Міністерство освіти і науки, молоді та спорту України
Національний педагогічний університет
імені М. П. Драгоманова
Кафедра інформаційних систем і технологій

Т. М. Слабошевська, І. М. Смекалін, С. М. Яшанов

Практикум з експлуатації інформаційної техніки

Частина II

Навчально-методичний посібник

Київ
Вид-во НПУ імені М. П. Драгоманова
2012

УДК 004(076)
ББК 32.97я73-5
С 47

Друкується за ухвалою Вченої ради
Національного педагогічного університету імені М. П. Драгоманова
(протокол № 11 від 14 червня 2012 р.)

Рецензенти: **Л. Н. Беркман**, доктор технічних наук, професор Державного університету інформаційно-комунікаційних технологій;

В. Д. Сиротюк, доктор педагогічних наук, професор, завідувач кафедри теорії та методики навчання фізики та астрономії НПУ імені Драгоманова.

Слабошевська Т. М.

С 47 Практикум з експлуатації інформаційної техніки : навчально-методичний посібник. Ч. 2 / Т. М. Слабошевська, І. М. Смекалін, С. М. Яшанов ; за заг. редакцією С. М. Яшанова ; Мін-во освіти і науки, молоді та спорту України, Нац. пед. ун-т імені М. П. Драгоманова. – К. : Вид-во НПУ імені М. П. Драгоманова, 2012. – 113 с.

У навчально-методичному посібнику представлено цикл лабораторних робіт з дисципліни “Практикум з експлуатації інформаційної техніки”, що включає лабораторні роботи, опрацювання яких дає навички підключення та експлуатації персональних комп’ютерів, принтерів, сканерів, фото-, відеотехніки, засобів комунікації та мобільних засобів інформаційної техніки.

Видання розраховано на студентів та викладачів вищих педагогічних навчальних закладів, інститутів післядипломної педагогічної освіти напряму підготовки “Технологічна освіта”.

УДК 004(076)
ББК 32.97я73-5

ISBN

Вступ

Істотною частиною методичної системи підготовки майбутнього вчителя технологій у галузі інформатичних дисциплін є лабораторний практикум. Лабораторні роботи дозволяють інтегрувати теоретичні, методологічні знання, а також практичні вміння і навички студентів у єдиному процесі діяльності навчально-дослідницького характеру. При вивченні інформатичних дисциплін можуть поєднуватися і фронтальна робота, що є одночасним виконанням загального завдання всіма студентами групи й індивідуальна робота, при якій кожному студентові даються завдання, різні за об'ємом, складності і часу виконання.

Виконання завдання сприяє формуванню певних умінь і навичок, які оцінюються викладачем під час звіту. Впровадження ІТ у навчальний процес актуалізує розробку і використання в цьому практикумі спеціалізованих електронних освітніх ресурсів, орієнтованих на застосування спеціальних, комп'ютеризованих приладів і устаткування призначеного для проведення експериментальних робіт.

Цикл лабораторних робіт з дисципліни "Практикум з експлуатації інформаційної техніки" продовжує знайомити студентів із правилами експлуатації інформаційної техніки. Даний навчально-методичний посібник включає лабораторні роботи опрацювання яких дає навички встановлення та налаштування програмного забезпечення різного типу для комплексної роботи з різноманітним устаткуванням, а

також знайомить студентів із спеціалізованими засобами інформаційної техніки.

У посібник включені хід роботи, індивідуальні і групові завдання, а також необхідні теоретичні відомості та вимоги до звіту, що містять контрольні питання з теми.

Запропоновані роботи мають виконуватися в умовах лабораторії з використанням необхідного устаткування, технічних засобів та наочних посібників.

ЛАБОРАТОРНА РОБОТА № 8

Тема: BIOS та його різновиди. Налаштування та оновлення *BIOS*

Мета роботи: ознайомити студентів із структурою і різновидами BIOS, налаштування та правилами оновлення.

Порядок виконання роботи:

1. Ввімкнути комп'ютер.
2. Запустити програму емуляції BIOS в режимі "Демо".
3. Ознайомитися з можливостями BIOS (виписати в звіт закладки та дати коротку характеристику кожної із закладок).
4. Змінити режим роботи програми на "Тест" (для переходу в режим тестування натисніть клавішу Esc).
5. Результати тестування показати викладачу.
6. Зробіть звіт про виконану роботу.
7. У звіті дайте письмові відповіді на контрольні запитання.

Теоретичні відомості

BIOS (Basic Input/Output System – базова система введення/виведення) – це обов'язкове програмне забезпечення комп'ютера, яке доступне без звертання до пристроїв зовнішньої пам'яті. Це набір програм перевірки й обслуговування апаратних засобів ПК. BIOS отримує управління при вмиканні або перезавантаженні ПК, тестує системну плату й основні блоки комп'ютера – відеоадаптер, клавіатуру, контролери дисків і портів введення/виведення, налаштовує чипсет і передає управління завантажувачу операційної системи.

BIOS складається з таких частин:

1. POST (Power On Self Test) – програма, відповідальна за тестування апаратних засобів комп'ютера при вмиканні живлення.

2. System Setup – програма налаштування системи.

3. Набір програм для управління апаратною частиною ПК.

BIOS узагалі унікальний для кожної моделі материнської плати комп'ютера, тобто він розробляється з урахуванням особливостей функціонування тієї комбінації обладнання, що властива саме для цієї моделі. BIOS для сучасних системних плат розробляється найчастіше однією з фірм, що спеціалізуються на цьому:

Award Software (яка поглинула Phoenix Technology – одного з найвідоміших у минулому виробників BIOS);

American Megatrends Inc. (AMI), InsydeBIOS.

Де зберігається BIOS

В усіх сучасних платах BIOS зберігається в електрично-програмованих ПЗП (постійний запам'ятовуючий пристрій) (Flash ROM), що допускають перепрошивку BIOS засобами самої плати за допомогою спеціальної програми. Це дозволяє підвищувати технічні можливості материнської плати. Однак, крім явних плюсів, у цій технології є також мінуси. Наприклад, сьогодні існує група вірусів, що, користуючись можливістю змінювати вміст BIOS, стирають або псують його й у такий спосіб роблять комп'ютер непрацездатним через неправильний або відсутній BIOS комп'ютер відмовляється завантажуватися. Виправити таку ситуацію можна тільки в сервісному центрі, де в спеціальному пристрої-програматорі – на мікросхему Rash ROM буде записана вихідна версія BIOS.

Свою конфігурацію BIOS зберігає в так званій CMOS RAM. CMOS RAM називається так тому, що вона виконана на основі CMOS-структурі (CMOS – Complementary Metal Oxide Semiconductor), що відрізняються малим енергоспоживанням. Однак CMOS-пам'ять енергозалежна, оскільки постійно підживлюється від батарейки, розташованої на системній платі. У ноутбуках та нетбуках живлення CMOS-пам'яті відбувається від акумуляторної батареї.

У той час, коли комп'ютер увімкнутий, CMOS RAM живиться від блока живлення комп'ютера.

У CMOS RAM зберігається інформація про поточні показники часу, конфігурацію комп'ютера: кількості пам'яті, типах накопичувачів тощо. У випадку ушкодження мікросхеми CMOS RAM (або розрядці батареї чи акумулятора) BIOS має можливість скористатися конфігурацією за замовчуванням.

Чи потрібно змінювати BIOS

Загальний принцип, якого слід дотримуватися: якщо комп'ютер працює стабільно і ніяких дефектів у його роботі, пов'язаних із BIOS, не виявлено (при цьому потрібно переконатися, що ці недоліки викликані саме BIOS, а не іншими причинами, наприклад неправильними драйверами пристроїв, неправильною конфігурацією операційної системи), при цьому відновлювати BIOS не доцільно.

Однак існують ситуації, коли відновлення BIOS необхідне. Зазвичай це вихід нового процесору, підтримка якого не була закладена в поточній версії BIOS. Перш ніж встановлювати нову версію, необхідно вийти на сайт технічної підтримки фірми-виробника системної плати, прочитати специфікації нової версії BIOS і при необхідності скачати їх, переконавшись, що ця версія виправляє саме ті дефекти, що були виявлені у вашому комп'ютері.

Як BIOS завантажує комп'ютер

Після вмикання комп'ютера на процесор подається напруга, і він "прокидається". Першими прочитаними процесором командами є інструкції з чіпа BIOS (про це піклуються мікросхеми системної плати). Першим запускається POST – програма самотестування. POST виконує такі кроки:

– ініціалізує системні ресурси й регістри чипсетів, систему управління електроживленням;

– визначає обсяг і тестує оперативну пам'ять (RAM);

– ініціалізує відеоадаптер;

– вмикає клавіатуру;

– тестує послідовні й паралельні порти;

– ініціалізує дисководи й контролери жорстких дисків;

– відображає підсумкову системну інформацію.

У процесі виконання цих дій BIOS порівнює дані поточної системної конфігурації з інформацією, що зберігається в CMOS, і при необхідності відновлює її. Якщо при виконанні якого-небудь кроку виникли збої, BIOS інформує про це повідомленнями на екрані монітора, а якщо це неможливо (наприклад, ще не був ініціалізований відеоадаптер), подає звуковий сигнал через системний динамік. Кількість та характер звукових сигналів відповідає кодам помилки.

Звукові сигнали POST різних фірм-виробників BIOS

На сьогодні не створені жодні стандарти, що регламентують формат звукових повідомлень. Проте слід зазначити, що більшість виробників використали короткий сигнал, щоб сповістити про успішне закінчення процедур POST.

Звукові повідомлення AwardBIOS

У AwardBIOS, який від 1998 року теж належить компанії Phoenix Technologies Ltd., система звукових повідомлень, що застосовується під час виконання його POST, доволі проста. Звукова індикація виконується лише у двох випадках:

– негаразди з оперативною пам’яттю: послідовність коротких сигналів;

– проблеми з відеокартою: після довгого сигналу подається два коротких.

Звукові повідомлення AMIBIOS

Під час виконання POST, розроблений компанією American Megatrends Inc. надсилає до системного динаміка послідовність звукових сигналів про наступні ситуації з комп’ютерним обладнанням:

- 1 сигнал – проблеми із схемами регенерації пам’яті;
- 3 сигнали – помилка оперативної пам’яті;
- 6 сигналів – негаразди з контролером клавіатури;
- 7 сигналів – помилка центрального процесору;
- 8 сигналів – проблеми з відеокартою.

Звукові повідомлення InsydeBIOS

де К – короткий звук, Д – довгий звук.

На сьогодні відомо дев’ять звукових повідомлень:

- ККК–ККД (помилки в роботі DMA-регістрів)
- ККК–КДК (помилки в роботі схем регенерації пам’яті)
- ККК–КДД (хибна контрольна сума BIOS)
- ККК–ДКК (помилки в CMOS-пам’яті)
- ККК–ДКД (помилки в роботі DMA-контролера)
- ККК–ДДК (помилки в роботі PIC-контролера)
- ККК–ДДД (помилки в роботі контролера клавіатури)
- ККД–ККК (помилки в роботі VGA-адаптера)
- ККД–ККД (помилки в оперативній пам’яті)

Після того як усі POST-завдання завершені, починає шукати програму-завантажник. Сучасні версії BIOS дозволяють завантажувати операційну систему з різних носіїв інформації (HDD, CD/DVD, USB-пристроїв).

Програма-завантажник, як правило, розташовується в першому секторі диска, на якому розміщена операційна система. Порядок перебору дисків при пошуку завантажника задається в конфігурації BIOS. Якщо завантажник знайдений, він переноситься в пам’ять і йому передається управління. Він у свою чергу знаходить і копіює в пам’ять власне програму завантаження операційної системи (operation system loader), що завантажує, ініціалізує і конфігурує операційну систему й драйвери пристроїв.

Налаштування BIOS (System Setup)

Після виконання послідовності тестів POST і перед початком пошуку програми-завантажника, BIOS надає користувачеві можливість увійти в програму конфігурації системи – System Setup. Про це BIOS повідомляє написом на екрані (зазвичай “Натисніть клавішу **Del** для входу в **Setup**”). Натиснувши відповідну клавішу (найчастіше – **Delete**), ви потрапляєте в меню програми конфігурації. З нього можна настроїти масу різних параметрів. Розглянемо деякі з них, наприкладі *AMIBIOS* (рис. 8.1).

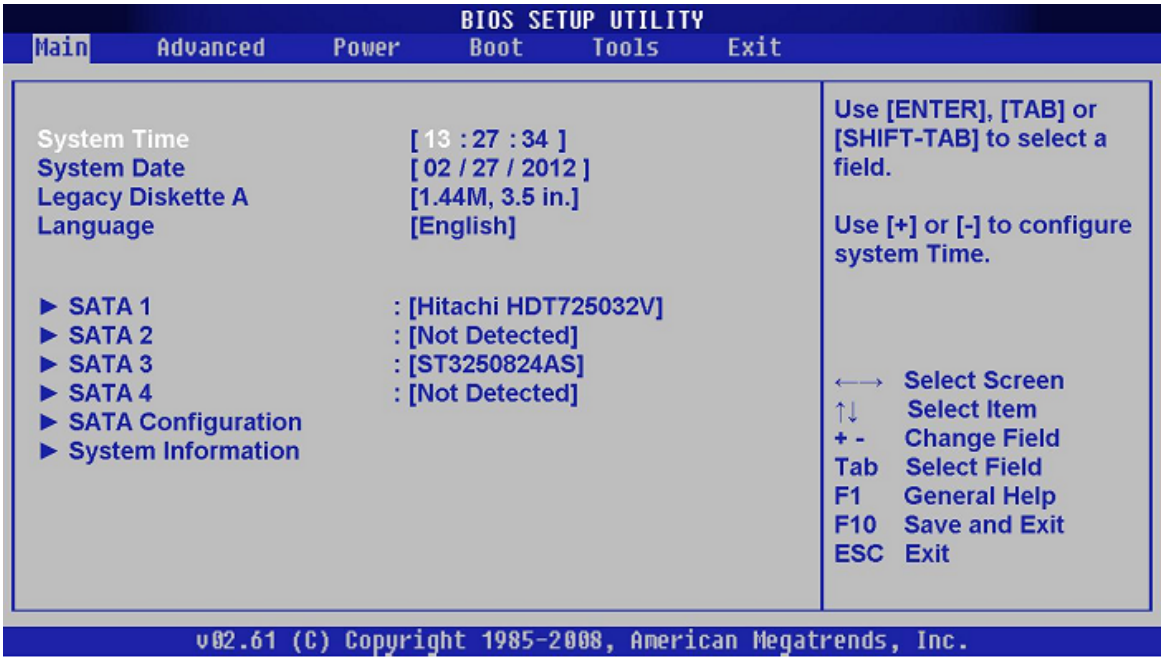

Рис. 8.1. Інтерфейс *AMIBIOS*

Розділ MAIN

У розділі *MAIN* (рис. 8.1) надається можливість самостійного налаштування часу та дати системи, а також налаштувати підключення жорстких дисків та інших накопичувачів.

Як правило, BIOS автоматично визначає всі підключені пристрої, їх не потрібно включати вручну, але можна змінити деякі параметри при їх автоматичному включенні. Для цього слід вибрати потрібний вам жорсткий диск або інший накопичувач, і натиснути “Enter” на клавіатурі. Після цього в меню налаштувань обраного накопичувача, ми бачимо всю інформацію про підключений до першого каналу жорсткий диск. Якщо до каналу не підключений жоден пристрій, то ми бачимо напис “Not Detected” (рис. 8.2).

Type – даний параметр надає змогу налаштувань жорстокого диску, слід змінити з Auto на User.

LBA/Large Mode – даний параметр відповідає за підтримку накопичувачів, об’єм яких більше 504 Мбайт. Таким чином тут бажано вибрати значення AUTO.

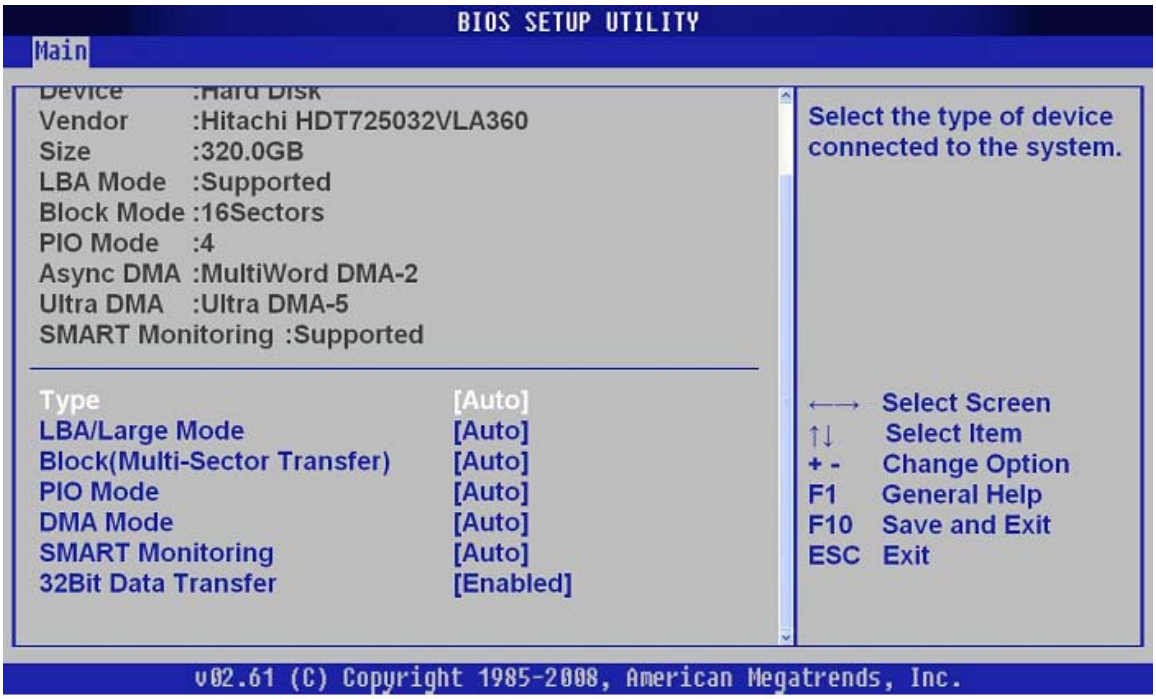

Рис. 8.2 Меню налаштувань обраного накопичувача

Block (Multi-Sector Transfer) – за допомогою цього параметру можна відключити передачу даних декількох секторів одночасно по 512 байт, тобто, відключаючи даний параметр, різко знизиться швидкість роботи жорсткого диска, адже за раз передаватиметься тільки 1 сектор рівний 512 байт. Для швидкої роботи краще поставити режим AUTO.

PIO Mode – за допомогою даного параметра, можна змусити жорсткий диск працювати в застарілому режимі обміну даними. Автоматично сучасні жорсткі диски працюють в найшвидшому режимі, тому, тут також краще виставити значення AUTO.

DMA Mode – прямий доступ до пам'яті. Для досягнення вищої швидкості зчитування/запису, слід залишити значення AUTO.

SMART Monitoring – за допомогою цієї технології можна відстежувати стан жорсткого диска. Іншими словами – це технологія самоспостереження, звітності і аналізу. Також краще виставити значення AUTO.

32 Bit DataTransfer – якщо встановлений параметр "Enabled" (включений), то данні по шині PCI передаватимуться в 32-бітовому режимі. Якщо встановлений параметр "Disabled" (відключений), то данні будуть передаватися в 16-бітовому режимі.

System Information

У розділі MAIN, також можна отримати деяку інформацію про систему. Для цього вибрати пункт меню System Information (рис. 8.3). У вікні, що відкрилося, ви побачите версію BIOS і дату його виробництва, також тут є інформація про процесор і системну пам'ять.

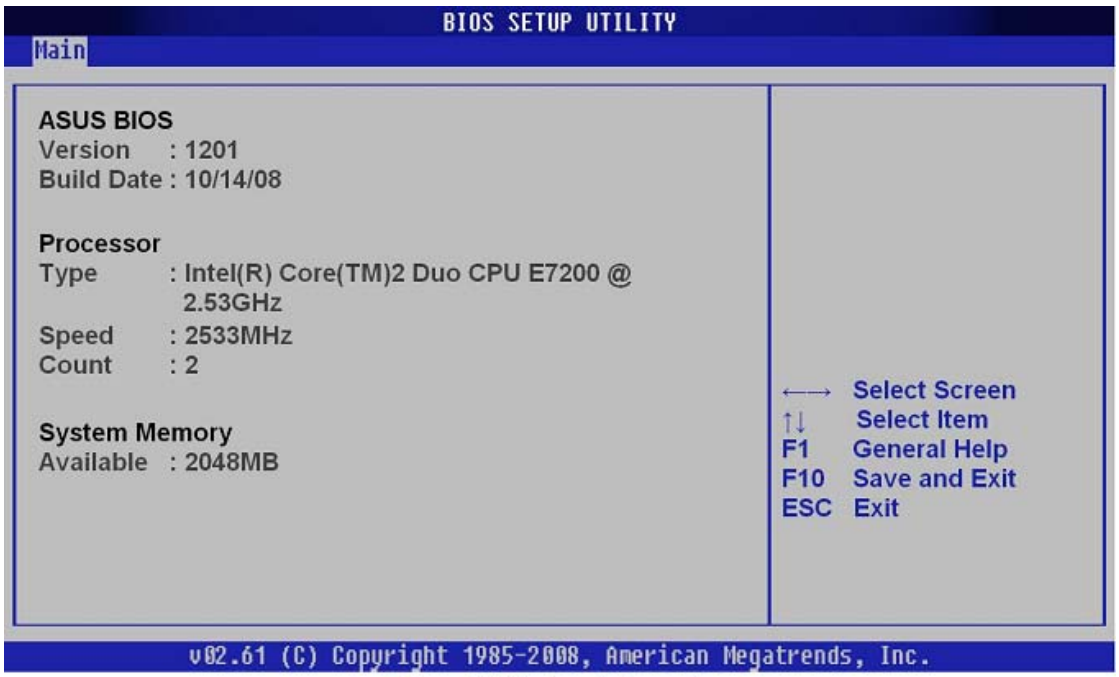

Рис. 8.3. System Information

SATA Configuration

Вибравши в розділі MAIN пункт SATA Configuration (рис. 8.4), відповідає за налаштування дискової підсистеми. SATA Configuration має три параметри:

- **Disabled –** відключає SATA-контролер;
- **Enhanced –** стандартний режим роботи;
- **Compatible** – дискова підсистема працюватиме в режимі сумісності із застарілими операційними системами (Windows 98, 95, Me).

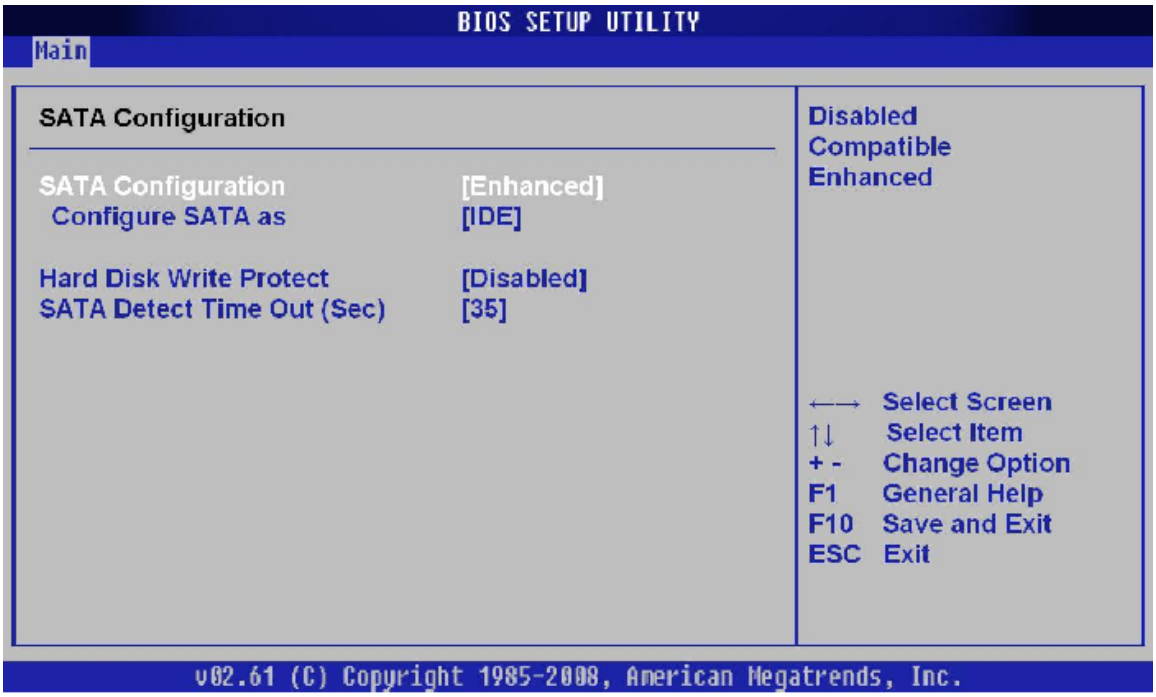

Рис. 8.4. SATA Configuration

Configure SATA as – має два режими:

- IDE – режим, який дозволяє бачити всі підключені диски у вигляді IDE-пристроїв;
- AHCI – режим, який дозволяє використовувати сучасну технологію Plug-in-Play.

Hard Disk Write Protect і **SATA Detect Time Out**. Основним завданням даних параметрів є захист дисків від запису, тобто краще залишити параметр Hard Disk Write Protect в режимі **Disabled**. Змінюючи параметр SATA Detect Time Out, можна змінити час, який буде витрачено комп'ютером на пошук дискової підсистеми.

