Розділ 4
СЛУЖБОВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

У цьому розділі ви дізнаєтеся про:

- шкідливе програмне забезпечення, комп'ютерні віруси, історію їх виникнення та класифікацію;
- програми для боротьби зі шкідливим програмним забезпеченням;
- засоби профілактики від ураження шкідливими програмами;
- принципи стискання даних;
- необхідність і засоби архівації даних;
- запис даних на оптичні диски;
- форматування та копіювання дисків.

4.1. Комп'ютерні віруси та антивірусні програми

1. Що відбудеться, якщо в банку будуть переплутані дані про рахунки клієнтів?
2. Що відбудеться, якщо комп'ютери каси продажу квитків працюватимуть у 10 разів повільніше?
3. Що відбудеться, якщо дані з вашої медичної картки будуть втрачені?
4. Що таке біологічний вірус? До яких наслідків може призвести ураження людини вірусом?

Комп'ютерні віруси та інші шкідливі програми

Крім корисних програм, які допомагають користувачеві опрацьовувати дані, існують і шкідливі програми. Для шкідливих комп'ютерних програм характерно:

- швидке розмноження шляхом приєднання своїх копій до інших програм, копіювання на інші носії даних, пересилання копій комп'ютерними мережами;
- автоматичне виконання **деструктивних дій**, які вносять дезорганізацію в роботу комп'ютера:
  - знищення даних шляхом видалення файлів певних типів або форматування дисків;
  - внесення змін у файли, зміна структури розміщення файлів на диску;
  - зміна або повне видалення даних із постійної пам'яті;
  - зниження швидкодії комп'ютера, наприклад за рахунок заповнення оперативної пам'яті своїми копіями;
  - постійне (***резидентне***) розміщення в оперативній пам'яті від моменту звернення до ураженого об'єкта до моменту вимкнення комп'ютера і ураження все нових і нових об'єктів;
  - примусове перезавантаження операційної системи;
  - блокування запуску певних програм;
  - збирання і пересилання копії даних комп'ютерними мережами, наприклад пересилання кодів доступу до секретних даних;

- використання ресурсів уражених комп'ютерів для організації колективних атак на інші комп'ютери в мережах;
- виведення звукових або текстових повідомлень, спотворення зображення на екрані монітора тощо.

За рівнем небезпечності дій шкідливі програми розподіляють на:

- ***безпечні*** – проявляються відео та звуковими ефектами, не змінюють файлову систему, не ушкоджують файли і не виконують шпигунські дії;
- ***небезпечні*** – призводять до перебоїв у роботі комп'ютерної системи: зменшують розмір доступної оперативної пам'яті, перезавантажують комп'ютер тощо;
- ***дуже небезпечні*** – знищують дані з постійної та зовнішньої пам'яті, виконують шпигунські дії тощо.

За принципами розповсюдження і функціонування шкідливі програми розподіляють на (рис. 4.1):

- ***комп'ютерні віруси*** – програми, здатні саморозмножуватися і виконувати несанкціоновані деструктивні дії на ураженому комп'ютері. Серед них виділяють:
  - ***дискові (завантажувальні) віруси*** – розмножуються копіюванням себе в службові ділянки дисків та інших змінних носіїв, яке відбувається під час спроби користувача зчитати дані з ураженого носія;
  - ***файлові віруси*** – розміщують свої копії у складі файлів різного типу. Як правило, це файли готових до виконання програм із розширенням імені **exe** або **com**. Однак існують так звані ***макровіруси***, що уражують, наприклад, файли текстових документів, електронних таблиць, баз даних тощо;
- ***хробаки (черв'яки) комп'ютерних мереж*** – пересилають свої копії комп'ютерними мережами з метою проникнення на віддалені комп'ютери. Більшість черв'яків поширюються, прикріпившись до файлів електронної пошти, електронних документів тощо. З ураженого комп'ютера хробаки намагаються проникнути на інші комп'ютери, використовуючи список електронних поштових адрес або іншими способами. Крім розмноження, черв'яки можуть виконувати деструктивні дії, які характерні для шкідливих програм;
- ***троянські програми*** – програми, що проникають на комп'ютери користувачів разом з іншими програмами, які користувач «отримує» комп'ютерними мережами. Шкідливі програми він отримує «в подарунок», так як у свій час захисники Трої отримали в подарунок від

Рис. 4.1. Схема класифікації шкідливих програм за принципами розповсюдження і функціонування

греків дерев'яного коня, всередині якого розміщалися грецькі воїни. Звідси й назва цього виду шкідливих програм. Як і інші шкідливі програми, троянські програми можуть виконувати зазначені вище деструктивні дії, але в основному їх використовують для виконання шпигунських дій.

Значна частина шкідливих програм у початкові періоди зараження не виконує деструктивних дій, а лише розмножується. Це так звана ***пасивна фаза*** їхнього існування. Через певний час, у визначений день або по команді з комп'ютера в мережі шкідливі програми починають виконувати деструктивні дії – переходять в ***активну фазу*** свого існування.

Серед вірусів виділяють ті, що використовують спеціальні способи приховування своїх дій і знаходження в операційній системі комп'ютера:

- ***поліморфні (мутанти)*** – віруси, які при копіюванні змінюють свій вміст так, що кожна копія має різний розмір; їх важче визначити, використовуючи пошук за відомою довжиною коду вірусу;
- ***стелс*** (англ. *stealth* – хитрість, викрут, *stealth virus* – вірус-невидимка) – віруси, що намагаються різними засобами приховати факт свого існування в операційній системі. Наприклад, замість дійсного об'єкта, ураженого вірусом, антивірусній програмі надається для перевірки його неуражена копія.

Розглянемо значення властивостей різних видів шкідливих програм на конкретних прикладах (табл. 4.1).

Таблиця 4.1. **Значення властивостей різних видів шкідливих програм**

Властивість	***Значення властивості***		
Ім'я	**Win95.CIN** або **Чорнобиль**	**Win32.HLLM. MyDom.based**	**Trojan.Plastix** або **Trojan.Win32. Krotten**
Тип	Комп'ютерний вірус	Хробак комп'ютерних мереж	Троянська програма
Дата створення	1998 р.	Січень 2004 р.	Жовтень 2005 р.
Розмір	Близько 1 Кбайт	29 149 байтів та інші	53 964 байти
Опис розмноження	При запуску програми, інфікованої цим вірусом, залишається резидентно в оперативній пам'яті і заражає всі файли з розширенням імені **exe**, які запускає на виконання користувач	Копіює себе в папку, в яку встановлено операційну систему, наприклад **C:\ Windows\ System32**, у файли з іменами **svrhost.exe** та **taskgmgr.exe**	Пропонує відвідати сайт за адресою **gsm-card.iscool. net** і завантажити універсальний генератор кодів для поповнення абонентських рахунків мобільних операторів України. При відвідуванні вказаного сайта вірус копіюється в папку **C:\Windows\System32** під іменем **services.db.exe** та в папку **C:\WINDOWS\inf** під іменем **svchost.exe**

