й випущені з мінімальними зусиллями по управлінню або взаємодія постачальника послуг. Ця хмарна модель складається з п'яти основних характеристик, трьох моделей обслуговування й чотирьох моделей розгортання.

Ключові слова

Хмарні обчислення; SaaS; PaaS; IaaS;
Самообслуговування на вимогу;
Резервний пул;
Швидка еластичність;
Обмірюване обслуговування;
Програмне забезпечення як сервіс;
Платформа як послуга; Інфраструктура як послуга

7.4.2. Характеристики хмарних обчислень

Як показано на рис. 7.44 модель хмари містить у собі п'ять характеристик:

Самообслуговування по запиту — мережевий адміністратор може придбати додаткові обчислювальні ресурси в хмарі без необхідності взаємодії з іншими людьми.

Широкий мережевий доступ — доступ до хмари можливий з використанням безлічі різних клієнтських пристроїв, наприклад ПК, ноутбуків, планшетів і смартфонів.

Об'єднання ресурсів — обчислювальна потужність постачальника хмарних послуг спільно використовується всіма його замовниками й може бути як призначена, так і перепризначена відповідно до потреб замовників.

Більша гнучкість — ресурси, виділювані для замовників, можуть швидко збільшуватися або узгоджуватися по запиту. З погляду замовника ресурси й можливості постачальника хмарних послуг здаються необмеженими.

Вимірювана якість обслуговування — можна легко контролювати використання ресурсів, управляти ними, становити відповідну звітність і виставляти рахунку з метою забезпечення повної прозорості по наданню хмарних послуг для замовника.



Рис. 7.44 – Модель хмарних обчислень

7.4.3 SaaS, IaaS і PaaS

На рис. 7.45 показано три основні моделі хмарного обслуговування. Постачальники хмарних послуг розширюють ці моделі з метою надання IT-Підтримки для кожної послуги хмарних обчислень (IT як послуга).

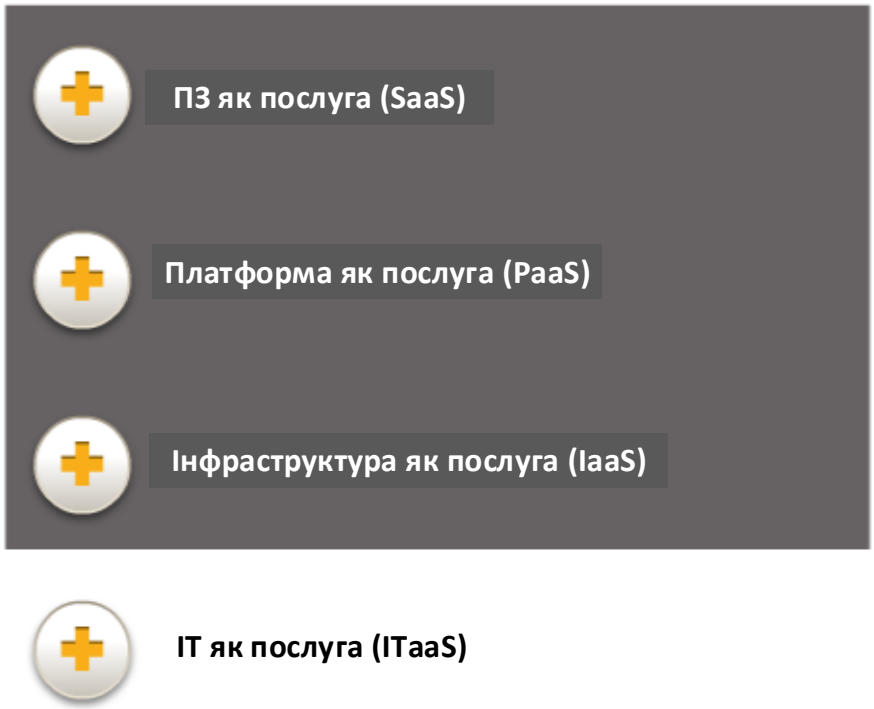


Рис. 7.45 – Модель хмарного обслуговування

ПЗ як послуга (SaaS)

Постачальник хмарних послуг відповідає за доступ до послуг, таким як електронна пошта, зв'язок і віртуальний робочі столи, що доставляються через Інтернет.

Платформа як послуга (PaaS)

Постачальник хмарних послуг відповідає за доступ до служб і засобам розробки, які використовуються для доставки додатків.

Інфраструктура як послуга (IaaS)

Постачальник хмарних послуг відповідає за доступ до мережного встаткування й виртуализированным мережним службам і опорній мережній інфраструктурі.

IT як послуга (ITaaS)

Постачальник хмарних послуг відповідає за IT-підтримку моделей послуг IaaS, PaaS і SaaS. У моделі ITaaS організація домовляється з постачальником хмарних послуг по індивідуальних або пакетним послугам.

7.4.4 Типи хмар

Чотири моделі розгортання хмари:

- Private (Приватна)
- Public (Загальнодоступна)
- Community (Суспільна)
- Hybrid (Гібридна)

Суспільна модель хмари розгортається в інтересах конкретного набору користувачів. Чотири приклади суспільної моделі розгортання хмари показано на рис. 7.46.

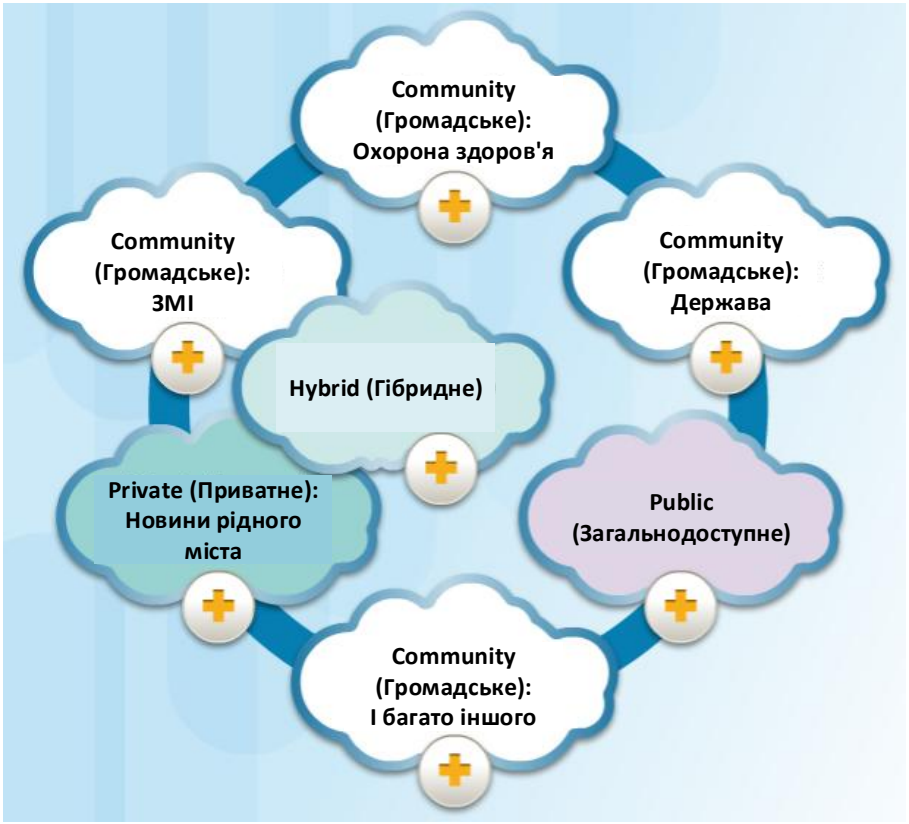


Рис. 7.46 – Приклади суспільної моделі розгортання хмари

Суспільні хмари

Це хмари, які створюються для задоволення потреб якої-небудь конкретної галузі, наприклад охорони здоров'я або ЗМІ. Суспільні хмари можуть бути приватними або загальнодоступними.

Гібридні хмари

Гібридна хмара полягає як мінімум із двох хмар (наприклад, одного суспільного й одного загальнодоступного), і кожна хмара залишається окремим об'єктом, але вони обидва з'єднані єдиною архітектурою. Користувачі, підключені до гібридної хмари, можуть мати різні рівні доступу до послуг залежно від своїх прав доступу.

Приватні хмари

Хмарні додатки й сервіси, пропоновані в приватній хмарі, доступні співробітникам певного підприємства або організації, наприклад державної компанії.

Приватна хмара можна організувати, використовуючи приватну мережу компанії. Однак створення й обслуговування такої хмари може бути витратним. Управління приватною хмарою можна доручити зовнішньої організації, яка здатна забезпечити максимальну безпеку доступу.

Загальнодоступні хмари

Хмарні додатки й послуги, пропоновані в загальнодоступній хмарі, доступні необмеженому колу осіб. Послуги можуть бути безкоштовними або можуть пропонуватися за схемою «оплата за фактом використання», наприклад, у випадку оплати інтернет– сховища. Загальнодоступна хмара використовує Інтернет для надання послуг.

Порівняння характеристик різновидів хмарних послуг по призначенню представлена в табл 7.6

Таблиця 7.6 Визначення хмарної термінології

Термін	Опис
Public (Загальнодоступна хмара)	Цей різновид хмари робиться загальнодоступної постачальником послуг, який володіє хмарною інфраструктурою.
Інфраструктура як послуга (Infrastructure as a Service, Iaas)	Постачальник хмарних послуг надає мережеве обладнання, віртуалізовані мережеві сервіси й опорну мережеву інфраструктуру.
Community (Суспільна хмара)	Цей різновид хмари є загальним для декількох організацій.
Private (Приватна хмара)	Ця хмарна інфраструктура управляється й використовується конкретною організацією.
ПО як послуга (Software as a Service, Saas)	Постачальник хмарних послуг управляє додатками для кінцевих користувачів і доставляє ці додатки через Інтернет.
Hybrid (Гібридна хмара)	Ця хмарна інфраструктура є комбінацією як мінімум двох різновидів хмари: загальнодоступної, приватної або суспільної.
Платформа як послуга (Platform as a Service, Paas)	Постачальник хмарних послуг управляє інфраструктурою, наприклад, апаратури й операційної системи.
IT як послуга (IT as a Service, Itaas)	Робоча модель для надання IT-підтримки Saas, Paas і Iaas.

7.4.5. Служби DHCP

Вузли в мережах виконують певну роль. Деякі із цих вузлів виконують завдання забезпечення безпеки, тоді як інші вузли надають вебпослуги. Також існують багато традиційні й вбудовані системи, які виконують певні завдання, такі як послуги з роботи з файлами або печатки.

Для відправлення даних по мережі вузлу необхідна інформація про IP-адресі. Двома важливими службами IP-адресації є протокол динамічного конфігурування вузла (DHCP) і служба доменних імен (DNS).

Саме служба DHCP використовується постачальниками послуг Інтернету, мережевими адміністраторами й безпроводовими маршрутизаторами для автоматичного призначення даних про IP-адресації вузлам, як показано на рис. 7.47.

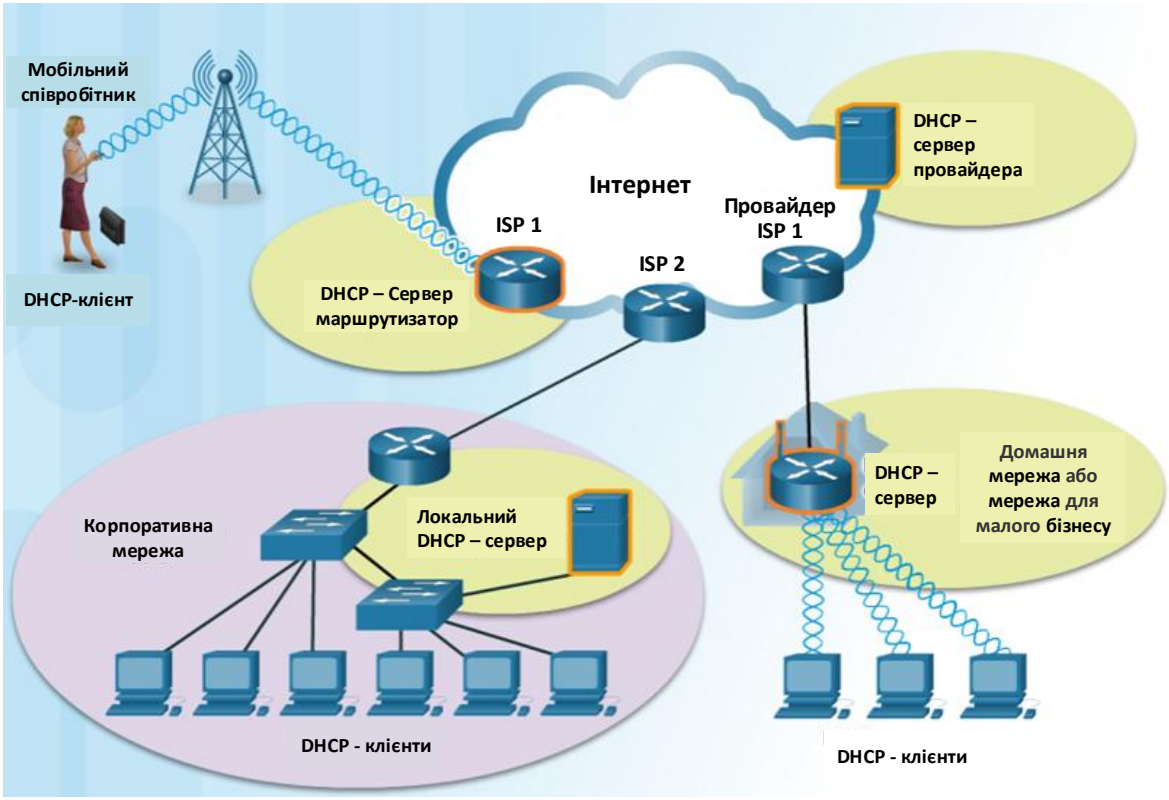


Рис. 7.47 – Служба DHCP

Як показано на рис. 7.48, коли пристрій IPv4, настроєний на використання DHCP, завантажується або підключається до мережі, клієнт виконує широкомовне розсилання повідомлення для виявлення DHCP (DHCPDISCOVER) з метою ідентифікації всіх доступних серверів DHCP у мережі.

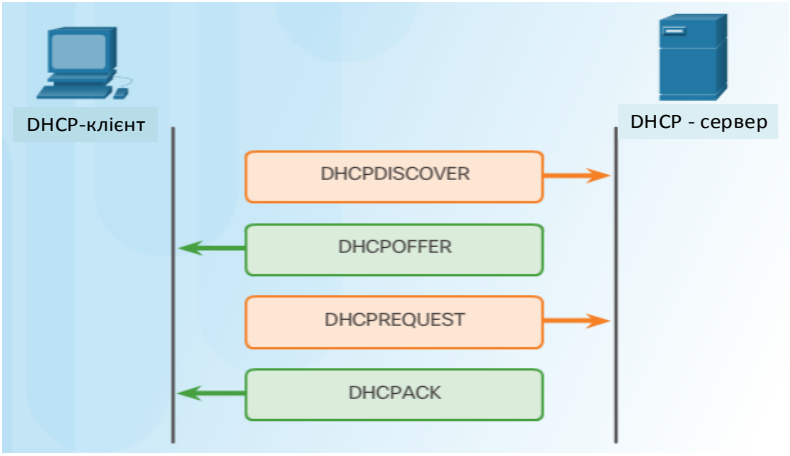


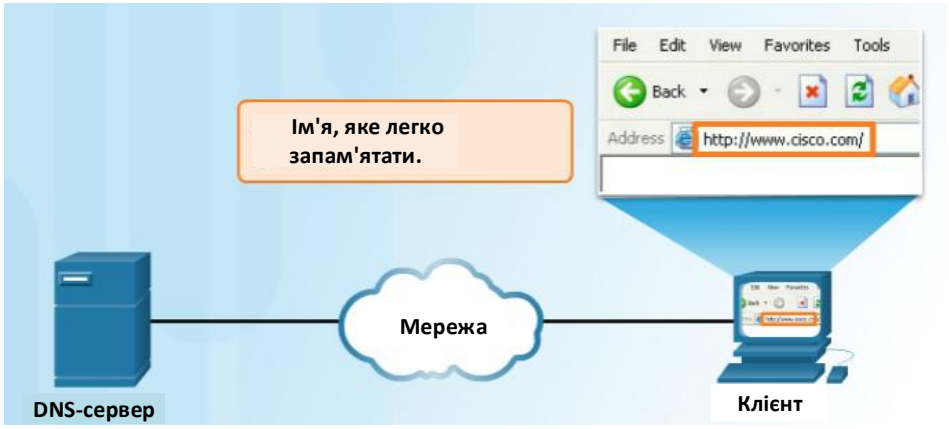
Рис. 7.48 – Взаємодія DHCP – клієнта з DHCP – сервером

Сервер DHCP відповідає повідомленням із пропозицією DHCP (DHCPOFFER), яке пропонує клієнтові «орендувати» (lease) адреса. Повідомлення із пропозицією містить призначувані адресу IPv4 і маску підмережі, адреса IPv4 DNS-Сервера й адреса IPv4 шлюзу за замовчуванням. У пропозиції оренди також вказується її строк.

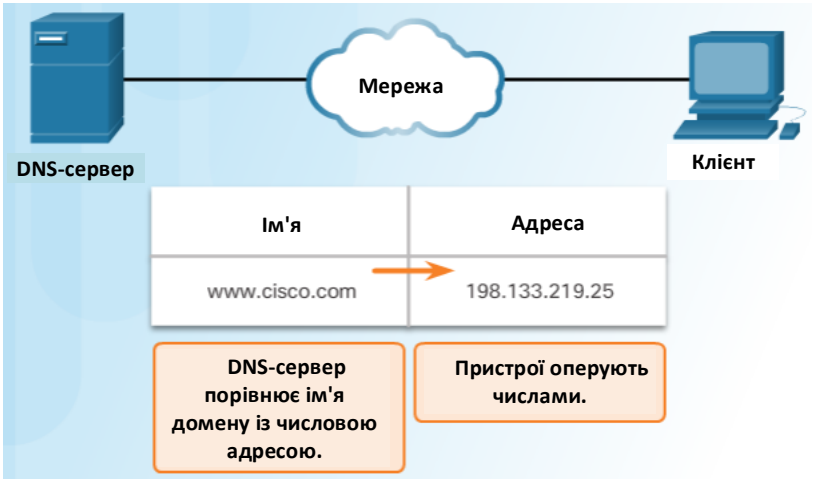
7.4.6 Служби DNS

Служба DNS використовується комп'ютерами для перетворення доменних імен в IP-адреси. В Інтернеті людям набагато простіше запам'ятати доменні імена, наприклад, http://www.cisco.com, чім 198.133.219.25, що є поточним числовим IP-адресом даного сервера. Якщо компанія Cisco вирішить змінити IP-адресу сайту www.cisco.com, це відбудеться непомітно для користувачів, тому що доменне ім'я залишиться без змін. Нова адреса буде просто прив'язана до існуючому імені домена без порушення зв'язку із сервером.

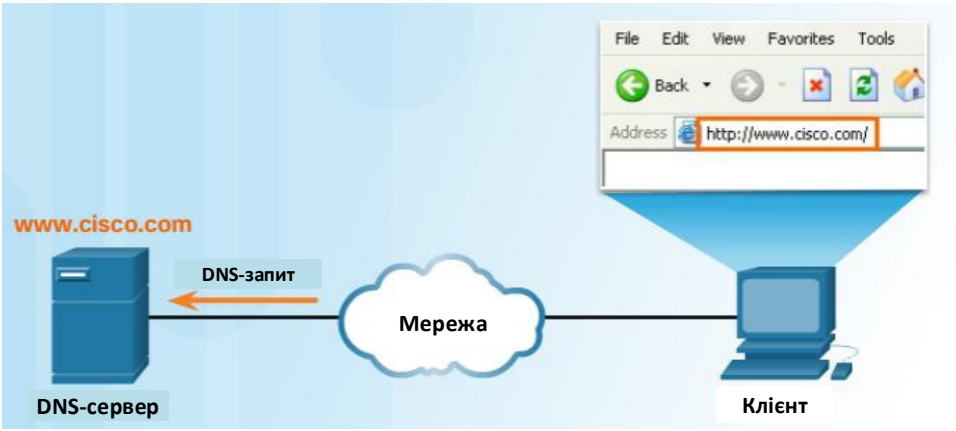
На рис. 7.49 починаючи з а) по д) показані кроки, з яких полягає процес дозволу імен у службі доменних імен.



а) Дозвіл адрес DNS: етап 1



б) Дозвіл адрес DNS: етап 2



в) Дозвіл адрес DNS: етап 3



г) Дозвіл адрес DNS: етап 4



д) Дозвіл адрес DNS: етап 5

Рис. 7.49 – Процес дозволу імен у службі доменних імен

7.4.7 Веб-служби

Веб-ресурси надаються веб-сервером. Вузол одержує доступ до веб-ресурсів Інтернету за допомогою протоколу передачі гіпертексту (HTTP)

або захищеного протоколу HTTP (HTTPS). HTTP являє собою набір правил для обміну текстом, графічними зображеннями, звуком і відео по Інтернету. HTTPS забезпечує підтримку шифрування й служб автентифікації з використанням протоколу рівня захищених сокетів (SSL) або більш нового протоколу захисту транспортного рівня (TLS). HTTP працює через порт 80. HTTPS працює через порт 443.

Щоб ви могли краще зрозуміти взаємодію браузера з веб-сервером, ми докладно опишемо, як веб-сторінка відкривається в браузері. У даному прикладі використовується URL-адреса http://www.cisco.com/index.html.

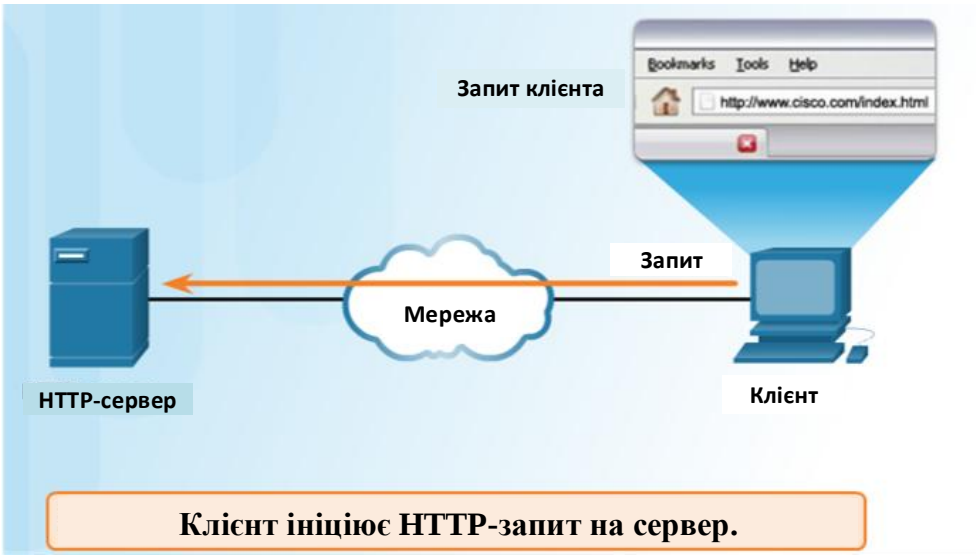
По-перше, як показано на рис. 7.50 а), браузер інтерпретує три частини URL:

1. **HTTP** (протокол або схема).
2. **www.cisco.com** (ім'я сервера).
3. **index.html** (назва конкретного запитуваного файлу).



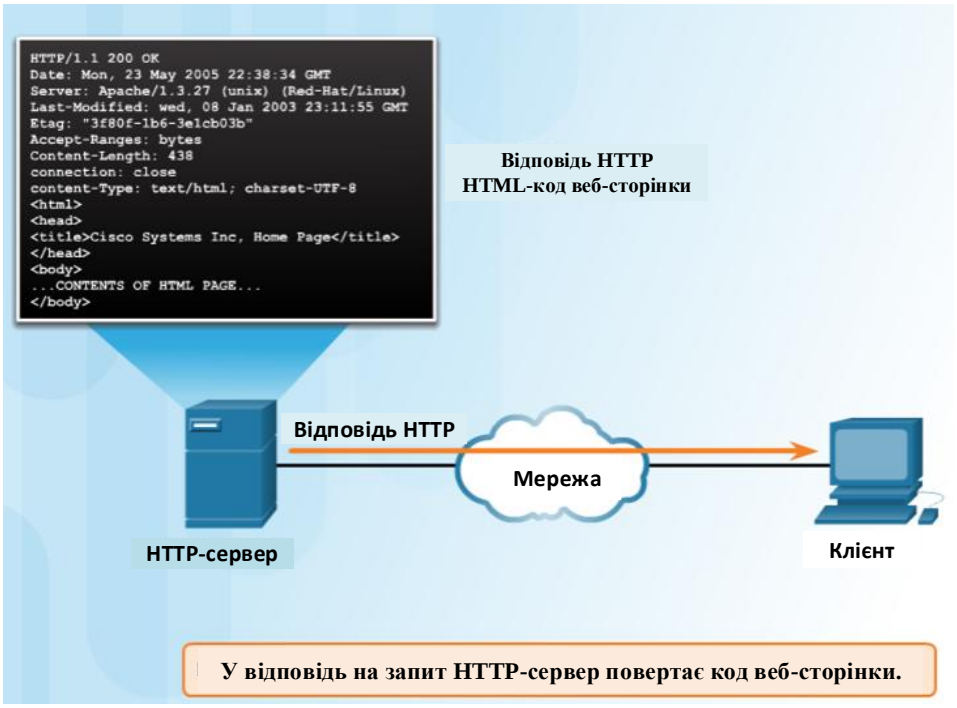
а) Протокол HTTP: інтерпретація URL

Потім браузер за допомогою сервера доменних імен (DNS) проводить перетворення імені www.cisco.com у числову адресу, яка використовується для підключення до сервера. Згідно з вимогами протоколу HTTP, браузер відправляє запит GET серверу й запитує файл index.html, як показано на рис. 7.50 б).



б) Протокол HTTP: етап 1

Сервер відправляє HTML-код цієї веб-сторінки назад веб-браузеру клієнта, як показано на рис. 7.50 в). І нарешті, як показано на рис. 7.50 г), браузер декодує HTML-код і форматує сторінку у вікні браузера.



в) **Протокол HTTP: етап 2**



г) Протокол HTTP: етап 3

Рис 7.50 – Протокол HTTP

7.4.8 Файлові служби

Протокол передачі файлів (FTP) був стандартизований в 1971 році, і дозволяє передавати дані між клієнтом і сервером. FTP-клієнт — це додаток, що запускається на комп'ютері, який використовується для завантаження даних із сервера, на якому запущений сервіс FTP, а також для одержання даних із цього сервера.

Як показано на рис. 7.51, для передачі даних по FTP потрібні два з'єднання між клієнтом і сервером, одне з яких призначене для команд і відповідей, а інше використовується для передачі файлів.



Рис. 7.51 – Процес передачі по FTP

FTP має багато слабких місць у системі забезпечення безпеки. У зв'язку із цим необхідно використовувати послуги більш захищеної передачі файлів, наприклад:

Захищений протокол передачі файлів (FTPS) — клієнт FTP може запросити сеанс передачі файлів із шифруванням за допомогою TLS. Файловий сервер може прийняти або відхилити запит.

Протокол передачі файлів поверх SSH (SFTP) — SFTP є розширенням протоколу Secure Shell (SSH) і може використовуватися для створення захищеного сеансу передачі файлів.

Протокол захищеного копіювання (SCP) — SCP також використовує SSH для захищеної передачі файлів.

7.4.9. Служби друку

Сервери друку забезпечують можливість доступу безлічі користувачів ПК до одному принтеру (рис. 7.52). Сервер друку виконує три функції:

- забезпечує клієнтський доступ до ресурсів друку;
- адмініструє завдання на друк, зберігаючи їх у черзі до того моменту, коли пристрій друку буде готове до роботи з ними, і потім направляючи або перенаправляючи інформацію для друку в принтер;
- забезпечує зворотний зв'язок з користувачем.

Сервери друку розглянуті більш докладно в іншій главі.



Рис. 7.52 Інтернет пристрої

7.4.10. Служби електронної пошти

Для електронної пошти необхідний ряд додатків і служб, як показано на рис. 7.53.

Електронна пошта — це набір засобів для доставки, зберігання й добування електронних повідомлень у мережі. Повідомлення електронної пошти зберігаються на серверах електронної пошти в базах даних.

Клієнти електронної пошти для відправлення й одержання повідомлень звертаються до серверів електронної пошти. Сервери електронної пошти взаємодіють із іншими серверами електронної пошти для обміну повідомленнями між доменами. Поштовий клієнт не з'єднується безпосередньо з іншим поштовим клієнтом для відправлення повідомлення. Обидва клієнта повинні довірити транспортування повідомлень серверу електронної пошти.

Електронна пошта підтримує використання трьох окремих протоколів: протоколу **Simple Mail Transfer Protocol** (Простий протокол передачі електронної пошти, **SMTP**), протоколу Post Office Protocol (протокол поштової відділення, **POP**) і протоколу **Internet Message Access Protocol** (протокол доступу до повідомлень в Інтернеті, **IMAP**). У процесі рівня додатків, на якому виконується відправлення пошти, використовується протокол SMTP. Клієнт одержує електронну пошту за допомогою одного із двох протоколів рівня додатків: POP або IMAP.

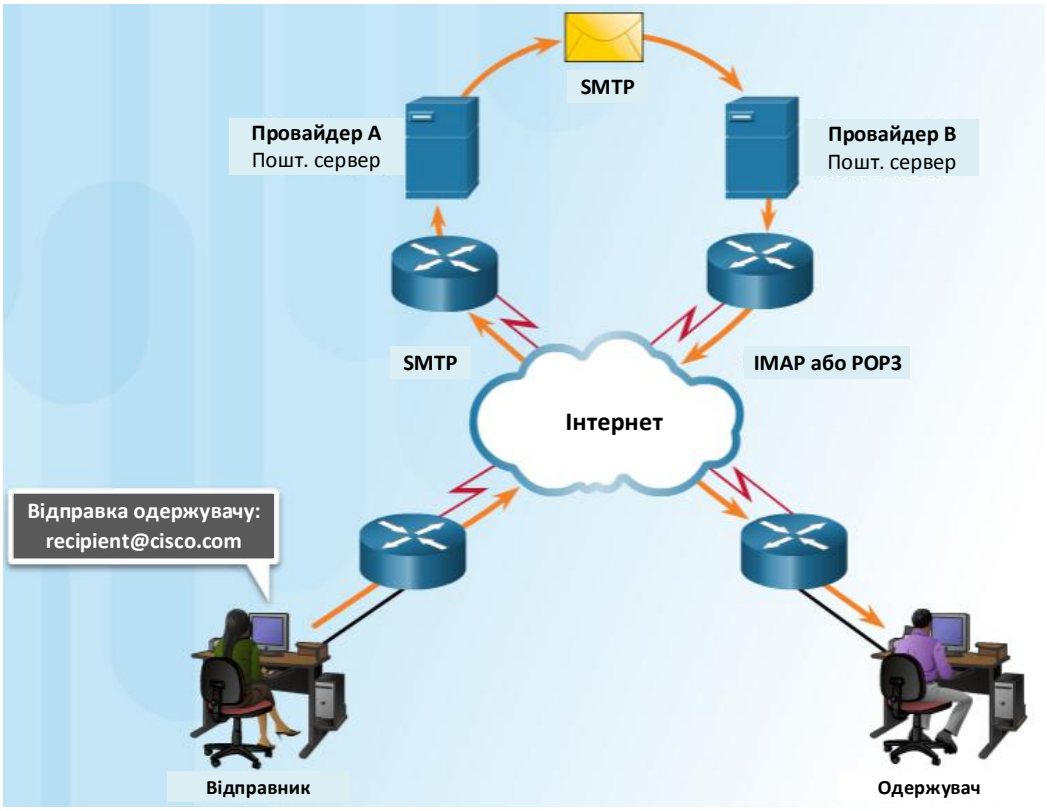


Рис. 7.53 – Електронна пошта

7.4.11 Настройка проксі

Проксі-сервер має право передавати дані від імені іншого комп'ютера. Проксі-сервер прийнято використовувати як сховище або кеш для веб-сторінок, до яких часто звертаються пристрої у внутрішній мережі. Наприклад, проксі-сервер на рис. 7.54 зберігає веб-сторінки для www.cisco.com. Коли який-небудь внутрішній вузол відправляє Http-Запит GET на www.cisco.com, проксі-сервер виконує наступні дії:

1. Перехоплює запити.
2. Перевіряє, чи був змінений уміст веб-вузла.
3. Якщо ні, проксі-сервер відправляє вузлу веб-сторінку.

Крім того, проксі-сервер може ефективно приховувати IP-адреси внутрішніх вузлів, оскільки всі запити, що відправляються в Інтернет, виходять із IP-адреси проксі-сервера.

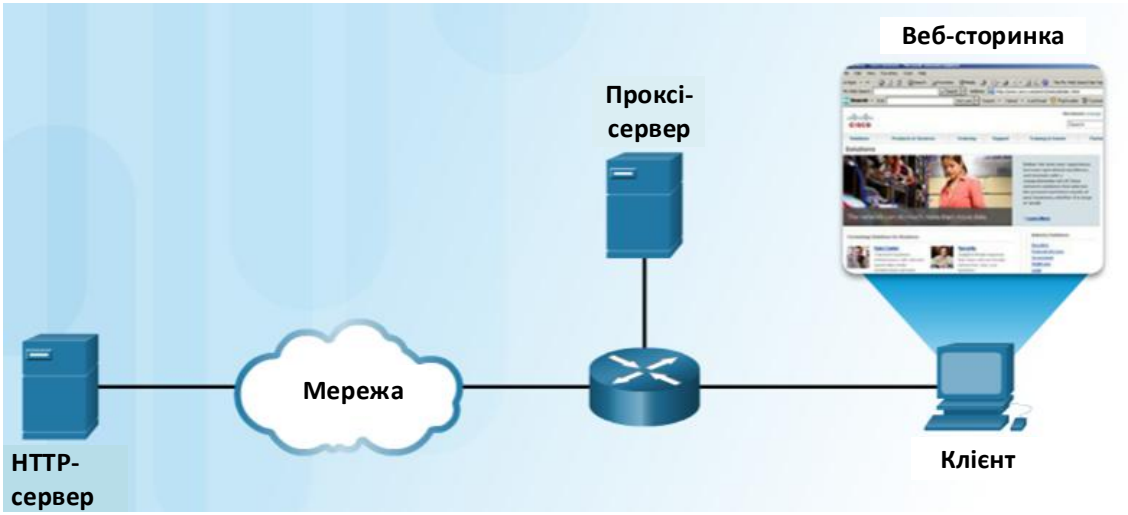


Рис. 7.54 – Проксі-сервер кешує веб-сторінки

7.4.12 Служби автентифікації

Доступ до мережевих пристроїв звичайно контролюється за допомогою служб автентифікації, авторизації й обліку. Ці служби, які називаються AAA або «трайплагов» (три букви А – authentication, authorization, accounting), забезпечують базову інфраструктуру для настроювання контролю доступу на мережевому пристрої. AAA дозволяє контролювати, які користувачі мають право доступу до мережі (автентифікація), які дії вони можуть виконувати, перебуваючи в мережі (авторизація), а також дозволяє стежити за їхніми діями під час доступу до мережі (облік).

Ця концепція схожа на використання кредитної карти, як показано на рис. 7.55. Кредитна карта визначає, хто може нею користуватися, яку суму може витратити користувач, а також веде облік товарів і послуг, які здобуває користувач.

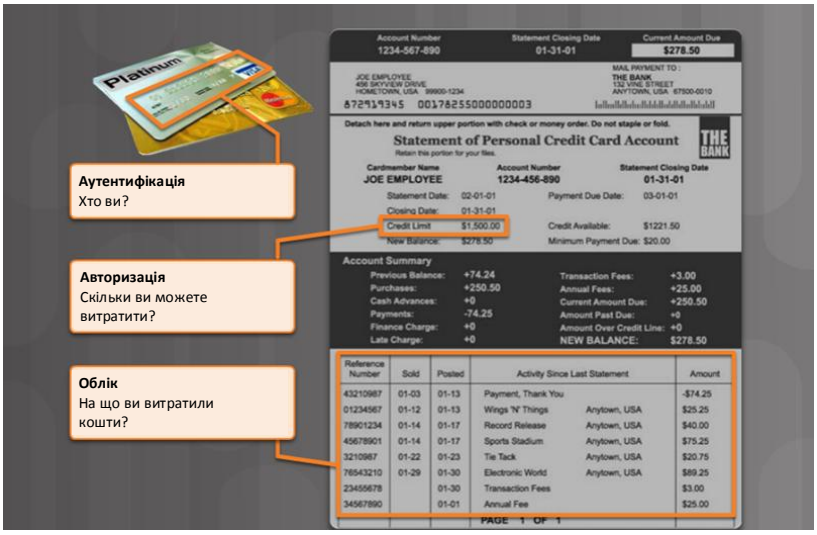


Рис. 7.55 – Концепція служб автентифікації, авторизації й обліку (AAA) схожа на використання кредитної карти

7.4.13 Служби виявлення й запобігання вторгнень

Системи виявлення вторгнень (IDS) пасивно відслідковують трафік у мережі. Ізольовані системи IDS значно уступають системам запобігання вторгнень (IPS). Однак функція виявлення IDS як і раніше є частиною будь-якої реалізації IPS. На рис. 7.56 показане, що пристрій із включеною системою IDS копіює потік трафіка й аналізує скопійований трафік, але не самі передані пакети. Працюючи в автономному режимі, система порівнює потік захопленого трафіка з відомими шкідливими сигнатурами аналогічно програмному забезпеченню, яке перевіряє наявність вірусів.

Система IPS створена на базі технології IDS. Але на відміну від неї, система IPS установлюється на шляху передачі трафіка. Це означає, що весь вхідний і вихідний трафік повинен проходити через цей пристрій для обробки. Як показано на рис. 7.57, IPS не дозволяє пакетам попадати в довірену частину мережі без попереднього аналізу. Пристрій може виявляти й негайно усувати проблеми в мережі.

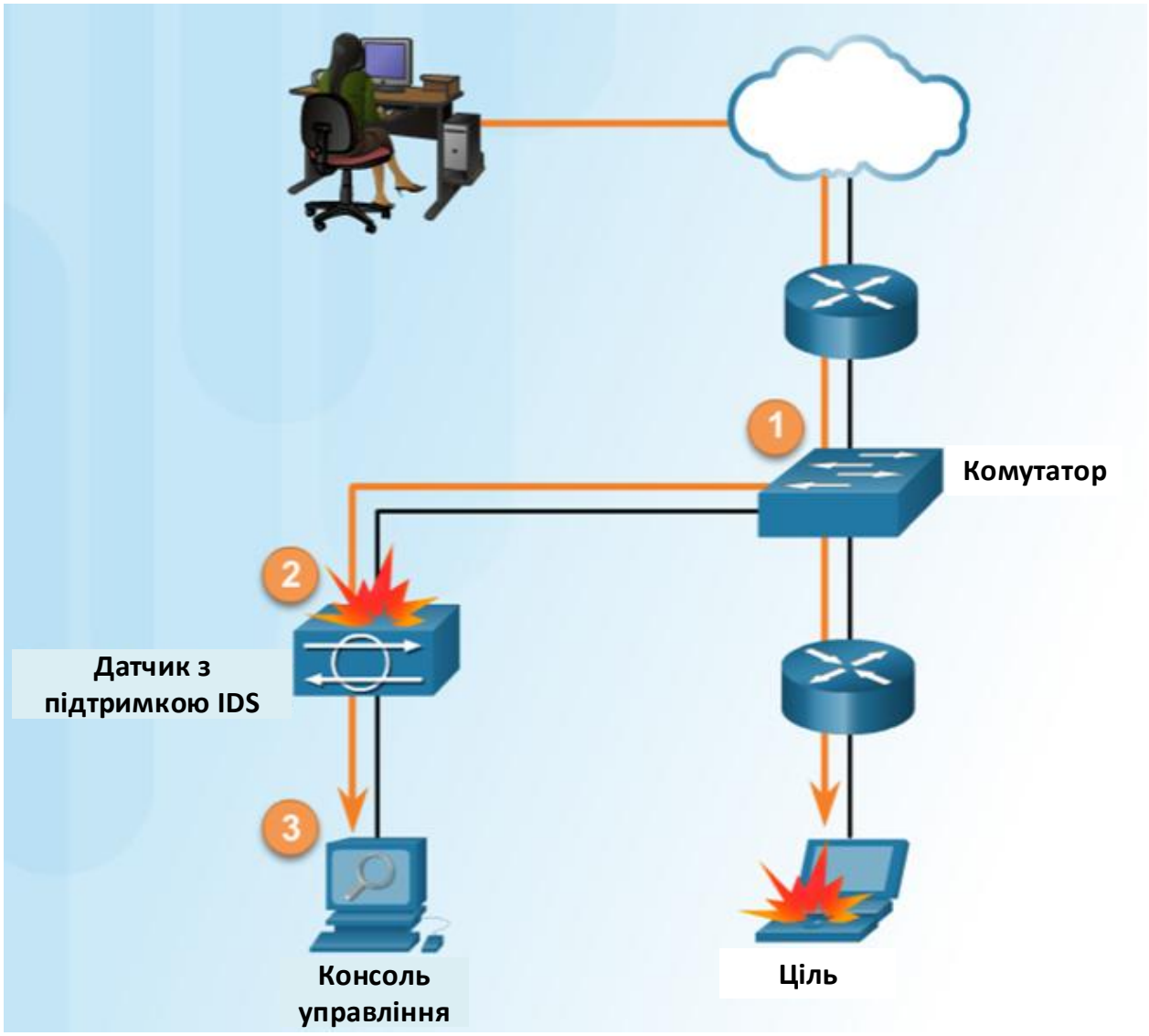


Рис. 7.56 – Робота IDS

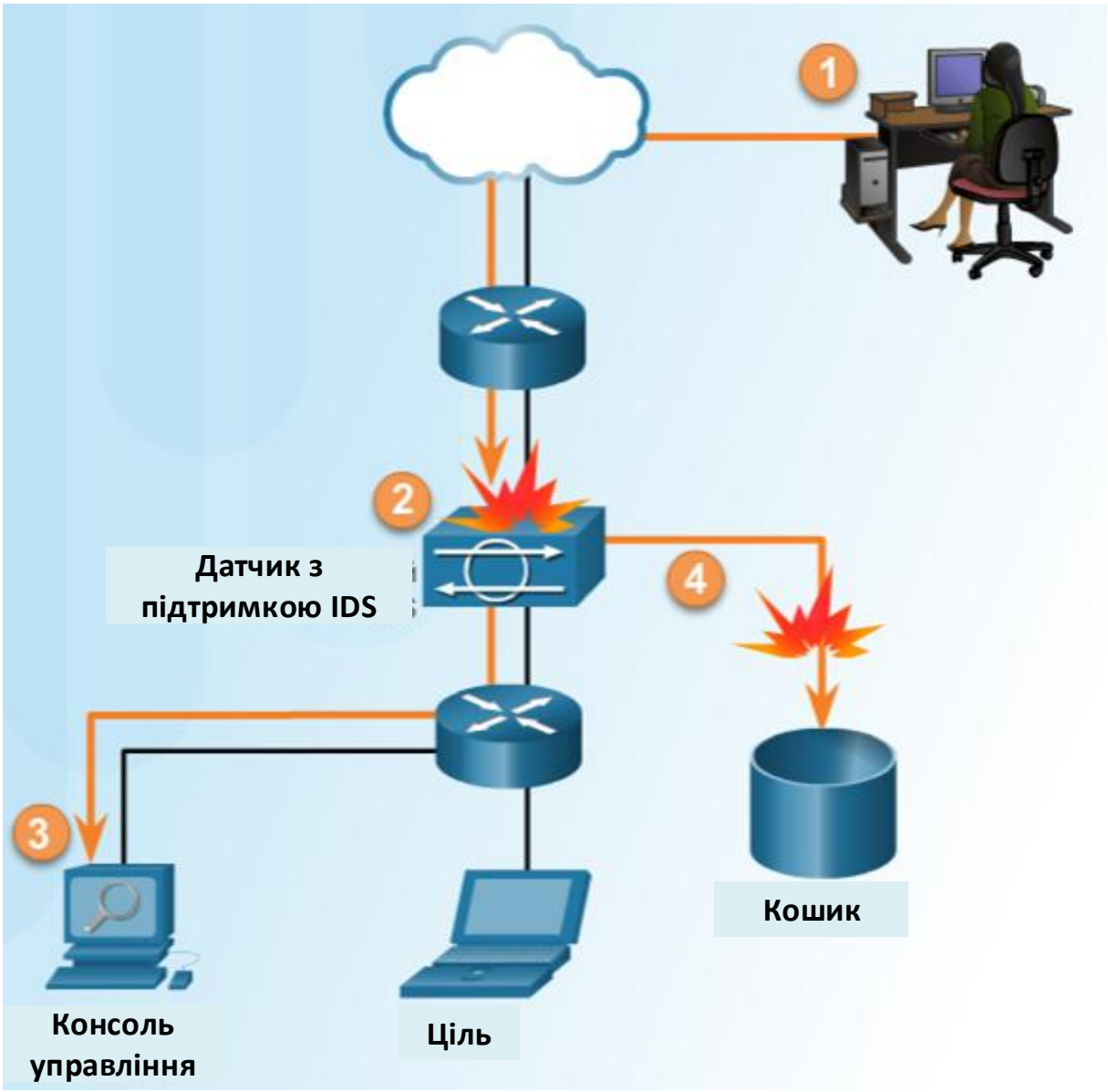


Рис. 7.57 – Робота IPS

7.4.14. Універсальна система управління погрозами

Універсальна система управління погрозами (UTM) є загальним найменуванням комплексної системи забезпечення безпеки. Системи UTM містять у собі всі функціональні можливості міжмережевих екранів з відстеженням стану й служб виявлення й запобігання вторгнень (IDS/IPS). Міжмережеві екрани з відстеженням стану забезпечують фільтрацію пакетів з відстеженням стану за допомогою використання інформації про активні підключення, яка зберігається в таблиці станів. Міжмережевий екран з відстеженням стану відслідковує кожне з'єднання, реєструючи адреси джерела й адресата, а також номера портів джерела й призначення.