Розділ Advanced (рис. 8.5)

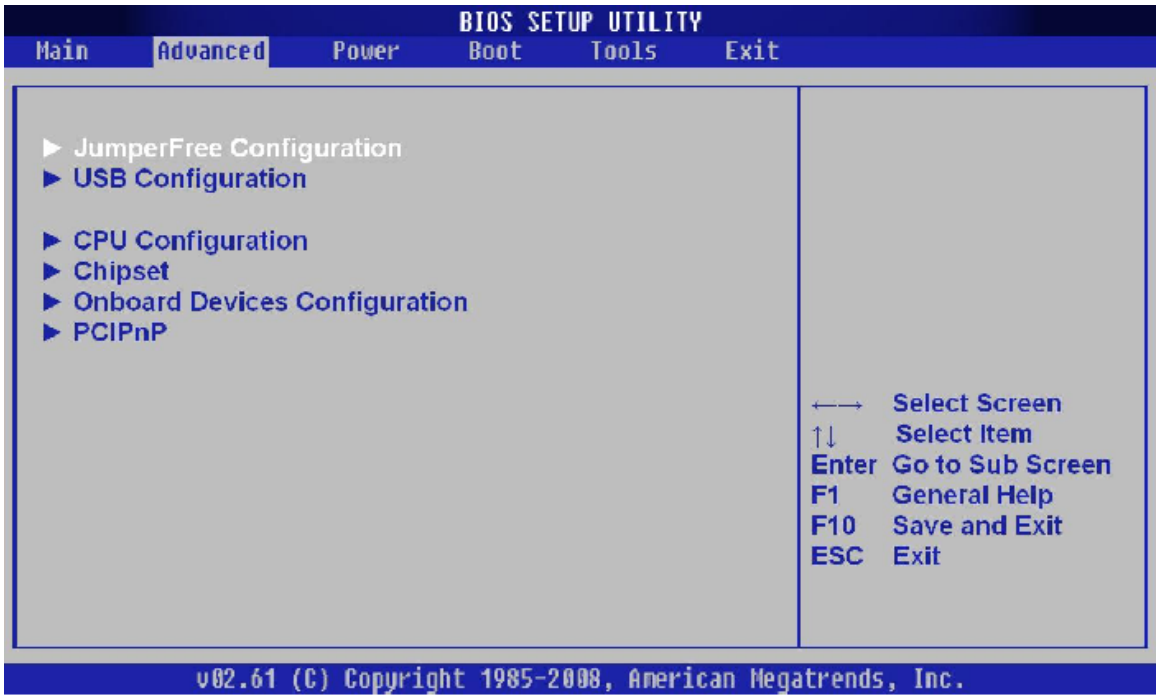

Рис. 8.5. Розділ Advanced

В даному розділі пункт **JumperFree Configuration**, відкриває доступ до групи параметрів **Configure System Perfomance Settings** (рис. 8.6).

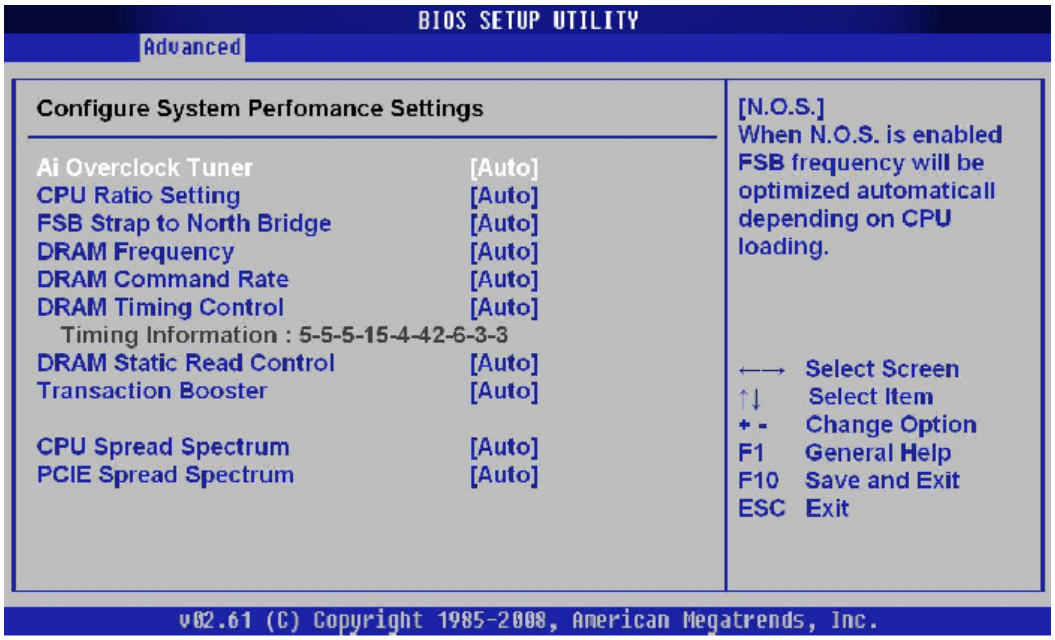

Рис. 8.6. Configure System Perfomance Settings

Ai Overclock Tuner – має два режими роботи:

- **AUTO** – процесор працює в штатному режимі;
- **Manual** – ручне налаштування режиму роботи процесору.

DRAM Frequency – цей параметр дозволяє задати частоту шини пам'яті незалежно від частоти шини процесора.

Елемент меню **CPU Configuration** (рис. 8.7) надає можливість змінювати всі налаштування пов'язані з центральним процесором, також можна спостерігати за його роботою і дізнаватися всі відомості про центральний процесор.

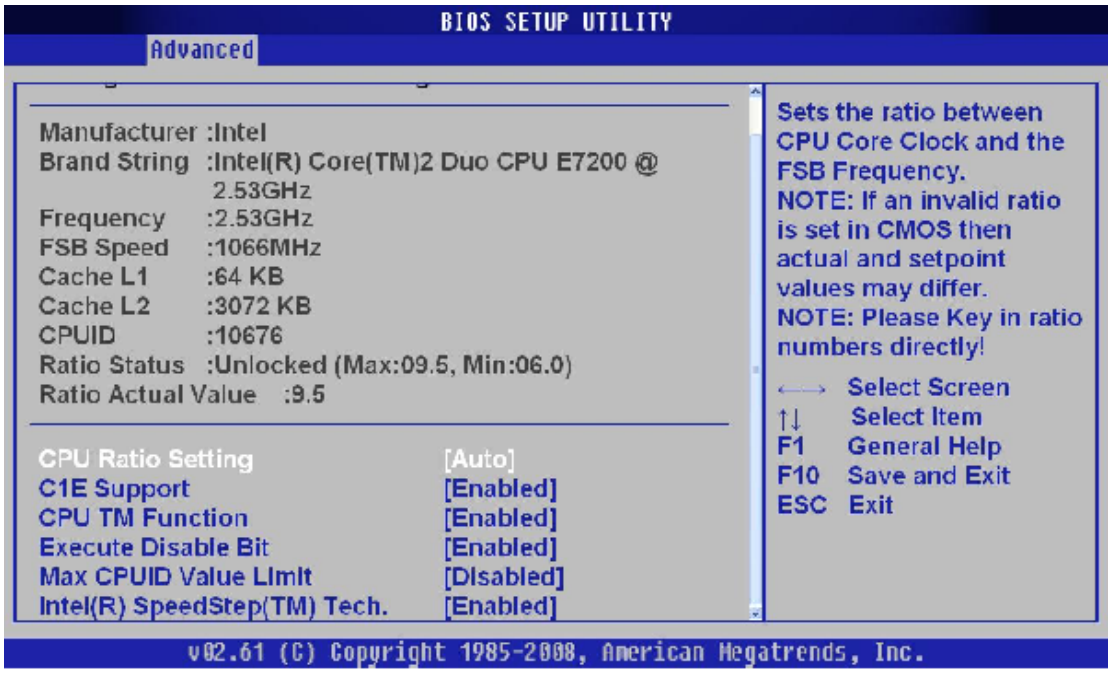

Рис. 8.7. Configure Advanced CPU Settings

Елемент меню **Onboard Devices Configuration** (рис. 8.8) це набір параметрів які впливають на роботу контролерів і портів материнської плати.

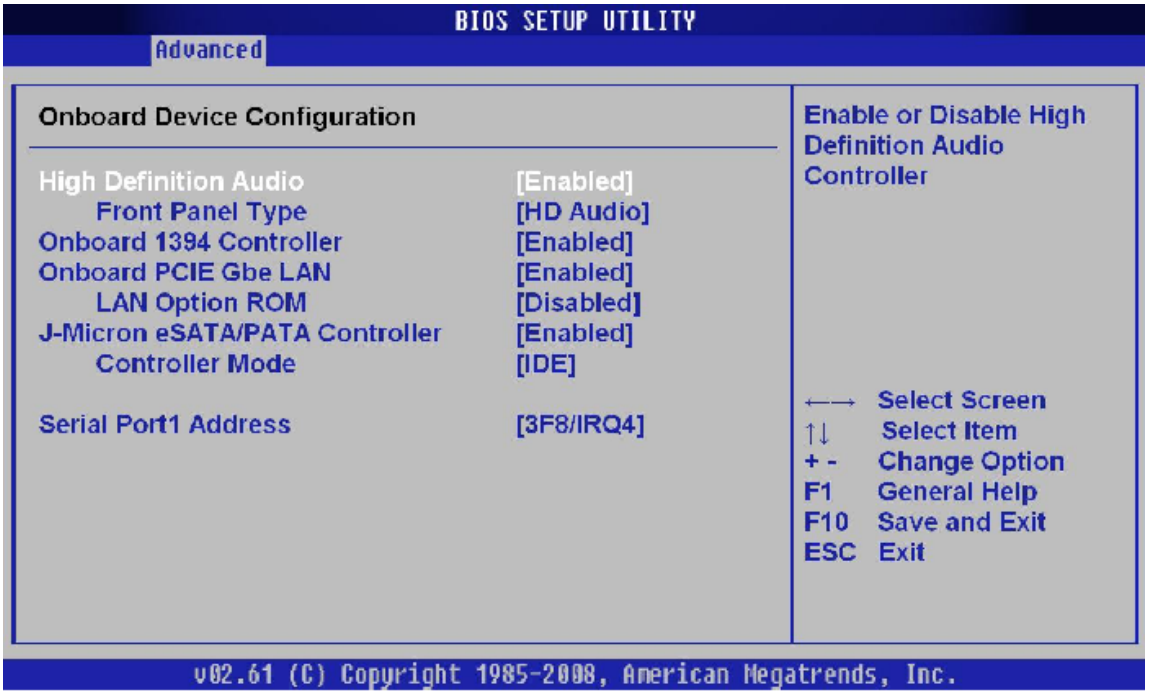

Рис. 8.8. Onboard Devices Configuration

Наприклад, змінюючи значення **Onboard 1394 Controller**, ми можемо відключити або навпаки включити його.

Елемент меню **USB Configuration** (рис. 8.9) відповідає за роботу послідовного інтерфейсу USB.

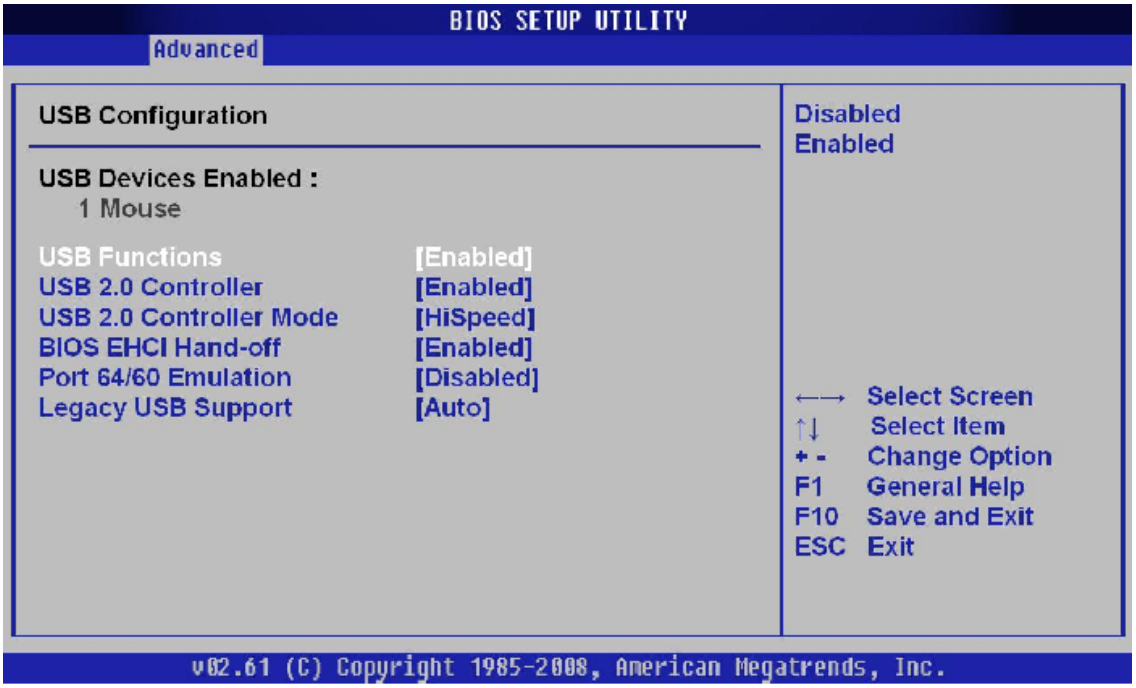

Рис. 8.9. USB Configuration

Розділ POWER (параметри живлення) (рис. 8.10)

У розділі **Power** можна налаштувати функції енергозбереження і включення і відключення вашого комп'ютера.

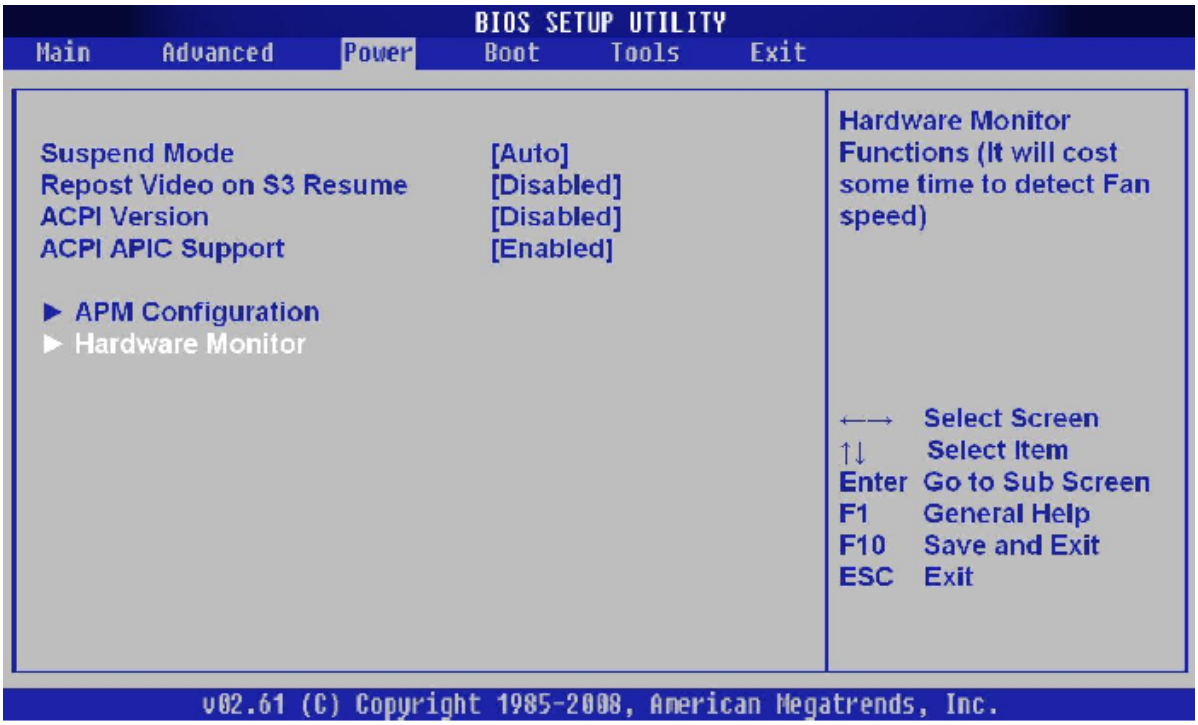

Рис. 8.10. Розділ POWER

Елемент меню **ACPI** – Advanced Configuration and Power Interface – цей інтерфейс розширеного управління живленням.

Елемент меню **Hardware Monitor** (рис. 8.11), надає інформацію про температуру центрального процесора і про швидкість обертання вентиляторів, а також можна отримати інформацію з решти всіх датчиків комп'ютера, і внести зміни в деякі параметри блоку живлення.

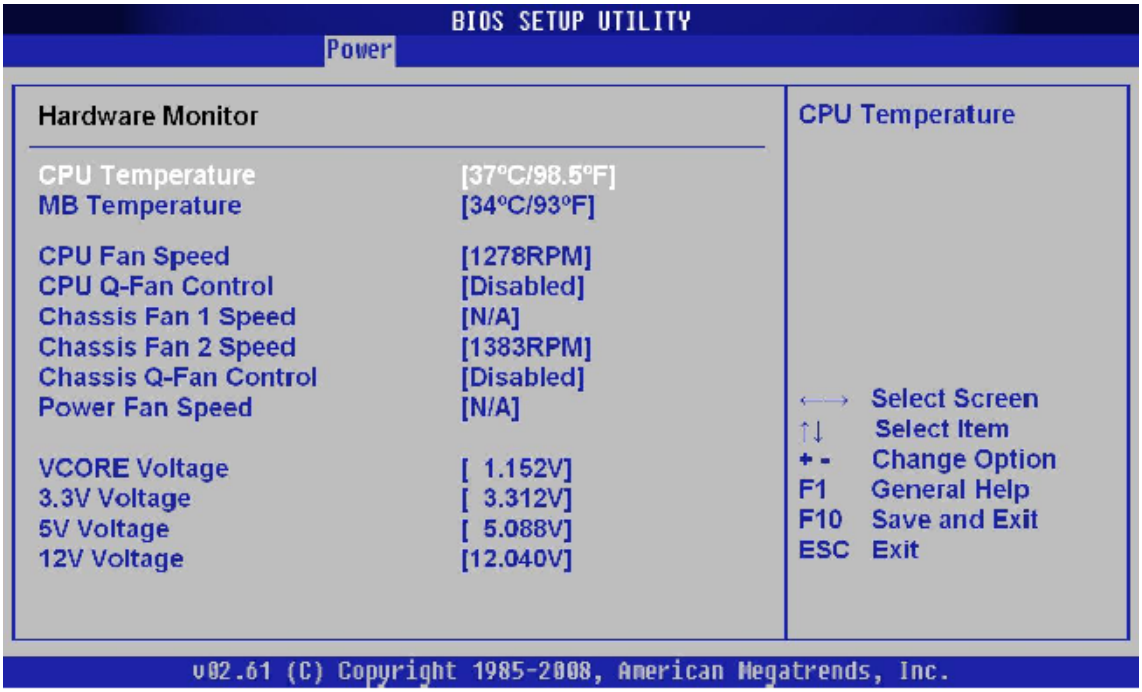

Рис. 8.11 Hardware Monitor

Розділ Boot (рис. 8.12) – у даному розділі можна провести зміни в параметрах завантаження.

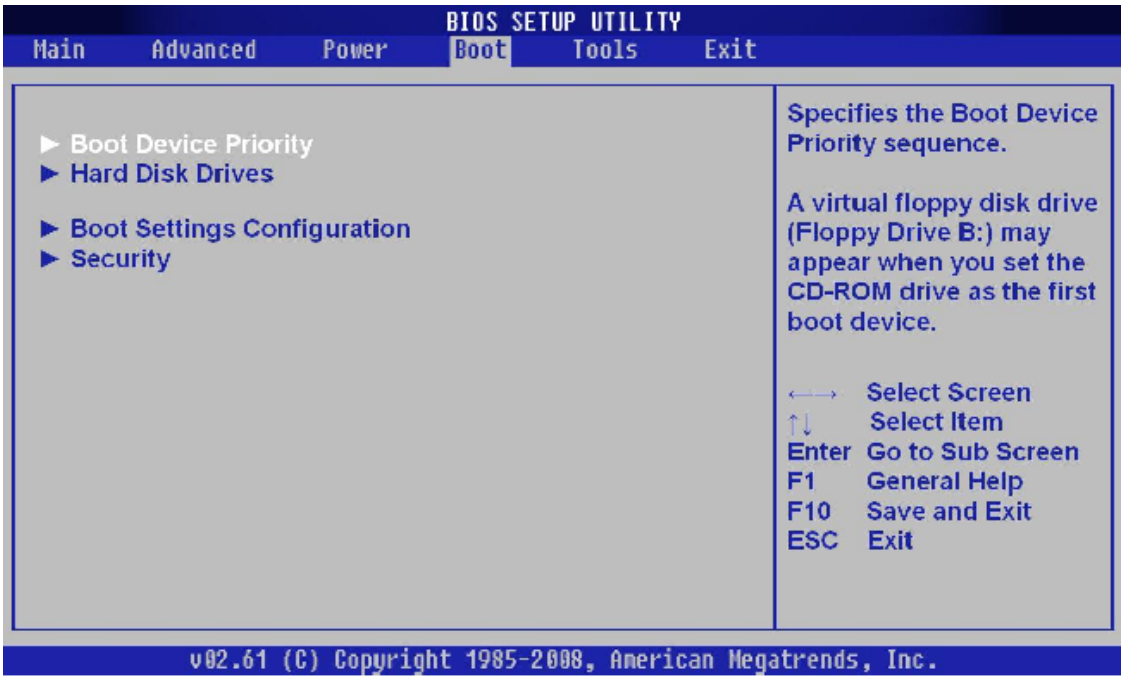

Рис. 8.12. Розділ Boot

Елемент меню **Boot Device Priority** (рис. 8.13) надає можливість встановити пріоритетність пристроїв для завантаження операційної системи, тобто який із пристроїв буде опитуватися першим, другим і т.д.

Для того, щоб встановити операційну систему потрібно першим вказати той пристрій з якого буде відбуватися інсталяція ОС.

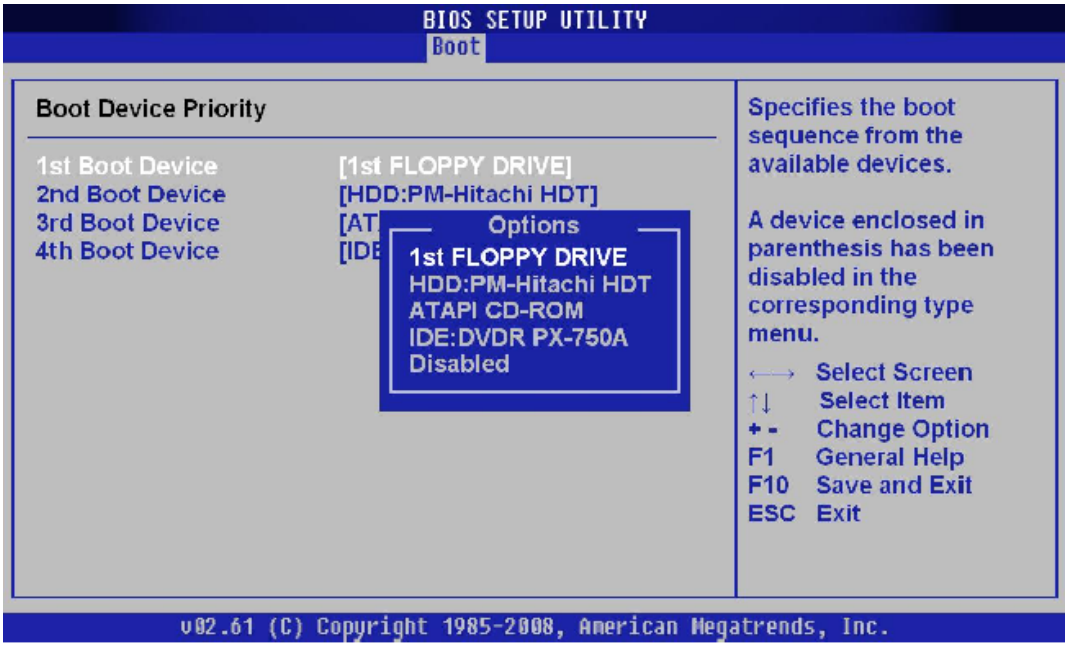

Рис. 8.13 Boot Device Priority

Елемент меню **Hard Disk Drivers** (рис 8.14) даний параметр дозволяє змінити послідовність пристроїв, з якого спочатку завантажуватиметься операційна система. Даний параметр слід використовувати, коли в комп'ютері встановлено декілька жорстких дисків з різними ОС.

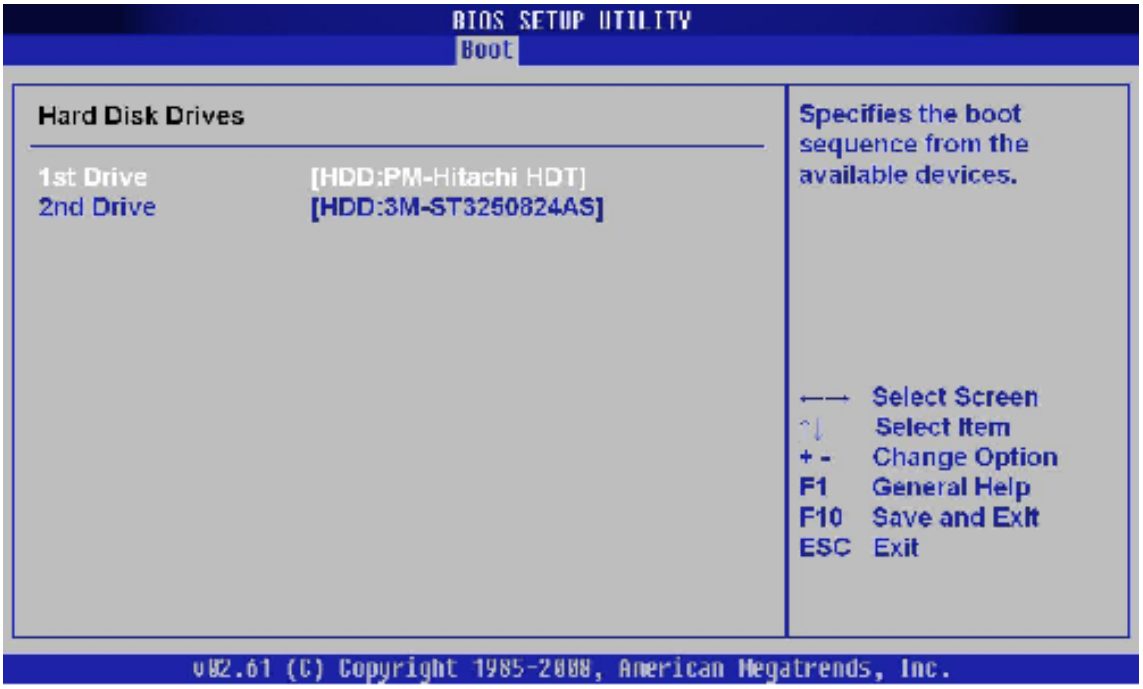

Рис. 8.14. Hard Disk Drivers

Елемент меню **Boot Setting Configuration** (рис. 8.15) містить налаштування, що впливають на процес завантаження операційної системи, ініціалізацію клавіатури і миші, обробку помилок і так далі.

