МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

«На правах рукопису»
УДК 681.3.06

«До захисту допущено»
Завідуючий кафедрою СІКЗ
_____ к.т.н. Г.В. Шуклін
«____» _____ 2021 р.

# МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 “Кібербезпека”

на тему: «ДОСЛІДЖЕННЯ БЕЗПЕКИ ТА СПОСОБІВ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ МУЛЬТИМЕДІЙНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ НА ОСНОВІ IP-ПРОТОКОЛУ»

студент групи СЗДМ-61 Очаковець Микита Русланович _____
(підпис)

Науковий керівник: к.т.н., доцент Пепа Юрій Володимирович _____
(підпис)

Нормоконтроль: Гребенніков Асаді Болдхоядович _____
(підпис)

КИЇВ – 2022

«ЗАТВЕРДЖУЮ»

Завідувач кафедри СІКЗ

_____ к.т.н. Г.В. Шуклін

(підпис)

«_____»_____ 2021 р.

# ЗАВДАННЯ

**на атестаційну роботу магістра**

студенту: Очаковець Микиті Руслановичу

**1. Тема роботи:** «Дослідження безпеки та способів підвищення ефективності мультимедійних інформаційно-комунікаційних систем на основі IP-протоколу», затверджена наказом по університету від «  » 2021 р. за №  .

**2. Термін здачі** студентом оформленої роботи « 18 » грудня 2021 р.

**3. Об'єкт дослідження:** процес захисту мультимедійної інформації.

**4. Предмет дослідження:** напрями захисту інформації від витоку інформаційно-комунікаційними лініями зв'язку.

**5. Мета роботи:** запропонувати систему захисту мультимедійної інформації та підівищити ефективність її передачі лініями зв'язку за IP-протоколом.

**6. Перелік питань, які мають бути розроблені:**

1. будова корпоративних мереж;
2. мультимедійна інформація та засоби її обробки;
3. дослідити способи і методи захисту мультимедійної інформації.

**7. Перелік публікацій:**

**8. Перелік ілюстративного матеріалу.** Презентація виконана на слайдах для подання за допомогою світлопроекторів та комп'ютерних засобів.

**9. Дата видачі завдання** «____» ___ 2021 р.

**Науковий керівник** _____ Пепа Ю.В.

(підпис)

**Завдання прийняв до виконання** _____ Очаковець М.Р.

(підпис)

# КАЛЕНДАРНИЙ ПЛАН

**Дата видачі завдання** «____» _____ 2021 р.

| № з/п | Назва етапів дипломної роботи | Строк виконання етапів роботи | Примітка |
|---|---|---|---|
| 1 | Огляд літератури | до 30.09.21 р. | виконано |
| 2 | Написання першого розділу роботи | до 10.10.21 р. | виконано |
| 3 | Написання другого розділу роботи | до 20.11.21 р. | виконано |
| 4 | Розробити архітектуру корпоративної мережі | до 10.11.21 р. | виконано |
| 5 | Написання третього розділу роботи | до 20.11.21 р. | виконано |
| 6 | Оформлення атестаційної роботи | до 10.12.21 р. | виконано |
| 7 | Підготовка демонстраційних матеріалів | до 18.12.21 р. | виконано |

**Студент:** СЗДМ - 61 Очаковець М.Р. _____
(підпис)

**Науковий керівник:** к.т.н., доц. Пепа Ю.В. _____
(підпис)

**Нормоконтроль:** Гребенніков А.Б. _____
(підпис)

# РЕФЕРАТ

Атестаційна робота містить: 97 сторінок, 39 рисунків, 2 таблиці.

Втрата мультимедійної інформації чи спотрворення її змісту несуть серйозну загрозу для її власника та отримувача. Тому її захист є першочерговою задачею. Організація її обробки на підприємстві у корпоративній комп‘ютерній мережі, організованої за IP-протоколами, має свої особливості і проблеми, які вирішуються автором в цій атестаційній роботі.

**Мета роботи –** розробити систему захисту мультимедійної інформації, яка циркулює у корпоративних мережах.

**Завдання дослідження:**

- розглянуті загрози витоку мультимедійної інформації;

- виявлені ризики і слабкі місця корпоративних мереж;

- проаналізовані особливості IP-протоколів і організація передачі інформації у комп‘ютерній мережі;

- запропоновано захисні пристрої та організаційні заходи захисту мультимедійного контенту.

**Об’єкт дослідження –** процес захисту мультимедійної інформації.

**Предмет дослідження –** способи та методи захисту інформації від витоку її з корпоративної мережі технічними каналами.

**Методи дослідження:** аналітичні, системні, порівняння.

Проведені дослідження дозволили створити архітектуру корпоративної мережі та запропонувати блок заходів і технічних засобів, які дозволяють зменшити ризик витоку мультимедійної інформації.

Галузь використання – кібербезпека.

**Ключові слова:** МУЛЬТИМЕДІЙНИЙ ПРИСТРІЙ, ІНФОРМАЦІЯ, ПРОТОКОЛ, ЗАГРОЗА ІНФОРМАЦІЇ, ВИТІК ІНФОРМАЦІЇ, ТЕЛЕФОНІЯ, КОНТЕНТ.

# ABSTRACT

The thesis contains 37 pages, 39 drawings, 2 tables.

Loss of or misrepresentation of multimedia information poses a serious threat to its owner and recipient. Therefore, its protection is a priority. The organization of its processing at the enterprise in the corporate computer network, organized according to IP protocols, has its own features and problems that are solved by the author in this certification work.

**The purpose of the work** is to develop a system of protection of multimedia information, which circulates in corporate networks.

**Objectives of the study:**

- threats of leakage of multimedia information are considered;
- identified risks and weaknesses of corporate networks;
- analyzed the features of IP protocols and the organization of information transmission in a computer network;
- proposed protective devices and organizational measures for the protection of multimedia content.

**Object of reserch** – research is the process of protection of multimedia information.

**The subject of reserch –** ways and methods of protecting information from leakage from the corporate network through technical channels.

**Research methods:** analytical, systemic, comparison..

The conducted research allowed to create the architecture of the corporate network and to offer a block of measures and technical means that reduce the risk of leakage of multimedia information.

Area of application - cybersecurity.

**Key words:** MULTIMEDIA DEVICE, INFORMATION, PROTOCOL, THREAT OF INFORMATION, LEAK OF INFORMATION, TELEPHONY, CONTENT.

# ЗМІСТ

# ВСТУП

Однією з найважливіших частин інформаційної інфраструктури сучасних підприємств і багатьох державних організацій є корпоративні мережі, які давно перейшли до розряду критичних для забезпечення безперервності бізнес-процесів. Вихід з ладу такої системи або спотворення підсистеми доступу до інформаційних ресурсів фактично означає зупинку діяльності всієї організації.

Забезпечення безпеки корпоративних мереж включає організацію протидії будь-якому несанкціонованому вторгненню в процес функціонування, а також спробам модифікації, розкрадання, виводу з ладу або руйнування її компонентів, тобто захист всіх компонентів інформаційно-комунікаційних систем та мереж – апаратних засобів, програмного забезпечення, даних та персоналу, тощо.

Для вирішення більшої частини проблем, які виникають при функціонуванні корпоративних мереж є обробка мультимедійного контенту. Це суттєво завантажує комп'ютерну мережу та її устаткування.

Таким, чином, виходить, що захист мультимедійного контенту у корпоративних мережах є доволі складним процесом, який включає в себе цілу низку взаємопов’язаних дій із визначення важливості інформації та створення програмно-апаратних засобів для визначення рівня захисту та розробки методів підвищення інформаційної безпеки корпоративних мереж.

Метою даної роботи є розробка алгоритмів оцінки систем захисту корпоративних мереж, що забезпечить змогу точно оцінювати важливість передаваної інформації та ефективність систем захисту.

# 1 ХАРАКТЕРИСТИКИ МУЛЬТИМЕДІЙНИХ ЦЕНТРІВ

Мультимедійні центри (точніше, багатофункціональні мультимедійні комбайни) та програми (або пакети програм) включають в себе різноманітні інструменти для роботи з мультимедіа. Зокрема, крім перегляду зображень, відео та прослуховування аудіо, мультимедійні комбайни можуть надавати користувачеві можливість створювати і перетворювати медіафайли, записувати диски, дивитися і зберігати потокове відео, публікувати персональні відеоматеріали в Інтернеті, робити резервне копіювання даних і багато іншого.

## 1.1 Комп’ютер в якості домашнього мультимедійного центру

Мультимедійний центр - це насамперед комп'ютер для розваг, який замінює собою побутову техніку. Взагалі, компанії, що виробляють компоненти для ПК, давно вже прагнуть роздобути шматок від такого ласого пирога, як ринок побутової електроніки. Нещодавно компанія Intel ввела в ужиток поняття «конвергенція всіх цифрових пристроїв». Зрозуміло, що поява мультимедійних центрів є логічним продовженням конвергенції і, звичайно ж, переслідує таку глобальну мету, як поступове витіснення з ринку традиційних пристроїв побутової електроніки шляхом заміни їх на мультимедійні комп'ютери.

Дійсно, як свідчать прогнози всіх аналітичних компаній, попит на традиційні комп'ютери поступово знижується на тлі збільшення попиту на мобільні комп'ютери (ноутбуки ). У цій ситуації єдине, що залишається, - знайти гідну нішу традиційним настільним комп'ютерам. І все що для цього потрібно - це перетворити їх з традиційних комп'ютерів в нетрадиційні. Власне, саме на цю мету і орієнтована концепція мультимедійний центр і саме в цьому полягає її революційність.

Концепція мультимедійного центру має на увазі створення комп'ютерів, які повинні мати такі функціональні можливості:

- можуть заміняти собою пристрої побутової електроніки (телевізори, DVD-програвачі, стереосистеми та ін.) У цьому сенсі мультимедійні центри є «симбіозом» комп'ютера та побутової техніки;

- є основою цифрового будинку, тобто повинні мати широкосмугове підключення до Інтернету, забезпечувати взаємодію з іншими комп'ютерами і пристроями цифрового будинку, надавати користувачам доступ до збереженої на ПК інформації в будь-який час з будь-якої кімнати будинку за допомогою самих різних пристроїв;

- надавати користувачам ефективний доступ до новітніх розважальним Інтернет-сервісів, що дозволяє завантажувати фільми і музику або приймати участь в багатокористувацьких мережевих іграх.

Мультимедійні центри - це абсолютно новий тип домашніх ПК, які не просто замінюють собою традиційні домашні комп'ютери, а розширюють їх функціональність і припускають абсолютно новий формат використання ПК. Такі комп'ютери встановлюються у вітальні і підключаються до плазмової панелі або до широкоекранного рідкокристалічного монітора-телевізора. З концептуальної точки зору комп'ютери на базі платформи Intel Viiv можуть взагалі не мати клавіатури (її можна замінити пультом дистанційного управління). Але, зазираючи в найближче майбутнє, варто відзначити, що перспективи у платформи Intel Viiv вельми незавидні.

Враховуючи функціональні можливості мультимедійних центрів, можна сформулювати і основні вимоги, яким вони повинні відповідати.

Насамперед, оскільки мова йде про комп'ютери, які здатні замінити собою пристрої побутової електроніки, особлива увага повинна приділятися корпусу такого ПК. Мультимедійні центри виконуються в стильних корпусах типу Desktop, оснащених пультом дистанційного керування, які за своїм зовнішнім виглядом не відрізняються від побутових DVD-програвачів. У більшості випадків на передній панелі таких корпусів поміщається РК-екран для відображення статусу роботи комп'ютера. Саме корпус має першорядне значення для мультимедійного центру.

Прикладом ідеального корпусу для мультимедійного центру може служити Zalman HTPC Enclosure HD160 (рис. 1.1).

Рисунок 1.1. Корпус Zalman HTPC Enclosure HD160

Корпус HTPC Enclosure HD160 передбачає горизонтальне розташування, його габарити складають 435x420x160 мм. Товщина стінок корпусу дорівнює 2 мм , а лицьовій панелі - 7 мм. Зрозуміло, що це повністю виключає вібрацію, а значить, створює непогані передумови для побудови малошумних ПК.

За зовнішнім виглядом корпус HTPC Enclosure HD160 майже неможливо відрізнити від Hi- Tec- підсилювача або музичного центру. І тільки детальне дослідження лицьовій панелі (наявність кнопок Power, Reset, світлодіодних індикаторів Power LED, HDD LED, а також роз'ємів USB і Firewire) дозволяє зрозуміти, що маємо справу з комп'ютером.

Важливою обставиною є той факт, що корпус HTPC Enclosure HD160 допускає використання системних плат з формфактором ATX або microATX, а також передбачає установку стандартного блоку живлення формфактора ATX. Можлива установка повнорозмірних PCI-карт у вертикальному положенні.

Крім того, мультимедійні центри повинні бути малошумними, тому необхідно забезпечити таке поєднання комплектуючих, яке дозволяє використовувати ефективну, але в той же час малошумну систему охолодження. Вельми продуманої є конструкція корпусу і в плані можливості по створенню ефективної системи охолодження. Обидві бічні стінки мають вентиляційні отвори, виконані у вигляді дрібної сітки, у верхній кришці корпусу прямо над кулером процесора є вентиляційний отвір, а на задній панелі

встановлені два додаткових 80-мм вентилятора. Крім того, висота корпусу дозволяє застосовувати різні кулери для процесора.

Незважаючи на компактні розміри корпусу HTPC Enclosure HD160, в ньому можна розмістити до трьох жорстких дисків і, звичайно, оптичний привід. Для кріплення жорстких дисків передбачені гумові демпфери, що зменшує рівень шуму, створюваний при їх роботі.

Корпус поставляється з пультом дистанційного керування і відповідає всім вимогам, що пред'являються до корпусів для мультімедіний центрів.

Наступний важливий аспект - це аудіопідсистема мультимедійного центру. Оскільки мультимедійні центри замінюють собою і музичний центр, і DVD-програвач, і домашній кінотеатр, необхідно, щоб в них була встановлена звукова карта, що забезпечує звук у форматі 5.1 або вище.

Зрозуміло, що будь мультимедійний центр повинен бути оснащений мультиформатним оптичним приводом, що забезпечує можливість читання і запису DVD- дисків різних форматів.

Важливим аспектом для мультимедійного ПК є і його видеопідсистема. У даному випадку мова не йде про потужну ігрову відеокарту, оскільки мультимедійний центр - це не ігровий ПК. Однак відеокарта в ньому повинна мати такі функціональні можливості, як підтримка апаратного кодування і декодування різних відеоформатів, забезпечення спільної роботи з ТВ-тюнером або з платою відеозахоплення з можливостями по апаратній обробці відеосигналу.

Сучасні відеокарти оснащені такими можливостями. У відкритих на графічних процесорах ATI подібна технологія називається AVIVO, а на графічних процесорах NVIDIA - PureVideo.

Розглянемо, наприклад, можливості технології AVIVO, яка включає як цілий ряд нових відеотехнологій по захопленню і стисненню відеозображення, так і новий конвеєр, що виконує подальшу обробку відеосигналу. Відеоконвейер складається з декількох функціональних блоків, що реалізують

захоплення цифрового або аналогового відеосигналу, його кодування, декодування, постобробку та виведення на екран телевізора або дисплея.

Зрозуміло, не всі пристрої мають або використовують повний відеоконвейер - наприклад ПК, який не має ТВ-тюнера або карти відеозахоплення, не зможе забезпечити захоплення аналогового відеозображення.

Процес обробки відеосигналу в конвеєрі починається з його захоплення, під яким розуміється отримання відеосигналу і його первинна обробка, що включає кілька стадій: автоматичне посилення, аналогово-цифрове перетворення (АЦП), гребенева фільтрація та шумозниження.

Автоматичне посилення дозволяє динамічно регулювати рівень вхідного сигналу для отримання правильного контрасту кольорів і максимальної яскравості зображення. Для оцифрування аналогового сигналу при його захопленні використовується 12-розрядний АЦП, що дозволяє мінімізувати шум квантування і підвищити деталізацію сигналу для поліпшення внутрішньої обробки . Гребенева фільтрація ( 3D Comb Filtering ) - це поділ колірного і яскравістного компонента аналогового відеосигналу, що необхідний у тому випадку, якщо ці компоненти транслюються разом (наприклад, сигнали в традиційному телебаченні або композитний сигнал). Від автоматичного шумозниження при захопленні сигналу в чималому ступені залежать всі інші етапи обробки сигналу.

Після захоплення відеосигнал піддається кодуванню ( компресії ). Навіть у тому випадку, коли захоплюється цифровий сигнал, його нерідко доводиться приводити або до іншого формату, або до іншого дозволом або бітрейту . Всі нові графічні процесори сімейства ATI Radeon X1000 підтримують програмно-апаратне кодування відеосигналу (рис. 1.2).

Наступний блок відеоконвейера виконує функції апаратного декодування відеосигналу. Відомо, що відтворення відеосигналу, закодованого сучасними форматами стиснення, - вельми ресурсномістка завдання, особливо якщо мова йде про відео високої роздільної здатності. Основне навантаження при цьому

лягає на центральний процесор, що накладає певні обмеження на його продуктивність. При апаратній підтримці декодування з боку відеокарти утилізація центрального процесора знижується, в результаті чого навіть відео високої роздільної здатності можна відтворювати без пригальмовування.

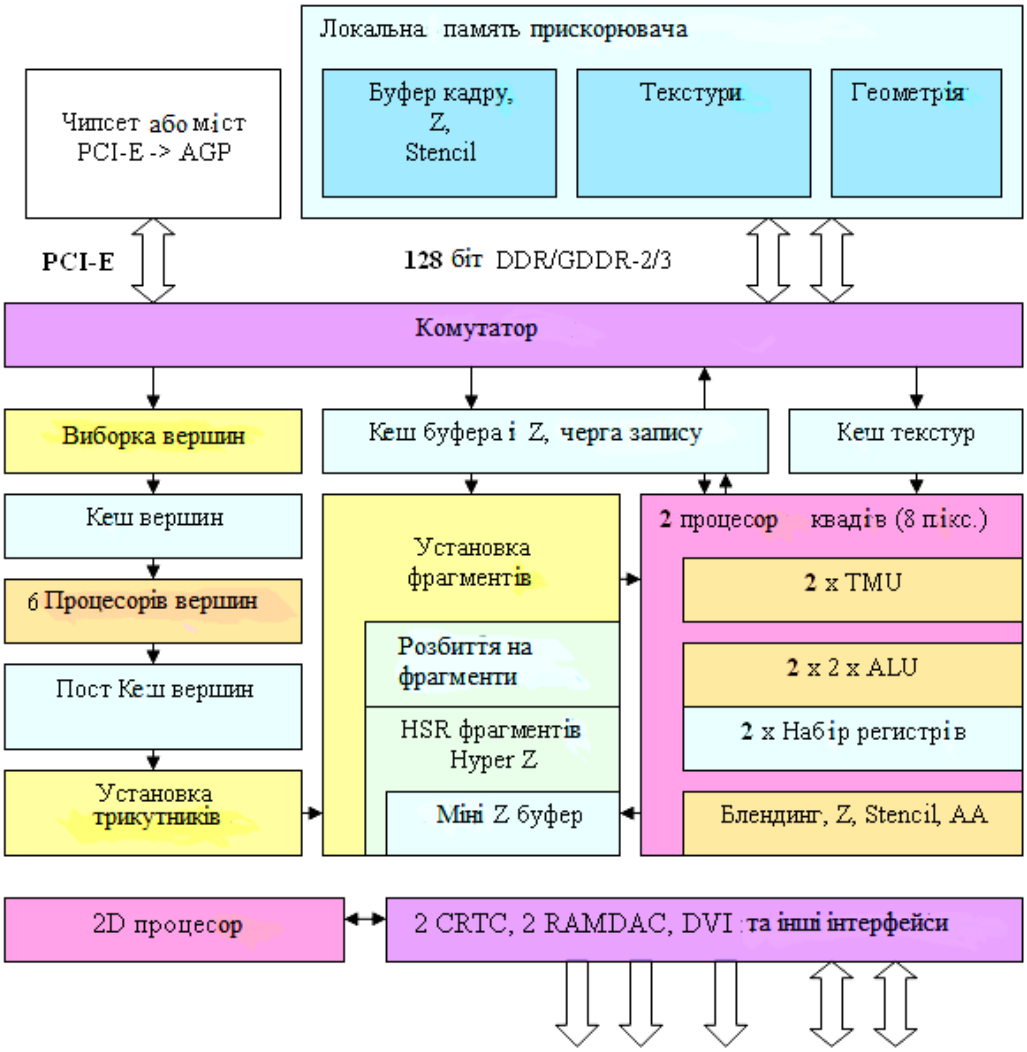


Рисунок 1.2. Загально схема чіпа відео карти сімейства ATI Radeon X1000

Відкрите з технологією AVIVO підтримують апаратне декодування таких форматів, як MPEG- 2, MPEG- 4, WMV9, H.264 і VC- 1. Нагадаємо, що кодек H.264 являє собою формат стиснення для перспективних стандартів Blu- Ray і HD -DVD. Зрозуміло , що для реалізації апаратної підтримки декодування відео необхідні як спеціальні декодери ( ATI DVD Decoder , Cyberlink H.264 video decoder), так і програвачі.

Важливим етапом в обробці відеоданих є постобробка, яка призначена для поліпшення якості виведеного на екран відео і включає такі операції, як деінтерлейсінг, масштабування зображення, зміна кількості кадрів в секунду, колірна корекція, шумозаглушення і зменшення артефактів блочності. Особливо важливий цей етап у тому випадку, коли початковий відеосигнал має розгорнення, а пристрій відображення підтримує прогресивну розгортку - це можливо, зокрема, при відтворенні телевізійного сигналу на моніторі. У цьому випадку необхідний переклад черезстрочного відеозображення в прогресивне за допомогою процесу, званого деінтерлейсинга.

Технологією AVIVO передбачається так званий векторно- адаптивний деінтерлейсінг. Якщо рух оброблюваного фрагмента в кадрі невелика, то для побудови прогресивного кадру використовуються дані одного поля. Для фрагментів з швидким рухом використовуються дані, інтерпольовані по декількох векторах, що забезпечує отриманому прогресивному кадру максимально можливу деталізацію.

Останній функціональний блок відеоконвейера AVIVO - це блок виведення зображення на екран , що включає два незалежних один від одного симетричних конвеєра для підтримки двох дисплеїв.

З усього вищесказаного випливає , що технологія AVIVO є вельми корисною функцією для мультимедійних центрів. Залишилося лише додати, що дана технологія реалізована в відкритих, побудованих на графічних процесорах сімейства ATI Radeon X1000. Оптимальним рішенням для мультимедійного центру, на наш погляд, в даному випадку буде відеокарта на базі графічного процесора ATI Radeon X1300Pro або ATI Radeon X1600XT.

Що стосується відеокарт на базі графічних процесорів компанії NVIDIA, то для мультимедійних центрів ми можемо рекомендувати відеокарти NVIDIA GeForce 7600 GT/GS, GeForce 7300 GT/GS або GeForce 6600 GT.

Вибір конкретного виробника відеокарти в даному випадку значення не має - це може бути відеокарта ASUS , Gigabyte або Sapphire. Враховуючи вимоги, пропоновані до відеопідсистеми мультимедійного центру, не зайве

зазначити, що укупі з відеокартою він, як правило, оснащується і ТБ-тюнером, що дозволяє використовувати центр як телевізор.

Наступна вимога, що пред'являється до мультимедійного центру, - це широкі комунікаційні можливості. У даному випадку мова йде про те, що мультимедійний центр повинен не тільки мати широкосмугове підключення до Інтернету, а й мати можливість ретрансляції цифрового контенту на інші ПК або пристрої. Тому, крім традиційного мережевого інтерфейсу Fast Ethernet або Gigabit Ethernet, мультимедійний центр повинен оснащуватися бездротовим адаптером стандарту 802.11g або підключатися до бездротової точки доступу (бездротового маршрутизатора). В останньому випадку бажано, щоб у мультимедійному центрі було два мережевих інтерфейсу Fast Ethernet або Gigabit Ethernet.

Ще одна вимога, що пред'являється до мультимедійного центру, - це рівень його продуктивності, який визначається встановленим процесором, а також типом і обсягом пам'яті. В ідеалі рівень продуктивності мультимедійного центру повинен відповідати типу розв'язуваних на ньому завдань. Мультимедійний центр - це не високопродуктивний ігровий ПК і не графічна станція , тому потужна процесорна підсистема в даному випадку необов'язкова. Водночас мультимедійний центр повинен забезпечувати можливість обробки цифрового контенту,  а саме: редагування цифрових фотографій, редагування і конвертування звукових файлів, редагування і конвертування відеофайлів. Крім того, враховуючи специфіку використання комп'ютера як мультіімедійного центру, його процесорна підсистема повинна надавати можливість ефективної багатопотокової і багатозадачного обробки даних.