Крім IDS/IPS і міжмережевих екранів з відстеженням стану, системи UTM також звичайно надають додаткові служби забезпечення безпеки, такі як:

- Захист від невідомих погроз (Zero Day)
- Захист від Dos-атак (атак на відмову в обслуговуванні) і Ddos-атак (розподілених атак на відмову в обслуговуванні)
- Фільтрація додатків на проксі-сервері
- Фільтрація електронної пошти на наявність спама й фішінгових атак
- Захист від шпигунських програм
- Управління доступом до мережі
- Служби VPN

Ці функції можуть значно змінюватися залежно від постачальника UTM.

Міжмережеві екрани наступного покоління, показані на рис. 7.58, забезпечують функціонал понад системи UTM, такий як:

- Контроль поведінки усередині самих додатків
- Обмеження використання Інтернету й веб-додатків на основі репутації вузла
- Превентивний захист від Інтернет-погроз
- Застосування політик на основі профілів користувачів, пристроїв, ролей, типів додатків і погроз

Перелік мережевих служб міжмережевих екранів доданий у табл 7.7



Рис. 7.58 – Міжмережеві екрани наступного покоління Cisco ASA

Таблиця 7.7 – Мережеві служби

Термін	Опис
Веб-служби	Вузли використовують HTTP або HTTPS для доступу до даної служби.
Служби автентифікації	Мережеві пристрої управляються за допомогою AAA.
DHCP	Ця служба автоматично призначає IP-адресацію вузлам.
Служби електронної пошти	Клієнт відправляє й одержує повідомлення за допомогою таких протоколів, як SMTP, POP і IMAP.

Термін	Опис
Служби друку	Ця служба дозволяє декільком користувачам одержувати доступ до принтера.
DNS	Ця служба перетворює доменні імена в IP-адреси.
Служби виявлення й запобігання вторгнень	Ця служба контролює й обробляє мережевий трафік.
Файлові служби	Ця служба використовує протокол FTP для передачі даних між сервером і клієнтом.

7.5 Процедури профілактичного обслуговування

Існує ряд стандартних методик профілактичного обслуговування, які слід періодично виконувати для забезпечення належної роботи мереж. Як правило, при збої одного комп'ютера в організації страждає тільки користувач цього комп'ютера. Однак збій мережі торкається значно більшого числа користувачів.

Профілактичне обслуговування мережі так само важливо, як і обслуговування комп'ютерів, підключених до цієї мережі. Необхідно регулярно перевіряти стан кабелів, мережних пристроїв, серверів і комп'ютерів, підтримувати їхню чистоту й гарний стан. Однієї з основних проблем з мережними пристроями, особливо в серверному приміщенні, є висока температура. Перегрів приводить до зниження продуктивності мережних пристроїв. Скупчення пилу усередині й на поверхні мережевих пристроїв перешкоджає циркуляції охолоджувального повітряного потоку, а в деяких випадках приводить до засмічування вентиляторів. Важливо підтримувати чистоту серверних приміщень і вчасно заміняти повітряні фільтри. Також корисно завжди мати під рукою змінні фільтри на випадок термінової заміни. Необхідно розробити графік проведення планових профілактичних робіт і очищення обладнання через регулярні проміжки часу. Програма технічного обслуговування допомагає запобігти простоям мережі й збоям обладнання.

Програма регулярного планового профілактичного обслуговування обов'язково повинна містити в собі огляд усіх кабелів. Переконайтеся, що кабелі правильно позначені й мітки не відклеїлися. Заміни поміток або маркування, що завжди додержуйтеся інструкцій компанії по маркуванню кабелів. Переконайтеся, що опори кабелів установлені належним чином, а точки контакту міцно закріплені. Кабелі піддаються ушкодженням і зношування. Для забезпечення належної роботи мережі необхідно стежити за справним станом кабелів. При необхідності зверніться до схеми з'єднань.

Перевірте кабелі, підключені до робочих станцій і принтерам. Користувачі часто зрушують кабелі, розташовані під столами, або наступають на них. Це може привести до зниження пропускної спроможності або втраті зв'язку.

Будучи фахівцем служби підтримки, ви можете помітити, що обладнання збоїть, ушкоджене або видає незвичайні звуки. Повідомите мережевого адміністратора про такі проблеми щоб уникнути небажаних простоїв мережі. Слід також проводити навчальні семінари для користувачів мережі. Покажіть їм, як правильно підключати й відключати кабелі і як переміщати їх якщо буде потреба.

7.5.1 Визначення проблеми

Неполадки мереж бувають простими й складними. Вони можуть виникати через проблеми з обладнанням, програмним забезпеченням і підключеннями. Комп'ютерні техніки повинні вміти проаналізувати неполадку й визначити причину помилки, щоб виправити її. Цей процес називається пошуком і усуненням неполадок.

Для оцінки неполадки необхідно визначити кількість комп'ютерів у мережі, на яких вона виникла. Якщо проблема тільки з одним комп'ютером у мережі, почніть процес пошуку й усунення неполадок на цьому комп'ютері. Якщо проблема торкнулася всіх комп'ютерів у мережі, почніть процес пошуку й усунення неполадок у серверному приміщенні, де підключені всі комп'ютери. У якості інженера ви повинні розробити логічний і послідовний метод діагностики мережевих неполадок, усуваючи кожну з них по черзі.

Додержуйтеся етапів, описаним у цьому розділі, щоб точно визначити, усунути й задокументувати неполадку. Першим етапом процедури пошуку й усунення неполадок є визначення проблеми. У табл 7.8 зображений перелік «відкритих» і «закритих» питань, які слід задати замовникові.

Таблиця 7.8 – Перелік «відкритих» і «закритих» питань, які слід задати замовникові

Крок 1. Визначення проблеми	
«Відкриті» питання	• Які неполадки виникли з вашим комп'ютером або мережевим пристроєм? • Яке програмне забезпечення ви недавно встановили на свій комп'ютер? • Що ви робили, коли виявилася неполадка? • Яке повідомлення про помилку ви одержали? • Який тип мережевих підключень використовується на цьому комп'ютері?
«Закриті» питання	• Чи використовував ваш комп'ютер недавно хтось ще? • Чи видите ви якісь-небудь загальні файли або папки • Чи міняли ви свій пароль останнім часом? • Чи можете ви вийти в Інтернет • Ви зараз у мережі? • Є хто-небудь ще з такою ж проблемою?

7.5.2. Формування припущень про можливу причину

Після розмови із замовником можна сформувати припущення про можливі причини неполадок. У табл 7.9. представлений перелік деяких розповсюджених можливих причин неполадок мереж.

Таблиця 7.9 – Перелік деяких розповсюджених можливих причин неполадок мереж

Крок 2. Формування припущень про можливу причину неполадки	
Розповсюджені причини неполадок у мережах	• Ненадійні кабельні з'єднання • Неправильно встановлена мережна плата • Відключений постачальник послуг Інтернету • Недостатньо сильний безпроводовий сигнал • Недійсний IP-адреса • Проблема з DNS-Сервером • Проблема з DCHP-Сервером • Проблема з мережевим обладнанням (комутатором, маршрутизатором і т д).

7.5.3 Перевірка припущень із метою визначення причини

Сформувавши кілька припущень про те, що викликало неполадку, перевірте їх, щоб визначити дійсну причину. В табл 7.10 представлений перелік швидких процедур, що дозволяє визначити точну причину неполадки або навіть усунути її. Якщо за допомогою швидкої процедури вдається усунути неполадку, після усунення можна провести повну перевірку функціонального стану системи. Якщо за допомогою швидкої процедури не вдається усунути неполадку, слід продовжити пошук точної причини.

Таблиця 7.10 – Перелік швидких процедур для визначення точної причини неполадки або та її усунення

Крок 3. Перевірка припущень для визначення причини неполадки	
Стандартні дії для визначення причини	• Переконаєтеся, що всі кабелі підключені туди, куди випливає. • Відключите й знову підключите кабелі й роз'єми. • Перезавантажите комп'ютер або мережевий пристрій. • Увійдіть у систему з обліковими даними іншого користувача. • Відновите або заново включите мережеве підключення. • Зв'яжіться з адміністратором мережі. Перевірте зв'язок зі шлюзом за замовчуванням. • Зайдіть на віддалену веб-сторінку, наприклад на http://www.cisco.com.

7.5.4 Розробка плану дій по усуненню неполадки і його виконання

Установивши точну причину неполадки, розробіть план дій для її усунення й виконаєте його. В табл 7.11 представлений ряд джерел. Їх можна використовувати для збору додаткової інформації, яка допоможе усунути неполадку.

Таблиця 7.11 – Ряд джерел для розробки плану дій по усуненню неполадки

Крок 4. Розробка плану дій по усуненню неполадки й реалізація вирішення	
Якщо на попередньому етапі проблема не була усунута, то для її вирішення необхідний подальший аналіз ситуації.	• Журнали обліку ремонтних робіт служби підтримки • Інші технічні фахівці • Веб-сайти виробників: розділ питань, що часто задаються • Технічні веб-сайти • Новинні групи • Керівництва до комп'ютера • Керівництва до пристроїв • Форуми в Інтернеті • Пошук в Інтернеті

7.5.5 Повна перевірка функціонального стану системи й вживання профілактичних заходів

Після усунення неполадки виконаєте повну перевірку функціонального стану системи й при необхідності впроваджуйте профілактичні заходи. В табл 7.12 представлений перелік дій для перевірки рішення.

Таблиця 7.12 – Перелік дій для перевірки рішення

Етап 5. Повна перевірка функціонального стану системи й вживання профілактичних заходів якщо буде потреба	
Перевірка всіх функцій системи	• За допомогою команди ipconfig /all відобразите відомості про IP-Адресах усіх мережевих адаптерів. • За допомогою команди Ping перевірте мережеве з'єднання. На зазначену адресу буде відправлений пакет, і відобразиться відповідна інформація. • За допомогою команди Nslookup запросите сервер доменних імен в Інтернеті. Відобразиться перелік вузлів у домені або інформація про один вузол. • За допомогою команди Tracert визначите маршрут, по якому пакети передаються по мережі. Так ви зможете визначити, на яких ділянках виникають труднощі при обміні інформацією між вашим комп'ютером і комп'ютером іншого користувача. • За допомогою команди Net View виведіть перелік комп'ютерів у робочій групі. Відобразяться доступні загальні ресурси в мережі.

7.5.6 Документування отриманих даних, вжитих заходів і результатів

На останньому етапі процедури пошуку й усунення неполадок виконується документування отриманих даних, виконаних дій і результатів. В табл 7.13 представлений перелік завдань, які слід виконати, щоб задокументувати неполадку й спосіб її усунення.

Таблиця 7.13 – Перелік завдань для документування неполадки й способи її усунення

Етап 6. Документування отриманих даних, вжитих заходів і результатів	
Документування отриманих даних, вжитих заходів і результатів	• Обговорите застосований розв'язок із замовником. • Попросите клієнта переконатися, що неполадка усунута. • Надайте замовникові всі документи. • Задокументуйте дії, початі для усунення неполадки, у робочому завданні й журналі інженера. • Задокументуйте компоненти, використані при ремонті. • Задокументуйте час, витрачене на усунення неполадки.

7.5.7 Визначення розповсюджених неполадок і способи їх усунення

Мережеві неполадки можуть бути пов'язані з устаткуванням, програмним забезпеченням або настроюваннями, або комбінацією цих трьох факторів. Деякі типи мережевих неполадок доводиться усувати частіше, чим інші. В табл 7.14 наведена діаграма розповсюджених мережевих неполадок і способів їх усунення.

Таблиця 7.14 – Розповсюджені неполадки й способи їх усунення.

Визначення проблеми	**Можливі причини**	**Можливі розв'язки**
Світлодіодні індикатори мережної плати не горять.	• Мережевий кабель не підключений або ушкоджений.	• Повторно підключите або замініте мережний кабель.
Користувачеві не вдається підключитися до вилученому пристрою по протоколу SSH.	• Мережна плата ушкоджена. • Вилучений пристрій не настроєне на доступ по протоколу SSH. • Доступ по протоколу SSH з боку користувача або певної мережі не дозволений.	• Замініте мережеву плату. • Настрійте вилучений пристрій на доступ по протоколу SSH. • Дозволите доступ по протоколу SSH з боку користувача або певної мережі.
Ноутбук не може знайти безпроводовий маршрутизатор.	• Безпроводовий маршрутизатор/точка доступу настроєні на використання іншого протоколу групи 802.11. • Не виконується широкомовне розсилання SSID.	• Настрійте безпроводової маршрутизатор, використовуючи підтримуваний ноутбуком протокол. • Настрійте безпроводовий маршрутизатор на широкомовне розсилання SSID.

Визначення проблеми	Можливі причини	Можливі розв'язки
	• Безпроводова мережева плата ноутбука відключена.	• Включите безпроводову мережеву плату ноутбука.
Комп'ютеру призначений IP-Адреса 169.254.X.X.	• Мережевий кабель відключений. • Маршрутизатор виключений або неправильне підключений до мережі. • Мережева плата ушкоджена.	• Повторно підключите мережний кабель. • Переконаєтеся, що живлення маршрутизатора включене й що він належним чином підключений до мережі. • Скиньте й обновите IP-Адресу комп'ютера. • Замініте мережеву плату.
Вилучений пристрій не відповідає на луну-запит.	• Брандмауер Windows по умовчанню не пропускає ping. • Вилучений пристрій настроєний так, щоб не відповідати на луни-запити.	• Дозволите на міжмережевому екрані протокол для перевірки зв'язку. • Настрійте вилучений пристрій, щоб воно відповідало на луни-запити.
Користувач може ввійти в локальну мережу, але не має доступу до Інтернету.	• Адреса шлюзу не задана або невірний. • Проблема з інтернет– провайдером.	• Переконаєтеся, що мережній платі призначена вірна адреса шлюзу. • Подзвоните постачальникові послуг Інтернету й повідомите про проблему зі зв'язком.
Мережа працює, але безпроводовий пристрій не може підключитися до мережі.	• Підтримка безпроводового зв'язки на пристрої відключена. • Пристрій перебуває поза зоною охвату безпроводової мережі. • Перешкоди від інших безпроводових пристроїв, працюючих у тому ж частотному діапазоні.	• Включите підтримку безпроводового зв'язку на пристрої. • Перемістите ноутбук ближче до безпроводового маршрутизатору/точки доступу. • Перемкнете безпроводової маршрутизатор на інший канал.
Комп'ютер з Windows, тільки що підключений до мережі з комп'ютерами, що працюють тільки під керуванням Windows, не бачить загальні ресурси.	• Невірне ім'я робочої групи. • Невірне мережеве розташування. • Відключені функції Network Discovery (Виявлення мережі) і File Sharing (Загальний доступ до файлів).	• Скорегуйте ім'я робочої групи. • Зміните мережеве розташування на правильне. • Включите функції Network Discovery (Виявлення мережі) і File Sharing (Загальний доступ до файлів).
Користувачеві не вдається підключити мережевий диск.	• У користувача немає відповідних дозволів. • Невірна робоча група. • Відключені функції Network Discovery (Виявлення мережі)	• Задайте відповідні дозволу для даного користувача. • Зміните ім'я робочої групи. • Включите функції Network

Визначення проблеми	Можливі причини	Можливі розв'язки
	і File Sharing (Загальний доступ до файлів).	Discovery (Виявлення мережі) і File Sharing (Загальний доступ до файлів).

Огляд Розділу 7. Прикладна мережева взаємодія

Цій розділ ознайомив вас зі способами підключення комп'ютерів до мережі, а також більшою кількістю служб, які доступні по мережі. У ньому розглянуті різні аспекти пошуку й усунення неполадок мережі, а також приклади аналізу й застосування простих рішень.

Список використаних джерел

1. Зінченко О.В., Іщеряков С.М., Проколов С.В., Сєрих С.О., Василенко В.В. Хмарні технології. – Навчальний посібник. – К: ФОП Гуляєва В.М., 2020. – 74с.
2. Хмарні та Грід-технології: конспект лекцій [Електронний ресурс] : навч. посіб. для студ. спеціальності 121 «Інженерія програмного забезпечення» (освітня програма «Програмне забезпечення комп’ютерних та інформаційно-пошукових систем»)/ В.Я. Юрчишин; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 5,93 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2019. – 264 с.
3. Войтович Н.В., Найдьонова А.В. Використання хмарних технологій Google та сервісів web 2.0 в освітньому процесі. Методичні рекомендації. – Дніпро: ДПТНЗ «Дніпровський центр ПТОТС», 2017 – 113 с.
4. Гніденко М.П., Гайдур Г.І., Сєрих С.О. Перспективні компоненти та засоби інфокомунікаційних технологій. – Навчальний посібник. – Київ: ДУТ, 2017. – 168 с.
5. О.Л. Недашківський Технології та протоколи Інфокомунікаційних мереж (частина перша) ДУТ К. – 2017. 67 с.
6. О.Л. Недашківський Технології та протоколи Інфокомунікаційних мереж (частина друга) ДУТ К. – 2018. 77 с.
7. Воробієнко П.П., Каразей В.М., Скопа 0.0. Протоколи міжмережної взаємодії. – Одеса, УДАЗ ім. О С. Попова, 1999. – 50 с.
8. Воробиенко П.П., Нечипорук О.Л., Струкало М.И. Принципы организации сетей с коммутацией пакетов: Учебное пособие. – Изд. 2-е пер. - Одесса: ОНАС им. А.С. Попова, 2001. – 100 с.; пл.
9. Е.В. Добровольский, А.Ю. Бессчётнов, А.А. Легунов, Д.С. Гуринович Принципы конфигурирования маршрутизаторов Cisco в сетях TCP/IP и Frame Relay: Методическое руководство к лабораторным работам № 1-6 / Под редакцией О.Л Нечипорука, М.И. Струкало. – Одесса: ОНАС им. А.С. Попова, 2001. – 63с.

10. Курс lT Essentials Мережевої академії Cisco [Електронний ресурс]. Режим доступу: https://www.netacad.com/ru/courses/os-it/it-essentials.
11. Введение в программу CiscoPacketTracer [Электронный ресурс]. Режим доступа: https://www.intuit.ru/studies/courses/3549/791/lecture/29211.

Питання та завдання для самостійного контролю знань

Контрольні питання:

1. Контрольний список монтажу мережі.
2. Перше підключення до маршрутизатора.
3. Домен і робоча група.
4. Спільне використання ресурсів у системі Windows.
5. Коротка історія технологій підключення. DSL і ADSL.
6. Центр обробки даних.
7. Служби DHCP. Служби DNS.
8. Веб-служби.
9. Процедури профілактичного обслуговування мереж.

Питання для тест-контролю

1. Компанії ABC потрібне профілактичне обслуговування всіх кабелів локальної мережі раз у рік. Яке завдання повинна входити в програму профілактичного обслуговування?

Заміна всіх кабель– каналів, щоб гарантувати надійність кріплення

Обстеження всіх сполучних кабелів на предмет обривів

Відключення й повторне підключення всіх сполучних кабелів

Перемаркування всіх кабелів

2. Який сервіс хмарних обчислень оптимальний для організації, яка не має технічні знання для розміщення й обслуговування додатків на своєму локальному вузлі?

IT-ресурси як послуга (IT as a Service, Itaas)

Платформа як послуга (Platform as a Service. Paas)

ПО як послуга (Software as a Service. Saas)

Інфраструктура як послуга (Infrastructure as a Service. laas)

3. Користувач може друкувати за допомогою принтера підключеного до тієї ж мережі, однак трафік користувача не досягає Інтернету. Укажіть можливу причину проблеми.

Комп'ютер має невірний IP-адреса.

До комп'ютера підключений несправний мережевий кабель

Адреса шлюзу за замовчуванням на комп'ютері не указаний або зазначений невірно

Мережева плата комп'ютера несправна

4. У чому полягає перевага регулярного проведення профілактичного обслуговування?

Скорочення можливостей підключення

Зменшення електромагнітних і радіочастотних перешкод

Скорочення часу простою мережі

Скорочення кількості погроз безпеки

5. Технічний фахівець вибирає для безпроводового маршрутизатора канал — 1.6 або 11. Яка мета вибору каналу?

Використання різних стандартів IEEE 802.11.

Виключення перешкод від працюючих поблизу безпроводових обладнань

Використання більш стійких алгоритмів захисту.

Відключення віщання ідентифікатора мережі (SSID).

6. Який тип підключення до Інтернету забезпечує максимальну швидкість передачі даних?

Супутниковий канал зв'язку

Оптоволокно

ISDN

Телефонна мережа загального користування

Кабельне підключення

7. Яке призначення мережевих профілів, які використовуються для створення нового мережевого підключення на ПК із ОС Windows?

Настроювання параметрів мережевого адаптера на найшвидшу доступну мережу

Усунення потреби в IP-адресах при підключенні до мережі

Надання списку доступних постачальників послуг доступу в Інтернет

Реалізація простого способу настроювання й застосування мережних функцій залежно від типу мережі, до якої здійснюється підключення.

8. Користувач помічає, що швидкість передачі даних через гігабітний мережний адаптер у його комп'ютері набагато нижче очікуваної. Яка можлива причина цієї проблеми?

З якихось причин на мережевому адаптері був настроєний напівдуплексний режим

Неправильно настроєна функція пробудження по локальній мережі в мережевому адаптері

Мережевий адаптер настроєний на одночасне використання IPv4 і IPv6.

Режим гібернації викликає непередбачене відключення мережевого адаптера.

РОЗДІЛ 8. ІНФОРМАЦІЙНА БЕЗПЕКА ВІДОМЧОЇ ЦИФРОВОЇ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ ДСНС УКРАЇНИ

У цьому розділі розглядаються типи атак, що загрожують безпеки комп'ютерів і даних, які на них зберігаються. Інженер відповідає за забезпечення безпеки даних і комп'ютерного обладнання в організації. Із цієї глави ви пізнаєте, як організувати найкращий захист інформації замовника.

Для успішного захисту комп'ютерів і мережі інженер повинен бути знаком з обома типами погроз комп'ютерної безпеки:

- **Фізичні** – події або атаки, спрямовані на викрадення, ушкодження або знищення обладнання, такого як сервери, комутатори й кабелі
- **Інформаційні** – події або атаки, спрямовані на видалення, ушкодження, заборону доступу авторизованим користувачам, надання доступу несанкціонованим користувачам або розкрадання інформації

8.1 Шкідливе ПЗ

Комп'ютери, що й зберігаються на них дані необхідно захистити від шкідливого програмного забезпечення (ПЗ) [9-13]:

- **Шкідливе ПЗ** – це програмне забезпечення, створене для виконання шкідливих дій. На жаргоні його ще називають "малварь" – від англійського malware (**mal** icious soft **ware**, тобто "шкідливе ПЗ").
- Як правило, такі програми встановлюються на комп'ютер без ведена користувача. Ці програми відкривають додаткові вікна на комп'ютері або міняють його настроювання.
- Шкідливе ПЗ може змінювати настройки веб-браузера для відкриття певних веб-сторінок, які не потрібні користувачу. Це називається перенапрямком браузера.
- Вони також можуть збирати відомості, що зберігаються на комп'ютері, без відому користувача.

1. Першим і найпоширенішим типом шкідливого ПЗ є комп'ютерні *віруси*. Вірус передається на інші комп'ютери по електронній пошті, на USB-накопичувачах, через обмін файлами й миттєвими повідомленнями. Вірус ховається шляхом прикріплення себе до комп'ютерного коду, програмного забезпечення або документів на комп'ютері. При доступі до файлу вірус виконується й заражає комп'ютер. Приклади того, які дії може виконувати вірус, наведені в табл. 8.1.
2. Іншим типом шкідливого ПЗ є *«троянські коні»*, або просто трояни. «Троянський кінь», або троян, звичайно замаскований під корисну програму, яка, однак, містить шкідливий код. Наприклад, трояни найчастіше можна знайти в безкоштовних онлайн-іграх. Користувачі завантажують такі ігри на комп'ютери. У такий спосіб трояни попадають на

комп'ютер. Під час гри троян установлюється в систему й продовжує працювати навіть після закриття гри. У табл. 8.2 перелічені деякі типи троянів.

Таблиця 8.1 – Віруси можуть...

Змінити, ушкодити, видалити файли й навіть стерти всі дані на жорсткому диску комп'ютера.
Блокувати завантаження комп'ютера, перешкоджати завантаженню додатків або їх правильній роботі.
Використовувати обліковий запис електронної пошти користувача для розсилання вірусу на інші комп'ютери.
Не діяти, поки їх не активує хакер.
Фіксувати натискання клавіш для захоплення конфіденційної інформації, такий як паролі й номера кредитних карт, а потім відправляти зібрані дані хакеру.

Таблиця 8.2 – Типи «троянських коней»

Види дій троянців	**Опис**
Дистанційний доступ	Троян уможливлює несанкціонований дистанційний доступ.
Відправлення даних	Троян дозволяє хакеру одержати доступ до конфіденційних даних, таким як паролі.
Руйнування даних	Троян ушкоджує файли або видаляє їх.
Проксі-сервер	Троян використовує комп'ютер жертви як джерело для нових атак і протиправних дій.
FTP	Троян уможливлює несанкціонований обмін файлами на кінцевих пристроях.
Вивід з ладу захисного ПЗ	Троян припиняє роботу антивірусних програм або брандмауерів.
Відмова в обслуговуванні (DoS-атака)	Троян сповільнює обмін даними по мережі або повністю блокує його.

Шкідливе ПЗ постійно удосконалюється. У табл. 8.3 наведені описи інших типів шкідливого ПЗ.

Таблиця 8.3 – Види шкідливого ПЗ

Режими безпеки	**Опис**
Хробаки	• Хробак – програма, що самовідтворюється, завдає шкоди мережам з метою уповільнити операції по мережі або блокувати • Звичайно хробаки поширюються автоматично, використовуючи відомі уразливості в легальному програмному забезпеченні.
Рекламне ПЗ	• Звичайно поширюється шляхом завантаження програмного забезпечення онлайн. • Такі програми відображають рекламу в спливаючому вікні. • Часто спливаючі вікна рекламного ПЗ важко контролювати, і нові вікна відкриваються швидше, чим користувач може їх закрити.

Режими безпеки	Опис
Шпигунське ПЗ	• Аналогічно рекламному ПЗ, але призначене для збору інформації про користувача й відправлення отриманих відомостей іншій стороні без відому користувача. • Шпигунське ПЗ може являти собою незначну загрозу, збираючи тільки дані про відкриті веб-сторінки, або досить серйозну небезпеку, якщо його метою є збір особистої або фінансової інформації.
Програми-здирники	• Такі програми схожі на рекламне ПЗ, однак служать для блокування доступу до зараженої системи. • Найчастіше в таких програмах відображається повідомлення із пропозицією заплатити зловмисникам, щоб зняти блокування.
Руткіти	• Програми, використовувані хакерами для одержання прав адміністратора комп'ютера. • Такі програми досить складно виявити, оскільки вони можуть управляти захисними програмами, щоб сховати своє існування. • Деякі руткіти вдається вилучити за допомогою спеціального ПЗ, але іноді для повного видалення потрібна переустановка операційної системи.

Щоб виявити, знешкодити й видалити шкідливе ПЗ, перш ніж воно встигне заразити комп'ютер, завжди використовуйте антивірусне ПЗ, вирішення для виявлення шпигунських програм і інструменти для видалення рекламного ПЗ табл. 8.4.

Таблиця 8.4 – Визначення типів шкідливого ПЗ

Тип шкідливого ПЗ	Опис шкідливого ПЗ
Рекламне ПЗ	Звичайно поширюється шляхом завантаження програмного забезпечення онлайн і найчастіше відображають спливаюче вікно, яке важко закрити.
Шпигунське ПЗ	Призначене для збору інформації про користувача й відправлення отриманих відомостей іншій стороні без ведена користувача.
Руткіт	Програми, використовувані хакерами для одержання прав адміністратора комп'ютера. Їх досить складно виявити.
Програми–здирники	Блокує доступ до зараженої системи й вимагає викуп за зняття блокування.
Хробак	Програма , що самовідтворюється, котра повільно розповсюджується. Сповільнює роботу мережі або блокує її.

Важливо знати, що бази даних таких програм швидко застарівають. Тому в обов'язок інженера входить установка актуальних оновлень, виправлень і визначень вірусів у рамках регулярного обслуговування. У багатьох організаціях використовується письмово зафіксована політика безпеки, що забороняє співробітникам установлювати програмне забезпечення, не надане компанією.

8.1.1 Фішинг

Фішинг (phishing)– це вид шахрайства, коли зловмисник відправляє повідомлення електронної пошти, телефонує або публікує текст із метою шляхом обману одержати від користувача його особисту або фінансову інформацію. Фішингові атаки також використовуються для того, щоб користувач сам того не знаючи встановив шкідливе ПЗ на свої пристрої рис. 8.1.

Наприклад, користувач може одержати електронне повідомлення, яке може виглядати як відправлене справжньої сторонньою організацією, такий як банк. Хакер може звернутися із проханням уточнити певні реквізити, наприклад, паролі, імена користувачів або PIN-код, нібито заради запобігання вкрай небажаних наслідків. Якщо користувач надав таку інформацію, фішингова атака вважається успішною.

Існує також вибірковий або прицільний фішинг (spear phishing). У цьому випадку фішингова атака націлена на визначеного людину або організацію.

Організаціям слід проводити для своїх співробітників навчальні заходи, на яких розглядаються питання захисту від фішингових атак. Як правило, конфіденційна особиста або фінансова інформація не запитується в інтерактивній формі. Справжні організації не запитують конфіденційну інформацію з електронної пошти. Будьте пильні. При виникненні сумнівів зв'яжіться з організацією поштою або телефону, щоб переконатися в дійсності запиту.



Рис. 8.1 – Фішинг облікових даних

8.1.2 Спам

Спам, також називаний небажаною або сміттєвою поштою, – це несанкціоновані повідомлення електронної пошти. У більшості випадків спам є одним з варіантів реклами. Однак у спамі можуть міститися небезпечні посилання, шкідливе ПЗ або облудний контент. Ціль такого спама – одержати конфіденційну інформацію, таку як номер соціального страхування або відомості про банківський рахунок. Більшість спама відправляється безліччю підключених до мережі комп'ютерів, заражених вірусом або хробаком. Ці заражені комп'ютери відправляють максимально можливе число повідомлень електронної пошти.

Зупинити спам неможливо, однак існують способи знизити його потік. Наприклад, більшість інтернет-провайдерів блокують спам до того, як він потрапить у поштову скриньку користувача. Багато антивірусних програм і поштові клієнти мають функцію автоматичної фільтрації пошти, як показано на рис. 8.2. Це означають, що вони виявляють і видаляють спам з папки вхідних листів.



Рис. 8.2 – Спам

8.1.3 Атаки TCP/IP

Для управління взаємодії з Інтернетом ваш комп'ютер використовує набір протоколів TCP/IP. На жаль, деякими функціями TCP/IP можна маніпулювати, що приводить до появи уразливості у мережі (рис. 8.3).

Як показано на рис. 8.3, протокол TCP/IP уразливий до наступних типів атак:

DoS (Denial of Service, відмова в обслуговуванні) (див. рис. 8.4) – тип атак, при яких створюється надмірно великий обсяг запитів до мережних серверів, таким як поштові сервери або сервер^-сервери-веб-

сервери. Такі атаки покликані повністю перевантажити сервер неправильними запитами, викликавши тим самим відмова в обслуговуванні справжніх користувачів.

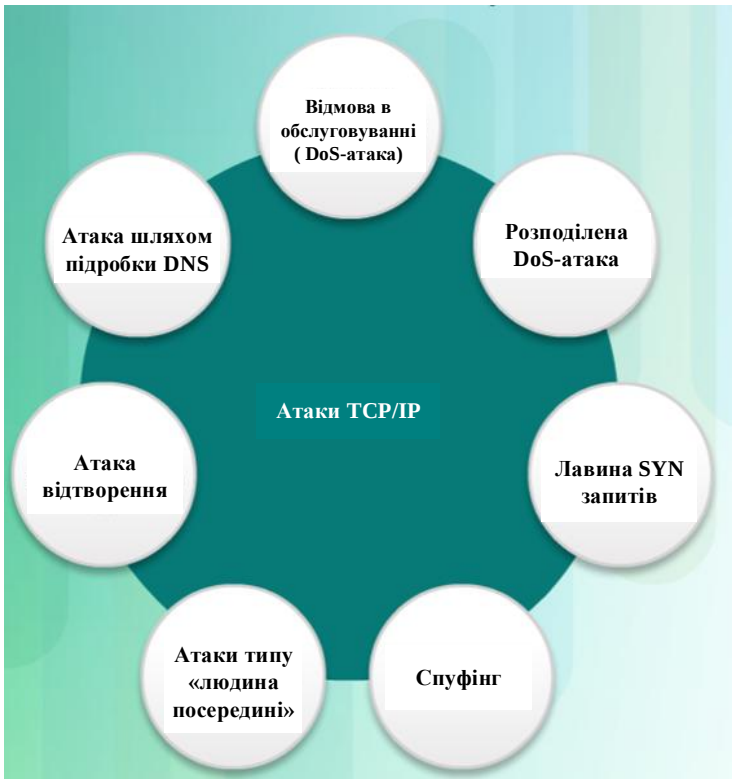


Рис. 8.3 – Типи атак TCP/IP

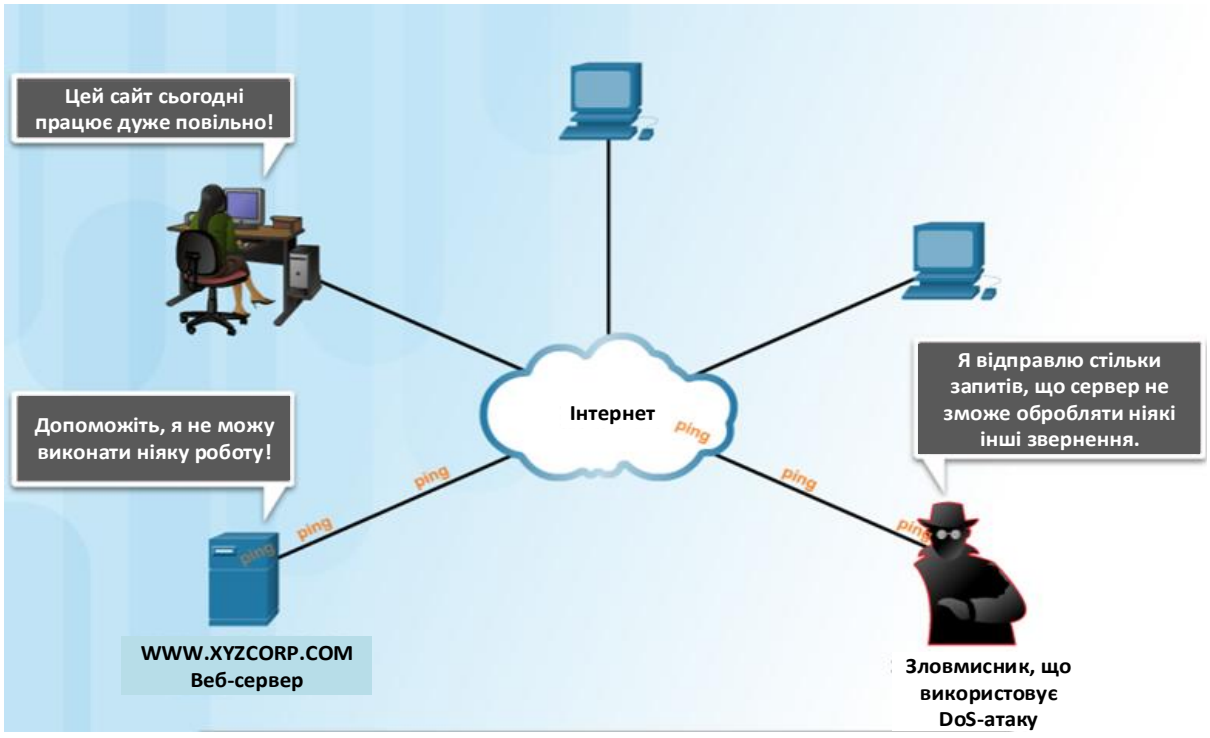
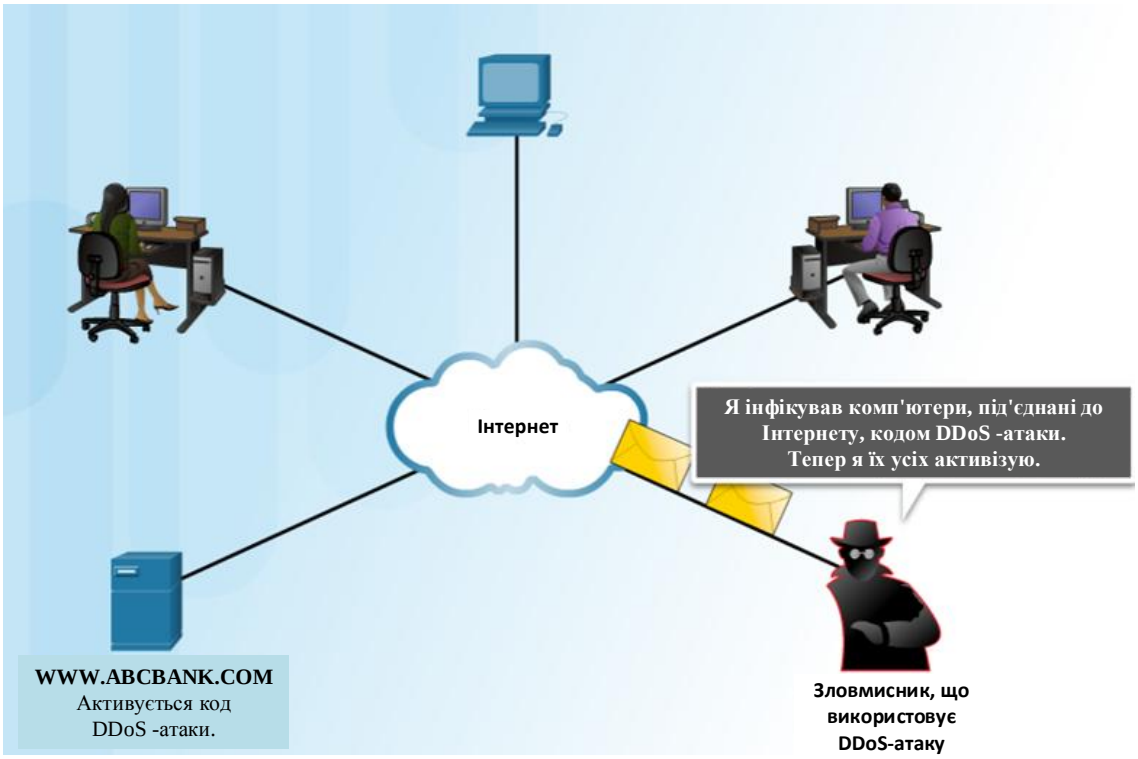
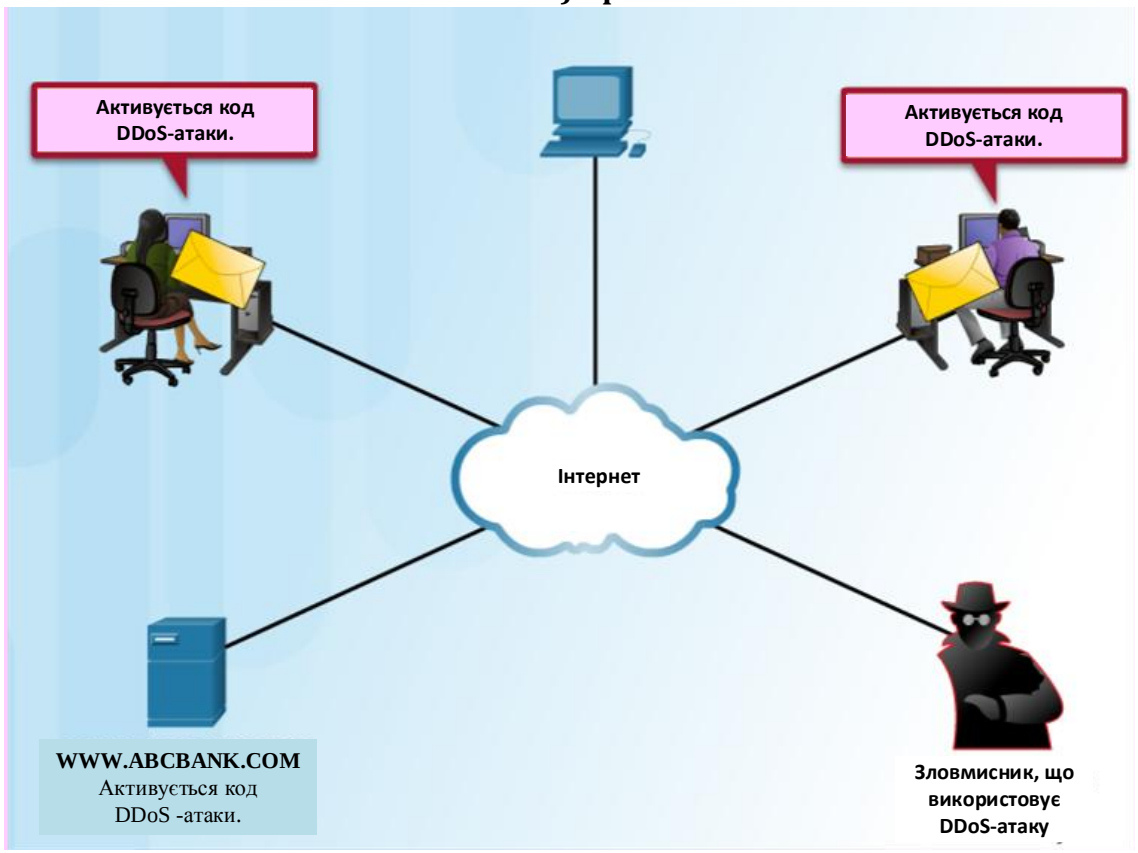