Продовження таблиці 4.1

Властивість	***Значення властивості***		
Деструктивні дії, які виконує вірус	• Стає активним у певний день – 26 квітня кожного року (за що і дістав назву **Чорнобиль**). • Видаляє всі дані з жорсткого диска. • Видаляє дані з **BIOS**	• Змінює налаштування операційної системи для автоматичного завантаження себе в оперативну пам'ять. • Шукає файли з поштовими адресами і розсилає за ними свої копії. • Вивантажує з оперативної пам'яті програми і модулі, які відповідають за безпеку комп'ютера. • Може мати модуль завантаження інших шкідливих програм	• Змінює налаштування операційної системи для автоматичного завантаження себе в оперативну пам'ять. • Змінює значення атрибута системних папок **Windows** та **Program Files** на *приховані*. • Блокує роботу програм відновлення ОС. • Знищує практично всі команди меню **Пуск**. • Знищує всі значки з **Робочого стола**. • Відкриває вікно з повідомленням (рис. 4.2)

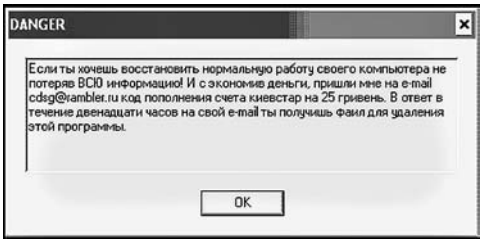

Рис. 4.2. Вікно повідомлення троянської програми

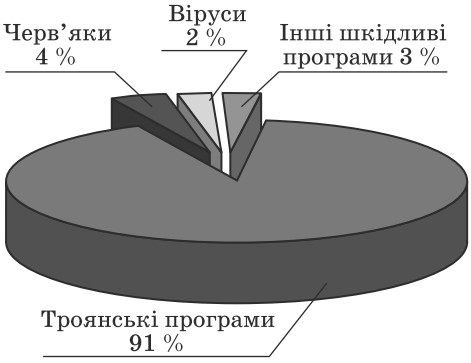

Рис. 4.3. Діаграма розповсюдженості шкідливих програм

На сьогодні найбільш розповсюдженими серед шкідливих програм є ***троянські програми*** та ***черв'яки*** (рис. 4.3).

У світі існує сотні тисяч шкідливих програм. Вони завдають значної шкоди як індивідуальним користувачам, так і підприємствам та організаціям. Тільки за 2007 р. ці програми нанесли збитків світовій індустрії на суму понад 135 млрд доларів. Щороку збитки зростають на 10–15 %. П'ятірка країн, що найбільше «відзначилися» в створенні шкідливих програм, на сьогодні виглядає так:

1. Росія – 27,89 %;
2. Китай – 26,52 %;
3. США – 9,98 %;
4. Бразилія – 6,77 %;
5. Україна – 5,45 %.

Дуже сумно, що і наша країна вийшла на перші місця по створенню шкідливих програм. У зв'язку з широким розповсюдженням шкідливих

програм в Україні, як і в більшості країн світу, введена кримінальна відповідальність за «несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації» (стаття 361 Кримінального кодексу України). Також кримінальна відповідальність уведена за «створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку» (стаття 361-1 Кримінального кодексу України).

Часто для позначення всіх видів шкідливих комп'ютерних програм використовується узагальнена назва – *комп'ютерний вірус*.

Антивірусні програми

Для захисту даних і пристроїв комп'ютера від шкідливих програм використовується спеціальне програмне забезпечення – **антивірусні програми**.

Розрізняють такі антивірусні програми:

- ***детектори*** **(*сканери*)** – програми, що здатні проводити перевірку комп'ютера на наявність шкідливих програм і повідомляти користувача про їх наявність. У ході перевірки програми використовують дані з так званих ***антивірусних баз*** – сукупності даних про відомі на даний момент часу шкідливі програми і способи боротьби з ними;
- ***лікарі*** – програми, що здійснюють «лікування» комп'ютерів від виявлених шкідливих програм, тобто знешкоджують їх, а при неможливості знешкодження можуть видаляти заражені об'єкти або розташовувати їх у спеціальних папках. Як і детектори, лікарі використовують антивірусні бази для оновлення даних про способи боротьби зі шкідливими програмами;
- ***монітори*** – програми, що постійно (*резидентно*) знаходяться в оперативній пам'яті комп'ютера з моменту завантаження операційної системи і перевіряють усі файли і диски, до яких іде звертання, блокують дії, що можуть ідентифікуватись як дії шкідливої програми;
- ***ревізори*** – програми, які аналізують стан системних файлів і папок та порівнюють їх зі станом, що був на початку роботи антивірусної програми. При певних змінах, які характерні для діяльності шкідливих програм, програма-ревізор виводить повідомлення про можливість ураження шкідливою програмою;
- ***блокувальники*** – програми, які аналізують обмін даними комп'ютера користувача з іншими комп'ютерами в мережі. Програма блокує з'єднання з певним комп'ютером у мережі, якщо фіксує дії, які характерні для шкідливих комп'ютерних програм, і виводить повідомлення про намагання їх проникнення на комп'ютер користувача.

Сучасні антивірусні програми – це комплексні програми, що мають властивості всіх перерахованих видів антивірусних програм. Такими є

програми **Dr.Web**, **Антивірус Касперського (AVP)**, **AVG Free Edition**, **NOD32**, **NORTON AntiVirus**, **Panda** та інші. Вони можуть виконувати такі дії:

- знаходячись резидентно в оперативній пам'яті, перевіряти на наявність шкідливих програм усі об'єкти, до яких звертається користувач;
- проводити ***евристичний аналіз*** (грец. εὑρηχα – знайшов) – здійснювати пошук нових шкідливих програм за стандартними діями вже відомих вірусів;
- перевіряти вхідну і вихідну електронну пошту, поштові бази даних;
- виконувати пошук шкідливих програм у архівах;
- виконувати лікування об'єктів – видаляти коди шкідливих програм із файлів, системних областей, відновлюючи їх функціональність;
- виконувати за встановленим розкладом повну перевірку комп'ютера, оновлення антивірусних баз та інше;
- створювати карантинну зону для підозрілих об'єктів;
- блокувати несанкціоновані користувачем дії по відправленню даних на віддалений комп'ютер, запуску програм, завантаженню з віддалених комп'ютерів різноманітних даних

та інше.

Антивірус Касперського

Якщо **антивірусна програма Касперського** встановлена, то при включенні ПК вона буде однією з перших автоматично завантажуватись в оперативну пам'ять комп'ютера і виконувати операції з перевірки наявності шкідливих програм та блокування їхніх дій. При цьому в **Області сповіщень** з'явиться значок програми **Антивірус Касперського**  .