### 1.2 Комп’ютер у складі системи домашнього кінотеатру

Для створення домашнього кінотеатру на основі персонального комп'ютера підходить тільки комп'ютер під управлінням Windows 7 або XP.

Конфігурація універсального мультимедіа комп'ютера виглядає наступним чином. Стандартний комп'ютер, який включає в себе материнську

плату з вбудованою або дискретною звуковою картою, процесор, пам'ять, жорсткий диск, відеокарту (бажано NVIDIA) обов'язково з двома відеовиходами. Звичайно, знадобляться клавіатура і миша, будь-який корпус, а також монітор.

Для того щоб комп'ютер отримав функції домашнього кінотеатру необхідно телевізор з HDMI інтерфейсом. При купівлі телевізора обов'язково потрібно подивитися яку роздільну здатність він підтримуватиме при підключенні до ПК. Також знадобиться пульт дистанційного керування. Для цих цілей можна рекомендувати Microsoft Remote Control and Receiver, але взагалі підійде практично будь-який навіть саморобний. Для ігор знадобитися джойстик. Найкращий геймпад для персонального комп'ютера це - Microsoft Xbox 360 Controlle. Для демонстрації телевізійних каналів знадобитися ТВ-тюнер, наприклад, це може бути DVB- S2 карта, призначена для прийому супутникового телебачення. Для міських жителів це може бути, наприклад, гібридний ТВ-тюнер який вміє приймати аналоговий і цифровий DVB-T сигнали. Можна обійтися IPTV, якщо провайдер надає такі послуги, в цьому випадку додатково купувати нічого не потрібно. Для перегляду YouTube та інших подібних сервісів, знадобитися тільки більш менш хороший інтернет канал.

В якості оболонки для медіацентру можна обрати MediaPortal. Взагалі існують кілька гідних альтернатив (наприклад, XBMC), але для описаних задач MediaPortal підійде ідеально. Найголовніша функція MediaPortal'a - це можливість запустити його незалежно на будь-якому підключеному екрані комп'ютера.

До відеокарти комп'ютера потрібно підключити монітор і телевізор одночасно. Якщо підключить телевізор через HDMI інтерфейс, то можна позбутись від зайвих проводів тому, що по ньому буде передаватися і відео, і звук. Після цього в настройках MediaPortal'a з'явиться опція вибору екрану запуску (рис. 1.3).

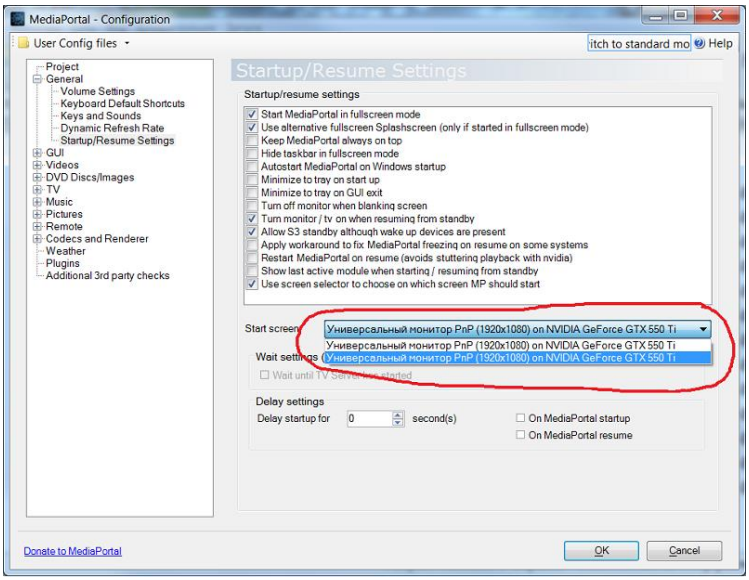


Рисунок 1.3. Опція вибору екрану запуску

Вибравши потрібну опцію, прив'язуємо MediaPortal до телевізора, тепер він буде запускатися тільки на цьому екрані. Зайшовши в налаштуваннях в розділ «Кодеки», виберемо HDMI-вихід в якості звукового рендера. Це потрібно зробити у всіх вкладках (ТБ, Відео, DVD) (рис. 1.4).

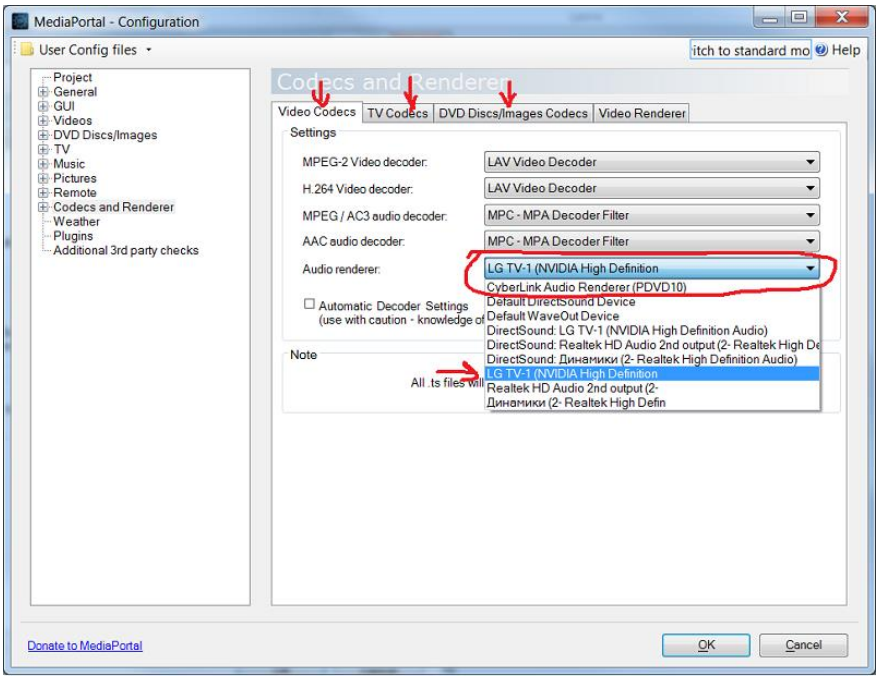


Рисунок 1.4. Вибір HDMI-вихід в якості звукового рендера

Тут же, у вкладці «відео рендер» (рис.2.4), криється перевага Windows 7 перед XP. Справа в тому, що Enhanced Video Render, доступний в Windows 7,

дозволяє використовувати всі функції MediaPortal'a та ігри одночасно. Тобто на телевізорі буде працювати MediaPortal, а за монітором ви можете грати в будь-яку гру. При цьому нічого один-один заважати не буде (рис. 1.5).

Рисунок 1.5. Незалежність роботи MediaPortal та комп’ютера

Варто знову звернути увагу на встановлення кодеків у системі. Недосвідчений користувач може скористатись спеціальними кодек-паками для MediaPortal'a - SAF v4 або SAF v6 (рис. 1.6). Потім потрібно правильно налаштувати кодеки, включивши апаратне прискорення і нарешті, вибрати їх в настройках MediaPortal'a.

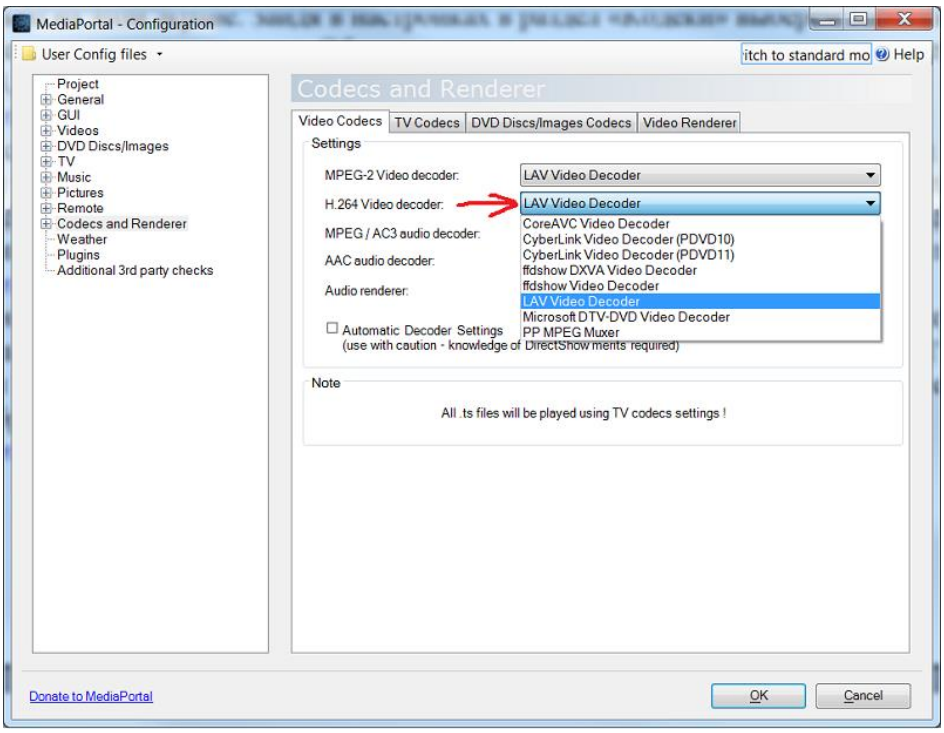


Рисунок 1.6. Спеціальні кодек-паки для MediaPortal'a - SAF v4 або SAF v6

Якщо у кодеки налаштовані правильно і відео буде програватися з апаратним прискоренням, то MediaPortal буде віднімати мінімальний відсоток ресурсів процесора (близько 2-7 %).

Як показує досвід та відгуки фахівців, відеокарти фірми NVIDIA краще AMD. Справа в тому що телевізор, підключений до другого входу відеокарти потрібно іноді вимикати. При цьому, якщо використовується відеокарта фірми NVIDA, то він не буде зникати зі списку пристроїв, навіть тоді, коли ввімкнений MediaPortal. Використовуючи відеокарту AMD, при вимиканні телевізора, він зникне зі списку пристроїв, при цьому запущений MediaPortal перевстановлюється на основний монітор, а також втрачає пристрій виведення звуку. В цьому випадку потрібно спочатку вимикати програму, і тільки потім вимикати телевізор. Тоді після включення телевізора він знову автоматично з'являється в системі. Можливо, все залежить не тільки від виробника відеокарт. Можна використовувати навіть інтегровану відеокарту, головне упевнитися, що в ній два відеовиходи і обидва можна використовувати одночасно.

Microsoft Remote Control and Receiver почне працювати відразу після того як буде підключений до комп'ютера. Але щоб отримати доступ до гнучких налаштувань під наші цілі, потрібно встановити спеціальну програму IR Server Suite (IRSS). Вона підтримує купу різних пультів, в тому числі й ті, що працюють через WinLIRC по com-порту . ПДУ від Microsoft програма розуміє відразу, налаштування інших пультів - тема окремого дослідження.

Відкриваємо налаштування MediaPortal'a і переходимо в розділ пультів, там знімаємо галочку на використанні пульта від Microsoft (рис. 1.7).

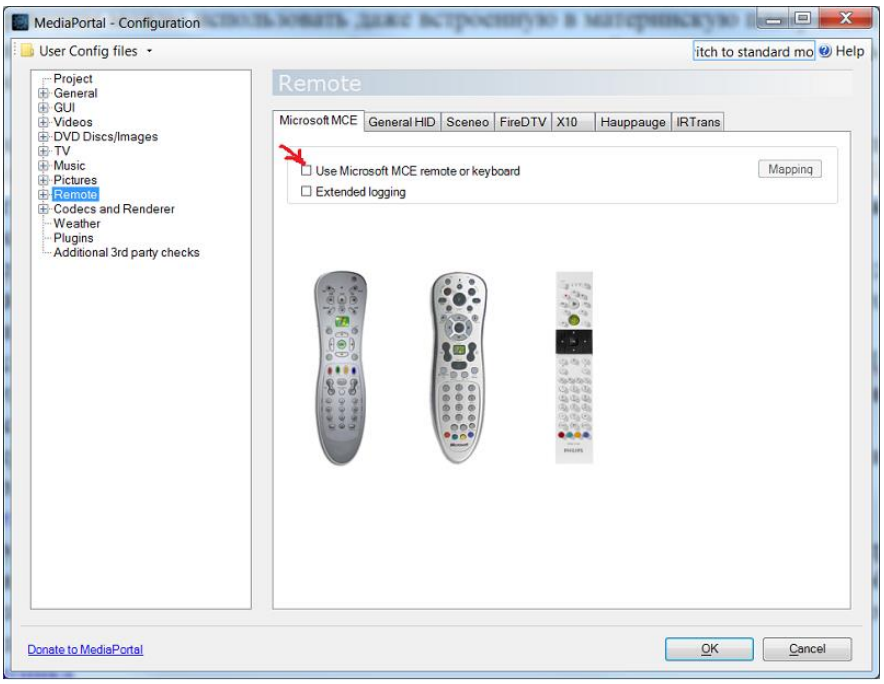


Рисунок 1.7. Налаштування дистанційних пультів керування MediaPortal'a

Перейшовши в розділ плагінів, знаходимо «MP Control». У цьому плагіні можна перепризначувати клавіші пульта за своїм смаком, створювати макроси тощо (рис. 1.8). Але взагалі, все має працювати без додаткових налаштувань. Єдине, що обов'язково потрібно зробити, це зняти галочку з опції «require focus», таким чином пульт навчиться управляти MediaPortal'ом без необхідності перемикатися на нього.

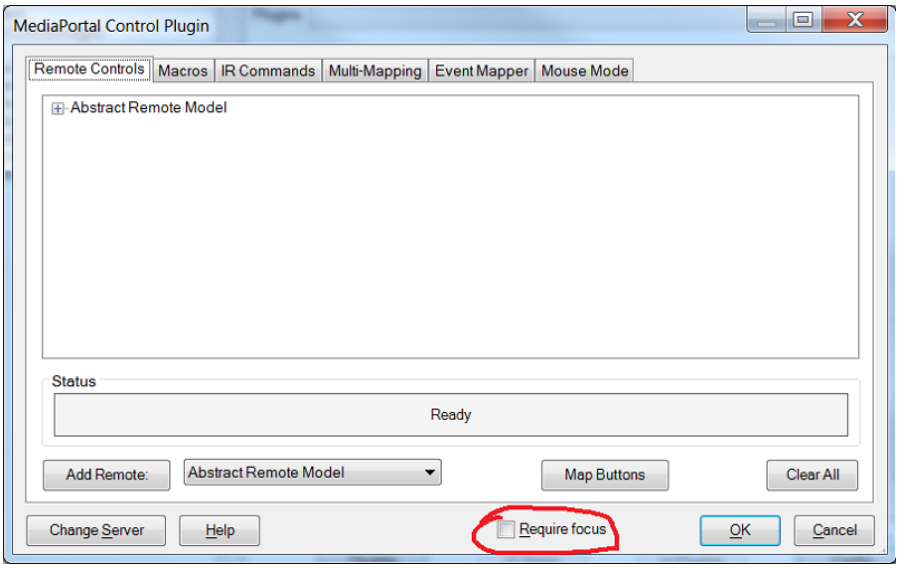


Рисунок 1.8. Налаштування клавішів пульта

У Microsoft Remote Control є ще одна чудова особливість, яка дозволяє позбутися зайвих пультів. Три кнопки у цього пульта програмуються. Кнопку TV програмуємо на вимикання, а VOL +, VOL - на управління гучністю телевізора.

Варто зауважити, що при грі за телевізором потрібно перемикати на нього звук. Це вирішується вибором виходу HDMI в якості звукового пристрою за замовчуванням перед запуском гри. Щоб кожен раз довго не налаштовувати систему, можна скористатися спеціальною програмою, що дозволяє робити це за допомогою одного кліка мишки по ярличку.

Для телебачення потрібно вставити DVB карту, поставити драйвера, налаштувати в сервері MediaPortal'a.

Мультимедійна домашня система на базі комп’ютера для трикімнатної квартири, представлена на рис. 1.9.

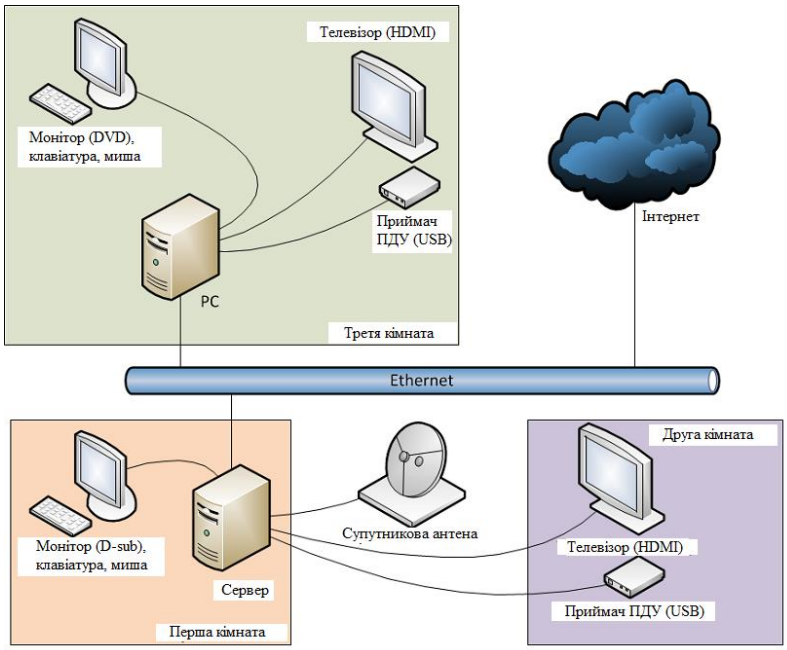


Рисунок 1.9. Мультимедійна домашня система на базі комп’ютера

У першій кімнаті знаходиться один з персональних комп'ютерів. Його завдання:

- Виступати в якості персонального комп'ютера в першій кімнаті, а також забезпечувати серфінг, перегляд фільмів, інтернет роликів, музика і т.п. Для

здійснення цього завдання в першій кімнаті поруч з системним блоком розташовуються монітор, клавіатура, миша і звукові колонки.

- Служити в якості медіацентру в другій кімнаті, забезпечувати перегляд фільмів, серіалів, ТВ-програм, а також спілкування через скайп. Для цього в другій кімнаті розташовуються телевізор і рессивер пульта дистанційного керування , а також вебкамера. Телевізор підключений HDMI кабелем, що проходить через всю квартиру. Рессивер ПДУ і камера підключені USB кабелями.

- Відповідати за прийом супутникового телебачення і подальшої трансляції потоків на клієнта, за допомогою запущеного сервера MediaPortal'a. Сигнал з супутника приймають дві DVD-карти, до яких підведені кабелі від однієї супутникової антени. Також цей комп'ютер служить як медіахранилище і «торрентокачалка». Працює він цілодобово, без зупинок.

У третій кімнаті знаходиться ще один персональний комп'ютер. Його завдання:

- Виступати в якості персонального комп'ютера в третій кімнаті. Поруч з системним блоком розташовуються - монітор , клавіатура , миша і звукові колонки.

- Одночасно служити в якості медіацентру, для перегляду роликів з YouTube і Vimeo, фільмів і серіалів. Для цього в цій же кімнаті розташовуються телевізор, підключений HDMI кабелем, і рессивер ПДУ.

- Комп'ютер активно використовується для ігрової платформи. Гра зручно управляється геймпадом на телевізорі та клавіатурою і мишкою - сидячи перед монітором. Якщо, наприклад хтось дивиться фільм за телевізором, а хтось при цьому грає у гру, то замість колонок використовуються навушники , щоб не заважати один одному.

Розглянута система дозволяє записувати ТВ-передачі. За це відповідає сервер MediaPortal'a запущений на першому комп'ютері, до нього другий комп'ютер підключається в якості клієнта по домашній мережі.

Отже, така мультимедійна система має два повноцінних робочих місця, що розташовуються в першій і третій кімнаті, плюс два повноцінних домашніх кінотеатри, що знаходяться в другій і третій кімнаті.

### 1.3 Ноутбук з мультимедійним оснащенням

Ноутбук з мультимедійним оснащенням або ноутбуки для розваг належать до найбільш дорогих споживчих портативних комп'ютерів. Вони адресовані вимогливим користувачам, яким потрібний не просто універсальний робочий лептоп, на якому можна іноді пограти в нескладну "стрілялку" або подивитися кіно, але й високопродуктивна система, здатна демонструвати HD-відео в максимальній якості і яка з легкістю справляється з будь-якими найсучаснішими комп'ютерними іграми. У певному сенсі будь-які ноутбуки можна вважати і мультимедійними, і ігровими, але ці машини - справжні професіонали у своїй справі.

Ігрові ноутбуки - особлива категорія портативних комп'ютерів, адресована любителям комп'ютерних ігор з тривимірною графікою. Ці машини оснащуються самими продуктивними центральними процесорами і графічними прискорювачами, причому інші їх характеристики можуть не бути настільки ж видатними. Зазвичай ігрові лептопи можна розпізнати, навіть не заглядаючи в список технічних характеристик: вони виділяються агресивним дизайном і незвичайним кольоровим виконанням, як правило, чорно-червоним або чорно-синім. Клавіатури геймерських ноутбуків нерідко оснащуються вбудованим підсвічуванням, а групи часто використовуваних в іграх клавіш можуть додатково виділятися кольором.

Основна маса ігрових лептопів - це великі ноутбуки з великими екранами, як правило, з діагоналлю 15,6 або 17,3 дюйма. Зустрічаються навіть моделі з 18,4-дюймовими дисплеями 18,4 дюйма. При цьому існують і невеликі тринадцатидюймові ноутбуки, оснащені потужними процесорами і продуктивною дискретною графікою, але в силу того, що в невеликому корпусі надзвичайно складно розмістити "гарячі" високопродуктивні

комплектуючі, за можливостями вони поступаються більш габаритним машинам. І вже зовсім екзотика - ігрові субноутбуки: зараз вони представлені, мабуть, єдиною моделлю Alienware M11x, яка, проте, постійно оновлюється.

Геймерські машини, як правило, оснащуються процесорами Intel високопродуктивної серії Core i7 - це як дво-, так і чотирьохядерні мобільні чіпи останнього покоління, відомі під кодовою назвою Sandy Bridge. Як дискретної графіки використовуються прискорювачі AMD серії Radeon HD 6000M і чіпи NVIDIA серії GeForce 500M, при цьому в продажу ще зустрічаються все ще зберігають конкурентоспроможність ноутбуки з графічними процесорами AMD попереднього покоління AMD Radeon HD 5000M і NVIDIA GeForce 400M, що недивно, адже конструктивно вони відрізняються нюансами.

Обов'язковий атрибут ігрового ноутбука для розваг - вінчестер великого об'єму (500-750 Гбайт), адже сучасні ігри займають чимало місця. Не рідкість - два жорсткі диски, які можна об'єднати в масиви різних рівнів, як для прискорення роботи, так і для підвищення надійності зберігання даних. Все частіше в геймерських машинах встановлюються і твердотільні SSD-накопичувачі, по продуктивності вони залишають далеко позаду навіть найшвидші вінчестери.

На випуску виключно ігрових ноутбуків спеціалізується компанія Alienware, що належить одному з найбільших виробників комп'ютерної техніки - компанії Dell. Моделі, адресовані шанувальникам комп'ютерних ігор, також є в модельних рядах багатьох провідних вендорів (рис. 1.10).

Рисунок 1.10. Ноутбук Dell Studio 17

Перш за все, нагадаємо, що всі без винятку сучасні ноутбуки - мультимедійні. Всі вони забезпечують відображення інформації в різних формах: текстовій, візуальній, звуковій, аудіовізуальній, анімаційній, а також інтерактивну взаємодію з користувачем. Тому, коли сьогодні мова йде про мультимедійні ноутбуках, маються на увазі портативні комп'ютери, орієнтовані на використання в якості мобільних медіацентрів. Це означає, передусім, розширену підтримку (в першу чергу, апаратну) різних аудіо-і відеоформатів, екран великої діагоналі і високого розширення, високоякісну, наскільки це можливо для ноутбука, аудіосистему, а також повний набір портів для підключення до побутової аудіо і відеотехніку.

