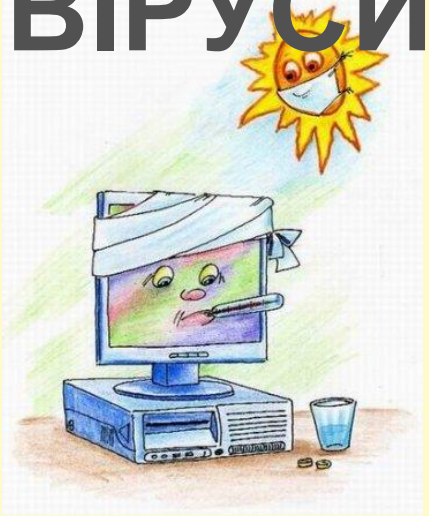
КОМП’ЮТЕРНІ ВІРУСИ І АНТИВІРУСИ



Що таке вірус?

Комп'ютерний вірус – це програма, яка при запуску має властивість розповсюджуватися без керування людиною.

Шкідливі дії:

- звукові і візуальні ефекти
- імітація збоїв ОС і апаратури
- перезавантаження комп'ютера
- розвалювання файлової системи
- знищення інформації
- передавання секретних даних через Інтернет
- масові атаки на сайти Інтернет

Ознаки:

- сповільнення роботи комп'ютера
- перезавантаження або зависання комп'ютера
- неправильна робота ОС або прикладних програм
- зміна довжини файлу
- появлення нових файлів
- зменшення об'єму оперативної пам'яті

Із історії

У1989 р. 23-річний американський студент Роберт Морріс написав невелику програму. За його задумом програма-жарт повинна була непомітно розповсюдитися з одного комп'ютера на інший, не заважаючи їхній роботі. Але допущена в програмі помилка змусила інформацію розповсюдитися з великою швидкістю, від чого всі канали зв'язку ЕОМ виявилися перевантаженими і наукова інформація, накопичена в обчислювальних центрах, у своїй більшості стала непридатною для використання. Всього за кілька годин найважливіші мережі східного і західного узбережжя США були виведені з ладу. Епідемія охопила шість тисяч комп'ютерів, об'єднаних у 70 систем, за допомогою яких відбувався обмін найважливішою інформацією.

На сході були пошкоджені комп'ютерні центри таких великих закладів, як Масачусетський технологічний інститут. Гарвардський, Пітсбургський, Мерілендський і Вісконсинський університети, науково-дослідна морська лабораторія. На заході Каліфорнійський і Стенфордський університети, науково-дослідна лабораторія НАСА, Ліверпульська лабораторія ядерних досліджень. Усі вони були зв'язані супутниковою системою «АРПАНЕТ». А причиною всього стала маленька програма-жарт, запущена в систему.