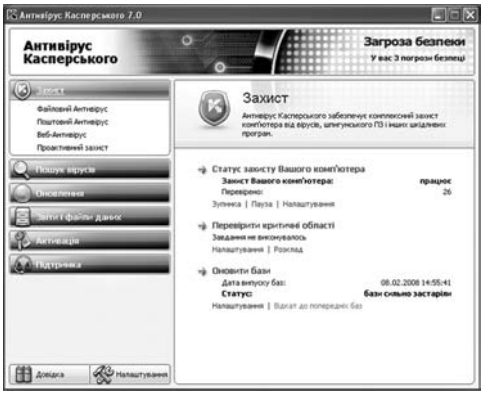

Рис. 4.4. Вікно програми **Антивірус Касперського**

Для відкриття вікна програми (рис. 4.4) потрібно виконати ***Пуск ⇒ Усі програми ⇒ Антивірус Касперського ⇒ Антивірус Касперського*** або двічі клацнути на значку програми в **Області сповіщень.**

Для ефективної боротьби з новими вірусними загрозами потрібно постійно оновлювати антивірусні бази. За замовчуванням у програмі **Антивірус Касперського** встановлено автоматичне оновлення антивірусних баз кожного дня із сайта компанії. Якщо користувач хоче змінити цей розклад, то потрібно змінити налаштування програми (рис. 4.5).

Для здійснення перевірки всього комп'ютера потрібно виконати такий алгоритм:

1. Запустити програму **Антивірус Касперського.**
2. Вибрати у лівій частині вікна програми команду **Пошук вірусів.**
3. Вибрати у лівій частині вікна програми команду **Мій Комп'ютер.**
4. Вибрати у правій частині вікна кнопку **Пошук вірусів.**

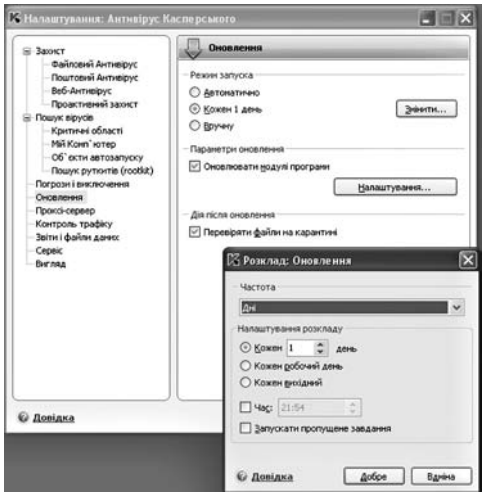

Рис. 4.5. Вікна налаштування оновлення і розкладу оновлення **Антивірусу Касперського**

Для здійснення перевірки одного із зовнішніх запам'ятовуючих пристроїв необхідно виконати такий алгоритм:

1. Запустити програму **Антивірус Касперського.**
2. Вибрати у лівій частині вікна програми команду **Пошук вірусів.**
3. Установити у правій частині вікна позначки прапорців біля тих об'єктів, які потрібно перевірити.
4. Вибрати у правій частині вікна кнопку **Пошук вірусів.**

Перевірку об'єктів операційної системи – зовнішніх запам'ятовуючих пристроїв, папок, файлів простіше виконувати, використовуючи контекстне меню цих об'єктів. Для цього у контекстному меню об'єкта слід вибрати команду **Перевірити на віруси.**

У ході перевірки у вікні програми відображається індикатор ходу перевірки та кількість перевірених файлів і знайдених шкідливих програм.

Залежно від налаштувань програма може виводити в інформаційних або діалогових вікнах повідомлення про знайдені шкідливі програми та пропонувати виконати дії над ними.

Будьте уважні до повідомлень антивірусної програми, не дозволяйте пропускати дії підозрілих програм, якщо ви не впевнені в їх безпечності. Якщо неможливо вилікувати файли, знищуйте їх.

Профілактика ураження шкідливими комп'ютерними програмами

З метою запобігання ураженню комп'ютера шкідливими програмами і збереження даних дотримуйтеся таких вимог:

- використовуйте ліцензійне програмне забезпечення;
- установіть антивірусну програму-монітор;
- регулярно здійснюйте повну перевірку комп'ютера на наявність вірусів, використовуючи одну з антивірусних програм;
- постійно оновлюйте антивірусні бази;
- регулярно проводьте резервне копіювання найбільш цінних даних;
- перед використанням перевіряйте всі змінні носії, отримані зі сторонніх джерел, антивірусною програмою;
- не відкривайте вкладені до листів електронної пошти файли, якщо вони прийшли від невідомого кореспондента;
- обмежте коло користувачів вашого комп'ютера, ознайомте їх з правилами антивірусного захисту, вимагайте їх неухильного дотримання.

Теоретичні основи створення програм, що можуть самостійно розмножуватись і виконувати дії без втручання користувача, були розроблені в ході вдосконалення теорії розробки автоматичних пристроїв (теорія автоматів) у 1950–1970-х роках. На початку 1970-х років створюються експериментальні зразки подібних комп'ютерних програм.

Однією з перших програм такого типу стала програма, що з'явилася в американській військовій комп'ютерній мережі ***APRANet***. Вона дістала назву ***Creeper*** і могла самостійно поширюватися мережею, створювати свою копію на іншому комп'ютері та виводити на монітор повідомлення «***I'M THE CREEPER: CATCH ME IF YOU CAN***» (англ. – «Я рептилія: зловіть мене, якщо зможете»). Водночас ця програма та інші аналогічні програми того часу (наприклад, **Animal**, **Xerox worm**) не завдавали шкоди, а лише доводили правильність теорії розробки комп'ютерних програм, здатних до саморозмноження й автоматичного виконання певних дій.

Одними з перших програм для нанесення шкоди комп'ютерним програмам і даним були програми **Virus 1, 2, 3** і **Elk Cloner**, розроблені для персональних комп'ютерів **Apple II**. Програма **Elk Cloner** розмножувалася шляхом запису своєї копії в початкові сектори дискет, які були на той час основним носієм даних для ПК. Її шкідливі дії зводилися до перевертання зображення на екрані монітора, мерехтіння тексту, виведення різноманітних повідомлень тощо. Приблизно в цей самий час за цим видом шкідливих програм закріплюється назва – **комп'ютерні віруси**.

У 1986 р. у світі зареєстрована перша епідемія комп'ютерного вірусу. Вірус **Brain** уражував початкові сектори дискет і за кілька місяців розповсюдився по всьому світу. Вірус був створений в Пакистані братами **Амжадом** і **Басітом Фарук Алві**.

З розвитком комп'ютерних мереж з'явилися шкідливі програми, які використовували засоби обміну даними в мережах для свого розповсюдження. У 1988 р. зареєстрована перша епідемія хробака мереж. Хробак дістав назву **хробака Moppica**. Він інфікував понад 6000 комп'ютерів, з'єднаних мережами в США, і практично паралізував їхню роботу. Загальні збитки склали 96 млн доларів. Автор хробака **Роберт Моррiс** був уперше засуджений як автор шкідливої комп'ютерної програми.

У грудні 1989 р. якийсь зловмисник надіслав 20 000 дискет за адресами, викраденими у **Всесвітній організації охорони здоров'я** та американського журналу **PC Business World**. Дискети містили троянську програму, яка після її запуску автоматично інсталювалась і вносила зміни в налаштування операційної системи. Після 90 завантажень троянська програма шифрувала імена всіх файлів і робила їх прихованими. На диску ставав доступним лише один файл із рахунком для оплати за відновлення даних. Цю подію можна вважати першою епідемією троянських програм.

Наприкінці 1980-х років створюються перші антивірусні програми **IBM Virscan**, **Norton AntiVirus**, **Dr. Solomon's Anti-Virus Toolkit** та ін.