Для сучасного мультимедійного ноутбука, який використовується для розваг, характерні наступні основні параметри. По-перше, дисплей з діагоналлю від 15,4 дюйма і більше. Найбільш універсальними вважаються моделі з сімнадцятидюймовий екранами, але якщо ви хочете замінити ноутбуком настільний комп'ютер, цілком можна придивитися і до лептопу з діагоналлю 18,4 дюйма і навіть з двадцатідюймовими дисплеями. По-друге, потужний дво-або чотирьохядерний процесор середнього або вищого класу, що дозволяє без проблем обробляти відео або фотографії великого розширення і, звичайно, справлятися з тривимірними іграми, - наприклад, Intel Core i5 і i7 серій або AMD Phenom II у дво, трьох або чотирьохядерному виконанні.

Абсолютний мінімум оперативної пам'яті для мультимедійного ноутбука - 2 Гбайта, краще - 4 Гбайта, не будуть зайвими і 8, і навіть 16 Гбайт. Вінчестер ноутбука, на якому будуть зберігатися фільми, музика, фотографія і гри, теж не може бути маленьким: мінімальний її обсяг - 320 Гбайт, оптимальний - 500-750 Гбайт, а найкращий варіант - два диска загальної ємністю 1,5 Тбайта.

Графічний прискорювач для мультимедійної машини так само важливий, як і для ігрової, але в подібних моделях рідко застосовуються топові моделі для екстремальних геймерів. Найчастіше мова йде про

дискретну графіку середнього та вищого середнього класів, тобто про AMD Radeon HD 6650M і HD 6630M, HD 6570M і HD 6550M або NVIDIA GeForce GTX 560M, GeForce GT 555M і GeForce GT 540M. Все це високопродуктивні чіпи останніх поколінь, на апаратному рівні підтримують відео високої чіткості, програмний інтерфейс DirectX 11 і відповідають всім вимогам, що пред'являються до потужних універсальних відеоприскорювачів.

У ноутбуці для розваг з великими екранами часто встановлюється аудіосистема підвищеної якості з двох або чотирьох гучномовців з мікросабвуфером. У багатьох виробників є модифікації з гібридним ТВ-тюнером, здатним приймати аналоговий і цифровий телесигнали. Крім того, такі машини нерідко комплектуються бездротовими пультами дистанційного керування.

У набір роз'ємів на мультимедійному ноутбуку для розваг повинні входити всі порти, необхідні для повноцінного підключення комп'ютера до домашньої аудіо і відеосистеми: насамперед, це цифровий відеоінтерфейс DVI і/або універсальний цифровий інтерфейс HDMI. Все частіше в лептопах цього класу зустрічається і новий цифровий відеоінтерфейс DisplayPort, в тому числі і у варіанті Mini DisplayPort. Крім того, в мультімендійних моделях можна зустріти багатоканальні аналогові і цифрові оптичні або коаксиальні звукові виходи.

Характеристики мультимедійного або ігрового ноутбука, важливі при його виборі:

- У мультимедійних ноутбуках найчастіше використовується процесор Pentium 4HT або Athlon XP , в бюджетних моделях - процесор Intel Celeron.

- Для забезпечення повноцінної гри або перегляду відео , дисплей ігрового ноутбука повинен бути не менше ніж 14 дюймів , оптимальний розмір дисплея - 15 дюймів. Матриця ноутбука повинна мати високу роздільну здатність (не гірше SXGA + 1400x1050), високий рівень яскравості і контрасту, реалістичність передачі кольору і високу однорідність яскравості по дисплею - щоб його краю не здавалися темніше або світліше, ніж центральні точки.

Також для того , щоб грати в ігри або переглядати відео могли декілька користувачів одночасно, дисплей мультимедійного ноутбука повинен мати великий кут огляду.

- Бажаний обсяг жорсткого диска мультимедійного ноутбука становить 60-80 Гб, швидкість його обертання - 5400 або 7200 обертів за хвилину.

- Рекомендована пам'ять мультимедійного ноутбука - це DDR 333 / 400 об'ємом від 256 до 512 Мб і вище.

- Більшість ноутбуків оснащені аудіокодеками AC- 97, які є аналогічними Аудіокодек, використовуваним в звичайних персональних комп'ютерах з інтегрованим звуком - для більшості ігрових програм цього звуку буде цілком достатньо. Однак любителі більш якісного звуку можуть придбати кращу звукову карту.

- Мало не найголовнішою складовою ігрового ноутбука є потужна відео-карта. Тим більше що, на відміну від звукової карти, зовнішніх відео-карт поки не існує, і згодом замінити вбудований чіп на більш сучасний не можна. Оптимальне відео для мультимедійного ноутбука - це графічний контролер Radeon Mobility 9600 ( M11 ) і nVidia GeForce FX 5700Go.

- Пристрої позиціонування, якими здійснюється управління ноутбуком - Touchpad, pointing stick, досить зручні для навігації в офісних програмах або як допоміжні пристрої у випадку, якщо основне навантаження лягає на клавіатуру, джойстик або кермо. До того ж, підключивши USB-мишу, можна користуватися і нею, і Touchpad одночасно. Складніше з клавіатурою - для більшості ігрових програм аркадного типу (симулятори, стрілялки тощо) клавіш не вистачає . Тому для забезпечення повноцінного процесу гри варто придбати ігровий маніпулятор (джойстик), підключити який можна за допомогою USB-порту, наявного у всіх сучасних ноутбуках.

## 1.4 Основні і допоміжні мультимедійні можливості та їх характеристики

Мультімедіа ( multimedia, M-media, від лат. multum - багато і media, medium - осередок, засоби) - комп'ютерна технологія, що забезпечує можливість створення, збереження і відтворення різнорідної інформації, включаючи текст, звук і графіку (у тому числі рухоме зображення і анімацію).

Характеристикою мультимедійних систем є якість відтворення всіх складових даних, а також можливість їх взаємопов'язаного або взаємодоповнюючe використання. Наприклад, поєднання відеоряду з текстом і звуковим супроводом; звукових фрагментів музичного твору з текстовими даними про виконуючих його музикантів і інструментах; зображення художнього твору з музичним фоном і текстом. Складовими частинами мінімального комплекту системи мультимедіа крім ПК є дисководи CD-ROM або DVD, звукова карта і стереофонічна система.

Технологія мультимедіа знайшла застосування у розробці Web- сторінок і Web -додатків.

Комплекс апаратних і програмних засобів мультимедіа дозволяє користувачеві працювати в інтерактивному режимі з різнорідними даними (графікою, текстом, звуком, відео) (рис. 1.11), організованими у вигляді єдиного інформаційного середовища.


Рисунок 1.11. Основні і допоміжні мультимедійні можливості

Розгляньмо лише основні пристрої введення інформації (рис. 1.12):

1. Клавіатура Це головний пристрій введення літерно-символьної інформації в комп’ютер, який з часів перших комп’ютерів практично не змінив свою форму та внутрішню схему. Дійсно, кількість клавіш та їх розмір на сучасних клавіатурах можуть бути різними, часто трапляються бездротові клавіатури, з кулькою трекболу тощо. Характеристики:

- кількість клавіш;
- наявність мультимедійних можливостей;
- розміри клавіш, вид, колір та стиль шрифту;
- сила натискання на клавіші, їх «звучання»;
- ергономічність.

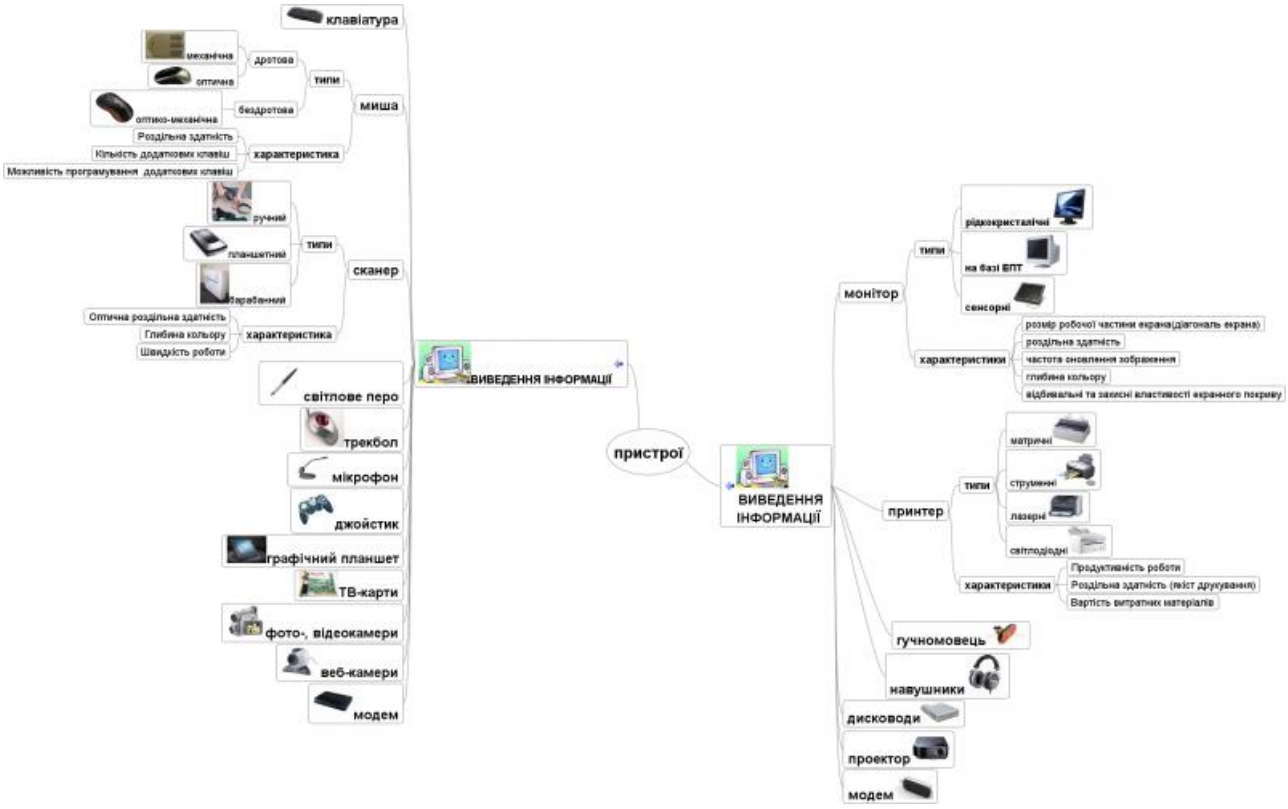


Рисунок 1.12. Пристрої введення та виведення інформації

2. Маніпулятор миша На сьогодні цей пристрій введення інформації і набуває все більшого значення, оскільки на сучасному комп’ютері працювати без миші майже неможливо. Маніпулятор миша є найпоширенішим пристроєм

для дистанційного керування графічними зображеннями на екрані, адже для його використання не треба набирати жодної команди, як це роблять за допомогою клавіатури. У разі переміщення миші по поверхні вказівник переміщується екраном у тому самому напрямку та з тією самою швидкістю. Характеристики:

- тип – механічна, оптична;
- роздільна здатність;
- кількість клавіш;
- наявність колеса прокрутки;
- наявність додаткових кнопок.

3. Сканер. Це ще один пристрій, призначений оптичним шляхом уводити в комп’ютер чорно-білу або кольорову графічну інформацію, яка до цього розміщувалася на аркуші паперу. Сканер — це «очі» комп’ютера, розроблені для введення в комп’ютер малюнків, фотознімків, креслень, схем, графіків та діаграм. Характеристики:

- тип – планшетний, ручний, барабанного типу;
- розмір зображення, що сканується;
- роздільна здатність;
- швидкість сканування;
- «глибина» кольору;
- можливість сканування фотоплівки.

До складу сучасного комп’ютера може одночасно входити багато пристроїв виведення інформації різного призначення. Основним з них, що входить до базової конфігурації персонального комп’ютера, є:

1. Монітор. Це пристрій призначений для відображення візуальної інформації. Характеристики:

- тип – ЕПТ, TFT, LCD, плазмові;
- роздільна здатність;
- частота розгортки;
- розмір екрану по діагоналі;

- час реакції матриці (TFT).

2. Принтер. Другий пристрій виведення інформації, без якого більшість користувачів не уявляють свій персональний комп’ютер, — це принтер — пристрій для роздрукування текстової чи графічної інформації. Характеристики:

- тип – матричний, струменевий, лазерний, термографічний;
- роздільна здатність;
- швидкість друку;
- формат паперу (А4, А3);
- можливість друку кольорових зображень (фото).

Мультимедійні проектори — сектор комп'ютерного ринку, що бурхливо розвивається. Вони дають змогу проектувати зображення від комп'ютера, відеомагнітофона, телевізора на великі екрани з діагоналлю понад 10 м. Їм властива висока роздільна здатність (1024 х 768 точок) та інтенсивний світловий потік (понад 1600 лм), що дає можливість застосовувати їх для презентацій у великих незатінених приміщеннях. Серед їх переваг — портативність і мобільність (маса деяких із них становить 3 кг). Практично всі мультимедійні проектори мають об'єктиви зі змінною фокусною відстанню, завдяки чому розміри зображення можна задавати, не переміщуючи проектора.

Сучасні мультимедійні проектори мають функцію тильного сканування зліва направо і знизу вгору, що дає змогу встановлювати їх із тильного боку екрана і навіть прикріпляти до стелі. При такому положенні проектор не займає багато місця і не заважає огляду. Багато мультимедійних проекторів мають вбудовану аудіосистему (підсилювач потужності та стереосистему) і забезпечують високоякісний звуковий супровід презентації у малих та великих аудиторіях.

Основою сучасного мультимедійного проектора є джерело світла і рідкокристалічний дисплей (LCD — Liquid Crystal Display,), що формують зображення. Є кілька LCD-технологій виготовлення мультимедійних проекторів.

TFT-технологія (рідкокристалічний дисплей на тонкоплівних транзисторах). Елемент зображення у такому проекторі створюється за допомогою трьох рідкокристалічних вічок (по одному на червону, зелену і синю складові зображення). Кожне вічко має керований тонкоплівний транзистор. Сукупність вічок, які керують одним кольором, утворює рідкокристалічну матрицю. Дисплей, що складається з трьох рідкокристалічних матриць, за формою є прямокутником зі сторонами 10х15 см (рис. 1.13).

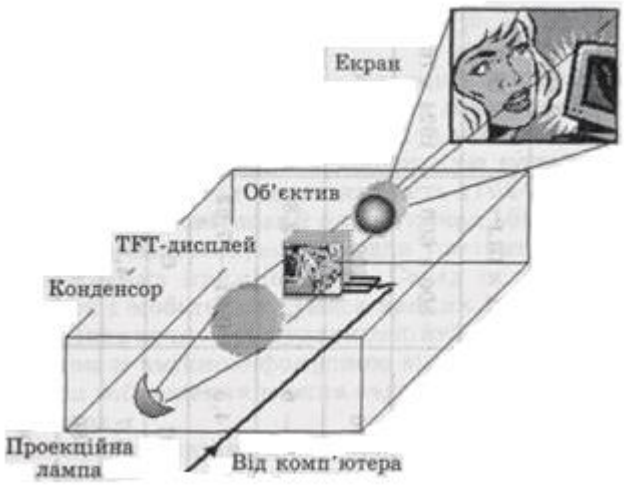


Рисунок 1.13. Система мультимедійного проектора з TFT-дисплеєм

Проекційні системи з TFT-дисплеєм особливо зручні для демонстрації даних у графічному форматі. Вони характеризуються високоякісним перенесенням кольорів і забезпечують високу швидкість зміни зображення на екрані.

*Полісиліконова LCD-технологія* ґрунтується на використанні трьох невеликих рідкокристалічних матриць (панелей) розміром від 2,3 до 3,3 см. Кожна матриця керує своїм кольором — червоним, зеленим або синім (рис. 1.14).

Матриці мають дуже добре світлопередавання і забезпечують підвищену яскравість кольорів. Проектори з полісиліконовими панелями дають змогу вручну або автоматично регулювати розмір зображення. За їх допомогою можна демонструвати як прості текстові, так і складні мультимедійні зображення.

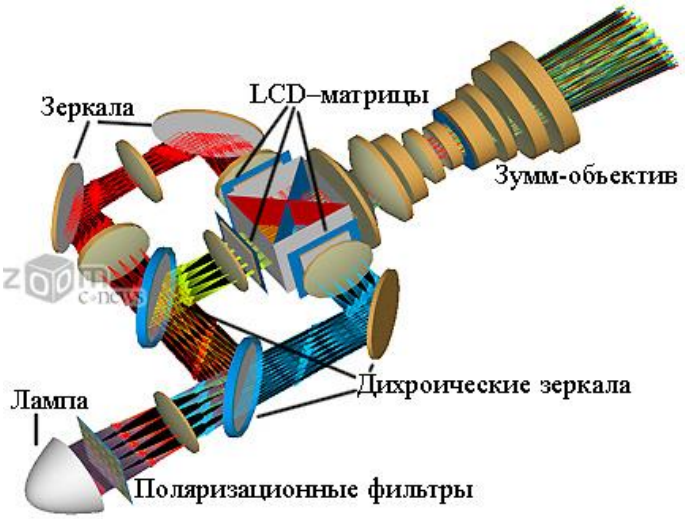


Рисунок 1.14. Схема 3LCD-проектора

Важливою перевагою проекційної технології 3LCD є відносно висока точність передачі кольорів у рамках того діапазону, який взагалі може забезпечити технологія рідких кристалів. Ця точність гарантується завдяки окремій обробці трьох колірних компонентів.

Недоліками технології 3LCD є ті обмеження, які існують у рідкокристалічних матриць, а саме: ефект пам'яті, що виникає при тривалому відображенні статичного зображення, вузькі межі перенесення кольорів. До недоліків ще відноситься необхідність використання більш потужних ламп, що пов'язано з просвітлювальним типом матриць, і, відповідно, серйозніших систем охолоджування, а також наявність міжпіксельної сітки на екрані.

DMD/DLP-технологія ґрунтується на використанні 1000 мікроскопічних дзеркал з електронним керуванням, розташованих на напівпровідниковій мікросхемі. Трикольоровий фільтр, крізь який проходить промінь світла, обертається синхронно з приладом контролю зображення. Завдяки високій швидкості зміни кадрів три окремих кольорових кадри, що з'являються послідовно один за одним, відбиваючись від мікроскопічних дзеркал, формують одне кольорове зображення (рис. 1.15).


Рисунок 1.15. DMD/DLP технології масивів мікродзеркал Texas Instumens

DMD/DLP відрізняється від інших технологій рівновагою, яскравістю зображення та тим, що вона не має зернистої структури. Схема мультимедійного проектора з DMD/DLP технологією показана на рис. 1.16.

Джерелом світла в проекційних системах може бути галогенна або металогалогенна лампа потужністю 120— 200 Вт з терміном служби від 1000 до 4000 год.

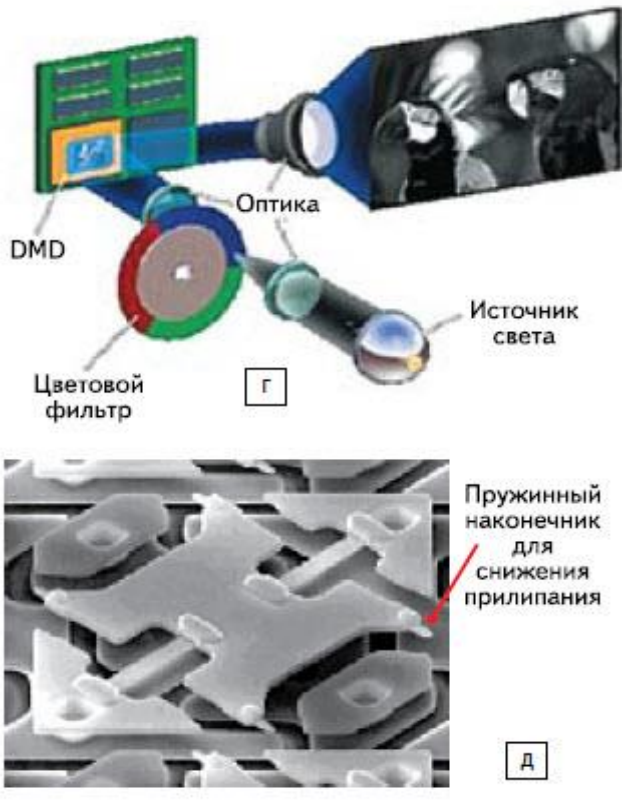


Рисунок 1.16. Схема мультимедійного проектора з DMD/DLP технологією

З розвитком технологій майже щомісяця з'являються нові, досконаліші моделі. Проектори стають яскравішими, легшими, економічнішими і дешевшими.

*Класифікація авторських засобів мультимедіа.*

Авторські засоби мультимедіа — це засоби (додатки), які мають заздалегідь підготовлені елементи для розроблення інтерактивних мультимедійних програм, їх використання є прискореною формою розроблення інтерактивного мультимедійного проекту, що в кілька разів зменшує вартість робіт. Ці засоби різняться спеціалізацією, можливостями і зручністю освоєння.

Мова сценаріїв - це об'єктоорієнтована мова програмування, у якій спеціальні оператори визначають взаємодію елементів мультимедіа, розташування активних зон, призначення кнопок тощо. Однак можливість редагування елементів мультимедіа (графічних зображень, відео, звуку) в такій мові є дуже обмеженою. Або її може навіть не бути. В основному мови сценаріїв належать до інтерпретувальних. Тому авторські засоби порівняно з іншими мають низьку швидкодію.

Авторськими засобами мультимедіа, що ґрунтуються на мові сценаріїв, є Ten Core Language (фірма Computer Teachinq), Media View (фірма Microsoft) тощо.

Основою авторського засобу цього типу є палітра значків (Icon Palette), які позначають різні функції взаємодії елементів засобу, і спрямовуючу лінію (Flow Line), яка вказує зв'язки між значками. За допомогою значків на екран виводять текст, графічні зображення, переміщують їх, відтворюють фільми, звук тощо.

Спрямовуюча лінія є своєрідним засобом побудови ієрархічної схеми додатка. На неї перетягують відповідні значки. Набір цих значків відповідає послідовності дій, які виконуються після запуску створеного додатка на виконання.

Суттєвою перевагою авторських засобів цього типу є скорочення термінів роботи з дизайном додатка зі складними функціями взаємодії.

Кадр - це тип авторських засобів подібний до типу образотворчого керування потоком даних. Він також має палітру значків. Однак зв'язки між ними можуть відображати навіть складні алгоритми, що розгалужуються. Ці авторські засоби мають високу швидкодію, але потребують автоматичного наладника, оскільки помилки візуально невловимі.

Картка з мовою сценаріїв - тип авторських засобів, що є потужним завдяки застосуванню мови сценаріїв. Однак вона сама потребує точного і жорсткого структурування сюжету. Процес розроблення додатків нагадує тут роботу з книгою. Створюють картку сторінка за сторінкою, а потім використовують гіпертекстові можливості для навігації між сторінками й об'єктами в межах сторінки.

Авторські системи постачаються з великою кількістю шаблонів, прикладів і готових графічних елементів призначеного для користувача інтерфейсу. А заздалегідь підготовлені спеціальні кнопки дають змогу керувати зовнішнім програвачем компакт-дисків, касетним магнітофоном або відеомагнітофоном.

Основним недоліком авторських засобів цього типу є неможливість забезпечити точне керування синхронізацією і виконання паралельних процесів. Наприклад, звуковий файл має запускатися і закінчуватися раніше, ніж зможе початися наступна за сценарієм подія. Використовуються такі авторські засоби в основному для розроблення гіпертекстових додатків (навчальних курсів, презентацій) та прикладних програм з інтенсивним перемі-щенням (ігор). Найкращим використанням картки з мовою сценаріїв є розроблення додатків, які можна логічно об'єднати у вигляді окремих карток із гіпертекстовими зв'язками.

Тимчасова шкала - це такі авторські засоби за структурою інтерфейсу користувача подібні до звукового редактора для багатоканального записування. Основними елементами є трупа (база даних об'єктів) і партитура (покадровий графік подій, які відбуваються з цими об'єктами). Кожна поява об'єкта з трупи в одному з каналів партитури називається спрайтом. Для керування спрайтами,

залежно від дій користувача, використовується об'єктно-подійна мова сценаріїв.

Авторські засоби на основі тимчасової шкали застосовуються для розроблення складних комерційних додатків і комп'ютерних ігор з інтенсивною мультиплікацією, в якій потрібна синхронізація різних мультимедійних складових.