Рис. 8.4 – DoS-атака

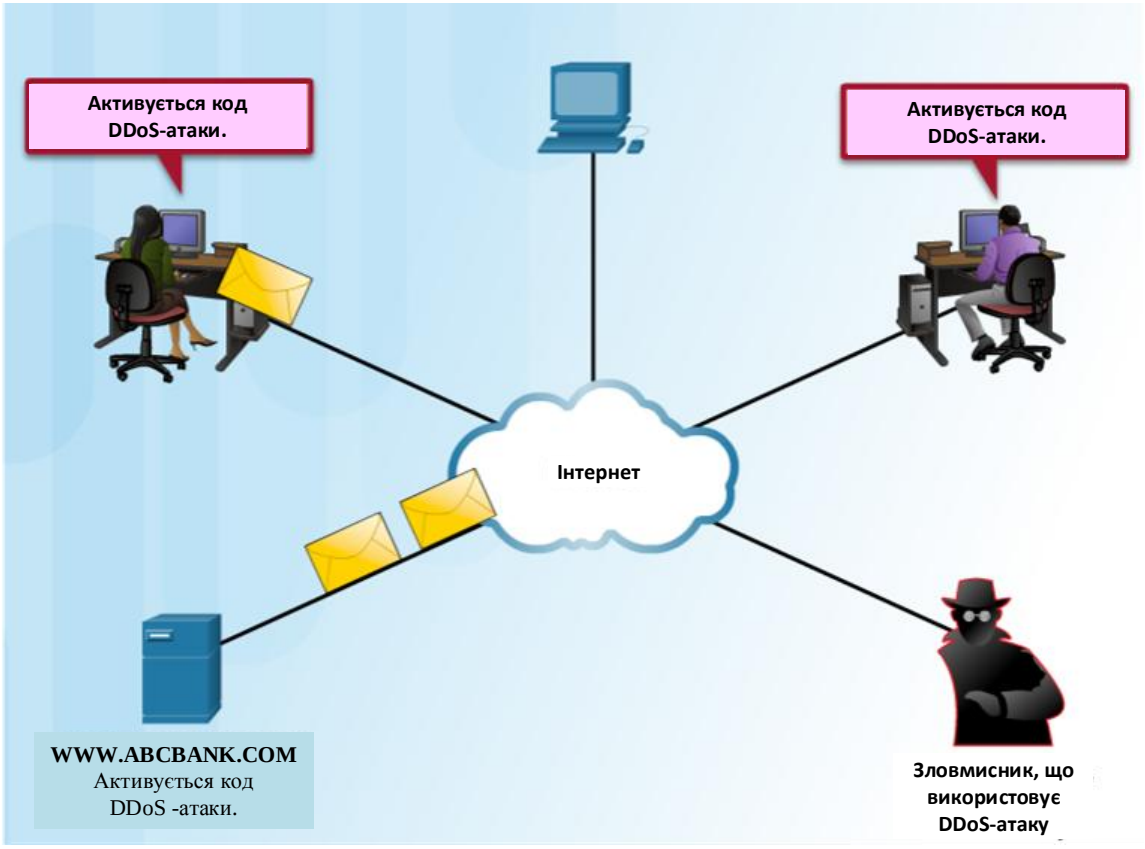
DDoS (Distributed DoS, Розподілена DoS-атака) (див. рис. 8.5) – атаки DDoS аналогічні атакам DoS, однак для проведення таких атак використовується набагато більше комп'ютерів. Іноді в таких атаках задіюються тисячі комп'ютерів.



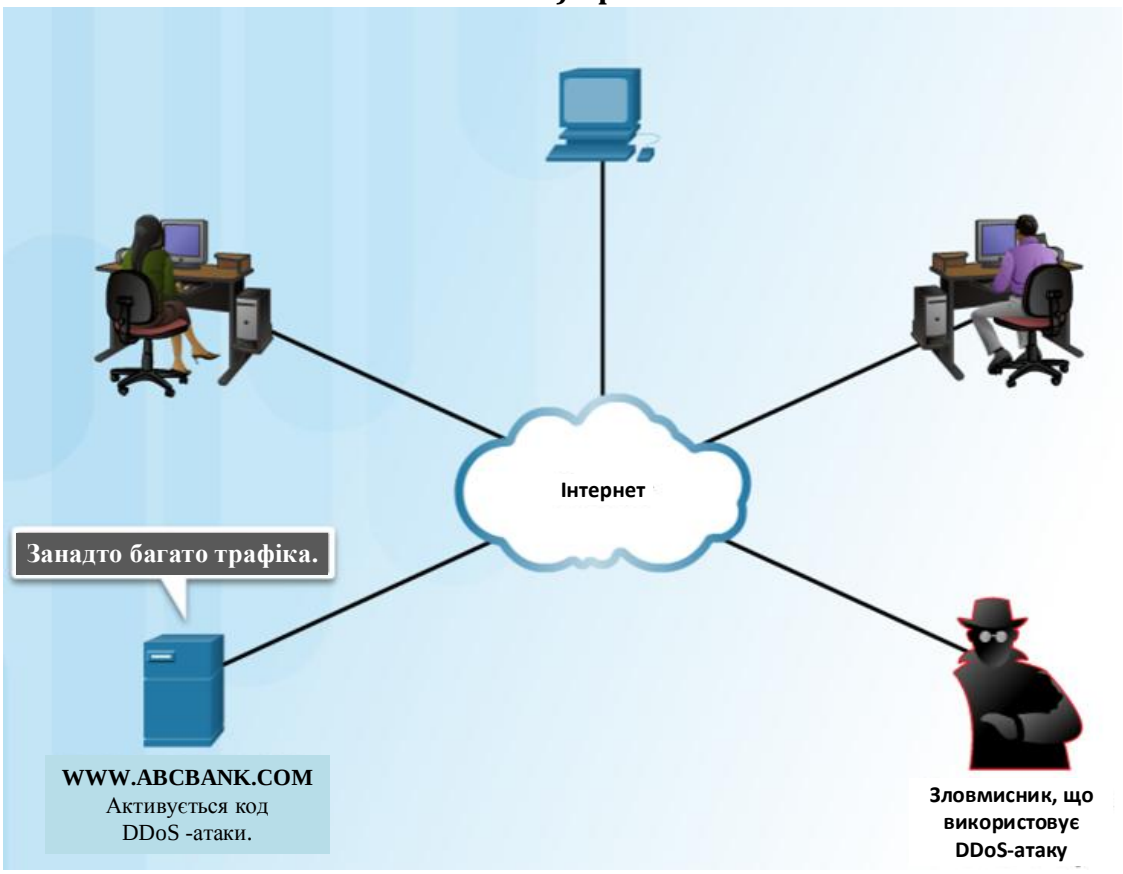
а) Крок 1



б) Крок 2



в) Крок 3



г) Крок 4

Рис. 8.5 – Розподілена атака DdoS

Спочатку комп'ютери заражаються шкідливим ПЗ для DDoS і стають «зомбі». Армія таких комп'ютерів-зомбі називається ботнетом (botnet). Після зараження комп'ютери працюють як звичайно, рівно доти, поки на них не буде відправлена команда почати атаку DDoS. Комп'ютери-Зомбі можуть перебувати в різних географічних місцях розташування, тому відстежити джерело атаки досить складно.

Лавина SYN запитів (SYN flood) (див. рис. 8.6) – запит SYN являє собою початкове повідомлення, що відправляється для встановлення підключення TCP. Лавинна атака SYN відкриває з'єднання з випадкових портів TCP на джерелі атаки й блокує мережеве обладнання або комп'ютер більшим числом неправильних запитів SYN. Це викликає відмови у встановленні сеансів для інших клієнтів. Атаки з використанням лавини SYN запитів ставляться до атак типу «відмова в обслуговуванні».

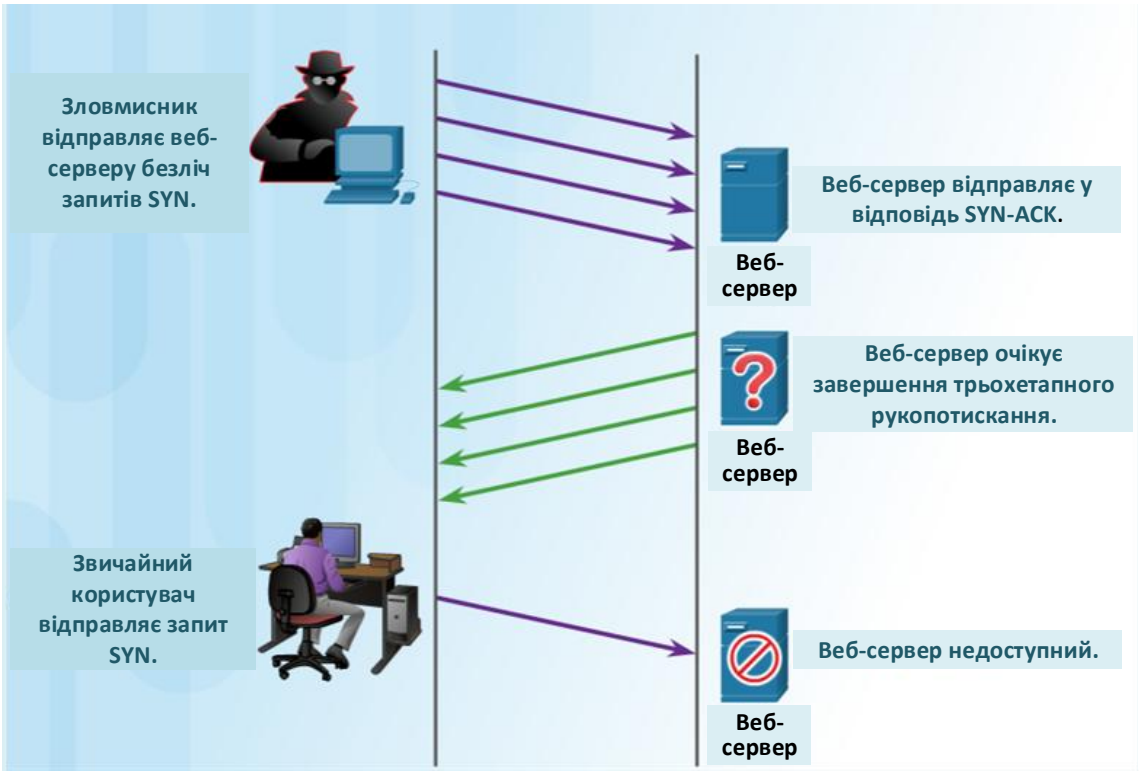


Рис. 8.6 – Приклад атаки з використанням лавини SYN запитів по протоколу TCP

Спуфінг (spoofing, підміна адрес) – при атаці за допомогою підміни адрес комп'ютер маскується під довірений комп'ютер для одержання доступу до ресурсів. Комп'ютер використовує підроблений IP або MAC-адреса з метою видати себе за комп'ютер, що є довіреним у мережі.

Атаки типу «людина посередині» (man-in-the-middle, також атака незаконного посередника) (див. рис. 8.7) – зловмисник здійснює атаку «людина посередині», перехоплюючи повідомлення між комп'ютерами для розкрадання інформації, переданої по мережі. Атака «людей посередині» також може використовуватися для маніпулювання повідо-

мленнями й передачі неправильної інформації між вузлами, оскільки вузлам невідомо про зміну повідомлень.

Наступні кроки атаки з «людиною посередині»:

- **Крок2** Комп'ютер зловмисника одержує запит і завантажує справжню сторінку зі справжнього веб-сайту.
- **Крок3** Зловмисник може змінити справжню веб-сторінку й застосувати перетворення даних.
- **Крок4** Зловмисник пересилає запитану сторінку жертві.

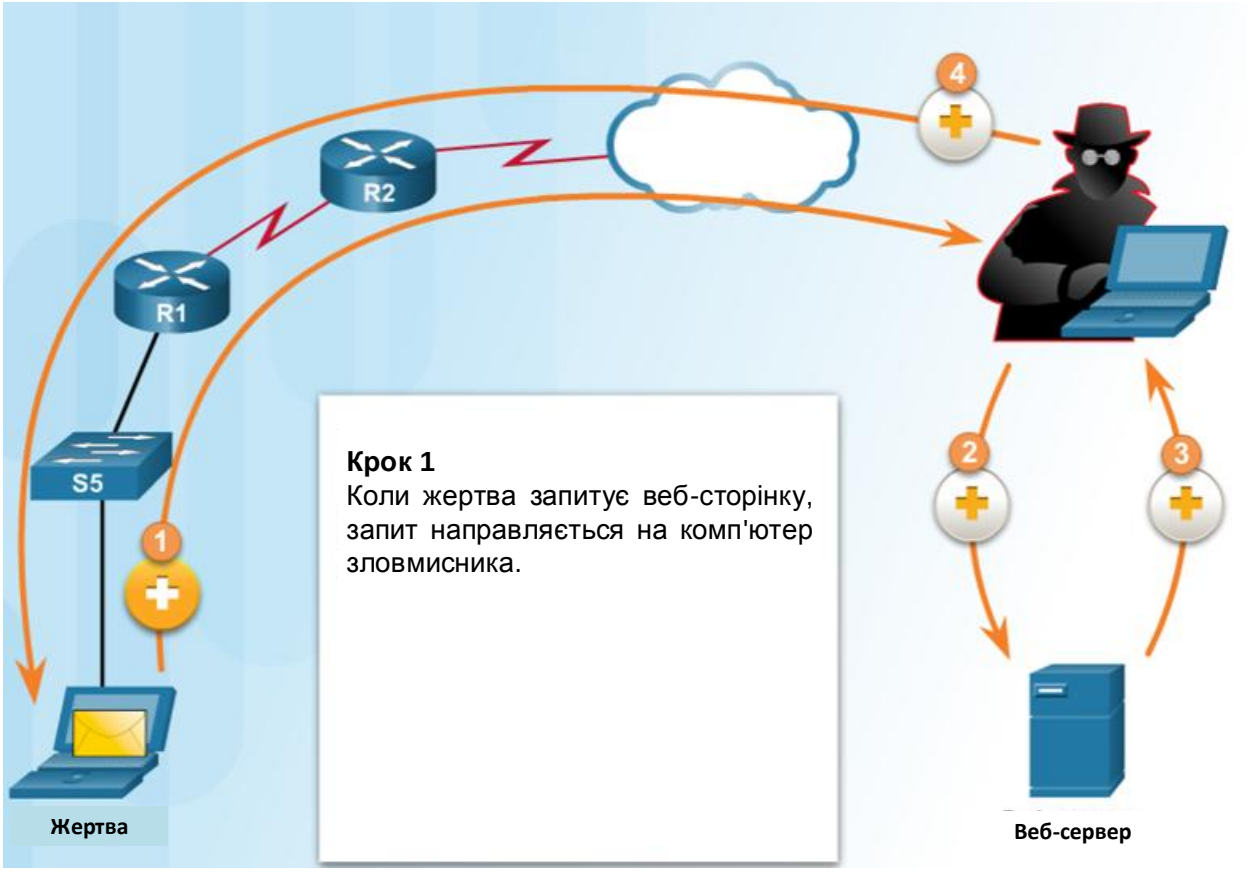


Рис. 8.7 – Приклад атаки з «людиною посередині»

Атака відтворення (replay) – для виконання атаки з відтворенням передача даних перехоплюється й записується зловмисником. Потім ці передачі передаються на комп'ютери призначення. Комп'ютер призначення обробляє ці передані дані як справжні й відправлені джерелом.

Атака шляхом підробки DNS (отруєння DNS, DNS Poisoning) – записи DNS у системі змінюються так, щоб вузол звертався на підроблені DNS-сервери. Користувач намагається відкрити справжній сайт, але трафік переадресується на підроблений веб-сайт. Підроблений веб-сайт використовується для виманювання конфіденційної інформації, такий як імена користувачів і паролі. Потім зловмисник може зібрати всі ці дані із сервера.

Визначення типів атак на TCP/IP презентовано в табл. 8.5

Таблиця 8.5 – Визначення типів атак на TCP/IP

Тип атаки TCP/IP	Опис атаки TCP/IP
Атаки типу «людина по середині»	Хакер перехоплює повідомлення між комп'ютерами з метою розкрадання інформації, переданої по мережі.
DoS (відмова в обслуговуванні)	Під час таких атак на мережевий сервер відправляється надмірно велика кількість запитів, тим самим перевантажуючи сервери.
Спуфінг	Комп'ютер використовує підроблений IP або MAC-адресу з метою видати себе за комп'ютер, що є довіреним у мережі, і одержати доступ до ресурсів.
Атака відтворення	Передача даних перехоплюється й записується зловмисником. Потім вони передаються на отримувач-комп'ютер-одержувач. Комп'ютер-одержувач уважає, що отримані дані справжні.
Лавина SYN запитів	Така атака відкриває велику кількість з'єднань із випадкових TCP-портів на джерело атаки шляхом відправлення великої кількості неправильних запитів SYN. Це викликає відмови у встановленні сеансів для інших клієнтів.

8.1.4 Атаки нульового дня

Атака нульового дня (zero-day), яку іноді називають погрозою невідомого типу, – це атака на комп'ютер з використанням уразливостей у програмному забезпеченні, про яких не знає розроблювач такого ПЗ або які він навмисно приховує рис. 8.8. Терміни «нульовий день» або «нульова годину» позначають момент виявлення експлойта. Протягом часу, коли розроблювач ПО створює виправлення й готовить його до випуску, мережа залишається уразливою до таких експлойтів, як показано на рис. 8.8. Для захисту від стрімких атак на мережу фахівцям з безпеки необхідно ретельно продумувати архітектуру мережі. У наш час неможливо перехопити спроби вторгнення в декількох певних місцях у мережі.

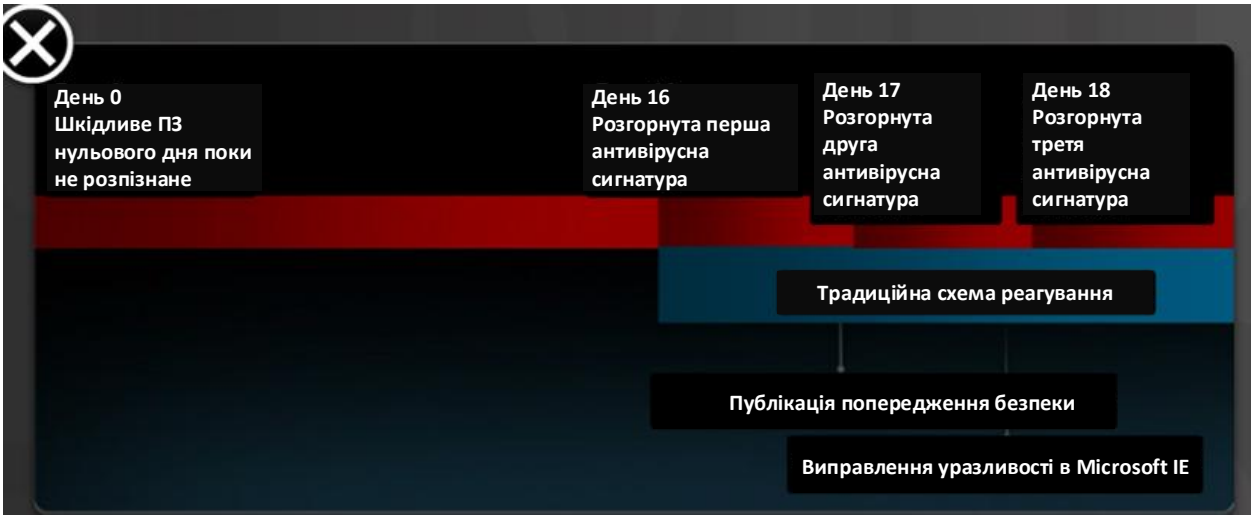


Рис. 8.8 – Уразливість нульового дня в браузері Microsoft Internet Explorer

8.1.5 Соціальна інженерія

Соціальна інженерія використовується в тих випадках, коли зловмисник намагається одержати доступ до обладнання або мережі, шляхом обману одержуючи від користувачів необхідну для доступу інформацію. Наприклад, як показано на рис. 8.9, часто зловмисник, що користується соціальною інженерією, завойовує довіра співробітника й переконує його повідомити ім'я користувача й пароль.

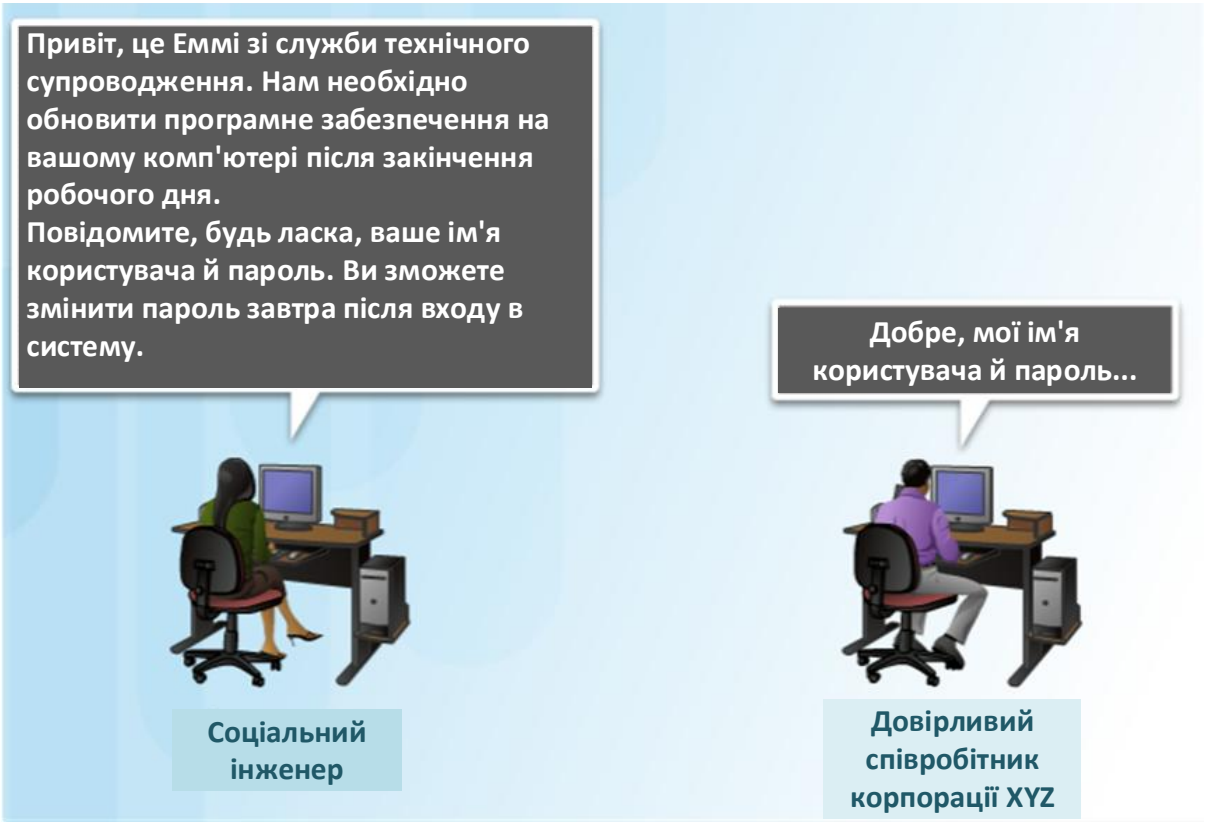


Рис. 8.9 – Приклад атаки із застосуванням соціальної інженерії

У табл. 8.6 описані деякі зі способів, до яких прибігають зловмисники, що користуються соціальною інженерією, щоб одержати необхідну інформацію.

Нижче наведені основні запобіжний заходи для захисту від соціальної інженерії:

- Ніколи не розкривайте свої облікові дані для входу (такі як ім'я користувача, пароль, PIN-код).
- Ніколи не записуйте свої облікові дані на робочому місці.
- Блокуйте комп'ютер, відлучаючись із робочого місця.

Нижче наведені рекомендації із забезпечення безпеки фізичного розташування для компаній.

- Впровадьте пропускну систему, щоб організувати доступ до розташування тільки по поіменному спискові співробітників.

- Проходячи через двері по карті доступу, не допускайте, щоб з вами пройшли сторонні особи.
- Завжди запитуйте в невідомих осіб посвідчення.
- Обмежте доступ відвідувачів.
- Супроводжуйте всіх відвідувачів.

Таблиця 8.6 – Прийоми соціальної інженерії

Прийоми	Опис
Вигаданий привід	Хакер прикидається, що йому необхідні особисті або фінансові дані користувача для підтвердження справжності одержувача.
Фішинг	Хакер відправляє підроблене повідомлення електронної пошти, замасковане під лист від законної організації. Воно призначене для того, щоб обдурити одержувача й переконати його встановити шкідливе ПЗ на пристрій або надати особисту або фінансову інформацію.
Вибірковий фішинг	Хакер підготовляє фішингову атаку, спрямовану на визначену людину або організацію.
Спам	Хакер використовує спам, щоб обдурити користувача й переконати його перейти по зараженому посиланню або завантажити заражений файл.
Прохід «паровозиком»	Зловмисник швидко іде за довіреною особою, щоб проникнути в захищене приміщення. У такий спосіб він може потрапити на захищену територію.
Послуга за послугу	Ситуації, коли зловмисник просить надати від іншої сторони особисту інформацію в обмін на що-небудь, наприклад, безкоштовний подарунок.
Принада	Хакер залишає в загальнодоступному місці, такому як убиральня для співробітників компанії, фізичний пристрій, заражений шкідливим ПЗ (наприклад, флеш-диск USB). Людина, що знайшла такий пристрій підключає його до комп'ютера й тим самим ненавмисно встановлює шкідливе ПЗ.

8.2 Що таке політика безпеки

Політика безпеки являє собою набір параметрів безпеки для захисту мережі, даних і комп'ютерних систем в організації. **Політика безпеки** – це постійно удосконалений документ, в основі якого лежать зміни вимог до застосування технологій, веденню бізнесу й поведінці співробітників.

Створенням політики безпеки й управлінням нею звичайно займається керівництво організації й співробітники IT-відділу, як показано на рис. 8.10. Спільними зусиллями вони створюють документ, який дозволяє одержати відповіді на запитання, наведені в табл. 8.7

Політика безпеки звичайно включає пункти, зазначені табл. 8.8. Цей список не є вичерпним і може включати й інші пункти, що стосуються функціонування кожної конкретної організації.

У рамках даного курсу ми розглянемо настроювання локальної політики безпеки в операційній системі Windows.



Рис. 8.10 – Створення політики безпеки мережі

Таблиця 8.7 – Питання по політиці безпеки

Політика безпеки визначає...
• Які ресурси вимагають захисту?
• Які можливі погрози?
• Які дії у випадку порушення безпеки?
• Яке навчання будуть проходити кінцеві користувачі?

Таблиця 8.8 – Політика безпеки

	Вид політики	**Функції політики**
1	Політики ідентифікації й автентифікації	Визначають коло уповноважених осіб, яким наданий доступ до ресурсів мережі, і процедури перевірки.
2	Політики відносно паролів	Забезпечують відповідність паролів мінімальним вимогам і їх регулярну зміну.
3	Політики цільового використання	Визначають ресурси мережі й порядок їх використання співробітниками організації. Також вони можуть визначати наслідки порушення цих політик.
4	Політики дистанційного доступу	Визначають, яким образом віддалені користувачі можуть одержати доступ до мережі, а також до чого одержує доступ користувач, що використовує віддалене підключення.
5	Політики обслуговування мережі	Визначають процедури відновлення операційних систем мережевих пристроїв і додатків кінцевих користувачів.
6	Політики обробки інцидентів	Описують порядок обробки інцидентів, пов'язаних з безпекою.

8.2.1 Доступ до локальної політики безпеки Windows

У більшості мереж, де використовуються комп'ютери Windows, для взаємодії в доменах під управлінням Windows Server застосовується служба каталогів Active Directory. Комп'ютери Windows входять у домени. Адміністратор настроює політику безпеки домена, яка застосовується до всіх комп'ютерів, що входять у домен. Після входу користувача в систему Windows автоматично застосовуються політики облікових записів.

На комп'ютерах, які не входять у домен, можна застосовувати локальну політику безпеки Windows. Для доступу до локальної політики безпеки на комп'ютерах з ОС Windows 7 і Vista послідовно виберіть наступні пункти:

Пуск > Панель управління > Адміністрування > Локальна політика безпеки

В ОС Windows 8 і 8.1 виберіть наступні пункти:

Пошук > secpol.msc, потім клацніть **secpol**.

Відкриється діалогове вікно інструмента настроювання локальної політики безпеки, як показано на рис.8.14.

Примітка. У всіх версіях Windows для запуску інструмента настроювання локальної політики безпеки можна вибрати пункт **Виконати** й увести **secpol.msc**.

8.2.2 Імена користувачів і паролі

Системний адміністратор звичайно визначає правила створення імен користувачів при створенні мережних імен користувачів. Розповсюджений приклад імені користувача – перша буква імені користувача й далі його прізвище цілком. Правила створення імен повинні бути простими, щоб їх можна було просто запам'ятати. Імена користувачів, як і паролі, – важливі елементи інформації й не повинні розкриватися.

Правила, що стосуються паролів, – важливий компонент політики безпеки. Будь-який користувач, якому необхідно ввійти в систему комп'ютера або підключитися до мережного ресурсу, повинен указати пароль. Паролі допомагають запобігти розкраданню даних і шкідливі дії. Паролі також допомагають забезпечити правильну реєстрацію подій, гарантуючи, що користувач має потрібні права.

Рекомендується використовувати три рівні захисту паролем.

- **BIOS** (див. рис. 8.11) – перешкоджає завантаженню операційної системи й зміні параметрів BIOS без уведення відповідного пароля.
- **Вхід у систему** (див. рис. 8.12) – дозволяє запобігти несанкціонованому доступу до локального комп'ютера.
- **Вхід у мережу** (див. рис. 8.13) – дозволяє запобігти доступу сторонніх осіб до мережі.



Рис. 8.11 – Автентифікація BIOS



Рис. 8.12 – Автентифікація Windows



Рис. 8.13 – Автентифікація мережі

8.2.3 Параметри безпеки політик облікових записів

При призначенні паролів рівень парольного контролю повинен відповідати необхідному рівню захисту. По можливості використовуйте надійні паролі. У табл. 8.9 наведені інструкції зі створення надійних паролів.

Щоб застосувати вимоги до паролів, скористайтеся параметром **Політика паролів** у розділі **Політики облікових записів**. Конфігурації, зазначені на рис. 8.14, відповідають наступним вимогам.

Вести журнал паролів – користувач може повторно використовувати пароль після того, як він зберіг 24 унікальних пароля.

Максимальний термін дії пароля – користувачу необхідно міняти пароль кожні 90 днів.

Мінімальний термін дії пароля – користувач може змінити пароль тільки після закінчення одного дня з моменту останньої зміни пароля. Завдяки цьому виключається можливість уведення 24 різних паролів, щоб можна було знову використовувати попередній пароль.

Мінімальна довжина пароля – пароль повинен містити не менш 8 символів.

Пароль повинен відповідати вимогам складності – у паролі не повинні вказуватися ім'я облікового запису користувача або частини повного імені користувача, які містять більш двох послідовних символів в імені. Пароль повинен включати символи хоча б трьох із чотирьох наступних категорій: прописні букви, малі літери, цифри й символи.

Таблиця 8.9 – Рекомендації зі створення надійних паролів

Характеристики пароля	Рекомендації
Мінімальна довжина	Використовуйте не менш восьми символів.
Складність	Пароль повинен містити букви, цифри, символи й розділові знаки. Використовуйте різні символи на клавіатурі, а не тільки розповсюджені букви й символи.
Різноманітність	Використовуйте різні паролі для кожного використовуваного сайту або комп'ютера.
Термін дії	Термін дії паролів повинен минати через прийнятний проміжок часу. Чим коротше цей період, тем вище безпека комп'ютера. Також установите нагадування про зміну паролів для електронної пошти, банківських сайтів і сайтів роботи із кредитними картами в середньому кожні три-чотири місяці.

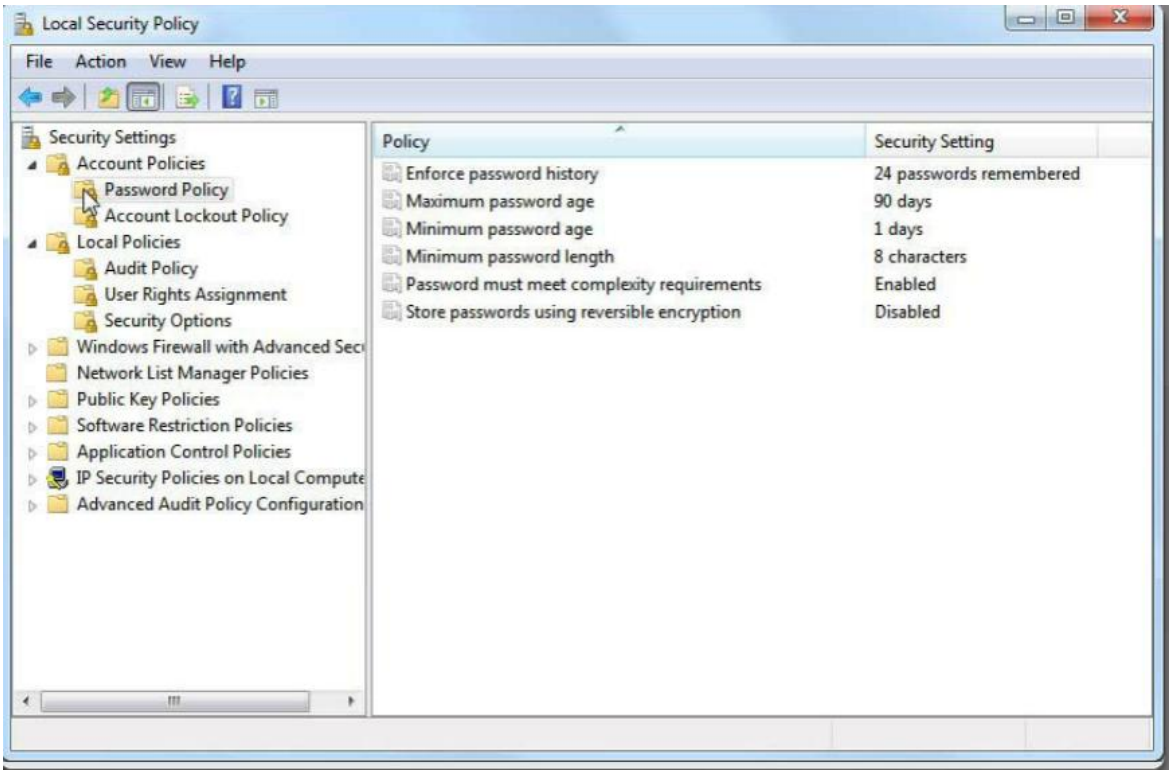


Рис. 8.14 – Настройка вимог до паролю

Зберігати паролі, використовуючи оборотне шифрування – такий спосіб зберігання паролів нічим не відрізняється від зберігання паролів у вигляді простого тексту. Тому цей параметр повинен бути завжди відключений, якщо тільки вимоги додатків не одержують пріоритет над захистом паролів.

Скористайтеся параметрами в пункті **Політика блокування облікового запису** роздягнуло **Політики облікових записів**, щоб запобігти атакам методом добору пароля. Наприклад, у конфігурації, наведеної на рис. 8.15, користувачу надається тільки п'ять спроб увести правильні ім'я

користувача й пароль. Після п'яти невдалих спроб обліковий запис блокується на 30 хвилин.

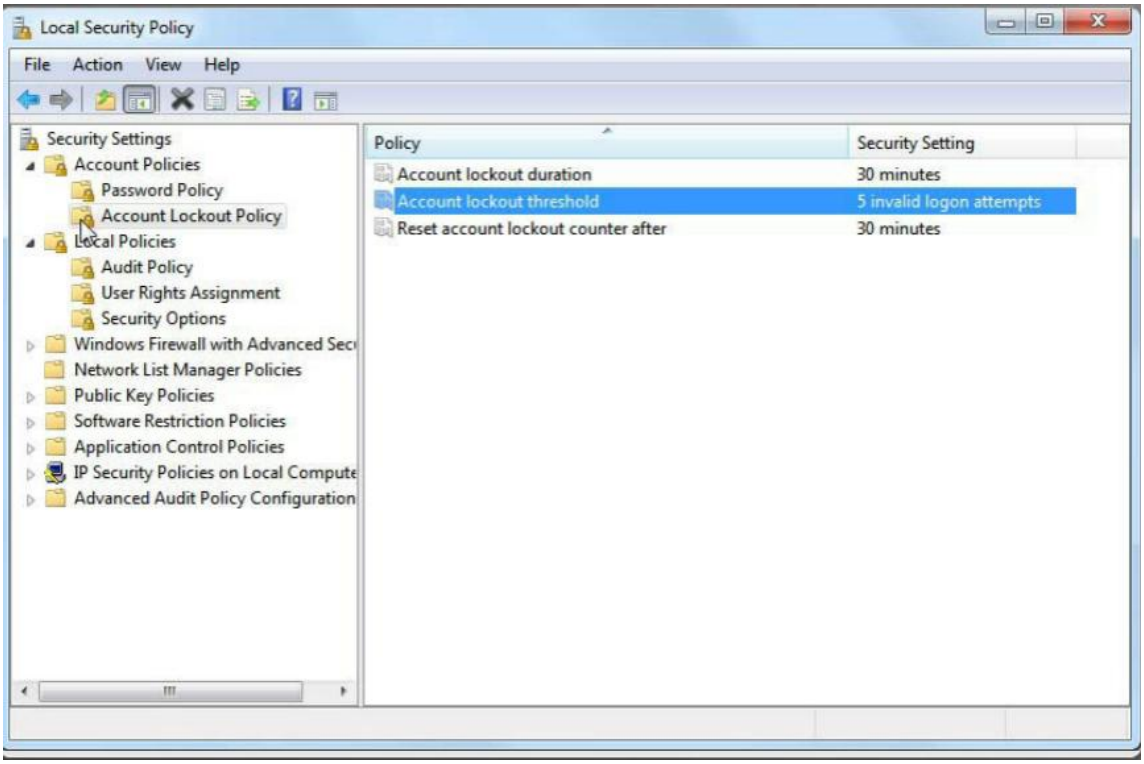


Рис. 8.15 – Настройка політики блокування облікового запису

Після закінчення цих 30 хвилин лічильник спроб скидається, після чого користувач може знову спробувати ввійти в систему. Ця політика також дозволяє захиститися від атак перебором по словникові, при яких при спробі одержати доступ уводиться кожне слово в словнику.

8.2.4 Управління локальними паролями

Управління паролями автономних комп'ютерів Windows здійснюється локально за допомогою інструмента **Облікові записи користувачів**. Для створення, видалення або зміни пароля в Windows використовуйте наступний шлях, як показано на рис. 8.16:

Панель управління > Облікові записи користувачів

Щоб запобігти доступу несанкціонованих користувачів до локальних комп'ютерів і мережевим ресурсам, блокуйте робочу станцію, портативний комп'ютер або сервер, якщо ви за ним не працюєте.