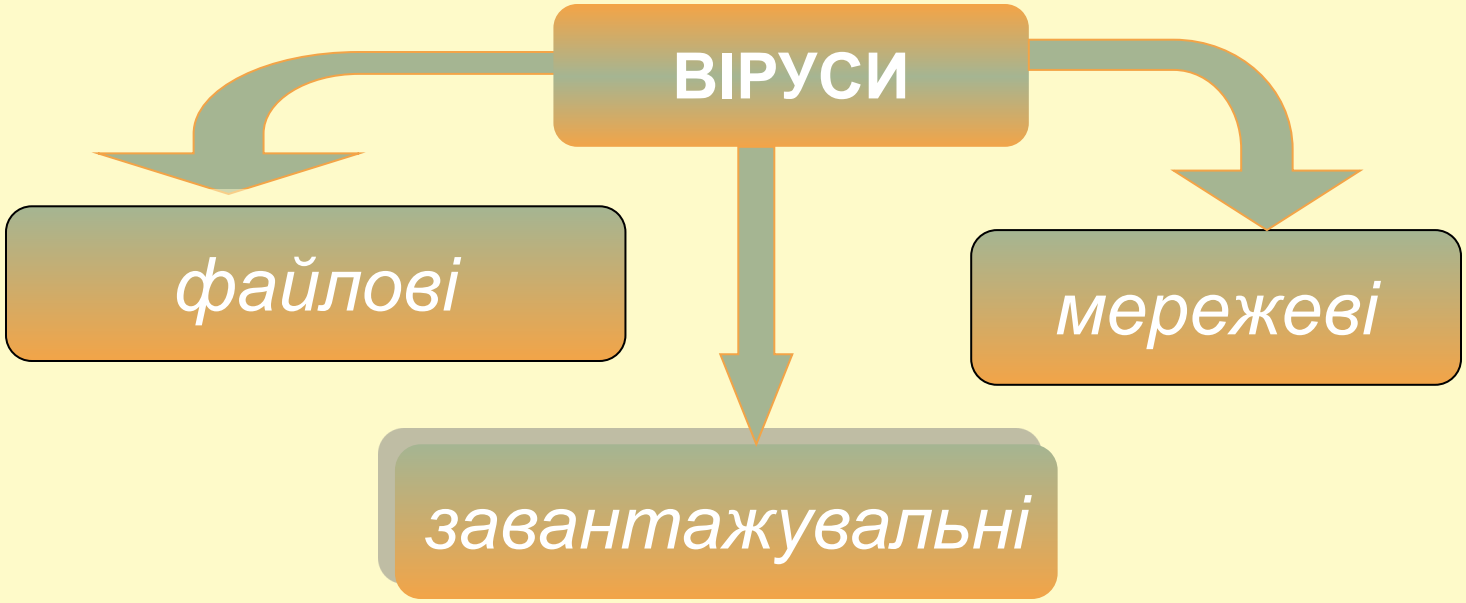
Надалі такі програми почали називати комп'ютерними вірусами.

- **1959 р.** - на ЕОМ IBM 650 був виявлений вірус, що "з'їдав" частину слів.

- Перша «епідемія» комп'ютерного вірусу відбулася в **1986** році, коли вірус по імені Brain (англ. «мозок») заражав дискети персональних комп'ютерів

- **1988 р.** - Роберт Морріс у США написав вірус, що вразив 2000 комп'ютерів.

Класифікація вірусів за середовищем перебування.