Quick Boot – параметр, активувавши який, кожного разу при включенні комп'ютера, BIOS проводитиме тест оперативної пам'яті, що призведе до швидшого завантаження операційної системи.

Full Screen Logo – параметр, який відповідає за вивід повноекраного графічного зображення логотипу материнської плати.

Add On ROM Display Mode – параметр, який визначає порядок появи на екрані інформації про пристрої, які підключені через плати розширення і мають свій власний BIOS.

Bootup Num-Lock – параметр, що визначає, в якому стані при включенні ПК повинна бути клавіша "Num Lock".

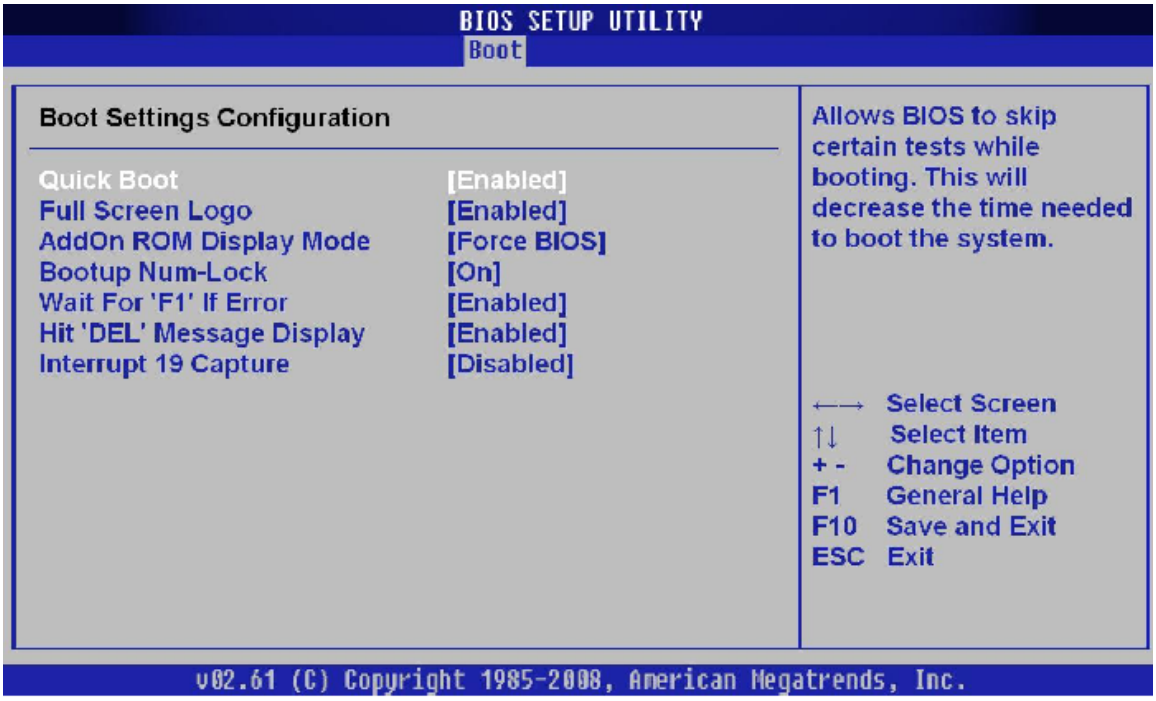

Рис. 8.15. Boot Setting Configuration

Wait For ’F1’ If Error – включення цього параметру, змусить користувача натиснути клавішу “F1”, якщо на початковій стадії завантаження ПК виявиться помилка.

Hit ’DEL’ Message Display – параметр, який керує появою на екрані напису, яку клавішу слід натиснути, щоб відкрити вікно налаштувань BIOS.

Елемент меню Security Setting (рис. 8.16) – налаштування захисту.

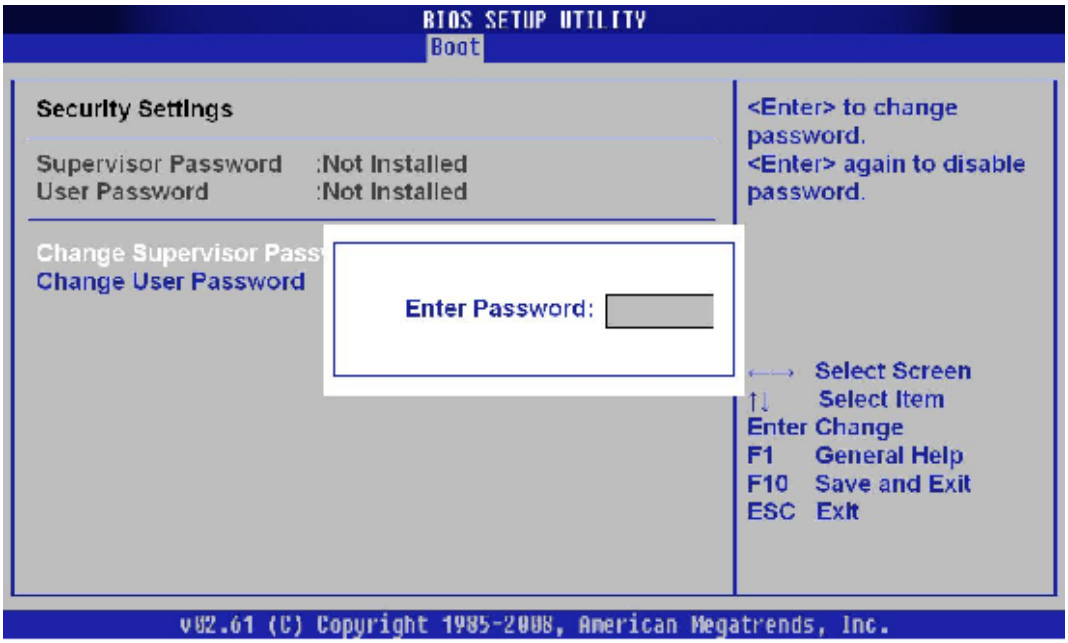

Рис. 8.16. Security Setting

Supervisor Password – даний параметр дозволяє змінити, видалити, або задати новий пароль адміністратора для доступу в BIOS.

User Password – даний параметр дозволяє змінити, встановити або видалити пароль користувача.

Розділ Tools (рис. 8.17)

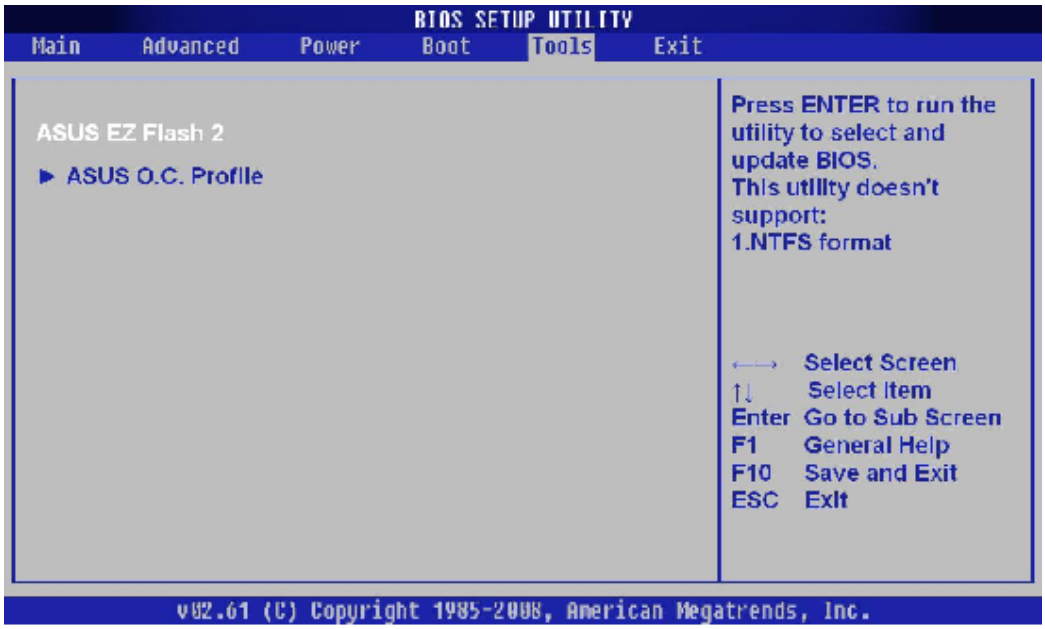

Рис. 8.17. Розділ Tools

Елемент меню ASUS EZ Flash – за допомогою даного елементу, у користувача є можливість оновлювати BIOS з таких накопичувачів як: дискета, USB-пристрою або компакт-диск.

Розділ Exit (рис. 8.18)

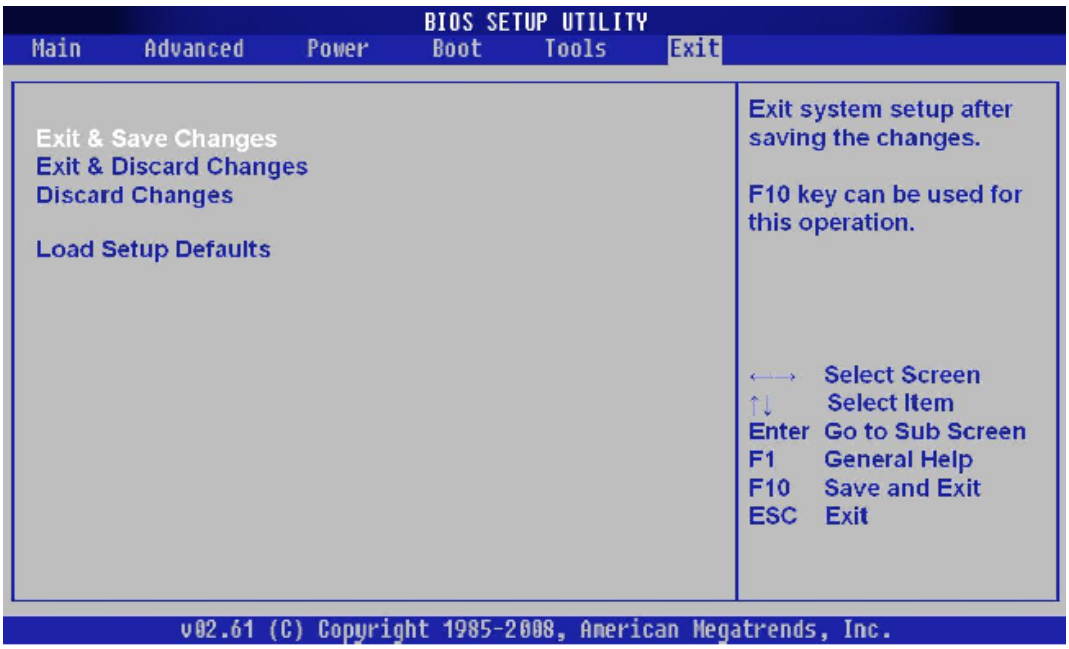

Рис. 8.18. Розділ Exit

Exit & Save Changes (F10) – використовується, щоб вийти з BIOS із збереженням всіх внесених змін.

Exit & Discard Changes – вихід з відміною всіх внесених змін.

Discard Changes – відміна всіх внесених змін.

Load Setup Defaults – встановлення параметрів за замовчанням.

Контрольні запитання:

1. Які параметри включені в елемент **PCI PnP**?
2. Які основні правила **BIOSy**?
3. В яких випадках слід скористатися елементом **CPU Configuration**?
4. На що впливає зміна параметрів **DRAM Timing Control**?
5. Чим відрізняються елементи **Supervisor Password і User Password**?

ЛАБОРАТОРНА РОБОТА № 9

Тема: Класифікація та способи встановлення операційних систем. Вимоги апаратного забезпечення до різних ОС. Типи файлових систем

Мета роботи: ознайомити студентів із різновидами сучасних операційних систем та навчити їх співвідносити апаратну частину ПК до різних операційних систем.

Порядок виконання роботи:

1. Підібрати операційні системи (Windows, Linux) в залежності від конфігурації запропонованого ПК.
2. Встановити обидві операційні системи створивши Boot Maneger.
3. Провести порівняльний аналіз швидкодії встановлених операційних систем.
4. Результати виконання роботи оформити у звіт.
5. У звіті дайте письмові відповіді на контрольні запитання.

Теоретичні відомості

Операційні системи (ОС) займають важливіше місце в сукупності сучасних системних програмних засобів, які складають програмне забезпечення ПК. Вони є основою організації обчислювального процесу в обчислювальній системі та визначають ефективність як використання апаратних компонентів системи, так і розв’язання поставлених задач. Від них залежить також ефективність праці користувачів.

В літературі можна зустріти різні визначення поняття “операційна система”.

Найбільш поширеним є ***визначення операційної системи як набору програм, призначених для управління ресурсами обчислювальної системи***.

Іноді під призначенням ОС мають на увазі розподіл та планування ресурсів, або динамічний і статичний розподіл ресурсів. Таким чином, на перший план виходить проблема розподілу ресурсів.

При цьому під ресурсами розуміють не тільки традиційні види ресурсів, такі як: час роботи окремих пристроїв, адресний простір різних рівнів, функції окремих пристроїв, набори даних, але і: окремі програми і програмні комплекси, які припускають сумісне використання. Це визначення базується на деякій моделі обчислювального процесу, у якому паралельно діє декілька учасників (задач, процесів, користувачів та ін.), які конкурують та змагаються за ресурси.

Підвищення надійності функціонування обчислювальної системи як одна з функцій ОС має на увазі наявність засобів забезпечення достовірності отриманих результатів, зменшення впливу збоїв та відмов апаратури, зменшення часу поновлення працездатності після збоїв та відмов, а також наявність засобів для створення контрольних точок та повторення розрахунків після збоїв з контрольної точки, засобів резервування даних, програм, процесів.

Особлива увага приділяється функціям ОС із забезпечення різних режимів використання обчислювальної системи – режиму пакетної обробки. Діалогових режимів, режиму реального часу, режиму розподілу часу, а також важливим функціям із забезпечення різних категорій користувачів обчислювальних систем.

Більшість розповсюджених визначень ОС відрізняються акцентами на ті, або інші властивості ОС, і як правило характеризуються їхньою комбінацією. Найбільш повним визначенням ОС варто визнати сукупність перерахованих вище характеристик.

Операційна система – це складний багатоцільовий та багатофункціональний комплекс програм, який є складовою частиною практично усіх сучасних обчислювальних систем.

При вивченні проблем розробки ОС виділяється ще один їх бік.

Операційна система є посередником між ПК, з однієї сторони, та людиною – з іншої. Іншими словами, операційна система – логічне розширення функцій апаратури у бік людини. Вона дозволяє від „фізичного” рівня апаратури перейти до більш високого „логічного” рівня, який стає рівнем обчислювальної системи і який є більш зручним для людини.

Склад та функції операційних систем

Компонентний склад ОС визначається набором функцій, для виконання яких вона призначена. Усі її програми можна поділити на дві групи: керуюча програма та системні обробляючі програми.

1. **Керуюча програма** – обов’язковий компонент будь-якої ОС. Її функції – планування проходження безперервного потоку завдань, управління розподілом ресурсів, реалізація прийнятих методів організації даних, управління операціями введення/виведення, організація мультипрограмної роботи, управління працездатністю системи після збоїв та інші.

Керуюча програма складається з ряду компонентів, серед яких слід виділити чотири основних:

- управління статичними ресурсами (управління завданнями);
- управління динамічними ресурсами (управління задачами);
- управління даними;
- управління поновленням.

Управління статичними ресурсами (управління завданнями) виконує попереднє планування потоку завдань для виконання і статичний розподіл ресурсів між завданнями, що одночасно виконуються у процесі підготовки до виконання. До таких ресурсів відносяться розподіл пам’яті (основної, віртуальної, зовнішньої), доступні для використання завданням пристрої, які припускають тільки монопольне використання, набори даних та інші. Такі ресурси закріплюються за завданням або його частиною з моменту його ініціалізації до моменту завершення та використовуються у монопольному режимі.

Управління динамічними ресурсами (управління задачами) виконує динамічний розподіл ресурсів системи між декількома задачами, які вирішуються одночасно, у мультипрограмному

режимі. Ці функції виконують програми супервізора, які входять до ядра ОС, що постійно знаходиться в оперативній пам'яті.

Управління даними забезпечує всі операції введення/виведення (обміну між оперативною пам'яттю та периферійними пристроями) на фізичному та логічному рівнях. Воно містить у собі ряд служб, які забезпечують виконання таких функцій, як управління каталогом, управління розподілом пам'яті прямого доступу, обробки помилок введення/виведення та інше. Вони реалізують різні структури даних та можливість доступу до них.

Управління поновленням реєструє машинні збої та відмови, і поновлює працездатність системи після збоїв, якщо це можливо.

2. **Системні обробляючи програми** виконуються під управлінням керуючої програми, так саме, як і будь-яка обробляюча програма. Це значить, що вона у повному обсязі може користуватися послугами керуючої програми і не може самостійно виконувати системні функції. Так, наприклад, обробляюча програма не може самостійно виконувати власне введення/виведення. Ці операції обробляюча програма реалізує за допомогою запитів до керуючої програми, яка їх безпосередньо виконує. Централізоване виконання системних функцій керуючою програмою дозволяє виконувати їх більш ефективно та забезпечує високий рівень послуг для користувача.

До системних обробляючих програм відносяться програми, які входять у склад ОС: асемблери, транслятори, редактори зв'язків, програми обслуговування та інші.

Призначення операційних система

На IBM-сумісних персональних комп'ютерах використовуються операційні системи Windows розроблені корпорацією Microsoft, вільно розповсюджувана операційна система Linux. На персональних комп'ютерах фірми Apple використовуються різні версії операційної системи Mac OS. На робочих станціях і серверах найбільше поширення отримали операційні системи Windows Server і UNIX.

Сучасні операційні системи мають складну структуру, кожний елемент якої виконує певні функції з керування комп'ютером.

Керування файловою системою. Процес роботи комп'ютера в певному змісті зводиться до обміну файлами між пристроями. В операційній системі є *програмні модулі, що управляють файловою системою.*

Командний процесор. До складу операційної системи входить спеціальна програма – командний процесор, яка запитує в користувача команди й виконує їх.

Користувач може дати команду запуску програми, виконання якої-небудь операції над файлами (копіювання, видалення, перейменування), виведення документа на друк і так далі. Операційна система повинна цю команду виконати.

Графічний інтерфейс. Для спрощення роботи користувача до складу сучасних операційних систем, і зокрема до складу Windows, входять *програмні модулі, що створюють графічний користувацький інтерфейс.* В операційних системах із графічним інтерфейсом користувач може вводити команди за допомогою миші, тоді як у режимі командного рядка необхідно вводити команди за допомогою клавіатури.

Сервісні програми. До складу операційної системи входять також *сервісні програми,* або *утиліти.* Такі програми дозволяють виконувати різноманітні сервісні функції з апаратною частиною ПК та інформацією, що зберігається.

Довідкова система. Для зручності користувача до складу операційної системи звичайно входить також *довідкова система.* Яка дозволяє оперативно отримати необхідну інформацію як про функціонування операційної системи в цілому, так і про роботу її окремих модулів.

Існує кілька схем класифікації операційних систем. Нижче наведена класифікація за деякими ознаками з погляду користувача:

1. Кількості одночасно працюючих користувачів – однокористувацькі та багатокористувацькі. Багатокористувацькі на відміну від однокористувацьких підтримують одночасну роботу декількох користувачів з різними терміналами.

2. Числу процесів, які одночасно можуть виконуватися під керуванням даної системи – однозадачні та багатозадачні. Поняття

багатозадачності означає підтримку паралельного виконання кількох задач, які існують в межах однієї обчислювальної системи в один момент часу. Однозадачні підтримують режим виконання лише одної програми в один момент часу.

3. Кількості підтримуючих процесорів – однопроцесорні та багатопроцесорні. Багатопроцесорні операційні системи підтримують режим розподілених ресурсів декількох процесорів для розв'язання однієї задачі.

4. Розрядності коду – 32-ох розрядні та 64-ох розрядні (вважається, що розрядність операційної системи не може перевищувати розрядність процесора).

5. Типу інтерфейсу – командні (з текстовим інтерфейсом) і об'єктно-орієнтовані (з графічним інтерфейсом).

6. Типу доступу користувача до обчислювальної системи: з пакетною обробкою, з розділенням часу, реального часу. В режимі пакетної обробки з виконуваних програм формується пакет (набір) завдань, які вводяться в систему і виконуються в послідовності чередування з можливим урахуванням пріоритетів. У режимі розділення часу кожній задачі почергово виділяється певний проміжок часу на виконання з імітуванням перед користувачами одночасного виконання всіх завдань. Режим реального часу забезпечує імітацію одноосібного обслуговування користувача в темпі розвитку реального процесу.

7. Типу використання ресурсів – мережеві та локальні. Локальна операційна система забезпечує роботу тільки одного користувача, в той час як мережева – дозволяє одночасно працювати багатьом незалежним користувачам в мережі, використовуючи спільні ресурси. Тобто мережеві операційні системи забезпечують обслуговування користувачів локальних обчислювальних мереж.

Основні критерії підходу до вибору операційної системи

Перед користувачем стоїть завдання визначити, яка операційна система краща за інших (за тими або іншими критеріями). Як відомо, що ідеальних систем не буває, будь-яка з них має свої переваги і недоліки. Обираючи операційну систему, користувач

повинен представляти, наскільки та або інша ОС забезпечить йому рішення його завдань. Щоб вибрати ту або іншу ОС, необхідно знати:

1. На яких апаратних платформах і з якою швидкістю працює ОС.
2. Яке периферійне апаратне забезпечення ОС підтримує.
3. Як повно задовольняє ОС потребам користувача, тобто які функції системи.
4. Який спосіб взаємодії ОС з користувачем, тобто наскільки наочний, зручний, зрозумілий і звичний користувачеві інтерфейс.
5. Чи існують інформативні підказки, вбудовані довідники і т. д.
6. Яка надійність системи, тобто її стійкість до помилок користувача, відмов устаткування і т. д.
7. Які можливості надає ОС для організації мереж.
8. Чи забезпечує ОС сумісність з іншими операційними системами.
9. Які інструментальні засоби має ОС для розробки прикладних програм.
10. Чи здійснюється в ОС підтримка різних національних мов.
11. Які відомі пакети прикладних програм можна використовувати при роботі з цією системою.
12. Як здійснюється в ОС захист інформації і самої системи.

Будь-яка ОС постійно модифікується, що може призвести до часткової несумісності з конкретними апаратними засобами. Для уникнення цієї несумісності перед встановленням тієї чи іншої версії ОС необхідно з’ясувати мінімальні апаратні вимоги самої ОС. Інакше це може призвести до серйозного уповільнення, або взагалі непрацездатності роботи ПК.

У більшості випадків при переході з однієї на іншу версію ОС виникають проблеми із спеціалізованими програмними засобами, які реалізують процес керування різноманітними апаратними устаткуваннями **(драйвери**).

Драйвери зазвичай розробляються не постачальниками операційної системи, а сторонніми фірмами – розробниками і виробниками периферійного устаткування. Проблема тут в тому,

що інтерфейс між драйвером і ядром ОС завжди двосторонній: не лише прикладні програми і ядро викликають функції драйвера, але і, навпаки, драйвер повинен викликати функції ядра. Структура інтерфейсів ядра, доступних драйверу, визначає багато аспектів архітектури ОС в цілому.

Тому інтерфейс драйвера є анітрохи не менш зовнішнім, ніж те, що зазвичай вважається зовнішнім інтерфейсом ОС – інтерфейс системних викликів. Відповідно, до нього пред'являються ті ж вимоги, що і до будь-якого іншого зовнішнього інтерфейсу: він повинен бути зрозумілим, виключно документованим і стабільним – змінюватися в залежності від однієї версії ОС до іншої. Ідеальним варіантом була б повна сумісність драйверів хоч би від низу до верху, аби драйвер попередньої версії ОС міг використовуватися зі всіма подальшими версіями.

Втрата сумісності в даному випадку означає, що всі незалежні виробники устаткування повинні будуть відновити свої драйвери. Організація такого оновлення виявляється складною, невдячною і часто просто нездійсненним завданням – наприклад, виробник устаткування вже не існує як організація, або відмовився від підтримки даного пристрою.

Типи файлових систем

Створюючи та копіюючи файли, ви за допомогою доволі простих команд операційної системи розміщуєте їх у певні папки, створені на визначеному диску вашого комп'ютера. Проте що відбувається при цьому насправді, не бачить жоден користувач персонального комп'ютера. Цей процес зберігання даних організує *файлова система – частина будь-якої операційної системи, що відповідає за організацію зберігання та доступ до даних на будь-яких її носіях.*

Розглянемо як приклад файлові системи жорстких магнітних дисків, адже саме на них зберігається основні масиви даних у комп'ютері.

Робочі поверхні пластин на логічному рівні поділені на кільцеві концентричні доріжки (треки), а доріжки – на сектори (сектор зберігає мінімальний обсяг даних, який можна записати на диск) (рис. 9.1).

Рис. 9.1. Поверхня магнітного диску

Зчитуючи/записуючі голівки та диски розміщено в герметично закритому корпусі. Пластини накопичувача обертаються постійно з великою швидкістю (від 4200 до 15 000 обертів за хвилину), тому над ним утворюється повітряний шар, що забезпечує зависання магнітної голівки на висоті 5-10 нм над поверхнею диска.

Сам пристрій може виконувати лише команди зчитування/запису даних в певний сектор на диску.

Користувач же хоче записати на диск або зчитати з нього певні файли, розмістивши їх у попередньо створених папках різного рівня. Тому саме файлова система має визначити, як виконати ці операції на фізичному рівні.

Файлова система включає:

- сукупність усіх файлів на диску;
- набори службових структур даних, що їх використовують для керування файлами (такими структурами є папки, таблиці розподілу вільного та зайнятого дискового простору);
- комплекс системних програмних засобів, що реалізують керування файлами (операціями створювання, зчитування, записування, змінювання назви, рівнів доступу, пошуку тощо).

Різні файлові системи відрізняються переважно способами розподілу дискового простору між файлами накопичувача та організацією на диску службових областей. Сучасні операційні системи забезпечують користувачеві можливість працювати одночасно з кількома файловими системами, кожна з яких забезпечує ефективний доступ до файлів, підтримку носіїв достатньо великого обсягу, захист від несанкціонованого доступу

до даних і збереження їх цілісності. Проте кожна файлова система має свої переваги та недоліки.

