Тема: Сервісне програмне забезпечення.

План.

1. Стандартні службові програми Windows. Виконання програм перевірки диска Scan Disk. Поняття втрачених кластерів.
2. Дефрагментація диска. Програма Defrag.
3. Архівація інформації. Програма архівації WinRar.
4. Комп'ютерні віруси. Методи боротьби із ними.
5. Антивірусні програми Aidstest, Drweb, Adinf.

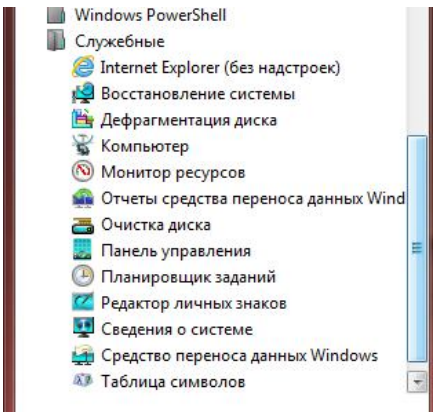
Література.

1. Редько М.М. Інформатика та комп’ютерна техніка. Навчально-методичний посібник. –Вінниця: Нова Книга, 2007. – 268 с.
2. Редько М.М. і ін.. Інформатика і комп’ютерна техніка. Навчально-методичний посібник.-К.:НМЦ
3. Гаєвський О.Ю. Інформатика. – К.: Видавництво А.С.К., 2003

1. Стандартні службові програми Windows. Виконання програм перевірки диска Scan Disk. Поняття втрачених кластерів.

У Windows є програми, які виконують роботи по обслуговуванню файлів, каталогів і дисків. Такі програми називаються службовими.

Для того, щоб знайти службові програми, переходимо в Пуск -> Всі програми -> Стандартні -> Службові



Програма відновлення системи — самостійно спостерігає за змінами в системі й автоматично створює точки відновлення (фіксує стан системи й для відновлення залишає всі документи без змін).

Відновлення системи дає можливість повернути системні файли комп’ютера до одного з попередніх станів. У такий спосіб можна скасувати зміни, внесені до системи комп’ютера, без впливу на особисті файли, наприклад електронну пошту, документи або фотографії.

Іноді інсталяція програми або драйвера може призвести до несподіваних змін у комп’ютері або непередбачених дій Windows. Зазвичай видалення програми або драйвера виправляє неполадку. Якщо після видалення неполадка залишилась, можна спробувати повернути систему комп’ютера до стану, коли все працювало належним чином.

Відновлення системи використовує функцію захисту системи для регулярного створення та збереження на комп’ютері контрольних точок відновлення. Ці контрольні точки відновлення містять відомості про настройки

реєстру та інші відомості про систему, які використовує система Windows. Точки відновлення можна також створювати вручну.

Відновлення системи не призначене для резервного копіювання особистих файлів, тому з його допомогою не можна відновити видалені або пошкоджені особисті файли. Слід регулярно здійснювати резервне копіювання особистих файлів і важливих даних за допомогою програми резервного копіювання.

Програма перевірки дисків — використовується для:

а) виявлення помилок файлової системи

б) перевірки диска на ушкоджені сектори.

Програма намагається усунути знайдені помилки. Якщо це вдається, то файли переміщаються із пошкодженої області, розірвані ланцюжки кластерів записуються як окремі файли.

Для перевірки диска необхідно виконати такі дії:

• Виконати команду «Пуск»/«Программы»/«Стандартные»/«Служебные».

• У списку вибрати «Проверка диска», де обрати потрібний диск.

• Встановити перемикач «Стандартная» і прапорець «Исправлять ошибки автоматически» у положення «Так». Клацнути на кнопці «Запуск».

Програма очищення дисків — пропонує очищення дисків від тимчасових файлів, створених під час роботи прикладних програм та при роботі в Інтернеті.

Програма дефрагментації диска — перевіряє диск на наявність фрагментованих ділянок і в процесі роботи програми розміщує фрагменти кожного файлу в кластерах, розташованих якнайближче один до одного, тим самим усуваючи фрагментацію дискового простору. Найчастіше доступна на вкладці Сервіс властивостей диска, яку можна викликати за допомогою контекстного меню диска.

Форматування диска — процес розмітки диска на сектори та доріжки для подальшого збереження інформації. *Слід* ***пам'ятати:*** при форматуванні носія дані на ньому знищуються

Втрачені кластери - це кластери, не відзначені як вільні, але в той же час не зайняті яким-небудь файлом. Подібний дефект не заважає нормальній роботі комп'ютера. Він призводить лише до того, що частина дискового простору не використовується.

