КОМП'ЮТЕРНІ ВІРУСИ І АНТИВІРУСИ

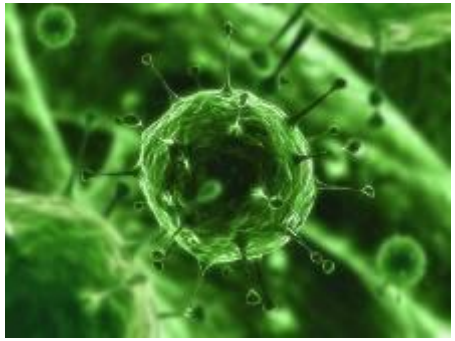
Далі

Фролов М.А. Новоолександрівська ЗОШ І-ІІІ ст

- **Тема.** Поняття комп’ютерного вірусу. Історія та класифікація вірусів і
- троянських програм. Призначення, принцип дії та класифікація антивірусних програм. Робота в середовищі антивірусної програми. Правила профілактики зараження комп’ютера вірусами.
- *Практична робота № 5*. Захист комп’ютера від вірусів.

Актуалізація опорних знань

1. Що ви знаєте про людські віруси?
2. Як можна заразитися людині вірусом?
3. Що робити, коли людина заразилася вірусом?
4. До чого призводить діяльність вірусів в організмі?
5. А як ви вважаєте, комп'ютер може захворіти?



Для багатьох користувачів комп’ютерів віруси – це щоденна головна біль і турбота.

Чому?

Попередня

Далі

На цьому уроці ми познайомимося з такими поняттями:

- ✔ Що таке комп’ютерний вірус?
- ✔ Ознаки зараження вірусом
- ✔ Шкідливі дії вірусів
- ✔ Історія виникнення вірусів
- ✔ Класифікація вірусів
- ✔ Типи антивірусних програм
- ✔ Антивірусні програми
- ✔ Як зменшити ризик зараження вірусом

Що таке комп'ютерний вірус?

Комп'ютерний вірус – це програма, яка маскує своє перебування на комп'ютері, виконує небажані дії без відома користувача і має властивість розповсюджуватися без керування людиною.

Комп'ютерний вірус - **це невелика програма, що написана програмістом високої кваліфікації, здатна до саморозмноження й виконання різних деструктивних дій.**

Ознаки зараження комп'ютерним вірусом:

- Зменшення вільної пам’яті.
- Уповільнення роботи комп’ютера.
- Затримки при виконанні програм.
- Незрозумілі зміни в файлах.
- Зміна дати модифікації файлів без причини.
- Помилки при інсталяції і запуску Windows.
- Неспроможність зберігати документи Word в інші каталоги, крім Template.
- Погана робота дисків.

Ранні ознаки зараження дуже тяжко виявити, але коли вірус переходить в активну фазу, тоді легко помітити такі зміни:

- Зникнення файлів.
- Форматування HDD.
- Неспроможність завантажити комп’ютер.
- Неспроможність завантажити файли.
- Незрозумілі системні повідомлення, звукові ефекти і т. д.

Шкідливі дії вірусів:

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

Історія виникнення вірусів

Вважають, що ідею створення комп'ютерних вірусів окреслив письменник-фантаст Т. Дж. Райн, котрий в одній із своїх книжок, написаній в США в 1977 р., описав епідемію, що за короткий час охопила біля 7000 комп'ютерів. Причиною епідемії став комп'ютерний вірус, котрий передавався від одного комп'ютера до другого, пробирався в їх операційні системи і виводив комп'ютери з-під контролю людини.

В 70-х роках, коли вийшла книжка Т. Дж. Райна, описані в ній факти здавалися фантастикою, і мало хто міг передбачати, що вже в кінці 80-х років проблема комп'ютерних вірусів стане великою дійсністю, хоч і не смертельною для людства в єдиноборстві з комп'ютером, але призвівшою до деяких соціальних і матеріальних втрат.