Важливо забезпечити безпеку комп'ютерів, коли користувачі не працюють за ними. Політика безпеки повинна містити правило вимоги блокування комп'ютера при запуску хоронителя екрана. Завдяки цьому через якийсь час відсутності користувача запуститься екранна заставка, і комп'ютер можна буде використовувати тільки після входу користувача в систему.



Рис. 8.16 – Зміна пароля в Windows

У всіх версіях Windows слід використовувати наступний шлях:

Панель управління > Персоналізація > Заставка. Виберіть екранну заставку й час очікування, потім установите прапорець **Починати з екрана входу в систему**, як показано на рис. 8.17.

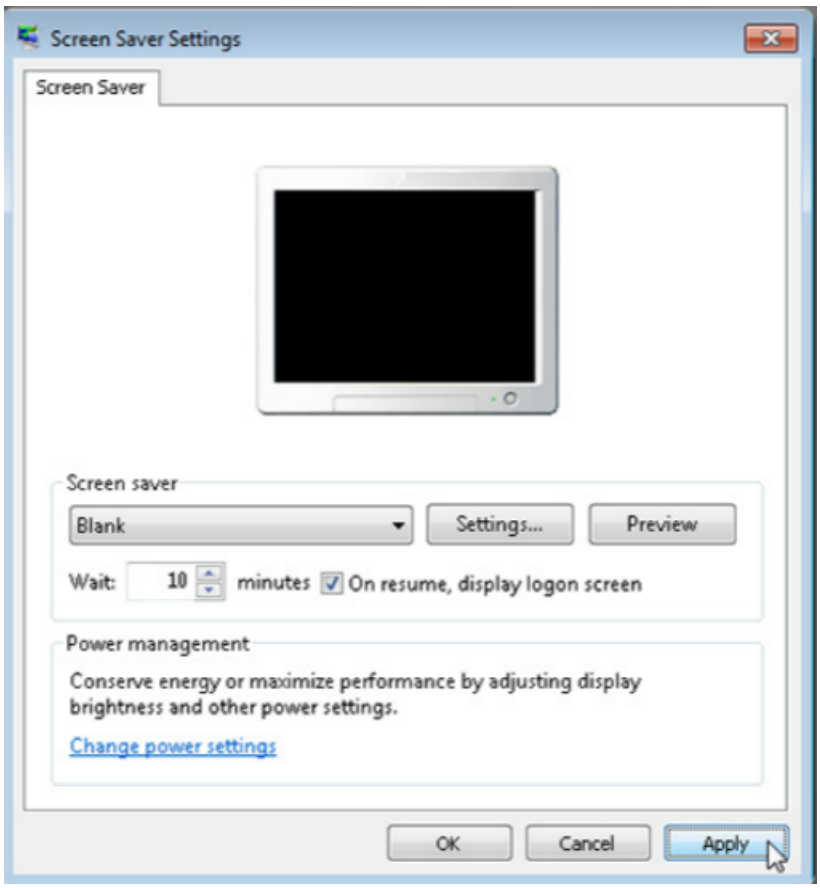


Рис. 8.17 – Настройка блокування хоронителя екрана

8.2.5 Параметри безпеки локальних політик

Більшість параметрів, що перебувають у пункті **Локальні політики** розділу **Локальна політика безпеки**, не розглядаються в рамках даного курсу. Однак вам слід включити аудита для кожного пункту в розділі **Політика аудита**. Наприклад, на рис. 8.18 показане, що аудит включений для всіх подій входу в систему.

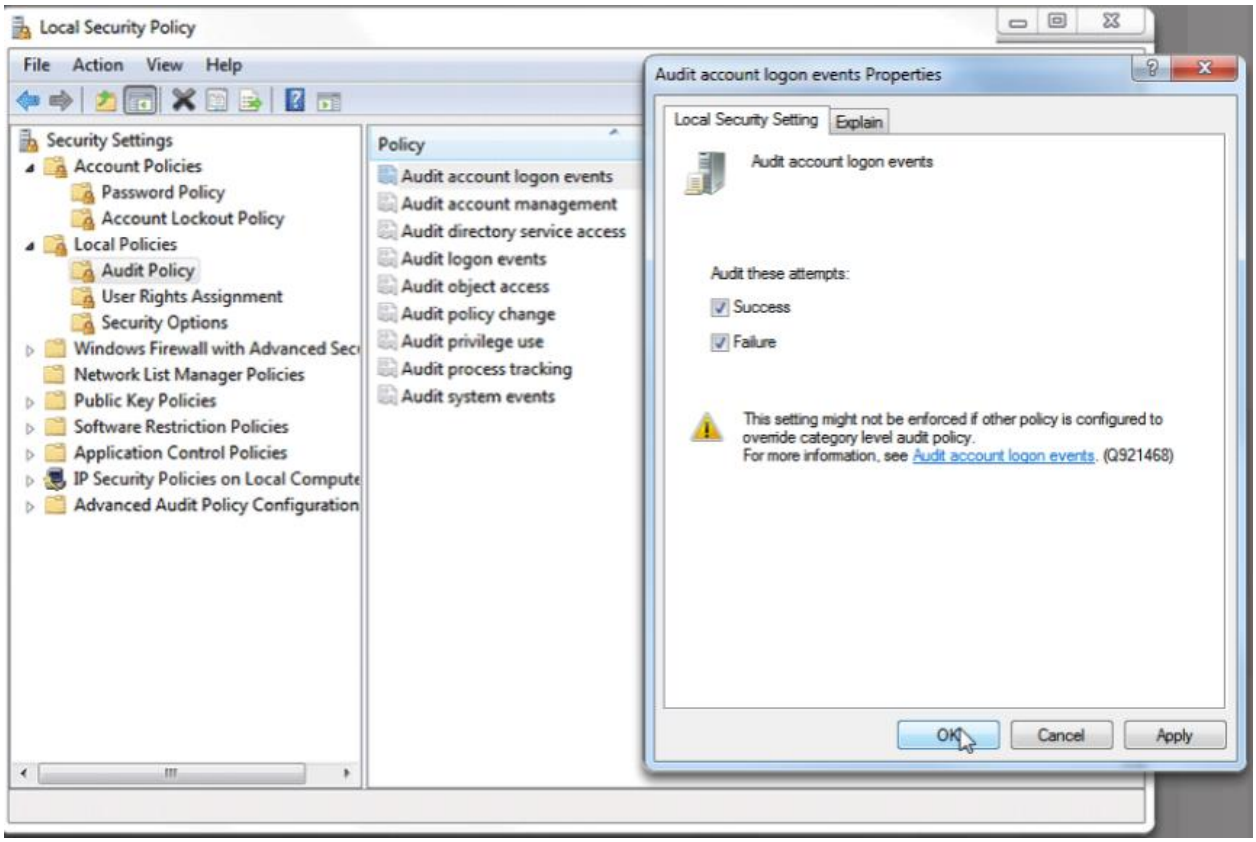


Рис. 8.18 – Вмикання політик аудита

Ви можете змінювати деякі параметри в розділах **Призначення прав користувача** й **Параметри безпеки**.

8.2.6 Експорт локальної політики безпеки

Якщо на всіх автономних комп'ютерах використовується однакова **локальна політика безпеки**, скористайтеся функцією експорту політики, як показано на рис. 8.19. Збережете політику, присвоївши їй зрозуміле ім'я, таке як **workstation.inf**. Потім скопіюйте файл політики на зовнішній носій або мережевий диск, щоб скористатися цим файлом на автономних комп'ютерах. Такий підхід корисний у випадках, коли адміністратору необхідно настроїти велику кількість локальних політик відносно прав користувачів і застосовуваних параметрів безпеки.

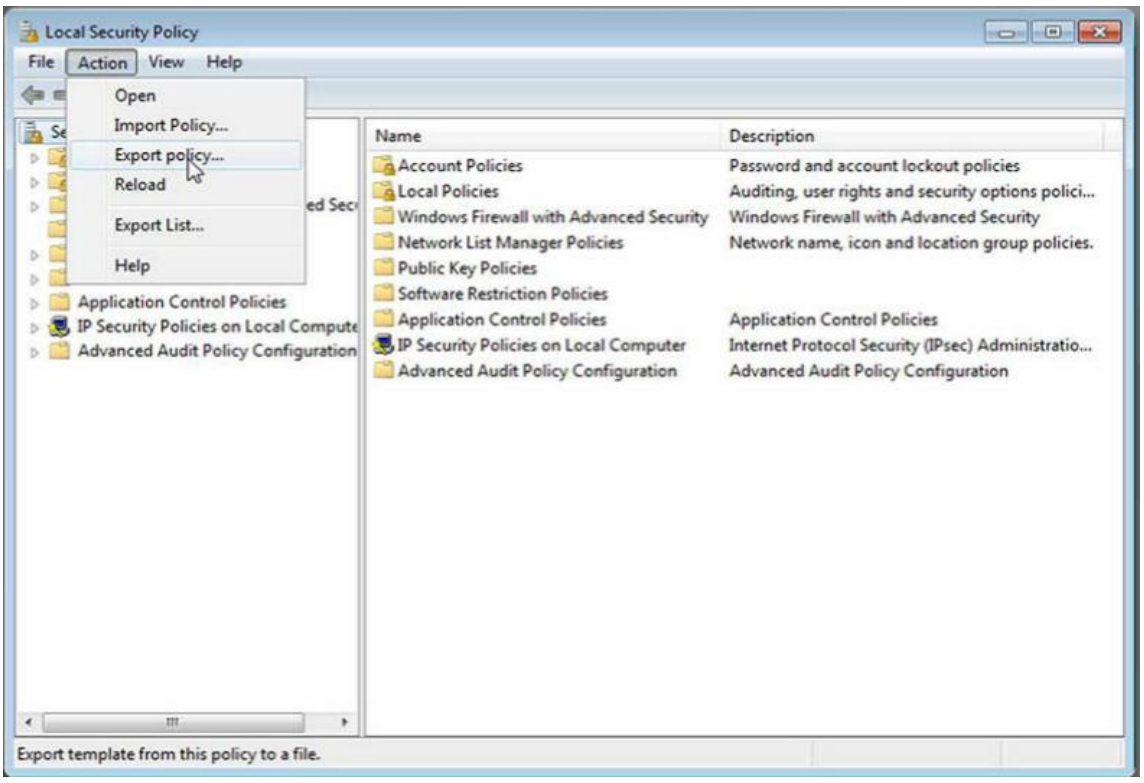


Рис. 8.19 – Експорт локальної політики безпеки

8.2.7 Забезпечення безпеки веб-трафіка

Хакери використовують різні веб-засоби (наприклад, Activex, Flash), щоб установити шкідливе ПО на комп'ютер.

Для запобігання таких дій у браузерах є засоби, що дозволяють підвищити безпека веб-трафіка рис. 8.20:

- Фільтрація Activex
- Програма блокування спливаючих вікон
- Фільтр Smartscreen
- Перегляд Inprivate



Рис. 8.20 – Функції безпеки веб-браузера

8.2.8 Фільтрація Activex

Деякі веб-сторінки правильно працюють тільки при установці елемента управління Activex. Деякі елементи управління Activex написані сторонніми постачальниками й можуть бути шкідливими. Фільтрація Activex забезпечує роботу в Інтернеті без запуску елементів управління Activex.

Якщо елемент управління Activex установлений на одному веб-сайті, він працює й на інших веб-сайтах. Це може привести до зниження продуктивності або появі погроз безпеки. При включенні фільтрації Activex можна вибирати веб-сайти, які можуть запускати елементи управління Activex. Незатверджені сайти не можуть запускати ці елементи управління, і браузер не відображає повідомлення про установку або дозвіл цих елементів управління.

Щоб включити фільтрацію Activex у браузері Explorer 11, виберіть наступні пункти:

Безпека > Фільтрація Activex

На рис. 8.21 представлений приклад активованої фільтрації Activex. Знову клацніть пункт **Фільтрація Activex**, щоб відключити цю функцію.

Для перегляду веб-сайту, що містить Activex-Контент при включеній фільтрації Activex, клацніть синій значок **Фільтрація Activex** в адресному рядку, потім виберіть **Відключити фільтрацію Activex**.

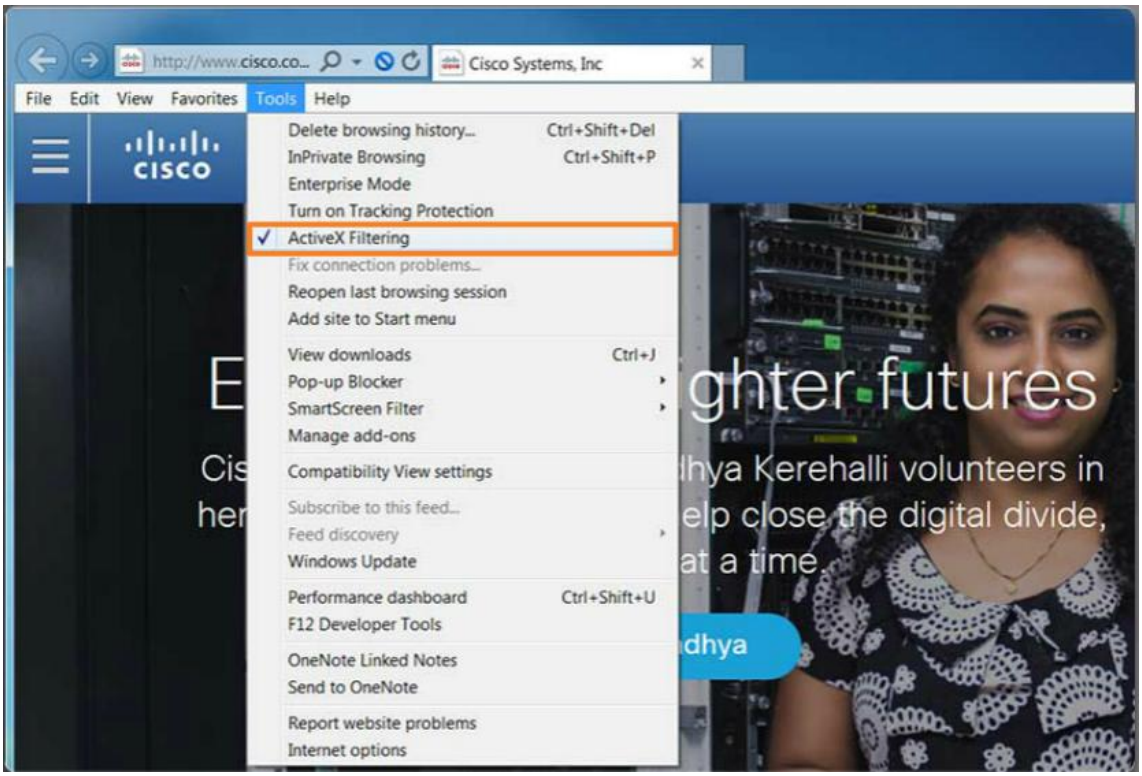


Рис. 8.21 – Включення функції фільтрації Activex

Після перегляду вмісту можна знову включити фільтрацію Activex для веб-сайту, виконавши ці ж дії.

8.2.9 Програма блокування спливаючих вікон

Спливаюче вікно – це вікно веб-браузера, що відкривається поверх іншого вікна браузера. Відкриття деяких спливаючих вікон зініціюється при перегляді, наприклад посилання на сторінці, що відкриває спливаю-

че вікно для одержання додаткової інформації або перегляду збільшеного зображення. Інші спливаючі вікна зініціюються веб-сайтом або рекламодавцем і часто можуть бути небажаними або дратувати користувачів, особливо при одночасному відкритті на веб-сторінці декількох спливаючих вікон.

У більшості браузерів є можливість заблокувати спливаючі вікна. Це дозволяє користувачу обмежити або блокувати більшість спливаючих вікон, що відкриваються при роботі в Інтернеті.

Щоб включити в браузері Internet Explorer 11 блокування спливаючих вікон, виберіть наступні пункти, як показано на рис. 8.22.

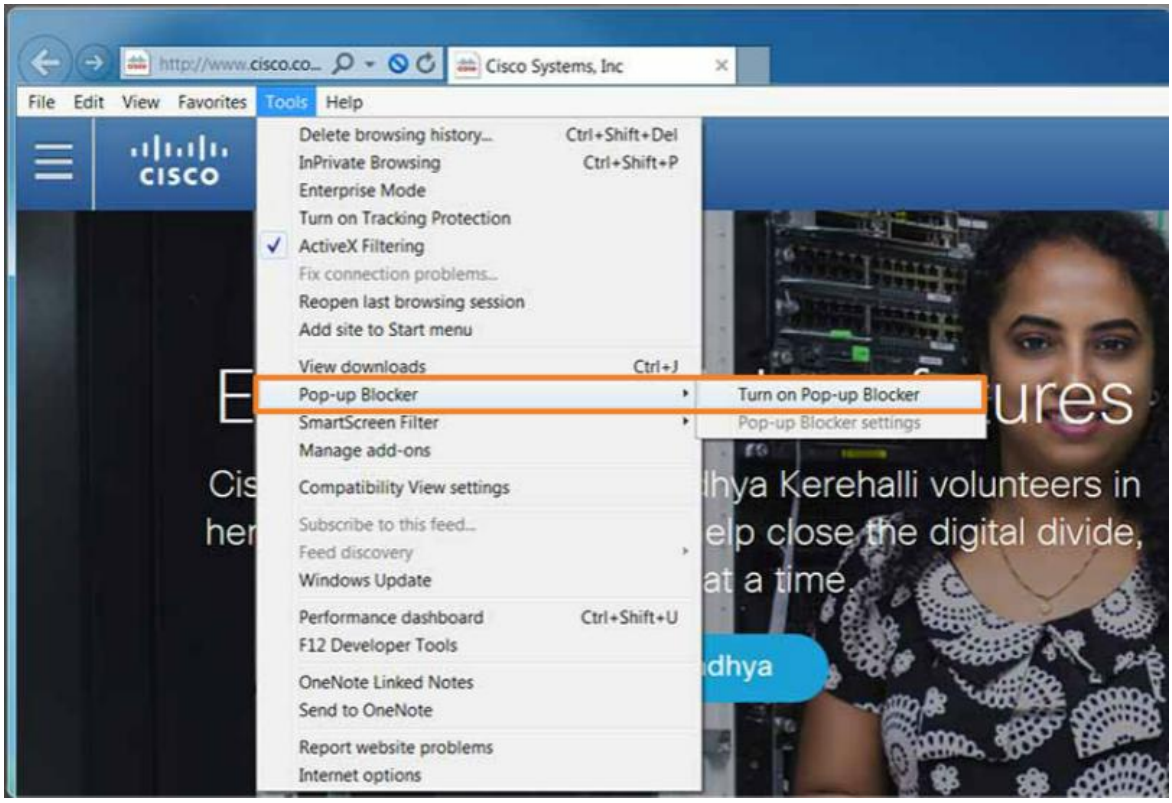


Рис. 8.22 – Включення функції блокування спливаючих вікон

Сервіс > Блокування спливаючих вікон > Включити блокування спливаючих вікон

Після цього можна перейти до настроювань блокування. Для зміни параметрів програми блокування спливаючих вікон в Internet Explorer виберіть наступні пункти (див. рис. 8.23):

Сервіс > Блокування спливаючих вікон > Параметри блокування спливаючих вікон

Можна настроїти наступні параметри блокування спливаючих вікон, як показано на рис. 8.24.

Можна додати веб-сайт у список веб-сайтів, для яких дозволено відкриття спливаючих вікон

Можна змінити повідомлення при блокуванні спливаючих вікон

Можна змінити рівень блокування. **Високий** – блокування всіх спливаючих вікон, **Середній** – блокування більшості спливаючих вікон, що автоматично відкриваються**,** і Низький – дозвіл спливаючих вікон з надійних сайтів.

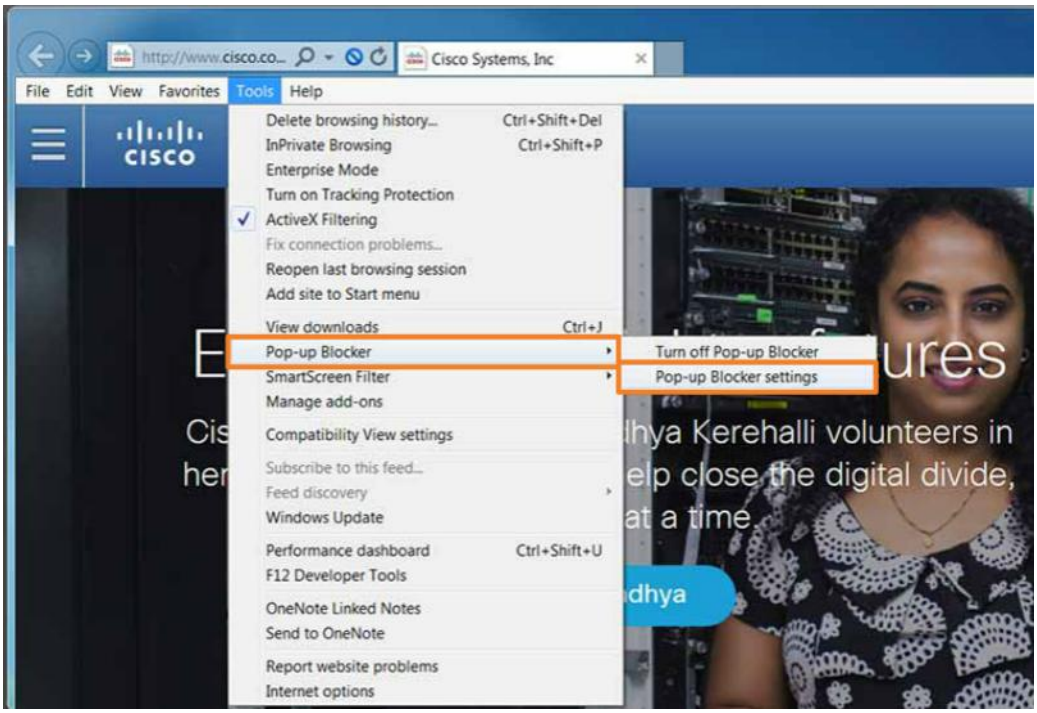


Рис. 8.23 – Зміна настроювань блокування спливаючих вікон

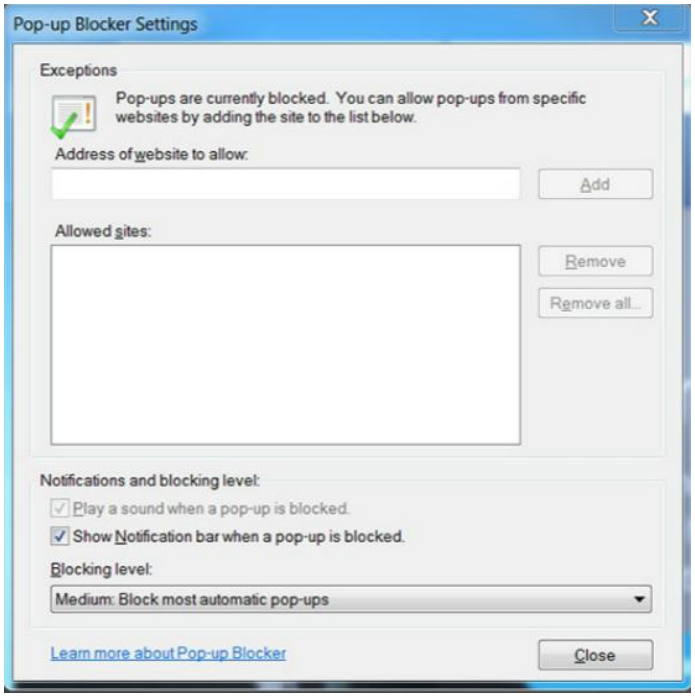


Рис. 8.24 – Вікно параметрів програми блокування спливаючих вікон

8.2.10 Фільтр Smartscreen

У веб-браузерах також можуть бути додаткові можливості фільтрації веб-трафіка. Наприклад, в Internet Explorer 11 є функція «Фільтр Smartscreen». Вона служить для виявлення фішингових веб-сайтів, аналізує веб-сайти на предмет наявності на них підозрілих елементів, а також перевіряє завантаження за списком відомих шкідливих сайтів і файлів.

Щоб включити в браузері Internet Explorer 11 фільтр Smartscreen, виберіть наступні пункти, як показано на рис. 8.25.

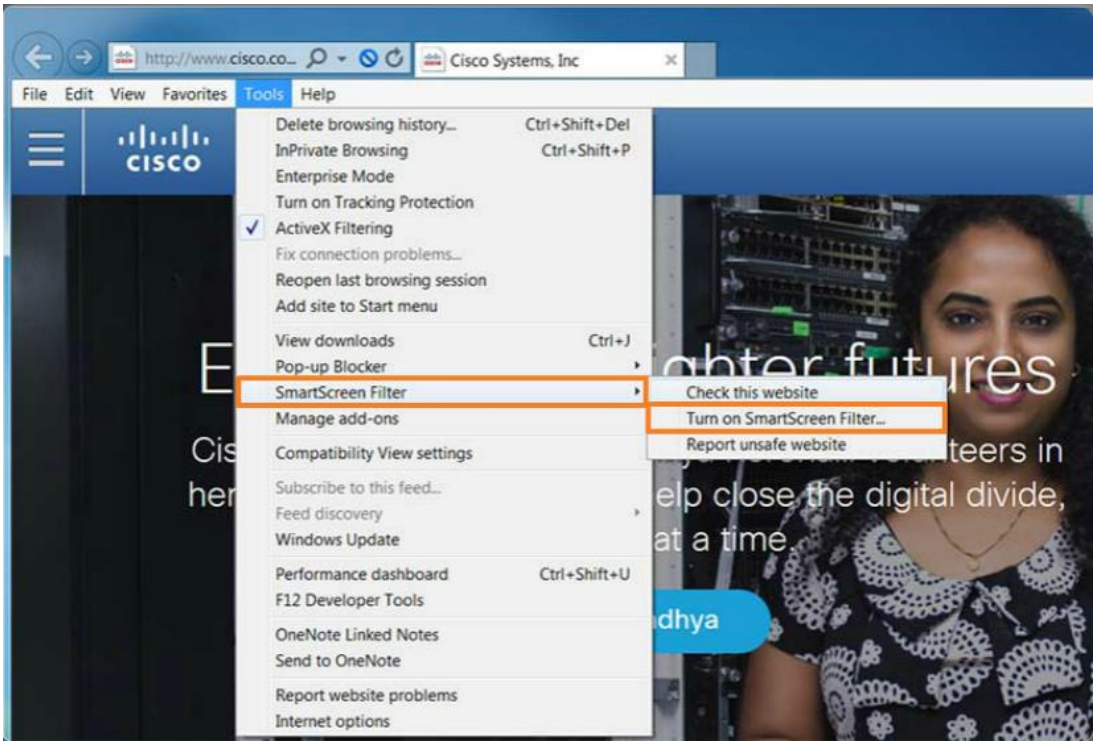


Рис. 8.25 – Включення фільтра SmartScreen

Безпека > Фільтр Smartscreen > Відключити фільтр Smartscreen

Після цього з'явиться діалогове вікно фільтра Microsoft Smartscreen, як показано на рис. 8.26. У цім вікні можна включити або відключити функцію.

Щоб включити функцію, установите перемикач **Включити фільтр Smartscreen (рекомендується)** і натисніть кнопку **ОК**.

Також можна перевірити вміст веб-сторінки. Для аналізу поточної веб-сторінки використовуйте наступний шлях:

Безпека > Фільтр Smartscreen > Перевірити веб-вузол

Для повідомлення про підозрілу веб-сторінку використовуйте наступний шлях:

Безпека > Фільтр Smartscreen > Повідомити про небезпечний веб-вузол

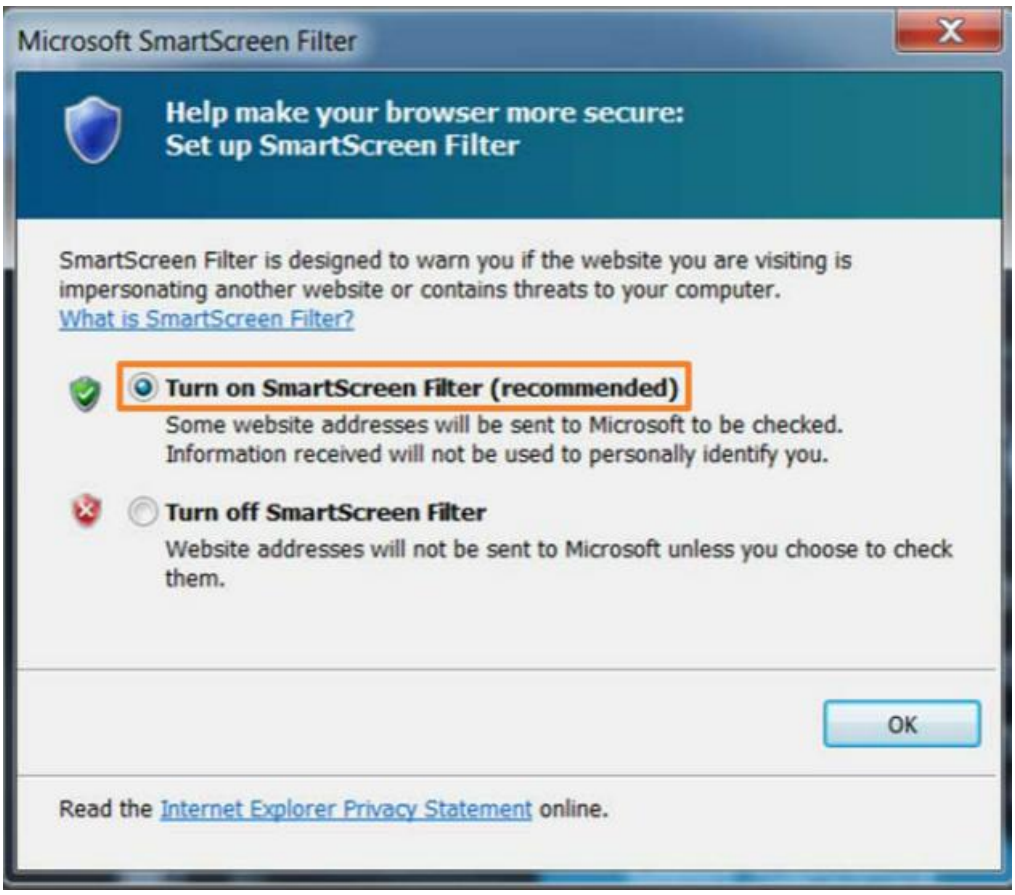


Рис. 8.26 – Вікно настроювань фільтра Smartscreen

8.2.11 Перегляд Inprivate

Браузери зберігають відомості про переглянуті веб-сторінки, уведені пошукові запити й іншу інформацію, яку можна використовувати для ідентифікації користувача, включаючи імена користувачів, паролі й інші дані. Це зручна функція при використанні домашнього комп'ютера, захищеного паролем. Однак така можливість браузера може викликати побоювання, якщо комп'ютер є загальнодоступним (наприклад, якщо він установлений у бібліотеці, бізнес-центрі готелю або в інтернет-кафе).

Інформацію, яка зберігається в браузері, можна відновити й використовувати в зловмисних цілях. Зловмисники можуть скористатися такими даними для крадіжки ідентифікаційних даних і коштів, а також для того, щоб змінити паролі для важливих облікових записів.

Щоб підвищити безпеку при роботі на загальнодоступних комп'ютерах, у веб-браузерах передбачена можливість анонімної роботи з вебсайтами, коли введені вами дані не зберігаються в браузері. Наприклад, у браузері Internet Explorer 11 є режим «Перегляд Inprivate», у якому відображувані відомості не зберігаються (див. табл. 8.10). Під час роботи в цьому режимі браузер тимчасово зберігає файли кукі й інші файли, а по завершенню сеансу перегляду Inprivate – видаляє їх.

Відкрити вікно браузера в режимі перегляду Inprivate можна як з робочого стола Windows, так і в самому браузері.

Таблиця 8.10 – Запуск перегляду Inprivate

У режимі перегляду Inprivate веб-браузер не зберігає наступні дані:
• Імена користувачів • Паролі • Файли кукі • Журнал браузера • Тимчасові файли Інтернету

Щоб перейти в режим перегляду Inprivate в Windows 7, клацніть значок браузера **Internet Explorer** правою кнопкою миші й виберіть пункт **Почати перегляд Inprivate**, як показано на рис. 8.27.

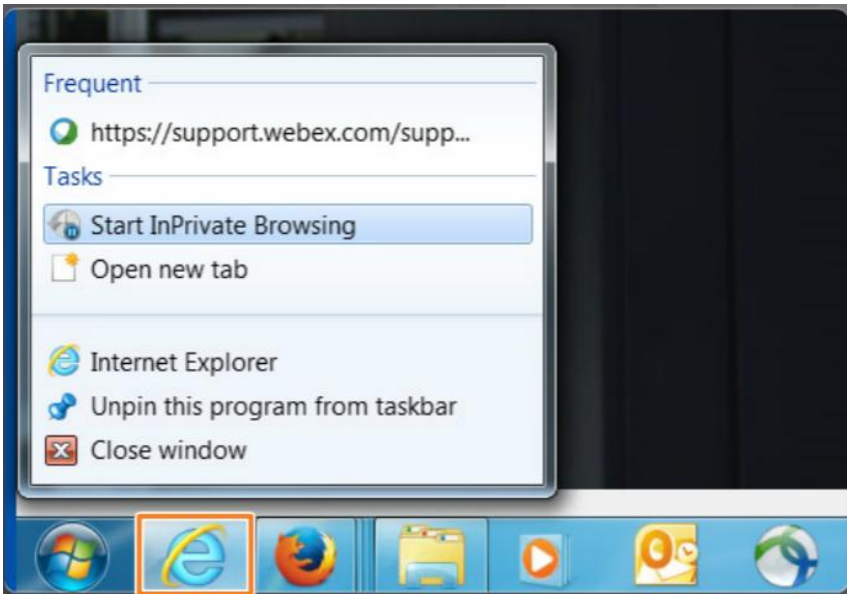


Рис. 8.27 – Запуск перегляду in Private в Windows

Після цього відкриється нове вікно браузера в режимі перегляду Inprivate, як показано на рис. 8.28. У цім вікні представлений опис функції перегляду Inprivate, а також підтвердження того, що функція включена. Також зверніть увагу, що в адресному рядку тепер є індикатор режиму Inprivate (див. виділену область на рис. 8.28). При закритті вікна браузера сеанс перегляду Inprivate завершується. Важливо відзначити, що конфіденційність забезпечується тільки в цім вікні браузера й у будь-яких вкладках, які відкриті в ньому. Інші відкриті вікна браузера не захищені переглядом Inprivate.

Щоб відкрити вікно браузера в режимі перегляду Inprivate через сам браузер Internet Explorer 11, виберіть наступні пункти, як показано на рис. 8.29.

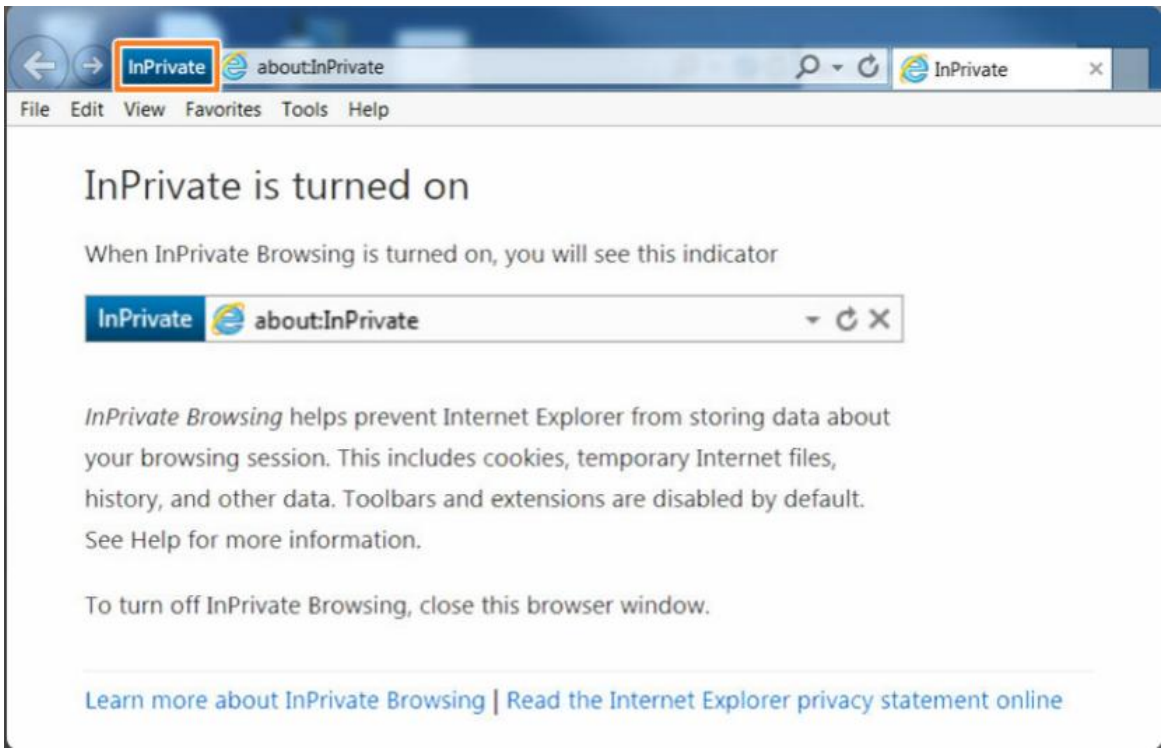


Рис. 8.28 – Веб-сторінка в режимі перегляду InPrivate

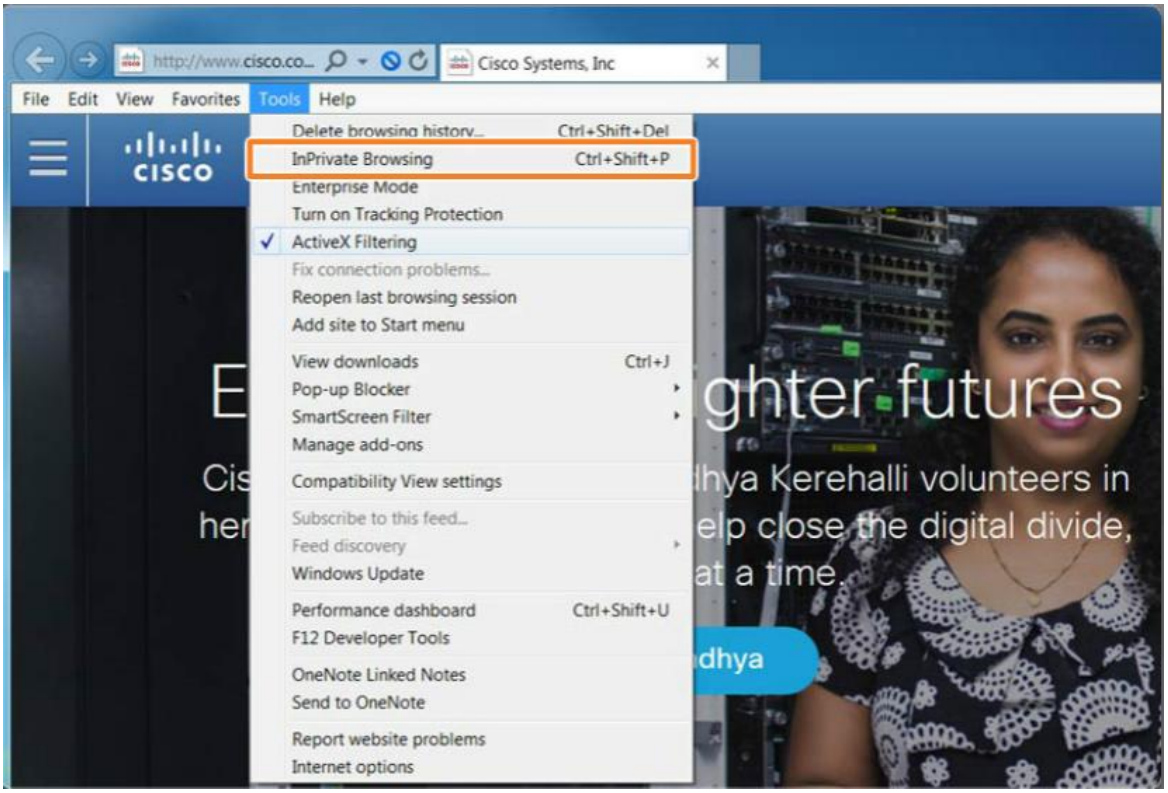


Рис. 8.29 – Запуск перегляду InPrivate в браузері Internet Explorer 11

Безпека > Перегляд Inprivate
Також можна скористатися комбінацією клавіш **Ctrl+Shift+P**.

8.2.12 Програмні міжмережеві екрани (брандмауери)

Програмний міжмережевий екран (брандмауер, фаерволл – від англійського firewall) – це програма, що запускається на комп'ютері для дозволу або заборони обміну трафіком між комп'ютером і іншими комп'ютерами, до яких він підключений. Програмний брандмауер застосовує набір правил для передачі даних за допомогою перевірки й фільтрації пакетів даних. Прикладом такої програми може служити брандмауер Windows (див. рис. 8.30). Він установлюється за замовчуванням при установці ОС.