Комплекс апаратних і програмних засобів мультимедіа дозволяє користувачеві працювати в інтерактивному режимі з різнорідними даними (графікою, текстом, звуком, відео), організованими у вигляді єдиного інформаційного середовища.

Мультимедіа знаходить різне застосування, включаючи освіту, медицину, виробництво, науку, мистецтво і розваги. В освіті, мультимедіа використовується в навчальних курсах, що базуються на інформаційних технологіях (медіаосвіта).

### 1.5 Інтеграція IP-TV та SAT-TV до складу мультимедійного центру

Аналіз сучасного стану і перспективи розвитку систем IP-телебачення.

IP-телебаченням (IP-TV) прийнято називати цифрову технологію багатопрограмного інтерактивного віщання телевізійного сигналу в мережах з комутацією пакетів. Технологія IP-TV в світі існує вже давно, але використовувалася переважно у вузькому крузі, будь то академічному (університетському) або урядовому. Прикладом одного з різновидів технології IP-TV є відеоконференцзв'язок. Як комерційний продукт для масового ринку IP-телебачення має не таку тривалу історію. Спочатку IP-TV впроваджували оператори, які прагнули швидко розвернути інноваційні послуги. Це були, як правило, крупні телефонні оператори і їх молоді конкуренти. Зниження вартості магістрального трафіку і скорочення доходів від традиційної телефонії змусило їх звернутися до інтерактивних мультимедійних функцій IP-TV, щоб мати переваги серед традиційних конкурентів – операторів кабельного і супутникового телебачення.

Сьогодні зростання проникнення широкосмугового доступу (ШСД) і пошук провайдерами додаткових джерел доходу є ключовими факторами розвитку технологій IP-телебачення. Провайдери ШСД починають розглядати IP-TV як додатковий спосіб підвищити рентабельність існуючих ліній абонентського доступу і отримати додаткову перевагу в конкурентній боротьбі, що загострюється. Технологія IP-TV, як один з видів цифрового телебачення, на даний момент поки що розглядається швидше як широкосмуговий додаток, додатковий сервіс, прив'язаний до надання доступу в Інтернет. Сьогодні на долю IP-TV доводиться біля одного відсотка світового телевізійного ринку. Все останнє, як і раніше, належить кабельним і супутниковим операторам, а також традиційним аналоговим телевізійним системам. IP-телебачення зараз знаходиться у стадії переходу від експериментальних запусків до масового комерційного надання.

У всьому світі діє понад 50 операторів IP-TV. Найбільші з них: Verizon Communications (США), France Telecom (Франція), Deutsche Telekom (Німеччина), British Telecom (Великобританія), FastWeb (Італія), China Telecom (Китай). Але говорити про те, що сьогодні технологія IP-TV в якійсь зі світових країн вже успішно реалізована, передчасно. В основному існують фрагменти цих мереж, дослідні зони. Іншими словами, поки ця технологія ще не покрила повністю територію якої-небудь держави.

В Україні, на території міст Києва і Одеси, в тестовому режимі послугу інтерактивного цифрового телебачення запустили оператори “Укртелеком”, “Комстар-Україна” і “Голден телеком Україна”. У комерційну експлуатацію IP-телебачення увійшло в 2010 році.

Очікується, що послуги IP-TV складуть достатньо сильну конкуренцію послугам традиційного телевіщання за рахунок низьких цін, унікального змісту і технічних нововведень. По прогнозах аналітиків, за чотири роки світова абонентська база IP-TV збільшиться уп'ятеро, з 10,8 млн. в 2007 році до 60 млн. в 2014 році. У перспективі ринок IP-TV стане одним з лідируючих разом з іншими видами цифрового телебачення. Одним з головних факторів, який

істотно сприятиме успіху IP-TV, стане збільшення попиту користувачів на інтерактивні послуги, які забезпечать вибухове зростання всієї галузі IP-TV. Також прогнозується, що виробники устаткування і компанії, розробляючі рішення IP-TV, остаточно вирішать проблеми стандартизації устаткування, що допоможе розвитку послуг.

Оскільки IP-TV говорить на мові "всесвітньої павутини", ця мережева система має можливість звести воєдино світ Інтернету і світ телебачення за рахунок конвергенції всіх форм комунікацій і розваг в єдиній гнучкій, повністю інтегрованій мультимедійній інфраструктурі.

Для реалізації технології IP-телебачення необхідна сучасна мультисервісна інфраструктура, що складається з мереж доступу, транспортної мережі, головної станції, а також кінцевих пристроїв і спеціалізованого програмного забезпечення.

На практиці доставка контента до користувача виглядає таким чином. Головне устаткування IP-TV передає, а абонентське устаткування приймає потокове відео (Streaming video). Цей термін позначає технології стиснення, скорочення і буферизації відеоданих, які дозволяють передавати відео в реальному часі через Інтернет. Головна особливість потокового відео полягає в тому, що при його передачі користувач не повинен чекати повного завантаження файлу для того, щоб його проглянути. Відеодані пересилаються безперервним потоком у вигляді послідовності IP-пакетів і програються у міру того, як передаються на абонентський пристрій. Для передачі потокового відео використовується транспортний протокол RTP. Протокол RTP переносить в своєму заголовку дані, необхідні для відновлення голосу або відеозображення в приймальному вузлі, а також дані про тип кодування інформації. RTP визначає і компенсує втрачені пакети, забезпечує безпеку передачі контента і розпізнавання інформації. Разом з RTP працює протокол RTCP. Він відповідає за перевірку ідентичності відправлених і отриманих пакетів, ідентифікує відправника і контролює завантаженість мережі. Для забезпечення мінімальних затримок і гарантованої швидкості передачі відеоданих в IP-мережі

використовується підтримка QoS, для чого може використовуватися, наприклад, відомий протокол RSVP, який забезпечує резервування необхідної ширини смуги в каналі.

Сформований потік телевізійних каналів – це потік IP-пакетів, що передаються в мережі за окремою груповою адресою, відповідною даному телеканалу. Таким чином, віщанням декількох каналів є формування декількох потоків multicast трафіка, коли кожен з каналів однозначно визначається унікальною адресою групової розсилки. Для підключення до мережі або виходу з групи розсилки використовується стандартний протокол IGMP.

IP-TV дозволяє передавати як зображення із звичайною якістю, що реалізовується аналоговим телевізором (близько 1,5 Мбіт/с), так і зображення з DVD-якістю (близько 6 Мбіт/с) і в новітньому HDTV-форматі (20 Мбіт/с). При цьому по одному інтернет-каналу може передаватися одночасно декілька програм, на мережу оператора він завантажується тільки в тому випадку, якщо абонент підписаний на цей канал.

Для проглядання потокового відео використовується спеціальна приставка до телевізора або в сучасній термінології Set top Box (STB), яка з одного боку підключена до мережі оператора (середовище віщання), а з іншої – має з'єднання з телевізором. Абонентський пристрій STB декодує відеодані і виводить розшифроване відео на екран телевізора. Організацію призначеного для користувача меню забезпечує протокол прикладного рівня HTTP.

IP-телебачення здійснює віщання телевізійного сигналу в пакетній формі по мережах передачі даних, побудованих на базі стека комунікаційних протоколів TCP/IP.

Протоколи TCP/IP були розроблені майже три десятиліття тому за замовленням Управління перспективних досліджень і розробок Міністерства оборони США і упроваджені в державній мережі DDN (defence data network), що включає мережі ARPANET і MILNET. Первинна мета була пов'язана з побудовою відмовостійкої комунікаційної мережі, яка змогла б функціонувати навіть при виході з ладу її більшої частини, наприклад, із-за ядерних

бомбардувань. У 1982 році великий внесок в розвиток стека TCP/IP вніс університет Берклі, реалізувавши протоколи стека в своїй версії ОС UNIX. Широке розповсюдження ОС UNIX привело і до широкого розповсюдження протоколу IP і інших протоколів стека. У тому ж році відбулася ще одна важлива подія в історії TCP/IP – в згаданий комплект був включений протокол перетворення адрес ARP, який ставить Ethernet-адреси у відповідності міжмережевим TCP/IP-адресам. Потім протоколи TCP/IP були реалізовані на робочих станціях сімейства Sun в мережевих файлових системах NFS (network file system) для забезпечення міжмережевих комутацій. Зараз практично неможливо знайти апаратуру або операційну систему, де не застосовувалися б в тій або іншій формі протоколи TCP/IP. На цьому ж стеку працює всесвітня інформаційна мережа Internet, чий підрозділ IETF (internet engineering task force) вносить основний внесок у вдосконалення стандартів стека, опублікованих у формі специфікацій RFC (request for comment).

Лідируюча роль стека TCP/IP пояснюється наступними його властивостями:

- TCP/IP є найбільш завершеним, стандартним і в той же час популярним стеком мережевих протоколів, що має багаторічну історію;

майже всі великі мережі передають основну частину свого трафіку за допомогою протоколу TCP/IP;

- TCP/IP – це метод одержання доступу до мережі Internet;

даний стек служить основою для створення intranet – корпоративної мережі, що використовує транспортні послуги Internet і гіпертекстову технологію WWW, розроблену в Internet;

- всі сучасні операційні системи підтримують стек TCP/IP;

- TCP/IP є гнучкою технологією для з'єднання різнорідних систем як на рівні транспортних підсистем, так і на рівні прикладних сервісів;

- TCP/IP – це стійке масштабоване міжплатформене середовище для програмних додатків клієнт-сервер.

Стек TCP/IP містить більше 100 протоколів, кожен з яких націлений на конкретне застосування в рамках об'єднаної мережі. Даний фактор робить TCP/IP надзвичайно гнучким, оскільки кожен протокол можна використовувати незалежно від інших з різною технологією транспортування.

Надійне транспортування даних між прикладними процесами шляхом встановлення логічного з'єднання в стеку протоколів TCP/IP забезпечує протокол управління передачею TCP. Протокол TCP приблизно відповідає транспортному рівню моделі OSI, але містить і деякі функції сеансового рівня. З його допомогою реалізується організація сеансу зв'язку між двома користувачами в мережі. Крім того, в його функції входить виправлення помилок і, що дуже важливе, перетворення інформації до виду дейтаграм, а також передача дейтаграм і відстежування їх проходження по мережі. TCP служить також для організації повторної передачі втрачених дейтаграм і забезпечення їх достовірності. Нарешті, в комп'ютері-адресаті TCP витягує повідомлення з дейтаграми і направляє його прикладній програмі-адресатові. Протокол TCP спирається на послуги IP.

В якості основного протоколу мережевого рівня (в термінах моделі OSI) в стеку використовується протокол міжмережевої взаємодії IP. Протокол IP спочатку проектувався як протокол передачі пакетів в складених мережах, що складаються з великої кількості локальних мереж, об'єднаних як локальними, так і глобальними зв'язками. Тому протокол IP добре працює в мережах зі складною топологією, раціонально використовуючи наявність в них підсистем і економно витрачаючи пропускну спроможність низькошвидкісних ліній зв'язку. Протокол IP включає набір правил, які втілюють в життя ідею ненадійної доставки пакетів. До основних функцій протоколу IP відносяться: перенесення між мережами різних типів адресної інформації в уніфікованій формі, маршрутизація по мережі, а також збірка і розбирання пакетів при передачі їх між мережами з різним максимальним значенням довжини пакету.

Існує три основні методи передачі трафіку в IP-мережах: unicast, broadcast, multicast. Розуміння різниці між цими методами є дуже важливим для

розуміння переваг IP-телечення і для практичної організації трансляції відео в IP-мережі. Кожен з цих трьох методів передачі використовує різні типи призначення IP-адресів відповідно до їх завдань і є велика різниця в ступені їх впливу на об'єм споживаного трафіку.

Unicast трафік (одноцільова передача пакетів) використовується перш за все для сервісів персонального характеру. Кожен абонент може запитати персональний відео контент в довільний, зручний йому час. Unicast трафік прямує з одного джерела до однієї IP-адреси призначення. Ця адреса належить в мережі тільки одному єдиному комп'ютеру або абонентському STB (рис. 1.17).

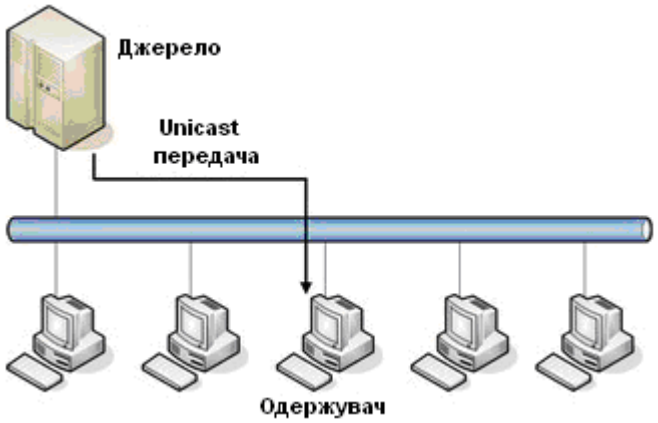


Рисунок 1.17. Unicast трафік

Число абонентів, які можуть отримувати unicast трафік одночасно, обмежене доступною в магістральній частині мережі шириною потоку (швидкістю потоку). Для випадку Gigabit Ethernet мережі, теоретична максимальна ширина потоку даних може наближатися до 1 Гб/сек, за вирахуванням смуги, необхідної для передачі службової інформації і технологічних запасів устаткування. Припустивши, що в магістральній частині мережі, для прикладу, виділяється не більше половини смуги для сервісів, яким потрібний unicast трафік. Отже, для випадку 5Мб/сек на телевізійний канал MPEG2, число одночасно одержуючих unicast трафік абонентів не може перевищувати 100.

Broadcast трафік (широкомовна передача пакетів) використовує спеціальний IP-адрес, щоб посилати один і той же потік даних до всіх абонентів даної IP-мережі (рис. 1.18). Наприклад, така IP-адреса може закінчуватися на 255 (192.0.2.255), або мати 255 у всіх чотирьох полях (255.255.255.255). Broadcast трафік приймається всіма включеними комп'ютерами (або STB) в мережі незалежно від бажання користувача. З цієї причини цей вид передачі використовується в основному для службової інформації мережевого рівня або для передачі іншої виключно вузькосмугової інформації. Для передачі відеоданих broadcast трафік не використовується.

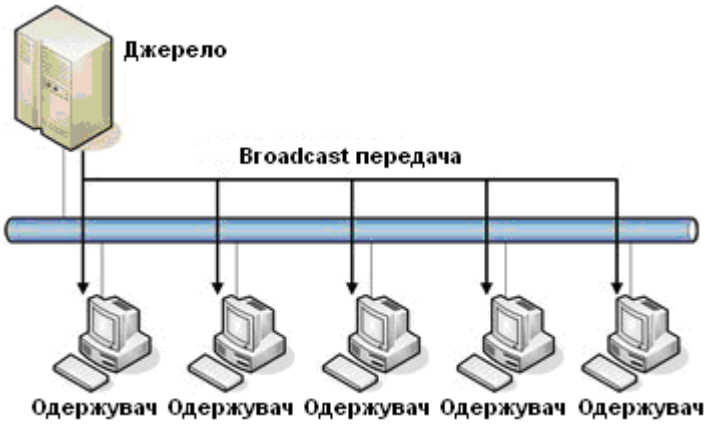


Рисунок 1.18. Broadcast трафік

Multicast трафік (групова передача пакетів) використовується для передачі потокового відео, коли необхідно доставити відеоконтент необмеженій кількості абонентів, не перенавантажуючи мережу (рис. 1.19). Це найбільш часто використовуваний тип передачі даних в IP-TV мережах, коли одну і ту ж програму дивляться велике число абонентів.

Multicast трафік використовує спеціальний клас IP-адрес призначення, наприклад адреси в діапазоні від 224.0.0.0 до 239.255.255.255. Це можуть бути IP-адреси класу D.

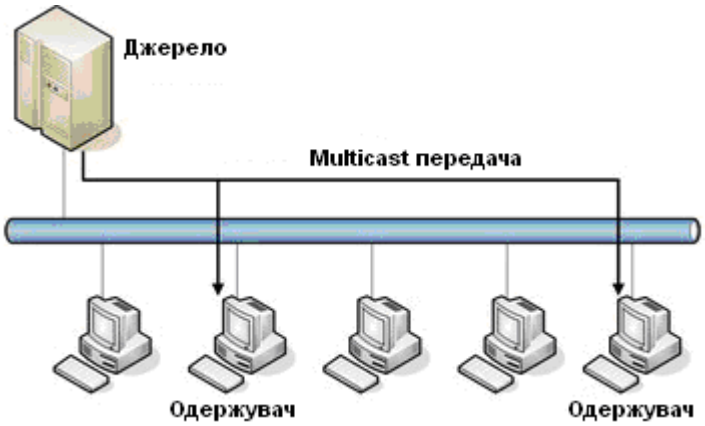


Рисунок 1.19. Multicast трафік

На відміну від unicast трафіку, multicast адреси не можуть бути призначені індивідуальним комп'ютерам (або STB). Коли дані посилаються по одному з multicast IP-адрес, потенційний приймач даних може ухвалити рішення приймати або не приймати їх, тобто буде абонент дивитися цей канал чи ні. Такий спосіб передачі означає, що головне устаткування IP-TV оператора передаватиме один єдиний потік даних по багатьом адресам призначення. На відміну від випадку broadcast передачі, за абонентом залишається вибір – приймати дані чи ні.

Важливо знати, що для реалізації multicast передачі в IP-сети повинні бути маршрутизатори підтримуючі multicast. Маршрутизатори використовують протокол IGMP для відстежування поточного стану груп розсилки (а саме, членство в тій або іншій групі того або іншого кінцевого вузла мережі).

Основні правила роботи протоколу IGMP наступні:

- кінцевий вузол мережі посилає пакет IGMP типу report для забезпечення запуску процесу підключення до групи розсилки;

- вузол не посилає ніяких додаткових пакетів при відключенні від групи розсилки;

- маршрутизатор multicast через певні тимчасові інтервали посилає в мережу запити IGMP. Ці запити дозволяють визначити поточний стан груп розсилки;

- вузол посилає у відповідь пакет IGMP для кожної групи розсилки до тих пір, поки є хоч би один клієнт даної групи.

Завантаження магістральної частини мережі multicast трафіком залежить тільки від кількості трансльованих в мережі каналів.

У ситуації з Gigabit Ethernet мережею, припустивши, що половину магістрального трафіку виділяється під multicast передачу, виходить близько 100 телевізійних каналів MPEG-2, кожен з яких має швидкість потоку даних 5 Мб/сек.

Зрозуміло, в IP-TV мережі присутні одночасно всі три види трафіку – broadcast, multicast і unicast. Операторові, плануючому оптимальну величину пропускної спроможності мережі, необхідно враховувати різний механізм впливу різних технологій IP-адресації на об'єм трафіку. Наприклад, оператор повинен ясно уявляти собі, що надання послуги “відео по замовленню” великому числу абонентів вимагає дуже високої пропускної спроможності магістральної мережі. Одним з вирішень цієї проблеми є децентралізація в мережі відеосерверів. В цьому випадку центральний відеосервер замінюється на декілька локальних серверів, рознесених між собою і наближених до периферійних сегментів багаторівневої ієрархічної архітектури IP-мережі.

Можливості протоколу IP дозволяють надавати широкий пакет інтерактивних і інтегрованих послуг, таких, наприклад, як:

- live TV (“власне IP-телебачення”). Віщання в реальному часі з використанням режиму IP-multicast. Базовою послугою, перш за все, є багатопрограмна трансляція телевізійних каналів, або власне IP-телебачення. Тут можуть бути реалізовані два варіанти проглядання телепрограм: перший – оператором формується декілька пакетів телеканалів, з яких глядачі можуть вибирати бажаний набір, причому кожен пакет має свою абонентську плату; другий – глядачі формують індивідуальні пакети з каналів, що транслюються оператором; абонентська плата визначається вартістю вибраних каналів, що входять в індивідуальний пакет;

- near video on demand (“віртуальний кінотеатр”). Трансляція фільмів з відеосервера оператора з жорстко визначеним розкладом сеансів, коли абонент купує зручний йому за часом сеанс для проглядання фільму. Тобто декілька екземплярів кожного з фільмів запускається на відтворення “по кругу” із зсувом початку відтворення в часі, і підписчик дістає доступ до каналу, на якому відтворюється конкретний фільм. Незручність для абонента полягає в тому, що він не може почати проглядання фільму в будь-який довільний момент часу. Перевагою для оператора є використання звичайної технології IP-адресації multicast, яка дуже сильно економить об'єм трафіку в магістральній мережі оператора. Так само, для зниження об'ємів трафіку, оператора надає можливість перегляду не дуже великої кількості фільмів, що зазвичай не перевищує двох-трьох десятків, як правило, це нові фільми, що недавно вийшли в прокат;

- video on demand (“відео по замовленню”). Фільм з відеосервера оператора персонально транслюється абонентові в будь-який довільно вибраний абонентом момент часу. В основі цього завдання достатньо складна технологія. В даному випадку кожному абонентові посилається його власний контент, який він запитав, і мережі передачі даних, у свою чергу, повинні мати велику пропускну спроможность. Об'єм трафіку тут залежить не від кількості фільмів, а від кількості користувачів цієї послуги, оскільки використовується персональна трансляції відеоданих абонентові за технологією IP-адресації unicast. На відміну від послуги “віртуальний кінотеатр” кількість фільмів тут набагато більше і може досягати іноді декількох тисяч. З'являється ряд дуже зручних призначених для користувача функцій віртуального відеоплеєра – перемотування назад, вперед, пауза;

- pay per view (“платний перегляд”). Покупка і перегляд абонентом окремо вибраних програм (наприклад, фінал чемпіонату світу по футболу). Трансляція ведеться в режимі реального часу і використовується технологія IP-адресації multicast;

- personal video recorder (“персональний відеомагнітофон”). Збереження контента в мережі або STB з метою подальшого індивідуального перегляду. На відеосервері оператора абонентові виділяється певний об'єм пам'яті і надається інтерфейс з аналогічними відеомагнітофону функціями для цифрового запису і відтворення телепередач. Абонент може по своєму бажанню записувати, стирати, відтворювати, перемотувати свої особисті записи. Тут також використовується технологія IP-адресації unicast;

- time shifted TV (“телебачення із зрушенням за часом”). Можливість повтору вподобаних фрагментів передачі за допомогою каналу, що передає контент із затримкою (зазвичай кратною 1 годині). Абонент купує послугу проглядання заздалегідь записаних на відеосервері програм. Послуга і сервісні функції, що реалізовуються в ній, близькі до “відео по замовленню”. Також використовується технологія IP-адресації unicast;

- services on demand (“сервіси по замовленю”). Замовлення товарів і послуг додому, різна довідкова інформація, розклад транспорту, готельний сервіс і тому подібне. Дані послуги близькі до аналогічних сервісів в Інтернеті;

- remote recording capabilities (“дистанційне керування відеомагнітофоном”). Засоби для управління сервісами з мобільного телефону, ПК і інших пристроїв;

- interactive services (“інтерактивні сервіси”). Забезпечення двостороннього каналу, зворотнім зв'язком між користувачем і виробником контента, а також іншими користувачами в цілях інтерактивної взаємодії;

- multiple camera (“підтримка декількох камер”). Можливість абонента перемикати ТВ-камери, що використовуються під час трансляції;

- net-surf on TV (“доступ в Інтернет”). За допомогою все того ж IP-підключення користувачеві надається доступ в інтернет з телевізора;

- videoconference (“відеоконференція”). Послуга надає можливість встановлювати відеоконференцзв'язок.

Послуги IP-TV повинні змінити характер використання телевізора, перевівши його на новий рівень. Багаті інтерактивні функції, що перетворюють

телевізори на мультимедійні центри, роблять IP-TV революційною технологією в цифровому телебаченні.

Завдяки передачі відеосигналу за допомогою протоколу IP з'являється ряд очевидних переваг:

- висока якість відеосигналу і велика різноманітність програм. По суті, технологія IP-TV не має обмежень по кількості каналів і якості трансльованого контента. Все залежить лише від пропускної спроможності мережі і території її обхвату. IP-мережі дозволяють вже зараз доставляти відеосигнал довільної якості, наприклад зображення HDTV із звуком Dolby Surround;

- інтерактивність. Можливість оператора взаємодіяти з абонентами в реальному часі, реагуючи на їх поведінку (перемикання ТВ-каналів, вибір пунктів меню на екрані телевізора, часу проглядання фільмів або прослуховування музики, голосування і так далі);

- інтеграція послуг. Технологія Video-over-IP дозволяє надати не тільки традиційну послугу проглядання ТВ-каналів на якісно вищому рівні, але і впровадити абсолютно нові інформаційні, комунікаційні, освітні і розважальні послуги;

- економія засобів на кабельній системі. Можливість використання існуючої інфраструктури широкосмугової мережі, таким чином, немає необхідності будувати і обслуговувати додаткову кабельну інфраструктуру;

- ефективне використання IP-мережі. Надання повного набору послуг Triple Play (Data, VoIP, TVoIP) по одиному широкосмуговому каналу.