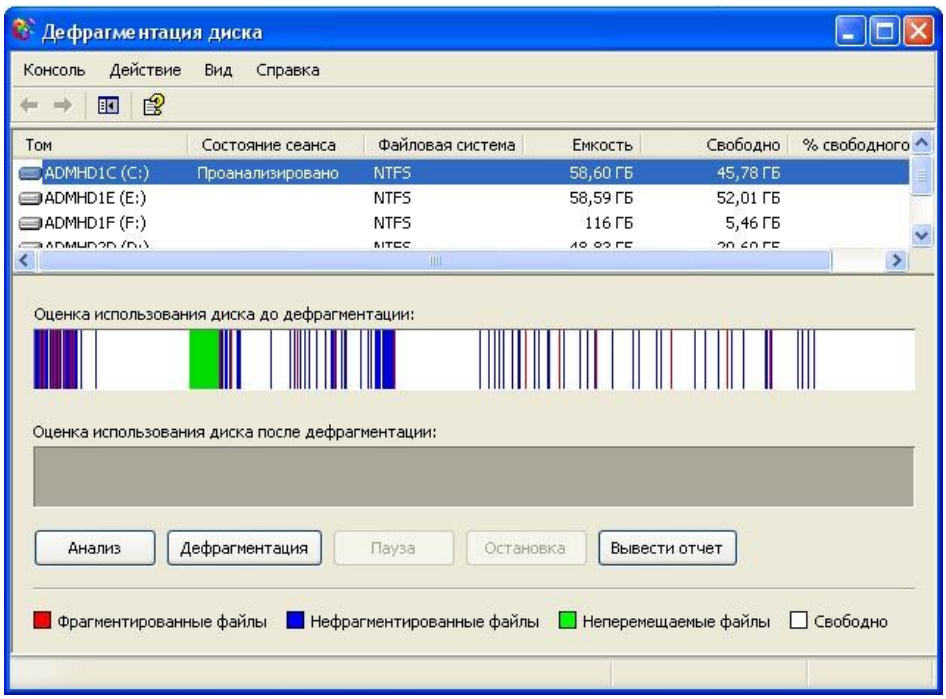
Усунути дефект можна або поверненням втрачених кластерів в категорію вільних, або утворенням з цих кластерів файлів.

2. Дефрагментація диска. Програма Defrag

Дефрагментацією дисків називають процес об’єднання фрагментованих файлів на жорсткому диску комп’ютера.

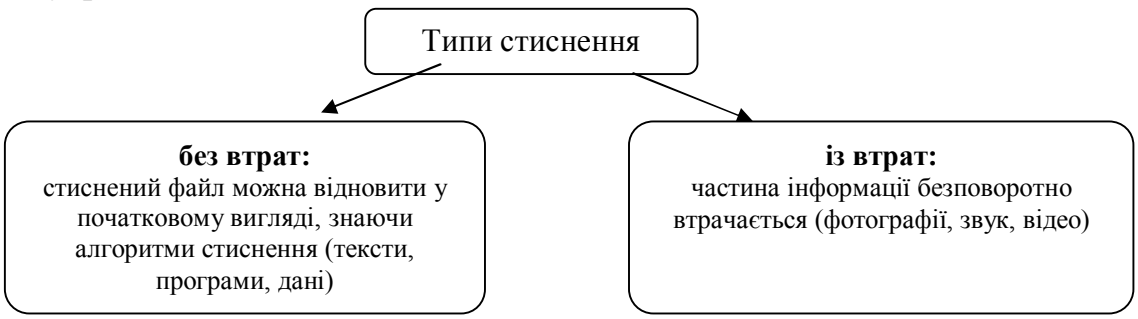
Фрагментування файлів відбувається під час кожного збереження, змінення або видалення файлів. Зміни, застосовані до файлу, часто зберігаються на жорсткому диску в іншому розташуванні, ніж вихідний файл. Додаткові зміни можуть зберігатися в кількох розташуваннях. Через деякий час файл і власне сам жорсткий диск стають фрагментованими, що призводить до зниження продуктивності роботи комп'ютера, оскільки для відкривання файлу потрібно шукати його фрагменти в багатьох розташуваннях.

Програма дефрагментації дисків впорядковує дані на диску та об'єднує фрагменти файлів, що підвищує продуктивність роботи комп'ютера. У цій версії Windows програма дефрагментації дисків запускається за встановленим вами розкладом (тому можна не турбуватися про її вчасний запуск), але можна змінити розклад її запуску або запускати програму вручну.



3. Архівація інформації. Програма архівації WinRAR.

Архівування даних — процес стискання інформації у файл для зручності її передавання та зберігання. Завдяки архівуванню збільшується вільний дисковий простір без утрати даних.



Архівний файл — файл, отриманий в результаті архівування, що містить один або декілька файлів та службову інформацію про даний архів.

Архіватор — програма, що здійснює архівування файлу шляхом стискання даних.

Розархівація файлу — процес повернення файлу до початкового стану.

SFX-архів (від англ. *SelF extracting* — саморозпаковувальний) — файл, що здатний до саморозпаковування, має розширення *.exe, містить стиснені дані та програму розпаковування

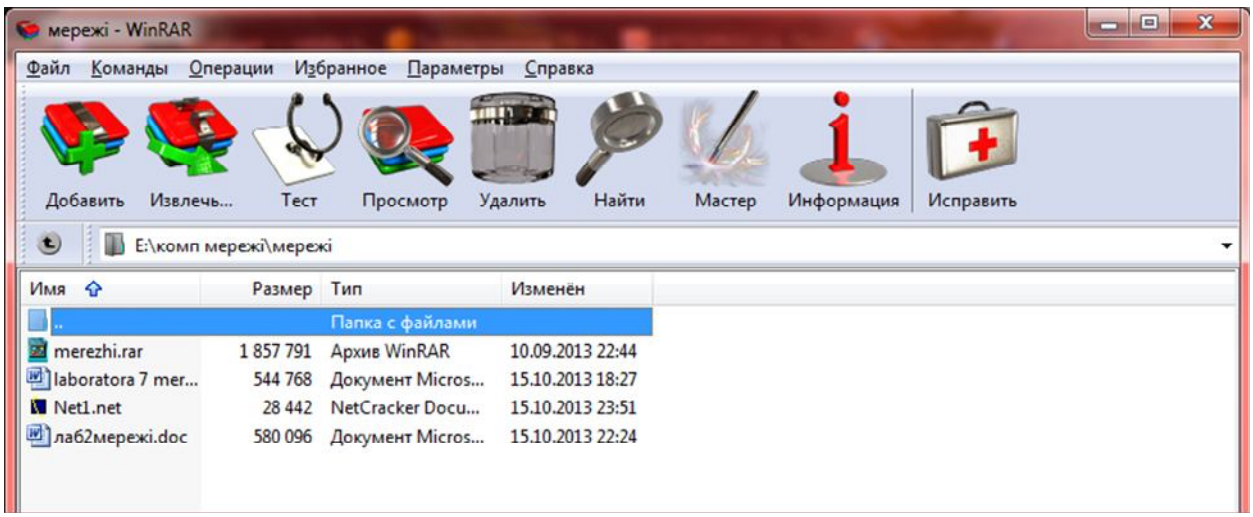
Багатотомний архів — архів, розділений на декілька частин.