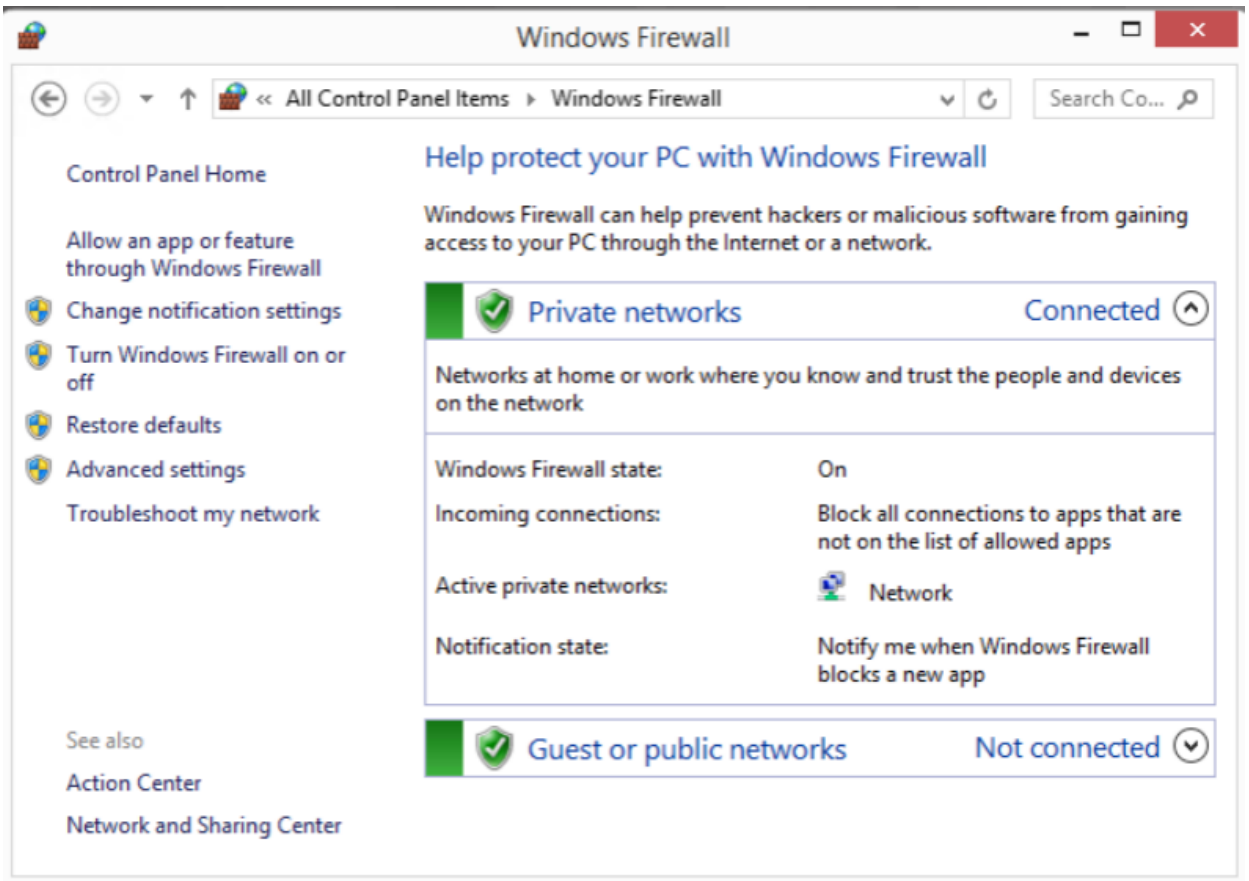


Рис. 8.30 – Брандмауер Windows

Можна контролювати тип даних, що відправляються на інший комп'ютер і одержуваних від нього, вибираючи порти, які будуть відкриті або заблоковані. Брандмауери блокують вхідні й вихідні мережеві підключення, крім випадків, коли для відкриття й закриття портів, необхідних для роботи цієї програми, визначені виключення.

Щоб відкрити або закрити порт у брандмауерові Windows в ОС Windows 7, 8.0 або 8.1, виконаєте зазначені нижче дії.

Крок 1. Послідовно виберіть **Панель управління > Брандмауер Windows > Додаткові параметри**.

Крок 2. В області ліворуч виберіть розділ **Правила для вхідних підключень** або **Правила для вихідного підключення**, а потім в області праворуч натисніть **Створити правило…**, як показано на рис. 8.31.

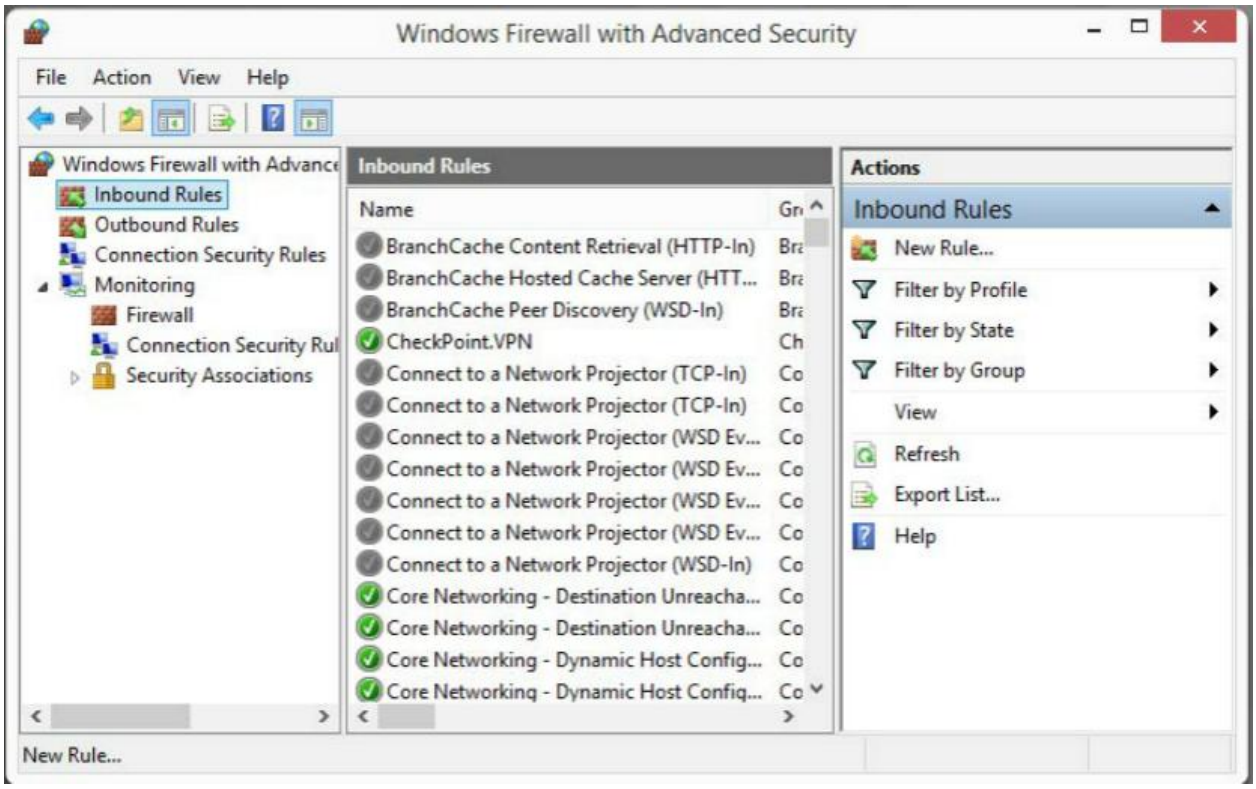


Рис. 8.31 – Настройка правил брандмауера

Крок 3. Установите перемикач **Для порту** й натисніть кнопку **Далі**.

Крок 4. Установите перемикач **Протокол TCP** або **Протокол UDP**.

Крок 5. Установите перемикач **Усі локальні порти** або **Певні локальні порти**, щоб визначити окремі порти або діапазон портів, потім натисніть кнопку **Далі**.

Крок 6. Установите перемикач **Блокувати підключення** й натисніть кнопку **Далі**.

Крок 7. Виберіть профіль застосування правила й натисніть кнопку **Далі**.

Крок 8. Укажіть ім'я й опис правила (необов'язково), а потім натисніть кнопку **Готове**.

Щоб відкрити або закрити порт у брандмауері Windows в ОС Windows Vista, виконайте зазначені нижче дії.

Крок 1. Послідовно виберіть пункти **Панель управління > Брандмауер Windows**, а потім виберіть елемент **Дозвіл запуску програми через брандмауера Windows**.

Крок 2. Натисніть **Додати порт...** і вкажіть ім'я порту, його номер і протокол (TCP або UDP).

8.2.13 Біометрія й смарт-карти

Нижче перелічені додаткові способи захисту доступу до пристроїв.

Система біометричної безпеки (див. рис. 8.32) – у системах біометричної безпеки при перевірці дійсності користувачів рівняються фізичні характеристики й збережені профілі. **Профіль** – це файл даних, що містить відомі характеристики користувача. Якщо фізичні характеристики людини збігаються з тими, які збережені в базі даних, то йому надається доступ. Прикладом розповсюдженого біометричного пристрою є пристрій зчитування відбитків пальців.

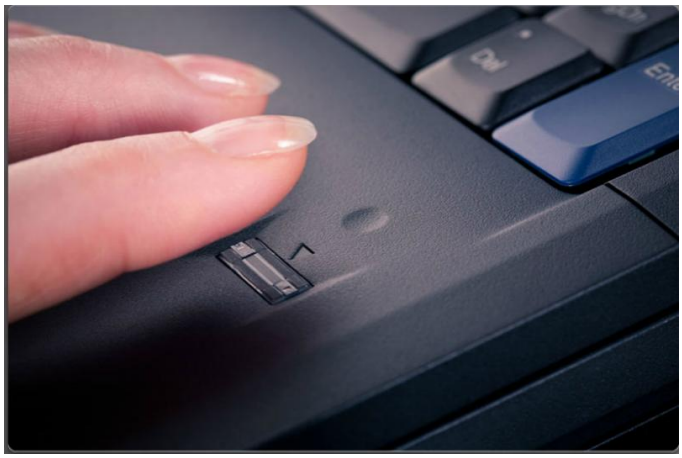


Рис. 8.32 – Пристрій зчитування відбитків пальців на ноутбуці

Забезпечення безпеки з використанням смарт-карт (див. рис. 8.33) – смарт–карта являє собою пластикову карту розміром із кредитну карту, у яку вбудована невелика мікросхема. Ця мікросхема дозволяє не тільки зберігати дані, але й обробляти їх, а також забезпечує захист збережених даних. На смарт-картах зберігається особиста інформація, така як номера банківських рахунків, інформація, що засвідчує особистість, медична документація й цифрові підписи. Смарт-карти забезпечують перевірку дійсності й шифрування для захисту даних.



Рис. 8.33 – Забезпечення безпеки з використанням смарт-карт



Рис. 8.34 – Ключ-брелок безпеки

Ключ-брелок безпеки (див. рис. 8.34) – невеликий пристрій, який можна причепити до зв'язування ключів. Такий пристрій застосовує процес, називаний двохфакторної автентифікацією, який набагато безпечніший процесу з використанням комбінації імені користувача й пароля. Спочатку користувач уводить свій персональний ідентифікаційний номер (PIN-код). У випадку введення правильного коду на дисплеї ключа-брелока безпеки відображається номер. Це другий етап автентифікації, на якому користувачу необхідно ввести цей номер для входу на пристрій або в мережу.

8.2.14 Резервне копіювання даних

Дані можуть бути загублені або ушкоджені в таких випадках, як крадіжки, збої обладнання або аварії. Саме тому надто важливо виконувати резервне копіювання даних.

При виконанні резервного копіювання даних комп'ютера копія інформації зберігається на знімному носії для резервних копій, який можна зберегти в надійному місці. Резервне копіювання даних – один з найефективніших способів захисту даних від втрати. У випадку збою комп'ютерного обладнання дані можуть бути відновлені з резервної копії на працюючім обладнанні.

Резервне копіювання даних слід виконувати регулярно й включати в політику безпеки. Резервні копії даних звичайно зберігаються окремо, щоб захистити носій з резервними копіями на випадок, якщо що-небудь відбудеться в основному приміщенні. Носії з резервними копіями часто використовуються повторно для економії на носіях. Завжди додержуйтеся правил організації по заміні носіїв.

Нижче наведені деякі практичні рекомендації з резервного копіювання даних.

Періодичність – операція резервного копіювання може зайняти дуже багато часу. Іноді простіше виконувати повне резервне копіювання щомісяця або щотижня, а потім виконувати часті часткові резервні копіювання даних, змінених з моменту повного резервного копіювання. Однак, чим більше часткових копій, тим більше затрачається часу на відновлення даних.

Зберігання – щоб забезпечити додаткову безпеку, необхідно переносити резервні копії в автономне сховище щодня, щотижня або щомісяця відповідно до політики безпеки.

Безпека – резервні копії повинні бути захищені паролями. Пароль уводиться до того, як дані на резервному носії можуть бути відновлені.

Перевірка – завжди перевіряйте резервні копії для забезпечення цілісності даних.

Щоб виконати резервне копіювання даних в Windows 7 або Vista, виберіть наступні пункти, як показано на рис. 8.35.

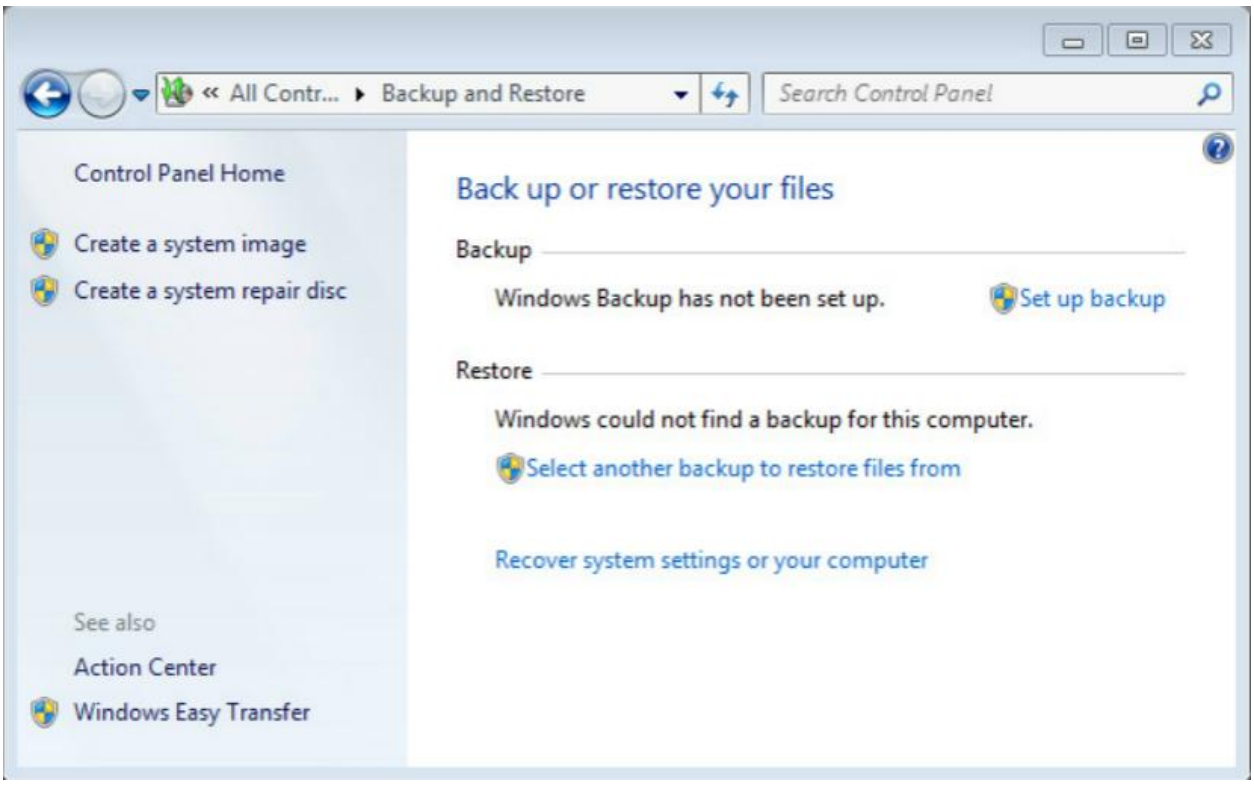


Рис. 8.35 – Вікно «Архівація й відновлення» в Windows 7

Панель управління > Архівація й відновлення

У діалоговому вікні, що з'явилося, можна виконати резервне копіювання даних, що зберігаються на жорсткому диску, і зберегти їх на знімний носій, створити образ системи або диск для відновлення системи.

В операційних системах Windows 8.0 і 8.1 пункт **Архівація й відновлення** був вилучений з панелі управління. Замість цього для резервного копіювання файлів слід використовувати пункт **Історія файлів**, який перебуває в панелі управління. На рис. 8.36 показане повідомлення про те, що не вдалося знайти диск, який можна використовувати для резервного копіювання. Спочатку необхідно настроїти диск для резервного копіювання, а потім включити функцію «Історія файлів». Для цих цілей підходить як зовнішній, так і внутрішній носій. На панелі ліворуч виберіть

пункт **Зміна диска**. Також можна клацнути посилання **Вибрати мережеве розташування**, як показано на рис. 8.36.

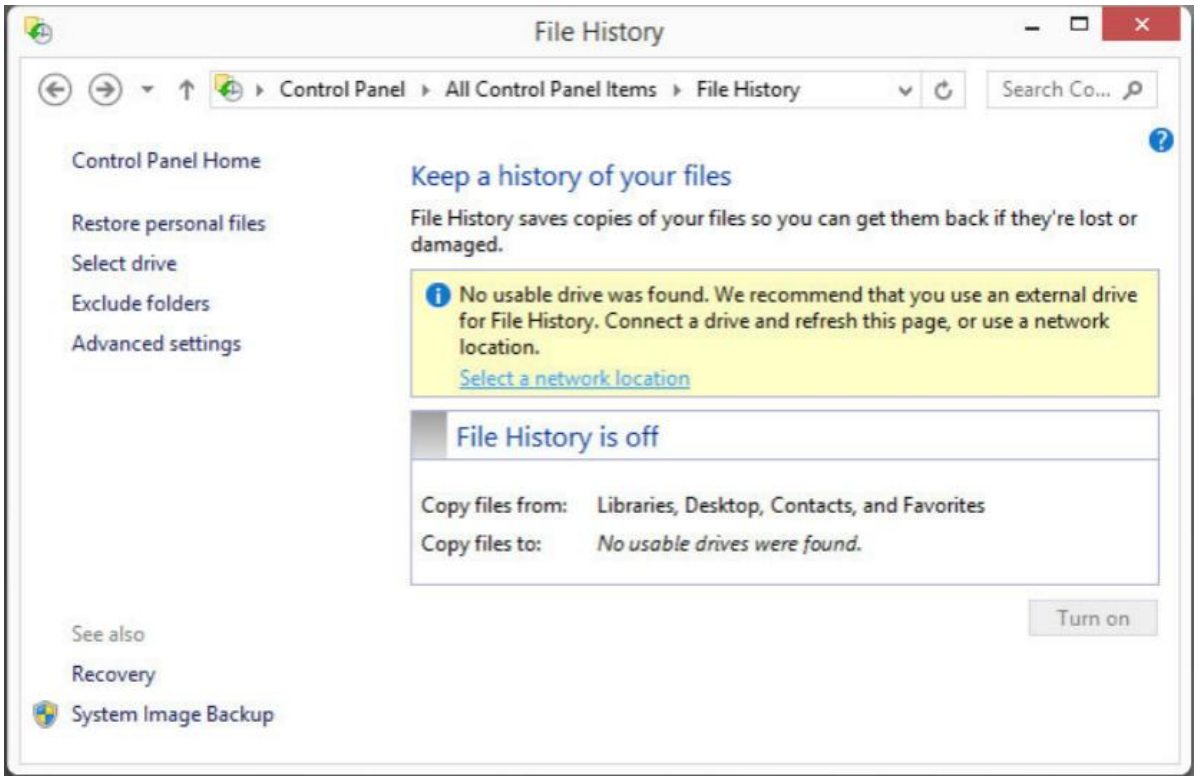


Рис. 8.36 – Вікно «Історія файлів» в Windows 8.1

8.2.15 Дозволи для папок і файлів

Дозволи – це набір правил, які можна настроїти, щоб обмежити доступ окремого користувача або групи користувачів до папки або файлу. У табл. 8.11 перелічені дозволи, які можна задати для файлів і папок. Щоб настроїти дозволи на рівні файлів або папок у будь-якій версії Windows, виберіть наступні пункти:

Клацніть файл або папку правою кнопкою миші й виберіть **Властивості > Безпека > Змінити**

Принцип надання мінімальних привілеїв

Користувачі повинні бути обмежені тільки необхідними ресурсами в комп'ютерній системі або мережі. Наприклад, для них слід скасувати доступ до всіх файлів на сервері, якщо їм потрібен доступ лише до певної папки. Може бути простіше надати користувачам доступ до всього диска, але більш надійно обмежити доступ тільки папкою, необхідною для виконання їх роботи. Це називається принципом надання мінімальних привілеїв. Обмеження доступу до ресурсів також запобігає доступу до них шкідливих програм у випадку зараження комп'ютера користувача.

Обмеження дозволів користувачів

Дозволи для загальних файлів і загальних мережевих ресурсів можуть бути надані окремим користувачам або через членство в групі. Такі

дозволи для загального ресурсу значно відрізняються від дозволів файлової системи NTFS на рівні файлів і папок. Якщо користувачу або групі відмовлене в дозволах для загального мережевого ресурсу, ця відмова перевизначає всі інші надані дозволи. Наприклад, якщо ви відмовляєте кому-небудь у дозволах для загального мережного ресурсу, цей ресурс буде недоступний для користувача, навіть якщо він є адміністратором або входить у групу адміністраторів. У локальній політиці безпеки повинні бути указані ресурси й типи доступу, дозволені для кожного користувача й групи.

Таблиця 8.11 – Типи дозволів

Рівень прав	**Опис**
Повний доступ	Користувач може переглядати вміст файлу або папки, змінювати й видаляти існуючі файли й папки, створювати нові файли й папки, а також запускати програми, наявні в папці.
Зміна	Користувач може змінювати й видаляти існуючі файли й папки, однак не може створювати нові файли й папки.
Читання й виконання	Користувач може переглядати вміст існуючих файлів або папок, а також запускати програми, наявні в папці.
Читання	Користувач може переглядати вміст папки, а також відкривати файли й папки.
Запис	Користувач може створювати нові файли й папки, а також вносити зміни в існуючі файли й папки.

При зміні дозволів для папки можна застосувати ці ж дозволи для всіх вкладених папок. Це називається спадкуванням дозволів. **Спадкування дозволів** – це простий спосіб швидкого застосування дозволів до безлічі файлів і папок. Якщо встановлені дозволи для батьківської папки, то файли й папки, створені усередині неї, успадковують її дозволи.

Крім того, порядок спадкування дозволів визначається розташуванням даних і діями, виконуваними з ними:

- **Дані переміщаються в межах того самого тому** – до даних застосовуються вихідні дозволи
- **Дані копіюються в межах того самого тому** – успадковуються нові дозволи
- **Дані переміщаються на інший том** – успадковуються нові дозволи
- **Дані копіюються на інший том** – успадковуються нові дозволи

8.2.16. Шифрування папок і файлів

Шифрування часто використовується для захисту даних. **Шифрування** – це перетворення даних з використанням складного алгоритму, щоб зробити їх нечитабельним. Для перетворення нечитаємої інформації в читаємі дані необхідно використовувати спеціальний ключ. Програмні продукти застосовуються для шифрування файлів, папок і навіть дисків цілком.

Шифрувальна файлова система (Encrypting File System, EFS) – це функція Windows для шифрування даних. EFS безпосередньо пов'язана з певним обліковим записом користувача. Після шифрування за допомогою EFS дані будуть доступні тільки користувачу, який виконав шифрування. Щоб зашифрувати дані за допомогою EFS в будь-якої версії Windows, виконайте такі дії.

Крок 1. Виберіть один або кілька файлів або папок.

Крок 2. Клацніть обрані дані правою кнопкою миші й виберіть пункт **Властивості**.

Крок 3. Клацніть **Додатково**.

Крок 4. Установите прапорець **Шифрувати вміст для захисту даних**.

Крок 5. Файли й папки, зашифровані з використанням EFS, позначаються зеленим кольором, як показано на рис. 8.37.

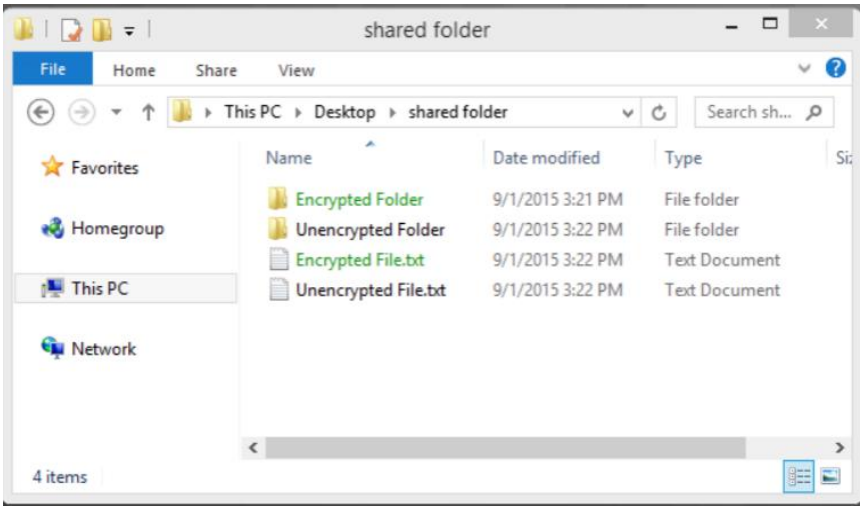


Рис. 8.37 – Шифрування файлової системи

8.2.17 Windows Bitlocker

Для шифрування всіх даних на жорсткому диску використовується функція Bitlocker. Для використання функції Bitlocker на жорсткому диску повинні бути хоча б два томи. Системний том залишається незашифрованим і повинен мати розмір не менш 100 МБ.

На цьому томі втримуються файли, необхідні для завантаження Windows.

Перед використанням Bitlocker в BIOS необхідно включити довірений платформний модуль (Trusted Platform Module, TPM). **TPM** – це спеціальна мікросхема на материнській платі. У модулі TPM зберігається інформація, що ставиться до системи розміщення, така як ключі шифрування, цифрові сертифікати й паролі. Додатки, що використовують шифрування, такі як Bitlocker, звертаються до мікросхеми TPM. Щоб включити TPM, виконаєте зазначені нижче дії.

Крок 1. Включите комп'ютер і ввійдіть у програму настроювання BIOS.

Крок 2. Перейдіть до пункту **TPM** на екранах настроювання BIOS. Для пошуку вірного екрана ознайомтеся з посібником з материнської плати. На рис. 8.38 показаний екран сервісної програми настроювання Lenovo Thinkpad.

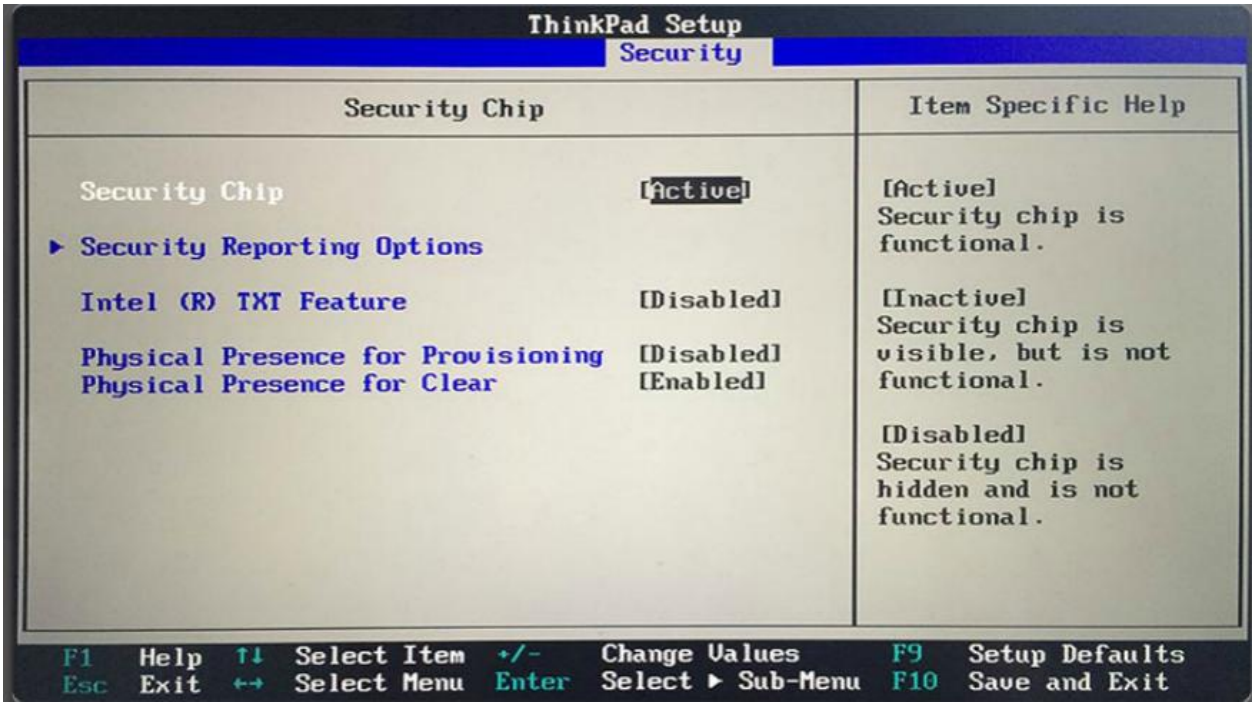


Рис. 8.38 – Шифрування тома диска

Крок 3. Виберіть **Enable** (Включити) або **Activate** (Активувати), щоб задіяти мікросхему безпеки.

Крок 4. Збережете зміни в BIOS.

Крок 5. Перезавантажите комп'ютер.

Щоб включити Bitlocker у будь-якій версії Windows, виконайте зазначені нижче дії.

Крок 1. Послідовно виберіть пункти **Панель управління > Шифрування диска Bitlocker**.

Крок 2. На сторінці **Шифрування диска Bitlocker** виберіть пункт **Включити Bitlocker** для тому операційної системи.

Крок 3. Якщо модуль TPM не ініціалізований, відкриється **майстер обладнання безпеки для TPM**. Для ініціалізації TPM додержуйтеся вказівок майстра. Перезавантажте комп'ютер.

Крок 4. На сторінці **Зберегти пароль відновлення** є наступні варіанти:

- **Зберегти пароль на USB-диску** – збереження пароля на накопичувачі USB.
- **Зберегти пароль у папці** – збереження пароля на мережевому диску або в іншому місці розташування.
- **Надрукувати пароль** – друк пароля.

Крок 5. Після збереження пароля відновлення натисніть кнопку **Далі**.

Крок 6. На сторінці **Шифрування обраного тому диска** встановите прапорець **Запустити перевірку системи Bitlocker**.

Крок 7. Натисніть **Continue** (Продовжити).

Крок 8. Клацніть **Перезавантажити зараз**.

Крок 9. З'явиться рядок стану **Виконується шифрування**. Після перезавантаження можна перевірити, чи запущена функція Bitlocker для тому, як показано на рис. 8.39. Щоб переглянути додаткові відомості про TPM, як показано на рис. 8.40, клацніть посилання **Адміністрування довіреного платформного модуля**.

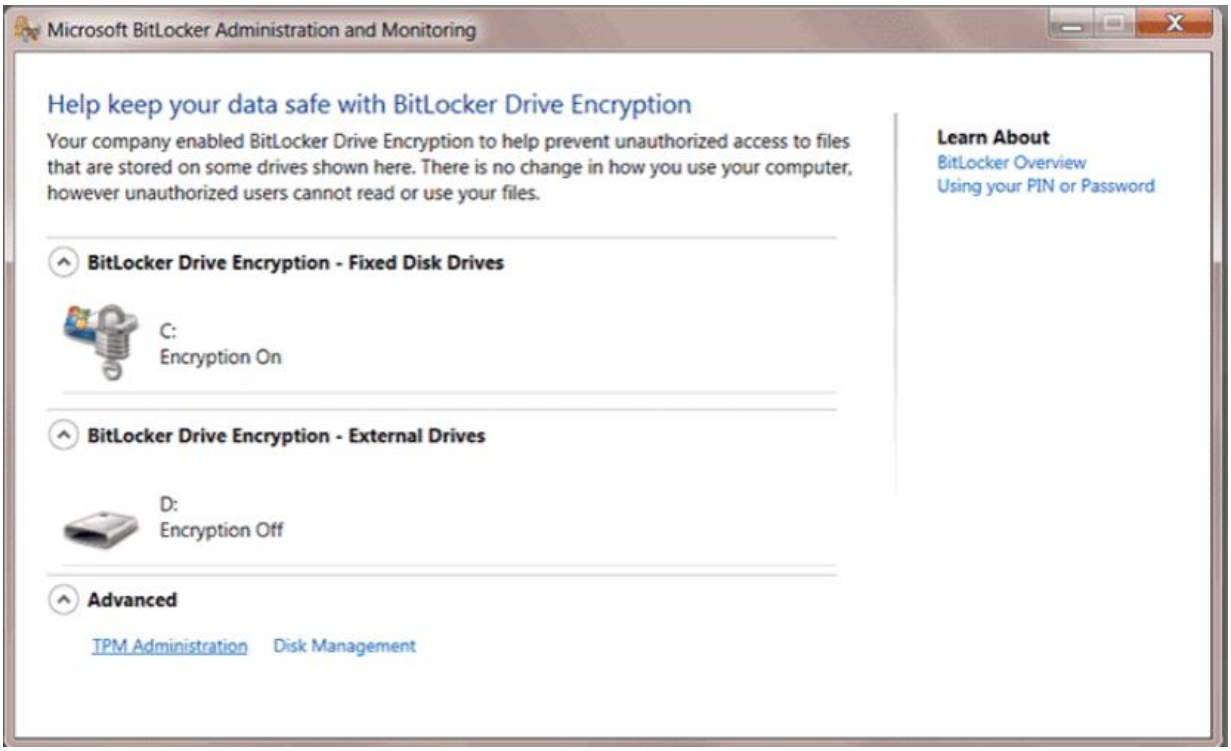


Рис. 8.39 – Перевірка того, що BitLocker включений

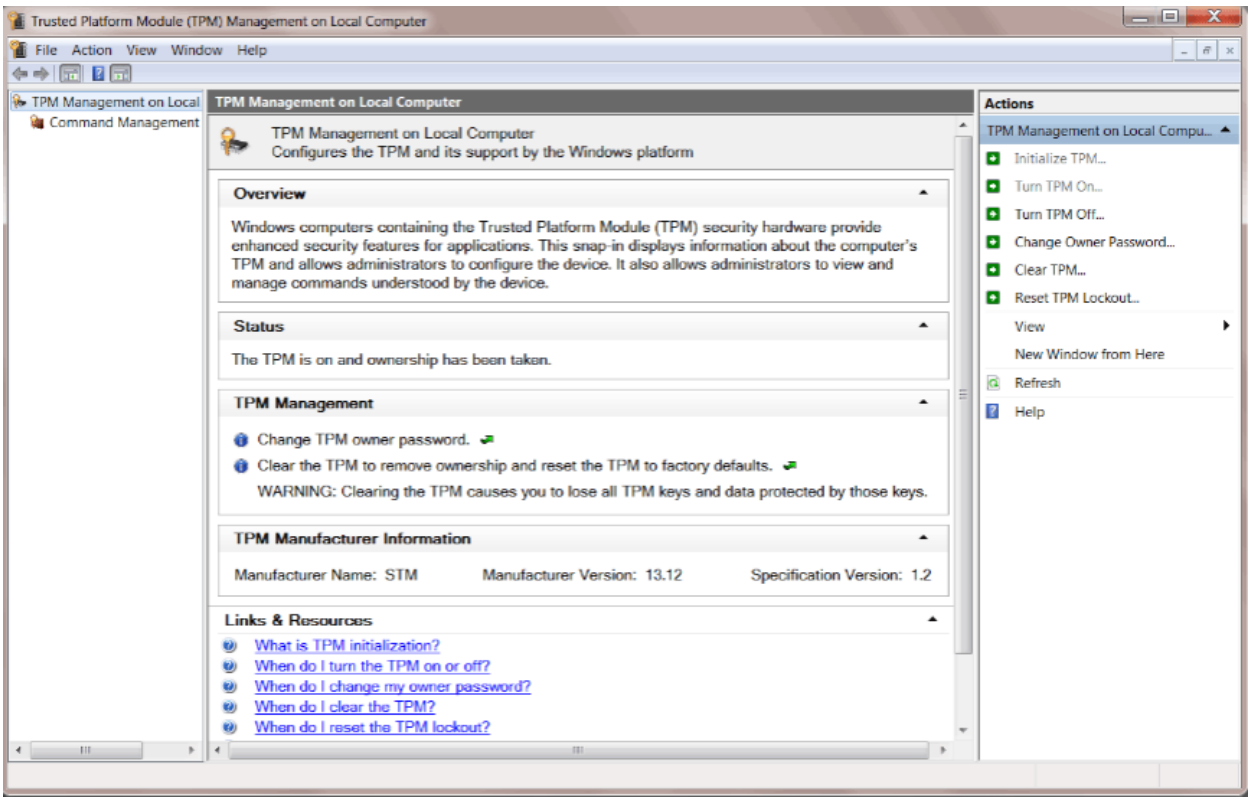


Рис. 8.40 – Перегляд відомостей про довірений платформний модуль

Примітка. Шифрування Bitlocker також можна застосовувати відносно схемних носіїв. Для цього використовується розширення Bitlocker To Go. Для використання Bitlocker To Go не потрібна мікросхема TPM, однак шифрування виконується тим же способом, а для доступу до зашифрованих даних потрібен пароль.

8.2.18 Стирання даних

Захист даних також містить у собі процедури стирання файлів на пристроях зберігання даних, коли ці пристрої стають не потрібні. Простого видалення файлів або переформатування диска може виявитися недостатнім для забезпечення конфіденційності. Наприклад, при видаленні файлів з жорсткого диска вони не видаляються повністю. Операційна система видаляє тільки посилання на файл у таблиці розміщення файлів. Однак самі дані залишаються на диску. Ці дані не видаляються повністю, поки жорсткий диск не збереже інші дані в цім же місці, перезаписавши колишні.

Тому існують програми для відновлення файлів, папок і навіть цілих розділів. Це може виявитися досить корисним, якщо дані були вилучені випадково. Однак якщо диск потрапив у руки зловмисника, відновлення даних може привести до катастрофічних результатів.

Із цієї причини необхідно виконувати повне стирання даних з носія одним із зазначених нижче способів.

- **Програми для стирання даних** – такий спосіб також називають безпечним стиранням, коли за допомогою спеціальної програми виконується багаторазовий перезапис існуючих даних, після чого вони стають непридатними для читання.
- **пристрій, що** розмагнічує (див. рис. 8.41) – це спосіб має на увазі використання пристрою з дуже сильними магнітами, яке підносять близько до магнітних пластин жорсткого диска, у результаті чого пластини розмагнічуються.
- **Електромагнітний пристрій, що** розмагнічує, – використання магніту, на який подається електричний струм, для створення дуже сильного магнітного поля. Такий пристрій дозволяє дуже швидко розмагнітити жорсткий диск.

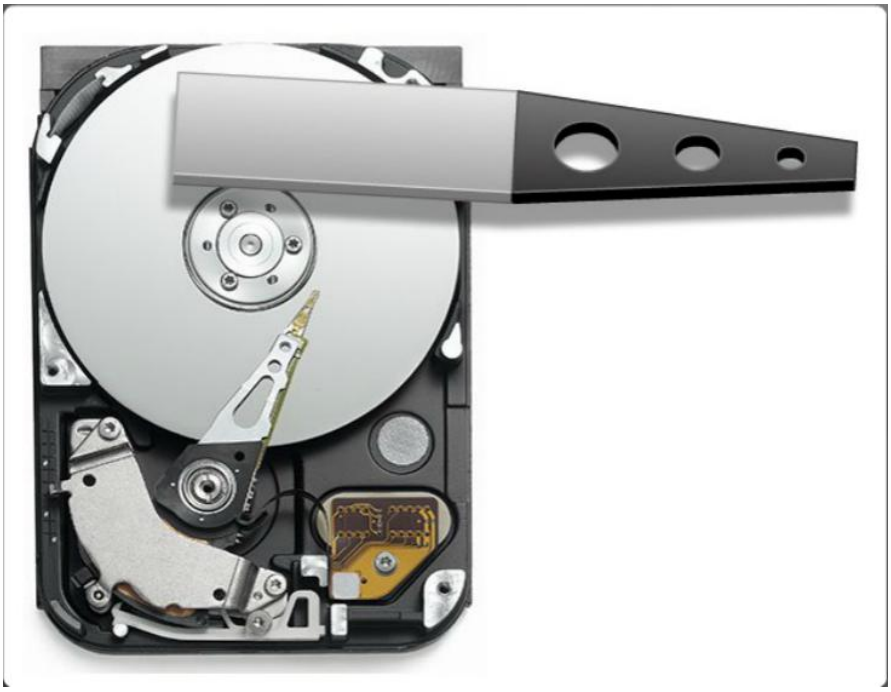


Рис. 8.41 – Пристрій, що розмагнічує

Більш докладно ці методи описані в табл. 8.12

Примітка. Важливо пам'ятати, що стирання даних і розмагнічування диска – необоротний процес, і дані не зможуть бути відновлені.

Твердотільні накопичувачі складаються не з магнітних пластин, а із флеш-пам’яті. Розповсюджені методи видалення даних, такі як розмагнічування, неефективні. Щоб повністю стерти дані з SSD без можливості їх відновлення, виконайте безпечне стирання. Цей же спосіб слід застосовувати й у відношенні гібридних SSD.

Інші носії й документи (наприклад, оптичні диски, EMMC, запам'ятовувальні пристрої USB) слід знищувати. Для цих цілей підійде подрібнювач або установка для спалювання, призначені для знищення документів і

носіїв певного типу. Конфіденційні документи, такі як секретна інформація або паролі, слід завжди зберігати в захищеному місці під замком.

Таблиця 8.12 – Методи стирання даних

Спосіб стирання даних	Опис
Стирання даних	• Корисно у випадках, коли дані на диску час від часу потрібно стирати. • Програмний засіб виконує стирання даних дуже довго. • У такій програмі можуть пропонуватися різні варіанти перезапису даних, включаючи спеціальні шаблони з використанням нулів і одиниць, математичні алгоритми й випадкові біти. • Інструменти стирання даних доступні безкоштовно.
Пристрій, що розмагнічує	• Корисно у випадках, коли дані на диску час від часу потрібно стирати. • Пристрій необхідно піднести до пластин диска приблизно на 2 хвилини. • Коштує набагато дешевше електромагнітного пристрою, що розмагнічує.
Електромагнітний пристрій, що розмагнічує	• Корисно у випадках, коли потрібно стерти дані з декількох дисків. • Стирання даних з жорсткого диска таким способом займає зовсім небагато часу (порядку 10 секунд). • Вартість пристрою, що розмагнічує, може бути досить високої (наприклад, 20 000 доларів США).