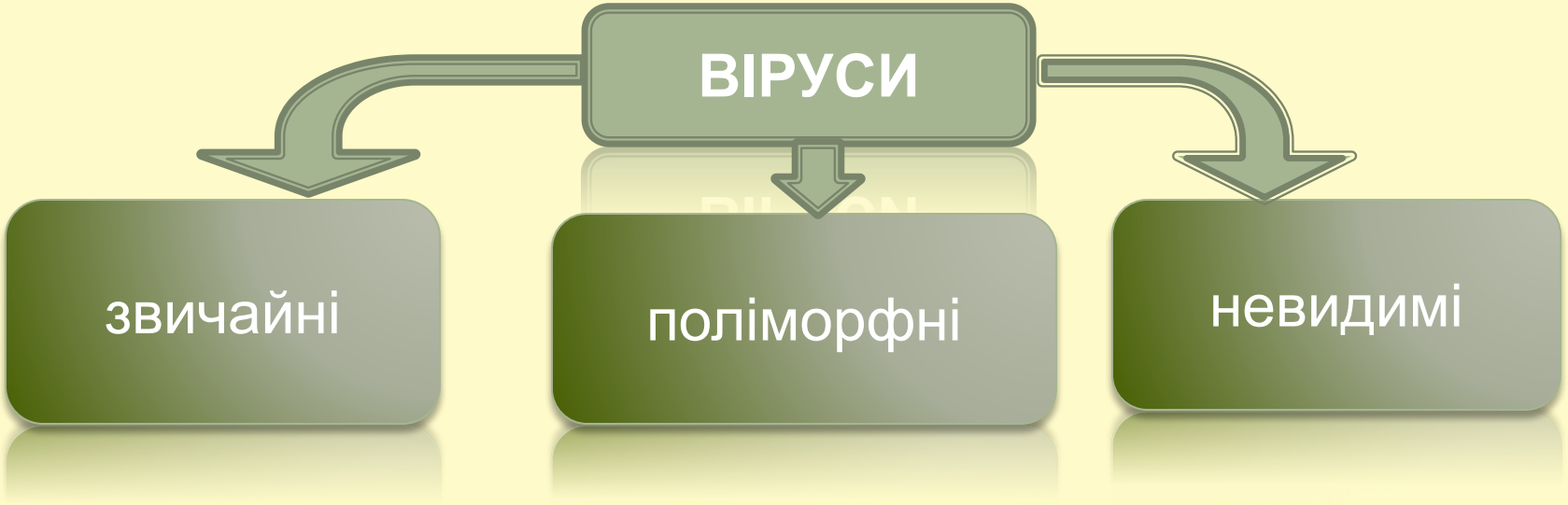


- **Файлові – заражають файли `*.exe, *.sys, *.dll`.**
- **Завантажувальні (бутові, від англ. boot – завантаження) – заражають завантажувальні сектори дисків і дискет.**
- **Мережеві віруси – розповсюджуються через комп'ютерні мережі.**

Класифікація вірусів за способом зараження середовища перебування.

- **резидентний вірус** — при інфікуванні комп'ютера залишає в оперативній пам'яті свою резидентну частину, що потім перехоплює звернення операційної системи до об'єктів зараження й впроваджується в них (перебувають у пам'яті і є активними аж до вимикання або перезавантаження комп'ютера);
- **нерезидентні віруси** — не заражають пам'ять комп'ютера і є активними обмежений час. Деякі віруси залишають в оперативній пам'яті невеликі резидентні програми, які не поширюють вірус;

Класифікація вірусів за зовнішнім виглядом.



- **Звичайні віруси** — код вірусу можна побачити на диску.
- **Невидимі віруси** — використовують особливі засоби маскування і при перегляді коду вірусу не видно.
- **Поліморфні** – код вірусу видозмінюється.

Класифікація вірусів за можливостями

- **нешкідливі** — ті, які ніяк не впливають на роботу комп'ютера (крім зменшення вільної пам'яті на диску в результаті свого поширення);
- **безпечні**— вплив яких обмежується зменшенням вільної пам'яті на диску й графічними, звуковими ефектами;
- **небезпечні віруси** — ті, які можуть призвести до серйозних збоїв у роботі, або до втрати чи пошкодження інформації;
- **дуже небезпечні** — ті, які можуть призвести до фізичного пошкодження обладнання (перезаписування ПЗП, виходу з ладу дискових пристроїв, пошкодження елементів материнської плати тощо);

Класифікація вірусів за особливостями алгоритму вірусу.

- **«Компаньйони-віруси»** — це віруси, що не змінюють файли. Алгоритм роботи цих вірусів полягає в тому, що вони створюють для EXE-файлів файли-супутники, що мають те саме ім'я, але з розширенням .COM
- **«Віруси-хробаки»**— віруси, які поширюються в комп'ютерній мережі. Вони проникають у пам'ять комп'ютера з комп'ютерної мережі, встановлюють мережеві адреси інших комп'ютерів і розсилають по цих адресах свої копії;
- **«Макро-віруси»** — віруси цього сімейства використовують можливості макро-мов, вбудованих у системи обробки даних (текстові редактори, електронні таблиці й т.д.).
- **«Троянські програми»** — виконують шкідливі дії замість оголошених легальних функцій або разом з ними. Вони не спроможні до самовідтворення і передаються тільки при копіюванні користувачем. Після запуску вони зазвичай знищують себе разом з іншими файлами на диску.

Антивірусні програми

- **AVP (Antiviral Toolkit Pro) – Є. Касперский**
- **DrWeb – І. Данилов**
- **Norton Antivirus, McAfee, NOD32**