Перевірте себе

1°. Чим характерні шкідливі комп'ютерні програми?
2°. Як поділяють шкідливі комп'ютерні програми за рівнем небезпечності дій?
3•. Опишіть класифікацію шкідливих програм за принципами розповсюдження і функціонування.
4°. Які дії можуть виконувати шкідливі комп'ютерні програми?
5•. Чим відрізняються віруси від троянських програм і хробаків мереж?
6•. Які з дій вірусів найнебезпечніші? Обґрунтуйте свою відповідь.
7•. Опишіть вимоги законодавства України по боротьбі з розповсюдженням шкідливих програм.

8°. Що таке антивірусні програми? Назвіть відомі вам антивірусні програми.
9•. Які функції антивірусних програм?
10°. Що потрібно робити для профілактики ураження шкідливими комп'ютерними програмами?
11*. Поясніть, чому серед заходів із профілактики ураження вірусом однією з основних вимог є використання ліцензійного програмного забезпечення.

Виконайте завдання

1•. Укажіть, які деструктивні дії не можуть виконувати шкідливі комп'ютерні програми: знищувати файли; знищувати мікросхеми оперативної пам'яті; пересилати дані на інший комп'ютер; змінювати логічну структуру жорсткого магнітного диска; відтворювати звукові та відео ефекти.
2°. Виконайте антивірусну перевірку зовнішнього запам'ятовуючого пристрою, вказаного вчителем.
3•. Запишіть алгоритм перевірки комп'ютера на наявність шкідливих програм.
4°. Проведіть оновлення антивірусних баз антивірусної програми, встановленої на вашому комп'ютері.
5•. Запустіть на виконання антивірусну програму та:
а) установіть такі значення параметрів перевірки: дії над ураженими об'єктами – *лікувати, а при неможливості лікування – знищувати*;
б) проведіть перевірку власної папки на наявність шкідливих програм.
6•. Запустіть на виконання антивірусну програму та:
а) установіть такі значення параметрів перевірки: рівень перевірки – *максимальний захист*; дії над ураженими об'єктами – *запитувати у користувача*; не перевіряти архівні файли;
б) проведіть перевірку диска **C**: на наявність шкідливих програм;
в) перегляньте звіт про виконання перевірки. Чи виявлені шкідливі програми? Якщо так, то до якого виду вони відносяться?
7*. Запустіть на виконання антивірусну програму та:
а) проведіть оновлення антивірусних баз;
б) визначте термін дії ліцензії на вашу програму;
в) проведіть перевірку об'єктів автозапуску і поштових баз на наявність вірусів;
г) перегляньте звіт про виконання перевірки. Чи виявлені віруси? Якщо так, то до якого виду вони відносяться?
8. Порівняйте можливості двох антивірусних програм (наприклад, **NOD32** та **Антивірус Касперського**). У чому переваги і недоліки кожної з них?
9*. Підготуйте реферат за однією з тем: «Сучасні засоби антивірусного захисту», «Що можуть і чого не можуть комп'ютерні віруси», «Міфи і реальність про комп'ютерні віруси» або «Історія комп'ютерних вірусів».

На сайті, присвяченому боротьбі з розповсюдженням шкідливих програм (http://www.viruslist.ru), ви можете отримати додаткову інформацію щодо вірусних загроз, які існують сьогодні.

Перегляньте пункт **Захист комп'ютера: основи безпеки Центру довідки та підтримки** операційної системи **Windows (*Пуск* ⇒ *Довідка та підтримка*).**

Практична робота № 5. Захист комп'ютера від вірусів

Увага! *Під час роботи з комп'ютером дотримуйтеся правил безпеки і санітарно-гігієнічних норм.*

1. Запустіть на виконання антивірусну програму.

2. Визначте за допомогою довідки, які операції виконує дана програма; до якого виду антивірусних програм її слід віднести.
3. Установіть такі значення параметрів перевірки:
   - рівень перевірки – *максимальний захист*;
   - дії над ураженими об'єктами – *запитувати у користувача*;
   - архівні файли – *не перевіряти*;
   - оновлення антивірусних баз – *один раз на тиждень автоматично*;
   - автоматична перевірка – *один раз на тиждень, у понеділок о 9-00*;
   - захист *увімкнути, завантажувати програму при ввімкненні комп'ютера*;
   - звуковий супровід дій антивірусної програми *увімкнути*.
4. Виконайте антивірусну перевірку об'єктів папки **Мої документи**. Скільки об'єктів було перевірено? Чи були знайдені віруси?
5. Проведіть перевірку дискети на наявність вірусів. Скільки об'єктів було перевірено? Чи були знайдені віруси?
6. Продемонструйте результати виконання практичної роботи вчителеві.

4.2. Стиснення та архівація даних

1. Що таке кодування повідомлень, для чого воно використовується?
2. Що таке інформаційна надлишковість?
3. Наведіть приклади систем кодування.
4. Як кодуються повідомлення при їх опрацюванні в комп'ютері?
5. Для чого призначені архіви?

Стиснення даних

Система двійкового кодування, що використовується в комп'ютерах, дуже зручна для зберігання, передавання й опрацювання даних з точки зору надійності цих процесів. Однак двійкове кодування збільшує розміри файлів порівняно з іншими системами кодування. Тому виникає потреба у зменшенні розмірів файлів для ефективнішої реалізації інформаційних процесів.

Для зменшення розмірів файлів використовують спеціальні способи стиснення даних, які називають **алгоритмами (методами) стиснення даних**. Стиснення даних використовується при створенні файлів певних типів, наприклад графічних типу JPEG або звукових типу MPEG3, для передачі файлів мережею тощо.

Стиснення даних **– це процес перекодування даних, який здійснюється з метою зменшення розмірів файлів.**

Розрізняють алгоритми стиснення, що забезпечують стиснення ***без втрати даних***, і алгоритми, що передбачають ***часткову втрату даних***. Алгоритми з частковою втратою даних використовують, коли цілісність даних не є дуже суттєвою. Наприклад, при стисненні графічних, відео, звукових файлів, оскільки органи чуття людини не здатні помітити незначну різницю у відтінках кольорів на фотографії, у відтворенні звукових або відеоданих тощо.

Кодування Хаффмана–Шенона. Цей метод часто застосовується при стисненні текстових даних. Він враховує частоту використання в конкретній мові певних літер. Наприклад, в українській мові найчастіше використовують

літери **і**, **а**, **о**, **е,** а літери **ш**, **щ**, **ф**, **х** – набагато рідше. У таких випадках використовують не 8-бітну систему кодування, а систему кодування змінної довжини, в якій символи, що трапляються частіше, кодуються 1–4 бітами, а ті, що трапляються рідше, – 7–8 бітами. Одним з прикладів такого кодування є кодування з використанням азбуки Морзе. У ній символи кодуються послідовністю крапок і тире. Наприклад, літера **а** української абетки позначається як крапка і тире, літера **м** – двома тире, літера **т** – одним тире, а літера **и** – двома крапками, літера **ш** – чотирма тире, літера **ц** – крапкою, тире, крапкою і тире, причому чим частіше використовується символ, тим менша довжина його коду.