Коли мова заходить про стирання або знищення даних із пристроїв, завжди слід пам'ятати, що крім комп'ютерів і мобільних пристроїв, для зберігання даних застосовується безліч інших пристроїв. Принтери й багатофункціональні пристрої можуть оснащуватися жорстким диском, на який кешуються надруковані або скановані документи. У деяких випадках цю функцію кешування можна відключити, а на пристрої можна регулярно виконувати стирання даних для забезпечення їх конфіденційності. По можливості на пристрої рекомендується активувати автентифікацію користувачів, щоб запобігти несанкціонованому доступу до настроювань конфіденційності.

8.2.19 Повторне використання й знищення жорстких дисків

Компаніям, що працюють із конфіденційними даними, завжди слід установлювати чіткі політики утилізації носіїв інформації. Коли носій більше не потрібний, зробити з ним можна двома способами:

- **Повторне використання** – жорсткі диски, на яких було виконане стирання даних, можна використовувати повторно на інших комп'ютерах. Диск можна переформатовати й установити на нього нову операційну систему. У табл. 8.13 зазначено два типи форматування.

Таблиця 8.13 – Знищення жорсткого диска

Спосіб стирання даних	Опис
Стандартне форматування	• Також називається високорівневим форматуванням. • Створюється завантажувальний сектор і на диску настроюється файлова система. Стандартне форматування може бути виконане тільки після завершення низькорівневого форматування.
Низькорівневе форматування	• У ході цієї процедури поверхня диска розмічається мітками секторів, позначаючи місце фізичного збереження даних, і створюються доріжки. • Найчастіше низькорівневе форматування виконується на заводі після виготовлення жорсткого диска.

- **Знищення** – знищивши жорсткий диск, можна бути повністю певен у тому, що дані з нього не підлягають відновленню. Якщо є велика кількість жорстких дисків для знищення, можна скористатися спеціальними пристроями, такими як машини для здрібнювання жорстких дисків, шредери жорстких дисків, установки для їхнього спалювання й багато інші подібні пристрої. Не менш ефективним способом є руйнування жорсткого диска молотком, як показано на рис. 8.42.



Рис. 8.42 – Знищення жорсткого диска

Для знищення носіїв інформації компанії можуть вдаватися до допомоги сторонніх підрядників. Такі підрядники звичайно підписують відповідні зобов'язання й строго додержуються постанов уряду в цім пи-

танні. Вони також можуть надати документ, що підтверджує знищення носія. Такий документ є доказом повного знищення носія.

Визначення термінів по безпеці даних зведені в табл. 8.14

Таблиця 8.14 –Визначення термінів по безпеці даних

Термін по безпеці даних	Опис
Розмагнічування	Містить дуже сильні магніти для розмагнічування пластин жорсткого диска.
Довірений платформний модуль	Потрібно для роботи Bitlocker і активується в BIOS.
Принцип надання мінімальних привілеїв	Користувачам надається доступ тільки до тем ресурсам на комп'ютері й у мережі, які необхідні їм для роботи.
Ключ-брелок безпеки	Невеликий пристрій для двохфакторної автентифікації.
Програмний міжмережевий екран	Програма, що запускається на комп'ютері для дозволу або заборони обміну трафіком між комп'ютером і іншими комп'ютерами, до яких він підключений.

8.3 Програми захисту від шкідливого ПЗ

До шкідливого ПЗ відносять віруси, хробаки, трояни, клавіатурні шпигуни (кейлоггери), програми-шпигуни й рекламне ПЗ. Вони розробляються з метою порушити право користувача на особисте життя, викрасти інформацію, нашкодити комп'ютерній системі, а також видалити або ушкодити дані.

Для захисту комп'ютерів і мобільних пристроїв важливо використовувати надійне ПЗ для захисту від шкідливих програм. Нижче перераховані типи такого ПЗ, яке доступно на сьогоднішній день.

- **Захист від вірусів** – такі програми постійно відслідковують систему на предмет наявності в ній вірусів. При виявленні вірусу програма повідомляє про це користувача й намагається видалити вірус або помістити його в карантин, як показано на рис. 8.43.
- **Захист від рекламного ПЗ** – програми захисту від рекламного ПЗ виконують пошук програм, що відображають рекламу на комп'ютері.
- **Захист від фішингу** – такі програми блокують IP-адреси відомих фішингових веб-сайтів і попереджають користувача про підозрілі сайти.
- **Захист від шпигунського ПЗ** – ці програми перевіряють комп'ютер на наявність клавіатурних шпигунів і іншого шпигунського ПЗ.
- **Надійні/ненадійні джерела** – такі програми попереджають користувача про небезпечні програми й веб-сайтах, які він збирається встановити або відвідати.

Для видалення всього шкідливого ПЗ може знадобитися використовувати кілька різних програм і виконувати пошук кілька раз. Запускайте тільки одну програму захисту від шкідливого ПЗ одночасно.

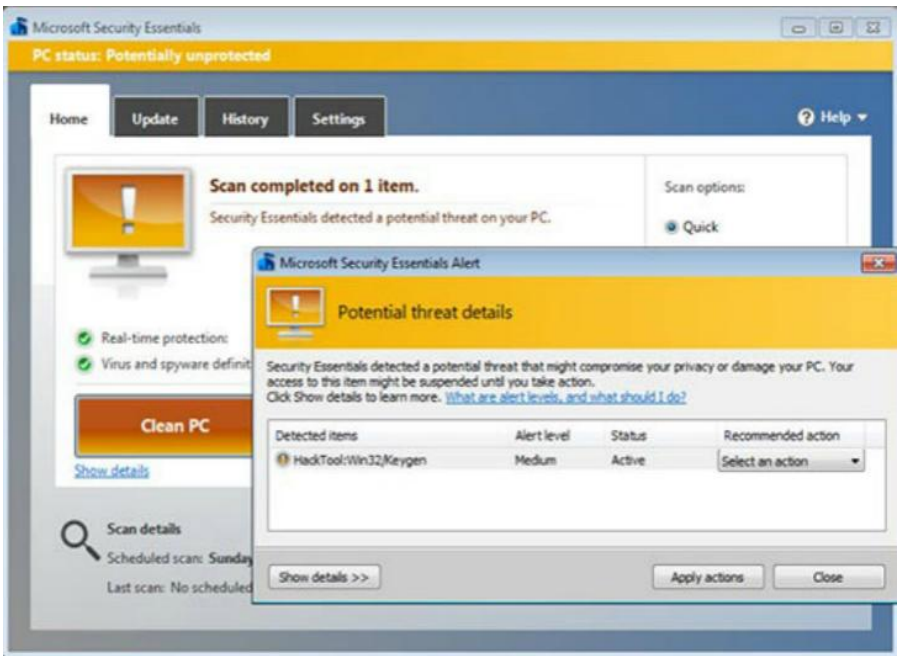


Рис. 8.43 Виявлення вірусів

Деякі авторитетні розроблювачі, такі як Mcafee, Symantec, Kaspersky, пропонують вирішення для комплексного захисту комп'ютерів і мобільних пристроїв.

Слід проявляти обережність при виборі продукту для захисту, оскільки в Інтернеті зустрічаються шахрайські антивіруси. Більшість таких шахрайських антивірусів відображають рекламні або спливаючі повідомлення, схожі на реальні попередження Windows, як показано на рис. 8.44.



Рис. 8.44 – Приклад шахрайського антивірусу

У таких повідомленнях звичайно вказується на те, що комп'ютер заражений і потрібно його очищення. При клацанні в будь-якому місці такого вікна може початися завантаження й установка шкідливого ПЗ.

З появою підозрілого вікна з попередженням ніколи не клацайте це вікно. Закрийте вкладку або оглядач, щоб забрати вікно з попередженням. Якщо вкладка або оглядач не закриваються, натисніть комбінацію клавіш **ALT+F4**, щоб закрити вікно, або використовуйте **диспетчер завдань** для завершення роботи програми. Якщо вікно з попередженням не закривається, перевірте комп'ютер, використовуючи загальновизнану актуальну антивірусну програму, щоб переконатися, що він не заражений.

До незатвердженого або не відповідному до вимог програмному забезпеченню ставляться не тільки програми, які встановлюються на комп'ютер ненавмисно. Це можуть бути програми, надані користувачами з наміром установити їх. Можливо, вони не шкідливі, однак не виключене, що вони можуть порушити політику безпеки. Така система, не відповідна до вимог, може порушити роботу програмного забезпечення компанії або мережних сервісів. Незатверджене програмне забезпечення слід видаляти негайно.

8.3.1 Відновлення заражених систем

Коли програма захисту від шкідливого ПЗ виявляє, що комп'ютер заражений, ***вона видаляє погрозу або поміщає її в карантин.*** Однак, швидше за все, комп'ютер як і раніше перебуває під загрозою.

Перший етап відновлення зараженого комп'ютера – відключення комп'ютера від мережі, щоб не відбулося зараження інших комп'ютерів. Від'єднаєте від комп'ютера всі мережеві кабелі й відключите всі безпроводові підключення.

Потім додержуйтеся вказівок застосовних політик управління інцидентами. У їхнє число може входити повідомлення співробітників відділу ІТ, збереження файлів журналів на знімних носіях або вимикання комп'ютера. Домашнім користувачам необхідно обновити встановлені програми захисту від шкідливого ПЗ або виконати повну перевірку всіх установлених на комп'ютері носіїв. Багато антивірусних програм можуть бути настроєні на запуск до завантаження Windows. Це надає програмі доступ до всіх областей диска без впливу операційної системи або якого-небудь шкідливого ПЗ.

Видалення з комп'ютера вірусів і хробаків може бути важким процесом. Для видалення вірусів і відновлення комп'ютерного коду, зміненого вірусом, потрібні програмні засоби. Ці програмні засоби надаються виробниками операційної системи й компаніями, що випускають ПЗ для забезпечення безпеки. Переконаєтеся, що ви завантажуєте ці засоби зі справжнього сайту виробника.

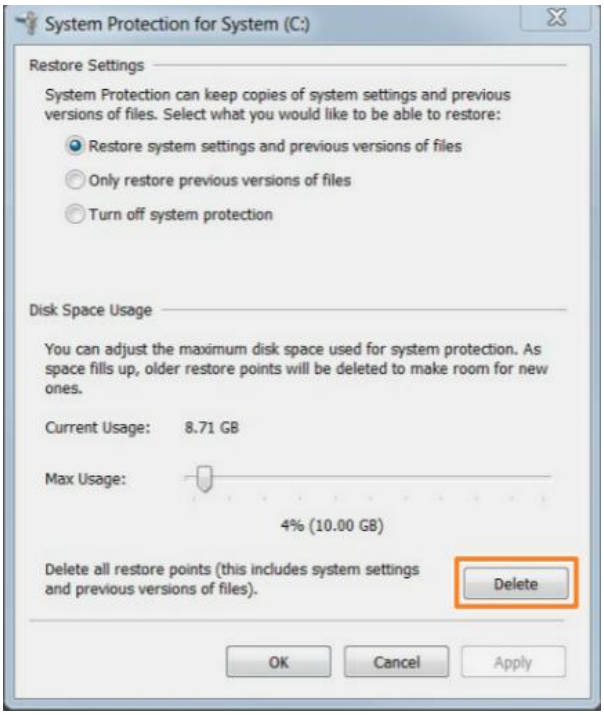


Рис. 8.45 – Видалення точок відновлення

Завантажте комп'ютер у безпечному режимі, щоб уникнути завантаження більшості драйверів. Установите додаткові програми захисту від шкідливого ПЗ й виконайте повну перевірку, щоб вилучити додаткове шкідливе ПЗ або помістити його в карантин. Для повного очищення комп'ютера може знадобитися звернутися до фахівця. У деяких випадках може знадобитися переформатування комп'ютера і його відновлення з резервної копії або ж переустановка ОС.

Служба відновлення системи може включати заражені файли в точку відновлення. Після видалення шкідливого ПЗ на комп'ютеру необхідно видалити файли відновлення системи, як показано на рис. 8.45.

8.3.2 Відновлення файлів сигнатур

Виробники програмного забезпечення повинні регулярно створювати й випускати нові виправлення для усунення помилок і уразливості у продуктах. Оскільки постійно розробляються нові віруси, програмне забезпечення безпеки повинне постійно обновлятися рис. 8.46. Цей процес може виконуватися автоматично, але інженер повинен знати, як обновляти будь-які типи програмного забезпечення безпеки й усі клієнтські програми вручну.

Шкідливі програми шукають шаблони в коді програмного забезпечення на комп'ютері. Ці шаблони визначаються шляхом аналізу вірусів, перехоплених в Інтернеті й локальних мережах. **Ці шаблони коду називаються сигнатурами**. Видавці захисного ПЗ компілюють сигнатури в таблиці визначень вірусів. Перед відновленням файлів сигнатур для захисту від вірусів спочатку переконаєтеся, що використовуються файли сигнатур останньої версії. Для перевірки стану файлу виберіть пункт **Про програму** в програмі для захисту або запустите засіб відновлення програми.

Щоб обновити файл сигнатур, виконаєте зазначені нижче дії.

Крок 1. Створіть точку відновлення Windows. Якщо завантажений файл ушкоджений, настроювання точки відновлення дозволяє повернутися до потрібного моменту.

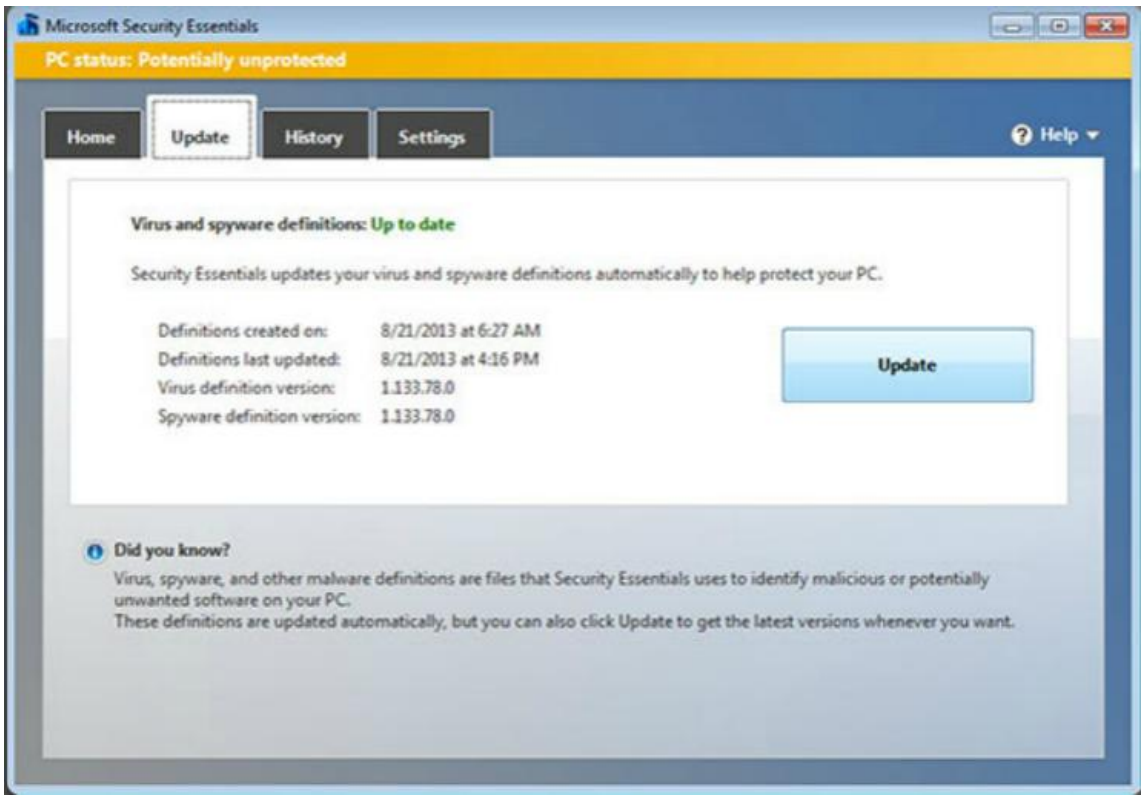


Рис. 8.46 – Відновлення визначень вірусів і шпигунського ПЗ

Крок 2. Відкрийте антивірусну програму. Якщо програма настроєна на автоматичне виконання або одержання відновлення, може знадобитися виключити функцію автоматичного відновлення, щоб виконати ці дії вручну.

Крок 3. Натисніть кнопку **Обновити**.

Крок 4. Після відновлення програми використовуйте її для перевірки комп'ютера.

Крок 5. Після завершення перевірки ознайомтеся зі звітом, щоб знайти віруси або інші проблеми, які не могли бути усунуті, щоб видалити їх самостійно.

Крок 6. Настрійте антивірусну програму на автоматичні відновлення й регулярний запуск.

Завжди одержуйте файли сигнатур з веб-сайту виробника, щоб забезпечити дійсність відновлення й відсутність ушкоджень, викликаних вірусами. Це може створити більше навантаження на веб-сайт виробника, особливо з появою нових вірусів. Щоб уникнути створення надмірного трафіка для одного веб-сайту, деякі виробники випускають файли сигнатур для завантаження на декількох сайтах. Ці сайти завантаження називаються дзеркалами.

УВАГА! При завантаженні файлів сигнатур із дзеркала переконайтеся, що сайт дзеркала не є підробленим. Завжди переходите на сайт дзеркала з веб-сайту виробника.

8.3.3 Розповсюджені типи шифрування зв'язку

Для взаємодії двох комп'ютерів може знадобитися організувати захищений зв'язок. Для цього необхідні наступні протоколи:

- **Використання хеш-коду (контрольної суми)**
- **Симетричне шифрування**
- **Асиметричне шифрування**

Використання хеш-коду або хешування гарантує цілісність повідомлення. Це означає, що повідомлення не буде ушкоджено або фальсифіковане в процесі передачі. Хешування використовує математичну функцію для підрахунку числового значення, називаного дайджестом повідомлення, яке є унікальним для переданих даних. Якщо змінити навіть один символ, то результат функції буде іншим. Функцію неможливо використовувати для зворотного перетворення. Тому знання хеша не дозволяє зловмисникові відновити вихідне повідомлення, що утрудняє перехоплення й зміна повідомлень. Використання хеш-коду проілюстроване на рис. 8.47. Найпоширенішим алгоритмом хешування є **SHA (Secure Hash Algorithm** – алгоритм безпечного хешування, який прийшов на зміну застарілому алгоритму MD5 (Message Digest 5)).



Рис. 8.47 – Використання хеш-коду (контрольної суми)

Симетричне шифрування забезпечує конфіденційність повідомлення. Якщо зашифроване повідомлення буде перехоплено, зрозуміти його вміст не вдасться. Розшифрувати таке повідомлення (тобто прочитати його) можна тільки за допомогою пароля (тобто ключа), за допомогою якого воно було зашифровано. Для симетричного шифрування необхідно, щоб на обох сторонах зашифрованого зв'язку використовувався ключ для шифрування й розшифрування даних. Відправник і одержувач повинні використовувати однакові ключі. Симетричне шифрування показане на рис. 8.48. Прикладами симетричного шифрування служать удосконалений стандарт шифрування **(Advanced Encryption Standard, AES**) і більш старий алгоритм потрійного шифрування даних **(Triple Data Encryption Algorithm, 3DES).**



Рис. 8.48 – Симетричне шифрування

Асиметричне шифрування також забезпечує конфіденційність повідомлення. Для цього потрібні два ключі: закритий (він же секретний або приватний) і відкритий (він же публічний). ***Відкритий ключ*** може вільно поширюватися, включаючи відправлення по електронній пошті у вигляді простого тексту або публікацію в Інтернеті. ***Секретний ключ*** зберігається користувачем і не повинен розкриватися іншим особам. Ці ключі можуть використовуватися двома способами:

- **Шифрування відкритим ключем** використовується, якщо однієї організації необхідно одержати зашифрований текст із декількох джерел. Відкритий ключ може широко поширюватися й використовува-

тися для шифрування повідомлень. ***Передбачуваний одержувач*** – це єдина сторона, що має секретний ключ, яким можна буде розшифрувати повідомлення. Асиметричне шифрування з використанням відкритого ключа показане на рис. 8.49.



Рис. 8.49 – Асиметричне шифрування

- При використанні цифрових підписів для шифрування повідомлень потрібен секретний ключ, а відкритий ключ потрібно для розшифрування повідомлення. Цей підхід дозволяє одержувачеві бути впевненим у джерелі повідомлення, оскільки за допомогою відкритого ключа може бути розшифроване тільки повідомлення, зашифроване за допомогою вихідного секретного ключа. Найпоширенішим алгоритмом асиметричного шифрування є **RSA**.

Примітка. Для симетричного шифрування необхідно, щоб у двох системах був попередньо заданий секретний ключ. В асиметричному же шифруванні потрібно, щоб секретний ключ був тільки в одній із систем.

8.3.4 Ідентифікатори наборів служб (імена мереж)

Оскільки для передачі даних у безпроводових мережах використовуються радіохвилі, зловмисники можуть просто відслідковувати й збирати дані без фізичного підключення до мережі. Зловмисники можуть одержувати доступ до мережі, перебуваючи в діапазоні дії незахищеної

безпроводової мережі. Інженеру потрібно настроїти відповідний рівень безпеки на точках доступу й безпроводових мережних платах.

При установці безпроводових служб необхідно негайно застосувати методи безпеки безпроводового зв'язку для запобігання небажаного доступу до мережі. Для безпроводових точок доступу повинні бути настроєні базові параметри безпеки, сумісні з існуючою безпекою мережі.

Ідентифікатор набору послуг (SSID) – це ім'я безпроводової мережі. Безпроводовий маршрутизатор або точка доступу за замовчуванням віщає ім'я мережі, дозволяючи безпроводовим пристроям виявити безпроводову мережу. Якщо на маршрутизаторі безпроводової мережі або на точці доступу відключене віщання ідентифікатора SSID, як показано на рис. 8.50, щоб підключити пристрій до такої безпроводової мережі, необхідно вручну ввести цей ідентифікатор SSID.

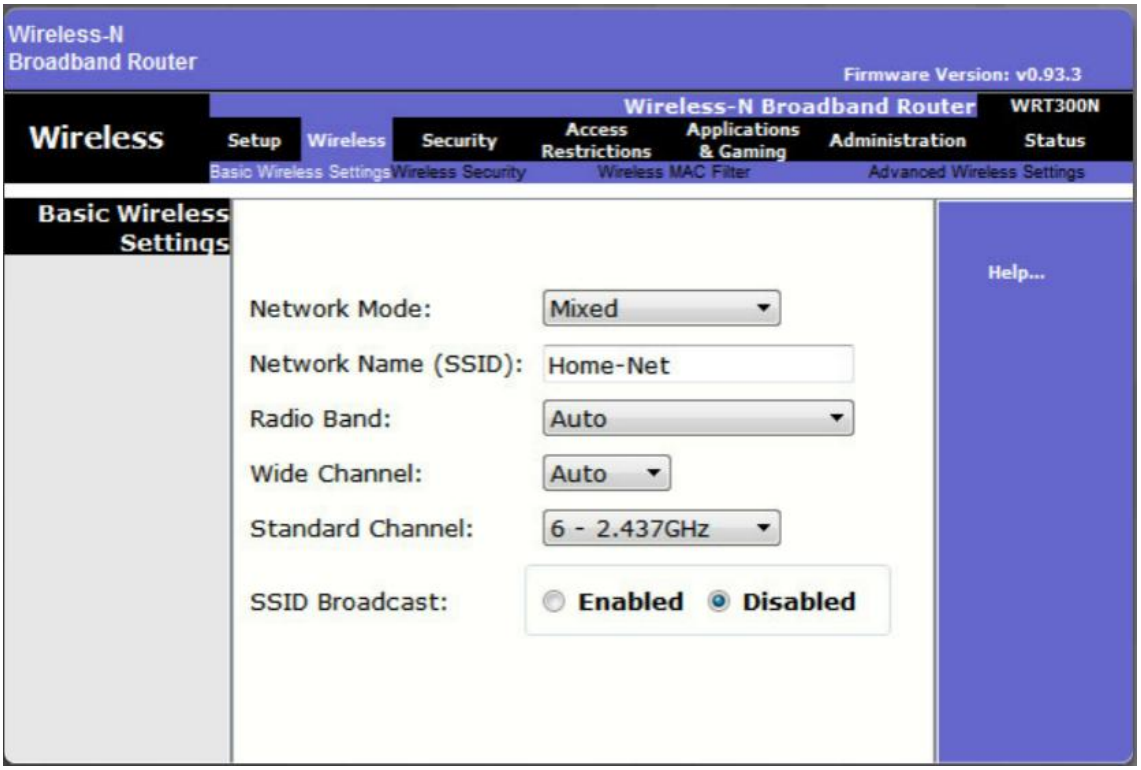


Рис. 8.50 – Відключене віщання імені мережі

Відключення віщання імені мережі забезпечує дуже невеликий рівень безпеки. У цьому випадку користувачу, який прагне підключитися до безпроводової мережі й знає відповідний ідентифікатор SSID, досить увести його вручну. При пошуку безпроводової мережі комп'ютер віщає ім'я мережі. Досвідчений зловмисник може просто перехопити цю інформацію й використовувати її, щоб видати себе за ваш маршрутизатор і перехопити облікові дані.

8.3.5 Режими безпеки безпроводового зв'язку

Використовуйте систему безпроводового шифрування, щоб зашифрувати, що відправляється інформацію й запобігти небажаному перехопленню й використання даних. Більшість точок безпроводового доступу підтримують кілька різних режимів безпеки, які перераховані на рис. 8.51. Як уже згадувалося в попередній главі, по можливості використовуйте режим, що забезпечує найвищий рівень безпеки **(WPA2).**



Рис. 8.51 – Режими безпеки

Багато маршрутизаторів забезпечують захищене настроювання Wi-Fi **(WPS).** WPS дозволяє з легкістю настроїти безпеку мережі Wi-Fi. У цьому режимі для автоматичного настроювання безпечного підключення між пристроями по мережі Wi-Fi на маршрутизаторі й безпроводовому пристрої необхідно натиснути відповідну кнопку. Також нерідко використовуються програмні розв'язки із застосуванням PIN-коду. Важливо відзначити, що WPS не забезпечує необхідний рівень захисту, оскільки він уразливий для атак методом повного перебору. З метою безпеки слід відключити WPS.

8.3.6 Універсальний Plug and Play

Універсальний Plug and Play (Universal Plug and Play, UPNP) – це протокол, що дозволяє пристроям динамічне додавати себе в мережу без участі користувача або якого-небудь настроювання. Незважаючи на зручність,

протокол UPNP не є безпечним, оскільки в ньому не реалізований метод автентифікації пристроїв. Тому він розглядає будь-який пристрій як надійне. Крім того, у протоколі UPNP є ряд уразливостей, пов'язаних з безпекою. Наприклад, шкідливе ПЗ може використовувати UPNP для перенапрямку трафіка на інший IP-Адресу за межами вашої мережі, що потенційно може привести до витоку конфіденційної інформації в руки хакерів.

На багатьох безпроводових маршрутизаторах для домашніх мереж і мереж невеликих офісів протокол UPNP включений за замовчуванням. Тому завжди слід перевіряти конфігурацію маршрутизаторів і ***відключати цей протокол***, як показано на рис. 8.52.

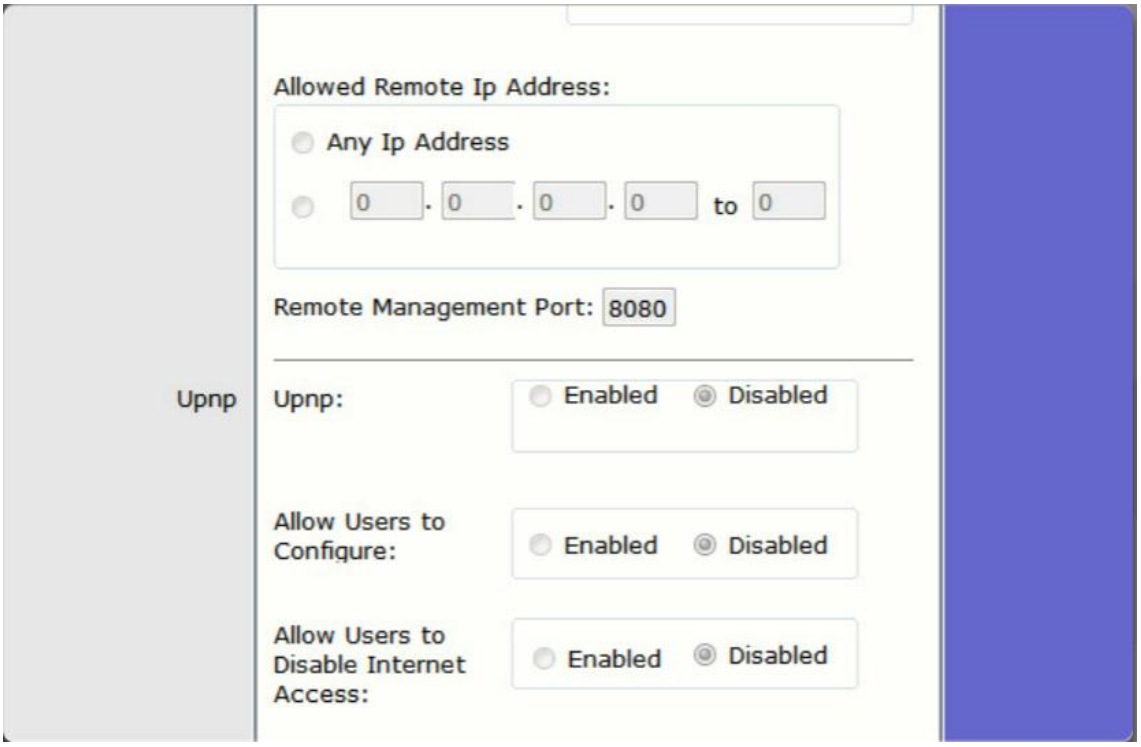


Рис. 8.52 – Відключений протокол UPNP

Дослідницька компанія Gibson Research Corporation (GRC) пропонує різні безкоштовні браузерні засоби для аналізу уразливостей. Клацніть здесь, щоб скористатися таким засобом, розробленим GRC, і перевірити свій безпроводовий маршрутизатор на предмет уразливостей UPNP.

8.3.7 Оновлення мікропрограмного забезпечення

Мікропрограмне забезпечення (прошивання) більшості безпроводових маршрутизаторів можна обновляти. У оновленнях мікропрограми можуть утримуватися виправлення розповсюджених проблем, про яких повідомляли замовники, а також виправлення, що дозволяють усунути уразливості в системі безпеки. Рекомендується регулярно перевіряти наявність оновленого мікропрограмного забезпечення на веб-сайті ви-

робника пристрою. Після завантаження мікропрограми її можна завантажити на безпроводовий маршрутизатор за допомогою графічного інтерфейсу користувача, як показано на рис. 8.53.

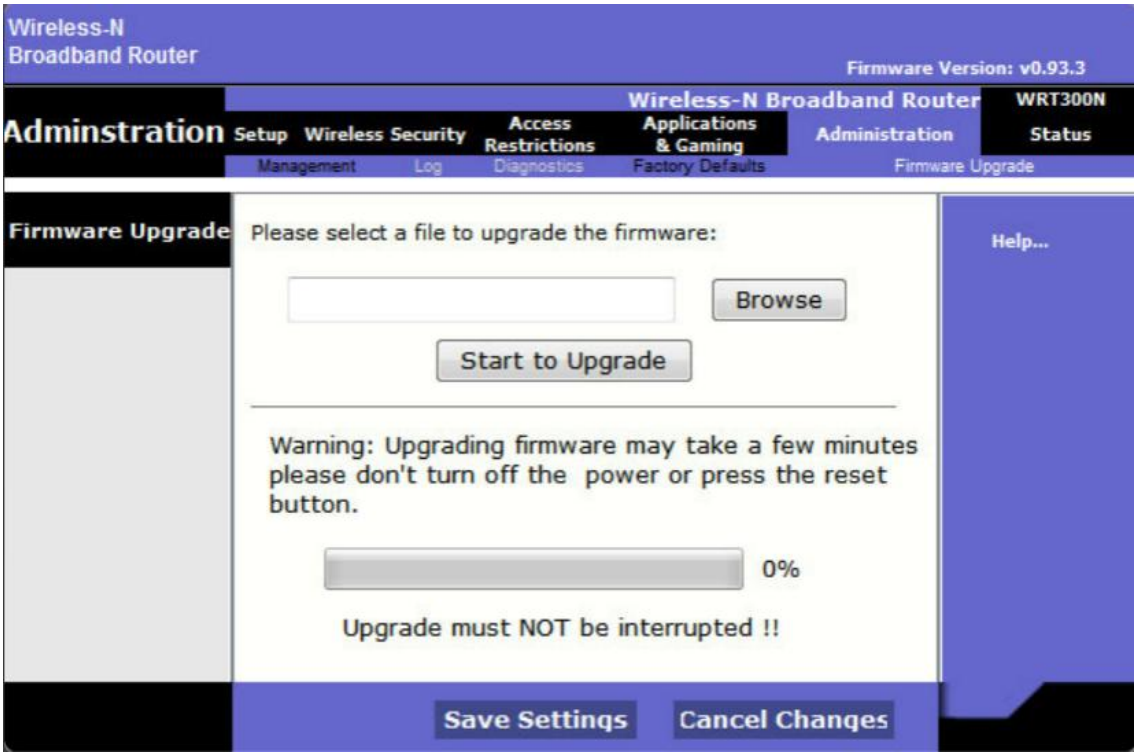


Рис. 8.53 – Відновлення мікропрограмного забезпечення

У процесі оновлення мікропрограми користувачі будуть відключені від безпроводової локальної мережі й Інтернету. Для поновлення звичайної роботи безпроводовому маршрутизатору може знадобитися кілька перезавантажень.

8.3.8 Міжмережеві екрани

Апаратний міжмережевий екран – це фізичний компонент фільтрації, перевіряючий пакети даних з мережі перед тем, як вони потраплять на комп'ютери й інші пристрої в мережі. **Апаратний міжмережевий екран** – це окремий пристрій, який не використовує ресурси комп'ютерів, що захищаються їм, тим самим не впливаючи на продуктивність. Міжмережевий екран може бути настроєний на блокування окремих портів, діапазону портів або навіть трафіка певного додатка. Більшість бездротових маршрутизаторів оснащуються вбудованим апаратним міжмережевим екраном.

Апаратний міжмережевий екран пропускає в мережу два типи трафіка:

- Відповідний трафік на запити, відправлені із внутрішньої мережі.
- Трафік на порти, які навмисно залишені відкритими.

Існує кілька типів апаратних міжмережевих екранів:

- **Фільтр пакетів** – пакети можуть пройти через міжмережевий екран, тільки якщо вони відповідають набору правил, настроєних на міжмережевому екрані. Фільтрація трафіка може здійснюватися на основі різних атрибутів, таких як IP-адреса відправника, порт відправника або Ip-Адреса або порт призначення. Фільтрація трафіка також може бути виконана на основі служб призначення або протоколів, таких як WWW і FTP.
- **Аналіз пакетів з відстеженням стану (Stateful packet inspection, SPI)** – це міжмережевий екран, що відслідковує стан мережевих підключень, що проходять через нього. Пакети, що не ставляться до відомих підключень, відкидаються. На рис. 8.54 показаний міжмережевий екран із включеною функцією SPI.
- **Міжмережевий екран рівня додатків** – усі пакети, що виходять від додатка або призначені йому, перехоплюються. Увесь небажаний вхідний трафік не досягає захищених пристроїв.
- **Проксі** – це міжмережевий екран, установлений на проксі-сервері, перевіряючий увесь трафік і розв'язний або відхиляючий пакети на основі настроєних правил. **Проксі-сервер** – це сервер ретрансляції між клієнтом і сервером призначення в Інтернеті.

Програмні й апаратні міжмережеві екрани захищають дані й обладнання в мережі від несанкціонованого доступу. Крім програмного забезпечення безпеки, необхідно використовувати міжмережевий екран.

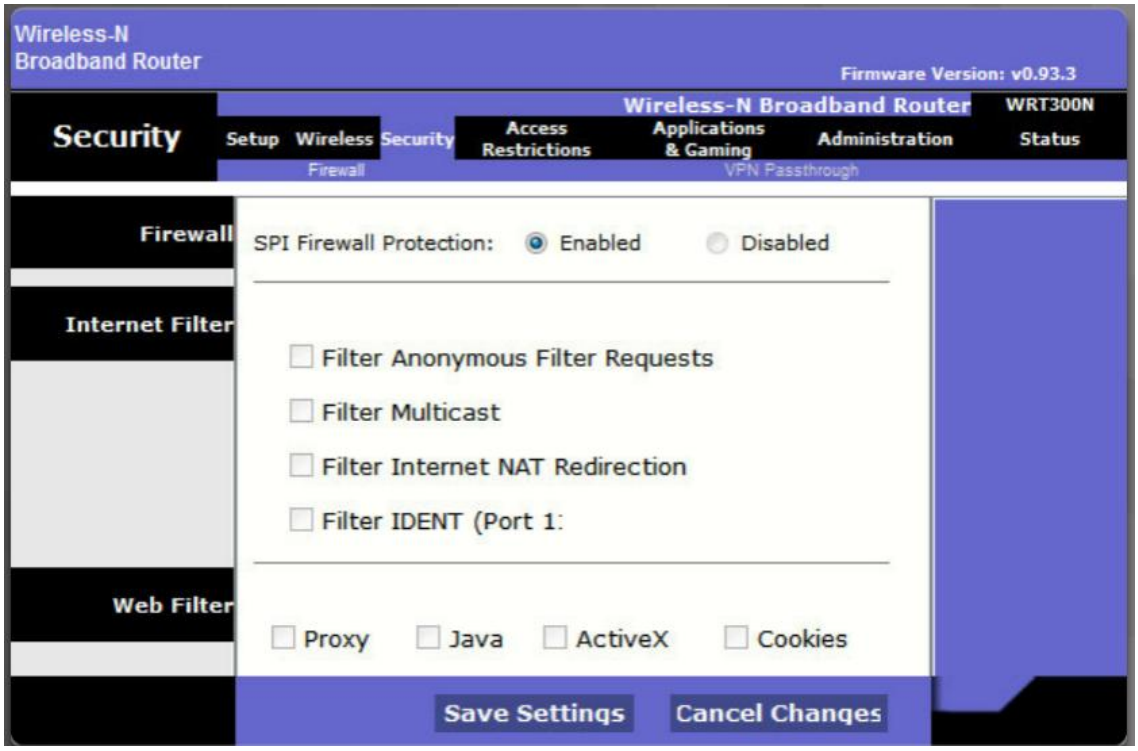


Рис. 8.54 – Захист за допомогою функції SPI міжмережевого екрана

У табл. 8.15 наведене порівняння програмних і апаратних міжмережевих екранів.

Таблиця 8.15 – Порівняння програмних і апаратних міжмережевих екранів

Апаратний міжмережевий екран	**Програмний міжмережевий екран**
Спеціалізований компонент обладнання	Доступний як програмне забезпечення сторонніх виробників, вартість різниться
Вихідна вартість оновлень обладнання й програмного забезпечення може бути дуже високою	Безкоштовна версія входить до складу операційної системи Windows
Може бути захищено кілька комп'ютерів	Звичайно захищає тільки комп'ютер, на якому встановлений
Не впливає на продуктивність комп'ютера	Використовує ресурси комп'ютера, що може потенційно вплинути на продуктивність системи

Демілітаризована зона

Демілітаризована зона (DMZ) – це підмережа, що обслуговує недовірений сегмент мережі. В DMZ часто розміщаються поштові сервери, веб-сервери або сервери FTP, щоб відокремити трафік для серверів і трафік для внутрішньої локальної мережі. Це захищає внутрішню мережу від атак із зовнішньої мережі, але ніяк не захищає сервери в DMZ. Трафік в DMZ і з неї часто захищається міжмережевим екраном або проксі.

На бездротовому маршрутизаторі можна створити DMZ для одного пристрою шляхом пересилання трафіка із усіх портів з боку Інтернету на певний IP– або MAC-Адреса. В DMZ може перебувати сервер, ігровий комп'ютер або веб-камера, щоб ці пристрої були доступні всім. Однак пристрій в DMZ піддане атакам хакерів через Інтернет.

8.3.9 Переадресація й включення портів

Апаратні міжмережеві екрани можуть використовуватися для блокування портів з метою запобігання несанкціонованого доступу в локальну мережу або з мережі. Однак у деяких випадках необхідно відкрити деякі порти, щоб певні програми й додатки могли зв'язуватися із пристроями в інших мережах. Переадресація (також перенапрямок або кидок) портів (port forwarding) – це спосіб напрямку трафіка між пристроями в різних мережах на основі правил.

Коли трафік досягає маршрутизатора, маршрутизатор визначає, повинен чи трафік пересилатися певному пристрою, на основі номера порту, знайденого в трафіку. Номера портів пов'язані з певними службами, такими як FTP, HTTP, HTTPS і POP3. Правила визначають, який трафік направляється в локальну мережу. Наприклад, маршрутизатор може бути настроєний на перенапрямок порту 80, який пов'язаний з HTTP. Коли маршрутизатор одержує пакет з портом призначення 80, він пересилає

трафік серверу в мережі, що обслуговує веб-сторінки. На рис. 8.55 показане, що на маршрутизаторі включений перенапрямок для порту 80 на веб-сервер, розміщений по Ip-Адресі 192.168.1.254.



Рис. 8.55 – Перенапрямок портів на веб-сервер

Включення портів (port triggering) дозволяє маршрутизатору тимчасово переадресовувати дані через вхідні порти певному пристрою. Включення портів можна використовувати для переадресації даних на комп'ютер, тільки якщо призначений діапазон портів використовується для створення вихідного запиту. Наприклад, відеогра може використовувати порти 27000-27100 для зв'язку з іншими гравцями. порти, що це запускають. Клієнт чата може використовувати порт 56 для зв'язку із цими ж гравцями, щоб вони могли спілкуватися один з одним. Якщо в цьому прикладі існує ігровий трафік на вихідному порту з діапазоном портів, що запускають, входить трафік чата на порту 56 перенаправляється на комп'ютер, використовуваний для відеогри й спілкування із друзями. Коли гра завершується порти, що й запускають, більше не використовуються, порту 56 більше не буде дозволено пересилати якийнебудь трафік цьому комп'ютеру.