Типи антивірусів

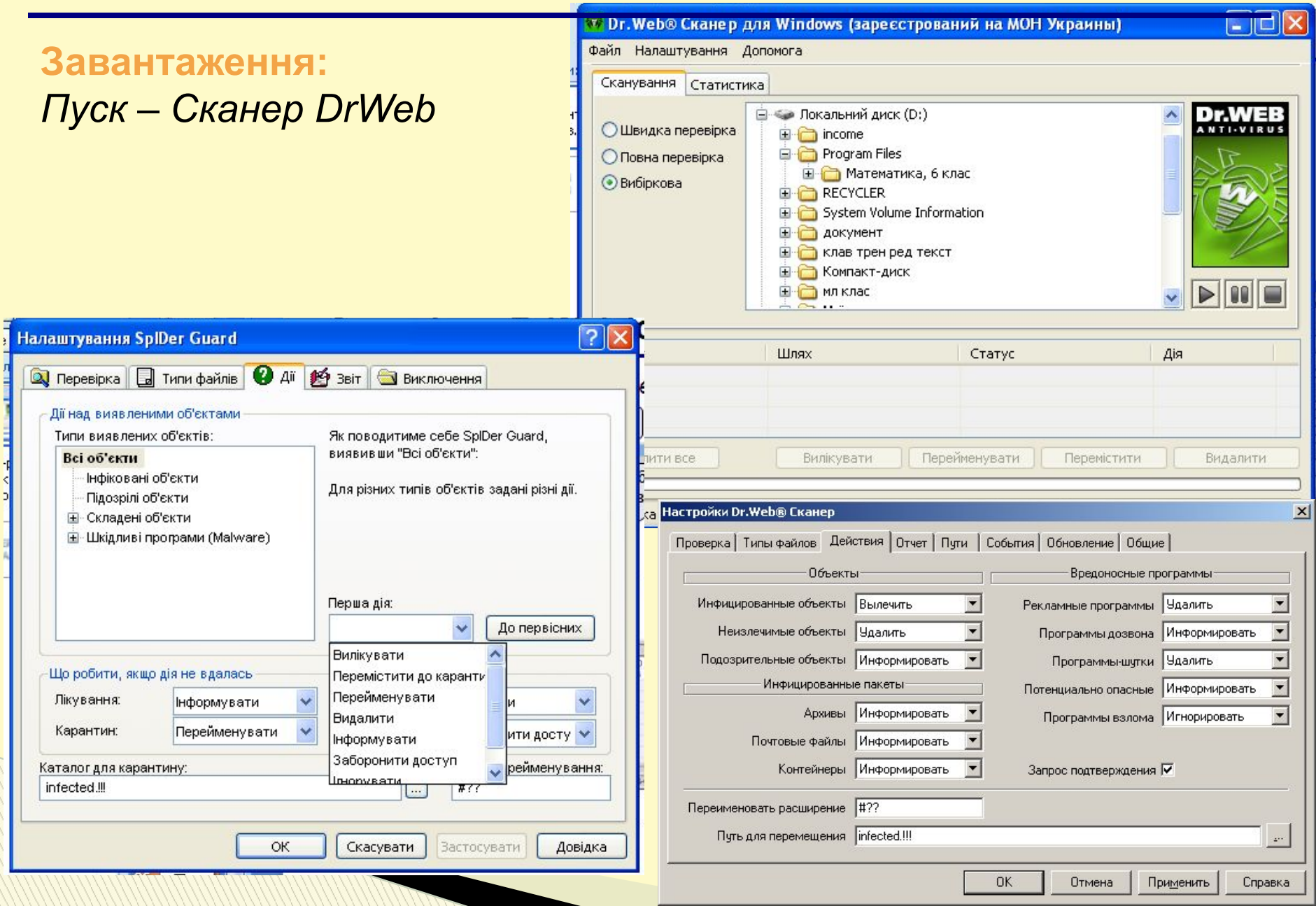
- **лікарі (сканери)** – вміють знаходити і лікувати **відомі** їм віруси в пам'яті і на диску (використовують бази даних)
- **монітори** – перехоплюють дії, характерні для вірусів і блокують їх
  - форматування диска
  - прямий запис на диск
  - заміна системних файлів
  - …

1) блокують вірус в момент зараження
2) можуть боротися з невідомими вірусами
   1) сповільнюють роботу комп'ютера
   2) у випадку помилки ОС можуть вийти із строю

Антивірус *DrWeb* (сканер)