Розглянемо основні файлові системи:

1. Файлова система FAT (File Allocation Table)

Цю систему розробили Білл Гейтс та Марк МакДональд у 1977 р. для використання в ОС *86-DOS.* FAT було призначено для роботи з гнучкими дисками обсягом не більше 1 Мбайт. Спочатку вона не підтримувала роботу з жорсткими дисками. На сьогодні ця файлова система організує роботу з файлами обсягом до 2 Гбайт.

Файлова системи FAT *використовує такі* домовленості щодо назв файлів:

- Назву (ім'я) файлу має починати буква або цифра, вона може містити будь-який символ, за винятком пропуску та таких спеціальних символів: " /\ [ ] : ; | = , " * ?
- Довжина імені файлу не може перевищувати *вісім символів,* за якими ставиться крапка та необов'язкове розширення завдовжки до трьох символів.
- Регістр символів у назвах файлів не розрізняється та не зберігається (файлова система не розрізняє великі та малі літери).

Файлова система *FAT* не може контролювати окремо кожен сектор жорсткого диска. Тому вона поєднує сусідні сектори в *кластери,* розмір яких визначають під час початкового розмічання(форматування) накопичувача. Цей розмір має бути ступенем числа 2. *Кластер є тим мінімальним простором, який може займати файл.* Це призводить до того, що частина дискового простору витрачається марно. Наприклад, якщо ми зберігаємо файл розміром 4 Кбайт, а розмір кластера становить 8 Кбайт, то половина обсягу кластера залишається вільною. Однак його все ж неможливо використати для записування інших даних.

Ця файлова система завжди заповнює вільне місце на диску послідовно від початку до кінця. Для створення нового файлу або збільшення вже наявного *FAT* шукає в спеціальній таблиці розміщення файлів перший вільний кластер, до якого і записує дані. Якщо в процесі роботи одні файли буде вилучено, а інші змінено в розмірі, то з'являться порожні кластери, розсіяні по

всьому диску. Якщо кластери, що містять один файл, розміщено не поруч, то файл буде *фрагментованим.* Наявність таких фрагментованих файлів суттєво знижує ефективність роботи, оскільки голівки зчитування/запису, шукаючи черговий кластер з наступним фрагментом файлу, повинні рухатися від однієї ділянки жорсткого диска до іншої.

Ще один недолік файлової системи *FAT* полягає в тому, що її продуктивність суттєво залежить від кількості файлів в одній папці. Якщо папка містить близько тисячі файлів, то операція зчитування списку файлів у каталозі може тривати декілька хвилин. Це пов'язано з тим, що *FAT* каталог має лінійну невпорядковану структуру, а назви файлів у папках розміщено в порядку їх створювання.

Цю файлову систему проектували для використання в операційній системі, розрахованій на роботу лише одного користувача. Через це вона не передбачає зберігання інформації про власника файлу або повноважень доступу до файлу чи папки.

2. Файлова система NTFS (New Technology File System)

Цю файлову систему створили для застосування в операційній системі *Windows*. Вона дає змогу використовувати *довгі назви файлів, що підпорядковуються таким правилам:*

1. Назва файлу може мати до 255 символів.
2. До імені можна включати кілька символів пропуску та крапок, проте текст після останньої крапки є розширенням.
3. Регістр символів не розрізняється, однак зберігається.
4. Для сумісності з файловою системою *FAT* система *NTFS* самостійно *генерує* з цих довгих назв *короткі за такими правилами:*

а. із довгої назви видаляє всі символи, що не можуть входити до назви в системі *FAT*. Із імені видаляє всі крапки, розміщені на початку, у кінці та в середині назви, крім останньої;

б. назву файлу до крапки обрізає до шести символів, у кінець назви додає ~1. До трьох символів обрізає розширення, розміщене за крапкою;

в. отримані літери перетворює на великі. Якщо створена таким чином коротка назва файлу вже існує, то збільшує число в рядку ~1.

5. Файлова система *NTFS* дає змогу зберігати файли розміром 16 Тбайт (244 байт) та містить убудований засіб стиснення файлів у реальному часі. Для зменшення фрагментації ця система завжди намагається зберігати файли в суцільних блоках, використовуючи для їх пошуку структуру каталогів у формі дерева. Завдяки такому впорядкуванню пошук файлів у папках відбувається достатньо швидко.

Систему *NTFS* було розроблено *як файлову систему, здатну відновлюватися.* Кожну операцію введення/виведення, що змінює файл, система розглядає як неподільний блок. Після зміни файлу система фіксує всю інформацію, потрібну для повторення або відмови від цієї операції. Якщо операція закінчилася вдало, файлова система фіксує зміну файлу. В іншому випадку система *NTFS* дає змогу відмовитися від виконання операції.

Зазначену файлову систему розробляли для використання в багатокористувацькій операційній системі. Тому вона зберігає певні атрибути (властивості) файлів, що *дають змогу обмежувати доступ до файлів та папок різних користувачів.* Нові версії файлової системи *NTFS* дозволяють заборонити доступ до певних файлів або заборонити змінювати їх вміст. Вони мають можливість обмежити розмір дискового простору, що надається різним користувачам, подавати будь-яку папку (і на локальному, і на віддаленому комп’ютері) як вкладену папку локального комп’ютера. У цих версіях файлової системи з’явилася можливість динамічно шифрувати файли та папки, що підвищує надійність зберігання інформації.

3. **Файлова система для ядра Linux**. **ext2** або 2-га розширена файлова система. Розроблена Rémy Card’ом як заміна для extended file system. Вона достатньо швидка для того, щоб бути використаною в якості еталону в тестах продуктивності файлових систем. Вона не є журнальованою файловою системою, і це її

основний недолік. Розвитком ext2 стала журнальована файлова система ext3, повністю сумісна з ext2.

4. **Файлові системи HFS і HFS+ –** основні файлові системи для операційних систем Apple MacOS. Однією з основних переваг є висока швидкість доступу до файлів та папок, а також низька ступінь фрагментації файлів.

Крім розглянутих, на сьогодні використовують такі файлові системи:

- Для носіїв з довільним доступом (наприклад, жорсткий диск): FAT32, HPFS, ext2 та інші. Останнім часом поширилися журнальовані файлові системи, такі як ext3, Reiserfs, JFS, NTFS, XFS.
- Для носіїв з послідовним доступом (наприклад, магнітні стрічки): QIC.
- Для оптичних носіїв – CD і DVD: ISO 9660, HFS, UDF.
- Віртуальні файлові системи: AEFS та інші.
- Мережеві файлові системи: NFS, SMBFS, SSHFS, Gmailfs.

Розвиток файлових систем персональних комп'ютерів визначили два чинники. По-перше, це поява нових стандартів на носії інформації, по-друге, зростання вимог до характеристик файлової системи з боку прикладного програмного забезпечення (розмежування рівнів доступу різних користувачів, підтримка довгих назв файлів тощо). Спочатку головною вимогою до розроблених файлових систем було підвищення швидкості доступу до даних та зменшення обсягу службової інформації, що її використовує файлова система. Постійний розвиток інформаційних технологій виводить на перший план вимоги надійності зберігання інформації, що призводить до необхідності зберігати надлишкові обсяги даних. Тому подальша еволюція файлових систем іде шляхом удосконалення механізмів зберігання даних, мультимедійних даних, використання нових технологій роботи з інформацією (можливість повнотекстового пошуку, сортування файлів за різними атрибутами тощо).

Контрольні запитання:

1. З яких основних частин складається будь-яка операційна система?
2. Які основні відмінності між багатокористувацькою та мережевою операційними системами?
3. Що таке файлова система? Які елементи вона включає?
4. Чим розрізняються різні файлові системи?
5. За якими правилами формують назви файлів у найпоширеніших файлових системах?

ЛАБОРАТОРНА РОБОТА № 10

Тема: Поняття драйверу. Відповідність драйверів до різних ОС. Пошук, встановлення та оновлення драйверів для всіх необхідних пристроїв

Мета роботи: ознайомити студентів із загальним поняттям драйверу та основними правилами їх встановлення або оновлення.

Порядок виконання роботи:

1. Після встановлення операційних систем (лабораторна робота № 9) перевірити наявність автоматичного визначення та встановлення драйверів пристроїв (звук, відео, мережева карта та інші).
2. У разі необхідності на сайті виробника материнської плати знайти драйвери у відповідності до встановлених ОС.
3. Встановити знайдені драйвери та перевірити їх працездатність.
4. У разі некоректності встановлених драйверів повторити операцію пошуку, використовуючи інші Інтернет ресурси (наприклад drivers.ru).
5. Результати виконання роботи оформити у звіт.
6. У звіті дайте письмові відповіді на контрольні запитання.

Теоретичні відомості

Драйвер – програма, що розширює можливості операційної системи.

Драйвер пристрою – програма операційної системи для керування роботою периферійними пристроями: дисководами, монітором, клавіатурою, принтером, маніпулятором “миші” та ін.

Драйвер пристрою повинен враховувати специфіку роботи зовнішнього приладу, усі тонкощі його функціонування. У зв'язку з цим кожному приладу повинен відповідати свій драйвер.

Функції драйвера пристрою складаються в наступному:

- прийняття та обробка запиту (керуючого сигналу), що надходить до даного периферійного пристрою;
- перетворення запиту про необхідність зв'язку з цим пристроєм у серію команд керування ним, з урахуванням усіх деталей конструкції та особливостей його роботи;
- обробка сигналу переривання, який надходить від відповідного цьому драйвера периферійного пристрою.

Драйверами також вважаються програми, які забезпечують керування розширеної пам'яті, а також створення і обслуговування віртуальних пристроїв, наприклад електронного диска в оперативній пам'яті.

Драйвери можуть бути або стандартні, або завантажувальними.

Стандартні (внутрішні) драйвери – це програми, які знаходяться усередині BIOS або його модуля розширення EMBIOS служать для керування зовнішніми пристроями, що входять до стандартного комплекту персонального комп'ютера. Ці драйвери підключаються до системи автоматично після переходу комп'ютера в нормальне робоче становище.

Завантажувальні (зовнішні, встановлювані) драйвери – це програми, що зберігаються на диску і призначені для керування зовнішніми пристроями, які відрізняються від стандартних за своїми технічними властивостями, або особливими режимами використання. Можливість використання завантажувальних драйверів полегшує адаптацію операційної системи до нових зовнішніх пристроїв.

Пошук, встановлення та налаштування драйверів для всіх необхідних пристроїв

Як правило, до кожного пристрою додається компакт-диск (CD, DVD, mini-CD), на якому міститься драйвер і обслуговуючі програми.

Для зменшення ймовірності непрацездатності з вини драйверів слід дотримуватися наступних рекомендацій:

- обирайте продукцію тільки відомих виробників (“брендів”). Найчастіше виробники, які потрапляють в категорію “noname”, звертають мало уваги на написання якісних драйверів, хоч це зовсім не означає, що драйвери від “noname” обов’язково будуть працювати нестабільно. Тут мова йде про статистику, яка, загалом-то, може виявитися необ’єктивною;
- враховуйте апаратну сумісність з будь-якою операційною системою, читайте огляди та статті, присвячені даній моделі, щоб дізнатися думку незалежних фахівців, або навіть просто користувачів;
- не поспішайте скачувати з Інтернету оновлені драйвери, спочатку уважно вивчіть, які зміни до них були внесені. Може так статися, що вони не мають жодних серйозних нововведень, зате при оновленні можна придбати цілий ряд недотягнутих модулів, що приводять до збоїв у роботі комп’ютера.

Варто відзначити, що драйвери розповсюджуються в двох варіантах. Перший варіант являє собою єдиний файл з розширенням **.EXE**, або набір файлів де файлом інсталяції є файл **Setup.exe,** при запуску яких автоматично здійснюються всі необхідні дії: копіювання файлів, створення ярликів і посилань в реєстрі. Другий варіант являє собою набір файлів, необхідних для роботи пристрою та файли з розширенням **.INF**, де прописаний алгоритм дій, необхідних для успішного встановлення драйвера.

У цьому випадку встановленням драйвера “завідує” операційна система. При цьому вам слід при запиті на встановлення драйвера пристрою вказати ім’я диску та папку, в якому знаходиться потрібний для його роботи драйвер, після чого, згідно з наявним INF-файлу, операційна система здійснить необхідні дії. Природно, що папка з драйвером повинна бути доступною протягом усього процесу інсталяції (встановлення).

Драйвери випускаються окремо для кожної версії операційної системи, що іноді ускладнює перехід з однієї версії на іншу, тому для нової версії ОС просто може не виявитися потрібного драйвера.

Доволі часто можна зустріти пакети драйверів, які призначені для роботи у всіх версіях Windows, або пакети, що містять драйвери не тільки для будь-яких версій Windows, але і для інших ОС.

Зверніть увагу, що драйвери для всіх пристроїв найкраще встановлювати ще до початку налаштування операційної системи і до встановлення прикладного програмного забезпечення.

Крім того, не рекомендується вимикати старе обладнання до повного завершення роботи комп'ютера, тому що це може викликати зависання операційної системи. Адже операційна система під час своєї роботи може подати запит готовності пристрою.

Контрольні запитання:

1. Які функції виконує драйвер в ОС?
2. Назвіть основні варіанти пакетів драйверів.
3. Як перевірити наявність необхідних драйверів в ОС Linux?
4. Як називається драйвер в ОС Mac OSX?
5. В яких випадках необхідно виконувати оновлення драйверу?

ЛАБОРАТОРНА РОБОТА № 11

Тема: Класифікація програмного забезпечення ПК. Встановлення і видалення прикладних програм

Мета роботи: ознайомити студентів із класифікацією програмного забезпечення та встановлення і видалення прикладних програм

Порядок виконання роботи:

1. Підібрати пакет програмних засобів різного типу необхідний для: роботи з документами та створення мультимедійних презентацій.
2. Забезпечити можливість архівування та розархівування файлів.
3. Забезпечити альтернативну навігацію по файловій структурі.
4. Розробки HTML-сторінки.
5. Можливості перегляду відеофайлів.
6. Забезпечення можливості проведення відеоконференцій.
7. Результати виконання роботи оформити у звіт.
8. У звіті дайте письмові відповіді на контрольні запитання.

Теоретичні відомості

Програма – це послідовність команд, яку виконує комп’ютер в процесі обробки даних.

Всі програми зберігаються у зовнішній та внутрішній постійній пам’яті. Але для того, щоб комп’ютер міг виконати ту чи іншу програму, вона має завантажитися в оперативну пам’ять і власне з нею працює процесор.

Всі програми, що містяться у комп’ютері називаються програмним забезпеченням або програмною конфігурацією цього комп’ютера.

Програмне забезпечення комп'ютера можна розподілити за рівнями:

1. Базовий рівень.
2. Системний рівень.
3. Службовий рівень.
4. Прикладний рівень.

Програми базового рівня

Базовий рівень є найнижчим рівнем, що відповідає за взаємодію з базовим апаратним забезпеченням.

Програми цього рівня містяться у мікросхемах постійного та енергонезалежного запам'ятовуючих пристроїв, і вони називаються програмами BIOS (див. лаб. роб. № 8).

Програми системного рівня

Системний рівень є важливою складовою програмного забезпечення будь якого комп'ютера. Без цих програм неможливо взаємодіяти з жодним пристроєм комп'ютерної системи. Власне програми системного рівня керують узгодженою роботою всіх елементів системи як апаратного так і програмного забезпечення.

Системні програми зазвичай орієнтовані на кваліфікованих користувачів – фахівців в комп'ютерній галузі: системних програмістів, адміністраторів тощо. Однак, знання роботи з системними програмами потрібні і звичайному користувачу, який мусить самостійно доглядати та налаштовувати свою комп'ютерну систему.

До програм системного рівня відносять:

- **Операційні системи** – це комплекс програм, які здійснюють діалог з користувачем, забезпечують керування ресурсами комп'ютера, запускають інші програми на виконання.
- **Інтерфейсні оболонки** – виконують посередницькі функції забезпечують ефективну взаємодію користувача та комп'ютера.
- **Графічний інтерфейс користувача** – це зручна система спілкування людини з комп'ютером за визначеними стандартами, що містять:
  - Систему меню.
  - Систему вікон для роботи з документами.

- Панелі інструментів.
- Шаблони форм документів та екранних форм.

Операційні системи постійно вдосконалюють і реалізовують “дружні” до користувача інтерфейси.

- **Драйвери –** це спеціальні програми для керування зовнішніми пристроями.
- **Системні утиліти –** здійснюють перевірку працездатності основних пристроїв комп’ютера, виправлення помилок та оптимізація роботи пристроїв.

Програми службового рівня

Програми службового рівня збагачують можливості системних програм і надають користувачеві зручний інструментарій для перевірки та налаштування комп’ютерної системи.

Зазвичай, програми службового рівня називають утилітами і вони можуть відразу міститися серед програм операційної системи або додатково доставлені.

До програм службового рівня відносяться:

. Файлові менеджери (провідники, диспетчери). Це “Мой компьютер”, Total Commander, Windows Commander. Ці програми забезпечують роботу з файловою структурою:

- Навігація по файловій структурі.
- Пошук файлів та папок (об’єктів файлової системи).
- Створення об’єктів.
- Копіювання об’єктів.
- Встановлення об’єктів.
- Перейменування об’єктів тощо.

Програми обслуговування дисків здійснюють перевірку якості поверхні жорсткого диску, контроль цілісності файлової системи, оптимізацію розміщення даних на носіях інформації.

Програми інсталяції/деінсталяції. Для того, щоб додати до комп’ютера нової програми, переважна їх більшість потребує програмного встановлення (інсталяції). Це, насамперед, потрібно для коректної роботи програми в існуючому програмному середовищі, можливість користуватися стандартними засобами для введення чи виведення інформації та узгодженої взаємодії з іншими

програмами.

Для видалення програми її слід деінсталювати, щоб коректно видалити всі зв'язки програми у програмному середовищі, які утворюються під час інсталяції.

Програми-пакувальники (архіватори) призначені для пакування та розпаковування файлів з метою зменшення їх розмірів. Упакований файл називається архівом, а процедури пакування/розпаковування, відповідно архівуванням/розархівуванням.

Архів – це копія файлу, де дані за певними алгоритмами перезаписуються в більш компактній формі. Файл-архів, зазвичай, має значно менший розмір ніж файл-оригінал. Файл-архів може містити в собі як один файл так і кілька файлів чи папок з файлами.

Для подальшого використання файл-архів обов'язково слід розпакувати, щоб отримати файл-оригінал, і працювати з ним в звичний спосіб.

Зазвичай, архіви створюють для:

- Тривалого збереження важливих документів.
- Пересилання документів засобами електронної пошти.
- Записування документів на носій інформації, що має невеликий обсяг вільного простору.

Сучасні архіватори є сумісними між собою і підтримують основні формати архівів – **.zip** та **.rar**.

Антивірусні програми призначені для виявлення та знищення комп'ютерних вірусів.

Програми прикладного рівня

Програми прикладного рівня призначені для вирішення конкретних практичних задач користувача в різних сферах людської діяльності.

Прикладні програми не містяться у складі операційної системи, їх розробкою займаються різні компанії, тому користувач має докупити потрібну програму та інсталювати її самостійно.

Асортимент прикладних програм є величезним, але їх можна умовно поділити на:

1. Програми загального призначення.
2. Програми спеціалізованого призначення.

3. Інструментарій для програмування.

Прикладні програми загального призначення

Офісні програми (комплект програм у пакеті MS Office)

Текстовий редактор Word. Програма для створення, редагування та оформлення текстових документів. Word має зручні інструменти для додавання до тексту таблиць, зображень, фотографій та мультимедійних об'єктів.

Табличний процесор Excel. Програма для статичної або математичної обробки великих об'ємів даних типів, що представлені у табличній формі. Зазвичай, це числові дані. Інтерфейс має зручні інструменти для наочної візуалізації результатів обробки у вигляді підсумкових таблиць та двох чи трьох вимірних графіків різних типів.

Система управління базами даних СУБД Access. Програма для обробки та збереження великих об'ємів структурованої інформації, що представлена у вигляді окремих таблиць.

Основними функціями СУБД є швидкий пошук, сортування та інша обробка існуючих даних, легке введення нових даних, зручне виведення результатів обробки за вказаними ознаками.

Програма презентації Power Point. Програма для створення низки міні плакатів (слайдів) і показ їх на екрані монітору. Power Point має зручні інструменти для підготовки слайд-фільмів (презентацій), їх редагування, визначення порядку та режиму показів слайдів.

Графічні редактори

Це програми для створення та обробки зображень, так звані засоби комп'ютерної графіки. Графічні редактори поділяються за тим типом комп'ютерної графіки, яку вони спроможні обробляти.

Растрова графіка. Тут будь який об'єкт (лінія, текст, квітка, обличчя тощо) представлено у вигляді сукупності окремих точок-растрів, кожен з яких має свій колір. У файлі зберігається інформація про колір кожного растру та їх кількість. Такі файли зазвичай є великого об'єму.

Растрові редактори є ефективними для обробки фотографій або інших зображень, що мають багато різнобарвних ділянок.

Відомі програми: MS Paint, Adobe PhotoShop.

Векторна графіка. Тут будь який об'єкт (лінія, текст, прямокутник, овал тощо) представлено кривою III порядку, що обчислюється за математичною формулою. Властивості об'єкту – колір, розміри, місце розташування – також є коефіцієнтами формули, тому векторні елементи дуже легко змінювати. У файлі зберігаються формули відповідно до кожного об'єкту, тому файли зазвичай є невеликими за об'ємом, але потребують потужних характеристик комп'ютера, бо потрібно обчислювати складні формули. Ілюстрований характер, де присутні чітко окреслені ділянки, зафарбовані в мінімальну кількість кольорів.

Відомі програми: внутрішній графічний редактор з пакету MS Office, Corel Draw, Adobe Illustrator.

Анімаційна графіка. Програми анімаційної графіки призначені для створення мультфільмів, презентацій, роликів, веб-банерів, де присутній рух об'єктів.

Відомі програми: Adobe Flash, Image Ready.

Тривимірна графіка. Програми тривимірної графіки призначені для створення об'ємних композицій. Елементи тривимірної сцени створюються із базових об'єктів (кубів, сфер, циліндрів, ліній тощо), їм надають властивостей і зафарблення певних матеріалів (металу, пластику, тканини), а сама сцена оснащується кількома джерелами природного чи іншого освітлення.

Відомі програми: 3D Studio MAX, Maya.

Фрактальна (інженерна) графіка. Програми фрактальної графіки призначені для обробки великих масивів числової інформації і побудова на їх підставі різноманітних двох та трьох вимірних графіків.

Відомі програми: внутрішній редактор з пакету MS Office, Surfer.

Засоби перегляду та відтворення мультимедійних документів.

До них відносяться так звані програвачі та переглядачі-програми, що дозволяють прослуховувати музику, переглядати

відеофільми, анімаційні та тривимірні ролики.

Відомі програми: Winamp, Windows Media Player, SM Player, ShockWave Player, Quick Time, ACDSee.

Засоби електронної комунікації

Це програми, що надають доступ до різноманітних ресурсів Інтернету або локальної мережі.

Браузери – універсальні засоби перегляду веб-сторінок. Окрім відтворення тексту та зображень веб-сторінки, браузери можна застосувати для:

– відтворення різних мультимедійних об'єктів (музики, відео, анімації);

– використання електронної пошти;

– спілкування у конференціях-чатах;

– участі у мережевих іграх;

– здійснення покупки в Інтернет магазині;

– завантаження з віддалених комп'ютерів різноманітної документації;

– використання інших послуг Інтернету.

Відомі браузери: Internet Explorer, Opera, Mozilla FireFox, Google Chrome.

Поштові програми – зручні засоби для користування послугами електронної пошти.

Відомі програми: Outlook Express, The Bat!, Mozilla Thunderbird.

Програми для обміну повідомленнями. Самою популярною програмою є ICQ (скорочення від звучання фрази "I seek you"). Призначена для спілкування з одним чи кількома користувачами в інтерактивному режимі. Підтримує популярні web та e-mail застосування, тому через програму ICQ можна переходити за гіперпосиланнями, відкривати електронні листи, пересилати файли.

Програми IP-телефонії. Відомою програмою є Scype, яка надає можливість голосового та відео спілкування з іншими користувачами в будь якому куточку світу. Для повноцінного функціонування потрібно доукомплектувати комп'ютер навушниками/колонками, мікрофоном та веб-камерою. Scype може

працювати і в режимі текстових повідомлень, підтримує пересилання файлів та відкривання гіперпосилань.

Програми автоматизованого перекладу тексту

Електронні словники. Це потужний інструмент для точного перекладу слів або словосполучень. Безперечним лідером серед програм є ABBYY Lingvo. Програма підтримує 12 мов і містить понад 100 тематичних словників.

Словникові статті містять всі значення слова, транскрипцію, тлумачення, синоніми/антоніми, коментарі, форми та приклади застосування слів у реченнях.

Для користувачів, які вивчають іноземну мову мають можливість скористатися Lingvo Tutor – інтерактивною навчальною програмою запам'ятовування нових слів та перевірки ефективності опрацювання матеріалу. Учбові картки Lingvo Tutor містять приклади, транскрипцію, приклади і звуковий об'єкт правильної вимови слова.

Програми-перекладачі

Виконують переклад тексти з однієї мови на іншу. Програми-перекладачі варто застосовувати:

- При повному незнанні іноземної мови.
- Для швидкого ознайомлення з загальним змістом документа.
- Для створення чернетки з подальшим якісним перекладом людиною.

За останні роки спостерігається суттєве вдосконалення програм-перекладачів. Вони збільшують кількість мов, тематичних словників, після інсталяції втілюються у популярні офісні програми та Інтернет програми: браузери, поштові і чат-програми, щоб користувач міг легко почуватися у всесвітньому інформаційному просторі.

Звісно, що літературний текст буде перекладений недостатньо якісно, але для простих технічних чи побутових текстів якість є цілком сприйнятою.

Відомі програми: Prompt – підтримка 7 європейських мов (англійська, французька, німецька, італійська, іспанська, португальська, російська). Pragma – підтримка української,

російської, англійської та німецької мов.

Програми розпізнавання текстів

Це так звані системи оптичного розпізнавання символів OCR (Optical Character Recognition). Вони призначені для розпізнавання друкованого тексту зі сканованих чи фотографованих зображень.

Лідером є програма ABBYY Fine Reader, де досягається висока точність розпізнавання тексту, набраного любим шрифтом, толерантне відношення до дрібних дефектів у тексті, вірне виокремлення різних об'єктів – таблиць, зображень, заголовків. Програма мультимовна і оснащена тематичними та загальними словниками.

