Міністерство освіти і науки України
КНУБА

Тема: Компютерні віруси та антивірусні програми

Виконала
студентка
групи БІКС-11
Гавенко Валерія
Віталіївна

Київ 2016

Комп'ютерні віруси та антивірусні програми

Тезаріус. Історична довідка.

Комп'ютерний вірус (англ. *computer virus*) — комп'ютерна програма, яка має здатність до прихованого само розмноження. Одночасно зі створенням власних копій віруси можуть завдавати школи: знищувати, пошкоджувати, викрадати дані, знижувати або й зовсім унеможливлювати подальшу працездатність операційної системи комп'ютера.

Антивірусна програма (антивірус) — програма для знаходження і лікування програм, що заражені комп'ютерним вірусом, а також для запобігання зараження файлу вірусом.

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 ОС і виводив комп'ютери з-під контролю людини.

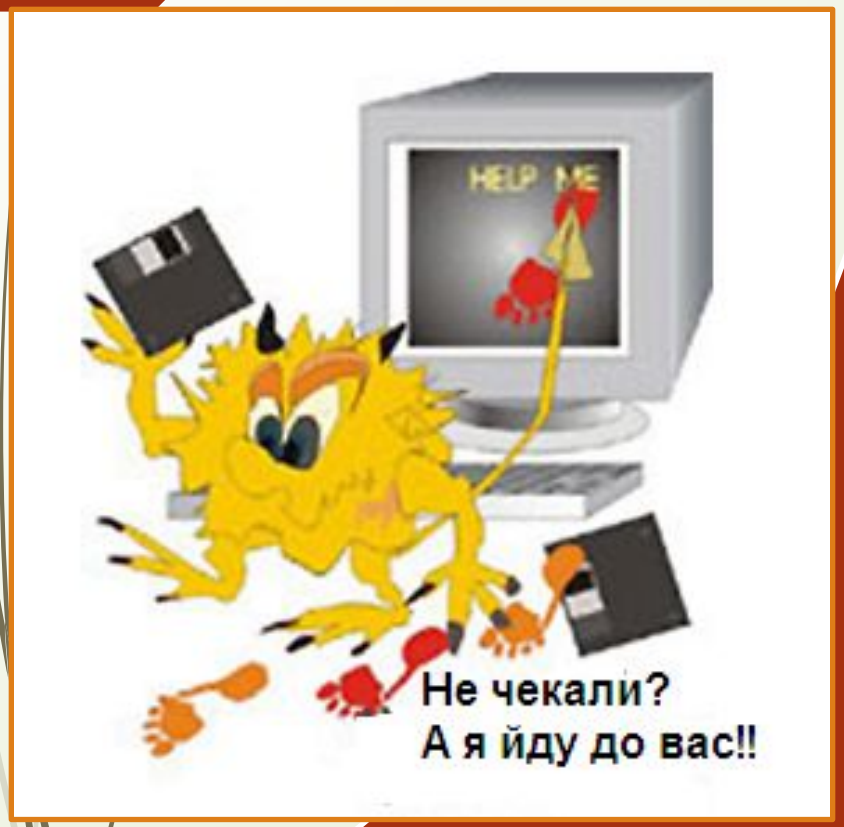
Роберт Морріс є винахідником "черв'яка Морріса". Ця програма стала першою програмою-вірусом, яка поширювалася через Інтернет.

Більше 6 000 комп'ютерів було виведено з ладу.

Морріса засудили до 3 років умовного ув'язнення, 400 годин суспільно-корисної праці, а також виплатити штраф 10 500 доларів.