Відомі програми-архіватори: WinRar, WinZip, 7z

Функції сучасних архіваторів:

1) розпаковування файлів із архівів
2) створення нових архівів
3) додавання файлів до архіву
4) створення архівів, що само розпаковуються
5) створення розподілених архівів на носіях малої ємності
6) тестування цілісності структури архівів
7) повне або часткове відновлення пошкоджених файлів
8) захист архівів від перегляду й несанкціонованої модифікації

Програма WinRAR - це 32 розрядна версія архіватора RAR для Windows - потужний засіб створення архівів і управління ними. Є декілька версій RAR для різних операційних систем: Windows, Linux, UNIX, DOS, OS/2 і так далі



Існує дві версії RAR для Windows:

• версія з графічним інтерфейсом користувача - WinRAR.EXE

• Консольна версія RAR.EXE пульт лінії команди (спосіб тексту) версія - Rar.exe

Можливості WinRAR

• Дозволяє розпаковувати архіви CAB, ARJ, LZH, TAR, GZ, ACE, UUE, BZ2, JAR, ISO, і забезпечує архівацію даних у формати ZIP і RAR

• Забезпечує повну підтримку архівів ZIP і RAR

• Має спеціальні алгоритми, оптимізовані для тексту і графіки. Для мультимедіа стискання можна використовувати тільки з форматами RAR

• Підтримує технологію перетягування (drag & drop)

• Має інтерфейс командного рядка

• Може здійснювати безперервну архівацію, яка забезпечує вищу міру стискання в порівнянні зі звичайними методами стискання, особливо при упаковці великої кількості невеликих файлів однотипного змісту

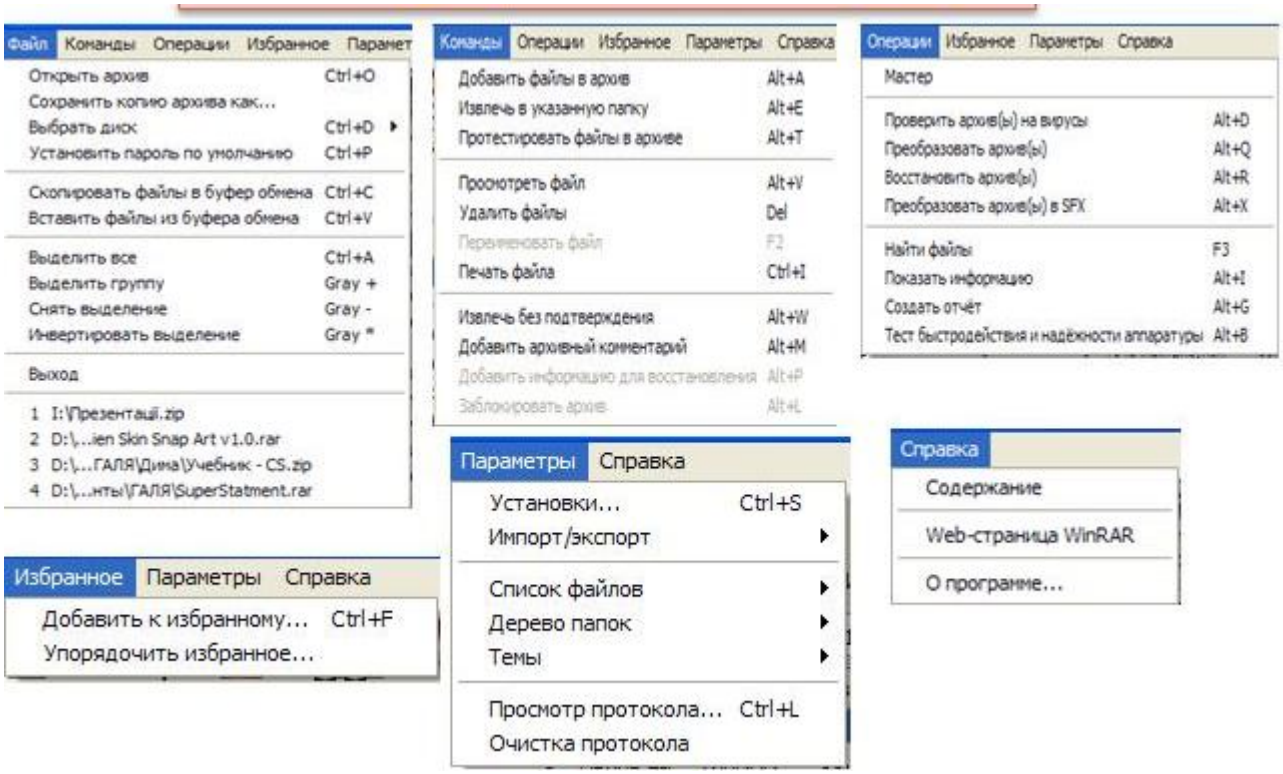
• Забезпечує підтримку багатотомних архівів, тобто здійснює розбиття архіву на декілька томів (наприклад, для запису великого архіву на диски). Розширення томів: RAR, R01, R02 і так далі.