Проблеми розвитку IP-телебачення в Україні. Серед чинників, що обмежують розвиток IP-телебачення, можна відзначити високу конкуренцію традиційних операторів, відносно низький рівень проникнення широкосмугового доступу, серйозні техніко-організаційні труднощі, високий рівень необхідних інвестицій і нерозвиненість сервісної сфери української економіки. В сукупності ці чинники знижують темпи зростання клієнтської бази, збільшують термін окупності інвестицій, а значить, знижують привабливість технології для операторів.

Впровадження IP-телебачення також стримується необхідністю модернізації мережевої інфраструктури. Для реалізації повноцінного ТВ-сервісу оператор повинен не тільки забезпечити користувачеві достатньо широку смугу в “останній милі”, але і значно розширити пропускну спроможність своєї транспортної мережі. Доставка відеосигналу обумовлює набагато вищі вимоги до мережі з погляду параметрів швидкості доставки, затримки даних і втрат пакетів, чим просто високошвидкісний доступ до Інтернету.

Перешкодою на шляху розвитку IP-телебачення стає і відсутність портфеля успішних впроваджень на широкій клієнтській базі. Більшість операторів розвернули лише дослідні зони, які працюють з декількома тисячами клієнтів.

Не дивлячись на великі можливості IP-TV, розповсюдження цієї технології гальмується бажанням операторів окупити інвестиції, вкладені в існуючі мережі. Сьогодні вартість переходу на IP-TV робить цю технологію недоступною більшості малих телекомунікаційних компаній. Поточний рівень необхідних інвестицій на одного абонента (від $1000 до $2000) робить проблематичною окупність сервісу. Для істотного зниження операційних витрат, включаючи витрати на контент, необхідне масштабування бізнесу і розширення клієнтської бази. Масштабування бізнесу вимагає значної модернізації транспортної мережі, мережі доступу, програмного забезпечення і операційних процесів. А надання користувачам реальних переваг у вигляді вигідних тарифів і унікальних послуг сформують звичку до масового їх споживання.

# 2 ТЕХНОЛОГІЇ ПОБУДОВИ КОРПОРАТИВНИХ МЕРЕЖ

## 2.1 Концепція корпоративної мережі

Будь-яка організація - це сукупність взаємодіючих елементів (підрозділів), кожен з яких може мати свою структуру. Елементи пов'язані між собою функціонально, тобто вони виконують окремі види робіт у рамках єдиного бізнес-процесу, а також інформаційно, обмінюючись документами, факсами, письмовими та усними розпорядженнями і т.д. Крім того, ці елементи взаємодіють із зовнішніми системами, причому їх взаємодія також може бути як інформаційним, так і функціональним. І ця ситуація справедлива практично для всіх організацій, яким би видом діяльності вони не займалися - для урядової установи, банку, промислового підприємства, комерційної фірми і т.д.

Такий загальний погляд на організацію дозволяє сформулювати деякі загальні принципи побудови корпоративних інформаційних систем, тобто інформаційних систем в масштабі всієї організації.

Призначення корпоративної мережі. Корпоративна мережа - система, що забезпечує передачу інформації між різними додатками, використовуваними в системі корпорації. Корпоративна мережа являє собою мережу окремої організації. Корпоративною мережею вважається будь-яка мережа, що працює по протоколу TCP / IP і використовує комунікаційні стандарти Інтернету, а також сервісні додатки, що забезпечують доставку даних користувачам мережі. Наприклад, підприємство може створити сервер Web для публікації оголошень, виробничих графіків та інших службових документів. Службовці здійснюють доступ до необхідних документів за допомогою засобів перегляду Web.

Сервери Web корпоративної мережі можуть забезпечити користувачам послуги, аналогічні послуг Інтернету, наприклад роботу з гіпертекстовими сторінками (що містять текст, гіперпосилання, графічні зображення та звуки), надання необхідних ресурсів по запитах клієнтів Web, а також здійснення доступу до баз даних. У цьому керівництві всі служби публікації називаються "службами Інтернету" незалежно від того, де вони використовуються (в

Інтернеті або корпоративної мережі).

Корпоративна мережа, як правило, є територіально розподіленої, тобто об'єднує офіси, підрозділи та інші структури, що знаходяться на значній відстані один від одного. Принципи, за якими будується корпоративна мережа, досить сильно відрізняються від тих, що використовуються при створенні локальної мережі. Це обмеження є принциповим, і при проектуванні корпоративної мережі слід вживати всіх заходів для мінімізації обсягів переданих даних. В іншому ж корпоративна мережа не повинна вносити обмежень на те, які саме додатки і яким чином обробляють стерпну по ній інформацію.

Процес створення корпоративної інформаційної системи

Можна виділити основні етапи процесу створення корпоративної інформаційної системи:

• провести інформаційне обстеження організації;

• за результатами обстеження вибрати архітектуру системи та апаратно-програмні засоби її реалізації. за результатами обстеження вибрати та / або розробити ключові компоненти інформаційної системи;

• система управління корпоративною базою даних;

• система автоматизації ділових операцій та документообігу;

• система управління електронними документами;

• спеціальні програмні засоби;

• системи підтримки прийняття рішень.

Розглянемо послідовно кожне з цих етапів.

**Інформаційне обстеження.** Інформаційна система потрібна організації для того, щоб забезпечувати інформаційно-комунікаційну підтримку її основної та допоміжної діяльності. Тому перш, ніж вести мову про структуру та функціональне наповнення інформаційної системи, необхідно розібратися в цілях і завданнях самої організації, щоб зрозуміти, що ж потрібно автоматизувати.

Відповіді на поставлені питання можна отримати тільки після детального інформаційного обстеження компанії, цілями якого є:

• формулювання та опис функцій кожного підрозділу компанії, а також вирішуються ними завдання;

• опис технології роботи кожного з підрозділів компанії і розуміння, що необхідно автоматизувати і в якій послідовності;

• опис технології роботи кожного з підрозділів і пов'язаних з ними інформаційних потоків;

• відображення технології на структуру, визначення її функціонального складу і кількості робочих місць в кожному структурному підрозділі компанії, а також опис функцій, які виконуються (автоматизуються) на кожному робочому місці;

• опис основних шляхів та алгоритми проходження вхідних, внутрішніх та вихідних документів, а також технології їх обробки.

Результатом обстеження є моделі діяльності компанії, і її інформаційної інфраструктури, на базі яких розробляються проект корпоративної інформаційної системи, вимоги до програмно-апаратних засобів і специфікації на розробку прикладного програмного забезпечення, якщо в цьому є необхідність.

При виборі описуваних коштів необхідно звернути увагу на те, щоб робота з ними була б доступна не тільки професійним працівникам, а й більш широкого класу.

**Архітектура.** За результатами обстеження необхідно вибрати архітектуру системи. Для корпоративних систем рекомендується архітектура клієнт / сервер. Архітектура клієнт / сервер надає технологію доступу кінцевого користувача до інформації в масштабах підприємства. Таким чином, архітектура клієнт / сервер дозволяє створити єдине інформаційне простір, в якому кінцевий користувач має своєчасний і безперешкодний (але санкціонований) доступ до корпоративної інформації.

Інформаційне обстеження дозволяє вибрати апаратно-програмну реалізацію системи.

**Вибір СУБД.** Вибір системи управління для корпоративної бази даних - один з ключових моментів у розробці інформаційної системи. На Російському ринку присутні практично всі СУБД, що належать до елітного класу - Oracle, Informix, Sybase, Ingres. Питання, яку СУБД використовувати, можна вирішити тільки за результатами попереднього обстеження та отримання інформаційних моделей діяльності.

**Вибір системи автоматизації документообігу.** Плутанина з документами (їх затримки, втрати, дублювання, довгий переміщення від одного виконавця до іншого і т.д.) - болюча проблема для будь-якої компанії.Тому система автоматизації документообігу, яка дозволяє автоматизувати ручні, рутинні операції, автоматично передавати і відслідковувати переміщення документів всередині корпорації, контролювати виконання доручень, пов'язаних з документами і т.д. - Одна з найважливіших складових інформаційної системи.

**Вибір програмних засобів для управління документами.** Поява на ринку систем управління електронними документами - EDMS (Electronic Document Management Systems) викликане прагненням скоротити потік паперових документів і хоча б частково зменшити труднощі, що виникають у зв'язку з їх зберіганням, пошуком і обробкою. На відміну від документів на паперових носіях електронні документи забезпечують переваги при створенні, спільному використанні, пошук, поширенні та зберіганні інформації. Системи EDMS реалізують введення, зберігання і пошук всіх типів електронних документів, як текстових, так і графічних. За допомогою систем цього класу можна організувати зберігання в електронному вигляді адміністративних і фінансових документів, факсів, технічної бібліотеки, зображень, тобто всіх документів, що входять в організацію та циркулюючих у ній.

**Вибір спеціалізованих прикладних програмних засобів.** При всієї описаної спільності кожна компанія має свою специфіку, яка визначається

родом її діяльності. Вибір спеціалізованих програмних засобів у значній мірі залежить від цієї специфіки.

Абсолютно для всіх компаній необхідно мати у складі інформаційної системи стандартний набір додатків, таких як текстові редактори, електронні таблиці, комунікаційні програми і т.д. Одним із критеріїв вибору подібних систем повинна бути можливість їх нескладної інтеграції в корпоративну інформаційну систему.

**Системи підтримки прийняття рішень.** Необхідно відзначити спеціальний клас додатків - систем підтримки прийняття рішень, що дозволяють моделювати правила та стратегії бізнесу і мати інтелектуальний доступ до неструктурованої інформації. Системи подібного класу засновані на технологіях штучного інтелекту.

**Структура корпоративної мережі.** Для підключення віддалених користувачів до корпоративної мережі самим простим і доступним варіантом є використання телефонного зв'язку. Там, де це можливо, можуть використовуватися мережі ISDN. Для об'єднання вузлів мережі в більшості випадків використовуються глобальні мережі передачі даних. Навіть там, де можлива прокладка виділених ліній (наприклад, в межах одного міста) використання технологій пакетної комутації дозволяє зменшити кількість необхідних каналів зв'язку і - що важливо - забезпечити сумісність системи з існуючими глобальними мережами. Підключення корпоративної мережі до Internet виправдано, якщо вам потрібен доступ до відповідних послуг. Використовувати Internet як середовище передачі даних варто лише тоді, коли інші способи недоступні і фінансові міркування переважують вимоги надійності та безпеки. Якщо ви будете використовувати Internet тільки як джерело інформації, краще користуватися технологією "з'єднання по запиту" (dial-on-demand), тобто таким способом підключення, коли з'єднання з вузлом Internet встановлюється тільки з вашої ініціативи і на потрібний вам час. Це різко знижує ризик несанкціонованого проникнення у вашу мережу ззовні. Для передачі даних усередині корпоративної мережі також варто використовувати

віртуальні канали мереж пакетної комутації. Основні переваги такого підходу - універсальність, гнучкість, безпека.

**Обладнання корпоративних мереж.** Корпоративна мережа - це досить складна структура, що використовує різні типи зв'язку, комунікаційні протоколи та способи підключення ресурсів.

Все обладнання мереж передачі даних можна умовно розділити на два великі класи - периферійне, яке використовується для підключення до мережі кінцевих вузлів, і магістральне або опорне, реалізує основні функції мережі (комутацію каналів, маршрутизацію і т.д.). Чіткої межі між цими типами немає - одні й ті ж пристрої можуть використовуватися в різних якостях або поєднувати ті й інші функції. Слід зазначити, що до магістрального устаткування звичайно пред'являються підвищені вимоги в частині надійності, продуктивності, кількості портів і подальшої розширюваності. Периферійне обладнання є необхідним компонентом будь-якої корпоративної мережі. Функції ж магістральних вузлів може брати на себе глобальна мережа передачі даних, до якої підключаються ресурси. Як правило, магістральні вузли у складі корпоративної мережі з'являються тільки в тих випадках, коли використовуються орендовані канали зв'язку або створюються власні вузли доступу.

Периферійне обладнання корпоративних мереж з точки зору виконуваних функцій також можна розділити на два класи. По-перше, це маршрутизатори (routers), службовці для об'єднання однорідних LAN (як правило, IP або IPX) через глобальні мережі передачі даних. У мережах, які використовують IP або IPX в якості основного протоколу - зокрема, в тій же Internet - маршрутизатори використовуються і як магістральний устаткування, що забезпечує стиковку різних каналів і протоколів зв'язку. Маршрутизатори можуть бути виконані як у вигляді автономних пристроїв, так і програмними засобами на базі комп'ютерів і спеціальних комунікаційних адаптерів.

Другий широко використовуваний тип периферійного обладнання - шлюзи (gateways), що реалізують взаємодію додатків, що працюють у різних

типах мереж. У корпоративних мережах використовуються в основному шлюзи OSI, що забезпечують взаємодію локальних мереж з ресурсами X.25 і шлюзи SNA, що забезпечують підключення до мереж IBM. Повнофункціональний шлюз завжди являє собою програмно-апаратний комплекс, оскільки повинен забезпечувати необхідні для додатків програмні інтерфейси.

Всі найбільші постачальники мережевого обладнання пропонують набори продуктів, надають керівникам інформаційних служб широкі можливості для побудови корпоративних мереж. Вони включають різноманітні апаратні засоби (концентратори, маршрутизатори, комутатори), орієнтовані на створення систем на базі передових комунікаційних технологій, включаючи Fast Ethernet, режим асинхронної передачі (ATM) і віртуальні мережі. Інтеграція цих технологій в широкомасштабні інформаційні системи спрямована на підвищення пропускної здатності.

**Багатошарове подання корпоративної мережі.** Корпоративну мережу корисно розглядати як складну систему, що складається з декількох взаємодіючих шарів. В основі лежить шар комп'ютерів-центрів збереження та обробки інформації, і транспортна підсистема, що забезпечує надійну передачу інформаційних пакетів між комп'ютерами.

Над транспортною системою працює шар мережевих операційних систем, який організовує роботу додатків в комп'ютерах і надає через транспортну систему ресурси свого комп'ютера в загальне користування.

Над операційною системою працюють різні додатки, але із-за особливої ролі систем управління базами даних, що зберігають у впорядкованому вигляді основну корпоративну інформацію і виробляють над нею базові операції пошуку, цей клас системних додатків зазвичай виділяють в окремий шар корпоративної мережі.

На наступному рівні працюють системні сервіси, які, користуючись СУБД, як інструментом для пошуку потрібної інформації серед мільйонів і мільярдів байт, що зберігаються на дисках, надають кінцевим користувачам цю інформацію в зручній для прийняття рішення формі, а також виконують деякі

загальні для підприємств усіх типів процедури обробки інформації. До цих сервісів відноситься служба World Wide Web, система електронної пошти, системи колективної праці та багатьох інших.

І, нарешті, верхній рівень корпоративної мережі представляють спеціальні програмні системи, які виконують завдання, специфічні для даного підприємства або підприємств даного типу. Прикладами таких систем можуть служити системи автоматизації банку, організації бухгалтерського обліку, автоматизованого проектування, управління технологічними процесами і т.п.

Стратегічні рішення, як правило, впливають на образ мережі в цілому, зачіпаючи декілька шарів, хоча спочатку стосуються тільки одного конкретного шару або навіть окремої підсистеми цього шару. Таке взаємний вплив продуктів і рішень потрібно обов'язково враховувати при плануванні технічної політики розвитку мережі, інакше можна зіткнутися з необхідністю термінової і непередбаченої заміни, наприклад, мережевої технології, через те, що нова прикладна програма зазнає гострий дефіцит пропускної здатності для свого трафіку.

Канали зв'язку корпоративної мережі. Перша проблема, яку доводиться вирішувати при створенні корпоративної мережі - організація каналів зв'язку. Канали зв'язку - створюються по лініях зв'язку за допомогою складної електронної апаратури та кабелів зв'язку.

Кабель зв'язку - це довгомірних виробів електротехнічної промисловості.Існують безліч різних модифікацій кабелів для ЛОМ:

• тонкі коаксіальні кабелі;

• товсті коаксіальні кабелі;

• екрановані виті пари, які виглядають як електрична проводка;

• неекрановані кручені пари;

• оптоволоконні кабелі, які можуть працювати на великих відстанях і з більшою швидкістю, ніж інші типи кабелів. Проте їх прокладання та мережеві адаптери для них досить дорогі.

З кабелів зв'язку (і маси інших речей) будують лінії зв'язку. . Довжина ліній зв'язку коливається від десятків метрів до десятків тисяч кілометрів. У будь-яку більш-менш серйозну лінію зв'язку, крім кабелів, входять: траншеї, колодязі, муфти, переходи через ріки, море й океани, а також грозозащита (так само як і інші види захисту) ліній.

За вже побудованим лініях зв'язку організовують канали зв'язку. При цьому канали за характером переданих сигналів можуть бути аналоговими або цифровими. Отже, на одній лінії зв'язку одночасно можна створити як аналогові, так і цифрові канали, що функціонують окремо. Причому якщо лінію, як правило, будують і здають відразу всю, то канали вводять поступово. Вже по лінії можна дати зв'язок, але таке використання доволі дорогих споруд дуже неефективно.Тому застосовують апаратуру каналоутворення. Число каналів збільшують поступово, встановлюючи все більш потужну апаратуру каналоутворення (іноді кажуть - мультиплексування, особливо стосовно до цифрових каналів).

Віртуальні мережі передачі даних. Ідеальним варіантом для приватної мережі було б створення каналів зв'язку тільки на тих ділянках, де це необхідно, і передача по них будь-яких мережевих протоколів, яких вимагають працюючі додатки. існують технології побудови мереж передачі даних, що дозволяють організувати всередині них канали, що виникають тільки в потрібний час і в потрібному місці. Такі канали називаються віртуальними. Систему, що об'єднує віддалені ресурси за допомогою віртуальних каналів, природно назвати віртуальної мережею. На сьогодні існують дві основних технології віртуальних мереж - мережі з комутацією каналів і мережі з комутацією пакетів. До перших відносяться звичайна телефонна мережа, ISDN і ряд інших, більш екзотичних технологій. Мережі з комутацією пакетів представлені технологіями X.25, Frame Relay і останнім часом - ATM.

## 2.2 Топології корпоративних мереж

Будь-яка мережа складається із сукупності кабелів, мережного встаткування, файлових серверів, робітників станцій і програмного забезпечення. Комбінуючи ці елементи, можна створити мережу, відповідним завданням і можливостям конкретної організації. Первісна установка деяких типів мереж не вимагає більших витрат, однак витрати з'являються при експлуатації або модернізації. Інші мережі, навпаки, вимагають значних капіталовкладень на етапі розгортання, але вони прості в обслуговуванні їх легко розширювати. Одним з найважливіших розходжень між різними типами мереж є їхня топологія.

***Топологія*** – це фізична конфігурація мережі в сукупності з її логічними характеристиками. Фізична конфігурація подібна до плану розведення кабелів в офісі, будинку. Іноді її називають *кабельною ділянкою* (cable plant). Логічні характеристики мережі описують спосіб передачі сигналу по кабелю від однієї точки до іншої.

***Шинна топологія*** (bus topology) являє собою кабель, послідовно з'єднуючи комп'ютери й сервери у вигляді ланцюжка. Як і звичайна мережа із шинною топологією має початкову й кінцеву точки, і до кожного кінця сегмента шинного кабелю підключається *термінатор* (terminator). Переданий пакет приймається всіма вузлами сегмента й на проходження всього сегмента потрібно деяка кількість часу, названа затримкою. Для того щоб пакети доходили протягом очікуваного часу, довжина сегмента мережі із шинної топологією повинна відповідати специфікаціям інституту інженерів по електротехніці й електроніці (Institute of Electrical and Electronics Engineers, IEEE). На рис. 2.1 зображена найпростіша мережа із шинною топологією.


Рисунок 2.1. Шинна топологія

Наявність термінатора обов'язково для шинної топології, оскільки термінатор вказує на фізичне закінчення сегмента. На практиці термінатор являє собою електричний опір, що гасить сигнал коли той досягає кінця мережі. Без термінатора сегмент не відповідав би специфікаціям IEEE і сигнали могли б відбиватися назад і повертатись в кабель, по якому вони були передані. Відбитий сигнал збиває синхронізацію мережі й може зіштовхнутися з новими сигналами переданими по мережі. Традиційна шинна топологія, показана на рис. 1.6, добре працює невеликих мережах, і вартість її реалізації відносно невелика. При розгортанні мережі витрати мінімальні, оскільки кабелю потрібно менше, ніж для інших топологій. Також легко можна додати нові робочі станції й небагато подовжити шину в межах кімнати або офісу. Недоліком цієї топології є висока вартість її експлуатації. Наприклад, важко виявити окремий несправний вузол або сегмент кабелю й пов'язані з ним рознімання, а один вузол, що відмовив, або сегмент із розємами може вивести з ладу всю мережу (хоча сучасне мережне встаткування зменшує ймовірність такої ситуації).

***Кільцева топологія*** (ring topology) являє собою безперервну магістраль для передачі даних, не маючу логічної початкової або кінцевої точки, отже, термінаторів. Робочі станціїі сервери підключаються до кабелю в точках, розташованих по кільцю (рис 2.2). Коли дані надходять у кільце, вони

передаються по ньому від вузла до вузла, поки не досягнуть точки призначення, після чого пересуватися далі до вузла відправника. Спочатку кільцева топологія дозволяла даним пересуватися тільки в одному напрямку, при цьому дані оббігали кільце й передача закінчувалася в передавальному (вихідному) вузлі. У нових високошвидкісних технологіях кільцевих мереж використовуються два кільця для додаткової передачі даних у зворотному напрямку. У результаті цього, якщо розривається кільце передачі в одному напрямку, дані все-таки можуть досягти пункту призначення, пересуваючись у зворотному напрямку по іншому кільцю.

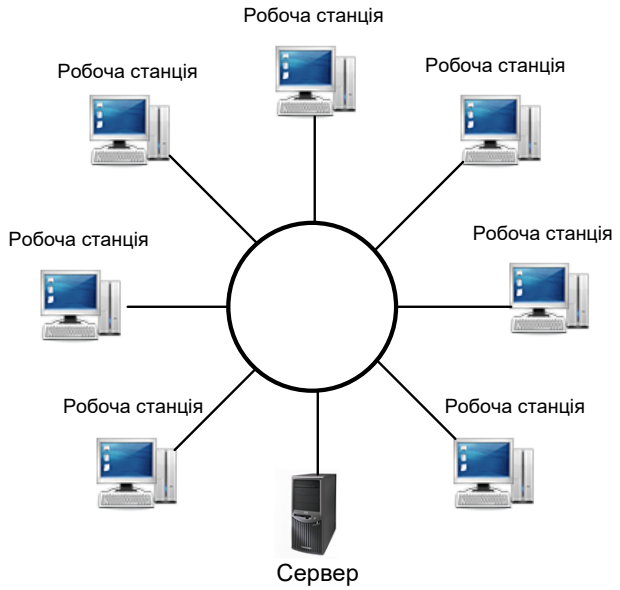


Рисунок 2.2. Кільцева топологія

У цілому можна сказати, що в порівнянні із шинною топологією, кільцева забезпечує більш надійну передачу даних.

***Зіркоподібна топологія*** (star topology), або просто "зірка", є найстаршим способом передачі сигналів, що мають свій початок у комутаційних телефонних станціях. Незважаючи на вік, переваги при використанні в мережах роблять зіркоподібну топологію вдалим вибором для сучасних мереж. Фізично зіркоподібна топологія складається з безлічі вузлів, підключених до центрального концентратора. Яким чином робочі станції й сервер підключені до концентратора, показано на рис. 2.3.

*Концентратор* (hub) – це центральний пристрій, об'єднуючи в мережу окремі кабельні сегменти або окремі локальні мережі. Деякі концентратори також називаються елементами доступу (access unit) Окремі сегменти передавального кабелю розходяться від концентратора як зірка.