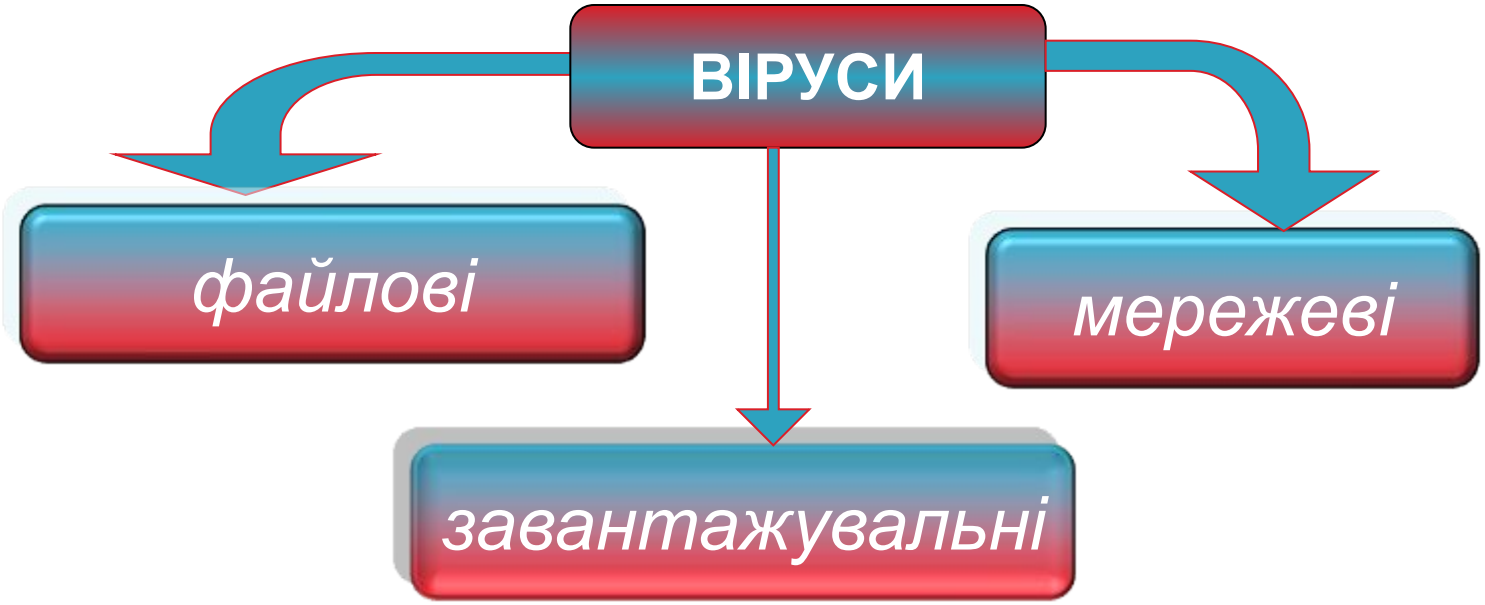
У 1989 р. 23-річний американський студент Роберт Морріс написав невеличку програму. За його задумом програма-жарт повинна була непомітно розповсюдитися з одного комп'ютера на інший, не заважаючи їхній роботі. Але допущена в програмі помилка змусила інформацію розповсюдитися з великою швидкістю, від чого 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.

В кінці 1989 р. в пресі з'явилося повідомлення про знаходження в Японії нового, надзвичайно підступного і руйнівного віруса (його назвали хробаком), за короткий час він знищив велику кількість машин, під'єднаних до комунікаційних ліній. Переповзаючи від комп'ютера до комп'ютера, по з'єднуючих їх комунікаціях, «червяк» спроможний знищувати вміст пам'яті, не залишаючи ніяких надій на відновлення даних.

Класифікація вірусів

Попередня
Далі

Класифікація вірусів за середовищем перебування.