• Створює саморозпаковуючі архіви (SFX), звичайні і багатотомні архіви, забезпечує захист їх паролями

• Забезпечує відновлення фізично пошкоджених архівів

• Має засоби відновлення, які дозволяють відновлювати відсутні частини багатотомного архіву

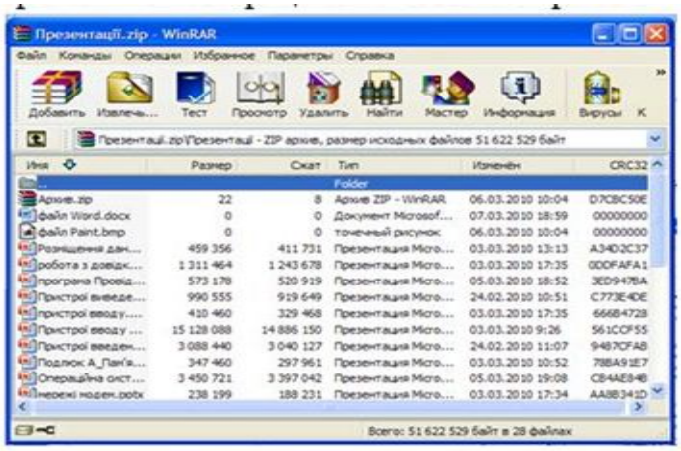
• Для новачків призначений режим Майстра (Wizard), за допомогою якого можна легко здійснити усі операції над архівами WinRAR має і інші додаткові функції. WinRAR здатний створити архів в двох різних форматах: RAR та ZIP.



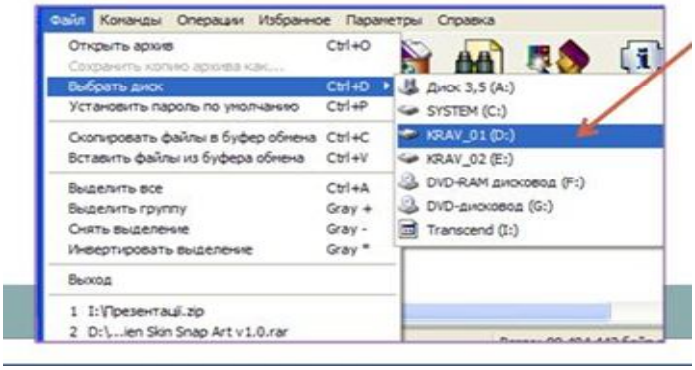
Головне меню (підменю) програми WinRAR:

Архівування файлів у програмі WinRAR

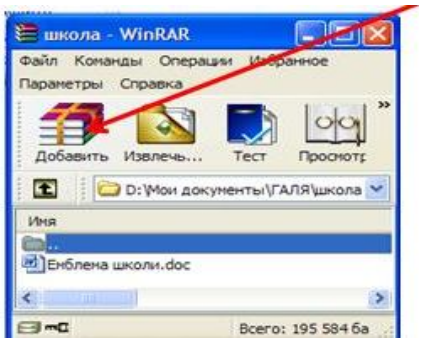
1. Після запуску програми WinRAR у її вікні буде відображено вміст тієї папки, з RAR – файлами, з якою працювали раніше.



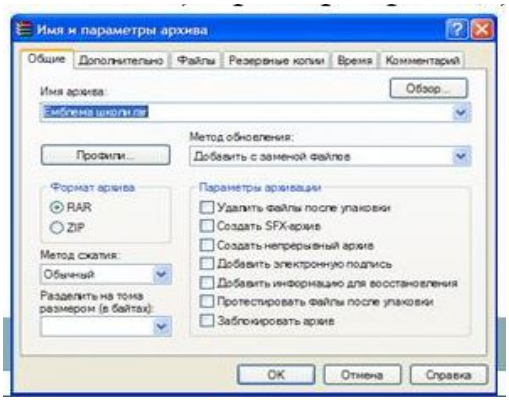
2. Можна вибрати диск з потрібними об’єктами за допомогою Файл, Вибрати диск, вказати потрібний диск.



3. Перейшовши до потрібної папки за допомогою миші виділити файли та папки, які потрібно архівувати, клацнути кнопку Додати.



4. У вікні Ім’я та параметри архіву ввести ім’я архіву, вибрати формат архіву, метод стиснення, метод обновлення, параметри архівації, натиснути Ок.