Рисунок 2.3. Зіркоподібна топологія

У цей час початкові витрати на реалізацію зіркоподібної топології нижче, ніж для традиційної шинної топології й порівнянні з витратами на створення кільця. Це пояснюється зниженням цін на мережне встаткування й кабель, викликаним широким поширенням цієї архітектури. Як і кільце, зіркоподібна топологія простіше в керуванні, чим традиційна шинна мережа (відмовивші вузли виявляються дуже швидко). Якщо вузол або кабель несправні, мережне встаткування легко може ізолювати їх від мережі й працездатність інших вузлів не порушиться. Зірку легше розширити, підключивши додаткові вузли або мережі. Також вона щонайкраще може бути модернизована для роботи на більших швидкостях. Зірка – це найпоширеніша топологія й тому для неї існує широкий вибір устаткування.

Недоліком зірки є те, що концентратор є єдиною крапкою відмови: при виході його з ладу всі підключені вузли втрачають можливість

передачі даних (якщо відсутні додаткові заходи забезпечення). Іншим недоліком є те, що для зірки потрібно більше кабелю, чим для шини; однак кабелі й рознімання для зіркоподібної топології в теперішній час дешевше, ніж для шинної.

***Реалізація шинної топології у вигляді фізичної зірки.*** У сучасних мережах логічна організація мережі із застосуванням шинної топології сполучається з фізичною реалізацією у вигляді зірки. При такій архітектурі кожний промінь зірки функціонує як окремий сегмент логічної шини, що має тільки один або два підключених комп'ютери. Такий сегмент шини як і раніше має два кінці, однак перевагою є відсутність термінаторів. У цьому випадку один кінець сегмента закінчується на концентраторі, а іншої – на мережному пристрої. Іншим достоїнством комбінованої архітектури є те, що для розширення мережі в різних напрямках можна з'єднати кілька концентраторів за умови виконання специфікацій IEEE на довжину кабелів, кількість концентраторів і підключених пристроїв. З'єднання між концентраторами являє собою магістраль, що найчастіше забезпечує високошвидкісну передачу даних між ними.

*Магістраль* (backbone) – це швидкодіюче середовище передачі інформації, що з'єднує мережі й центральні мережні пристрої в масштабах поверху, усього будинку або декількох вилучених площадок.

## 2.3 Етапи розробки корпоративних мереж

Першими кроками проектування мережі мають бути мета й завдання, які залежно від конкретної організації або ситуації, що склалася, передбачено покласти на інформаційну мережу.

Основні вимоги для більшості мережних проектів:

– ***Функціональність*** – мережа має задовольняти робочі вимоги користувачів і забезпечувати зв’язок користувач – користувач і користувач – прикладна програма з необхідною швидкістю і надійністю.

– ***Масштабованість*** – мережа має бути здатною до зростання. Початковий проект має розширюватися без будь-яких серйозних змін загального проекту.

– ***Адаптованість*** – мережа має розроблятися з урахуванням упровадження перспективних технологій. Мережа не повинна містити елементів, які можуть обмежувати реалізацію нових технологій.

– ***Керованість*** – проектована мережа не повинна ускладнювати розв'язання питань мережного моніторингу та управління.

При проектуванні високотехнологічних інформаційно-комунікацій-них мереж доводиться розв'язувати такі базові питання:

– формування та розподіл інформаційних ресурсів мережі;

– топологія мережі;

– комунікаційне устаткування:

– функції та розміщення серверів;

– домени колізій;

– сегментація мережі;

– широкомовні домени тощо.

Сервери дозволяють мережним користувачам взаємодіяти і спільно використовувати файли, принтери та сервіси прикладних програм. Сервери зазвичай не використовують як робочі станції. На них запущено спеціалізовані операційні системи, наприклад NetWare, Windows NT, UNIX і Linux. Кожний сервер, як правило, реалізує одну функцію, наприклад електрону пошту або доступ до файлів.

***Файл-сервер інформаційно-комунікаційної мережі*** *– вузол мережі, що обслуговує та надає сервіс іншим вузлам* (*користувачам*) *за допомогою програмного забезпечення та комунікаційного устаткування на фоні розподілу спільно використовуваного інформаційного ресурсу.*

Програмне забезпечення, яке дає змогу серверу надавати послуги іншим комп'ютерам, часто також називають сервером, з яким контактують програми-клієнти, установлені на цих комп'ютерах.

Програмне забезпечення, орієнтоване на роботу в мережі, перебуваючи на мережному файл-сервері, водночас доступне групі користувачів.

***Клієнт-серверною інформаційною мережею*** *називається мережа, що використовує один чи кілька центральних виділених серверів.*

Серверне устаткування може виконувати свої функції в інтересах всієї інформаційно-комунікаційної мережі або окремих її сегментів чи робочих груп.

Сервер інформаційно-комунікаційної мережі підтримує всіх користувачів у межах цієї мережі, пропонуючи загальні сервіси, наприклад електрону пошту або розподіл адресації та контроль трафіку. Сервер робочої групи підтримує специфічний склад користувачів і реалізує, наприклад, текстову обробку та файлове розділення.

Сервери доцільно встановлювати в центральній серверній зоні (main distribution facility – MDF) – рис. 2.4.

По змозі, трафік до серверів інформаційно-комунікаційної мережі має передаватися безпосередньо в MDF і не зачіпати інших мереж. Проте деякі мережі використовують маршрутизовану базову магістраль для серверів. У цих випадках руху трафіку через інші мережі зазвичай не можна запобігти.

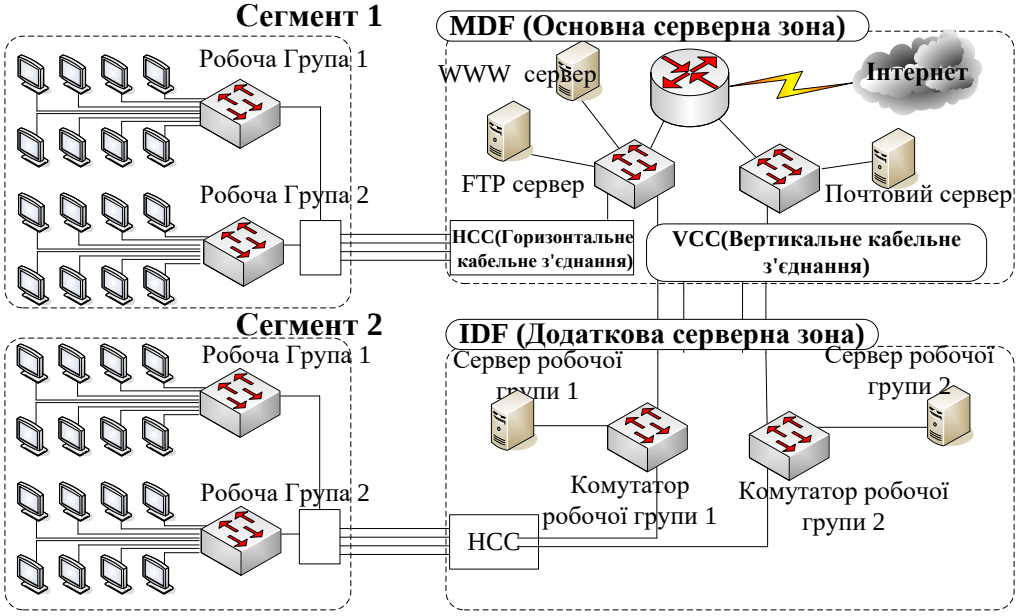


Рисунок 2.4. Розміщення серверів і робочих груп інформаційно-комунікаційної мережі

В ідеалі сервери робочих груп мають установлюватися в додаткових серверних зонах (intermediate distribution facilities – IDF) ближче до користувачів, що мають доступ до прикладних програм на цих серверах. Таке розміщення дає змогу трафіку рухатися тільки через мереж-ну інфраструктуру додаткових серверних зон і не впливати на інших користувачів у цьому мережному сегменті. Мережні комутатори *рівня 2* моделі OSI інформаційно-комунікаційної мережі розміщено в центральній серверній зоні, при цьому сервери додаткових серверних зон мають працювати зі швидкостями 100 Мбіт/с або вищими.

Оскільки вузли Ethernet використовують протокол CSMA / CD, то кожний вузол мережі має «змагатися» з усіма іншими вузлами щодо отримання доступу до середовища передачі (домену колізій). Якщо два вузли мережі починають одночасну передачу – відбувається колізія. При зіткненні кадрів переданий фрейм знищується, а в усі вузли сегмента посилається відповідний сигнал. Вузли чекають довільний період часу, потім передають дані повторно.

Надмірна кількість зіткнень може знизити доступну ширину смуги частот мережного сегмента і відповідно зменшити продуктивність мережі до 35 або 40 %. Розв’язання цієї проблеми – *сегментація*.

***Сегментація*** *– поділ єдиного домену колізій на кілька дрібніших областей.* У доменах меншого розміру кількість колізій менша, що дає змогу ефективніше використовувати ширину смуги частот.

Для сегментації домену колізій на *рівні 2* моделі OSI можуть використовуватися мости та комутатори. Сегментація на *рівні 3* досягається застосуванням маршрутизаторів.

Важливим при проектуванні є оцінювання доступності мережі. Через доступність оцінюється корисність мережі. На доступність впливають продуктивність, час відгуку та доступ до ресурсів.

Фізична топологія мережі визначає, в який спосіб пов’язані між собою різні компоненти інформаційної мережі (рис. 2.5). Логічне проектування мережі

стосується інформаційних потоків даних, а також імен і схем адресації, використаних у реалізації проектного рішення зазначеної мережі.

***Топологія мережі згідно з рівнями моделі OSI. Топологія мережі рівня 1.*** Одним із найважливіших компонентів мережі є кабельне устат-кування. Сьогодні з'єднання інформаційно-комунікаційної мережі най-частіше базується на технології *Fast Ethernet*. Fast Ethernet – це 10 Мбіт/с Ethernet, модернізований для швидкості 100 Мбіт/с і такий, що характеризується повнодуплексною функціональністю.

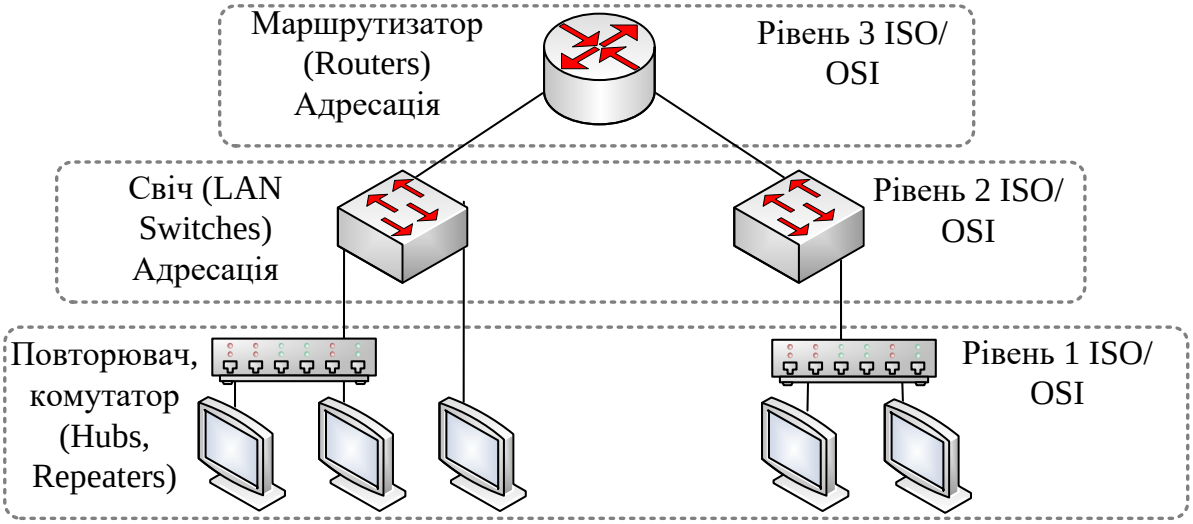


Рисунок 2.5. Проектування топології мережі по рівнях моделі OSI

Він використовує стандартну Ethernet-орієнтовану логічну топологію шини для адреси канального рівня (MAC-адреса) (рис. 2.6).

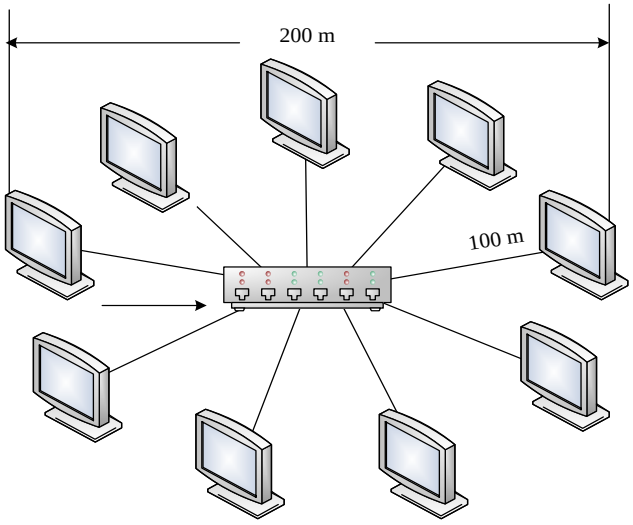


Рисунок 2.6. З'єднання мережі за технологією Fast Ethernet

Проектні питання для топології *рівня 1* містять тип використаного для прокладання кабелю (зазвичай мідь або волоконно-оптичний) і загальну структуру кабельного устаткування.

Сильні і слабкі сторони топології мають бути ретельно проаналізовані, оскільки ефективність мережі повністю залежить від використовуваних кабелів.

Для магістральних ліній (вертикального з'єднання) необхідно використовувати волоконно-оптичний кабель (рис. 2.7).

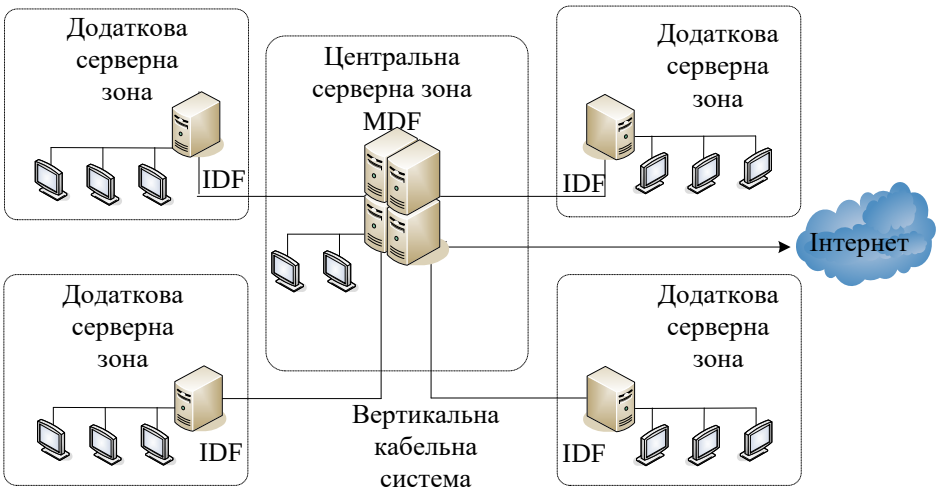


Рисунок 2.7. Вертикальне з'єднання мережі

У великих мережах, де неможливо виконати обмеження на 100-метрову довжину кабелю для окремого сегмента (особливо для кількох додаткових серверних зон), може використовуватися кілька комутаційних панелей. Схему з'єднання для такої топології наведено на рис. 2.8.

Сполучні кабелі (патч-кабелі) слугують для підімкнення горизонтальних мережних кабелів *рівня 1* до портів мережного комутатора *рівня 2*. Вихідний порт комутатора *рівня 2* з'єднується патч-кабелем з Ethernet-портом маршрутизатора *рівня 3*, чим забезпечується фізичне з'єднання окремої кінцевої хост-машини з маршрутизатором.

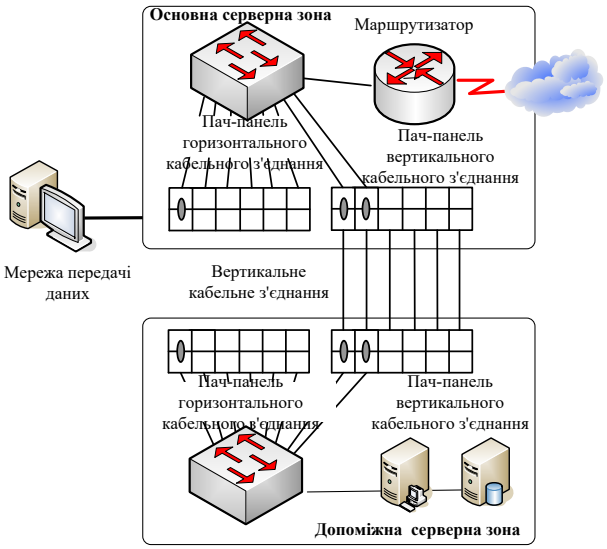


Рисунок 2.8. Комутування основної та додаткової серверної зони на базі вертикальної та горизонтальної крос-панелі

Для зв’язку різних додаткових серверних зон із центральним MDF використовуються крос-панелі для вертикальних кабелів (VCC). Тут необхідне застосування волоконно-оптичного кабелю, оскільки вертикальні кабельні довжини перевищують стандартну 100-метрову межу.

***Топологія мережі рівня 2***. Призначення пристроїв *рівня 2* моделі OSI в мережі – переспрямування фреймів на основі інформації з MAC-адреси вузла-одержувача, виявлення помилок і зниження перевантажень у мережі. Найбільш поширені мережні пристрої *рівня 2* – це мости (bridges) і мережні комутатори (switches). Пристрої *рівня 2* обмежують розмір домену колізій.

Колізії та розмір домену колізій – два показники, які негативно впливають на продуктивність мережі. Розміри домену колізій і, відповідно, кількість колізій зменшуються шляхом мікросегментації мережі. Принцип мікросегментації ілюструє рис. 2.9.

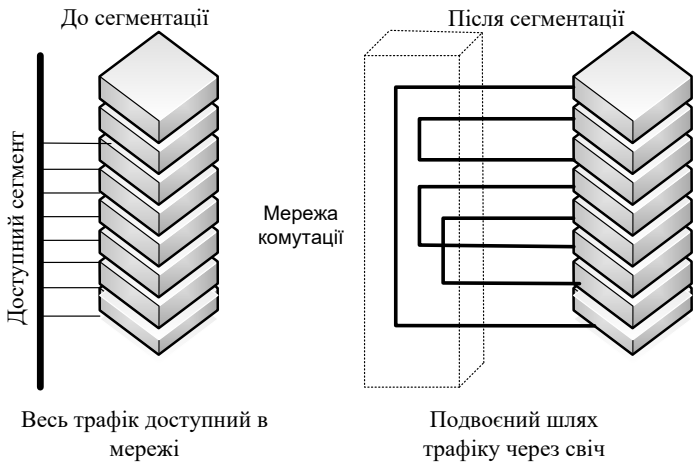


Рисунок 2.9. Мікросегментація

Крім мікросегментації мережний комутатор підтримує так звану асиметричну комутацію, іншими словами, пересилання фреймів між каналами з різними швидкостями передачі. Ця характеристика мережного комутатора важлива для узгодження трафіку між спільною для всієї компанії частиною мережі та елементами мережі в підрозділах компанії (рис. 2.10).

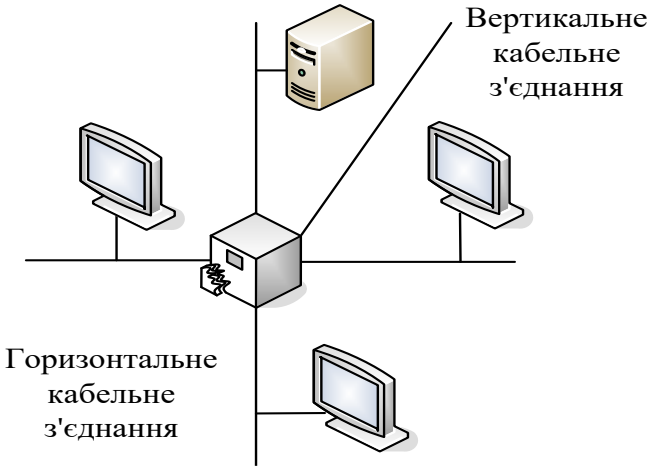


Рис. 1.10. Асиметрична комутація

Одне із завдань проектування мережі – визначення кількості 10- і 100-мегабітних портів для центральної та додаткової серверної зон. Це завдання виконується шляхом аналізу вимог користувачів щодо кількості горизонтальних кабельних з’єднань для кожної кімнати та сумар-ної кількості портів на всі кімнати компанії. Крім того, підраховується кількість вертикальних кабельних прогонів.

Розмір домену колізій визначається кількістю хостів, які фізично підмикаються до окремого порту мережного комутатора. Цей розмір фактично визначає доступну для окремого користувача частину смуги пропускання кабелю.

В ідеальному випадку до окремого порту мережного комутатора має підмикатися один користувач. Проте насправді до окремого порту комутатора через багатопортові повторювачі (Hubs) підімкнено кілька користувачів, що збільшує розміри домену колізій та кількість колізій, а отже, знижує ефективну продуктивність відповідного сегмента мережі та мережну продуктивність окремої хост-маши-ни (рис. 2.11).

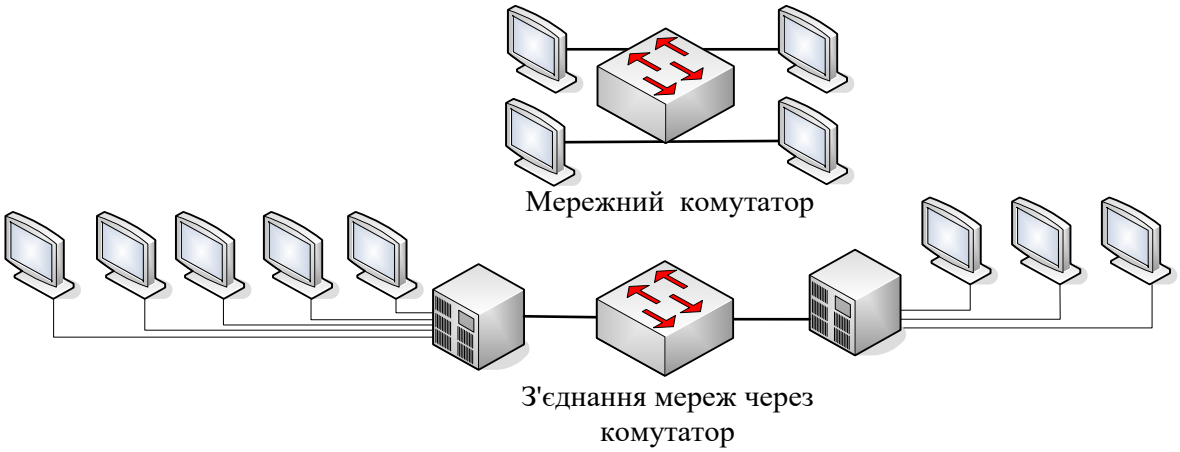


Рисунок 2.11. Способи підключення до мережних комутаторів

У результаті проектування топології мережі *рівня 2* визначають необхідну кількість мережних комутаторів, їхній тип, кількість портів з урахуванням резерву й можливого зростання мережі, а також типи й необхідну кількість багатопортових повторювачів (Hubs).

***Топології мережі рівня 3***. Пристрої *рівня 3* використовуються для створення унікальних сегментів. До таких пристроїв насамперед належить маршрутизатор. Пристрої забезпечують взаємодію між сегментами на основі адрес *рівня 3* моделі OSI, таких як IP-адреси. Використання пристроїв *рівня 3* реалізує поділ мереж на унікальні фізичні і логічні мережі. Маршрутизатори обслуговують вихід у глобальні мережі, наприклад Інтернет.

Маршрутизація *рівня 3* визначає рух трафіку між унікальними фізичними мережними сегментами на основі спеціальної системи адресації. При цьому пересилаються пакети даних на основі адреси одержувача і не пересилається службова інформація мережі, наприклад запити ARP. Отже, інтерфейс маршрутизатора вважається входом і вихідною точкою домену широкомовлення, що зупиняє широкомовлення в інші сегменти інформаційно-комунікаційної мережі.

Маршрутизатори забезпечують масштабованість мережі, оскільки вони є завадою широкомовленню і поділяють мережі на підмережі на основі адреси *рівня 3* (рис. 2.12).