8.4 Способи захисту фізичного обладнання

Фізична безпека так само важлива, як і безпека даних. При розкраданні комп'ютера також відбувається крадіжка даних. Важливо обмежити доступ до приміщень за допомогою заборів, замків і дверей. Наприклад, для запобігання проходу «паровозиком» часто застосовуються тамбури-шлюзи, які являють собою невеликі кімнати із двома дверима. Щоб відкрити одну з них, необхідно обов'язково закрити іншу. Захистите інфраструктуру мережі, наприклад, кабелі, телекомунікаційне обладнання й мережеві пристрої, за допомогою наступних заходів:

- Захищені телекомунікаційні кімнати, відсіки для обладнання й кожухи
- Кабельні замки й захисні гвинти для обладнання
- Безпроводове визначення несанкціонованих точок доступу
- Апаратні міжмережеві екрани
- Система управління мережею, що визначає зміни в комутації й комутаційних панелях
- Безпроводові пристрої для запобігання механічного від'єднання проводів

Паролі BIOS/UEFI

Паролі, установлювані для входу користувачів в операційну систему Windows, Linux або MAC, не дозволяють захистити комп'ютер від завантаження з компакт-диска або флеш-диска з іншої операційною системою. Після завантаження з такого носія зловмисник може одержати доступ до ваших файлів або стерти їх. Щоб запобігти несанкціонованому завантаженню ПК або ноутбука, установите пароль для BIOS або UEFI. Хоча найкращим способом захисту даних визнане шифрування вмісту жорсткого диска, існують ситуації, коли підходить саме установка пароля для BIOS або UEFI. Наприклад, такий спосіб захисту підходить для загальнодоступних комп'ютерів. Пароль BIOS або UEFI досить складно скинути. Тому його слід запам'ятати.

Автоматичне виконання й автоматичний запуск

Автоматичне виконання (Autorun) – це функція Windows, що автоматично виконує інструкції, що втримуються в спеціальному файлі (**autorun.inf**), при підключенні флеш-диска або вставці компакт– або DVD-диска в привод оптичних дисків. Функція автоматичного запуску відрізняється від автоматичного виконання. Функція автоматичного запуску (Autoplay) – зручний спосіб визначення установки або підключення до комп'ютера нових носіїв, таких як оптичні диски, зовнішні жорсткі диски або флеш-карти пам'яті. Функція автоматичного запуску запитує в користувача вибір дії на основі вмісту нового носія, наприклад запустити програму, включити відтворення музики або перегляд мультимедіа.

В Windows спочатку запускається функція автоматичного виконання, якщо вона не відключена. Якщо функція автоматичного виконання не відключена, вона виконує команди у файлі autorun.inf. Починаючи з Windows Vista, функції автоматичного виконання забороняється обходити автоматичний запуск. Однак все-таки залишається ризик ненавмисно запустити шкідливе ПО з діалогового вікна автоматичного завантаження. Тому з метою безпеки слід визначити список програм, яким дозволяється використовувати функцію автоматичного виконання. Найбільш безпечним вирішенням буде відключити цю функцію, як показано на рис. 8.56. У всіх версіях Windows, починаючи з Windows Vista параметр, що відповідає, перебуває **в розділі Панель управління** > Автозапуск.

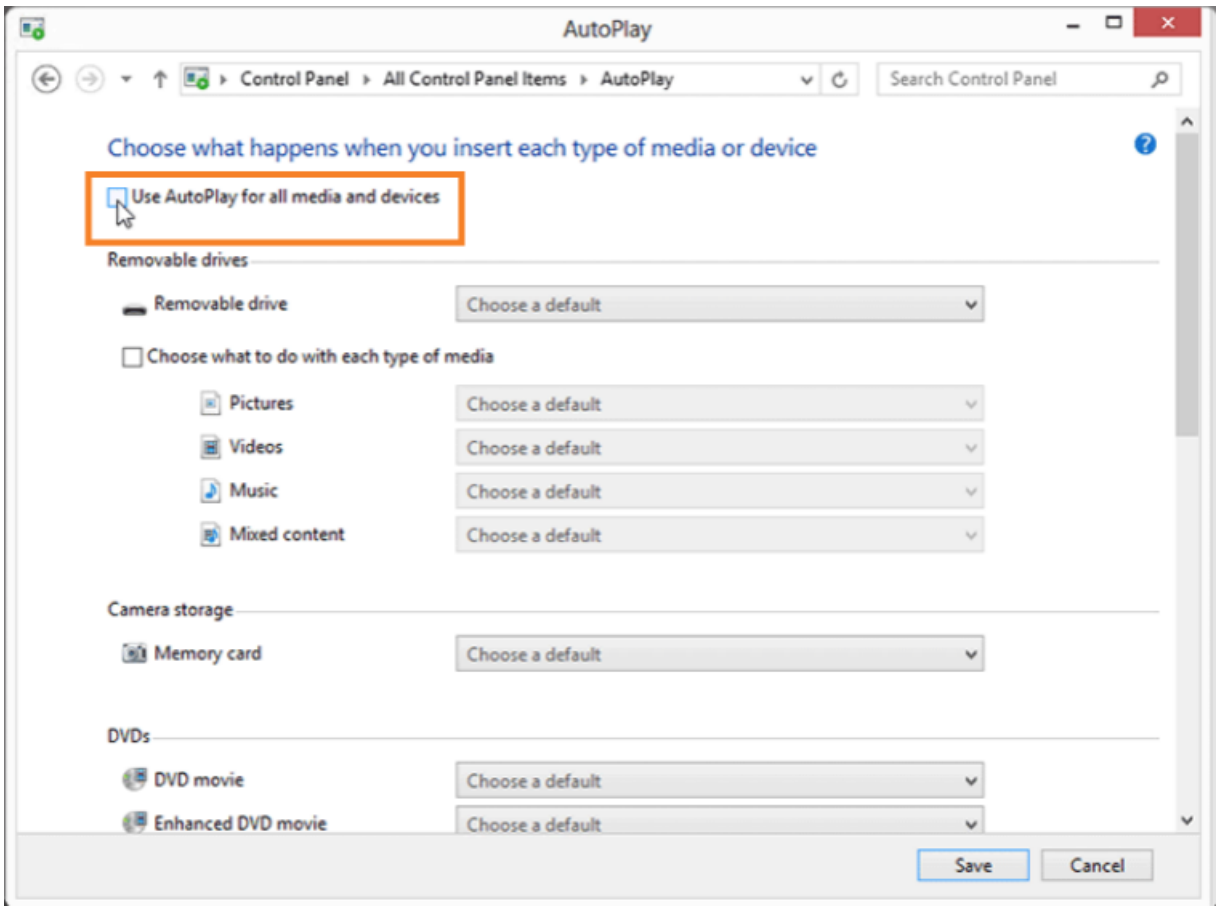


Рис. 8.56 – Відключення автоматичного запуску

Багатофакторна автентифікація

Раніше ми розглядали двохфакторну автентифікацію на прикладі ключа-брелка безпеки. Двома факторами є те, що вам відомо, наприклад, пароль, і те, що у вас є, наприклад, ключ-брелок безпеки. У багатофакторній автентифікації додатково застосовується біометричний параметр користувача, такий як відбиток пальця, як показано на рис. 8.57. При плануванні системи безпеки бюджет на спеціальне устаткування слід визначати виходячи із цінності даних або обладнання, які слід захистити.

Концепція BYOD

Крім корпоративних мобільних пристроїв, необхідно також забезпечити захист особистих мобільних пристроїв співробітників. Раніше в рамках корпоративної інфраструктури можна було користуватися тільки пристроями компанії. Однак значний ріст обсягів особистих пристроїв вніс свої корективи у відношення компаній до використання особистих пристроїв співробітників на робочому місці: практично всі компанії впровадили у свою практику концепцію BYOD. Одна із самих складних завдань, з якої зустрічаються компанії, полягає у визначенні того, у якому ступені компанія може контролювати використання особистого пристрою співробітника. Безсумнівно, важлива, конфіденційна й службова інформація повинна бути захищена в кожному разі – не важливо, хто во



Рис. 8.57 – Сканування відбитків пальців

лодіє пристроєм. Концепція BYOD може заощадити для компанії чималі гроші, однак користувач повинен прийняти її й додержуватися вимог цієї концепції. Іншим завданням є забезпечення конфіденційності співробітника. Коли співробітник передає частину функцій управління своїм пристроєм, він тим самим довіряє компанії частина своїх особистих відомостей.

Вимоги профілю безпеки

Для захисту мобільних пристроїв рекомендується створювати й застосовувати профілі безпеки. Профіль безпеки звичайно являє собою текстовий файл із параметрами безпеки й конфігурації пристрою. Ці параметри можна застосовувати як до пристрою, так і до певного користувача або групи користувачів. Також можна застосовувати відразу кілька профілів одночасно. Звичайно для пристроїв, використовуваних у рамках концепції BYOD, і корпоративних пристроїв застосовуються різні профілі безпеки. Вимоги таких профілів безпеки залежать від ролі окремого співробітника або групи працівників, типу пристрою й операційної системи, а також від політик, застосовуваних в організації.

8.4.1 Захисне обладнання

У число заходів фізичного контролю доступу входять замки, відеоспостереження й охорона табл. 8.16. Ключ-карти захищають фізичний доступ до приміщень. При втраті або крадіжці ключ-карти повинна бути дезактивована тільки відсутня карта. Система ключ-карти більш дорога, чім замки безпеки, але при втраті звичайного ключа необхідно замінити або перекодувати замок.

Мережеве обладнання повинне бути змонтоване в захищених приміщеннях. Усі кабелі повинні перебувати в закритих кабель-каналах або бути прокладені в стінах для запобігання несанкціонованого доступу або ушкодження. Кабель-канали захищають середовища передачі даних і інфраструктуру від ушкодження й несанкціонованого доступу. Невикористовувані мережеві порти повинні бути відключені.

Таблиця 8.16 – Пристрої контролю доступу на об'єкті й відповідні описи

Пристрої контролю доступу	Опис
Ідентифікаційні картки з фотографіями	Пристрої для відображення зовнішності користувача
Картки радіочастотної ідентифікації (RFID)	Датчики для відстеження місцезнаходження й доступу
Картки-ключі	Пристрої для зберігання інформації про користувача й рівень доступу
Біометричні датчики	Пристрої для визначення фізичних характеристик користувача
Тросові замки	не використовуються

Біометричні пристрої, що вимірюють фізичні характеристики користувача, ідеально підходять для приміщень із високою безпекою. Однак для невеликих організацій цей тип вирішення є занадто дорогим. У політику безпеки повинне визначатися апаратне забезпечення й обладнання, яке може використатися для запобігання крадіжок, вандалізму або втрати даних. Фізичний захист включає чотири взаємозалежні аспекти: доступ, дані, інфраструктура й фізичний комп'ютер.

Існує кілька способів організувати фізичний захист обладнання комп'ютера.

- Використовуйте кабельні замки для обладнання, як показано на рис. 8.58.
- Закривайте телекомунікаційні приміщення.
- Установите на обладнанні захисні гвинти.
- Використовуйте захисні кожухи для обладнання.
- Настроюйте й установлюйте датчики, такі як наклейки радіочастотної ідентифікації, на обладнанні.



Рис. 8.58 – Кабельний замок для ноутбука

- Установите фізичну сигналізацію з датчиками руху.
- Використовуйте веб-камери із програмним забезпеченням для визначення руху й спостереження.

Існує кілька засобів захисту доступу до приміщень:

- Ключ-карти, на яких збережені дані користувача, включаючи рівень доступу
- Електронні пропуски з фотографією
- Біометричні датчики для визначення фізичних характеристик користувача, таких як відбитки пальців
- Пости охорони

- Датчики, такі як електронні пропуски з радіочастотною ідентифікацією, для відстеження доступу й переміщення співробітників у будинках.

Використання корпусів із замками, кабельних замків і замків для док-станцій портативних комп'ютерів для захисту комп'ютерів від переміщення. Використання контейнерів, що защіпаються, для переносу жорстких дисків, а також надійне зберігання й перевезення резервних носіїв для захисту даних і носіїв від розкрадання.

Захист використовуваних даних

За допомогою захисного екрана можна гарантувати, що сторонні не підглянуть інформацію, відображувану на моніторі. Захисний екран являє собою панель, часто виготовлену із пластику. Він перешкоджає проходженню світла при гострих кутах падіння, тому екран може бачити тільки користувач, що дивиться на нього прямо. Наприклад, у літаку користувач може захистити екран портативного комп'ютера від імені, що сидить поруч.

Правильна комбінація засобів безпеки

У число факторів, що визначають найбільш ефективне обладнання безпеки, використовуване для захисту обладнання й даних, входять наступні:

- Спосіб використання обладнання
- Місце розташування комп'ютерного обладнання
- Необхідний тип доступу користувача до даних

Наприклад, для комп'ютера в популярному громадському місці, такому як бібліотека, потрібна додатковий захист від крадіжки й вандалізму. В активно працюючому кол-центрі сервер звичайно встановлюється в закритій кімнаті для обладнання. При необхідності використання портативного комп'ютера в громадському місці апаратний ключ безпеки й ключ-брелок забезпечують блокування системи, якщо користувач відходить від комп'ютера табл. 8.17.

Таблиця 8.17 – Визначення пристроїв забезпечення фізичної безпеки

Пристрій забезпечення фізичної безпеки	**Опис пристрою**
Біометричний пристрій	Використовує фізичні характеристики користувача для перевірки автентичності.
Смарт-Карта	Використовує вбудовану інтегральну схему для безпечного зберігання даних.
Ключ-Брелок	Використовує невелику радіосистему для зв'язку з комп'ютером.

8.5 Пакети відновлення й виправлення безпеки операційної системи

Виправлення – це оновлення коду, що випускаються виробниками для запобігання атак нових виявлених вірусів і хробаків. Періодично виробники поєднують виправлення й оновлення в комплексні додатки відновлення, які називаються пакетами оновлення рис. 8.59. Багато руйнівних атак вірусів могли бути менш серйозними, якби більше число користувачів завантажило й установило останній пакет оновлення.

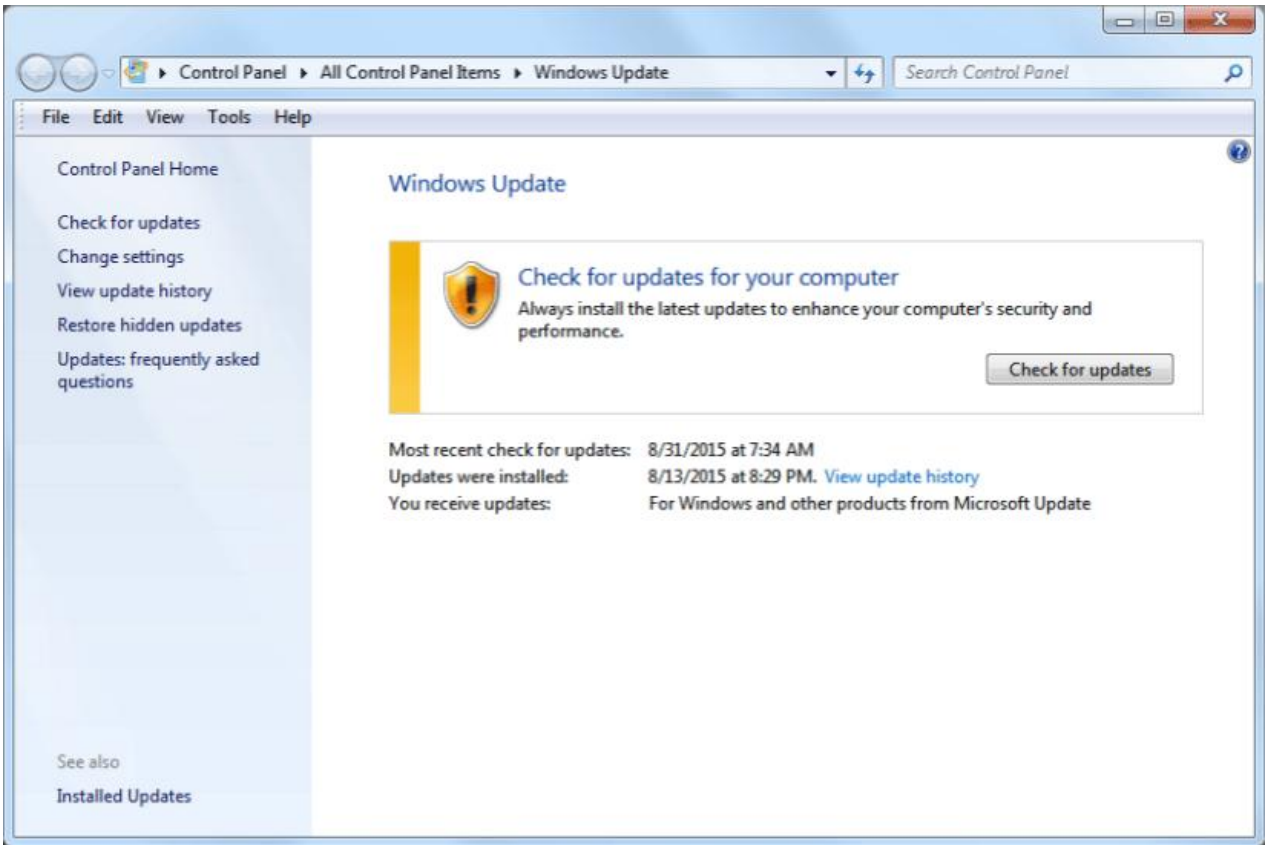


Рис. 8.59 – Центр оновлення Windows

Операційна система Windows регулярно перевіряє наявність на веб-сайті Центру оновлення Windows високопріоритетних оновлень для захисту комп'ютера від останніх погроз безпеки. У число цих оновлень входять оновлення безпеки, критичні оновлення й пакети оновлення. Залежно від обраного варіанта Windows автоматично завантажує й установлює високопріоритетні оновлення, необхідні комп'ютеру, або повідомляє про наявність таких оновлень. Процедури оновлення Windows були розглянуті в попередній главі.

8.5.1 Резервне копіювання даних

Можна виконати резервне копіювання Windows вручну або запланувати частоту автоматичного резервного копіювання. Для успішного резервного копіювання й відновлення даних в Windows потрібні відповідні права й дозволи користувача.

- Усі користувачі можуть виконувати резервне копіювання власних файлів і папок. Вони також можуть виконувати резервне копіювання файлів, на які в них є дозвіл на читання.
- Усі користувачі можуть відновлювати файли й папки, на які в них є дозвіл на запис.
- Члени групи адміністраторів, оператори архіву й оператори сервера (якщо приєднані до домену) можуть виконувати резервне копіювання й відновлення всіх файлів незалежно від призначених дозволів. За замовчуванням члени цих групи мають права на резервне копіювання й відновлення файлів і каталогів.

Для першого запуску майстра резервного копіювання файлів Windows 7 послідовно виберіть наступні пункти:

Панель управління > Архівація й відновлення > Настроїти архівацію

Щоб запустити майстер резервного копіювання файлів Windows Vista, виберіть наступні пункти:

Панель управління > Центр архівації й відновлення > Архівувати файли

Починаючи з Windows 8, параметри резервного копіювання й відновлення перебувають у розділі «Історія файлів», як показано на рис. 8.60.

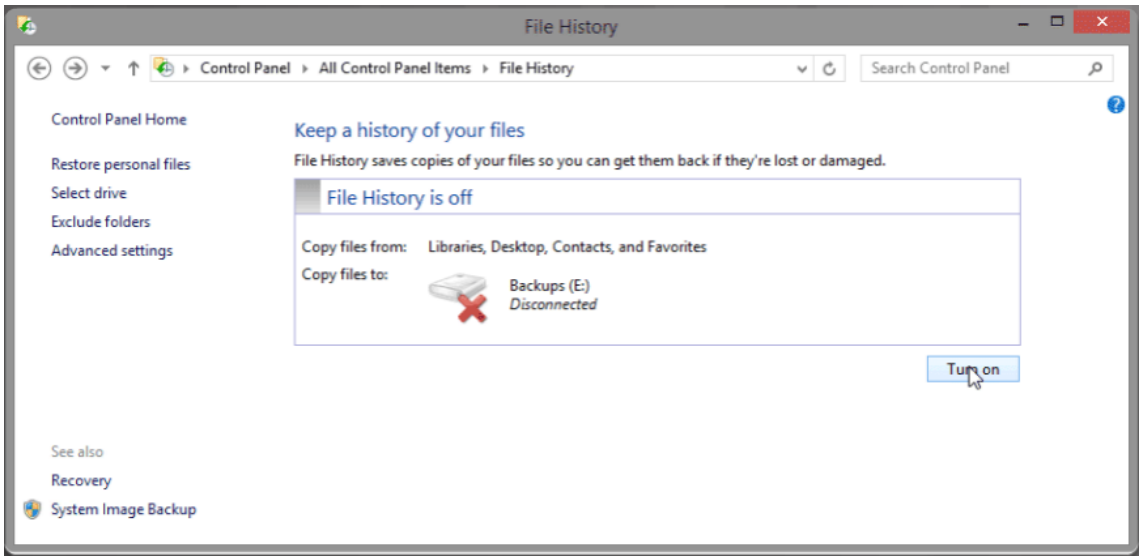


Рис. 8.60 – Історія файлів

В ОС Windows 8 і 8.1 виберіть наступні пункти:

Панель управління > Історія файлів > Включити

Буде потрібно вибрати розташування для зберігання історії файлів. Для цього підходить інший внутрішній або зовнішній жорсткий диск, а також мережеве розташування. Резервне копіювання даних займає якийсь час, тому рекомендується виконувати його при низькому завантаженню комп'ютера й мережі.

Клацніть пункт «Додаткові параметри», щоб змінити параметри резервного копіювання, як показано на рис. 8.61.

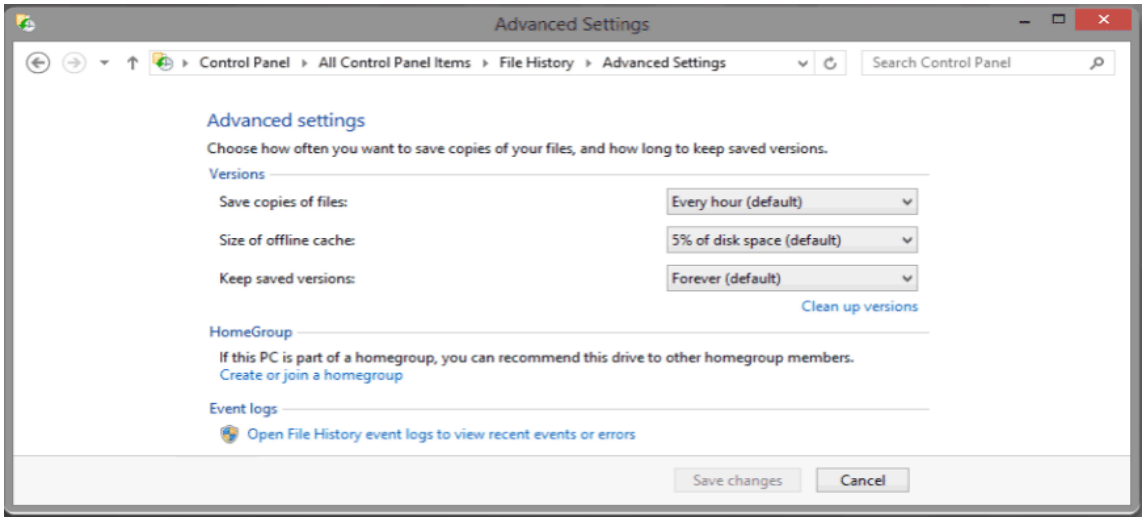


Рис. 8.61 – Додаткові параметри

8.5.2 Брандмауер Windows

Брандмауер вибірково відхиляє трафік, призначений комп'ютеру або сегменту мережі. Брандмауери працюють шляхом відкриття й закриття портів, використовуваних різними додатками. Заборонна політика безпеки реалізується шляхом відкриття тільки тих портів, які необхідні. Відхиляються всі пакети, що не мають явного дозволу. На відміну від цього розв'язна політика безпеки дозволяє доступ до портів, за винятком явно закритих портів. У минулому програмне забезпечення й устаткування поставлялися з дозвільними параметрами. Оскільки користувачі зневажали настроюванням свого обладнання, дозвільні параметри, установлені за замовчуванням, відкривали зловмисникам доступ до безлічі пристроїв. Тепер більшість пристроїв по можливості поставляються із заборонними параметрами й з можливістю простого настроювання.

Настроїти брандмауер Windows або Windows Vista можна двома способами:

- **Автоматично** – користувачеві пропонується «Блокувати», «Розблокувати» або «Відкласти» несанкціоновані запити. Ці запити можуть виходити як від звичайних додатків, які просто ще не встигнули настроїти, так і від вірусів і хробаків, що заразили систему.
- **Управління параметрами безпеки** – користувач вручну додає програму або порти, необхідні додаткам для використання в мережі.

Щоб надати програмам доступ через брандмауера Windows в Windows 7, послідовно виберіть наступні пункти:

Панель управління > Брандмауер Windows > Дозволити запуск програми або компонента через брандмауера Windows > Дозволити іншу програму

Щоб надати програмам доступ через брандмауера Windows в Windows Vista, послідовно виберіть наступні пункти:

Панель управління > Центр безпеки > Брандмауер Windows > Змінити параметри > Продовжити > Виключення > Додати програми

Щоб надати програмам доступ через брандмауера Windows в Windows 8 і 8.1, послідовно виберіть наступні пункти:

Панель управління > Брандмауер Windows > Дозвіл взаємодії з додатком або компонентом у брандмауерові Windows > Змінити параметри > Дозволити інший додаток

Якщо планується використовувати інший брандмауера, необхідно відключити брандмауера Windows. Щоб відключити брандмауер Windows в Windows 7, послідовно виберіть наступні пункти:

Панель управління > Брандмауер Windows > Включення й відключення брандмауера Windows > Відключити брандмауер Windows (не рекомендується) > ОК

Щоб відключити брандмауер Windows в Windows Vista, послідовно виберіть наступні пункти:

Панель управління > Центр безпеки > Брандмауер Windows > Включення й відключення брандмауера Windows > Продовжити > Виключити (не рекомендується) > ОК

Щоб відключити брандмауер Windows в Windows 8 і 8.1, як показано на рис. 8.62, послідовно виберіть наступні пункти:

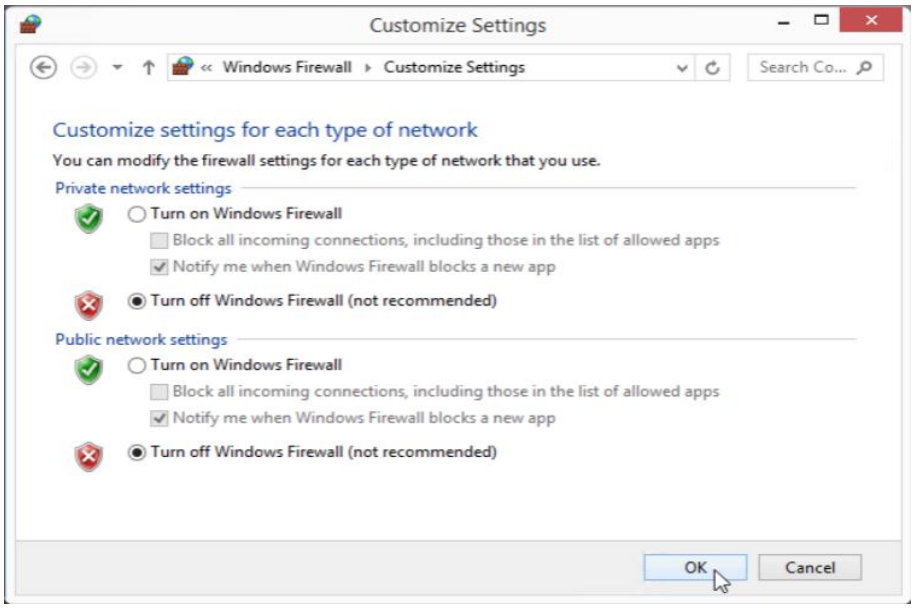


Рис. 8.62 – Відключення брандмауера Windows

Панель управління > Брандмауер Windows > Включення й відключення брандмауера Windows > Відключити брандмауер Windows (не рекомендується) > ОК

8.5.3 Підтримка облікових записів

Співробітникам організації часто потрібні різні рівні доступу до даних. Наприклад, керівник або бухгалтер можуть бути єдиними співробітниками організації з доступом до платіжних відомостей.

Співробітники можуть групуватися по вимогах до роботи, і їх може надаватися доступ до файлів відповідно до дозволів групи. Цей процес допомагає управляти доступом співробітників до мережі. Для співробітників, яким потрібен короткочасний доступ, можна настроїти тимчасові облікові записи. Точне управління мережевим доступом допомагає обмежити області уразливості, які можуть бути використані вірусами або шкідливим програмним забезпеченням для проникнення в мережу.

Припинення доступу співробітників

Коли співробітник іде з організації, його доступ до даних і встаткування мережі повинен бути негайно припинений. Якщо колишній співробітник має збережені файли в особистому місці на сервері, необхідно закрити доступ, відключивши обліковий запис. Якщо новому співробітникові, що замінив колишнього, потрібен доступ до додатка й особистому місцю для зберігання даних, можна знову настроїти обліковий запис і змінити ім'я на ім'я нового співробітника.

Гостьові облікові записи

Тимчасовим співробітникам і гостям може знадобитися доступ до мережі. Наприклад, відвідувачам може знадобитися доступ до електронної пошти, Інтернету й принтеру в мережі. Ці ресурси можуть бути надані за допомогою спеціального облікового запису, який називається гостьовий. При наявності гостей їм може бути призначений гостьовий обліковий запис. При відсутності гостей обліковий запис може бути відключена до появи нових гостей.

Для деяких гостьових облікових записів потрібен розширений доступ до ресурсів, наприклад, для консультантів або фінансового аудитора. Цей тип доступу повинен надаватися тільки на час виконання роботи.

Для настроювання всіх користувачів і груп на комп'ютері використовується **диспетчер локальних користувачів і груп**, як показано на рис. 8.63 (в ОС Windows 8.1). Щоб запустити цей диспетчер, у будь-якій версії Windows уведіть у рядку пошуку або в командному рядку «Виконати» команду **lusrmgr.msc**.

Час входу в систему

У деяких випадках може знадобитися, щоб співробітники могли ввійти в систему тільки в певний проміжок часу, наприклад з 7:00 до 18:00. У будь-який інший час спроба ввійти в систему буде блокуватися.

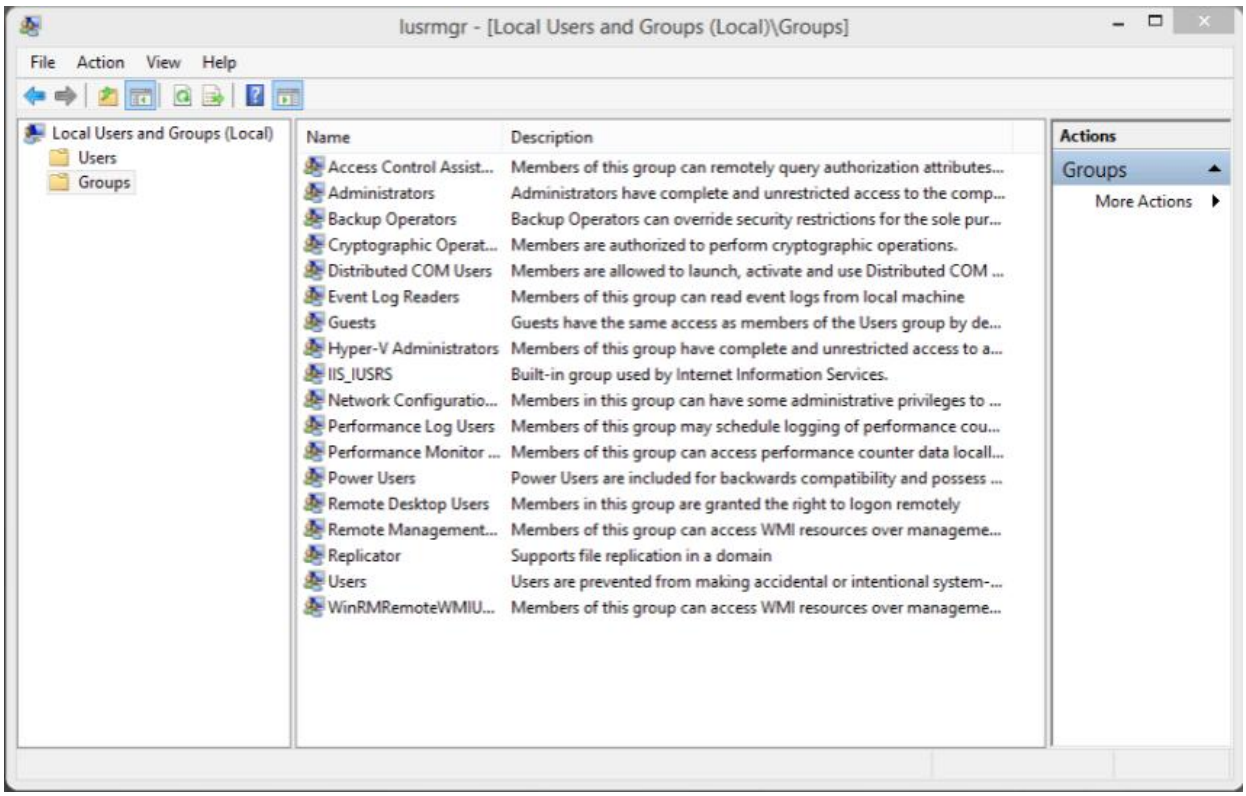


Рис. 8.63 – Диспетчер локальних користувачів і груп

Невдалі спроби входу в систему

Може знадобитися настроїти граничне значення для кількості спроб входу в систему. За замовчуванням в Windows не задане обмеження на кількість невдалих спроб входу в систему, це означає, що користувач не буде заблокований доти, поки не буде змінене значення відповідного параметра.

Час очікування й блокування екрана

Коли співробітники залишають своє робоче місце, вони не завжди виходять із системи й зі свого облікового запису. Тому з метою безпеки рекомендується настроїти таймер очікування, після спрацьовування якого користувач автоматично виходить із системи, а екран блокується на певний час. Щоб розблокувати екран, користувачу необхідно знову ввійти в систему.

8.5.4 Управління користувачами

У список завдань адміністратора входить регулярне створення користувачів і їх видалення з мережі, зміна паролів облікових записів, а також зміна дозволів користувачів рис. 8.64.

Нижче перелічені завдання, які виконуються в рамках управління обліковими записами користувачів.

- Створення локальних облікових записів користувачів

- Скидання паролів для локальних облікових записів користувачів
- Відключення локальних облікових записів користувачів
- Видалення локальних облікових записів користувачів
- Перейменування локальних облікових записів користувачів
- Призначення сценаріїв входу в систему для локальних облікових записів користувачів
- Призначення домашніх папок для локальних облікових записів користувачів.

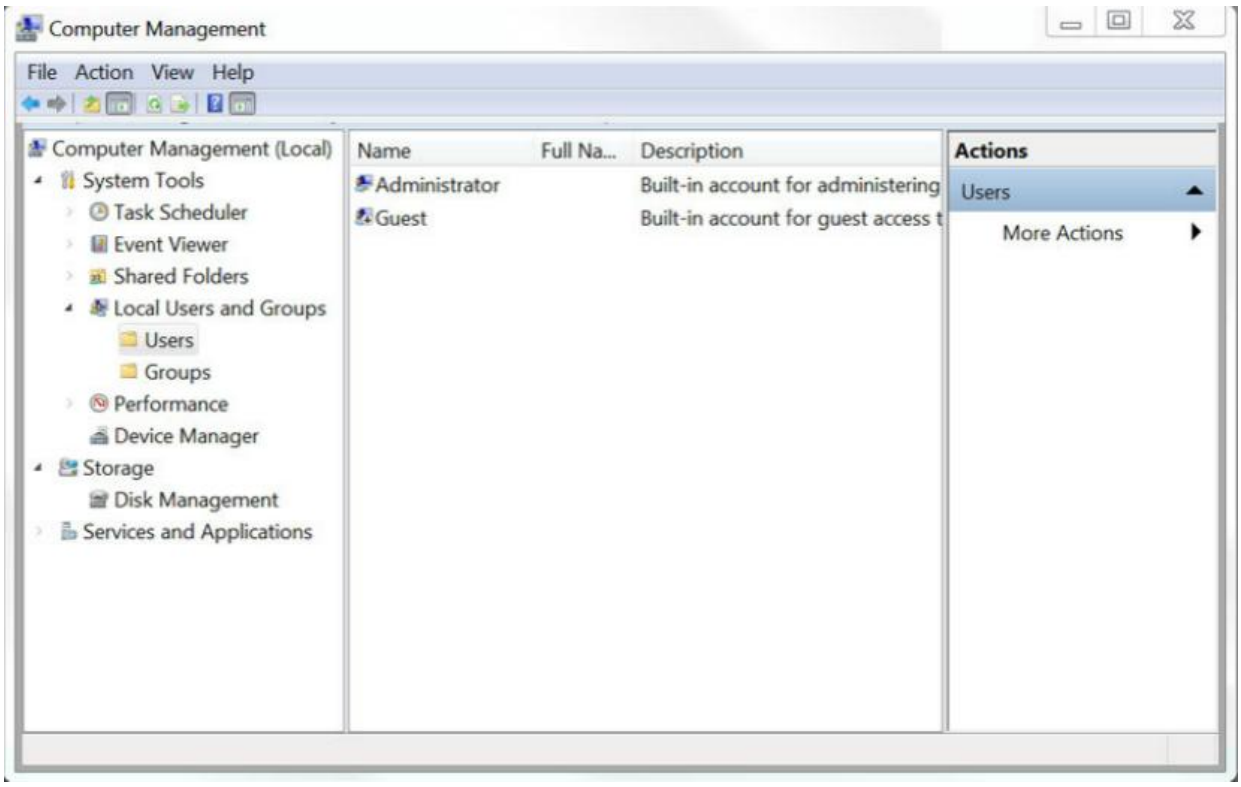


Рис. 8.64 – Список поточних користувачів

Для виконання всіх цих завдань використовуються два інструменти:

- **Управління обліковими записами** – цей інструмент служить для додавання, видалення або зміни атрибутів для окремих користувачів. Увійдіть у систему як адміністратора й скористайтеся інструментом управління обліковими записами для настроювання параметрів, що дозволяють запобігти одержанню шкідливим кодом привілеїв адміністратора.
- **Диспетчер локальних користувачів і груп** – це засіб можна використовувати для створення користувачів і груп, що зберігаються локально на комп'ютері, а також управляти ними.

Примітка. Для управління користувачами потрібні привілеї адміністратора.

Щоб відкрити засіб управління обліковими записами, послідовно виберіть наступні пункти:

Панель управління > Облікові записи користувачів > Управління іншої обліковим записом

Щоб відкрити диспетчер локальних користувачів і груп, послідовно виберіть наступні пункти:

Панель управління > Адміністрування > Управління комп'ютером > Локальні користувачі й групи

За допомогою цього диспетчера можна обмежити можливість користувачів і груп виконувати певні дії, призначивши їм права й дозволу. Право дозволяє користувачу виконувати ті або інші дії на комп'ютері, такі як резервне копіювання файлів і папок, а також вимикання комп'ютера. **Дозвіл** – це правило, пов'язане з об'єктом (звичайно з файлом, папкою або принтером), яке вказує те, яким користувачам дозволений доступ до такого об'єкта, а також спосіб доступу до об'єкта.

У вікні «Локальні користувачі й групи» двічі клацніть елемент **Користувачі**.

Є два вбудовані облікові записи:

- **Адміністратор** – за замовчуванням цей обліковий запис відключений. Власник цього облікового запису має повний доступ до системи й може призначати необхідні права й дозволу на доступ іншим користувачам. Обліковий запис «Адміністратор» входить у групу «Адміністратори» комп'ютера. Її неможливо видалити із групи «Адміністратори», однак її можна перейменувати або відключити.
- **Гість** – за замовчуванням цей обліковий запис відключений. Даний обліковий запис призначений для тих, у кого немає обліковому запису на комп'ютері. За замовчуванням для використання цього облікового запису не потрібно вводити пароль. Даний обліковий запис входить у групу за замовчуванням «Гості». З її допомогою користувач може ввійти в систему комп'ютера.

Щоб додати користувача, клацніть меню **Дії** й виберіть **Створити користувача**. Після цього відкриється діалогове вікно створення облікового запису, як показано на рис. 8.65.

Тут можна вказати ім'я користувача, його повне ім'я, опис і параметри обліковому запису.

Двічі клацніть потрібного користувача або клацніть його ім'я правою кнопкою миші й виберіть пункт **Властивості**, щоб відобразити діалогове вікно властивостей обліковому запису, як показано на рис. 8.66. У цім вікні можна змінити параметри облікового запису користувача, які були задані при її створенні. Крім того, тут можна заблокувати обліковий запис. Також у цім діалоговому вікні можна додати користувача в групу на вкладці **Членство в групах** або вказати папки, до яких у користувача є доступ, звернувшись до вкладки **Профіль** .