Багатотомний архів

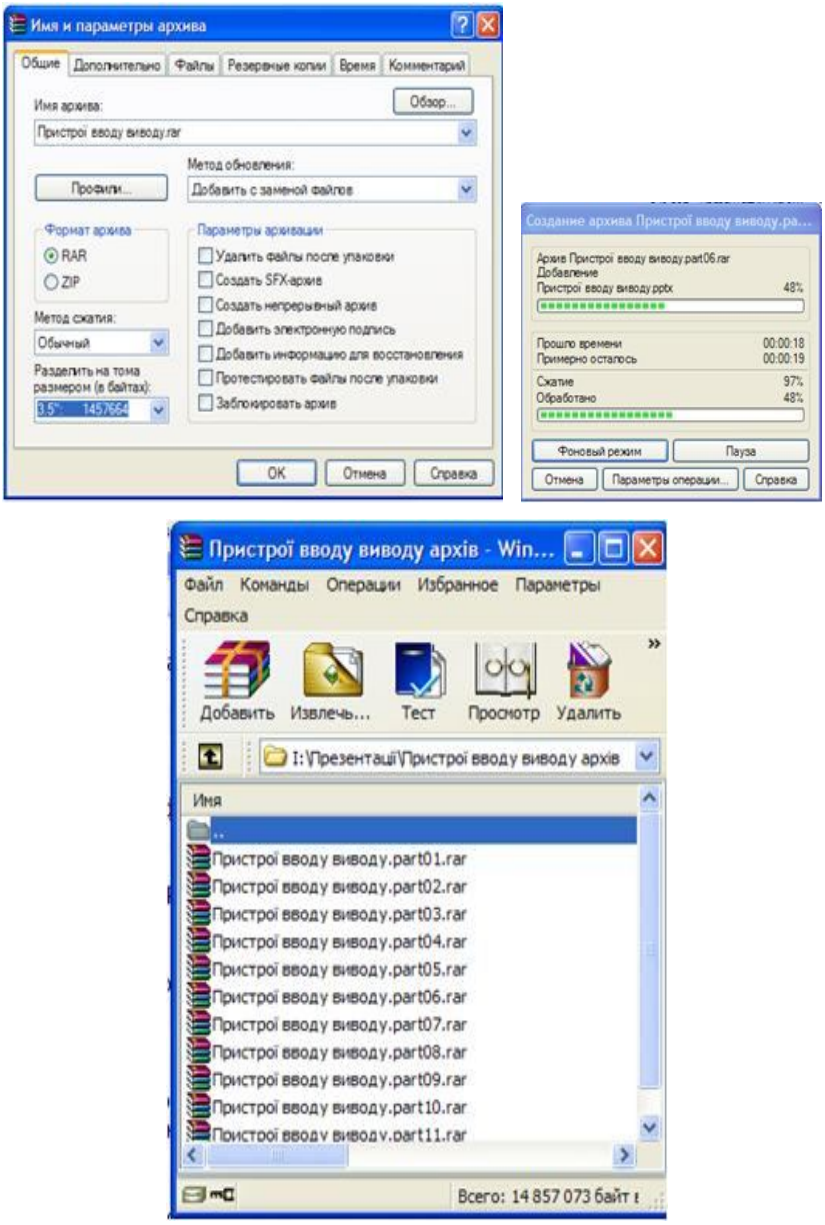
Часто виникає потреба поділити архів на «шматки» (томи), наприклад для передавання його через Інтернет або запису на оптичні диски. Такий архів називають **багатотомним**.

Багатотомний архів – це архів RAR, що зберігається в декількох файлах, які називаються томами.

Томи підтримує лише формат RAR. За умовчанням кожен том (частина багатотомному архіву) отримує ім'я *ім'я_тому.partNNN*, де NNN – номер тому.

Усі томи мають бути збережені в одній папці; розпакувати їх слід, починаючи з першого.

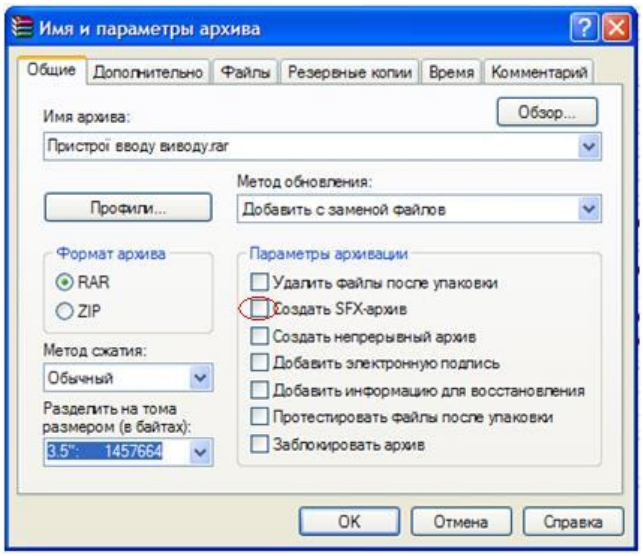
Щоб створити багатотомний архів, потрібно відкрити вікно **Ім'я архіву та параметри**, у полі **Розбити на томи, байти** зазначити обсяг тому і клацнути кнопку **ОК**.



Саморозпаковуваний архів

Саморозпаковуваний архів – це архів із приєднаним виконуваним модулем, який дає змогу видобути файли без запуску відповідного архіватора. Ім’я такого архіву, як і будь-якого виконуваного файлу, має розширення exe. Якщо користувач, для якого призначено архів, не має програми для його розпакування, він не зможе видобути файл з цього архіву. У такому випадку доцільно створювати саморозпаковуваний архів. Для цього у вікні Ім’я архіву та параметри потрібно встановити прапорець Створити SFX-архів.

Саморозпаковуваний архів – це архів із приєднаним виконуваним модулем, який дає змогу видобути файли без запуску відповідного архіватора. Ім’я такого архіву, як і будь-якого виконуваного файлу, має розширення exe.



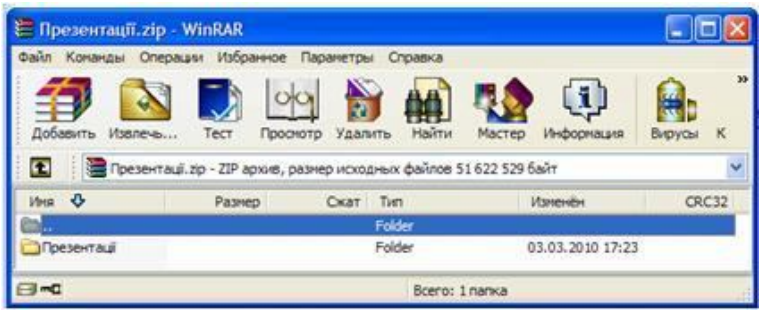
Видобування файлів з архіву

Щоб видобути файл з архіву, той потрібно спочатку відкрити. Для цього слід двічі клацнути мишею його ім'я у вікні **Провідника** або вибрати файл архіву у вікні **WinRAR** і натиснути клавішу **Enter**. Коли архів буде відкрито, у вікні програми WinRAR відобразиться його вміст. Виділіть файли та папки, які потрібно видобути, та клацніть кнопку **Видобути** до на панелі інструментів або виберіть команду Видобути файли до зазначеного каталогу в меню **Команди.**

У вікні **Шлях для видобування та параметри** введіть ім'я папки, до якої слід записати файли з архіву, та клацніть кнопку **ОК.**

Під час видобування на екрані відображатиметься вікно з інформацією про перебіг операції. Якщо процес розпакування завершиться вдало, відкриється вікно програми WinRAR, а ні – то вікно діагностичних повідомлень.