Архівація даних

Незважаючи на підвищення надійності комп'ютерів і комп'ютерних носіїв даних, все ж повної гарантії збереження даних вони не дають. Втрата даних може призвести до дуже серйозних наслідків. Так, знищення даних про вклади та перерахування коштів клієнтів призведе до краху банку, втрата даних про продаж квитків спричинить перебої у перевезенні пасажирів, втрата результатів дослідів може звести нанівець багаторічні наукові дослідження. Навіть втрата записника з номерами телефонів друзів принесе вам значні проблеми. Тому виникає потреба у створенні копій даних. Найважливіші дані дублюють, записуючи на інші жорсткі диски, на магнітну плівку стримера, на оптичні диски тощо.

Розміри файлів, які потрібно зберігати, великі і потребують додаткових затрат. Щоб зменшити ці розміри у копіях і відповідно зменшити затрати, використовують стиснення даних. При цьому використовуються методи, що забезпечують стиснення без втрат даних.

Створення копій даних за допомогою спеціальних програм, що можуть використовувати стиснення даних, називається *архівацією*.

Програми, які використовуються для виконання архівації, називаються *архіваторами*.

Результатом роботи цих програм є **архівний файл,** або просто **архів**, який містить у стисненому або не стисненому стані файли і папки. У процесі архівації можуть бути використані додаткові заходи стосовно захисту даних від несанкціонованого доступу, наприклад встановлення пароля на доступ до даних в архіві.

Залежно від алгоритмів, за якими здійснюється архівація даних, розрізняють такі ***формати*** архівних файлів: ZIP, RAR, ARJ, CAB, LZH, ACE, ISO та ін. Найчастіше, особливо в мережі Інтернет, використовують архівні файли формату ZIP.

При виборі формату архівного файлу слід враховувати, що за даними тестів, проведених авторами підручника, формат RAR забезпечує найефективніше стиснення. Однак на процес архівації в цьому форматі затрачається більше часу.

Прикладами архіваторів є програми **WinZIP**, **WinRAR**, **7-Zip**, **Winace**, **PowerArchiver**, **ArjFolder**, **BitZipper**, **Gnochive**, **bzip2** та ін.

Одним з архіваторів є програма **WinRAR** російського програміста **Олександра Рошала**, яка використовує високоефективні алгоритми стиснення даних (рис. 4.6).

Основні функції цієї програми такі:

- створення архівів файлів і папок з можливим стисненням даних;
- додавання файлів і папок до вже існуючих архівів;
- перегляд вмісту архівів;
- заміна й оновлення файлів і папок в архівах;
- видобування з архіву всіх або тільки обраних файлів і папок;
- створення багатотомних архівів (архів розбивається на кілька окремих файлів – томів); розмір томів установлює користувач;

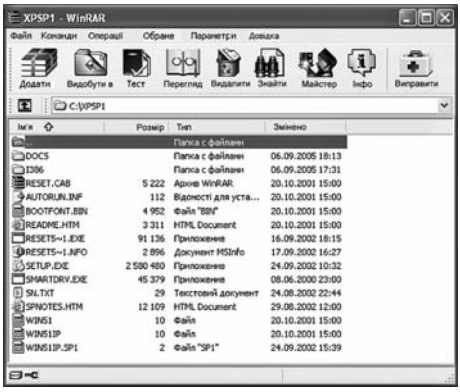

Рис. 4.6. Вікно програми **WinRAR**

- створення звичайних і багатотомних архівів, які містять програму самостійного видобування файлів і папок, без участі програми-архіватора – так званих **SFX-архівів** (англ. ***SelF eXtracting*** – самовидобування);
- перевірка цілісності даних в архівах;
- шифрування даних та імен файлів в архівах

та ін.

Програма **WinRAR** виконує всі ці операції над архівними даними формату RAR і ZIP, а також дає змогу переглядати і видобувати об'єкти з архівів форматів CAB, ARJ, LZH, TAR, GZ та ін.

Для створення архіву з використанням програми **WinRAR** потрібно виконати алгоритм:

1. Запустити програму **WinRAR** на виконання (наприклад, ***Пуск ⇒ Усі програми ⇒ WinRAR ⇒ WinRAR***).
2. Виконати ***Команди ⇒ Добавити файли до архіву*** (або вибрати кнопку **Додати** на **Панелі інструментів**).
3. Вибрати вкладку **Файли**.
4. Вибрати потрібні об'єкти для архівації, для цього використати кнопку **Додати** біля поля **Файли, що добавляються**.
5. Вибрати вкладку **Загальні** (рис. 4.7).
6. Увести в полі **Ім'я архіва** ім'я архівного файлу.
7. Указати папку, в якій буде збережено архів (кнопка **Огляд**).
8. Обрати у списку **Метод стиснення** один із шести методів стиснення: від методу *без стиснення* до методу, що забезпечує *максимальне* стиснення (при максимальному стисненні розмір архівного файлу буде найменшим, але час архівації буде найбільшим).

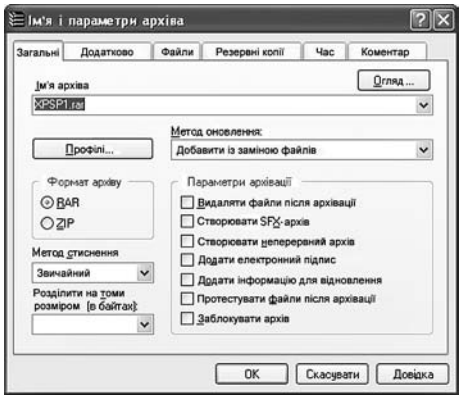

Рис. 4.7. Вікно встановлення значень параметрів архівації у **WinRAR**

9. За потреби вказати значення параметрів архівації встановленням позначок прапорців.
10. Вибрати формат архівного файлу (RAR або ZIP) вибором відповідного перемикача.
11. Якщо планується розділити архівний файл на кілька частин, то указати розмір тому в полі зі списком **Розділити на томи розміром (в байтах).**
12. Вибрати кнопку **ОК.**

Багатотомні архіви **створюються для розділення архівного файлу на кілька частин, якщо повністю архів не вміщується на одному носієві, наприклад на дискеті, на компакт-диску, на DVD-диску тощо, або якщо потрібно передати файл мережею з низькою швидкістю передавання даних.**

Для додавання об'єктів до вже існуючого архіву необхідно виконати такий алгоритм:

1. Запустити архіватор **WinRAR.**
2. Відкрити архів, до якого потрібно додати об'єкт (***Файл ⇒ Відкрити архів***).
3. Виконати ***Команди ⇒ Добавити файли до архіву*** (або вибрати кнопку **Додати** на **Панелі інструментів**).
4. Виділити у діалоговому вікні **Виберіть файли, які необхідно додати** об'єкти, які слід помістити до архіву.
5. Установити значення параметрів архівації.
6. Вибрати кнопку **ОК.**

Іншим способом додавання файлів до архіву є перетягування файлів у вікно вже існуючого архіву або на значок архіву.