Довідники та енциклопедії

Це – надвеликі збірки структурованої інформації з різних напрямків. Вони мають зручний інтерфейс, різноманітні інструменти для ефективного пошуку та легкого виведення на монітор чи роздрукування отриманих результатів.

Навчальні програми та ігри

2. Прикладні програми спеціалізованого призначення

Бухгалтерські та фінансові системи

Це програми, що призначені для ведення бухгалтерського обліку, підготовки фінансової звітності, аналіз обігу фінансів та матеріальних цінностей, статистичної обробки інформації.

Найвідомішим є програмні продукти компанії 1С.

Системи автоматизованого проектування САПР

Професійні програми, що призначені для розробки та проектування технологічних креслень та проектів: електронних схем, машин, механізмів, архітектурних споруд тощо.

Відомі програми: AutoCad, Compass.

Системи штучного інтелекту та експертні системи

Це програми, що аналізують дані, які містяться у базах знань системи і видають фахові відповіді при запитах користувача. За допомогою таких систем вирішуються складні задачі, які потребують для свого розв'язання людської інтуїції.

Широко застосовують у медицині, фармакології, хімії, юриспруденції, освіті, там, де для прийняття рішення потрібні

глибокі професійні знання.

Системи відеомонтажу

Різноманітні програми, що призначені для цифрової обробки відеоматеріалів, монтажу, створення відеоефектів, виправлення дефектів, додавання звуку, титрів, субтитрів. Відомі програми: Pinnacle Studio, Adobe Premiere, Windows Movie Maker.

3. Інструментарій для програмування

Це засоби, що призначені для створення програмного забезпечення, тобто нових системних, службових чи прикладних програм.

Мови програмування

Мовою програмування називається визначений набір команд, синтаксисом і правилами створення програм.

1. Мови низького рівня є дуже наближеними до машинного коду, це так звані асемблери. Вони є вкрай складними та незручними для широкого застосування.

2. Мови високого рівня є наближеними до людської мови і легкими для вивчення і використання. Популярними мовами високого рівня є: Pascal, C, C++, Basic, Java, Pithon.

Транслятори

Трансляторами називають програми, що перекладають текст програми, що написана мовою високого рівня у машинний код.

Відлагоджувачі

Відлагоджувачами називають засоби пошуку та виправлення помилок у тексті програми.

Середовище програмування

Середовища програмування підтримують певну мову програмування і містять комплекс різних інструментів:

- Текстовий редактор для набору тексту програми.
- Транслятор.
- Відлагоджувач.
- Бібліотеки стандартних програм.
- Інструменти для автоматизації робіт.
- Зручні засоби для виведення отриманих результатів.

Контрольні запитання:

1. Які функції покладаються на програми базового рівня?
2. Які класи програм службового рівня ви знаєте?
3. До програм якого рівня відносяться програми-драйвери?
4. Які програми називають утилітами ?
5. Які категорії графічних редакторів існують?
6. Які основні класи програм прикладного рівня існують?
7. За допомогою яких програм можна пересуватися по файловій структурі комп’ютера?

ЛАБОРАТОРНА РОБОТА № 12

Тема: Базові вимоги для роботи в мережі: устаткування, програмне забезпечення. Налаштування програмного забезпечення для мережевих карт. Бездротові мережі. Встановлення програмного забезпечення та налаштування мережі Wi-Fi

Мета роботи: ознайомити студентів із основами налаштування та правилами експлуатації локальних та бездротових мереж.

Порядок виконання роботи:

1. Визначити топологію запропонованої локальної мережі. Дати її характеристику та визначити необхідне устаткування.
2. Використовуючи запропоноване обладнання підключити комп'ютер до мережі використовуючи Wi-Fi з'єднання.
3. Налаштувати зону Wi-Fi використовуючи топологію точка-точка.
4. Використовуючи статичні та динамічні IP-адреси забезпечити можливість підключення створеної зони Wi-Fi до мережі Інтернет.
5. Зробіть звіт про виконану роботу.
6. У звіті дайте письмові відповіді на контрольні запитання.

Теоретичні відомості

Комп'ютерна мережа (обчислювальна мережа, мережа передавання даних) – система зв'язку комп'ютерів і/або комп'ютерного устаткування (сервери, маршрутизатори та інше устаткування, канали зв'язку). Для передавання даних можуть бути використані різні фізичні явища, як правило – різні види електричних, світлових сигналів або електромагнітного випромінювання.

Розрізняють два поняття мережі: **комунікаційна та інформаційна**.

Комунікаційна мережа призначена для передавання даних і виконує завдання, пов'язані з їх перетворенням. Комунікаційні мережі розрізняються за типом використовуваних фізичних засобів з'єднання.

Інформаційна мережа призначена для зберігання інформації і складається з інформаційних систем. На базі комунікаційної мережі може бути побудована група інформаційних мереж.

Під інформаційною системою слід розуміти систему, яка є постачальником або споживачем інформації. Іншими словами – об'єкт, здатний здійснювати зберігання, обробку або передачу інформації. До складу інформаційної системи входять: комп'ютери, програми, користувачі та інші складові, призначені для процесу обробки і передавання даних. Надалі інформаційна система, призначена для вирішення завдань користувача, називатиметься – робоча станція (client). Робоча станція в мережі відрізняється від звичайного персонального комп'ютера (ПК) наявністю мережевої карти (мережевого адаптера), каналу для передавання даних і мережевого програмного забезпечення.

Під каналом зв'язку слід розуміти шлях або засіб, по якому передаються електричні сигнали.

Канали зв'язку (data link) створюються по лініях зв'язку за допомогою мережевого устаткування і фізичних засобів зв'язку. Фізичні засоби зв'язку побудовані на основі витих пар, коаксіальних кабелів, оптичних каналів або ефіру. Між взаємодіючими інформаційними системами через фізичні канали комунікаційної мережі й вузли комутації встановлюються логічні канали.

Логічний канал – це шлях для передавання даних від однієї системи до іншої. Логічний канал прокладається за маршрутом в одному або декількох фізичних каналах. Логічний канал можна охарактеризувати, як маршрут, прокладений через фізичні канали і вузли комутації.

Інформація в мережі передається блоками даних за процедурами обміну між об'єктами. Ці процедури називають *протоколами* передавання даних. Протокол – це сукупність правил, що встановлюють формат і процедури обміну даними між двома або декількома пристроями. Завантаження мережі характеризується параметром, який називається *трафіком*. Трафік (traffic) – це потік повідомлень в мережі передавання даних. Під ним розуміють кількісний вимір у вибраних точках мережі числа блоків даних і їх довжини, що проходять, виражене в бітах у секунду.

Істотно впливає на характеристику мережі *метод доступу*. Метод доступу – це спосіб визначення того, яка з робочих станцій зможе наступною використовувати канал зв'язку і як керувати доступом до каналу зв'язку (кабелю).

У мережі всі робочі станції фізично сполучені між собою каналами зв'язку за певною структурою, так званою топологією. Топологія – це опис фізичних з'єднань в мережі, що вказує які робочі станції можуть зв'язуватися між собою. (див. лаб. роб. № 6)

Склад основних елементів у мережі залежить від її *архітектури*. Архітектура визначає принципи побудови і функціонування апаратного і програмного забезпечення елементів мережі.

Огляд дротового мережевого устаткування

1. Мережеве устаткування першого рівня

Для підключення комп'ютера або терміналу до мережі потрібне устаткування ліній зв'язку (DCE – англ. Data Circuit – terminating Equipment або Data Communication Equipment або Data Carrier Equipment) – устаткування, що перетворює дані, комп'ютером або терміналом у сигнал для передавання по лінії зв'язку та здійснюють зворотнє перетворення. Основними видами такого обладнання є мережеві *адаптери і модеми*.

Нагадаємо, що **мережевий адаптер** (Network Interface Card, NIC) – це пристрій комп'ютера, що безпосередньо взаємодіє з середовищем передавання даних, який прямо або через інше комунікаційне устаткування зв'язує його з іншими комп'ютерами. Цей пристрій вирішує завдання надійного обміну двійковими

даними, представленими відповідними електромагнітними сигналами, по зовнішніх лініях зв'язку. Як і будь-який контролер комп'ютера, мережевий адаптер працює під управлінням драйвера операційної системи.

У більшості сучасних стандартів для локальних мереж передбачається, що між мережевими адаптерами взаємодіючих комп'ютерів встановлюється спеціальний комунікаційний пристрій, який бере на себе деякі функції з управління потоком даних.

Мережевий адаптер зазвичай виконує наступні функції:

- Оформлення даних у вигляді кадру певного формату. Кадр включає декілька службових полів, серед яких є адреса комп'ютера призначення і контрольна сума кадру.
- Надання доступу до середовища передавання даних. У локальних мережах в основному застосовуються канали зв'язку (загальна шина, кільце), що розділяються між групою комп'ютерів, доступ до яких надається за спеціальним алгоритмом (найчастіше застосовуються метод випадкового доступу або метод з передачею маркера доступу по кільцю).
- Кодування послідовності біт кадру послідовністю електричних сигналів при передаванні даних і декодування при їх прийомі. Кодування повинне забезпечити передачу даних лініями зв'язку з певною смугою пропускання і певним рівнем перешкод так, щоб приймаюча сторона змогла розпізнати дані з високою мірою вірогідності.
- Перетворення інформації з паралельної форми в послідовну і навпаки. Ця операція пов'язана з тим, що в обчислювальних мережах дані передаються в послідовній формі, біт за бітом, а не побайтно, як у комп'ютерних системах.
- Синхронізація бітів, байтів і кадрів. Для стійкого прийому даних потрібна підтримка постійної синхронізації приймача і передавача даних.

Мережеві адаптери розрізняються за типом і розрядністю використовуваної в комп'ютері внутрішньої шини даних – PCI, MCA, PCI-Express.

Мережеві адаптери розрізняються також за типом прийнятої в мережі мережевої технології і тому подібне. Як правило, конкретна модель мережевого адаптера працює за певною мережевою технологією.

У зв'язку з тим, що для кожної технології зараз є можливість використання різних середовищ передавання даних, мережевий адаптер може підтримувати як одне, так і декілька середовищ одночасно. У разі, коли мережевий адаптер підтримує тільки одне середовище передавання даних, а необхідно використовувати інше, застосовуються *трансивери і конвертори*.

Трансивер (приймач, transmitter+receiver) – це частина мережевого адаптера, його пристрій, що виходить на роз'єм кабелю. У деяких варіантах виявилося зручним випускати мережеві адаптери, до яких можна приєднати трансивер для необхідного середовища.

Замість підбору відповідного трансиверу можна використовувати конвертор, який може сполучати вихід приймача, призначеного для одного середовища, з іншим середовищем передавання даних.

Модем (абревіатура, складена із слів модулятор/демодулятор) – пристрій, що застосовується в системах зв'язку і виконує функцію модуляції і демодуляції.

2. Мережеве устаткування другого рівня (проміжне). Повторювачі і концентратори.

Основна функція **повторювачів (repeater)** – це повторення сигналів, що поступають на його порт. Повторювач покращує електричні характеристики сигналів і їх синхронність, і за рахунок цього з'являється можливість збільшувати загальну довжину кабелю між самими віддаленими в мережі вузлами.

Багатопортовий повторювач часто називають **концентратором** (concentrator) або **хабом** (hub) – це устаткування реалізує не лише функцію повторення сигналів, але і концентрує в одному центральному пристрої функції об'єднання комп'ютерів у мережу. Практично в усіх сучасних мережевих стандартах

концентратор є необхідним елементом мережі, що сполучає окремі комп'ютери в мережу.

Відрізки кабелю, сполучаючи два комп'ютери або два інших мережевих пристрої, називаються фізичним сегментом, тому концентратори і повторювачі, які використовуються для додавання нових фізичних сегментів, є засобом фізичної структуризації мережі.

Концентратор – пристрій, у якого сумарна пропускна спроможність вхідних каналів вища за пропускну спроможність вихідного каналу. Оскільки потоки вхідних даних в концентраторі більше вихідного потоку, то головним його завданням є концентрація даних. При цьому можливі ситуації, коли число блоків даних, що поступає на входи концентратора, перевищує його можливості. Тоді концентратор ліквідовує частину цих блоків.

Концентратор є активним устаткуванням. Концентратор служить центром (шиною) зіркоподібної конфігурації мережі і забезпечує підключення мережевих пристроїв. У концентраторі для кожного вузла (ПК, принтери, сервери доступу, телефони та ін.) має бути передбачений окремий порт.

Нарощувані концентратори є окремими модулями, які об'єднуються за допомогою швидкодіючої системи зв'язку. Такі концентратори надають зручний спосіб поетапного розширення можливостей і потужності мережі.

Концентратор здійснює електричну розв'язку відрізків кабелю до кожного вузла, тому коротке замикання на одному з відрізків не виведе з ладу всю мережу (рис. 12.1).

Концентратори утворюють з окремих фізичних відрізків кабелю загальне середовище передавання даних – **логічний сегмент.** Логічний сегмент також називають доменом колізій, оскільки при спробі одночасного передавання даних будь-яких двох комп'ютерів цього сегменту, що хоч би і належать різним фізичним сегментам, виникає блокування передавального середовища.

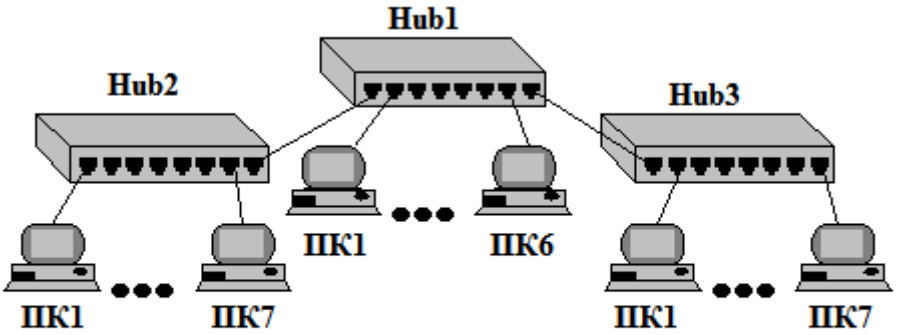

Рис. 12.1. Логічний сегмент, побудований з використанням концентраторів

Слід, особливо підкреслити, що яку б складну структуру не утворювали концентратори, наприклад шляхом ієрархічного з'єднання (рис. 12.1), всі комп'ютери, підключені до них, утворюють єдиний логічний сегмент, в якому будь-яка пара взаємодіючих комп'ютерів повністю блокує можливість обміну даними для інших комп'ютерів. Концентратори підтримують технологію "plug-in-play" і не вимагають встановлення параметрів. Необхідно просто спланувати свою мережу і вставити роз'єми в порти хаба і комп'ютерів.

Планування мережі з хабом

При плануванні мережі із використанням концентратора беруть до уваги наступні аспекти:

- місце розташування;
- відстані;
- живлення.

Вибір місця розташування концентратора є найбільш важливим етапом планування невеликої мережі. Хаб розумно розташувати поблизу геометричного центру мережі (на однаковій відстані від усіх комп'ютерів). Таке розташування дозволить мінімізувати витрату кабелю. Довжина кабелю від концентратора до будь-якого з комп'ютерів, що підключаються до мережі, або периферійних пристроїв не повинна перевищувати 100м.

При плануванні мережі є можливість нарощування (каскадування) хабів.

Переваги концентратора

Концентратори мають багато переваг. По-перше, в мережі використовується топологія зірка. Така топологія спрощує налаштування і управління мережею. Будь-які переміщення комп'ютерів або додавання в мережу нових вузлів при такій топології дуже нескладно виконати. Крім того, ця топологія значно надійніша, оскільки при будь-якому пошкодженні кабельної системи мережа зберігає працездатність (перестає працювати лише пошкоджений промінь). Світлодіодні індикатори хаба дозволяють контролювати стан мережі і легко виявляти несправності.

Різні виробники концентраторів реалізують у своїх пристроях різні набори допоміжних функцій, але найчастіше зустрічаються наступні:

- об'єднання сегментів з різними фізичними середовищами (наприклад, з різними видами кабелів);
- автосегментація портів – автоматичне відключення порту при його некоректній поведінці (пошкодження кабелю, інтенсивна генерація пакетів помилкової довжини і тому подібне);
- підтримка між концентраторами резервних зв'язків, які використовуються при відмові основних;
- захист даних, що передаються мережею від несанкціонованого доступу (наприклад, шляхом спотворення поля даних в кадрах, повторюваних на портах, що не містять комп'ютера з адресою призначення).

Мости і комутатори

Міст (bridge) – ретрансляційна система, що сполучає канали передавання даних та об'єднує різнотипні канали в один загальний.

Міст (bridge), а також його швидкодіючий аналог – комутатор (switching hub), ділять загальне середовище передавання даних на логічні сегменти. Логічний сегмент утворюється шляхом об'єднання декількох фізичних сегментів (відрізків кабелю) за допомогою одного або декількох концентраторів. Кожен логічний сегмент підключається до окремого порту моста/комутатора. При появі кадру на який-небудь з портів міст/комутатор повторює цей

кадр, але не на всіх портах, як це робить концентратор, а тільки на тому порту, до якого підключений сегмент, комп'ютер-адресат.

Мости можуть сполучати сегменти, що використовують різні типи носіїв і сполучати мережі з різними методами доступу до каналу.

Відмінність між мостом і комутатором

Різниця між мостом і комутатором полягає в тому, що міст у кожен момент часу може здійснювати передачу кадрів тільки між однією парою портів, а комутатор одночасно підтримує потоки даних між усіма своїми портами. Іншими словами, міст передає кадри послідовно, а комутатор паралельно.

Мости використовуються тільки для зв'язку локальних мереж з глобальними, тобто як засоби віддаленого доступу, оскільки в цьому випадку необхідність в паралельній передачі між декількома парами портів просто не виникає.

Коли з'явилися перші пристрої, що дозволяють роз'єднувати мережу на декілька сегментів вони були двопортовими і дістали назву мостів (bridge). У процесі розвитку цього типу устаткування, вони стали багатопортовими і дістали назву комутаторів (switch). Деякий час обидва поняття існували одночасно, а пізніше замість терміну "міст" стали застосовувати "комутатор". Слід зазначити, що останнім часом локальні мости повністю витиснені комутаторами.

3. **Мережеве устаткування третього рівня (комутатори, маршрутизатори).**

Комутатор (switch) – пристрій, що здійснює вибір одного з можливих варіантів напряму передавання даних. У комунікаційній мережі комутатор є ретрансляційною системою (система, призначена для передавання даних або перетворення протоколів), прозорості (тобто комутація здійснюється без будь-якої обробки даних). Комутатор не має буферів і не може накопичувати данні. Тому при використанні комутатора швидкості передавання сигналів у сполучних каналах передавання даних, мають бути однаковими. На відміну від інших видів ретрансляційних систем, тут, як правило, не використовується програмне забезпечення.

Комутатор (switch) може сполучати сервери і служити основою для об'єднання декількох робочих груп. Він направляє пакети даних між вузлами мережі. Кожен комутований сегмент дістає доступ до каналу передавання даних без конкуренції і бачить тільки той трафік, який прямує в його сегмент. Комутатор повинен надавати кожному порту можливість з'єднання з максимальною швидкістю без конкуренції з боку інших портів (на відміну від спільно використовуваного концентратора). Зазвичай в комутаторах є один або два високошвидкісні порти, а також інструментальні засоби управління. Комутатором можна замінити маршрутизатор, доповнити їм нарощуваний маршрутизатор або використовувати комутатор як основа для з'єднання декількох концентраторів. Комутатор може служити відмінним пристроєм для напряму трафіку між концентраторами мережі робочої групи і завантаженими файл-серверами.

Комутатор локальної мережі

Комутатор локальної мережі (local – area network switch) – пристрій, що забезпечує взаємодію сегментів одній або групі локальних мереж.

Комутатор локальної мережі, як і звичайний комутатор, забезпечує взаємодію підключених до нього локальних мереж. Але на додаток до цього він здійснює перетворення інтерфейсів, якщо з'єднуються різні типи сегментів локальної мережі. У перелік функцій, що виконуються комутатором локальної мережі, входять забезпечення наскрізної комутації, наявність засобів маршрутизації, підтримка простого протоколу управління мережею, імітація моста або маршрутизатора, організація віртуальних мереж, швидкісна ретрансляція блоків даних.

Маршрутизатор (router) – ретрансляційна система, що сполучає дві комунікаційні мережі або їх частини. З'єднання пар комунікаційних мереж відбувається через маршрутизатори, які здійснюють необхідне перетворення вказаних протоколів. Маршрутизатор працює з декількома каналами, направляючи в який-небудь з них черговий блок даних. Маршрутизатори обмінюються даними про зміни структури мереж, трафік і їх стан.

Завдяки цьому, вибирається оптимальний маршрут дотримання блоку даних у різних мережах від абонентської системи-відправника до системи-одержувача. Маршрутизатори забезпечують також з'єднання адміністративно незалежних комунікаційних мереж. Маршрутизатором може бути як спеціальний електронний пристрій, так і спеціалізований комп'ютер, підключений до декількох мережевих сегментів за допомогою декількох мережевих карт.

Шлюз (gateway) – ретрансляційна система, що забезпечує взаємодію інформаційних мереж. Шлюз є найбільш складною ретрансляційною системою, що забезпечує взаємодію мереж із різними наборами протоколів. У свою чергу, набори протоколів можуть спиратися на різні типи фізичних засобів з'єднання. У тих випадках, коли з'єднуються інформаційні мережі, то в них частина рівнів може мати одні і ті ж протоколи. Тоді мережі з'єднуються не за допомогою шлюзу, а на основі простіших ретрансляційних систем, наприклад маршрутизаторами і мостами. Необхідність у мережевих шлюзах виникає при об'єднанні двох систем, що мають різну архітектуру. Як шлюз, зазвичай використовується виділений комп'ютер, на якому активоване програмне забезпечення шлюзу і проводяться перетворення, що дозволяють взаємодіяти декільком системам у мережі. Іншою функцією шлюзів є перетворення протоколів. Шлюзи складні в налаштуванні та працюють повільніше, ніж маршрутизатори.

Організація та налаштування локальних мереж

Кожен комп'ютер у мережі TCP/IP має IP-адресу. IP-адреса (від англ. Internet Protocol Address) – унікальна мережева адреса вузла в комп'ютерній мережі, побудованій за протоколом IP. У мережі Інтернет потрібна глобальна унікальність адреси; у разі роботи в локальній мережі – унікальність адреси в межах мережі. У версії протоколу IPv4 IP-адреса має довжину 4 байти.

IPv4 є 32-бітовим двійковим числом. Зручною формою запису IP-адреси (IPv4) є запис у вигляді чотирьох десяткових чисел значенням від 0 до 255, розділених точками, наприклад, 192.168.0.1,

значення 255 не використовується безпосередньо в адресах, а є зарезервованим значенням і використовується для масок підмережі.

У термінології мереж TCP/IP маскою підмережі або маскою мережі називається бітова маска, визначена, яка частина IP-адреси вузла мережі. Наприклад, вузол із IP-адресою 12.34.56.78 і маскою підмережі 255.255.255.0 знаходиться в мережі 12.34.56.0/24 з довжиною префікса 24 біта.

Інший варіант визначення – це визначення підмережі IP-адрес. Наприклад, за допомогою маски підмережі можна сказати, що один діапазон IP-адрес буде в одній підмережі, а другий діапазон відповідно в іншій підмережі.

Широкомовна адреса – умовна (не присвоєний ніякому пристрою в мережі) адреса, яка використовується для передавання широкомовних пакетів в комп'ютерних мережах.

Стек протоколів TCP/IP тісно пов'язаний із мережею Internet. Створений він був в 1969 році, коли для мережі ARPANET знадобилися ряд стандартів для об'єднання в єдину мережу комп'ютерів із різною архітектурою й операційними системами. На базі цих стандартів і був розроблений набір протоколів, що дістали назву TCP/IP.

Разом із розвитком Internet протокол TCP/IP завойовував позиції і в інших мережах. На сьогодні цей мережевий протокол використовується як для зв'язку комп'ютерів всесвітньої мережі, так і в переважній більшості корпоративних мереж. Найбільш частіше використовується версія протоколу IP, відома як IPv4.

Згідно із специфікацією протоколу, кожному вузлу приєднаному до IP-мережі, надається унікальний номер. Вузол може бути комп'ютером, маршрутизатором, міжмережевим екраном та інші. Якщо один вузол має декілька фізичних підключень до мережі, то кожному підключенню надається свій унікальний номер. Цей номер, або по-іншому IP-адреса, має довжину в чотири октети, і складається з двох частин. Перша частина визначає мережу до якої належить вузол, а друга – унікальна адреса самого вузла всередині мережі.

Номер мережі Номер вузла
11011100 11010111 00001110 00010110

У класичній реалізації протоколу першу частину адреси називали “мережевим префіксом”, оскільки вона однозначно визначала мережу.

Класична адресна схема протоколу IP. Спочатку весь адресний простір розділили на п’ять класів: A, B, C, D і E. Така схема дістала назву “класовою”. Кожен клас однозначно ідентифікувався першими бітами лівого байта адреси. Самі ж класи відрізнялися розмірами мережевої і вузлової частин. Знаючи клас адреси, можна було визначити межу між його мережевою і вузловою частинами. Крім того, така схема дозволяла при маршрутизації не передавати разом із пакетом інформацію про довжину мережевої частини IP-адреси (див. табл. 12.1).

Клас A орієнтований на дуже великі мережі. Всі адреси, що належать цьому класу, мають 8-бітовий мережевий префікс, на що вказує перший біт лівого байту адреси встановлений у нуль.

Клас B призначений для мереж великого і середнього розмірів. Адреси цього класу ідентифікуються двома старшими бітами, рівними відповідно до 1 і 0. Мережевий префікс класу складається з шістнадцяти біт або перших двох октетів адреси.

Клас C найрозповсюджений клас мереж який має 24 бітовий мережевий префікс, визначається старшими бітами, встановленими в 110, і може ідентифікувати до 221 мережі.

Таблиця 12.1

Клас	1 байт					2 байт	3 байт	4 байт
A	0							
B	1	0						
C	1	1	0					
D	1	1	1	0	Адрес групи Mulnicast			
E	1	1	1	1	0	Зарезервовано		

Класи IP-мереж

Адреса мережі		Адреса вузла
Найменший номер мережі	**Найбільший номер мережі**	**Число вузлів у мережі**
1.0.0.0	**126.0.0.0**	2^4
128.0.0.0	**192.255.0.0**	2^{16}
192.0.1.0	**223.255.255.0**	2^8
224.0.0.0	**239.255.255.255**	
240.0.0.0	**247.255.255.255**	

Структура IP-адрес

Останні два класи займають восьму частину, що залишилася, в адресному просторі призначені для службового – клас D і клас E – експериментального використання. Для класу D старші чотири біта адреси встановлені в 1110, для класу E – 1111. Сьогодні клас D використовується для групової передачі даних.