Зазначимо, що діалогове вікно **Шлях для видобування та параметри** можна відкрити в програмі **Провідник**. Для цього слід клацнути правою кнопкою миші файл архіву, а потім вибрати в контекстному меню команду **Видобути файли.**



4. Комп'ютерні віруси. Методи боротьби із ними.

Шкідливими називають програми, що само розмножуються й виконують руйнівні дії в процесі роботи комп’ютера.

Вони поділяються на:

- Комп’ютерні віруси — переважно невеликі спеціально створені програми, які здатні до саморозмноження й виконання недозволених і шкідливих дій
- Мережні хробаки – зараджають невеликі повідомлення електронної пошти й поширюються протягом кількох годин при спробі прочитати таке повідомлення.
- Троянські програми – мають виконувати певні функції, але після запуску виконують зовсім інші дії (як правило, деструктивні,наприклад форматування жорсткого диска). Не можуть розмножуватись самостійно, а поширюються тільки в разі копіювання користувачем. Після запуску зазвичай знищують себе разом з іншими файлами на диску.

Ознаки зараження комп'ютера вірусом

2. Зменшення обсягу вільної оперативної пам'яті;
3. сповільнення завантаження та роботи комп'ютера;
4. незрозумілі (без причин) зміни у файлах, а також зміни розмірів і дати останньої модифікації файлів;
5. помилки під час завантаження операційної системи;
6. неможливість зберігати файли в потрібних каталогах;
7. незрозумілі системні повідомлення, музикальні та візуальні ефекти;
8. неспроможність завантаження файлів або операційної системи;
9. зникнення файлів тощо

Основні джерела вірусів

1. Носій, на якому містяться заражені вірусом файли;
2. комп'ютерна мережа, наприклад система електронної пошти та Internet;
3. жорсткий диск, на який потрапив вірус унаслідок роботи із зараженими програмами, тощо.

Класифікації вірусів

Класифікація	Типи вірусів	Дія
За способом зараження середовища перебування	Резидентні	Заражають оперативну пам'ять, залишаючи в ній свою частину, що не сприймається як шкідлива. Вона перехоплює звернення операційної системи до об'єктів і вбудовується в них
	Нерезидентні	Не заражають пам'ять і зберігають активність обмежений час
За об'єктами зараження	Файлові	Після запуску самостійно вбудовуються в інші програми, де записують свій програмний код (заражають файли *.exe, *.sys, *.dll)
	Завантажувальні	Записуються в завантажувальний сектор диска (boot-сектор), змінюють важливу інформацію, необхідну для запуску системи. Один із наслідків — неможливість завантаження операційної системи
	Текстові	Активізуються під час запуску текстових файлів
За зовнішнім виглядом	Звичайні	Програмний код вірусу видно на диску
	Невидимі	Програмний код вірусу не видно на диску
	Поліморфні	Видозмінюють свій власний програмний код, тому їх складно виявити
За особливостями діяльності	Паразитичні	Змінюють зміст файлів та секторів на диску
	Віруси-компаньйони	Створюють для exe-файлів файли-супутники з таким самим ім'ям, але з розширенням *com*
За можливостями пошкодження	Безпечні	Призводять до зменшення вільної пам'яті на диску, появи графічних та звукових ефектів, але не мають необоротних наслідків
	Небезпечні	Призводять до серйозних збоїв у роботі або до втрати чи пошкодження інформації
	Особливо небезпечні	Призводять до фізичного пошкодження обладнання (перезаписування ПЗП, вихід із ладу дискових пристроїв, пошкодження елементів материнської плати

Примітка. В Україні передбачена карна та кримінальна відповідальність за створення та розповсюдження шкідливих програм

Правила профілактики зараження комп'ютера вірусами

1. Виконувати резервне копіювання інформації (створювати копії файлів і системних ділянок жорстких дисків).

2. Уникати користування випадковими й невідомими програмами (найчастіше віруси поширюються разом із комп'ютерними програмами).

3. Перезавантажувати комп'ютер перед початком роботи, особливо у випадку, якщо за цим комп'ютером працювали інші користувачі).

4. Користуватись антивірусними програмами

5. Антивірусні програми Aidstest, Drweb, Adinf.

Антивірус — програма, яка виявляє та знешкоджує відомі їй комп'ютерні віруси.

Примітка. Вибір одного «найкращого» антивірусу є помилковим рішенням. Слід використовувати декілька різних антивірусних пакетів. Найвідоміші антивірусі пакети: DrWeb, ADINF, Kaspersky Internet Security, Avast!, Panda тощо

«Aidstest» - антивірусна програма-сканер (поліфаг). Призначена для пошуку та знешкодження файлових, завантажувальних і файлово-завантажувальних вірусів. Пошук вірусів Aidstest здійснює за допомогою сигнатур. Підтримувалася і поширювалася протягом 1988-1998 років ЗАТ «Диалогнаука». Автор програми - Дмитро Лозинський.