Для видобування об'єктів з архіву потрібно:

1. Запустити архіватор **WinRAR.**
2. Вибрати архів, об'єкти якого потрібно видобути.
3. Виконати ***Команди ⇒ Добути у вказану папку*** (або вибрати кнопку **Видобути в** на **Панелі інструментів**).
4. Указати у діалоговому вікні **Шлях і параметри видобування** папку, в яку буде здійснено видобування.
5. Установити значення параметрів видобування.
6. Вибрати кнопку **ОК.**

Для видалення окремих об'єктів з архіву потрібно виконати такий алгоритм:

1. Запустити архіватор **WinRAR.**
2. Відкрити архів, об'єкти з якого потрібно видалити.
3. Виділити об'єкти, які необхідно видалити.
4. Виконати ***Команди ⇒ Видалити*** (або вибрати кнопку **Видалити** на **Панелі інструментів**).
5. Закрити вікно програми.

У випадках, коли потрібно перенести архівний файл на інший комп'ютер і невідомо, чи встановлений на ньому архіватор, при архівації використовують спеціальний формат архівних файлів – **SFX**. Архівні файли, створені в цьому форматі, мають розширення **exe** і включають модуль самовидобування, що дає змогу видобувати файли з архіву без архіватора.

Для захисту архіву від стороннього доступу користувач може встановити пароль доступу до архіву. Для цього необхідно на вкладці **Додатково** вибрати кнопку **Пароль** та ввести пароль і його підтвердження у відповідні поля.

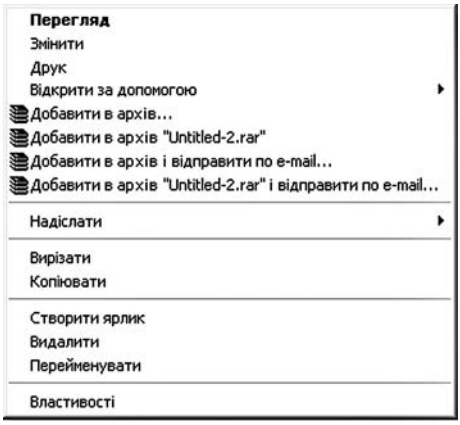

Рис. 4.8. Контекстне меню файлу, яке містить команди роботи з архівами

При інсталяції програми **WinRAR** до контекстного меню об'єктів додаються основні команди роботи з архівами (рис. 4.8).

Вибір команди **Добавити в архів** або **Добавити в архів і відправити по e-mail** відкриває вікно встановлення режимів архівації. Вибір інших двох команд – **Добавити в архів «Untitled-2.rar»** або **Добавити в архів «Untitled-2.rar» і відправити по e-mail** приводить до створення архіву із запропонованим іменем (у нашому прикладі – **«Untitled-2.rar»**).

Контекстне меню файлу архіву (рис. 4.9) містить команди видобування файлів: **Видобути файли**, **Видобути в поточну папку** або **Видобути в Untitled-2**. В останньому випадку буде створена папка з іменем архіву.

Рис. 4.9. Контекстне меню файлу архіву

Перевірте себе

1°. Для чого використовується стиснення даних?
2°. У яких випадках можливе використання стиснення з частковою втратою даних?
3•. Опишіть відомі вам методи стиснення даних.
4°. Для чого виконується архівація даних?
5•. Що таке архівація і що таке стиснення файлів? Який між ними зв'язок і яка різниця?
6°. Як називаються програми, що виконують архівацію даних? Які їх можливості?
7°. Назвіть найбільш поширені формати архівних файлів.
8°. Опишіть один із способів запуску на виконання архіватора в операційній системі **Windows**.
9°. Яку команду потрібно вибрати в **WinRAR** для створення архіву; для видобування файлів з архіву?
10•. Наведіть алгоритм створення багатотомного архіву за допомогою програми **WinRAR**. У яких випадках створюються такі архіви?
11•. У яких випадках створюються архіви, що самовидобуваються? Наведіть алгоритм їх створення.

Виконайте завдання

1°. Запустіть на виконання архіватор. Створіть архів із перших п'яти файлів з розширенням імені **doc**, що зареєстровані в папці **Архів** папки **Тема 4**. Помістіть цей файл у своїй папці.

2°. Видобудьте усі файли з файлу **Архів1.rar** з папки **Тема 4\Архів** у власну папку.

3°. Додайте до архівного файлу **Архів2.zip**, який знаходиться в папці **Тема 4\Архів**, два останні файли цієї самої папки. Збережіть змінений архів з тим самим ім'ям у власній папці.

4°. Відкрийте папку **Мої малюнки** та:
а) виділіть перші п'ять файлів із цієї папки;
б) відкрийте контекстне меню виділеної групи файлів;
в) виберіть команду створення архіву **Мої малюнки.rar**;
г) скопіюйте створений архів у попередньо створену папку **Мій архів** у папці **Мої документи**;
д) видобудьте усі файли з архіву **Мої малюнки.rar** у поточну папку, використовуючи контекстне меню скопійованого архіву.

5•. Запустіть архіватор та:
а) створіть архів із перших п'ятнадцяти файлів із розширенням **doc**, що зареєстровані в папці **Мої документи** (або з п'ятнадцяти останніх файлів із розширенням імені **doc**, що зареєстровані в папці **Архів** папки **Тема 4**);
б) установіть при архівації такі значення параметрів: ім'я архіву – *документи*; папка – *Робочий стіл*; формат архіву – *ZIP*; метод стиснення – *без стиснення*; *протестувати файли після архівації*;
в) використовуючи контекстне меню, видобудьте усі файли зі створеного архіву в папку **DOC**, яку створіть у папці **Мої документи**.

6•. Запустіть архіватор та:
а) створіть архів із перших двох файлів, що зареєстровані в папці **Зразки музики (*Мої документи ⇒ Моя музика ⇒ Зразки музики*)**, установивши при цьому такі значення параметрів архівації: ім'я архіву – *Archiv02*; формат архіву – *RAR*; *SFX*-архів; метод стиснення – *максимальний*; коментар такого змісту «Музичні файли з папки **Зразки музики**» (вкладка **Коментар**);
б) видаліть зі створеного архівного файлу **Archiv02.exe** останній файл;
в) додайте до цього архіву третій файл з папки Зразки музики (***Мої документи ⇒ Моя музика ⇒ Зразки музики***);
г) видобудьте усі файли зі створеного архівного файлу в папку **Мої документи**.

7. Проведіть дослідження щодо ефективності стиснення файлів різних типів у форматах ZIP та RAR і заповніть таблицю.

Ім'я файлу	***Розмір файлу до стиснення***	***Розміри файлів-архівів різних форматів, створених із різними значеннями параметрів стиснення***			
		RAR		***ZIP***	
		нормальний	***максимальний***	***нормальний***	***максимальний***
*.txt					
*.doc					
*.docx					
*.bmp					

8*. Підготуйте повідомлення про способи захисту даних від втрат.

9*. Підготуйте повідомлення про методи стиснення з втратами даних.

10*. Розгляньте, як виконуються основні операції над архівами з використанням архіватора **WinZIP**. Використовуйте при цьому дії «за аналогією» з **WinRAR** або скористайтеся **Довідкою**.