Оскільки довгі послідовності з одиниць і нулів важко запам’ятати, IP-адреси зазвичай записують в десятковій формі. Для цього кожен октет адреси представляється у вигляді десяткового числа. Між собою октети відокремлюється точкою. Іноді октети позначаються як w.x.y.z і називаються “z-октет”, “y-октет”, “x-октет” і “w-октет”.

Представлення IP-адреси у вигляді чотирьох десяткових чисел розділених точками і називається “Точково-десяткова нотація”.

Адреса 11011100 11010111 00001110 00010110

220 215 14 22

Точково-десятковий формат 220.215.14.22

Неважко порахувати, що всього в просторі адрес IP-128 мереж по 16 777 216 адрес класу A, 16384 мереж по 65536 адрес класу B і 2 097 152 мереж по 256 адрес класу C, а також 268 435 456 адрес багатоадресної розсилки і 134 317 728 зарезервованих адрес. Із зростанням мережі Інтернет ця система виявилася неефективною і була доповнена CIDR (безкласовою адресацією).

Організація підмереж. Дуже рідко в локальну обчислювальну мережу входить більше 100-200 вузлів: навіть якщо взяти мережу з великою кількістю вузлів, багато мережевих середовищ накладають обмеження, наприклад, в 1024 вузли. Виходячи з цього, доцільність

використання мереж класу А і В дуже сумнівна. Та і використання класу С для мереж, що складаються з 20-30 вузлів, теж є марнотратством.

Порядок призначення IP-адрес. За визначенням схема IP-адресації повинна забезпечувати унікальність нумерації мереж, а також унікальність нумерації вузлів у межах кожної з мереж. Отже, процедури призначення номерів як мережам, так і вузлам мереж повинні бути *централізованими.*

Коли справа стосується мережі, яка є частиною Інтернету, унікальність нумерації може бути забезпечена тільки зусиллями спеціально створених для цього центральних органів. У невеликій же автономній IP-мережі умова унікальності номерів мереж і вузлів може бути виконана силами мережевого адміністратора.

У цьому випадку в розпорядженні адміністратора є весь адресний простір, тому що збіг IP-адрес у незв'язаних між собою мережах не викличе ніяких негативних наслідків. Адміністратор може вибирати адреси довільно, дотримуючись лише синтаксичних правил, враховуючи обмеження на особливі адреси.

Однак, при такому підході виключена можливість у майбутньому приєднати дану мережу до Інтернету. Дійсно, довільно обрані адреси даної мережі можуть збігтися із централізовано призначеними адресами Інтернету. Для того щоб уникнути колізій, пов'язаних з такого роду збігами, у стандартах Інтернету визначено декілька так званих приватних адрес, які рекомендують для автономного використання:

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

Ці адреси виключені з адрес, які розподіляються централізовано, і становлять величезний адресний простір, достатній для нумерації вузлів автономних мереж практично будь-яких розмірів. Варто також відзначити, що приватні адреси, як і при довільному виборі адрес, у різних автономних мережах можуть збігатися. У той же час використання приватних адрес для адресації

автономних мереж робить можливим коректне підключення їх до Інтернету.

Огляд бездротового устаткування

Безпроводові мережі

У 1997 році IEEE (*Institute of Electrical and Electronics Engineers* – міжнародна організація вчених, інженерів з електротехніки і електроніки) був прийнятий стандарт для безпроводових мереж IEEE 802.11. Розробкою і підтримкою стандарту 802.11 займається комітет Wi-Fi Alliance. Термін Wi-Fi (Wireless Fidelity) використовується як загальне ім’я для стандарту 802.11, а також всіх подальших специфікацій, що відносяться до безпроводових локальних мереж (wireless LAN).

Безпроводові мережі можуть мати **дві логічні топології**:

1. Точка доступу (Infrastructure) – зіркоподібна топологія застосовується в пристроях стандарту 802.11b і RADIOLAN. Тут точка доступу (вузловий передавач) грає роль концентратора, оскільки всі комп’ютери з’єднуються через неї, а не взаємодіють один з одним безпосередньо. Декілька мережевих адаптерів можуть бути об’єднані однією точкою доступу, або декілька точок доступу сполучено з однією точкою доступу. Цей режим застосовується для створення локальної безпроводової мережі з декількох користувачів, для з’єднання цієї мережі з провідною мережею (наприклад, для виходу в Інтернет), для з’єднання між собою декількох провідних мереж.

2. Точка-точка (Ad-hoc). Два мережеві адаптери або дві точки доступу з’єднуються між собою. Метод застосовується для безпосереднього з’єднання двох комп’ютерів або для організації радіо-моста між двома проводовими мережами. Ця топологія використовується в пристроях MOMERF (Home Radio Freqiuently – домашній радіодіапазон) і застосовується в пристроях Bluetooth. Такі пристрої безпосередньо з’єднуються один з одним і не вимагають ніяких вузлових передавачів або інших пристроїв, подібних до концентратора, для взаємодії один з одним.

Таким чином, устаткування безпроводових мереж включає вузлові передавачі – точки безпроводового доступу (Access Point) і

безпроводові адаптери для кожного абонента. Точки доступу виконують роль концентраторів, що забезпечують зв'язок між абонентами і між собою, а також функцію мостів, що здійснюють зв'язок із кабельною локальною мережею й Інтернетом. Декілька близько розташованих точок доступу створюють зону доступу Wi-Fi (Hotspot), в межах якої всі абоненти, що забезпечені безпроводовими адаптерами, дістають доступ до мережі. Кожна точка доступу може обслуговувати декілька абонентів, але чим більше абонентів, тим менш ефективна швидкість передавання для кожного з них. Клієнтські системи автоматично перемикаються на вузловий передавач з сильнішим сигналом або на передавач із меншим рівнем помилок.

Метод доступу до такої мережі – множинний доступ із запобіганням колізіям CSMA/CD (Carrier Sense Multiple Access with Collision Detection). Мережа будується за стільниковим принципом. У мережі передбачений механізм роумінгу, тобто підтримується автоматичне підключення до точки доступу і перемикання між точками доступу при переміщенні абонентів, хоча строгих правил роумінгу стандарт не встановлює.

Налаштування безпроводового устаткування проводиться згідно інструкції яка додається до комплекту пристрою.

Контрольні запитання:

1. Призначення та відмінності повторювача та концентратора?
2. Призначення та відмінності шлюзу та мосту?
3. Що таке комутатор і чим він відрізняється від моста?
4. Що таке маршрутизатор і чим він відрізняється від моста?
5. Призначення IP-адреси та маски підмережі?
6. Дайте визначення та основне призначення DNS-сервера?
7. Перерахуйте основні топології безпроводових технологій?

ЛАБОРАТОРНА РОБОТА № 13

Тема: Безпека та захист ОС Windows. Комп'ютерні віруси та засоби захисту від них. Засоби захисту комп'ютерних мереж

Мета роботи: ознайомити студентів із основами безпеки та захисту інформації ОС Windows, комп'ютерних мереж, класифікацією комп'ютерних вірусів та антивірусною роботою.

Порядок виконання роботи:

1. Ознайомитися з теоретичними відомостями.
2. Ознайомитися з опціями діалогового вікна "Диспетчер задач".
3. Створити точку відновлення системи з поточною датою та перевірити її працездатність.
4. На прикладі антивірусної системи ESS (Eset Smart Security) ознайомитися з усіма модулями що входять до її складу.
5. Налаштувати персональний Firewall у режимі навчання.
6. Оновити базу даних вірусних сигнатур, при необхідності зареєструвати програму за допомогою імені користувача та пароля.
7. Зробіть звіт про виконану роботу.
8. У звіті дайте письмові відповіді на контрольні запитання.

Теоретичні відомості

Безпека та захист ОС Windows

У складі ОС Windows є засіб під назвою ***"Безопасность Windows",*** який можна викликати у будь-який момент натиснувши комбінацію клавіш **Ctrl+Alt+Del**. Потреба у ньому виникає в разі зависання комп'ютера. У вікні під назвою **БЕЗОПАСНОСТЬ WINDOWS** можна завершити роботу (кнопка **ЗАВЕРШЕНИЕ РАБОТЫ**), зняти блокування функцій, заборонених

адміністратором (кнопка **БЛОКИРОВКА**), змінити пароль (кнопка **СМЕНА ПАРОЛЯ**), вийти з системи (кнопка **ВЫХОД ИЗ СИТЕМЫ**); викликати вікно **ДИСПЕТЧЕР ЗАДАЧ** для з'ясування стану завантаження системи. Диспетчер задач дозволяє з'ясувати, який додаток "винний" у зависанні (у вкладці **ПРОЦЕССЫ** цей додаток покаже надто великі втрати ресурсів **ЦП**) і при відсутності іншого виходу зняти цю задачу (рис. 13.1).

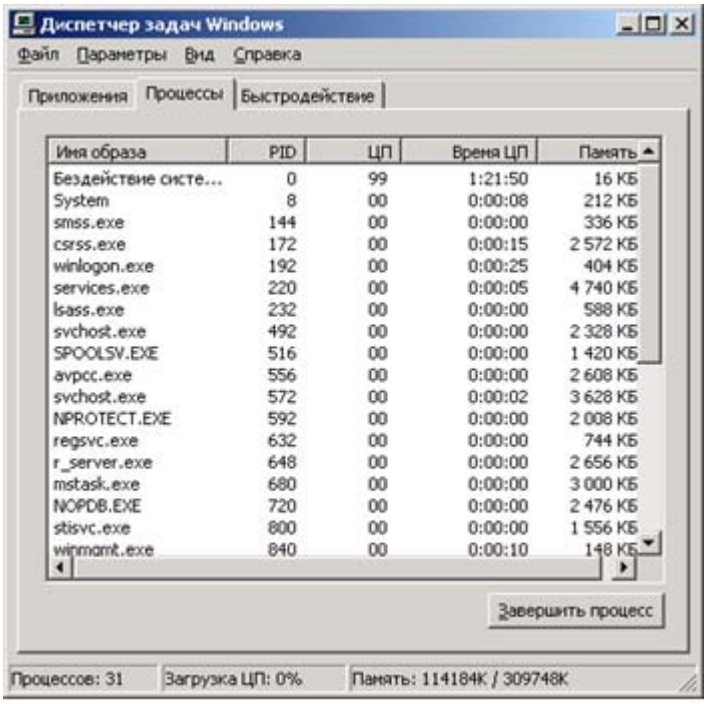

Рис. 13.1 Діалогове вікно Диспетчер задач

Перевірка диску

Перевірка диску це корисна операція, яку варто використовувати регулярно. Вона дозволяє виявляти логічні помилки у файловій структурі, а також фізичні помилки, зв'язані з дефектами поверхні жорсткого диску. Виконується у послідовності: МОЙ КОМПЬЮТЕР вибрати диск, який треба перевірити **ФАЙЛ→СВОЙСТВА→СЕРВИС→ПРОВЕРКА ДИСКА →ВЫПОЛНИТЬ ПРОВЕРКУ.** Встановити прапорець **ПРОВЕРЯТЬ И ВОССТАНАВЛИВАТЬ ПОВРЕЖДЕННЫЕ СЕКТОРА** (рис. 13.2).

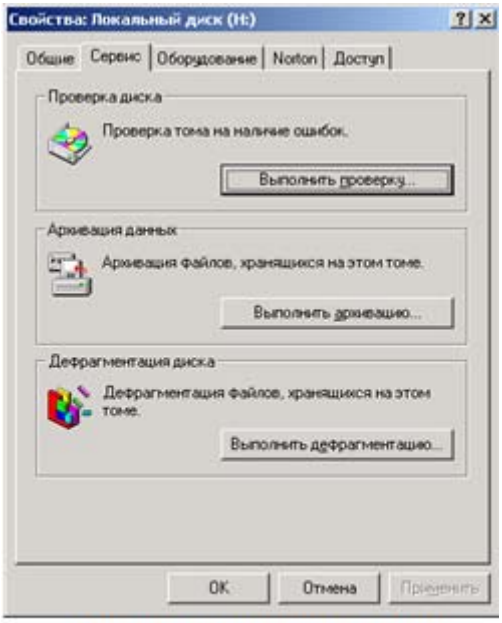

Рис. 13.2 Діалогове вікно сервісу перевірки диску

Захист системи

Захист системи – це функція, яка регулярно створює та зберігає відомості про системні файли та налаштування комп'ютера. Захист системи також зберігає попередні версії змінених файлів. Ці файли зберігаються в *контрольних точках відновлення*, які створюються перед значними системними подіями, такими як інсталяція програми або драйверу пристрою. Вони також створюються автоматично один раз щотижня, якщо за попередній тиждень не створено інших контрольних точок відновлення, але можна в будь-який час створювати контрольні точки відновлення вручну.

Захист системи автоматично вмикається для диска, на якому інстальована ОС Windows. Захист системи можна ввімкнути лише для дисків, які відформатовано за допомогою файлової системи NTFS.

Існує два способи скористатися перевагами захисту системи:

• Якщо комп'ютер працює повільно або неправильно, можна скористатися засобом *відновлення системи*, щоб відновити системні файли та налаштування комп'ютера до попереднього стану за допомогою контрольної точки відновлення.

• Якщо випадково змінено чи видалено файл або папку, її можна повернути до попередньої версії, збереженої як частина контрольної точки відновлення.

Відновлення системи дає змогу повернути системні файли комп'ютера до попереднього стану. У такий спосіб можна скасувати зміни, внесені до комп'ютера, не впливаючи на особисті файли, наприклад електронну пошту, документи або фотографії.

Іноді інсталяція програми або драйверу може спричинити неочікувані

зміни в системі комп'ютера або привести до непередбачуваної поведінки ОС Windows. Зазвичай видалення програми або драйверу виправляє помилку. Якщо після видалення помилка залишилася, можна спробувати відновити систему комп'ютера до попереднього стану, коли все працювало належним чином. Для запуску "Відновлення системи", натисніть кнопку **Пуск→Программы→ Стандартные→Служебные→Восстановление системы (Start→ Programs→Accessories→System Tools→System Restore)**. Якщо буде запропоновано ввести пароль адміністратора або підтвердити видалення, введіть пароль або надайте підтвердження.

Резервні копії образу системи, які зберігаються на жорстких дисках, також можна використовувати для відновлення системи, так само як контрольні точки відновлення, створені функцією захисту системи. Навіть якщо резервні копії образу системи містять системні файли й особисті відомості, відновлення системи не вплине на файли даних.

Образ системи – це точна копія диска. За замовчуванням образ системи включає диски, необхідні для запуску ОС Windows. Він також містить файли, програми та налаштування системи Windows, а також ваші файли програм та налаштування. Відновлення комп'ютера з образу системи – це повне відновлення; не можна вибрати окремі елементи для відновлення, і всі поточні файли, програми та налаштування системи замінюються вмістом образу системи.

Для створення образу системи можна скористатися відповідними утилітами, наприклад, **Acronis Disk Director, Norton Ghost** та інші, або власними засобами ОС Windows.

Засіб відновлення системи не призначений для резервного копіювання особистих файлів, тому за його допомогою не можна відновити видалені або пошкоджені особисті файли. Слід регулярно здійснювати резервне копіювання особистих файлів і важливих даних.

Комп'ютерні віруси та антивірусна робота

Комп'ютерний вірус – це шкідлива програма, здатна до саморозмноження та розповсюдження при передаванні даних з одного комп'ютера на інший.

Офіційно вважається що термін "комп'ютерний вірус" уперше використав співробітник Лехайського університету (США) Ф. Коен в 1984 р. на 7-ій конференції з безпеки інформації, що проходила в США.

Нині окрім класичних комп'ютерних вірусів існують мережеві віруси (черв'яки і троянські програми), а також інші шкідливі програми.

Типи вірусів:

- файлові;
- завантажувальні;
- макро-віруси;
- скриптові;
- мережеві.

Файлові віруси різними способами впроваджуються у виконувані файли, або створюють файли-двійники.

Прикладом, що показує, наскільки складними є подібні програми – вірус WinNT.RemEx (Remote Explorer). При запуску файлу вірусу його код копіюється в системний каталог WinNT System32\Drivers під ім'ям IE403R.SYS і запускається як системний сервіс, який один раз в 10 хвилин запускає одну зі своїх підпрограм або зараження, або "замітання слідів". Процедура зараження сканує випадково вибрані локальні та доступні мережеві папки, шукає *.EXE-файли і заражає їх. При зараженні вірус компресує файл-

жертву, записує в нього свій код і додає компресований первинний код файлу в його кінець. При запуску зараженого файлу вірус копіює його в тимчасовий файл, розпаковує і виконує початковий файл програми. Залежно від випадкового лічильника вірус також псує й інші файли: компресує їх тим же методом і потім шифрує крипто-алгоритмом середньої складності. Процедура "замітання слідів" запускається слідом за зараженням і знищує сліди життєдіяльності вірусу. Вірус закриває повідомлення про помилки, що сталися при зараженні файлів, і виконує інші дії.

Завантажувальні віруси записують себе в завантажувальний сектор диска (boot-сектор), або в сектор, системний завантажувач вінчестера (Master Boot Record), що містить, або міняють покажчик на активний boot-сектор. Цей тип вірусів був досить поширений в 1990-х роках, але практично зник з переходом на 32-розрядні операційні системи і відмовою від використання дискет як основного способу обміну інформацією.

Макро-віруси заражають файли даних різних найбільш розповсюджених програм. Багато текстових, табличних і графічних редакторів, системи проектування, мають свої мови програмування для роботи з різними об'єктами, присутніми у файлах цих систем (наприклад, Visual Basic for Application (VBA системі Microsoft Office). Текст програм на мові VBA зберігається в модулях процедур (макросах), що зберігаються у файлах документів. Макро-віруси є програмами на мовах, вбудованих в такі системи обробки даних. Наприклад, при відкритті документу Word перевіряє його на наявність процедури з ім'ям AutoOpen, якщо вона є присутньою, то Word виконує її. Для свого розмноження віруси цього класу використовують можливості мов цих систем і при їх допомозі переносять себе з одного зараженого файлу (документу, таблиці або іншого файлу даних) в інші.

Скриптові віруси написані на різних скрипт-мовах (VBS – Visual Basic Script, JS – Java Script, BAT, PHP та ін.), які широко використовуються в ОС Windows і Web-програмуванні. Вони або заражають інші скрипт-програми, присутні у вигляді програмних

файлів або фрагментів тексту html-коду, або є частинами багатокомпонентних вірусів.

Приклад: Virus.VBS.Redlof – написаний на мові VBS та зашифрований. При першому запуску створює файл зі своїм виконуваним кодом в системному каталозі Windows з ім'ям Kernel.dll. Крім того, копіює себе в усі каталоги на інших дисках зараженого комп'ютера у вигляді файлу налаштування відображення файлів і папок – folder.htt. Заражений файл folder.htt отримує керування і копіюється вірусом в усі папки при їх відкритті за допомогою Провідника. Вірус дописує себе в усі HTM-файли, що знаходяться в каталозі Windows\web і таким чином він також отримує керування при відкритті цих файлів.

Мережеві віруси використовують для свого поширення протоколи і команди комп'ютерних мереж та електронної пошти.

Троянська програма – програма, яка таємно від користувача виконує на комп'ютері будь-які небажані для нього дії.

За своїми функціями вони підрозділяються на:

- бекдор (Backdoor) – несанкціонований доступ до віддаленого адміністрування комп'ютера;
- PSW-троянці – викрадення паролів;
- Trojan Clicker – відкриває на комп'ютері веб-посилання без відома користувача;
- Trojan Downloader – завантаження з Інтернету яких-небудь файлів без відома користувача;
- Trojan-Dropper – інсталює без відома користувача інші шкідливі програми на заражений комп'ютер і запускає їх;
- Trojan Proxy – запускає без відома користувача проксі-сервер на зараженому комп'ютері;
- Та багато інших.

Мережеві черв'яки підрозділяються на поштових (Email-Worm), які використовують Інтернет-пейджери типу ICQ (IM-Worm), IRC – засоби Інтернет-спілкування (IRC-Worm), що заражають Інтернет-сервери та інші.

Поштові черв'яки після інсталяції в системі можуть розсилати себе за всіма адресами, виявленими в адресній книзі Windows і у

файлах електронної пошти. Інші види мережевих черв'яків можуть розсилати URL-адресу на себе або інші сайти за адресами, виявленими у базах Інтернет-пейджерів або IRC-клієнтів, відкриваючи повний мережевий доступ до локальних дисків комп'ютера.

До шкідливих програм відносяться також руткіти (rootkits) – утиліти, що використовуються хакерами для приховування своєї шкідливої діяльності на зараженому комп'ютері. Для цього вони модифікують операційну систему комп'ютера. Руткіти не лише приховують свою власну присутність, але також і дії, які робить зловмисник. Руткіти можуть приховувати присутність інших шкідливих програм на комп'ютері, змінюючи файлові дані, ключі реєстру або активні процеси.

Особливості алгоритмів роботи вірусів :

- резидентність;
- використання стелс-алгоритмів;
- самошифрування та поліморфічність;
- використання нестандартних прийомів.

Резидентний вірус при інфікуванні комп'ютера залишає в оперативній пам'яті свою резидентну частину, яка потім перехоплює звернення операційної системи до об'єктів зараження і вбудовується в них. Резидентні віруси знаходяться в пам'яті та залишаються активними до вимкнення або перезавантаження комп'ютера.

Резидентними можна вважати макро-віруси, оскільки вони постійно є присутніми в пам'яті комп'ютера на весь час роботи зараженого редактора.

Нерезидентні віруси не заражають пам'ять комп'ютера і зберігають активність обмежений час. Деякі віруси залишають в оперативній пам'яті невеликі резидентні програми, які не поширюють вірус. Такі віруси вважаються нерезидентними.

Використання стелс-алгоритмів дозволяє вірусам повністю або частково приховати себе в системі. Найбільш поширеним стелс-алгоритмом є перехоплення запитів ОС на читання/запис заражених об'єктів. Стелс-віруси при цьому або тимчасово лікують їх, або

“підставляють” замість себе незаражені ділянки інформації. У разі макро-вірусів найбільш популярний спосіб – є заборона викликів меню перегляду макросів.

Самошифрування і поліморфічність використовуються практично усіма типами вірусів для того, щоб максимально ускладнити процедуру детектування вірусу. Поліморфні віруси (polymorphic) – це віруси які досить складно виявити, тому що вони не мають сигнатури, тобто не містять жодної постійної ділянки програмного коду. У більшості випадків два зразки одного і того ж поліморфного вірусу не матимуть жодного збігу. Це досягається шифруванням основного тіла вірусу і модифікаціями програм дешифрування.

За деструктивними можливостям віруси підрозділяються на:

- нешкідливі, тобто ніяк не впливають на роботу комп’ютера (окрім зменшення вільного місця на диску в результаті свого розмноження);
- безпечні, вплив яких обмежується зменшенням вільного місця на диску і наявністю графічних, звукових та інших ефектів;
- небезпечні віруси, які можуть привести до серйозних збоїв в роботі комп’ютера;
- дуже небезпечні, в алгоритм роботи яких свідомо закладені процедури, які призводять до псування програм, знищення файлів. Повну інформацію про численні відомі віруси можна знайти на сайтах фірм, виробників антивірусних програм.

Антивірусні програми

Для боротьби з комп’ютерними вірусами використовуються антивірусні програми. Оскільки комп’ютери простих користувачів, не підключені до Інтернету, незабаром перестануть існувати, першою програмою, що встановлюється на ПК після установки операційної системи, має бути антивірусна система. Інтернет нині – джерело підвищеної вірусної небезпеки, особливо при відвідуванні хакерських, розважальних сайтів, соціальних мереж та їм подібних!

До складу сучасних антивірусних систем входять, як правило, декілька програмних модулів:

- сканер перевірки заданих дисків, папок або файлів за вказівкою користувача, за розкладом або за командою програми монітору, програми перевірки електронної пошти або скриптів;
- програма монітору, що запускає програму-сканер для перевірки всіх програм, що запускаються на ПК, і файлів даних, що відкриваються, починаючи з моменту запуску ОС;
- програми перевірки файлів електронної пошти і скриптів у файлах Інтернету, що поступають на комп'ютер;
- програма оновлення антивірусних баз сигнатур;
- центр керування, що дозволяє задати розклад сканування папок, оновлення баз та інші параметри роботи.

В антивірусних сканерах для пошуку відомих вірусів використовуються два основні методи: сигнатурний пошук і евристичний аналіз.

Сигнатурою або маскою вірусу є деяка постійна послідовність коду, специфічна для цього конкретного вірусу. Всі сигнатури розміщені в антивірусній базі – спеціальному сховищі, в якому програма-антивірус зберігає характерні коди шкідливих програм.

Метод евристичного аналізу перевіряє не код підозрілого файлу, а його дії. Для того, щоб розмножуватися, вірус повинен копіювати своє тіло в пам'ять, відкривати інші виконувані файли і записувати туди своє тіло, записувати дані в сектори жорсткого диска і так далі. Є характерні дії і у мережевого черв'яка – доступ до адресної книги і сканування жорсткого диску на предмет виявлення адрес електронної пошти. Завдяки цьому евристичний аналізатор здатний виявити навіть ті шкідливі коди, сигнатури які ще невідомі.

Антивірусні сканери можна розділити на дві категорії – **універсальні та спеціалізовані**. Універсальні сканери розраховані на пошук і знешкодження всіх типів вірусів незалежно від операційної системи, на роботу в якій розрахований сканер. Спеціалізовані сканери призначені для знешкодження обмеженого числа вірусів або тільки одного їх класу, наприклад макро-вірусів. Спеціалізовані сканери, розраховані тільки на макро-віруси, часто

виявляються найбільш зручним і надійним рішенням для захисту систем документообігу в середовищах Microsoft Word і Excel.

До переваг універсальних сканерів відноситься велика кількість вірусів, які вони “знають” і можуть виявляти і знешкоджувати. Недоліки - відносно невисока швидкість роботи і великий розмір антивірусної бази, яку необхідно систематично оновлювати (бажано щодня або частіше).

Існують також CRC-сканери, принцип роботи яких заснований на підрахунку контрольних сум файлів і системних секторів. Ці CRC – суми потім зберігаються у базі даних цієї програми, як, втім, і деяка інша інформація: довжини файлів, дати їх останньої модифікації і тому подібне. При наступному запуску CRC-сканери звіряють дані, що містяться у базі даних, з реально підрахованими значеннями. Якщо інформація про файл, записана у базі даних, не співпадає з реальними значеннями, то CRC-сканери сигналізують про те, що файл був змінений або заражений вірусом.