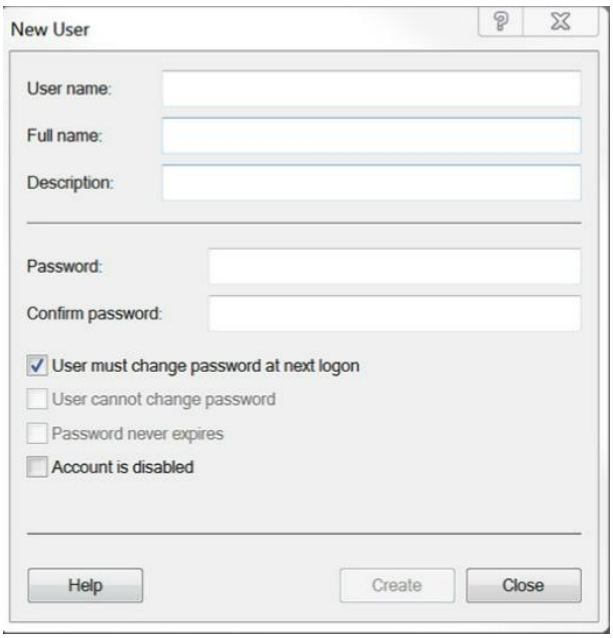


Рис. 8.65 – Додавання нового користувача

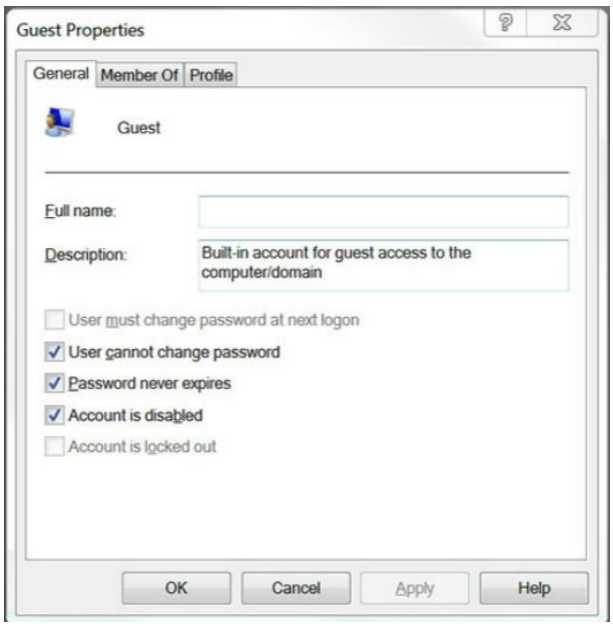


Рис. 8.66 – Зміна властивостей користувача

Примітка. Також існує інший важливий тип облікових записів – «Досвідчений користувач». Даний обліковий запис має більшість дозволів адміністратора, такими як установка програм або зміна параметрів брандмауера, однак з метою безпеки в неї відсутній ряд привілеїв, якими має тільки адміністратор.

8.5.5 Управління групами

Для зручності управління користувачам можна призначати групи.

Нижче перелічені завдання, які виконуються в рамках управління локальними групами користувачів.

- Створення локальної групи користувачів
- Додавання користувачів у локальні групи
- Визначення учасників локальних груп користувачів
- Видалення локальної групи користувачів
- Створення локальних облікових записів користувачів

Щоб відкрити диспетчер локальних користувачів і груп, послідовно виберіть наступні пункти:

Панель управління > Адміністрування > Управління комп'ютером > Локальні користувачі й групи

У вікні «Локальні користувачі й групи» двічі клацніть елемент **Групи**. У системі є безліч вбудованих груп, як показано на рис. 8.67. Однак найбільше часто використовуються наступні групи:

- **Адміністратори** – учасники цієї групи мають повний доступ до системи й можуть призначати необхідні права й дозволу на доступ іншим користувачам. Обліковий запис «Адміністратор» за замовчуван-

ням є учасником цієї групи. Оскільки всі, хто входять у цю групу, мають повний доступ до системи, слід проявляти обережність при додаванні в неї нових учасників.

- **Гості** – для учасників цієї групи при вході в систему створюється тимчасовий профіль, який видаляється після виходу такого користувача із системи. Обліковий запис «Гість» (яка відключена за замовчуванням) входить у цю групу за замовчуванням.
- **Користувачі** – учасники цієї групи можуть виконувати розповсюджені завдання, такі як запуск додатків, використання локальних і мережевих принтерів, а також блокувати комп'ютер. Однак вони не можу надавати загальний доступ до каталогів і створювати локальні принтери.

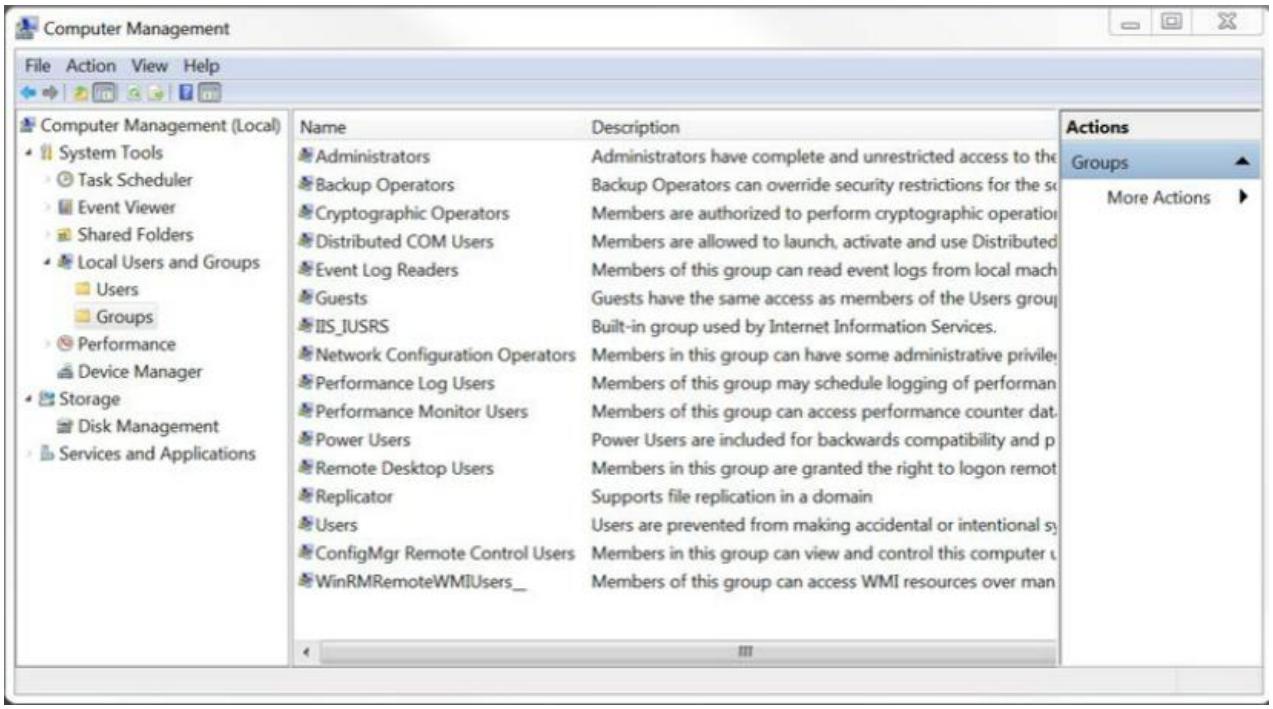


Рис. 8.67 – Список поточних груп

Важливо відзначити, що використовуючи на комп'ютері обліковий запис, який входить у групу «Адміністратори», ви тим самим робите систему вразливої для троянців і піддаєте її іншим погрозам безпеки. Обліковий запис користувача домена, яку планується використовувати для виконання рутинних завдань, включаючи установку програм і відвідування веб-сайтів, рекомендується додавати тільки в групу «Користувачі» (**не додаватиме її в групу «Адміністратори**»). Коли на локальному комп'ютері буде потрібно виконати завдання адміністрування, скористайтеся пунктом **Запуск від імені адміністратора**, щоб запустити програму, використовуючи облікові дані адміністратора.

Щоб створити групу, клацніть меню **Дії** й виберіть **Створити групу**. Також можна клацнути пункт **Групи** правою кнопкою миші й вибрати

команду **Створити групу**. Після цього відкриється діалогове вікно **Нова група**, як показано на рис. 8.68. Тут можна створювати групи й додавати в них користувачів.

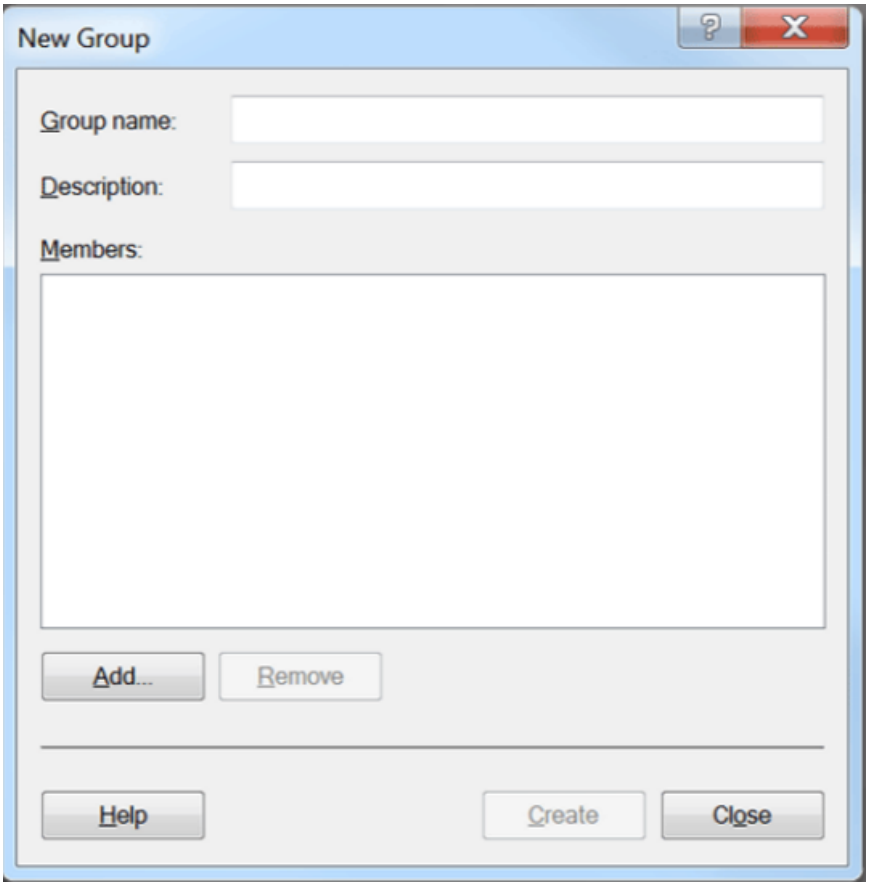


Рис. 8.68 – Додавання нової групи

8.6 Визначення проблеми

Процес усунення неполадок використовується для вирішення проблем безпеки. Серйозність цих неполадок лежить в інтервалі від простій, такий як запобігання підглядання за вашим екраном, до більш складної, наприклад, видалення заражених файлів на декілька підключені до мережі комп'ютерах вручну. Використовуйте етапи процедури пошуку й усунення неполадок як посібник з пошуку неполадок і відновленню працездатності.

Комп'ютерні інженери повинні вміти проаналізувати погрозу безпеки й визначити відповідний спосіб захисту активів і усунення збитку. Першим етапом процедури пошуку й усунення неполадок є визначення проблеми. В табл. 8.18 зображений перелік «відкритих» і «закритих» питань, які слід задати замовнику.

8.6.1 Визначення проблеми

У табл. 8.18 наведені питання для визначення проблеми

Таблиця 8.18 –**Крок 1**. Визначення проблеми

Відкриті питання	• Коли почалася неполадка? • Які проблеми виникли? • Які веб-сайти ви недавно відвідували? • Яке програмне забезпечення безпеки встановлене на комп'ютері? • Хто ще недавно користувався вашим комп'ютером?
Закриті питання	• Чи оновлене ваше ПО безпеці? • Чи проводили ви недавно сканування комп'ютера на наявність вірусів? • Чи відкривали ви вкладення з підозрілого повідомлення електронної пошти? • Чи міняли ви свій пароль останнім часом? • Чи повідомляли ви свій пароль кому-небудь ще?

8.6.2 Формування припущень про можливу причину неполадки

Після розмови із замовником можна приступати до формування припущення про можливі причини неполадок. На основі відомостей про симптоми, отримані від замовника, може знадобитися провести додаткове внутрішнє або зовнішнє дослідження. У табл. 8.19 наведений список розповсюджених можливих причин неполадок із забезпеченням безпеки.

Таблиця 8.19 – **Крок 2.** Формування припущень про можливу причину неполадки

Розповсюджені причини неполадок із забезпеченням безпеки	• Віруси • Трояни • Хробак • Шпигунське ПЗ • Рекламне ПЗ • Умовно шкідливе або шкідливе ПО • Схема фішингу • Втрата пароля • Незахищені кімнати для обладнання • Незахищене робітниче середовище

8.6.3 Перевірка припущень із метою визначення причини

Сформувавши кілька припущень про те, що викликало неполадку, перевірте їх, щоб визначити дійсну причину. У табл. 8.20 представлений перелік швидких процедур, що дозволяє визначити точну причину неполадки або навіть усунути її. Якщо за допомогою швидкої процедури вдається усунути неполадку, після усунення можна провести повну перевірку функціонального стану системи. Якщо за допомогою швидкої процедури не вдається усунути неполадку, слід продовжити пошук точної причини.

Таблиця 8.20 – **Крок 3**. Перевірка припущень із метою визначення причини

Крок 3. Перевірка припущень із метою визначення причини	
Стандартні дії для визначення причини	• Відключите пристрій від мережі. • Обновите сигнатури антивірусного ПЗ й програми захисту від шпигунського ПЗ. • Перевірте комп'ютер за допомогою захисного ПЗ. • Перевірте наявність новітніх виправлень і оновлень ОС комп'ютера. • Перезавантажте комп'ютер або мережевий пристрій. • Увійдіть у систему як адміністратора, щоб змінити пароль користувача. • Захистите кімнати з обладнанням. • Захистите робітниче середовище. • Застосуйте політику безпеки.

8.6.4 Розробка плану дій по усуненню неполадки і його виконання

Установивши точну причину неполадки, розробіть план дій для її усунення й виконаєте його. У табл. 8.21 представлений ряд джерел. Їх можна використовувати для збору додаткової інформації, яка допоможе усунути неполадку.

Таблиця 8.21 – **Крок 4.** Розробка плану дій по усуненню неполадки і його виконання

Якщо на попередньому етапі проблема не була усунута, то для її вирішення необхідний подальший аналіз ситуації.	• Журнали обліку ремонтних робіт служби підтримки • Інші технічні фахівці • Перелік питань, що часто задаються, який публікується виробником • Технічні веб-сайти • Новинні групи • Керівництва до комп'ютера • Керівництва до пристроїв • Форуми в Інтернеті • Пошук в Інтернеті

8.6.5 Повна перевірка функціонального стану системи й вживання профілактичних заходів якщо буде потреба

Після усунення неполадки виконаєте повну перевірку функціонального стану системи й при необхідності впровадження профілактичних заходів. У табл. 8.22 представлений перелік дій для перевірки вирішення.

Таблиця 8.22 – **Крок 5**. Перевірка всіх функцій системи й (при необхідності) вживання профілактичних заходів

Повна перевірка функціонального стану системи	• Повторно перевірте комп'ютер, щоб переконатися у відсутності вірусів. • Повторно перевірте комп'ютер, щоб переконатися у відсутності шпигунського ПО. Перевірте журнали програмного забезпечення безпеки, щоб переконатися у відсутності неполадок. • Перевірте наявність новітніх виправлень і оновлень ОС комп'ютера. • Перевірте зв'язок з мережею й Інтернетом. • Перевірте працездатність усіх додатків. • Перевірте доступ до авторизованих ресурсів, таким як загальні принтери й бази даних. • Переконайтеся, що входи захищені. • Переконаєтеся в застосуванні політики безпеки.

8.6.6 Документування отриманих даних, вжитих заходів і результатів

Останнім етапом процесу пошуку й усунення неполадок є документування отриманих даних, вжитих заходів і підведення підсумків. У табл. 8.23 представлений перелік завдань, які слід виконати, щоб задокументувати неполадку й спосіб її усунення.

Таблиця 8.23 – **Крок 6.** Документування отриманих даних, вжитих заходів і результатів

Документування отриманих даних, вжитих заходів і результатів	• Обговорите застосований вирішення із замовником. • Попросите замовника переконатися, що неполадка усунута. • Надайте замовнику всі документи. • Задокументуйте дії, початі для усунення неполадки, у робочому завданні й журналі технічного фахівця. • Задокументуйте все компоненти, використані при ремонті. • Задокументуйте час, витрачене на усунення неполадки.

8.6.7 Визначення розповсюджених неполадок і способів їх усунення

Неполадки із забезпеченням безпеки можуть бути пов'язані з неполадками встаткування, програмного забезпечення, зв'язку або з комбінацією цих факторів. Деякі типи проблем безпеки прийдеться вирішувати частіше, чим інші. табл. 8.24 являє собою діаграму розповсюджених неполадок із забезпеченням безпеки й способів їх усунення.

Таблиця 8.24 – Розповсюджені неполадки й способи їх усунення

Ознака неполадки	Причини неполадки	Можливі розв'язки
Безпроводова мережа скомпрометована, навіть незважаючи на використання 128– розрядного шифрування WEP.	Зловмисник використовує наявні в продажі безпроводові засоби злому для злому шифрування.	Перейдіть на шифрування WPA. • Додайте фільтрацію по MAC– адресам для старих клієнтів, що не підтримують WPA.
Користувач одержує сотні або тисячі небажаних повідомлень електронної пошти щодня.	Мережа не забезпечує визначення або захист сервера електронної пошти від спамерів.	Установите антивірус або поштову програму, що видаляє спам з папки «Вхідні».
Помічене, що незнайомий фахівець із ремонту принтерів заглядає під клавіатури й на робочі столи.	Спостереження за відвідувачами не ведеться належним чином, або облікові дані користувачів для входу в будинок украдені.	• Звернетеся в службу безпеки або поліцію. • Порадьте користувачам ніколи не зберігати паролі поруч зі своїми робітниками місцями.
У мережі виявлена несанкціонована безпроводова точка доступу.	Користувач додав безпроводову точку доступу для збільшення діапазону безпроводової мережі компанії.	• Відключите несанкціонований пристрій і конфіскуйте його. • Застосуєте політику безпеки, почавши необхідні заходи відносно особи, відповідального за порушення безпеки.
Користувачі із флеш-дисками заражають вірусами комп'ютери в мережі.	Флеш-диск заражений вірусом і не перевіряється програмним забезпеченням захисту від вірусів при доступі до нього комп'ютера в мережі.	Настроювання антивірусного ПО для сканування знімних носіїв при доступі до даних.
Відображається попередження безпеки.	• Брандмауер Windows виключений. • Визначення вірусів застаріли. • Виявлене шкідливе ПЗ.	• Включити брандмауер Windows. • Обновите визначення вірусів. • Перевірте комп'ютер, щоб вилучити шкідливе ПЗ.
Збій Центру оновлення Windows.	• Завантажене оновлення ушкоджене. • Для оновлення потрібне попереднє оновлення, яке не встановлене.	• Завантажите оновлення вручну й установите його. • Використайте оновлення системи, щоб виконати відкіт комп'ютера на момент до виконання спроби оновлення. • Здійснити оновлення з резервної копії.
Системні файли були перейменовані, не запускаються додатки, зникли	Комп'ютер заражений вірусом.	• Видалите вірус, використовуючи антивірусне ПО. • Здійснити відновлення з

Ознака неполадки	Причини неполадки	Можливі розв'язки
файли або були змінені дозволи.		резервної копії.
Адресати електронної пошти повідомляють, що з вашої адреси розсилається спам.	Ваша електронна пошта зламана.	• Перемініте пароль електронної пошти. • Зверніться в службу підтримки електронної пошти для відновлення облікового запису.

8.7 Система управління інформаційною безпекою ВЦТМ ДСНС України

Об'єкт інформаційної діяльності (**ОІД)** – будівлі, приміщення, транспортні засоби чи інші інженерно-технічні споруди, функціональне призначення яких передбачає обіг інформації з обмеженим доступом [1-8].

Об'єкт критичної інформаційної інфраструктури – комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури.

Інформація з обмеженим доступом – інформація, що становить державну або іншу передбачену законом таємницю, а також службова та конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України «Про доступ до публічної інформації», та інша конфіденційна інформація, вимога щодо захисту якої встановлена законом.

Прихованість (таємність) – здатність телекомунікаційних систем та інформаційних технологій обмеження несанкціонованого доступу до схем організації телекомунікацій, переданої інформації й засобів телекомунікації та інформатизації.

Інцидент кібербезпеки (ІК) – подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактору) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів.

Кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів,

що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту.

Кібербезпека – захищеність життєвоважливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

Кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем.

Підрозділ ТЗІ – підрозділ, призначений для виконання робіт з технічного захисту інформації (ТЗІ) у системі ДСНС відповідно до повноважень, наданих ДСНС згідно з Дозволом на проведення робіт з технічного захисту інформації для власних потреб.

Комплекс ТЗІ – сукупність організаційних, інженерних і технічних заходів та засобів, призначених для захисту від витоку інформації з обмеженим доступом технічними каналами на об'єктах інформаційної діяльності.

Захист інформації в системах розглядається в контексті критично важливих секторів; захист інформаційної інфраструктури передбачає забезпечення гарантії того, що подібні та мережі стійкі до ризиків інформаційної безпеки, мережевої безпеки, Інтернет, так само як і ризиків кібербезпеки.

Напрямки захисту інформації формуються виходячи із конкретних особливостей інформаційної системи як об'єкту захисту. Виходячи з типової структури інформаційної системи (ІС) і історично складених висновків робіт по захисту інформацією, можна виділити наступні напрямки:

захист об'єктів інформаційних систем;

захист процесів, процедур і програм обробки інформації;

захист каналів зв'язку;

пригнічення побічних електромагнітних наведень;

управління системою захисту.

Забезпечення діяльності щодо заходів технічного захисту інформації досягається:

створенням комплексних систем захисту інформації (КСЗІ) в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах ДСНС на об’єктах інформаційної діяльності ДСНС;

забезпечення сталого функціонування впроваджених в експлуатацію комплексних систем захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах ДСНС на об’єктах інформаційної діяльності ДСНС.

Виконання заходів кібербезпеки та технічного захисту інформації є елементами системи управління інформаційною безпекою (ІБ).

За впровадження та функціонування системи управління інформаційною безпекою (СУІБ) відповідає керівник установи.

Основні функції системи управління інформаційною безпекою:

виявлення та аналіз ризиків інформаційної безпеки;

планування та практична реалізація процесів, спрямованих на мінімізацію ризиків ІБ;

контроль цих процесів;

внесення в процеси мінімізації інформаційних ризиків необхідних коригувань.

До регламенту входять політики безпеки (інформаційна, мережева, адміністративна), що визначають розмежування прав доступу користувачів до внутрішньої мережі та внутрішньої інфраструктури установи відповідно до їх повноважень (адміністратор, модератор, авторизований користувач тощо), а також порядок резервного копіювання інформації.

У політиці безпеки Системи мають бути розглянуті такі проблеми, як віддалений доступ, перелік критичних ресурсів, керування та конфігурація IP-адрес, безпека засобів телекомунікацій, процедура виявлення вторгнення у мережу.

Вимоги щодо захисту інформації у Системах

Для забезпечення захисту інформації у Системах виконується комплекс організаційно-технічних заходів зі створення та впровадження комплексної системи захисту інформації з підтвердженою Державною службою спеціального зв'язку та захисту інформації України відповідністю вимогам нормативно-правових документів технічного захисту інформації.

Захисту в Системах підлягає така інформація:

відкрита інформація, яка відноситься до державних інформаційних ресурсів;

інформація з обмеженим доступом, яка поділяється на конфіденційну, службову та секретну інформацію;

технологічна інформація.

Для забезпечення функціонування комплексної системи захисту інформації у Системах призначаються посадові особи, відповідальні за експлуатацію, захист інформації, технічне обслуговування та модернізацію.

Організація обліку Систем

На всі інформаційні ресурси в установі має вестись інформаційна картка за формою, що додається.

За щорічне оновлення і зберігання інформаційних карток на Системи в установі відповідає Служба технічної підтримки.

Інформаційні картки мають бути в актуальному стані і зберігатися в електронній формі.

8.7.1 Рекомендація Ради національної безпеки і оборони України по захисту відомчої електронної пошти

Щоб уникнути зламу електронної поштової скриньки, необхідно:

– увімкнути двофакторну автентифікацію за допомогою мобільного пристрою. В такому випадку під час спроби отримання паролю до поштової скриньки сторонніми особами буде надходити попередження на мобільний телефон у вигляді SMS-повідомлення про спробу злому;

– встановити надійний пароль;

– не використовувати для відновлення паролю російські сервіси («Yandex.ru», «Mail.ru» тощо);

– не запускати на пристроях вкладення підозрілих листів, що містять виконуваний файл з такими розширеннями як «.exe», «.hat», «.cmd», «.vhs», «.docm», «.xlsm» тощо;

– державні службовці та військовослужбовці повинні пам 'ятати, що службові електронні скриньки не слід використовувати для приватного листування.

8.7.2 Види робіт з ТЗІ, які можуть виконуватися підрозділами ТЗІ

Розроблення, впровадження, випробування, обслуговування на об’єктах інформаційної діяльності комплексів (систем) технічного захисту інформації, носіями якої є акустичні поля.

Розроблення, впровадження, випробування, обслуговування на об’єктах інформаційної діяльності комплексів (систем) технічного захисту інформації, носіями якої є електромагнітні поля та електричні сигнали.

Розроблення, впровадження, випробування, супроводження комплексів технічного захисту інформації в інформаційних системах, інформаційних технологій із захистом інформації від несанкціонованого доступу.

Виявлення та блокування витоку мовної та видової інформації через закладні пристрої на об’єктах інформаційної діяльності.

8.7.2.1 Організація діяльності підрозділів ТЗІ

У системі ДСНС роботи з технічного захисту інформації проводяться підрозділами ТЗІ відповідно до Дозволу на проведення робіт з технічного захисту інформації для власних потреб, наданого ДСНС у встанов-

леному порядку, та повноважень на проведення відповідних видів робіт відповідно до наказу ДСНС. Роботи з технічного захисту інформації у системі ДСНС також можуть проводити організації, які мають ліцензію на проведення відповідних видів робіт з технічного захисту інформації та спеціальний дозвіл на провадження діяльності, пов'язаної з державною таємницею.

Повноваження підрозділу ТЗІ на проведення відповідних видів робіт з ТЗІ надаються наказом ДСНС.

Координацію, облік проведених робіт та контроль за діяльністю підрозділів ТЗІ підрозділів здійснює Управління зв'язку та оповіщення ДСНС.

Основні завдання, функції, обов'язки та відповідальність підрозділу ТЗІ визначаються Положенням про підрозділ ТЗІ, яке затверджується керівником підрозділу.

Впровадження заходів ТЗІ в підрозділі, до складу якої входить Підрозділ ТЗІ, організовується керівником підрозділу.

Безпосередній контроль за виконанням завдань підрозділом ТЗІ покладається на керівника підрозділу зв'язку та інформатизації підрозділу.

Організація заходів ТЗІ у центральному апараті ДСНС здійснюється Управлінням.

Інструментальний контроль виконання вимог та норм технічного захисту інформації на об'єкті інформаційної діяльності (далі – ОІД), де розроблено та впроваджено підрозділом ТЗІ комплекс технічного захисту інформації, може здійснюватися Центром ТЗІ Вузла зв'язку та автоматизації ДСНС.

8.7.2.2 Умови та порядок надання повноважень на проведення робіт з технічного захисту інформації

Для одержання повноважень підрозділу ТЗІ на проведення окремих видів робіт або усього зазначеного переліку необхідно мати:

Призначених наказом керівника підрозділу спеціалістів для проведення обраних видів робіт, які мають повну чи базову вищу освіту за напрямом підготовки «Інформаційна безпека» або інженерно-технічну освіту фахового спрямування, відповідного обраному виду роботи, з додатковою підготовкою на курсах перепідготовки та підвищення кваліфікації фахівців з питань ТЗІ чи стажем роботи у галузі ТЗІ за обраним видом роботи не менше 3 років, а також мають оформлені у встановленому порядку допуски до державної таємниці.

Нормативно-правові акти та нормативні документи з технічного захисту інформації, необхідні для проведення обраних видів робіт.

Повірені в установленому порядку засоби вимірювань і контролю (як власні, так і залучені на договірних засадах), а також засоби елект-

ронної обчислювальної техніки (ЕОТ) в обсязі, що забезпечує проведення обраних видів робіт.

Приміщення, у яких впроваджено і атестовано комплекси ТЗІ та інформаційні системи з впровадженою КСЗІ з підтвердженою відповідністю.

Спеціальний дозвіл на провадження діяльності, пов'язаної з державною таємницею.

Окреме приміщення, в якому розміщується начальницький склад та працівники, а також апаратура підрозділу ТЗІ і забезпечується обмежений доступ сторонніх осіб.

Начальницький склад та працівники підрозділу ТЗІ повинні знати методики та порядок виконання робіт з ТЗІ відповідно до вимог нормативних документів та уміти застосовувати наявну апаратуру і обладнання. Методичний супровід підвищення кваліфікації начальницького складу та працівників підрозділу ТЗІ забезпечується Управлінням.

За умов виконання зазначених вимог підрозділ ТЗІ, подає до ДСНС заяву про надання повноважень на проведення робіт з ТЗІ.

Після отримання заяви ДСНС перевіряє відомості, що містяться у поданих матеріалах, створені умови для проведення заявлених видів робіт, підготовленість начальницького складу і працівників підрозділу ТЗІ та приймає рішення про надання повноважень на виконання заявлених видів робіт або надає рекомендації щодо усунення виявлених недоліків і термін наступної перевірки.

8.7.3 Створення та впровадження комплексних систем захисту інформації

Етапи побудови КСЗІ необхідно пройти в рівній кількості для всіх і кожного окремо напрямків (з врахуванням всіх основ). Виділяють наступні етапи побудови КСЗІ:

визначення інформаційних ресурсів (ІР), які підлягають захисту;

виявлення всієї можливої кількості загроз безпеки ІР, які підлягають захисту;

проведення оцінки чутливості і ризиків для ІР, які підлягають захисту, при виявленні великої кількості загроз;

розробка проекту (плану) системи захисту інформації, знижаючого за вибраним критерієм ризику для ІР, які підлягають захисту, при виявленні великої кількості загроз.

реалізація проекту (плану) захисту інформації;

визначення якості реалізації системи захисту;

здійснення контролю функціонування і управління системою захисту.

Аналіз стану і уточнення вимог до СЗІ об'єднує складові блоків основи, напрямки, етапи за принципом один з одним.

8.7.4 Створення та впровадження комплексів технічного захисту інформації

Захист інформації з обмеженим доступом при автономному використанні на ОІД пристроїв обробки інформації здійснюється шляхом створення комплексу ТЗІ, який складається із сукупності:

організаційних заходів захисту від несанкціонованих дій з інформацією (для захисту конфіденційної інформації, що є власністю держави або вимога щодо захисту якої встановлена законом);

організаційних заходів захисту від несанкціонованих дій з інформацією та технічних засобів захисту інформації від витоку технічними каналами за наявності можливості створення таких каналів (для захисту інформації, що становить державну таємницю).

За результатами спеціального дослідження приймається рішення про необхідність встановлення активних та/або пасивних засобів захисту. Після цього проводиться оцінка захищеності ІОД від витоку технічними каналами на об'єкті ЕОТ (атестація комплексу ТЗІ).

Організаційні заходи захисту від несанкціонованих дій з інформацією при автономному використанні пристроїв (ПАВ) обробки інформації:

встановлення порядку користування ПАВ;

встановлення порядку використання зовнішніх пристроїв пам'яті в ПАВ;

визначення та встановлення обов'язків осіб, що користуються ПАВ та здійснюють контроль за користуванням ПАВ;

встановлення порядку фізичного захисту ОІД, де функціонує ПАВ;

визначення та встановлення змісту і порядку контролю за користуванням ПАВ.

8.7.5 Організація заходів протидії кіберзагрозам

З метою забезпечення надійного функціонування засобів кіберзахисту в установі щороку проводиться визначення ризиків кібербезпеки, оцінка надійності засобів кіберзахисту, коригування поточного профілю кібербезпеки. Ці заходи виконуються фахівцями установи ,у разі потреби до їх виконання можуть бути залучені сторонні фахівці чи організації в сфері кіберзахисту.

За рекомендаціями Державної служби спеціального зв'язку та захисту інформації України з метою запобігання ІК і сприяння підвищенню рівня кіберзахисту електронних ресурсів та систем необхідно:

Провести аудит запроваджених заходів захисту та рівня інформаційної безпеки систем у цілому.

Провести роз'яснювальну роботу з працівниками, які користуються службовою електронною поштою, щодо правил та вимог безпеки, особливо в частині, що стосується вхідних листів (повідомлень).

Заборонити відкриття вкладень у підозрілих повідомленнях (листах від адресатів, щодо авторства яких виникають сумніви та зобов'язати користувачів службової електронної пошти негайно повідомляти про такі листи адміністратора безпеки.

Зобов'язати користувачів службової електронної пошти провести її ревізію на предмет виявлення листів, що мають вкладення «MoF critical IT needs_eng.xls», заборонивши їх відкриття, та невідкладно повідомляти про наявність таких листів адміністратора безпеки.

Заборонити використання приватної електронної пошти для цілей службової діяльності.

Заборонити використання точок публічного доступу до Інтернет для входу до службової електронної пошти.

Адміністраторам безпеки рекомендовано звести до мінімуму мережеву активність усіх пристроїв систем управління з Інтернет, ужити заходів до дотримання вимог із сегментування, не допускати циркуляції технологічної інформації поза межами адміністративного сегмента мережі.

Для організації віддаленого доступу використовувати лише безпечні методи (наприклад, такі технологічні рішення, як VPN).

Для унеможливлення проведення атак типу Man-in-the-Middle з використанням техніки ARP-spoofing ужити заходів з налаштування статичних значень ARP-таблиць АРМ і серверного обладнання. Для цього здійснити прив'язку MAC-адрес АРМ до конкретного інтерфейсу комутатора, цим самим заборонивши підключення сторонніх пристроїв.

Передбачити моніторинг та фіксацію (журналювання) подій, які мають відношення до інформаційної безпеки (доступ до баз даних, адміністративний доступ до обладнання тощо).

Запровадити політику, що потребує використання лише надійних паролів.

Провести рекомендоване виробником оновлення програмного забезпечення, щоб запобігти вже виявленим уразливостям.

Контролювати створення аккаунтів на рівні адміністраторів системи.

Здійснити зміну авторизаційних даних до критично важливих вузлів системи, попередньо перевіривши їх на наявність процесів, які можуть скомпрометувати дані.

Проводити постійний аналіз вхідного/вихідного Інтернет-трафіку.

Проводити аналіз лог-файлів мережевого та серверного обладнання на наявність у них відомостей про аномальну активність (доступ до системи із систем, які перебувають поза адміністративним сегментом мережі; наявність нелегітимних авторизаційних даних).

Здійснювати перевірку ПЕОМ адміністраторів мережі та критично важливих вузлів системи на наявність підозрілих процесів і програм (наприклад: системних служб, що запускаються не зі стандартного розташування; програм, що не мають цифрового підпису виробника, тощо).

Дотримуватися організації заходів протидії кіберзагрозами у відповідності до рекомендацій Національного стандарту України ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT) Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки.

Список використаних джерел

Керівні документи

1. Порядок організації роботи відомчої цифрової телекомунікаційної мережі ДСНС Наказ ДСНС 23.10.2019 № 608.

Наказ ДСНС України – ДСНС України (dsns.gov.ua)

2. Наказ МВС України 08.02.2019 № 93 Про затвердження Інструкції щодо практик чи процедур проектування, дослідження, введення в експлуатацію, експлуатації та технічного обслуговування (супроводження) автоматизованих систем централізованого оповіщення.

Про затвердження Інструкції щодо ... | від 08.02.2019 № 93 (rada.gov.ua)

3. Наказ МВС України 20.10.2017 № 870 Про затвердження Положення про автоматизовану інформаційну систему оперативного призначення єдиної інформаційної системи МВС.

Про затвердження Положення про а... | від 20.10.2017 № 870 (rada.gov.ua)

4. Деякі питання оперативно-технічного управління телекомунікаційними мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану Постанова Кабінету Міністрів України від 29 червня 2004 р. N 812 Київ.

Деякі питання оперативно-технічн... | від 29.06.2004 № 812 (rada.gov.ua).

5. Наказ ДСНС 03.12.2018 № 700 Інструкція з документування управлінської інформації в електронній формі та організації роботи з електронними документами в діловодстві, електронного міжвідомчого обміну в Державній службі України з надзвичайних ситуацій.

Наказ ДСНС України – ДСНС України (dsns.gov.ua)

6. Наказ ДСНС 01.10.2020 № 533 Про затвердження Положення з організації заходів забезпечення кібербезпеки в ДСНС

https://www.dsns.gov.ua/files/2020/10/2/Nakaz-533.pdf

7. Національний стандарт України ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT) Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки. Видання офіційне. Київ, ДП «УкрНДНЦ», 2018. – 50с.

https://metrology.com.ua/ntd/skachat-dstu-gost-gost-r/dstu/dstu-iso-iec-27032-2016/

Література

8. В. О. Собина, Д. В. Тарадуда, М. М. Піксасов, Л. В. Борисова, О. В. Закора, А. Б. Фещенко, М.В. Маляров, Д. Л. Соколов, Дослідження проблем функціонування системи зв'язку ДСНС, використання засобів телекомунікацій та інформатизації в системі ДСНС, шляхів їх розвитку із застосуванням сучасних телекомунікаційних та інформаційних технологій, Звіт про НДР: № держреєстрації 0119U001009, Х.: НУЦЗУ, 2020. – 85 с. Режим доступу: http://ndr.dsns.gov.ua/?p=7135

9. Лаптєв О.А., Савченко В.А., Шуклін Г.В. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності Навчальній посібник – Київ: ДУТ, 2020. – 126 с.

10. Ю. А. Тарнавський Технології захисту інформації: підручник. – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с.

11. Быченок Н. Н. Основы обеспечения информационной безопасности государства в военной сфере : учебник / Н. Н. Быченок, В. А. Савченко, Т. М. Дзюба. – К.: НУ ОУ им. И. Черняховского, 2017. – 244 с.

12. Глинчук Л.Я. Криптологія: навч.-метод. noci6. / Людмила Ярославівна Глинчук – Луцьк: Вежа-Друк, 2014.– 164 с.

13. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Теорія. Практика. Застосування: монографія. Харків: Видавництво «Форт», 2012. – 870 с.

Огляд Розділу 8. Інформаційна безпека відомчої цифрової телекомунікаційної мережі ДСНС України

У цьому розділі обговорюється комп'ютерна безпека і її важливість для захисту комп'ютерного обладнання, мереж і даних. Щоб допомогти вам у забезпеченні безпеки комп'ютерного обладнання й даних, у главі описані погрози, процедури й профілактичне обслуговування, що належить до даних і фізичної безпеки. От деякі важливі концепції із цієї глави, які потрібно запам'ятати:

- погрози безпеки можуть надходити з організації або інших джерел;
- віруси й чирви – розповсюджені погрози, що атакують дані;
- розробіть і застосуйте план безпеки для захисту даних і фізичного обладнання від втрати.
- підтримуйте актуальність і безпеку ОС і додатків за допомогою виправлень і пакетів оновлення.

Розглянута система управління інформаційною безпекою ВЦТМ ДСНС України, яка регламентує:

- види робіт з ТЗІ, які можуть виконуватися підрозділами ТЗІ;
- організацію діяльності підрозділів ТЗІ;
- умови та порядок надання повноважень на проведення робіт з технічного захисту інформації;

- порядок створення та впровадження комплексних систем захисту інформації;
- порядок створення та впровадження комплексів технічного захисту інформації;
- організацію заходів протидії кіберзагрозам.

Питання та завдання для самостійного контролю знань

Контрольні питання

1. Шкідливе ПО.
2. Політика безпеки.
3. Забезпечення безпеки веб-трафіка.
4. Резервне копіювання даних. Шифрування папок і файлів. Windows Bitlocker.
5. Стирання даних. Повторне використання й знищення жорстких дисків.
6. Програми захисту від шкідливого ПО.
7. Способи захисту фізичного встаткування. Захисне встаткування.
8. Пакети відновлення й виправлення безпеки операційної системи.
9. Визначення проблеми інформаційної безпеки.
10. Забезпечення інформаційної безпеки України в умовах надзвичайних ситуацій.
11. Державна таємниця як особливий вид інформації, що захищається. Відомості щодо цивільного захисту, що становлять державну таємницю.
12. Загрози інформаційній безпеці

Питання для тест-контролю

1. Які характеристики описують програму-хробак? (Виберіть два варіанти.)

він самостійно розмножується

виконується при запуску ПО на комп'ютеру

перебуває в неактивному стані, поки не знадобиться зловмисникові

переходить на нові комп'ютери без якого-небудь втручання й без ведена користувача

заражає комп'ютери, прикріплюючись до програмного коду

2. Компанія XYZ вирішила замінити трохи старих ПК. Які запобіжний заходи повинна прийняти компанія перед утилізацією застарілих комп'ютерів?

Виконати високорівневе форматування жорсткого диска

Вилучити ОЗП з материнської плати

Стерти дані з жорсткого диска

Знищити монітор

Вилучити ЦП

3. Який мінімальний рівень захисту файлів в Windows необхідний, щоб локальний користувач міг відновлювати файли з резервних копій?

Запис

Читання

Повний доступ

Створення

4. Хтось розсилає по електронній пошті листа, що виглядають схожими на листи від відомого відправника. У листах, що розсилаються ім. пропонується відвідати підставний веб-сайт, де користувача просять увести конфіденційні дані. До якого типу погроз безпеки ставиться ця ситуація?

фішинг

хробак

вірус-невидимка

рекламне ПО

5. Інженер зайнятий усуненням проблеми з безпекою комп'ютера. Зловмисник зміг скористатися комп'ютером завдяки ненадійному паролю користувача. Яку дію слід почати інженеру в якості профілактики подібних атак?

Переконатися в дотриманні політики безпеки

Просканувати комп'ютер за допомогою захисного ПО

Перевірити наявність новітніх виправлень і відновлень ОС комп'ютера

Перевірити фізичну безпеку всіх офісів

6. Який параметр міжмережевого екрана Windows дає користувачеві можливість вручну дозволяти доступ до портів, необхідних для роботи додатка?

Відключити міжмережевий екран Windows

Автоматично

Включити міжмережевий екран Windows

Управління параметрами безпеки

Навчальне видання

Фещенко Андрій Борисович
Борисова Лариса Володимирівна
Закора Олександр Вікторович
Собина Віталій Олександрович
Тарадуда Дмитро Віталійович
Демент Максим Олександрович
Неклонський Ігор Михайлович

ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У СФЕРІ ЦИВІЛЬНОГО ЗАХИСТУ

Підручник

Підписано до друку 21.11.2021. Формат 60х84/16.
Ум. друк. арк. 41,7.
Вид. № 54/21.
Сектор редакційно-видавничої діяльності
Національного університету цивільного захисту України
61023, м. Харків, вул. Чернишевська, 94

www.nuczu.edu.ua

717