Практична робота № 6. Архівування та розархівування даних

Увага! *Під час роботи з комп'ютером дотримуйтеся правил безпеки і санітарно-гігієнічних норм.*

1. Запустіть на виконання архіватор **WinRAR.**
2. Створіть у своїй папці архів із перших шістнадцяти файлів з розширенням імені **doc**, що містяться в папці **Тема 4\Архів**, установивши при цьому такі значення параметрів архівації:
   - формат архіву – *RAR*;
   - метод стиснення – *швидкий*;
   - створити ***SFX***-архів;
   - протестувати файли після архівації;
   - додати інформацію для відновлення.
3. Виконайте такі дії:
   - додайте до архіву коментар з вашим прізвищем та ім'ям;
   - збережіть у архіві час створення файлів (вкладка **Час**);
   - створіть у своїй папці папку **Копія архіву**, скопіюйте в неї архів і видаліть з нього останні п'ять файлів.
4. Перегляньте, використовуючи команду ***Показати інформацію*** (кнопка **Інфо** на **Панелі інструментів**), властивості створеного архіву (для багатотомного архіву – першого файлу), визначте і запишіть у зошит:
   - загальний розмір файлів до архівації;
   - загальний розмір файлів в архіві після архівації;
   - ступінь стиснення;
   - розмір даних для відновлення;
   - зміст коментарю;
   - розмір ***SFX***-модуля.
5. Використовуючи контекстне меню **Робочої області** вікна **Провідника**, розархівуйте усі файли зі створеного вами архіву в папку **DOC**, яку створіть у своїй папці.
6. Використовуючи архіватор, видобудьте перші десять файлів зі створеного вами архіву в папку **1_10**, яку створіть у своїй папці.
7. Закрийте усі відкриті вікна.

4.3. Запис даних на оптичні носії. Форматування та копіювання дисків

1. Які види оптичних дисків ви знаєте? Опишіть їх.
2. Як переглянути вміст диска?
3. Як здійснити копіювання файлів і папок з одного диска на інший?
4. Що таке файлова система, які файлові системи ви знаєте?
5. Опишіть структуру розміщення даних на диску.

Запис даних на оптичні носії

Використовуючи засоби програми **Провідник**, **Windows XP** може здійснювати запис тільки на оптичні диски CD-R або CD-RW.

Для виконання цієї операції потрібно, щоб у комп'ютері було встановлено пристрій для запису оптичних дисків. Алгоритм для запису такий:

1. Вставити у пристрій диск для запису.
2. Відкрити вікно папки **Мій комп'ютер** (наприклад, ***Пуск ⇒ Мій комп'ютер***).

3. Відкрити вікно оптичного диска (значок).
4. Відкрити вікно папки, яка містить потрібні дані.
5. Виділити файли і папки, які потрібно записати на оптичний диск.
6. Вибрати команду **Копіювати** (наприклад, ***Правка ⇒ Копіювати***).
7. Зробити поточним вікно оптичного диска.
8. Вибрати команду **Вставити** (наприклад, ***Правка ⇒ Вставити***) (при цьому біля значків скопійованих файлів і папок з'явиться позначення , а над списком об'єктів – заголовок **Файли, підготовані для запису на компакт-диск)** (рис. 4.10).
9. Вибрати у списку **Завдання для запису** вікна оптичного диска команду **Записати ці файли на компакт-диск** (або ***Файл ⇒ Записати ці файли на компакт-диск***).
10. Увести в поле **Ім'я компакт-диска** вікна **Майстер запису компакт-дисків** ім'я компакт-диска і вибрати кнопку **Далі**.
11. Дочекатися завершення процесу запису файлів і папок на оптичний диск.
12. Установити позначку прапорця **Так, записати ці файли на інший компакт-диск** у вікні **Майстра запису компакт-дисків** (рис. 4.11), якщо планується записати вибрані об'єкти ще на один диск (тобто зробити кілька копій).
13. Вибрати кнопку **Готово**.

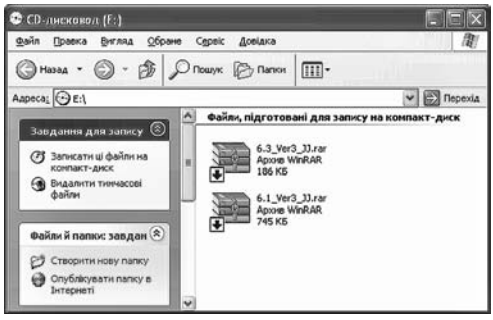

Рис. 4.10. Вікно оптичного диска з підготовленими для запису файлами

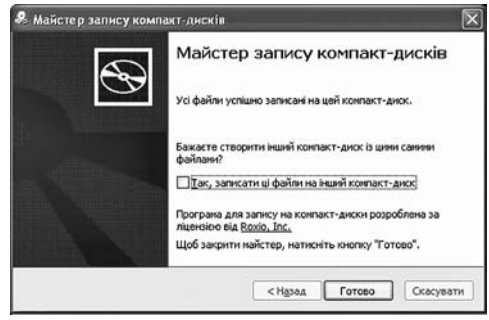

Рис. 4.11. Завершальне вікно **Майстер запису компакт-дисків**

Не слід переривати процес запису на диск! Це, як правило, призводить до пошкодження оптичного диска, який стає непридатним для подальшого використання.

Диски CD-RW за потреби можна попередньо очистити, використавши команду **Стерти цей CD-RW** зі списку **Завдання для запису** вікна оптичного диска (або ***Файл ⇒ Стерти цей CD-RW***).

Для запису оптичних дисків **DVD** в операційній системі **Windows XP** слід використати додаткову програму запису оптичних дисків, наприклад **NERO** версії **6.0** і вище.

В операційній системі **Windows Vista** можна записувати оптичні диски як **CD**, так і **DVD**. Для їх запису треба відкрити вікно оптичного диска, наприклад виконавши ***Запуск ⇒ Мій комп'ютер ⇒ Дисковод оптичних дисків***, скопіювати у це вікно файли і папки, які потрібно записати, і вибрати на **Панелі**

інструментів кнопку **Записати на диск**.

Якщо на диск ще не проводився запис, то програма відкриє вікно **Записати диск**, у якому у відповідне поле потрібно ввести ім'я диска та встановити значення параметрів форматування диска. За замовчуванням параметри форматування приховані від користувача, і для їх відображення необхідно вибрати кнопку **Показати параметри форматування** (рис. 4.12). Можна провести форматування у файловій системі **Live File System**, яка надає можливості видаляти і записувати файли так, як на пристроях флеш-пам'яті, однак записані в цій системі диски не читатимуться при використанні операційних систем, випущених до **Windows XP**.

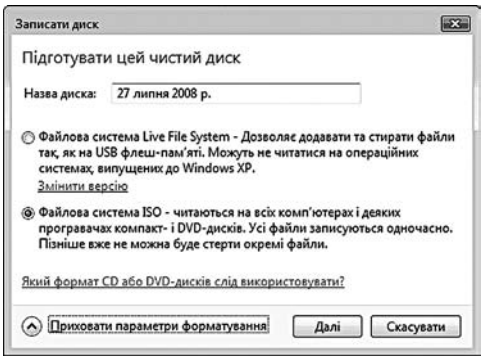

Рис. 4.12. Параметри форматування оптичного диска у вікні **Записати диск**

Диски, записані у файловій системі **ISO**, будуть читатися при використанні раніше створених версій операційної системи **Windows**. Однак стирати файли поодинці не можна. Можна буде лише стерти весь диск (при використанні дисків, що забезпечують багаторазове стирання і записування даних).