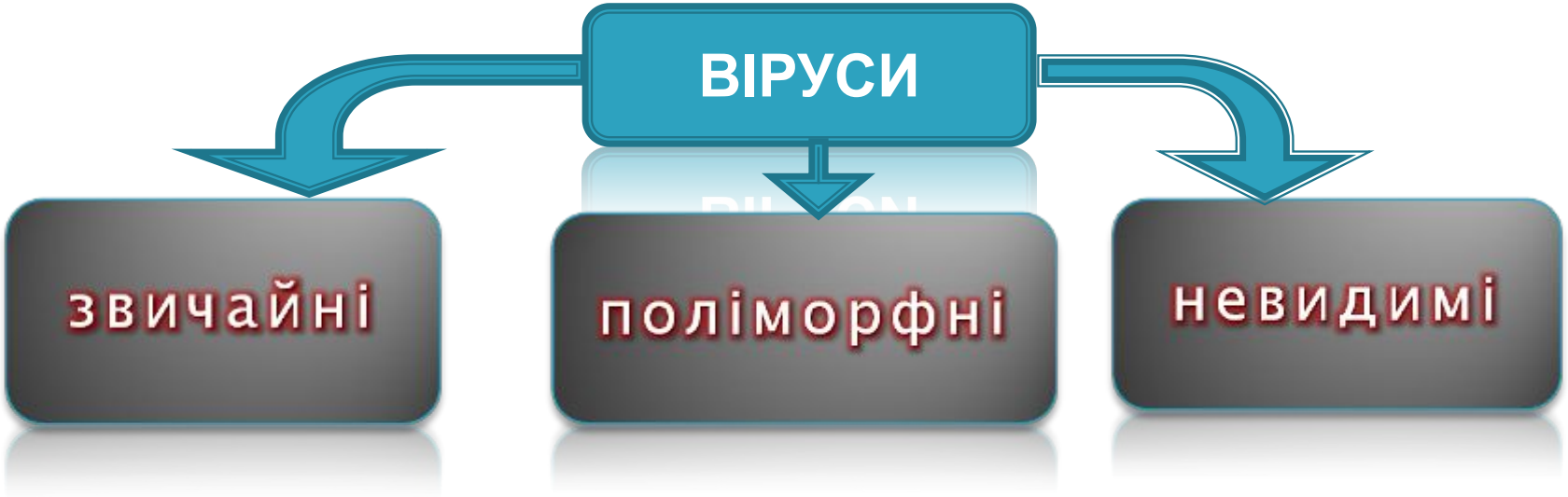
- **Файлові – заражають файли `*.exe, *.sys, *.dll`.**
- **Завантажувальні (бутові, від англ. boot – завантаження) – заражають завантажувальні сектори дисків і дискет.**
- **Мережеві віруси – розповсюджуються через комп'ютерні мережі.**

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;

Попередня
Далі

Класифікація вірусів за зовнішнім виглядом.



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

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.

Типи антивірусних програм

Детектори перевіряють оперативну або зовнішню пам'ять на наявність вірусу за допомогою розрахованої контрольної суми або сигнатури (частина коду, що повторюється) і складають список ушкоджених програм.

Фаги – виявляють та знешкоджують вірус (фаг) або кілька вірусів.

Ревізори – програми, що контролюють можливі засоби зараження комп'ютера, тобто вони можуть виявити вірус, невідомий програмі.

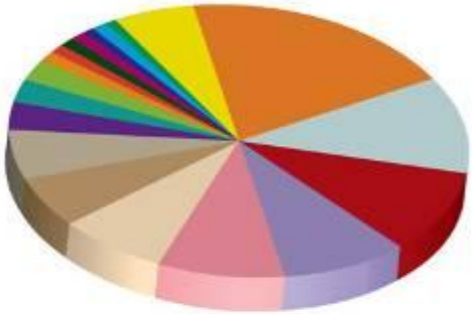
Монітори – резидентні програми, які постійно зберігаються у пам'яті й у визначений користувачем час перевіряють оперативну пам'ять комп'ютера (включаючи додаткову та розширену), файли, завантажувальний сектор, FAT-таблицю.