http://uk.wikipedia.org

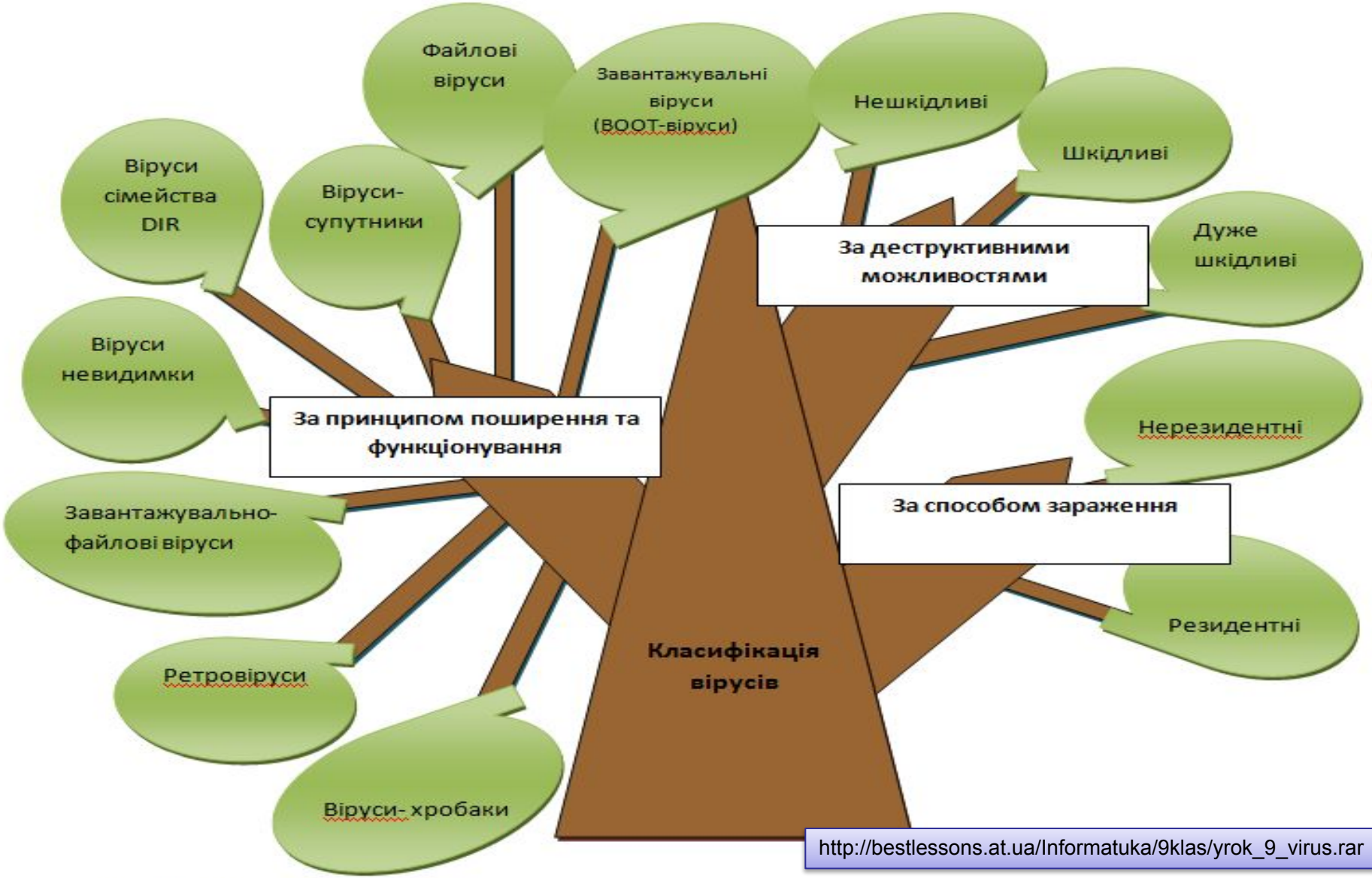
Ознаки діяльності комп'ютерних вірусів



- робота на комп'ютері уповільнюється;
- деякі програми не працюють або працюють неправильно;
- комп'ютер «зависає» ;
- зміна розмірів файлів;
- зникнення файлів та папок або збільшення кількості файлів на диску;
- втрачається доступ до робочих дисків ;
- виведення на екран несподіваних повідомлень, малюнків, подання непередбачених звукових сигналів;
- зменшення обсягу вільної оперативної пам'яті.

http://www.victoria.lviv.ua/html/oit/html/lesson11.htm

Класифікація вірусів



http://bestlessons.at.ua/Informatuka/9klas/yrok_9_virus.rar

Способи зараження комп'ютерними вірусами

- ***Флеш-накопичувачі (флешки)***

  Велика кількість вірусів поширюється через знімальні накопичувачі (цифрові фотоапарати, цифрові відеокамери, цифрові плеєри (MP3-плеєри), мобільні телефони. Використання цього каналу обумовлено можливістю створення на накопичувачі спеціального файлу autorun.inf, в якому можна вказати програму, яка запускається Провідником Windows при відкритті такого накопичувача. Флешки — основне джерело зараження для комп'ютерів, не підключених до Інтернету.