Форматування дисків і пристроїв флеш-пам'яті

Вам уже відомо, що перед початком експлуатації диски готують до запису даних. Цей процес називається **форматуванням диска.**

Для форматування ***магнітних дисків*** потрібно виконати такий алгоритм:

1. Відкрити вікно папки **Мій комп'ютер.**
2. Вибрати один із дисків.
3. Виконати ***Файл ⇒ Форматувати*** (або вибрати команду **Форматувати** з контекстного меню диска).
4. Установити значення параметрів форматування (рис. 4.13):

- **місткість** – максимальний розмір даних, що можуть бути записані на цей диск;
- **файлова система** – для гнучких дисків використовується тільки FAT, для жорстких дисків – FAT32 або NTFS;
- **розмір кластера;**
- **мітка тому** – ім'я диска, яке задає користувач для зручності розпізнавання окремих дисків. Мітка може містити до 11 символів для **FAT** і до 32 символів для **NTFS** (диск може не мати мітки);
- **способи форматування:**
  - ***швидкий***, що здійснюється шляхом очищення змісту диска (кореневої папки) без очищення його вмісту;
  - ***з використанням стискання*** – у цьому режимі дані перед записом на диск попередньо стискаються;

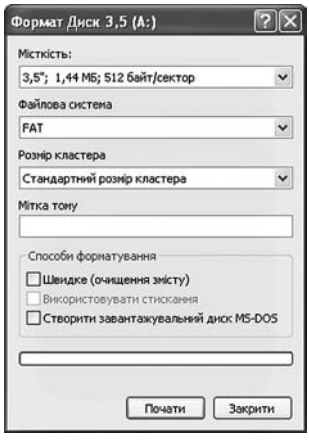

Рис. 4.13. Вікно програми форматування дисків

- ***створити завантажувальний диск MS-DOS*** – цей режим можливий лише для гнучких дисків, після форматування на дискету записуються компоненти операційної системи **MS-DOS**, що робить диск системним.

5. Вибрати кнопку **Почати**.
6. Підтвердити виконання операції форматування.

Операція форматування небезпечна, і її помилкове виконання, особливо для жорсткого диска, може призвести до втрати даних.

Пристрої флеш-пам'яті, як і дискети або оптичні диски, поступають у продаж уже відформатованими. Потреба у форматуванні може виникнути, якщо відбувся збій у роботі пристрою, який був викликаний дією комп'ютерних вірусів або некоректним від'єднанням пристрою від комп'ютера. Форматування цих пристроїв практично нічим не відрізняється від форматування магнітних дисків.

Процес форматування використовується і для оптичних дисків. Форматування оптичних дисків у операційній системі **Windows XP** відбувається під час їх стирання.

Копіювання дисків

Копіювання засобами ОС дає змогу створювати копії тільки гнучких магнітних дисків і за певних умов оптичних дисків.

Для створення копії дискети потрібно виконати такий алгоритм:

1. Відкрити вікно папки **Мій комп'ютер**.
2. Вибрати значок дисковода гнучких дисків.
3. Виконати ***Файл ⇒ Копіювати диск***.
4. Вибрати кнопку **Почати** (рис. 4.14).
5. На запит програми вставити диск, з якого потрібно копіювати дані (вихідний диск).
6. Дочекатися, поки копія даних з диска буде занесена в оперативну пам'ять.
7. На запит програми замінити диск на той, на який буде скопійовано дані (кінцевий диск).
8. Вибрати кнопку **Далі**.
9. Дочекатися повідомлення про завершення копіювання.

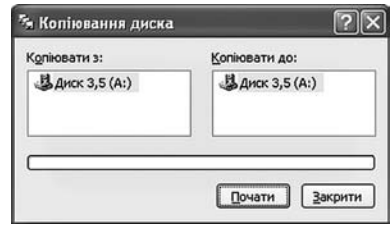

Рис. 4.14. Вікно програми **Копіювання диска**

При копіюванні дисків можуть порушуватися чиїсь авторські чи майнові права, що переслідується відповідно до законодавства України.

Перевірте себе

1°. Як позначаються файли, підготовлені для запису на компакт-диск?
2•. Як записати файли і папки на оптичні диски?
3•. Опишіть процес підготовки даних для запису на оптичний диск.

4*. Поясніть, що таке сесія запису на оптичний диск.
5•. У чому полягає форматування оптичних дисків?
6°. Як надати ім'я диску, на який записуються файли і папки?
7°. Які оптичні диски можна записувати за допомогою **Провідника** у **Windows XP**?
8•. Як скопіювати гнучкий магнітний диск?
9°. Як провести форматування оптичних дисків; пристроїв флеш-пам'яті?
10*. Які файлові системи використовуються у пристроях флеш-пам'яті? Як вибрати файлову систему при форматуванні?
11°. Для чого виконується форматування дисків?
12•. У чому особливості швидкого способу форматування?
13°. Чому слід бути дуже обережним, виконуючи операції форматування диска?
14°. Що слід врахувати, створюючи копії дисків?

Виконайте завдання

1°. Візьміть чистий оптичний диск CD-RW та:
а) запишіть на нього два перші файли з папки **Мої документи\Моя музика\Зразки музики**;
б) перевірте, чи записалися ці файли на диск;
в) зітріть CD-RW диск.
2•. Запишіть алгоритм стирання даних з оптичних дисків.
3•. Запишіть алгоритм виконання форматування пристроїв флеш-пам'яті.
4•. Зробіть копію дискети, запропонованої вчителем. Перевірте, чи збігається вміст дискет після копіювання.
5•. Візьміть чистий оптичний диск CD-RW та:
а) запишіть на нього два файли з папки **Тема 4\Архів**;
б) перевірте, чи записалися ці файли на диск;
в) запишіть на диск папки **Бібліотека** та **Фото_кращих_учнів** з папки **Тема 4**;
г) перевірте, чи записалися ці папки на диск, порівняйте вміст цих папок із вмістом папок, що входять до папки **Тема 4**;
д) спробуйте видалити папку **Бібліотека** з вашого оптичного диска. Чи вдалося це вам? Поясніть чому;
е) зітріть увесь диск.
6•. З дозволу вчителя підготуйте ***завантажувальний диск MS-DOS***. Чи успішно пройшло форматування? Які об'єкти є на диску **A:** після форматування?
7•. Складіть алгоритм копіювання оптичного диска засобами **Windows**.
8. Візьміть два однакові оптичні диски (бажано CD-RW). Запишіть на них однакові дані (одні й ті самі файли і папки). Тільки в одному випадку дані запишіть за один раз, а в другому – за 3–4. Визначте після запису ємність вільного місця на дисках. Чи є різниця? Якщо є, то чому?
9*. Знайдіть інформацію про файлову систему **Live File System**. Визначте, для яких носіїв даних вона використовується. У чому її переваги перед іншими файловими системами для подібних носіїв? Чи можна цю систему використовувати для дисків CD-R і DVD-R?