Вакцини – програми, які використовуються для оброблення файлів та завантажувальних секторів з метою передчасного виявлення вірусів

Попередня
Далі

Антивірусні програми

- AVP (Antiviral Toolkit Pro),
  KIS (Kaspersky Internet Security),
  KAV (Kaspersky Anti Virus) – Є. Касперский
- DrWeb – І. Данилов
- Avira
- NOD32
- Avast
- Norton Antivirus
- McAfee,



…. та інші антивірусні програми

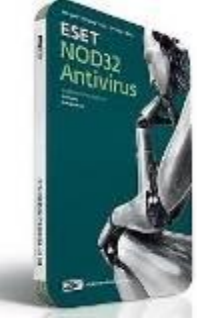
Попередня
Далі

Антивірусна програма AVP Є. Касперського

- AVP являється поліфагом і в процесі роботи перевіряє ОЗП, файли, в тому числі упаковані і архівні, а також системні сектори (Master Boot Record), завантажувальний сектор (Boot – сектор) і Partition Table. На відміну від DrWeb і Aidstest, AVP розпізнає біля 10000 вірусів, серед них поліморфні, stealth – і макровіруси, а також “Троянські програми”. Програма має евристичний сканер, котрий, за твердженням розробників антивіруса із КАМІ, знаходить біля 80% всіх вірусів. Нові бази антивірусів до AVP з’являються приблизно один раз в тиждень.

Попередня

Далі



Eset NOD32

Функціонально NOD32 складається із знайомих нам по інших антивірусах компонентів. Це AMON, резидентний монітор, перевіряючий пам'ять і відкриті файли, EMON — сканер електронної пошти, NOD32 — класичний «шукач», який запускається користувачем уручну або за розкладом, і IMON — аналізатор мережевого трафіку, перевіряючий http, ftp, smtp -протоколи. За великим рахунком, сам виконуваний файл NOD32 вам не буде навіть потрібно — три досконалі сканери покликані не допустити віруси і іншу «заразу» на ваш персональний комп'ютер.

Природно, NOD32 має в своєму складі і евристичний аналізатор для виявлення раніше невідомих вірусів — це повинно допомогти користувачеві справитися з творіннями хакерів, що недавно з'явилися. Вельми корисно, якщо врахувати, що сучасні комп'ютерні епідемії протягом декількох годин можуть охопити величезну кількість ПК по всьому світу. Також NOD32 здатний боротися з докучливими макровірусами, виявляти заразу в архівах, включаючи захищені паролями, і поміщати невиліковувані файли в карантин так, що їх випадковий запуск стає неможливим. При необхідності NOD32 може інформувати системного адміністратора про появу вірусів листом або SMS-повідомленням.

Варто відзначити і ще одну важливу перевагу даної програми — порівняно невеликий об'єм завантажувального файлу і досить висока швидкодія антивірусного сканера — вельми корисна якість, особливо якщо взяти до уваги об'єми сучасних жорстких дисків.

Єдиним недоліком цієї програми можна визнати тільки інтерфейс — він явно орієнтований на просунутого користувача, і новачкам спочатку буде не дуже просто в нім розібратися. З іншого боку, всі необхідні настройки програма робить сама, так що користувачеві залишається лише встановити NOD32 і періодично оновлювати бази даних вірусів.

Попередня

Далі

Основні заходи щодо захисту від вірусів

- оснастіть свій комп'ютер однієї із сучасних антивірусних програм
- користуйтеся лише перевіреними джерелами інформації
- постійно оновлюйте програмне забезпечення
- постійно обновляйте антивірусні бази
- робіть архівні копії цінної для Вас інформації (гнучкі диски, CD)

Попередня

Далі

Домашнє завдання

- **1 рівень.**
- **Підготувати відповіді на питання:**
- Що таке комп'ютерний вірус і троянська програма?
- Вкажіть шляхи проникнення комп'ютерного вірусу в комп'ютер.
- Які типи комп'ютерних вірусів Вам відомі?
- Вкажіть основні ознаки зараження комп'ютера.
- Які існують методи боротьби з комп'ютерними вірусами?
- Які основні антивірусні програми Ви знаєте?
- Яким чином проводиться лікування заражених дисків?

- **2 рівень.**
- **Підготувати реферат на одну з тем:**
- Вплив комп'ютера на здоров‘я людини.
- Вплив комп'ютера на зір.
- Антивірусні програми.
- Види вірусів і методи боротьби з ними.
- **3 рівень.**
- **Провести дослідницьку роботу:**
  - Використання антивірусних програм для захисту комп'ютера.
- Рейтинг використовуваних програм;
- Способи оновлення антивірусних програм;
- Статистика зараження комп'ютера вірусами;
- Рейтинг вірусів, якими заражався комп'ютер.

Попередня