У локальних мережах підприємств можуть використовуватися спеціальні заходи боротьби з проникненням вірусів: заборона користувачам, що не мають прав адміністрування, використовувати пристрої для роботи з оптичними дисками, флеш-картами, USB-флеш пам’яттю та ін.; захист комп’ютерів міжмережевим екраном (брандмауером); налаштування проксі-сервера з доступом користувачів тільки до дозволених ресурсів локальної мережі та Інтернету. Стратегічним компонентом захисту даних від вірусів є систематичне резервне копіювання інформації.

Сертифікацією антивірусних програм займається ICSA – International Computer Security Association – Міжнародна асоціація з комп’ютерної безпеки (заснована в 1992 році). У тестуваннях, ICSA Labs, що проводяться, використовується шкідливий код як з власної колекції, так і із списку WildList (список вірусів неформальної міжнародної організації WildList Organization International). За результатами досліджень продуктам видається сертифікат ICSA – його отримують ті антивіруси, які здатні виявити 100% вірусів із списку WildList, що з’явилися за місяць до випробувань, і не менше 90% вірусів з власної колекції ICSA.

У списку сертифікованих ICSA антивірусів нині велика кількість програм більш ніж 20-ти різних виробників, деякі з програм приведені в таблиці 13.1.

Таблиця 13.1

Антивірусні програми, сертифіковані ICSA для Windows

Продукт	Виробник
AntiVirus with Spy Sweeper	Webroot Software, Inc
eScan Internet Security	MicroWorld Technologies, Inc.
ESET NOD32 Antivirus	Eset spol. s.r.o.
Microsoft Forefront Client Security	Microsoft Corporation
Microsoft Security Essentials	Microsoft Corporation
Norton Security Suite	Norman ASA
Panda for Desktops	Panda Security
Panda Internet Security	Panda Security
PC Tools Spyware Doctor with AntiVirus	PC Tools Software
Webroot Internet Security Essentials	Webroot Software, Inc.

Антивірусні програми постійною удосконалюються, тому в їх підсистемах оновлення може бути заданий параметр завантаження не лише оновлень антивірусних баз, але і програми антивірусного сканера.

Нині найбільш великі фірми, виробники антивірусних програм, випускають їх у складі комплексних систем забезпечення комп'ютерної безпеки.

Одна з лідируючих компаній в цій області Лабораторія Касперського (http://www.kaspersky.ru/business products).

Деякі фірми випускають безкоштовні антивірусні програми для домашнього використання або пробні версії з обмеженою функціональністю. Наприклад, німецька фірма AVIRA пропонує викачати безкоштовну версію – програму AntiVir Personal Edition Classic (http://www.free-av.com), ця програма захищає користувача не лише від вірусів, черв'яків і троянів, але також від програм-жартів, руткітів та їм подібних. Шпигунські та рекламні модулі ця версія виявляти не вміє, подібний захист є тільки в платній версії AntiVir Personal Edition Premium і версіях продукту для робочих

станцій і серверів. Ці версії також можна безкоштовно викачати для попереднього ознайомлення з ними впродовж 30 днів.

Подібна ситуація з антивірусними програмами Avast! – версію для домашнього використання Home Edition можна завантажити через Інтернет і використовувати безкоштовно після реєстрації користувача й отримання ключа для використання через електрону пошту. Інші версії – Avast! Professional Edition, Avast! Server Edition та інші є платними.

Засоби захисту комп'ютерних мереж

При роботі в мережі важливим є захист інформації від несанкціонованого доступу зловмисників, що намагаються дістати доступ до комп'ютера в локальній мережі або мережі Інтернет (атаки хакерів, віруси, спами тощо). З цієї причини локальні мережі потребують засобів для заборони проникнення ззовні.

В якості таких засобів захисту широко застосовуються міжмережеві екрани (рис. 13.3):

- **Brandmauer** (від нім. *brand* – горіти, *mauer* – стіна), найчастіше вживається як **брандмауер**.
- **Firewall** (від анг. *fire* – вогонь, *wall* – стіна), вживається як "**фаєрвол"**.

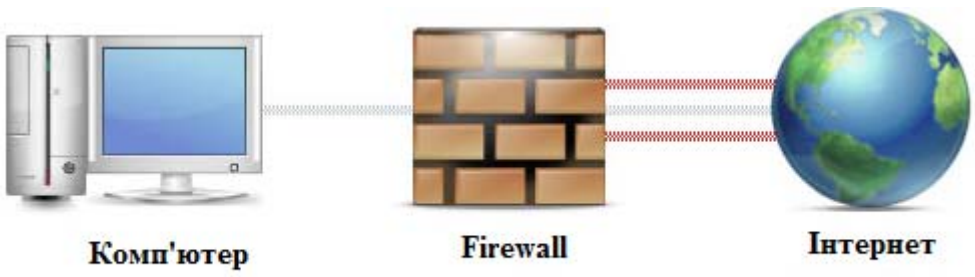

Рис 13.3. Міжмережевий екран

Брандмауер – це система чи комбінація систем, яка дозволяє розділити мережу на дві або більше частин та реалізувати набір правил, що визначають умови проходження пакетів з однієї частини в іншу. Як правило, такий поділ проводиться між мережею Internet і локальною корпоративною мережею, хоча його можна провести й усередині. В результаті брандмауер пропускає через себе весь трафік і для кожного вхідного пакета приймає рішення пропускати його чи ні. Для того, щоб брандмауер міг приймати такі

рішення, йому необхідно визначити певний набір правил, виходячи з політики безпеки даної установи (корпоративної мережі).

Система Firewall з маршрутизатором та шлюзом.

Вибір оптимальних міжмережевих екранів (firewalls) – це, головним чином, питання правильного співвідношення між вимогами користувачів стосовно доступу та вірогідності несанкціонованого доступу. В ідеалі система має запобігати будь-якому несанкціонованому вторгненню. Однак, враховуючи широкий спектр Web-сервісів, необхідних користувачам, ftp, telnet, SNMP, Network File System, IP телефонія, електронна пошта тощо, досягнути певного рівня запобігання несанкціонованому втручанню дуже важко.

Насправді мірою ефективності firewall є зовсім не його здатність відмовити в наданні сервісів, а його властивість надавати сервіси користувачам у ефективному, структурованому й надійному середовищі. Системи firewall мають аналізувати вхідний та вихідний мережевий трафік і правильно визначати, які з транзакцій є санкціонованими, а які – ні.

Фахівці вважають, що багато проблем, пов’язаних з безпекою Internet, можна відкоригувати або зробити менш серйозними за допомогою широко відомих методів та засобів контролю безпеки – хостів firewall.

Firewall може значно підвищити рівень безпеки мережі, в той же час дозволяючи доступ до необхідних служб Internet. Приклад firewall, що включає маршрутизатор з фільтрацією пакетів і прикладний шлюз.

Необхідно зазначити, що firewall – це не просто маршрутизатор або сукупність систем, котрі гарантують безпеку мережі. Firewall – це ще й метод гарантування безпеки; він допомагає реалізувати більш надійну систему безпеки, котра визначає, яким службам і який саме доступ може бути наданий. Основна мета полягає в тому, щоб контролювати потік даних в мережі, що захищається. Ця система реалізовує такий порядок доступу до мережі, коли зв’язок здійснюється через firewall, де йому можна запобігти.

Firewall-системою може бути маршрутизатор, ЕОМ, хост або сукупність хостів, встановлених спеціально для захисту мережі або під мережі, протоколів і служб, які можуть бути використані зловмисниками з хостів поза мережею. Firewal, як правило, розташовують на шлюзі, наприклад, на місці з'єднання мережі з Internet, однак ці системи можуть розміщуватися і на шлюзах більш низьких рівнів для захисту меншої сукупності хостів або підмереж.

Головний аргумент на користь firewall полягає в тому, що без них системи зазнають небезпеки з боку таких незахищених систем, як NFS (Network File System) і NIS (Network Information System), а також атак з будь-яких інших хостів внутрішньої мережі. В середовищі, яке не має firewall, безпека мережі цілком залежить від безпеки хоста, підключеного до Internet. У свою чергу всі хости мають бути об'єднані для досягнення однакового рівня безпеки. Чим більше підмережа, тим менше вона здатна підтримувати у всіх хостів однаковий рівень безпеки. Оскільки помилки і недоліки в системі безпеки стають звичайним явищем, порушення виникають не в результаті складних атак, а через помилки в конфігурації та ненадійності паролів.

Використання firewall має чимало переваг, дозволяє підвищити загальний рівень безпеки.

Firewall може значно підвищити безпеку мережі та зменшити ризик для хостів підмережі, фільтруючи явно незахищені служби, внаслідок чого мережеве середовище зазнає меншого ризику, оскільки через firewall зможуть пройти тільки вказані протоколи.

Firewall може перешкоджати отриманню із захищеної підмережі або впровадженню в захищену підмережу даних за допомогою будь-яких вразливих служб, типу NFS. Це дозволяє запобігати використанню таких служб зовнішніми порушниками та використовувати їх з набагато меншим ризиком.

Firewall можуть також забезпечити захист від таких атак, як маршрутизація джерела або спроби направити маршрути до об'єктів через перепризначення ICMP (Internet Control Message Protocol). Firewall може відкидати всі пакети з маршрутизацією джерела, а потім інформувати адміністраторів про інциденти.

Firewall також дає можливість контролювати доступ до систем мережі. Одні хости можуть залишитися вразливими ззовні, а інші, навпаки, - бути надійно захищеними від небажаного доступу. Можна заборонити зовнішній доступ до всіх своїх хостів, крім деяких, наприклад, залишити доступними тільки поштові або інформаційні сервери, що визначається політикою доступу, заснованої на принципі мінімальної достатності. Організація firewall може потребувати менших витрат у тому випадку, якщо всі або значна частина модифікованих програм і додаткові програми безпеки будуть розміщені у firewall-системах, а не розподілені по багатьох хостах. Зокрема, системи одноразових паролів та інші додаткові програми аутентифікації можна вмістити на firewall, замість того, щоб встановлювати їх у кожну систему, до якої необхідний доступ з мережі Internet.

Інші методи розв’язання проблеми мережевої безпеки, наприклад, система Kerberos, вимагають модифікації кожної хост-системи. Звичайно, організація firewall не відміняє застосування Kerberos та інших методів, оскільки вони мають ряд переваг, і в певних ситуаціях можуть бути більш придатними, ніж firewall, однак реалізація такого захисту полегшується тим, що для цього створення достатньо лише запуску спеціальних програм. Для деяких додатків конфіденційність має величезне значення, оскільки інформація, що вважається нешкідливою, насправді може містити ключі, якими може скористатися порушник. З допомогою firewall деякі об’єкти блокують такі служби, як finger і DNS. Finger відображає інформацію про користувачів: коли вони востаннє входили в систему, чи прочитали вони пошту тощо. Ці дані програми finger можуть бути корисними і для порушника, який дізнається, наскільки часто система використовується, список активних користувачів, і чи можна її атакувати, не привертаючи уваги.

Firewall можна використати також для блокування інформації DNS таким чином, щоб імена і IP-адреси систем були недоступні з Internet. Дехто вважає, що таким чином приховується інформація, якою в іншому випадку могли б скористатися злочинці. Коли весь

доступ до Internet та з Internet здійснюється через firewall, він може реєструвати всі спроби доступу і надавати необхідну статистику про використання Internet. Firewall також може повідомляти про небезпеку за допомогою відповідних сигналів тривоги, які спрацьовують у разі якоїсь підозрілої діяльності або спроб зондування чи атаки.

Ведення статистики про використання мережі та спроби порушень важливе з цілого ряду причин. Головне – знати, наскільки протистоїть firewall зондуванню й атакам, визначити, чи здійснюваний ним контроль є адекватним.

Статистика використання мережі також має значення для отримання даних про визначення потреб мережі та проведення аналізу ризику.

Аналіз основних схем застосування firewall дозволяє виділити такі його три типи: фільтруючі маршрутизатори, шлюзи прикладного рівня та шлюзи мережевого рівня. Відповідно до цього, можна виділити такі основні схеми:

- firewall на основі фільтрації пакетів;
- firewall на основі простого шлюзу;
- firewall екранований шлюз,
- firewall екранована підмережа.

Система Firewall на основі фільтрації пакетів

Firewall, заснований на фільтрації, певно є найбільш поширеним і найлегшим для реалізації. Однак він має безліч недоліків і менш ефективний порівняно з усіма іншими схемами, що розглядаються далі. Як правило, firewall цього типу складається з фільтруючого маршрутизатора, розташованого між Internet і підмережею, яка перебуває під захистом. Такий маршрутизатор сконфігурований для блокування або фільтрації відповідних протоколів та адрес. При цьому комп’ютери, що знаходяться в цій мережі, як правило, мають прямий доступ до Internet, тоді як велика частина доступу з Internet до них блокується. Зазвичай блокуються такі небезпечні системи, як NIS, NFS та Windows. Firewall, заснованим на фільтрації пакетів, властиві ті ж недоліки, що й фільтруючим маршрутизаторам, однак вони стають більш

серйозними по мірі того, як вимоги до безпеки об'єкта, який знаходиться під захистом, зростають. Ось деякі з таких недоліків:

• слабкі або взагалі відсутні можливості реєстрації події. Адміністратору важко визначити чи скомпрометований маршрутизатор і дізнатися чи не зазнавав він атаки;

• вичерпне тестування правил фільтрації дуже трудомістке або неможливе. Це означає, що мережа залишається незахищеною від неопротестованих типів атак;

• достатня складність правил фільтрації, через що у певних випадках ситуація може стати некерованою;

• для кожного хосту, безпосередньо пов'язаного з Internet, потрібні свої засоби посиленої аутентифікації.

Фільтруючий маршрутизатор може реалізувати будь-яку з політик безпеки. Однак, якщо маршрутизатор не фільтрує по порту джерела і номер вхідного та вихідного портів, то реалізація політики "заборонено все, що не дозволено" може бути ускладнена. Якщо необхідно реалізувати саме цю політику, то треба використати маршрутизатор, що забезпечує найбільш гнучку стратегію фільтрації.

Така схема організації захисту краща, ніж firewall на основі фільтруючого маршрутизатора.

Firewall на основі шлюзу складається з хост-системи з двома мережевими інтерфейсами, при передаванні даних між якими і здійснюється фільтрація. Крім того, для забезпечення додаткового захисту між мережею, що знаходиться під захистом й Internet, можна вмістити фільтруючий маршрутизатор. Це створює між шлюзом і маршрутизатором внутрішню екрановану підмережу, яку можна використати для розміщення систем, доступних ззовні, наприклад, інформаційних серверів.

На відміну від фільтруючого маршрутизатора, шлюз повністю блокує трафік IP між мережею Internet і мережею, що знаходиться під захистом. Послуги і доступ надаються тільки повноважними серверами, розташованими на шлюзі. На перший погляд, це проста організація firewall, але дуже ефективна. Деякі шлюзи не використовують повноважних служб, зате вимагають, щоб

користувачі здійснювали доступ до Internet тільки за допомогою реєстрації на шлюзі. Такий тип шлюзу є не досить поширеним, оскільки підключення до нього великої кількості користувачів може призвести до помилок, а це полегшить атаку для зловмисника.

Згаданий тип firewall реалізовує політику безпеки, коли заборонено все, що не дозволено, оскільки робить недоступними всі служби, крім тих, для яких визначені відповідні повноваження. Шлюз ігнорує пакети з маршрутизацією джерела, тому передати в захищену підмережу такі пакети неможливо. Цим досягається високий рівень безпеки, оскільки маршрути до захищеної підмережі стають відомі тільки firewall і приховані від зовнішніх систем, оскільки firewall не буде передавати назовні інформації DNS.

Для створення простої схеми шлюзу необхідно встановити повноважні служби для TELNET і FTP та централізовану електронну пошту, за допомогою якої firewall буде отримувати всю пошту, яка відправляється в мережу, що знаходиться під захистом, а потім пересилати її хостам мережі. Цей firewall може вимагати від користувачів застосування засобів посиленої аутентифікації, реєструвати доступ, а також спроби зондування і атак системи порушником.

Firewall, що використовує шлюз, як і firewall з екранованою підмережею, який буде розглянутий далі, надає можливість відділити трафік, пов’язаний з інформаційним сервером, від іншого трафіка між мережею й Internet. Інформаційний сервер можна розмістити в під мережі між шлюзом і маршрутизатором. Передбачаючи, що шлюз надає інформаційному серверу відповідні повноважні служби (наприклад, ftp, gopher або http), маршрутизатор може запобігти прямому доступу до firewall і забезпечити, щоб цей доступ здійснювався тільки через firewall. Якщо дозволений прямий доступ до інформаційного серверу, то його ім’я й IP-адреса стають відомими за допомогою DNS. Розміщення інформаційного серверу до шлюзу збільшує безпеку

основної мережі, оскільки, навіть проникнувши в інформаційний сервер, злочинець не зможе отримати доступ до систем мережі.

Недостатня гнучкість шлюзу може виявитися неприйнятною для деяких мереж. Оскільки блокуються всі служби, крім певних, доступ до інших служб здійснити неможливо; системи, що вимагають доступу, треба розташовувати до шлюзу зі сторони Internet. Маршрутизатор можна використати для утворення підмережі між шлюзом і маршрутизатором, і тут же можна вмістити системи, що вимагають додаткових служб.

Необхідно зазначити, що безпека хост-систем, які використовуються як шлюз, має підтримуватися на дуже високому рівні, оскільки будь-яка прогалина в її захисті може призвести до серйозних наслідків. Якщо шлюз вивести з ладу, злочинець буде мати можливість проникнути в мережу, що знаходиться під захистом.

Система Firewall на основі екранованого шлюзу

Firewall на основі екранованого шлюзу є більш гнучким рішенням, ніж просто шлюз, однак ця гнучкість досягається за рахунок деякого пониження рівня безпеки. Firewall на основі екранованого шлюзу об’єднує фільтруючий маршрутизатор і прикладний шлюз, розміщений зі сторони підмережі, що знаходиться під захистом. Прикладний шлюз можна також розмістити до маршрутизатора зі сторони Internet без шкоди для безпеки. Розміщення прикладного шлюзу з зовнішнього боку сприятиме тому, що саме він буде зазнавати атак в якості помилкової цілі для зловмисника.

Для прикладного шлюзу необхідний тільки один мережевий інтерфейс. Повноважні служби прикладного шлюзу мають забезпечувати сервіс TELNET, FTP та інших повноважних служб для систем мережі, що знаходиться під захистом. Маршрутизатор фільтрує інші протоколи, не дозволяючи їм досягнути прикладного шлюзу і систем мережі. Він забороняє (або дозволяє) трафік за такими правилами: трафік з Internet до прикладного шлюзу дозволений, весь інший трафік з Internet заборонений,

маршрутизатор забороняє будь-який трафік з мережі, крім того, що походить від прикладного шлюзу.

На відміну від firewall, заснованого на звичайному шлюзі, для прикладного шлюзу потрібний тільки один мережевий інтерфейс і не потрібно окремої підмережі між прикладним шлюзом і маршрутизатором. Це дозволяє зробити firewall більш гнучким, але менш безпечним, оскільки існує потенційна можливість передавання трафіка в обхід прикладного шлюзу безпосередньо до систем мережі. Служби, що не мають відповідних повноважень, можна вважати надійними в тому значенні, що ризик використання цих служб вважається допустимим. Наприклад, можна дозволити передавати через маршрутизатор до систем мережі служби, що зазнають меншого ризику, наприклад NTP. Якщо системи мережі вимагають доступу DNS до Internet, то його можна дозволити. У цьому випадку firewall може реалізувати обидві політики безпеки одночасно, залежно від того, які типи служб доступні системам мережі.

При використанні firewall з екранованим шлюзом виникають дві проблеми. По-перше, тепер є дві системи – маршрутизатор і прикладний шлюз, які треба ретельно конфігурувати. Як уже було зазначено, правила, котрим підлягає фільтруючий маршрутизатор, можуть бути дуже складними для здійснення конфігурації, важкими для перевірки і можуть призводити до помилок і “дір” у системі захисту. Проте, оскільки маршрутизатор вимагає дозволу прикладного трафіка тільки для прикладного шлюзу, набір правил може бути менш складним, ніж для мережі, що використовує firewall тільки з фільтруючим маршрутизатором.

Друга проблема полягає в тому, що гнучкість конфігурації допускає можливість порушення політики безпеки (як це було вказано для firewall з фільтруючим маршрутизатором). Ця проблема більш серйозна, ніж у випадку firewall з простим шлюзом, оскільки є технічна можливість здійснювати трафік в обхід шлюзу.

Схема firewall, яка складається з екранованої підмережі, становить собою різновид firewall з екранованим хостом. Його

можна використати для розміщення кожного компонента firewall у окремій системі, що дозволить збільшити пропускну здатність і гнучкість за рахунок деякого ускладнення архітектури. Кожна система, що входить у цей firewall, потрібна тільки для виконання конкретного завдання.

Для створення внутрішньої, екранованої підмережі використовується підмережа “DMZ"(“демілітаризована зона”), яка містить прикладний шлюз, однак вона може також включати в себе інформаційні сервери й інші системи, що вимагають доступу, ретельно контролюється. Зовнішній маршрутизатор забороняє доступ з Internet до систем екранованої підмережі та блокує всі трафіки до Internet, що йдуть від систем. Маршрутизатор можна використати і для блокування будь-яких інших вразливих протоколів, які не повинні передаватися хостам екранованою підмережею або від них. Внутрішній маршрутизатор здійснює трафік до систем екранованої підмережі та від них за такими правилами:

• трафік від прикладного шлюзу до систем мережі дозволений;

• трафік електронної пошти від серверу електронної пошти до систем мережі дозволений;

• прикладний трафік від систем мережі до прикладного шлюзу дозволений;

• трафік електронної пошти від систем мережі до серверу електронної пошти дозволений;

• трафік ftp, gopher;

• весь інший трафік заборонений.

Таким чином, усі системи мережі є недосяжними безпосередньо з Internet і навпаки. Головною відмінністю є те, що маршрутизатори використовуються для направлення трафіка до конкретних систем, що виключає необхідність для прикладного шлюзу виконувати роль маршрутизатора. Це дозволяє досягнути більшої пропускної здатності. Отже, firewall з екранованою підмережею найбільше підходить для мереж з великими обсягами трафіка або з дуже високою швидкістю обміну.

Наявність двох маршрутизаторів є доцільним, оскільки для того, щоб проникнути безпосередньо в систему мережі, злочинець має подолати обидва маршрутизатори. Прикладний шлюз, сервер електронної пошти та інформаційний сервер мають бути налаштовані таким чином, щоб тільки вони були доступні з Internet.

У базі даних DNS, досяжній для зовнішніх систем, не повинні використовуватися імена інших систем. Прикладний шлюз може містити програми посиленої аутентифікації. Очевидно, він вимагає складного конфігурування, однак використання для прикладних шлюзів і фільтрів окремих систем спрощує конфігурування й управління.

Firewall з екранованою підмережею, як і firewall з екранованим шлюзом, можна зробити більш гнучким, допускаючи трафік між Internet і системами мережі для деяких перевірених служб. Однак така гнучкість може призвести до необхідності зробити деякі виключення з політики безпеки, що ослабить ефективність firewall. У багатьох випадках більше підходить firewall з простим шлюзом, який не допускає ослаблення політики безпеки, оскільки через нього не можуть пройти служби, що не мають відповідних повноважень. Однак там, де пропускна здатність і гнучкість мають велике значення, краще використовувати firewall з екранованою підмережею.

Замість того, щоб пересилати служби безпосередньо між Internet і системами мережі, можна розмістити системи, що вимагають цих служб, прямо в екранованій підмережі. Наприклад, мережа, що не допускає трафіка Windows або NFS між Internet і системами мережі, може розмістити системи, що вимагають доступу, в екрановану підмережу. Ці системи можуть, як і раніше, зберігати доступ до інших систем мережі через прикладний шлюз. Такий варіант підходить для мереж, що вимагають високого рівня безпеки.

Схемі firewall з екранованою підмережею властиві два недоліки.

По-перше, існує принципова можливість доступу в обхід прикладного шлюзу. Це вірно і для випадку firewall з екранованим

шлюзом, однак firewall з екранованою підмережею допускає розміщення в ній систем, що вимагають прямого доступу до служб Internet.

Другим недоліком є те, що маршрутизатори потребують великої уваги для забезпечення необхідного рівня безпеки. Як вже відмічалося, фільтруючі маршрутизатори складно конфігурувати, і через помилки можуть виникнути недоліки в безпеці всієї мережі. Чимало мереж дозволяють доступ через модеми, розміщені в різних точках мережі. Такий доступ є потенційно небезпечним і може знищити весь захист, який забезпечується firewall.

Отже, варто наголосити, що комп'ютерні системи, включені в Internet, потерпають від значного ризику бути атакованими порушниками або стати плацдармом для атаки на інші системи. Це зумовлене рядом недоліків, властивих певним службам Internet. На думку фахівців, системи firewall у даний час можуть служити досить надійним додатковим бар'єром для захисту мереж від зовнішніх атак (зі сторони Internet). Хоч застосування систем firewall і дозволяє захиститися від цілого ряду загроз, вони також не є досконалими, крім того, існують загрози, яким вони не можуть протистояти.

Різні схеми застосування firewall призначені для гарантування безпеки комп'ютерним системам від загроз певного виду. Для успішної протидії загрозам зі сторони Internet мають застосовуватися різні схеми конфігурації firewall, відповідно до прийнятої політики безпеки.

Як свідчить практика, firewall не може протистояти атакам, які йдуть у обхід цієї системи. Так, наприклад, firewall не може перешкодити витоку інформації з системи при копіюванні даних. Крім того, системи класу firewall не спроможні забезпечити захист від автономних реплікативних програм, таких, як віруси і програмні закладки. І зрештою, firewall – системи, беззахисні перед "атакою даних", коли в систему, що уражається під виглядом мережевої пошти, копіюється яка-небудь програма, котра після цього запускається на виконання.

Як висновок треба зазначити, що основна мета firewall – не допустити несанкціонованого доступу в локальну мережу через Internet шляхом перегляду пакетів даних і використання спеціальних засобів підтвердження повноважень для додатків. Перегляд пакетів проводиться з метою блокування підозрілих видів трафіка. Функції підтвердження повноважень, які орієнтовані на прикладні програми, здійснюють повний контроль і перевірку на допустимість усіх вхідних і вихідних даних. Усе більше фахівців у галузі захисту інформації приходить до розуміння, що використання firewall для захисту локальної мережі значно зменшує ризик несанкціонованого втручання через Internet.