Програма викликається таким командним рядком (вказані тільки основні параметри):

Aidstest path[/f][/g][/s][/p[ім'я файлу]][/q][/e]

Параметри програми:

path - задає підмножину файлів для перевірки на зараженість. Кодується практично за тими ж правилами, що і в команді DIR операційної системи. Замість цього параметра можна поставити символ "*", що задає роботу з усіма логічними розділами жорстких дисків, або символи "**", які задають роботу з усіма дисками, починаючи з "C:" і включаючи ті, що працюють у мережі, CD та subst-диски. Для перевірки поточного каталогу задається просто символ ".";

/f - лікувати заражені програми та витирати безнадійно зіпсовані;

/g - глобальна перевірка всіх файлів (не тільки COM, EXE та SYS). З цим параметром програму рекомендується запускати лише тоді, коли відомо про наявність у комп'ютері вірусів;

/s - використовується у випадку, коли вірус, об'явлений видаленим, продовжує з'являтися знову;

/p - [ім'я файлу] виводить протокол роботи. Якщо ім'я файлу не задане, виведення відбувається на принтер без нагадування;

/q - виводить підказку про дозвіл на витирання безнадійно зіпсованих файлів.

Якщо ви запустили програму без параметрів або помилилися при їх завданні, на екран видається короткий опис параметрів програми.

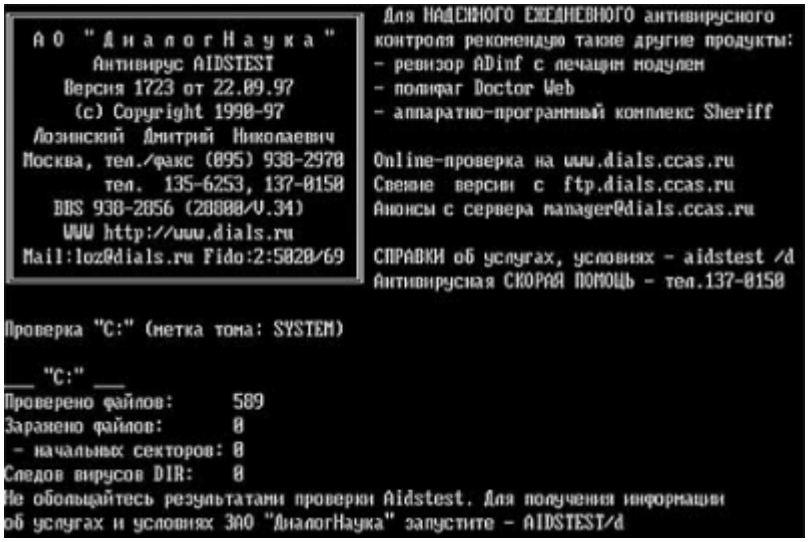
Приклади використання програми Aidstest.

Aidstest * перевірка всіх EXE-, COM- і SYS-файлів на всіх дисках, починаючи з "C:".

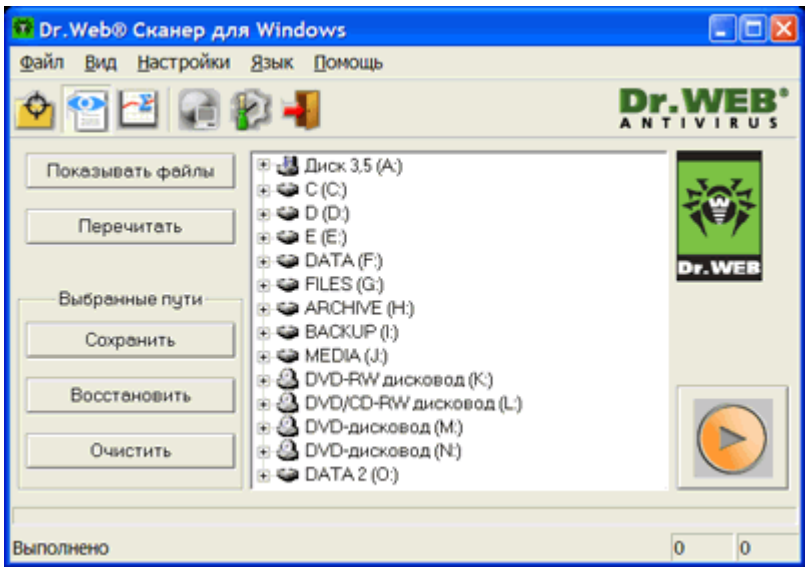
Aidstest a: перевірка всіх EXE-, COM- і SYS-файлів на дискеті в пристрої "A:".

Aidstest d:/g/f лікування всіх доступних файлів на диску "D:".

Під час роботи програма Aidstest виводить повідомлення, зміст яких достатньо простий та зрозумілий.



Dr.Web - антивіруси цього сімейства призначені для захисту від поштових і мережевих черв'яків, руткітів, файлових вірусів, троянських програм, стелс-вірусів, поліморфних вірусів, безтілесних вірусів, макровірусів, вірусів, що вражають документи MS Office, скрипт-вірусів, шпигунського ПЗ (spyware), програм-викрадачів паролів, клавіатурних шпигунів, програм платного дозвону, рекламного ПЗ (adware), потенційно небезпечного ПЗ, хакреських утиліт, програм-люків, програм-жартів, шкідливих скриптів й інших шкідливих об'єктів, а також від спаму, скамінг-, фармінг-, фішинг-повідомлень і технічного спаму.



Для запуску програми необхідно ввести у командний рядок DOS команду DRWEB. Після натискання клавіші Enter на екрані з'явиться головне вікно. У верхній частиш вікна зображується меню: Dr.Web, Тест, Настройки, Дополнения и Помощь.