- ***Електронна пошта***

  Зараз один з основних каналів поширення вірусів. Зазвичай віруси в листах електронної пошти маскуються під цілком безпечні вкладення: картинки, документи, музику, посилання на сайти.

- ***Системи обміну миттєвими повідомленнями***

  Також поширена розсилка посилань на нібито фото, музику чи програми, в дійсності це віруси.

- ***Веб-сторінки***

  Можливе зараження через сторінки Інтернет на яких наявні різного типу «активного» вмісту: скриптів, ActiveX-компонентів.

- ***Інтернет і локальні мережі (хробаки)***

  Хробаки — вид вірусів, які проникають в комп'ютер-жертву без участі користувача. Хробаки використовують так звані «діри» в програмному забезпечені операційних систем, щоб проникнути в комп'ютер.

http://lopushno.ucoz.ru/index/informatika_9_klas/0-51

Способи захисту від комп'ютерних вірусів

- резервне копіювання інформації (створення копій файлів і системних областей жорстких дисків);
- уникнення користування випадковими і невідомими програмами;
- перезавантаження комп’ютера перед початком роботи, зокрема у випадку, якщо за цим комп’ютером працювали інші користувачі;
- обмеження доступу до інформації, зокрема фізичний захист диска під час копіювання файлів із неї;
- якомога частіше оновлення версій програмного забезпечення комп’ютера новими антивірусними програмами.

http://uk.wikipedia.org/wiki

Антивірусні програми

- **програми-детектори** здійснюють пошук характерної для конкретного вірусу сигнатури в оперативній пам'яті й у файлах і при виявленні видають відповідне повідомлення. Недоліком таких антивірусних програм є те, що вони можуть знаходити тільки ті віруси, які відомі розроблювачам таких програм;
- **лікарі (фаги)**, а також програми-вакцини не тільки знаходять заражені вірусами файли, а й «лікують» їх, тобто видаляють із файлу тіло програми-вірусу, повертаючи файли у початковий стан. На початку своєї роботи фаги шукають віруси в оперативній пам'яті, знищуючи їх, і тільки потім переходять до «лікування» файлів. Серед фагів виділяють поліфаги, тобто програми-лікарі, призначені для пошуку і знищення значної кількості вірусів. Найбільш відомі з них: Aidstest-, Scan, Norton Antivirus, Doctor Web;
- **програми-ревізори** належать до найнадійніших засобів захисту від вірусів. Ревізори запам' ятовують вихідний стан програм, каталогів і системних областей диска тоді, коли комп'ютер не заражений вірусом, а потім періодично або за бажанням користувача порівнюють поточний стан із вихідним. При порівнянні перевіряються довжина файлу, код циклічного контролю (контрольна сума файлу), дата і час модифікації, інші параметри. Програми ревізори мають досить розвинуті алгоритми, виявляють,Stealth- віруси і можуть навіть очистити змінені версії програми, що перевіряється, від змін, спричинених вірусом. До програм ревізорів належить значно поширена в Україні програма Adinf;
- **фільтри (сторожі)** являють собою невеликі резиденти і програми, призначені для виявлення підозрілих дій при роботі комп'ютера, характерних атак та вірусів. Програми-фільтри дуже корисні, тому що здатні виявити вірус на початковій стадії його існування — до розмноження. Однак вони не «лікують» файли і диски. Для знищення вірусів потрібно застосовувати інші програми, наприклад фаги. Прикладом програми-фільтра є програма Vsafe, що входить до складу пакета утиліт MS DOS;
- **вакцини (імунізатори)** — це резидентні програми, що запобігають зараженню файлів. Вакцини застосовують у разі якщо відсутні програми-лікарі, які «лікують» цей вірус. Вакцинація є можливою тільки від відомих вірусів. Вакцина модифікує програму або диск таким чином, щоб це не відображалося на їх роботі, а вірус сприймав їх зараженими і припиняв спроби зараження. У наш час програми-вакцини практично не застосовуються.

Дякую за увагу!