Для ухвалення рішення про використання маршрутизаторів або комутаторів важливо докладно розглянути цю проблему. Якщо проблема зумовлюється протоколом, а не питаннями конкуренції, то переважають маршрутизатори. Маршрутизатори розв’язують проблеми, що стосуються широкомовлення, протоколів, які погано масштабуються, аспектів безпеки та адресації мережного рівня. Проте вони більше кош-тують і складніше конфігуруються.

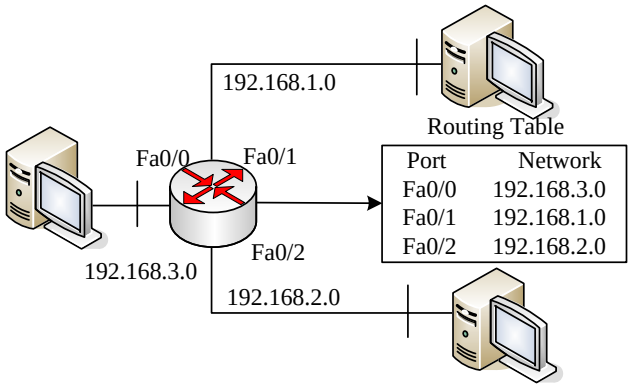


Рисунок 2.12. Метод розподілу інформаційної мережі
на підмережі на базі маршрутизаторів

Приклад проекту, що містить кілька мереж, наведено на рис. 2.13. Увесь трафік із мережі 1 у мережу 2 має пройти через маршрутизатор. У цій реалізації є два широкомовні домени. Обидві мережі мають унікальну схему мережної адресації. За такою технологією може створюватися безліч фізичних мереж,

якщо горизонтальні і вертикальні кабелі підімкнути до порту відповідного комутатора *рівня 2*. Підімкнення можна виконати патч-кабелями. Зазначена реалізація забезпечує належ-ний рівень безпеки, оскільки інформаційний потік, що входить і виходить з локальної мережі, має пройти через маршрутизатор.

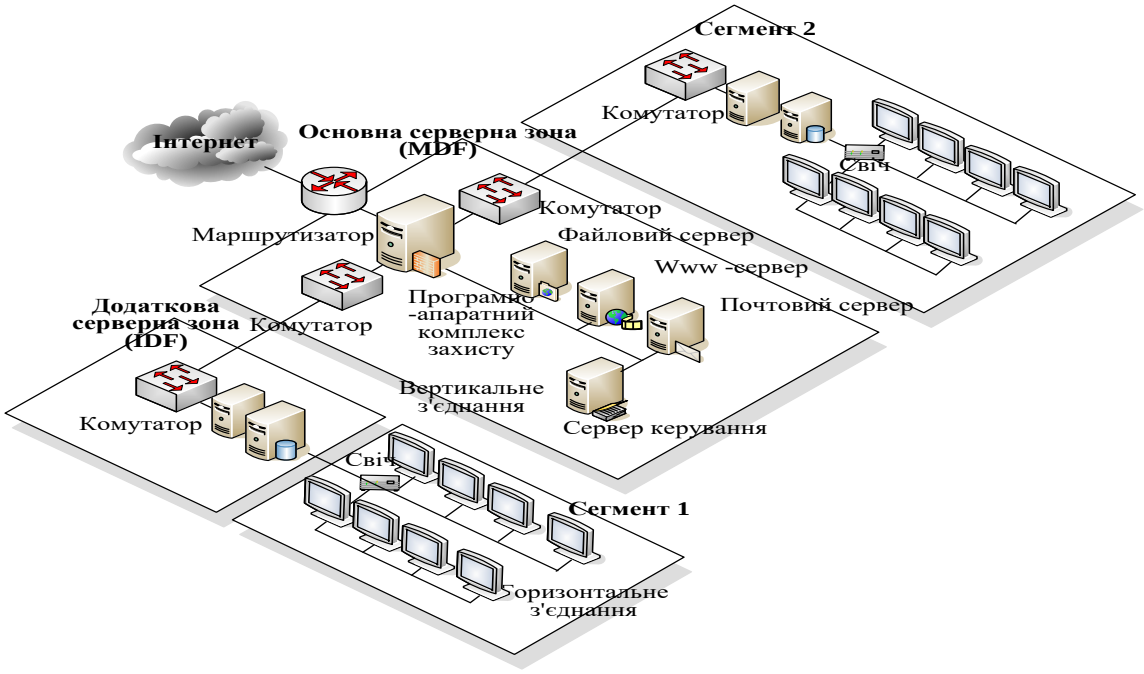


Рисунок 2.13. Топологія розгалуженої інформаційної мережі з застосуванням сегментації, основних та додаткових серверних зон та базового комунікаційного устаткування

***Концепція віртуальних інформаційно-комунікаційних мереж.*** Концептція віртуальних мереж (VLAN) припускає майже повну незалежність фізичної і логічної топологій. Адміністратори можуть використовувати засоби віртуальних мереж для групування робочих станцій навіть тоді, коли вони відокремлюються комутаторами і розміщені в інших сегментах інформаційно-комунікаційної мережі. Окрема віртуаль-на мережа припускає один домен колізій і один широкомовний домен.

***Особливості та переваги використання віртуальних інформацій-но-комунікаційних мереж.***

Віртуальна мережа полегшує адміністрування логічних груп стан-цій і серверів, які можуть взаємодіяти так, ніби вони перебувають у тому самому фізичному сегменті інформаційно-комунікаційної мережі.

– Віртуальні мережі логічно сегментують комутовані мережі, спираючись на робочі функції, належність користувача до конкретного відділу або сегмента незалежно від фізичного розміщення корис-тувачів або фізичного підімкнення до мережі.

– Усі робочі станції та сервери, використовувані конкретною робочою групою, належать одній віртуальній мережі незалежно від їх фізичного розміщення.

– Логічна група мережних станцій, сервісів і пристроїв не обмежена фізичним сегментом інформаційно-комунікаційної мережі (рис. 2.13).

– Конфігурація або деконфігурація віртуальних мереж реалізується через програмне забезпечення. Отже, конфігурація віртуальної мережі не потребує фізичного переміщення або перемикання мережного устаткування. Функціонування робочих станцій обмежується взаємодією з файловими серверами в тій самій віртуальній мережі.

Віртуальні мережі спрощують адміністрування змін структури цих груп.

VLAN логічно сегментують мережу в різні широкомовні домени в такий спосіб, що пакети комутуються тільки між портами, призначеними тій самій віртуальній мережі.

Віртуальні мережі створюються для підтримки сервісів сегментації, що традиційно реалізовуються маршрутизаторами. Маршрутизатори в топологіях віртуальних мереж реалізують широкомовну фільтрацію, безпеку та управління трафіком.

Комутатори не забезпечують трафіку між різними віртуальними мережами, оскільки це порушує цілісність широкомовного домену VLAN. Трафік між віртуальними мережами реалізує маршрутизатор.

Для визначення віртуальних мереж використовується фізичне призначення портів мережного комутатора. Зв’язок між двома чи більше

віртуальними мережами (VLAN1 і VLAN2, рис. 2.14) може існувати тільки через маршрутизатор.

Концепція віртуальних інформаційно-комунікаційних мереж об'єднує технології комутації *рівня 2* і маршрутизації *рівня 3* моделі OSI на тлі обмеження розмірів доменів колізій і широкомовних доменів.

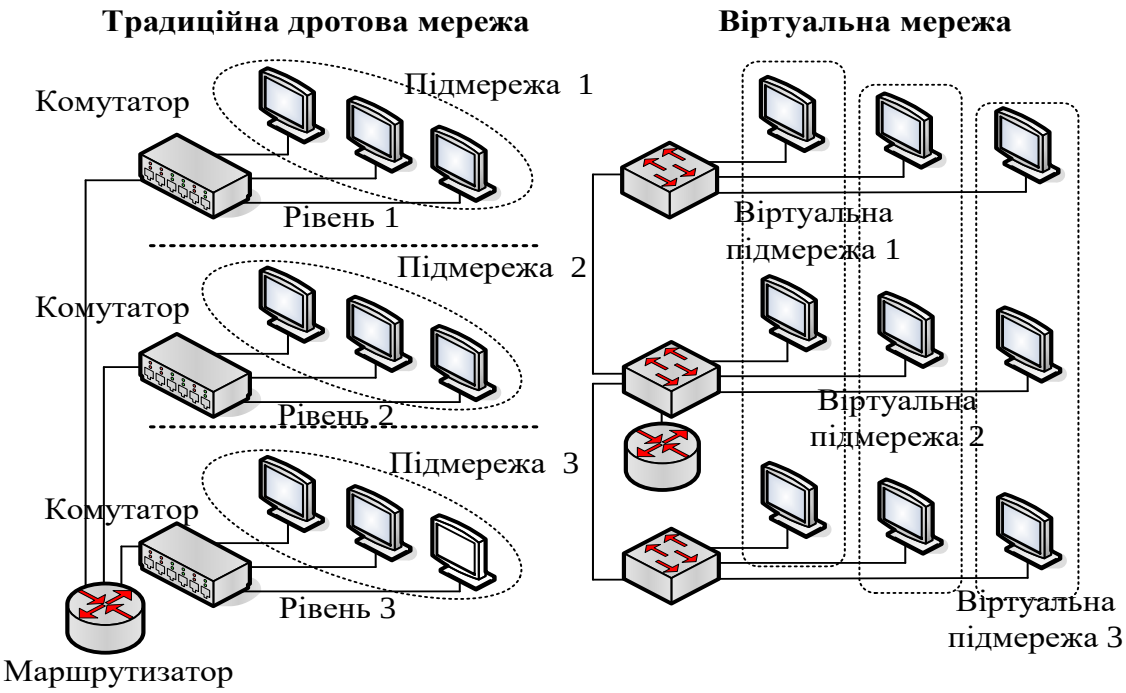


Рисунок 2.14. Концепція побудови віртуальних мереж

# 3 АНАЛІЗ СИСТЕМ ЗАХИЩЕНОСТІ МУЛЬТИМЕДІЙНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

## 3.1. Системи пошуку вразливостей

Системи пошуку вразливостей проектування не отримали широкого поширення в російських та українських компаніях. Пов'язано це, на мій погляд, з високою вартістю таких рішень і недостатнім розумінням їх значимості. Єдиний клас організацій, де ці системи знайшли своє застосування, - це лабораторії, що здійснюють сертифікацію програмно-апаратного забезпечення та атестацію інформаційних систем за вимогами безпеки.

Системи аналізу захищеності другого і третього класів одержали найбільше поширення серед кінцевих користувачів. Існує кілька додаткових класифікацій цих систем. Наприклад, системи аналізу вихідного тексту і виконуваного коду тестованого програмно-апаратного забезпечення і т.д. Перші також застосовуються звичайно при сертифікації програмного забезпечення за вимогами безпеки. Такі систему існують у зарубіжних (наприклад, SLINT) і російських (наприклад, AICT, ACTMA і COTMA) виробників.

У більшості випадків програмне забезпечення поставляється в організації без вихідних текстів. Крім того, аналіз вихідних текстів вимагає високої кваліфікації від обслуговуючого їх персоналу. Та і відсутність ефективних систем аналізу вихідних текстів не дозволяє проводити такий аналіз на якісному рівні. За словами співробітника однієї з вітчизняних сертифікаційних лабораторій, "виконання вказаних робіт проводиться шляхом ручного аналізу вихідних текстів програм". Саме тому великий інтерес викликають системи пошуку вразливостей в виконуваному коді, найпоширенішим підкласом яких є системи імітації атак, які моделюють різних несанкціонованих впливів на компоненти інформаційної системи. Саме ці системи здобули широку популярність у всьому світі через свою відносну простоту і дешевизну. За допомогою таких імітаторів виявляються уразливості ще до того, як вони

будуть використані порушниками для реалізації атак. До числа систем даного класу можна віднести SATAN, Internet Scanner, Cisco Secure Scanner і т.д.

Системи імітації атак з однаковим успіхом виявляють не тільки уразливості реалізації, а й уразливості експлуатації. Саме ці системи, разом з системами пошуку вразливостей експлуатації, набули найбільшого поширення серед користувачів.

Як показано на рис. 3.1 функціонувати системи аналізу захищеності, зокрема системи пошуку вразливостей реалізації та експлуатації, можуть на всіх рівнях інформаційної інфраструктури будь-якої компанії, тобто на рівні мережі, операційної системи, СУБД і прикладного програмного забезпечення.Найбільшого поширення набули засоби аналізу захищеності мережевих сервісів і протоколів. Пов'язано це, в першу чергу, з універсальністю використовуваних протоколів. Вивченість і повсюдне використання таких стеків протоколів, як TCP / IP, SMB / NetBIOS і т.п. дозволяють з високим ступенем ефективності перевіряти захищеність корпоративної мережі, що працює в даному мережевому оточенні, незалежно від того, яке програмне забезпечення функціонує на більш високих рівнях. Прикладом такої системи є Internet Scanner компанії ISS. Другими за поширеністю є засоби аналізу захищеності операційних систем. Пов'язано це також з універсальністю і поширеністю деяких операційних систем (наприклад, UNIX та Windows NT). Однак, через те, що кожен виробник вносить в операційну систему свої зміни (яскравим прикладом є безліч різновидів ОС UNIX), засоби аналізу захищеності ОС аналізують в першу чергу параметри, характерні для всього сімейства однієї ОС. І лише для деяких систем аналізуються специфічні для неї параметри. Прикладом такої системи є System Scanner компанії ISS. Коштів аналізу захищеності СУБД і додатків на сьогоднішній день не так багато, як цього хотілося б. Такі кошти поки існують тільки для широко поширених прикладних систем, типу Web-броузери (Netscape Communicator, MS Internet Explorer), СУБД (MS SQL Server, Oracle) і т.п.Прикладом такої системи є Online Scanner і Database Scanner також компанії ISS.

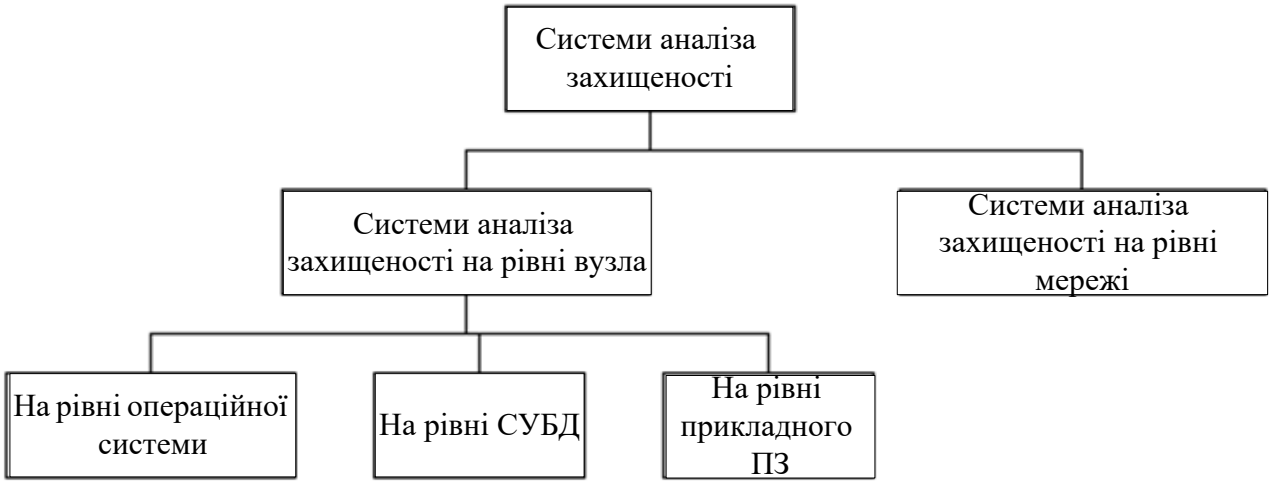


Рисунок 3.1. Системи аналізу захищеності

При проведенні аналізу захищеності ці системи реалізують дві стратегії. Перша - пасивна, - реалізована на рівні операційної системи, СУБД і додатків, при якій здійснюється аналіз конфігураційних файлів та системного реєстру на наявність неправильних параметрів; файлів паролів на наявність легко вгадувані паролів, а також інших системних об'єктів на порушення політики безпеки. Друга стратегія, - активна, - здійснювана в більшості випадків на мережевому рівні, що дозволяє відтворювати найбільш поширені сценарії атак, і аналізувати реакції системи на ці сценарії.

Однак не варто думати, що за допомогою засобів аналізу захищеності можна тестувати тільки можливість несанкціонованого доступу в корпоративну мережу з мереж відкритого доступу (наприклад, Internet). Ці кошти з не меншим успіхом можуть бути використані для аналізу деяких сегментів або вузлів внутрішньої мережі організації. Системи аналізу захищеності можуть бути використані як відділами захисту інформації (для оцінки рівня безпеки організації), так і управліннями інформатизації (для контролю ефективності встановлення мережевої, системного та прикладного програмно-апаратного забезпечення).Ця два найбільш поширених варіанту застосування систем аналізу захищеності.Однак є й інші варіанти. Наприклад, зовнішніми аудиторськими та консалтинговими компаніями, які здійснюють інформаційні обстеження мереж своїх замовників. Є й більш цікаві варіанти - наприклад, для

тестування і сертифікації того або іншого програмно-апаратного забезпечення. Цей варіант дуже популярний на Заході при оцінці мережевого устаткування, міжмережевих екранів і т.п. різними тестовими лабораторіями.

На даний момент існує більше сотні різних засобів, що автоматизують пошук вразливостей на рівні мережі, ОС, СУБД і прикладного ПЗ. Одні кошти орієнтовані на виявлення цілого спектру різних вразливостей, інші - тільки на певну їх категорію. Наприклад, система Internet Scanner є одним з найбільш відомих засобів пошуку "дірок" і виявляє більше 900 різних вразливостей, які належать різним категоріям: Denial of Service, Brute Force, FTP, LDAP, SNMP, RPC, NIS, NFS, DNS і т.д . А система Whisker була створена спеціально для сканування Web-серверів і дозволяє виявляти вразливі CGI-скрипти.

### 3.2 Побудова захищених систем в Україні

Я не ставив перед собою мети порівнювати пропоновані в Україні рішення. Оскільки порівнювати різні кошти - завдання невдячне; особливо в Україні. Адже між кінцевим користувачем і виробником завжди встає третя ланка (або декілька) - постачальник, який може звести "нанівець" всі переваги пропонованого рішення за рахунок низької якості післяпродажній і обов'язком. Друга причина відмови від порівняння в тому, що дані рішення - це далеко не все, що має порівнюватися. Для кожного продукту повинна існувати своя інфраструктура (яка також має братися до уваги при виборі), що включає в себе якість документації (у тому числі і російською мовою) та технічної підтримки, наявність авторизованого навчання і кваліфікованих консультацій, виїзди фахівців організації до замовника і т . д. Ну і нарешті, порівняти і вибрати продукти може тільки кінцевий користувач і тільки у своїй власній мережі, щоб перевірити поведінку і зручність використання того чи іншого рішення саме в тій технології обробки інформації, яка прийнята в організації.

У табл. 3.1 наведено список засобів аналізу захищеності, найбільш часто використовуваних в Україні.

Таблиця 3.1

Засоби аналізу захищеності, використовувані в Україні

| Назва | Виробник | Категорія | Опис |
|---|---|---|---|
| Internet Scanner | Internet Security Systems | На рівні мережі | Перша система, що отримала сертифікат ГТК. |
| System Scanner | Internet Security Systems | На рівні ОС | За системою існує авторизоване вивчення в Україні |
| Database Scanner | Internet Security Systems | На рівні СУБД | За системою існує авторизоване вивчення в Україні |
| Cisco Secure Scanner | Cisco Systems | На рівні мережі | |
| CyberCop Scanner | Network Associates | На рівні мережі | |
| WebTrends Security Analyzer | WebTrends Corporation | На рівні мережі | |
| NetRecon | Symantec | На рівні мережі | Доля продукту поки що не відома |
| Enterprise | Security Manager | Symantec | На рівні ОС |
| SFProtect | Hewlett Packard | На рівні мережі, ОС, СУБД | |
| Nessus | Вільно розповсюджується | На рівні мережі | Система имає сертифікат ГТК. |

В Україні вартість є, мабуть, одним з основних критеріїв вибору системи виявлення атак. Часто такий вибір робиться не на користь більш ефективного, ана користь більш дешевого рішення. Можна сперечатися, що така практика порочна, але вона існує і з нею треба рахуватися. Розуміючи це, багато виробників крім ціни, зазначеної у прайс-листі, пропонують спеціальні програми утримання потенційного покупця. Саме тому у вищенаведеній

таблиці немаєколонки "Ціна". Можна навести деякі приклади без зазначення назв фірм, які використовують такі методи:

- пропозиція для України цін нижче європейських та американських;
- оплата обраній системи в розстрочку;
- знижки при придбанні декількох засобів одного виробника;
- знижки для освітніх установ;
- знижки при переході з продукту-конкурента.

У середньому вартість аналізу одного вузла може змінюватися в діапазоні від 100 до 3 тис. доларів США, в залежності від кількості сканованих пристроїв.

### 3.3 Виявлення атак в корпоративній мережі і методи боротьби

У цій роботі розглядаються проблеми, які виникають в системах управління політикою безпеки корпоративних мереж у разі раптового несанкціонованого доступу. Ця тема набуває все більшої актуальності у зв'язку з розширенням практики формування внутрікорпопоратівних мережевих систем та збільшенням спроб їх атакувати.

Для вирішення цих проблем необхідно проаналізувати функції системи виявлення та запобігання вторгнень в корпоративну мережу і ступінь її захищеності.

Почнемо з аналізу проблемних складових ступеня захищеності системи. Забезпечення надійного захисту корпоративної мережі - дуже складний процес, який являє собою безперервну і постійну послідовність дій щодо реалізації комплексу заходів інформаційної безпеки. З моєї точки зору, найбільш вразливою ланкою в цьому ланцюжку дій є кадрове питання. Більшість експертів з безпеки рекомендують починати формування системи безпеки з ретельного відбору (в тому числі з етичних і моральних критеріїв) співробітників, в завдання яких входитиме адміністрування корпоративної мережі. Вони отримують доступ до всіх конфіденційним матеріалів не за статусом посади, а по можливості технічного доступу до інформації. А оскільки вони, як правило, не мають пайової участі в прибутках компанії, то

представляють собою одну з найбільш серйозних потенційних загроз для безпеки компанії. Тому цілком очевидно, що люди, які претендують на цю роботу, повинні бути ретельно перевірені. Але система підбору кадрів не аналізується в даному доповіді.

Хочеться лише акцентувати увагу на посадових обов'язках таких співробітників з точки зору спеціальних знань. Слід враховувати, що фахівець з безпеки інформації відповідає за розробку, реалізацію та експлуатацію системи забезпечення інформаційної безпеки, спрямованої на підтримку цілісності, придатності та конфіденційності даних, накопичених в компанії. У його функції входить забезпечення та фізичної (технічні засоби, лінії зв'язку і віддалені комп'ютери), і логічного (самі дані, прикладні програми, операційна система) захисту інформаційних ресурсів.

Другою проблемою є архітектура системи захищеності корпоративної мережі.При її формуванні необхідно розробити концепції та політики безпеки, які будуть прийняті в компанії і які нерозривно пов'язані із загальним планом її розвитку. У першу чергу потрібно визначити список об'єктів, на які можуть бути спрямовані атаки. Природно, в даний список повинні бути включені всі критично важливі вузли корпоративної мережі. Для цього необхідно провести аудит і аналіз існуючих і можливих зовнішніх і внутрішніх загроз, визначити їх джерела і оцінити ризики. Ці відомості дозволять скласти реальне уявлення про існуючу і прогнозовану ступеня уразливості корпоративної мережі, а також про потреби в захисті інформаційних ресурсів. При цьому потрібно враховувати можливість організації атак як зовні - від зовнішніх, сторонніх осіб і організацій (наприклад, від хакерів, які намагаються проникнути в корпоративну мережу), так і зсередини з боку співробітника компанії, який вже має до мережі (ні в якому разі не можна забувати про небезпеку внутрішніх загроз).

За результатами проведеного аналізу можливих загроз визначаються методи і засоби виявлення ворожого впливу і захисту від відомих загроз, а також методи і засоби реагування при інцидентах. З урахуванням всіх обставин

приймаються рішення про розробку та реалізацію комплексних проектів на базі широкого спектру систем і рішень, поєднання яких дозволяє забезпечити ефективний захист інформаційних ресурсів корпоративної мережі.