Ряд firewall дозволяють також організовувати віртуальні корпоративні мережі Virtual Private Network (VPN), що об'єднують декілька локальних мереж, включених у Internet в одну віртуальну мережу. Така система дозволяє організувати прозоре для користувачів з'єднання локальних мереж, зберігаючи секретність і цілісність інформації, що передається за допомогою шифрування. При цьому під час передавання даних по Internet шифрується не лише інформація, призначена для користувача, але і мережева – мережеві адреси, номери портів тощо. VPN створює захищене з'єднання через Internet. Зараз подібне використовується в багатьох технологіях.

Контрольні запитання:

1. Як визначити завантаженість ОС Windows?
2. З якою метою проводиться перевірка жорсткого диску?
3. В яких випадках виникає необхідність відновлення системи?
4. Яку небезпеку несуть в собі троянські програми та черв'яки?
5. Що таке спам?
6. При яких умовах антивірусна система забезпечує максимальний рівень захисту?

7. Дайте визначення поняттю міжмережевий екран та назвіть його складові частини.
8. Назвіть призначення та основні функціональні можливості брандмауера Windows.

ЛАБОРАТОРНА РОБОТА № 14

Тема: Спеціалізовані засоби інформаційної техніки

Мета роботи: ознайомити студентів із спеціалізованими засоби інформаційної техніки та їх функціональним призначенням.

Порядок виконання роботи:

1. Ознайомитися з теоретичними відомостями.
2. Знайти та дати короткий опис інших спеціалізованих засобів інформаційної техніки.
3. Результат записати у звіт.
4. У звіті дайте письмові відповіді на контрольні запитання.

Теоретичні відомості

Спеціалізовані засоби інформаційної техніки – це сукупність апаратних засобів, програмного забезпечення спрямованих на виконання однієї або декількох задач пов’язаних з отриманням, збереженням, обробкою та відтворенням, передачею інформаційних потоків різного типу.

Спеціалізовані засоби інформаційної техніки в залежності від їх призначення поділяються на:

1.Пристрої введення інформації.

2. Пристрої виведення інформації.

3. Комбіновані пристрої.

13.1 Пристрої введення інформації

Дигітайзер – це пристрій введення графічної інформації, що має порівняно вузьке застосування для деяких спеціальних цілей. Назва дигітайзер походить від англійського digit-цифра. Тобто по-українському їх можна назвати просто “оцифровувачі”. Утім, є і більш благозвучна назва цифрові перетворювачі. Зазвичай дигітайзери являють собою планшет. Тому такі пристрої часто називають графічними планшетами. Застосовується такий

дигітайзер для покрапіксельного координатного введення графічних зображень у системах автоматичного проектування, у комп'ютерній графіці й анімації. Треба відзначити, що це далеко не найшвидший і зручний спосіб побудови малюнків і креслень, особливо у випадку складної геометрії. Але зате графічний планшет забезпечує найбільш точне введення графічної інформації в комп'ютер.

Дигітайзер може мати розмір робочого поля А1 яке має вигляд креслярської дошки. Зазвичай поряд з робочим полем пристрою знаходяться кнопки керування. Для введення інформації використовується спеціальне перо або координатний пристрій з "прицілом", підключений кабелем до планшета або з безпровідною передачею даних. Сам дигітайзер підключається до комп'ютера кабелем через USB-порт. Роздільна здатність таких графічних планшетів не менше 100 dpi (точок на дюйм).

У деяких дигітайзерах введення інформації може відбуватися без спеціального пера або прицілу, оскільки робоча поверхня планшета має чутливість до натиснення пера, заснованою на використанні п'єзоелектричного ефекту. При натисненні на точку, в межах робочої поверхні планшета, під якою прокладена сітка з найтонших провідників, на пластині п'єзоелектрика виникає різниця потенціалів. Координати цієї точки зчитується програмою, яка сканує сітку провідників. Ця програма запам'ятовує координати точок і показує графічні об'єкти на моніторі.

У графічних планшетах та інтерактивних моніторах (рис. 14.1) для малювання використовується пристрій введення (безпровідне перо), натиснення якого на поверхню робочого поля зчитується з використанням технології електромагнітного резонансу.

Основні завдання, що вирішуються з використанням цих пристроїв:

- малювання;
- редагування фотографій і зображень;
- створення колажів, листівок і календарів;
- комп'ютерна анімація і 3D-моделювання;
- робота в мультимедійних додатках;

- аудіо- та відеомонтаж;
- розпізнавання рукописного тексту та інші.

Рис.14.1 Дигітайзер та інтерактивний монітор

Музичні пристрої введення

До музичних пристроїв введення передусім відноситься MIDI-клавіатура, що підключається до ПК через його звукову плату. Наприклад, клавіатура M-Audio Pro Keys 88 (рис. 13.2) – повнорозмірне (88 клавіш з професійною рояльною механікою) цифрове піаніно і MIDI-контролер. Існують інші музичні пристрої, що підключаються до ПК, наприклад, M-Audio Black Box – потужний ефект-процесор, здатний моделювати 12 відомих гітарних передпідсилювачів зі вбудованою drum-машиною і гітарним тюнером.

Рис.14.2 MIDI-клавіатура

WEB-камера – є цифровим пристроєм, що забезпечує відеозйомку, оцифровування, стискання, збереження та передачу цифрового відео по комп'ютерній мережі (рис. 14.3).

Рис.14.3 Web-камера

До складу web-камери входять наступні компоненти: ПЗС-матрица, об'єктив, оптичний фільтр, плата відеозахоплення, блок компресії (стискання) відеозображення, центральний процесор і вбудований web-сервер, ОЗП, флеш-пам'ять, мережевий інтерфейс, послідовні порти.

Деякі моделі камер мають поворотні пристрої і можуть виконувати відеоспостереження на 360^0, а також мають варіфокальний об'єктив, яким можна керувати по мережі.

Підключатися камери можуть до мережевого комутатора або концентратора, або напряму до комп'ютера.

Пристрої розпізнавання голосу. Говорячи про системи розпізнавання голосу, можна відзначити два аспекти – одна справа дізнатися голос окремої людини, а інше перетворити його в текст, який можна бачити на екрані монітора або зберігати в пам'яті комп'ютера. Системи першого типу відносно прості, вони не перетворюють людський голос в текст, а всього лише його "дізнаються" (відрізняють від сказаного іншим, не "вникаючи в сенс"). Частіше за все це використовується в якості пароля для захисту окремих даних або доступу до комп'ютера. Системи

другого типу набагато складніше та інтелектуальніше, вони повинні не просто перетворювати одні сигнали в інші (аналогові сигнали в цифрові), але і представляти звукову інформацію як в пам'яті комп'ютера, так і на екрані монітора в текстовому вигляді. Розв'язання цієї проблеми дозволить людині спілкуватися з комп'ютером найбільш природним для нього способом – за допомогою голосу. Однак такі системи вимагають, щоб їх попередньо налаштували на тембр голосу тієї людини, або декількох чоловік, які будуть з ними працювати.

Системи введення (датчики). Останнім часом у пристроях введення застосовуються нові технології. Як приклад можна навести пристрої, які відстежують положення зіниць очей. Використовуючи такий пристрій, можна поглядом переміщати курсор по екрану. Це дає можливість використовувати комп'ютер практично повністю паралізованим людям. При використанні комп'ютера для управління робототехнічних комплексів, пристроями введення служать всілякі датчики (температурні, що визначають інтенсивність кольору, положення, радіаційний фон, вологість повітря, загазованість та інші).

Пристрої виведення інформації

Плотер (графічний пристрій) – пристрій виведення графічної інформації (креслень, схем, карт, плакатів) на паперові та інші листові носії розміром А1 (594х841 мм), А0 (841х1189 мм) і великих форматів за рахунок рулонної подачі паперу.

До недавнього часу використовувалися різні типи пір'яних плотерів, проте нині в основному використовуються широкоформатні струменеві плотери, з термічною і п'єзоелектричною технологіями друку, лазерні та LED-плотери (див. рис. 14.4).

Принцип дії лазерних плотерів аналогічний описаному для принтерів. LED-плотери замість лазеру і системи призм використовують лінійку піксельних світловипромінюючих напівпровідникових світлодіодів (light emitted diod – LED). Загальний принцип створення зображення той же, що і в лазерних принтерах – зображення формується на зарядженому барабані із селеновим або органічним фоточутливим покриттям, до якого

притягується сухий тонер, який потім переноситься на папір, що проходить під барабаном. LED-плотери відносяться до класу растрових, кожній точці рядка зображення відповідає свій світлодіод (наприклад, при роздільній здатності 400 точок на дюйм, лінійка для формату А1 24” складається з 9600 діодів.

Рис.14.4 Плотер

До плотерів різного виду призначення існують наступні вимоги:

• САПР (системи автоматизованого проектування) – виведення чорно-білих і кольорових креслень; відтворення тонких ліній і дрібних об’єктів; досить висока швидкість виведення; можливість друку на папері низької якості;

• ГІС (геоінформаційні системи) – висока точність, максимально допустима похибка викреслювання карт дорівнює 0,2 мм;

• повно-кольоровий широкоформатний друк зображень – можливість друку як на папері, так і на синтетичних матеріалах з використанням водного чорнила або чорнила на органічних розчинниках (сольвентний друк).

У свою чергу, третій тип плотерів можна підрозділити за сферами використання:

- друк художніх зображень,
- професійна поліграфія,
- фотодрук,

- рекламний та оперативний друк.

Основні технічні характеристики плотерів:

- розмір паперу;
- роздільна здатність при друці, точок на дюйм;
- швидкість друку, м/г або $м^2$/г;
- пам’ять плотера;
- наявність жорсткого диску та його об’єм;
- інтерфейс підключення (USB, IEEE-1284, IEEE-1394a, Ethernet 10/100/1000).

Принтер 3D-друку

3D-друк є однією з форм технології адитивного (рос. *аддитивность*, англ. *additivity*, нім. *Addition, Additivität*) – властивість величин, яка полягає в тому, що значення величини, яка відповідає цілому об’єкту, дорівнює сумі значень величин, що відповідають його частинам, незалежно від того, яким чином поділено об’єкт.) виробництва, де тривимірний об’єкт створюється шляхом накладання послідовних шарів матеріалу. 3D-принтери, як правило, швидші, більш доступні і прості у використанні, ніж інші технології адитивного виробництва. 3D-принтери пропонують розробникам продуктів можливість друку деталей і механізмів з декількох матеріалів та з різними механічними і фізичними властивостями за один процес складання.

3D-друк часто називають “магічною” технологією. Ви розробляєте щось у CAD (система автоматизованого проектування), запускаєте на друк, і через кілька хвилин постає повністю сформований об’єкт. У реальності 3D процес друку вимагає багато ручної праці. Величезна кількість попередньої підготовки і подальшої обробки необхідна для якості надрукованої деталі.

З 2003 року спостерігається значне зростання у продажі 3D принтерів. Крім того, вартість 3D-принтерів знизилася. Технологія також знаходить застосування в сфері ювелірних виробів, взуття, промислового дизайну, архітектури, проектування та будівництва (AEC), автомобільної, аерокосмічної, стоматологічних та медичних галузях.

3D-принтер – пристрій, що використовує метод створення фізичного об'єкта на основі віртуальної 3D-моделі (рис. 14.5).

Рис.14.5 3D-принтер

Комбіновані пристрої

Стример (від англ. streamer) або **стрічковий накопичувач** (від **англ.** tape drive) – запам'ятовуючий пристрій на принципі магнітного запису на стрічковому носієві, з послідовним доступом до даних, за принципом дії аналогічний побутовому магнітофону. Використовуються для створення архівних даних і дозволяють зберігати на одній касеті з магнітною стрічкою до декількох сотень гігабайтів.

Основне призначення: запис і відтворення інформації, архівація та резервне копіювання даних (рис. 14.6).

Рис.14.6 Стример

Існує два базових методи занесення інформації на магнітну стрічку в стримерах:

Лінійний магнітний запис

При використанні даного методу запису, дані записуються на стрічку у вигляді декількох паралельних доріжок. Стрічка має

можливість рухатися в обох напрямках. Зчитуюча та записуюча головки під час зчитування та запису перебувають у статичному положенні. З досягненням кінця стрічки головки зміщуються на наступну доріжку, а стрічка починає рухатися в протилежному напрямку. Технологія за суттю, аналогічна побутовому аудіомагнітофону. Можливе застосування декількох головок, які працюють з декількома доріжками одночасно *(багатодоріжковий стример).*У сучасних пристроях цей метод домінує.

Похило-рядковий магнітний запис (“Helical Scan”)

Якщо використовується даний метод, то блок головок запису-відтворення (БГЗВ) розміщується на обертаючомуся барабані, повз якого механізм простягає стрічку, при зчитуванні та записі. Запис при цьому ведеться в одному напрямку. Залежно від використовуваного формату запису стрічка проходить навколо БВГ (блоку відтворюючих головок) під деяким кутом, причому вісь самого циліндра БГЗВ (блоку головок запису відтворення) також нахилена під невеликим кутом до стрічки. Стрічка при запису/зчитуванні рухається в одному напрямку. Тут застосовується так звана металевопорошкова стрічка (metal-particle tape). Даний спосіб запису передбачає наявність коротких поперечних доріжок на поверхні стрічки, а технологія аналогічна побутовому відеомагнітофону (формату VHS). Похило-рядковий метод був винайдений, щоб домогтися більш високої щільності запису, ніж при лінійному методі, без необхідності зменшення зазору в головках і збільшення швидкості руху стрічки (проте в даний час ці технічні обмеження подолані і в рамках лінійного методу).

Магнітна картка

Магнітна картка – це пластикова картка, яка відповідає специфікаціям ISO, має на зворотному боці магнітну стрічку з інформацією об’ємом близько 100 байт пам’яті, яка прочитується спеціальним зчитуючим пристроєм та місце для підпису (рис. 3.2). Такі магнітні картки широко використовуються в усьому світі як банківські кредитні та платіжні картки. Стрічка може бути виготовлена для різних потужностей магнітного поля, і за цим

параметром розрізняють низько (300 ерст.) і висококоерцитивні (до 4000 ерст.) магнітні стрічки. Для стандартних зчитуючих пристроїв (рідерів) магнітна стрічка має ширину 12,7мм (0.4” дюйми) і розташовується на відстані 4 мм від краю картки.

У режимі off-line інформація про покупку, зроблену власником картки, нікуди не передається, а зберігається в торговому терміналі або електронній касі. Через певний проміжок часу термінал зв’язується з банком і передає всю інформацію на хост. Для друку чеків використовуються спеціальні пристрої – імпринтери, або POS-термінали.

Картки з магнітною смугою широко використовуються в банківських платіжних системах, транспортних системах та в системах ідентифікації і безпеки.

Магнітний запис є одним з найпоширеніших на сьогоднішній день способів нанесення інформації на пластикові картки, але він не забезпечує необхідного рівня захисту від підробок. А це є критичним моментом в платіжних системах, які використовують магнітні картки. Останнім часом спостерігається значне збільшення використання як платіжного засобу смарт-карток.

Смарт-картка

Смарт-картка (smart – інтелектуальна, або “розумна”) – це звичайна пластикова картка з вбудованою мікросхемою. Ступінь “інтелектуальності” мікросхеми може бути дуже різним – від найпростішого контролера зчитування/запису даних в електронну пам’ять картки, до мікропроцесора, що має розвинуту систему команд, вбудовану файлову систему і т.п.

Смарт-картка здатна виконувати складні операції з обробки інформації та зберігати її. Звідси і назва – Smart (“інтелектуальна”) картка.

Смарт-картка була винайдена французом Роланом Морено в середині 70-х років, але тільки в кінці 80-х років технологічні досягнення зробили її достатньо зручною і недорогою для практичного використання.

Існує декілька видів класифікації смарт-карток (наприклад, за типом мікросхеми, яка в ній вбудована та за функціями, які виконує

смарт-картка). Найпростіші типи карток містять тільки пам'ять, більш складніші є мікро-ЕОМ, яка забезпечує великий набір сервісних функцій. Розглянемо деякі з них.

Залежно від типу мікросхеми, вбудованої в картку, розрізняють такі типи смарт-карток:

- картки з програмованим постійним пристроєм для запам'ятовування (PROM) є найпростішим типом карток. Основне їх застосування – розрахунки за телефонні розмови;
- картки з енергозалежною пам'яттю та можливістю перепрограмування (EEPROM) дозволяють перезаписувати інформацію, що зберігається в них. Основне їх застосування – зберігання індивідуальних даних;
- картки із захищеним перепрограмуванням пам'яті, які забезпечують доступ для зчитування/запису тільки після введення спеціального коду. Основне їх застосування – розрахункові картки або зберігання захищених індивідуальних даних;
- багатофункціональні картки містять великий об'єм енергозалежної пам'яті, можливість перепрограмування, а також спеціальний мікропроцесор і вбудовану операційну систему, що забезпечує набір сервісних функцій. Ці картки можуть застосовуватися для будь-яких додатків, включаючи розрахунки користувача.

За призначенням можна виділити:

Картки-лічильники – застосовуються для такого типу розрахунків, коли потрібне віднімання фіксованої суми за кожну платіжну операцію. Такі картки ще називають наперед оплаченими картками.

Найбільшого поширення в світі набули телефонні картки пам'яті, власники яких можуть зробити певну кількість телефонних дзвінків, оскільки в телефонах-автоматах одиниця часу розмови має фіксовану ціну. Картка застосовується в контактному режимі (мікросхема фізично контактує із зчитуючим пристроєм). При кожному новому контакті число "дозволених дзвінків" у пам'яті картки зменшується на один біт пам'яті. Після того, як ліміт сплачених дзвінків вичерпаний, картка перестає функціонувати.

Картки пам’яті – використовуються для збереження інформації. Сама їх назва говорить про те, що мікросхема картки містить тільки пристрій, що запам’ятовує. Є два типи таких карток: *із захищеною і незахищеною пам’яттю.*

У картках з незахищеною пам’яттю немає обмежень щодо зчитування або запису даних. Використовувати такі картки як платіжні дуже небезпечно. Достатньо легально придбати таку картку, скопіювати її пам’ять на диск, а далі після кожної покупки відновлювати її пам’ять копіюванням початкового стану даних з диска. Зрозуміло, що таку операцію може виконати лише кваліфікований програміст, але практика показує, що людей, здатних на це, достатньо.

У картках із захищеною пам’яттю використовується спеціальний механізм для дозволу зчитування/запису або вилучення інформації. Щоб провести ці операції, необхідно ввести спеціальний секретний код (а іноді й не один). Як правило, картки із захищеною пам’яттю містять область, куди записуються ідентифікаційні дані. Ці дані не можуть бути змінені, що дуже важливо для забезпечення неможливості фальсифікації картки. Картки із захищеною пам’яттю можна використовувати, як платіжний засіб, а також для зберігання конфіденційних даних.

Мікропроцесорні картки схожі на картки пам’яті, але мікросхема містить мікропроцесор (чіп-модуль), що робить ці картки дійсно інтелектуальними.

Мікропроцесор – це мікросхема (інтегральна схема, чіп) (рис. 14.7), яка здатна зберігати великий обсяг інформації і виконувати арифметичні та логічні операції. Мікропроцесорні картки, практично є мікрокомп’ютерами зі своїм процесором, оперативною та постійною пам’яттю і навіть операційною системою. Як правило, у такі картки вбудовані криптографічні засоби, що забезпечують шифрування інформації.

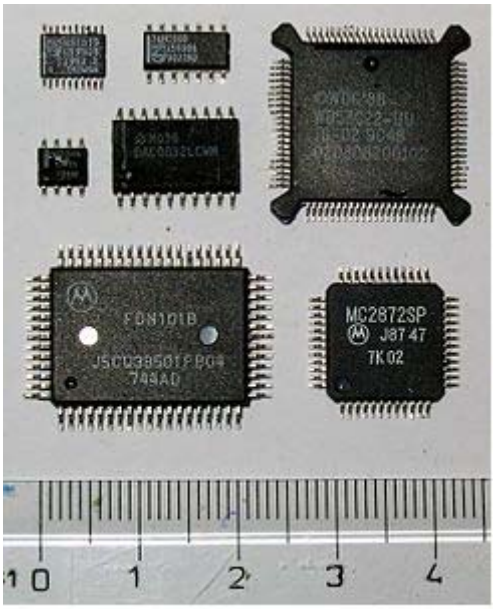

Рис.14.7 Інтегральні схеми смарт-карток

Мікропроцесори, встановлені на смарт-картках, мають такі основні характеристики:

- тактова частота до 5 Мгц;
- об’єм оперативної пам’яті (ОЗП) до 256 байт (для виконання команд);
- об’єм постійної пам’яті (ПЗП) до 10 Кбайт (для зберігання операційної системи);
- ємність енергозалежної пам’яті з можливістю перепрограмування до 8 Кбайт.

У картку вбудовується спеціалізована операційна система, що забезпечує великий набір сервісних операцій і засобів безпеки.

Операційна система картки підтримує файлову систему, що передбачає розмежування доступу до інформації.

Картки забезпечують різний спектр сервісних команд. Для банківської діяльності ці засоби ведення електронних платежів.

До спеціальних засобів відносяться можливість блокування роботи з карткою. Розрізняють два види блокування: при пред’явленні неправильного транспортного коду і при несанкціонованому доступі.

За доступом розрізняють контактні і безконтактні смарт-картки. Найбільшого поширення сьогодні набули контактні картки, де процес зчитування/запис відбувається при безпосередньому механічному контакті картки з рідером.

Безконтактні пластикові картки є одним з основних елементів систем радіочастотної ідентифікації об'єктів (RFED-систем), які працюють на відстані від рідера (разом з чіпом у пластиковій картці розміщується антена, за допомогою якої проводиться прийом і випромінювання радіохвиль).

Зчитування і перезапис інформації на картці здійснюється за допомогою радіосигналу, який передається рідером і приймається індукційною котушкою картки. Завдяки "індуктивній підзарядці" мікросхема картки отримує можливість передавати інформацію назад на рідер.

Відстань між карткою і зчитуючим пристроєм може коливатися від кількох міліметрів до декількох метрів залежно від конструкції, яка використовується.

Основними перевагами безконтактних пластикових карток є:

- висока надійність і необмежений ресурс картки (забезпечується відсутністю необхідності механічного контакту між карткою і рідером);
- велика швидкість обміну інформацією між карткою та рідером (мсек);
- можливість багаторазового використання ;
- висока надійність зберігання інформації (інформація на картці не схильна до дії зовнішніх полів і може зберігатися до 10 років);
- високий ступінь захисту від підробок (картку практично не можливо підробити);
- можливість багатофункціональності безконтактних пластикових карток (картки можуть нести великий об'єм перезаписуваної інформації та використовуватися одночасно для цілого ряду додатків).

Контрольні запитання:

1. На які групи поділяються спеціалізовані засоби інформаційної техніки?
2. Назвіть різницю між функціональними можливостями дигітайзеру та інтерактивного монітору.
3. Назвіть типи та принцип роботи плотерів.
4. Назвіть галузі адитивного виробництва де отримали найбільш розповсюдження 3D-принтери.
5. Які технології запису використовуються у стримерах?
6. Яке устаткування можна віднести до спеціалізованих засобів інформаційної техніки та наведіть їх приклади.

Використана література

1. *Борисенко А. А.* Локальная сеть. Просто как дважды два / А. А. Борисенко. – М. : Эксмо, 2009. – 192 с.
2. *Карпов В. Е.* Основы операционных систем. Курс лекций. / В. Е. Карпов, К. А. Коньков. – М. : Интернет-университет информационных технологий, 2005. – 536 с.
3. *Крис Фейли.* Мастерская Windows, XP, Vista и Office / Крис Фейли. – М., 2009. – 608 с.
4. *Леонов В.* Самоучитель работы на компьютере / В. Леонов. – М., 2009. – 352 с.
5. *Леонтьев В. П.* Новейшая энциклопедия персонального компьютера 2010 / В. П. Леонтьев. – М. : ОЛМА Медиа Групп, 2010. – 800 с.
6. *Пол Мак-Федрис*. Microsoft Windows 7. Полное руководство / Пол Мак-Федрис. – М. : Вильямс, 2009. – 800 с.
7. *Рудненко В. Д.* Практичний курс інформатики / В. Д. Рудненко, О. М. Макарчук, М. О. Патланжоглу ; за ред. В. М. Мадзігона. – К. : Фенікс, 2007. – 304 с.
8. *Симонович С. В.* Информатика. Базовый курс / С. В. Симонович. – СПб., Питер, 2007.
9. *Старков В.* Архитектура персонального компьютера: организация, устройство, работа / В. Старков. – М. : Горячая Линия - Телеком, 2009. – 536 с.
10. pcnews.ru, computer-news.ru, www.hardvision.ru, news.ferra.ru, www.ixbit.com,www.computerra.ru,www.compulenta.ru, www.comp-life.ru – комп'ютерні новини.
11. www.itnews.ru, http://subscribe.ru/catalog/comp, www.studioit.ru, www.it-top.ru, www.cnews.ru, www.it-technologies.ru, www.worldnewsit.ru – новини інформаційних технологій.
12. www.3dnews.ru – Daily Digital Digest, все о комп'ютерах – огляд, аналітика, новини Hardware, новини Software, мережі, програмне забезпечення, енциклопедія та інші тематичні розсилання.

Зміст

Наукове видання

Тетяна Миколаївна Слабошевська,
Ігор Миколайович Смекалін,
Сергій Микитович Яшанов

Практикум з експлуатації інформаційної техніки

Частина ІІ

Навчально-методичний посібник

Технічне редагування – Т. М. Ветраченко
Верстка – Т. С. Меркулова

ВИДАВНИЦТВО
НАЦІОНАЛЬНОГО ПЕДАГОГІЧНОГО УНІВЕРСИТЕТУ
ІМЕНІ М. П. ДРАГОМАНОВА

Підписано до друку *14 червня* 2012 р.
Формат 60х84/16 Папір офісний. Гарнітура Times New Roman.
Ум. друк. арк. 7,06. Об.-вид. арк. 4.04.
Наклад 300 прим. Зам №
Віддруковано з оригіналів

Видавництво Національного педагогічного університету
імені М. П. Драгоманова. 01601, м. Київ-30, вул. Пирогова, 9.
Свідоцтво про реєстрацію ДК № 1101 від 29.10.2002 (044) 234-75-87
Віддруковано в друкарні Національного педагогічного університету
імені М. П. Драгоманова (044) 239-30-26