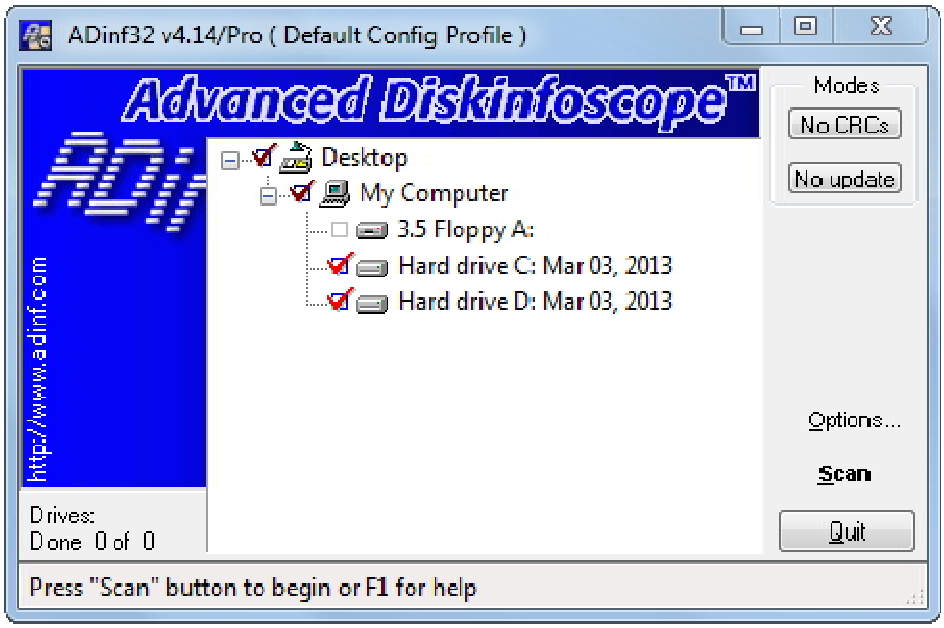
Призначення меню:

Dr.Web - використовується для отримання інформації про програму, тимчасового виходу в DOS та завершення роботи програми;

Тест - дозволяє запустити програму в режимі перевірки та лікування файлів;

Настройки - використовується для наладки інтерфейс програми та зміни режимів її роботи;
Дополнения - забезпечує підмикання зовнішніх файлів - баз даних, які мають інформацію про нові віруси;
Помощь - призначена для отримання довідкової інформації.
Режим пошуку вірусів вмикається вибором команди тестування в меню Тест, або натискуванням клавіші F5. При цьому на екрані над головним вікном з'являється діалогова панель Путь для тестирования. У рядку введення цієї панелі потрібно указати диск, каталог (каталоги) або групи файлів, де потрібно шукати віруси. Тестування починається після натискування кнопки ОК діалогової панелі. Для тестування з лікуванням потрібно натиснути Ctrl+F5.
Результати роботи програми відображені у її головному вікні.

Adinf - антивірус-ревізор диска ADINF (Avanced DiskINFoscope) дозволяє знаходити та знищувати, як існуючі звичайні, stealth- і поліморфні віруси, так і зовсім нові. Антивірус має в своєму розпорядженні лікуючий блок ревізору ADINF - Adinf Cure Module - який може знешкодити до 97% всіх вірусів. Цю цифру наводить "ДіалогНаука", виходячи з результатів тестування, котре відбувалося на колекціях вірусів двох визнаних авторитетів в цій області - Д.Н.Лозинського й фірми Dr.Solomon's (Великобританія).



ADINF завантажується автоматично у разі вмикання комп'ютера і контролює boot-сектор і файли на диску (дата й час створення, довжина, контрольна сума), виводячи повідомлення про їх зміни. Завдяки тому, що ADINF здійснює дискові операції в обхід операційної системи, звертаючись до функцій BIOS, досягаються не тільки можливість виявлення активних stealth-вірусів на рівні переривання Int 13h, але і висока швидкість перевірки диску. Якщо знайдено

boot-вірус, то ADINF просто відновить попередній завантажувальний сектор, котрий зберігається в його таблиці.

Якщо вірус є файловим, то тут на допомогу приходить лікуючий блок Adinf Cure Module, який на основі звіту основного модуля про заражені файли порівнює нові параметри файлів із попередніми, які зберігаються в спеціальних таблицях. При виявленні розбіжностей ADINF відновлює попередній стан файлу, а не знищує тіло вірусу, як це роблять поліфаги.

Контрольні запитання

1. Які програми входять до стандартних службових програм Windows?
2. Як викликати стандартні службові програми Windows?
3. Поясніть призначення програми Перевірка диска.
4. Поясніть призначення програми Дефрагментація диска.
5. Поясніть призначення програми Очистка диска.
6. Що таке втрачені кластери?
7. Які помилки можуть з'являтись на диску під час його експлуатації?
8. Що таке архівація інформації?
9. Що таке архівний файл
10. Назвіть програми для архівації інформації.
11. Опишіть роботу програми WinRar.
12. Що таке комп’ютерні віруси
13. Яким чином вірус заражує комп'ютер?
14. Основні джерела зараження комп’ютерів вірусами?
15. За якими ознаками можна виявити факт зараження комп'ютерним вірусом?
16. Назвіть методи боротьби із комп’ютерними вірусами
17. Які ви знаєте типи вірусів? Які деструктивні дії вони здійснюють?
18. Опишіть види вірусів та їх шкідливу дію.
19. Які заходи рекомендується вживати, щоб запобігти зараженню комп'ютерним вірусом?
20. Які програми називаються антивірусними? Які типи антивірусів ви знаєте?
21. Наведіть приклади антивірусних програм. Коротко охарактеризуйте