А тепер більш детально розглянемо засоби виявлення і запобігання вторгнень, а також інструменти аналізу захищеності ресурсів корпоративної мережі від атак.

Перш за все відзначимо, що в доповіді не розглядаються методи захисту від таких зловмисних дій, як використання побічних електромагнітних випромінювань і наведень, - для протидії подібного роду порушень повинен бути реалізований комплекс організаційно-технічних заходів з фізичного контролю (розміщення, охорона і т.п .) контрольованих вузлів корпоративної мережі.

У комплекс функцій системи має входити забезпечення моніторингу, контролю і збору інформації про дії легальних користувачів корпоративної мережі і можливість швидкої блокування дій порушника - організатора атаки.

Для цього необхідно збирати та систематизувати інформацію про наступні події в корпоративній мережі:

- зміна файлової системи контрольованого вузла корпоративної мережі;
- використання зовнішніх пристроїв введення-виведення (дисководів, USB-пристроїв тощо);
- запуск і зупинка процесів на контрольованому вузлі;
- локальна або віддалена реєстрація початку сеансу роботи користувача, а також завершення роботи користувачів;
- користування принтерів і інших периферійних пристроїв;
- ведення статистики використання мережевих сервісів;
- зміна апаратної і програмної конфігурації контрольованого вузла.

При цьому система управління політикою безпеки та захисту від несанкціонованого доступу повинна мати розподілену архітектуру і включати такі компоненти, як програмні сенсори, сервер управління сенсорами і консоль адміністратора. Програмні сенсори встановлюються на контрольовані вузли

корпоративної мережі і забезпечують збір, фільтрацію і передачу параметрів зібраних подій серверу управління сенсорами. Сервер управління сенсорами здійснює збереження та аналіз інформації про події, що надходять від сенсорів системи. Консоль адміністратора служить для централізованого управління сервером управління сенсорами і сенсорами системи, відображення результатів роботи системи і формування звітів.

Така архітектура системи дозволить з великою часткою ймовірності виявити атаки і зловживання щодо вузлів корпоративної мережі компанії (як конкретного вузла, так і цілого мережевого сегмента).

Система виявлення та запобігання вторгнень на підприємстві повинна виконувати наступні завдання:

- Виявити в реальному масштабі часу мережеві атаки на мережевому рівні та рівні інформаційних вузлів (робочих станцій і серверів);
- Оперативно оповістити у разі виявлення атаки і запобігти її вплив;
- Блокувати атаку до того, як вона буде реалізована;
- Виявити уразливості, що дозволяють реалізувати атаку;
- Усунути (компенсувати) уразливості.
- Основний принцип роботи системи виявлення та блокування мережевих атак в корпоративній мережі з боку як зовнішніх, так і внутрішніх порушників грунтується на аналізі пакетів даних, що циркулюють у цій мережі, і в подальшому виявленні аномалій мережевого трафіку мережі.

Для виявлення вторгнень в систему використовується кілька методів у комплексі: метод, заснований на виявленні сигнатур відомих атак, а також метод, який базується на аналізі поведінки мережі. Перший метод забезпечує виявлення атак за допомогою спеціальних шаблонів. Як сигнатури атаки можуть виступати рядок символів, семантичне вираження на спеціальній мові, формальна математична модель та ін, причому кожна сигнатура може бути співвіднесена з відповідною атакою порушника. При отриманні вихідних даних про мережевому трафіку корпоративної мережі система проводить їх аналіз на відповідність певним шаблонам або сигнатурах атак, збереженим в постійно

оновлюється базі даних системи. У разі виявлення сигнатури у вихідних даних система фіксує факт виявлення мережевої атаки і блокує її подальші дії. Перевагою сигнатурного методу є його висока точність.

Другий метод виявлення нових типів атак в системі виявлення вторгнень заснований на аналізі поведінки корпоративної мережі та використанні інформації про штатний процесі функціонування корпоративної мережі. Принцип роботи цього методу полягає у виявленні невідповідності між поточним режимом функціонування корпоративної мережі і моделлю штатного режиму роботи, закладеної в параметрах роботи методу. Будь-яка невідповідність розглядається як інформаційна атака. У разі здійснення атаки, яка може призвести до виведення з ладу вузлів корпоративної мережі, можливі автоматичне завершення з'єднання з атакуючим вузлом, блокування облікового запису порушника (якщо він є співробітником компанії) або реконфігурація міжмережевих екранів і маршрутизаторів таким чином, щоб надалі з'єднання з атакуючим вузлом були заборонені.

Мережеві сенсори, призначені для захисту об'єктів мережевих сегментів корпоративної мережі, забезпечують перехоплення і аналіз всього мережевого трафіку, що передається в рамках того сегмента, де вони встановлені.Серверні сенсори встановлюються на сервери корпоративної мережі і забезпечують захист певних мережевих сервісів мережі. У числі таких сенсорів можуть бути серверні сенсори для поштових, файлових і Web-серверів, а також для серверів баз даних. На одному сервері корпоративної мережі може бути одночасно встановлено декілька типів сенсорів. Датчики виконують функції управління серверними і мережевими сенсорами, а також функції забезпечення передачі інформації між сенсорами і сервером управління сенсорами. Сервер управління сенсорами забезпечує централізований збір, збереження та аналіз інформації, що надходить від серверних і мережевих сенсорів, і дає можливість виявлення розподілених мережевих атак на основі аналізу отриманої інформації. Консоль адміністратора призначена для централізованого управління компонентами системи і відображення результатів роботи системи.

Повідомлення про виявлену атаці, як правило, формується відповідно до стандарту IDMEF (Intrusion Detection Message Exchange Format) і містить наступну інформацію: - дата і час виявлення атаки;

- загальний опис атаки, включаючи можливі посилання на додаткові джерела інформації про виявлену атаці;

- символьний ідентифікатор атаки за класифікатором CVE (Common Vulnerabilities Exposures, http://cve.mitre.org) або CERT (Computer Emergency Response Team, http://www. cert.org);

- рівень пріоритету виявленої атаки (низький, середній або високий);

- інформація про джерело атаки (IP-адресу, номер порту, доменне ім'я та ін);

- інформація про об'єкт атаки (IP-адресу, номер порту, доменне ім'я та ін);

- рекомендації по усуненню вразливості, в результаті якої був зафіксований факт реалізації атаки.

База даних сигнатур атак системи виявлення та запобігання вторгнень повинна регулярно оновлюватися.

Один з варіантів вирішення завдань, описаних вище, побудовано на основі ситем виявлення вторгнень ManHunt і IntruderAlert компанії Symantec, а так же мережевих сканерів безпеки NetRecon і VulnerabilityAssesment. Рішення може бути розширено системою контролю політики безпеки встановленої в організації Symantec Enterprise Security Management. Перевірка мережного трафіку здійснюється в режимі реального часу на швидкостях до 2 гігабіт на секунду.Виявляються відомі і невідомі мережеві атаки, а також атаки «відмова в обслуговуванні» і спроби скритного сканування мережі. Механізми кореляційного аналізу подій, значно підвищують оперативність виявлення атак і вторгнень. Гнучкі варіанти розгортання і відмінні можливості масштабування сприяють скороченню сукупної вартості володіння системи. Автоматичні механізми отримання та розгортання пакетів оновлень для систем безпеки. До складу рішення включені потужні та високопродуктивні засоби аналізу мережевого трафіку.

Переваги описаного варіанта - у комплексній системі захисту інформації від різного типу атак на різних рівнях корпоративної інформаційної системи.

У разі застосування всіх перерахованих вище заходів корпоративна мережа набуває певну ступінь безпеки і захищеності від атак.

Яка надійність вжитих заходів? Відповідь може дати аналіз захищеності на основі проведення регулярних, всебічних або вибіркових тестів з метою виявлення та усунення вразливостей програмно-апаратного забезпечення корпоративної мережі: мережевих сервісів, операційних систем, прикладного програмного забезпечення, систем управління базами даних, маршрутизаторів, міжмережевих екранів, а також для перевірки наявності останніх модулів оновлення і т.п. При виявленні вразливостей система надає адміністратору звіти, що містять докладний опис кожної виявленої уразливості, дані про їхнє розташування у вузлах корпоративної мережі та рекомендації щодо їх корекції або усунення. До складу системи аналізу захищеності входять сканери безпеки, призначені для проведення заданої множини перевірок відповідно до параметрів, визначених адміністратором безпеки; сервер зберігання результатів роботи системи; консоль адміністратора для централізованого управління системою. Сканер безпеки являє собою програмний засіб для віддаленої або локальної діагностики різних елементів мережі на предмет виявлення в них вразливостей, використання яких може призвести до комп'ютерних порушень. Основними користувачами таких сканерів є системні адміністратори і фахівці з безпеки. Сканери безпеки скорочують час, необхідний для пошуку вразливостей, за рахунок автоматизації операцій з оцінки захищеності систем. Принципи роботи такого сканера полягає в тому, що основний модуль програми під'єднується по мережі до віддаленого комп'ютера.У залежності від активних сервісів формуються перевірки та тести. Знайдена при скануванні кожного порту службова інформація порівнюється з таблицею правил визначення мережевих пристроїв, операційних систем і можливих вразливостей. На основі проведеного порівняння робиться висновок про наявність чи відсутність потенційної уразливості.

Система аналізу захищеності вимагає постійної уваги та контролю. Будь-яка зміна конфігурації корпоративної мережі компанії, а також мережевого програмного забезпечення має бути досліджено системою аналізу захищеності.Невідповідність в конфігурації може призвести до збільшення кількості помилкових спрацьовувань, а також до появи дірок в безпеці. Робота системи заснована на аналізі мережевого трафіку з використанням методу сигнатур, тому система аналізу захищеності вимагає постійного оновлення бази вразливостей. Експлуатація даної системи має сенс тільки за умови, що вона розвивається разом з мережею, яку вона захищає. Зрозуміло, це передбачає регулярне проведення тестів.

Подібні системи дозволяють вести єдину базу даних шаблонів, варіантів реагування і оновлень для всіх компонентів підсистеми безпеки, автоматизувати рутинні завдання адміністраторів безпеки (оновлення сигнатур атак, сканування віддалених вузлів і т.д.), а також проводити всебічний аналіз різних подій шляхом кореляції даних від різноманітних засобів захисту.

В даний час багато компаній, що займаються питаннями інформаційної безпеки (наприклад, Internet Security Systems та ін), пропонують стратегію застосування описаних вище систем у складі єдиних комплексів, які дозволяють здійснювати централізоване управління інформаційною безпекою корпоративної мережі. За допомогою єдиного керування всіма компонентами підсистеми інформаційної безпеки корпоративної мережі, а також на основі збору та аналізу інформації від різних компонентів у режимі реального часу можна значно підвищити ефективність роботи адміністраторів безпеки, скоротити число співробітників відповідних служб і зменшити витрати на їхнє навчання.

За повідомленням CNews.ru, в січні цього року, у зв'язку з наявністю широкого спектру антішпіонскіх програмних комплексів, компанії McAfee, Symantec, Trend Micro, ICSA Labs і Thompson Cyber Security Labs оголосили про укладення угоди щодо створення методологій ідентифікації і тестування для технологій, що забезпечують протидія шпигунським програмам.

Тестування продуктів буде засновано на стандартизованих, незалежних критеріях оцінки, а в середовищі виявлення та тестування будуть використовуватися загальні стандартні зразки.На думку учасників проекту, за рахунок використання стандартних метрик для оцінки третьою стороною, а також наявності загального стандарту для зразків можна буде порівнювати між собою характеристики продуктів, які раніше з працею піддавалися вимірюванню.

Але залишаються проблеми. Використання таких засобів захисту, як міжмережеві екрани, системи контролю доступу користувачів і т.п., не дає повної гарантії стійкості корпоративної мережі до атак. Будь-яке програмне чи апаратне забезпечення не є досконалим, і в ньому є уразливості, що дозволяють зробити які-небудь дії в порушення встановленого порядку використання інформаційних ресурсів. Крім того, реагувати на несанкціоновану активність або спроби злому мережі в режимі реального часу практично дуже складно, якщо ці функції виконуються вручну.

Тому своєчасне виявлення спроб злому інформаційних ресурсів та оперативна реакція на ці дії на основі наведених у доповіді методів дозволяють значно підвищити рівень захищеності корпоративної мережі.

### 3.4 Планування захисних заходів

Захист процесів або процедур обробки і зберігання інформації:

- програмні системи захисту інформації;

- криптографічна система захисту інформації (IP-шифратори) представлено на рис.3.2;

- захист місць зберігання інформації.

Захист каналів зв'язку:

- акустичні засоби захисту;

- захист від радіозакладок;

- захист від вбудованих вузьконаправлених мікрофонів;

- пасивний захист каналів зв'язку;

- контроль дротяних ліній;

- захист апаратів факсиміле і телефонних ;

- екранування приміщень.


Рисунок 3.2. IP-шифратори: а – «Канал - 201»; б – «Канал-401»

IP-шифратори забезпечують: шифрування та контроль цілісності IP-пакетів; інкапсуляцію IP-пакетів та їх маршрутизацію між мережними інтерфейсами; прийом та введення в дію ключових даних; встановлення захищених з'єднань з іншими IP-шифраторами.

Для захисту від силової дії по ланцюгах живлення застосовують фільтри мережеві трансформаторні. Вони призначені:

- для захисту електронної техніки від індустріальних і атмосферних перешкод, поширюваних по мережі живлення, окремих одиниць і комплексів електронної техніки;

- для захисту електронної техніки мережі живлення від навмисної силової дії з метою її нестійкої роботи або висновку з ладу;

- для запобігання розповсюдженню індустріальних перешкод по живлячій мережі від промислового устаткування, що є джерелом перешкод;

- для придушення в живлячій мережі інформаційних випромінювань від обчислювальної техніки оброблювальної конфіденційну інформацію;

- для підвищення електробезпеки шляхом гальванічного розділення первинної і вторинної мережі;

- для перетворення мережі TN-C в TN-S і організаціях “виділеної” мережі живлення;

- для стабілізації живлячої напруги в мережах з напругою відмінним від номінального.

Забезпечують:

- гальванічну розв'язку споживачів від первинної живлячої мережі;

- ослаблення імпульсних перешкод і шумів в діапазоні частот 0.001-30 МГц не менше чим в 1000 разів;

- стабілізацію живлячої напруги.

На рис. 3.3 зображено розподільчий шкаф ФСТТ-1500, який вбудовується в електрощитову для забезпечення живлення обєкту захисту. В табл. 3.2 приведено технічні харакрeристики розподільчого шкафа.

Рисунок 3.3. ФСТТ-1500

Таблиця 3.2

Технічні харакрeристики розподільчого шкафа

| Модель | Номінальна напруга, В, Гц | Номінальна потужніть, кВА | ККД не менше, % | R ізоляції, Вх./ вих., МОм | Вага не більше, кг | Габаритні розміри, мм |
|---|---|---|---|---|---|---|
| ФСТТ-1500 | 380,50 | 1500 | 0,97 | 10 | 24,0 | 310 x 220 x 400 |

Циркулююча в тих або інших технічних засобах конфіденційна інформація може потрапити в ланцюги і мережі електричного живлення і через них вийти за межі контрольованої зони. Наприклад, в лінію

електроживлення висока частота може передаватися за рахунок паразитних місткостей трансформаторів блоків живлення. Як заходи захисту широко використовуються методи розв'язки (розводки) ланцюгів живлення за допомогою окремих стабілізаторів, перетворювачів, мережевих фільтрів для окремих засобів або приміщень. Можливе використання окремих трансформаторних вузлів для всього енергопостачання об'єкту захисту, розташованого в межах контрольованої території. Це надійніше рішення локалізації даного каналу витоку.

Однією з важливих умов захисту інформації від витоку по ланцюгах заземлення є правильне їх устаткування. В даний час існують різні типи заземлень. Найчастіше використовуються одноточкові, багатоточкові і комбіновані (гібридні) схеми. На рис. 3.4 представлена одноточкова послідовна схема заземлення.

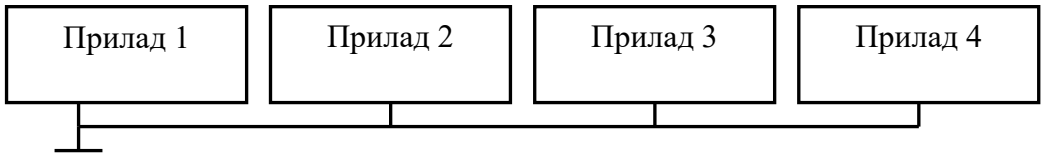


Рисунок 3.4. Одноточкова послідовна схема заземлення

Ця схема найбільш проста. Проте їй властивий недолік, пов'язаний з протіканням зворотних струмів різних ланцюгів по загальній ділянці заземляючого ланцюга. Внаслідок цього можлива поява небезпечного сигналу в сторонніх ланцюгах.

У одноточковій паралельній схемі заземлення (рис. 3.5) цього недоліку немає. Проте така схема вимагає великого числа протяжних заземляючих провідників, із-за чого може виникнути проблема із забезпеченням малого опору заземлення ділянок ланцюга. Крім того, між заземляючими провідниками можуть виникати небажані зв'язки, які створюють декілька шляхів заземлення для кожного пристрою. В результаті в системі заземлення можуть виникнути зрівняльні струми і з'явитися різниця потенціалів між різними пристроями.

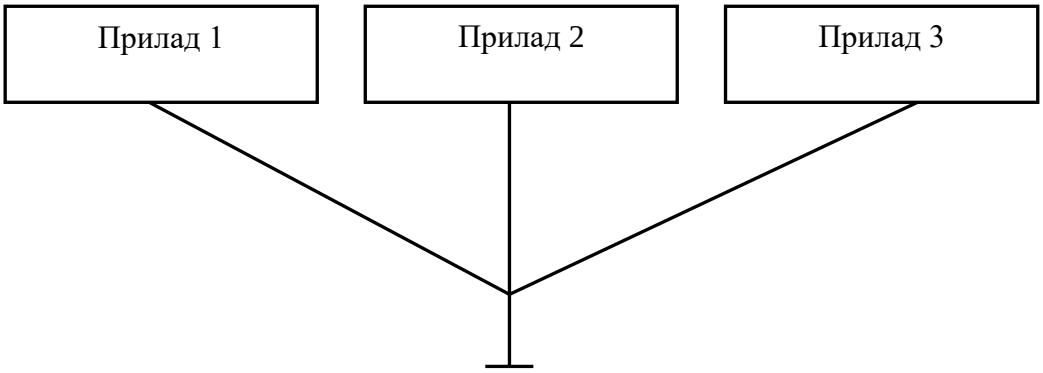


Рисунок 3.5. Одноточкова паралельна схема заземлення

Багатоточкова схема заземлення (рис. 3.6) практично вільна від недоліків, властивих одноточковій схемі. В цьому випадку окремі пристрої і ділянки корпусу індивідуально заземлені. При проектуванні і реалізації багатоточкової системи заземлення необхідно приймати спеціальні заходи для виключення замкнутих контурів.

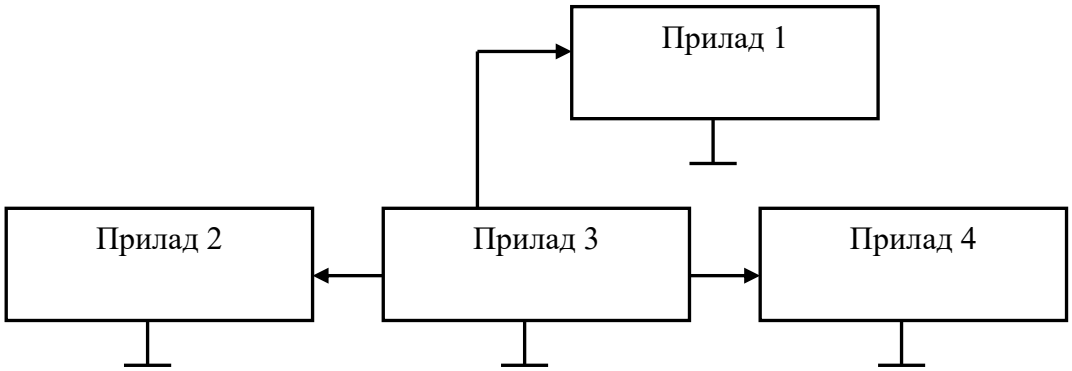


Рисунок 3.6. Багатоточкова схема заземлення

Як правило, одноточкове заземлення застосовується на низьких частотах при невеликих розмірах пристроїв, що заземляються, і відстанях між ними менше 0,5•λ. На високих частотах при великих розмірах пристроїв, що заземляються, і значних відстанях між ними використовується багатоточкова система заземлення. У проміжних випадках ефективна комбінована (гібридна) система заземлення, що є різними поєднаннями одноточковою, багатоточковою і плаваючою заземляючих систем.

Заземлення технічних засобів систем інформатизації і зв'язку повинне бути виконане відповідно до певних правил.

Основні вимоги, що пред'являються до системи заземлення, полягають в наступному:

- система заземлення повинна включати загальний заземлитель, що заземляє кабель, шини і дроти, сполучаючі заземлітель з об'єктом;

- опору заземляючих провідників, а також земляних шин повинні бути мінімальними;

- кожен елемент, що заземляється, повинен бути приєднаний до заземлителя або до заземляючої магістралі за допомогою окремого відгалуження. Послідовне включення в заземляючий провідник декількох елементів, що заземляються, забороняється;

- у системі заземлення повинні бути відсутніми замкнуті контури, утворені з'єднаннями або небажаними зв'язками між сигнальними ланцюгами і корпусами пристроїв, між корпусами пристроїв і землею;

- слід уникати використання загальних провідників в системах екрануючих заземлень, захисних заземлень і сигнальних ланцюгів;

- якість електричних з'єднань в системі заземлення повинна забезпечувати мінімальний опір контакту, надійність і механічну міцність контакту в умовах кліматичних дій і вібрації;

- контактні з'єднання повинні виключати можливість утворення оксидних плівок на контактуючих поверхнях і пов'язаних з цими плівками нелінійних явищ;

- контактні з'єднання повинні виключати можливість утворення гальванічних пар для запобігання корозії в ланцюгах заземлення;

- забороняється використовувати як заземляючий пристрій нульові фази електромереж, металоконструкції будівель, що мають з'єднання із землею, металеві оболонки підземних кабелів, металеві труби систем опалювання, водопостачання, каналізації і т.д.

# ВИСНОВКИ

Оскільки корпоративні мережі займають все більший сегмент телекомунікаційних систем у всіх сферах суспільного життя, бізнесі, підприємствах, науці тощо. Тому розробка і впровадження систем захисту мультимедійної інформації в корпоративних мережах є дуже актуальним завданням, вирішення якого вимагає багато складних операцій та алгоритмів.

В ході виконання данної роботи було проаналізовано концепцію корпоративної мережі, розглянуті мережеві технології, топології мереж та специфіка їх використанн, розглянуто проблему вразливостей корпоративних мереж та способи їх уникнення.

Запропоновано комплекс захисних заходів та апаратно-програмні засоби захисту мультимедійної інформації на підприємстві.

# СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Максименко Г.А., Хорошко В.А. Методы выявления, обработки и идентификации сигналов радиозакладных устройств. – К.: ООО “ПолиграфКонсалтинг”, 2004. – 317 с.

2. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. − СПб.: “Наука и техника”, 2004. − 384 с.

3. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособ. − М: “Горячая линия − Телеком”, 2004. − 280 с.

4. Корченко А.Г. Построение систем защиты информации на нечётких множествах. Теория и практические решения. − К.: “МК-Пресс”, 2006. − 320 с.

5. Домарев В.В. Безопасность информационных технологий. Системный подход. − К.: ООО “ТИД “ДС”, 2004. − 992 с.

6. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. − М.: “Вильямс”, 2004. − 1104 с.

7. Новиков Ю.В., Карпенко Д.Г. Аппаратура локальных сетей: функции, выбор, разработка / Под ред. Ю.В. Новикова. – М., Издательство ЭКОМ, 1998. – 288 с.

8. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А. Олифер. – СПб: Издательство “Питер”, 2000. – 672 с.

9. Куин Л., Рассел Р. Fast Ethernet. – К.: Издательская группа BNV, 1998. – 448 с.

10. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних. – К.: Вид-во ТОВ «НВП ІНТЕРСЕРВІС», 2009. – 716 с.

11. Конахович Г.Ф., Чуприн В.М. Мережі передачі пакетних даних – К: «НК-Пресс», 2006 -272 с.