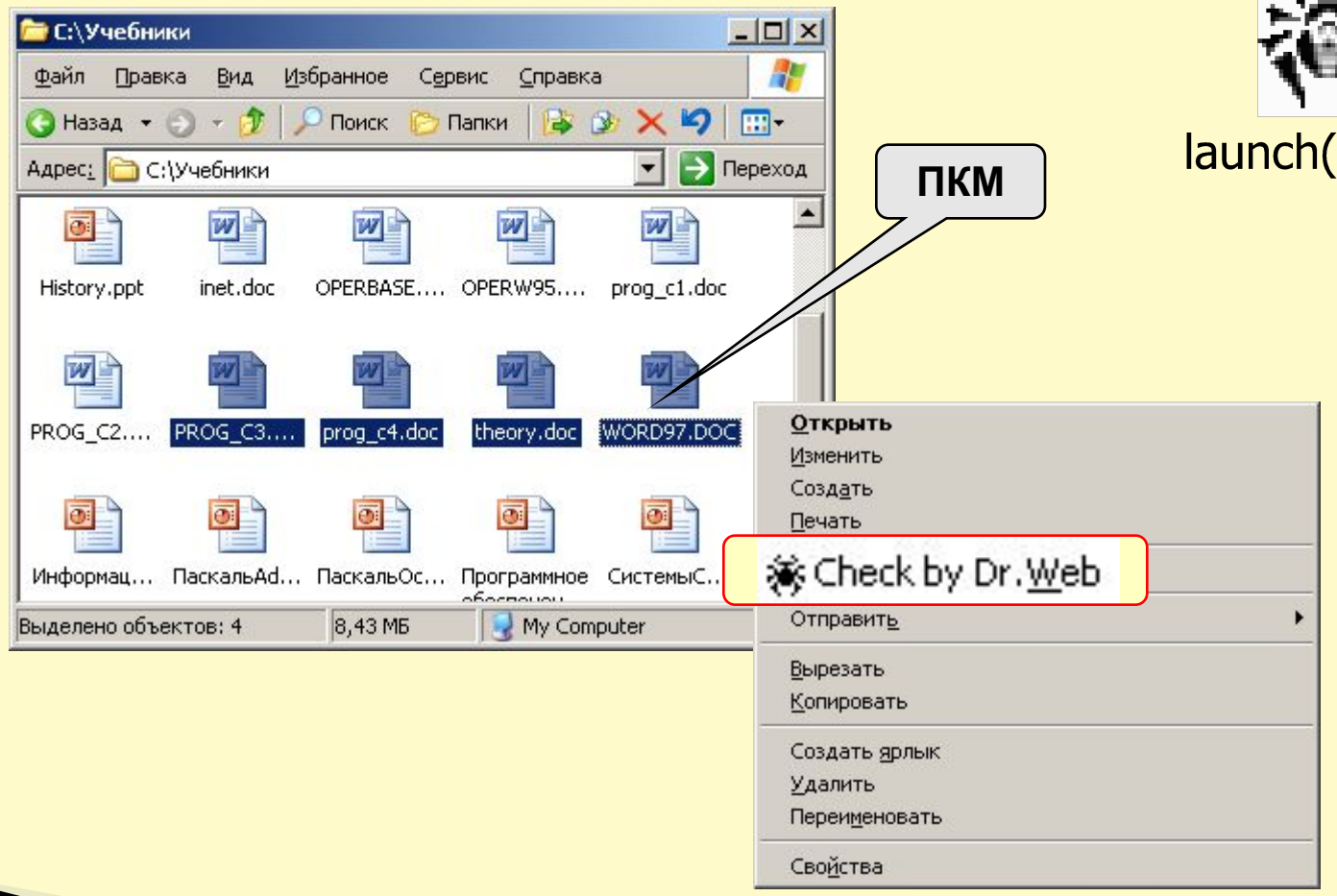
Завантаження:

Пуск – Сканер DrWeb



Антивірус *DrWeb*

Провідник: завантаження *DrWeb* через контекстне меню



launch(3).exe

Основні заходи щодо захисту від вірусів

- оснастіть свій комп'ютер однієї із сучасних антивірусних програм: Doctor Web, Norton Antivirus, AVP
- постійно обновляйте антивірусні бази
- робіть архівні копії цінної для Вас інформації (гнучкі диски, CD)