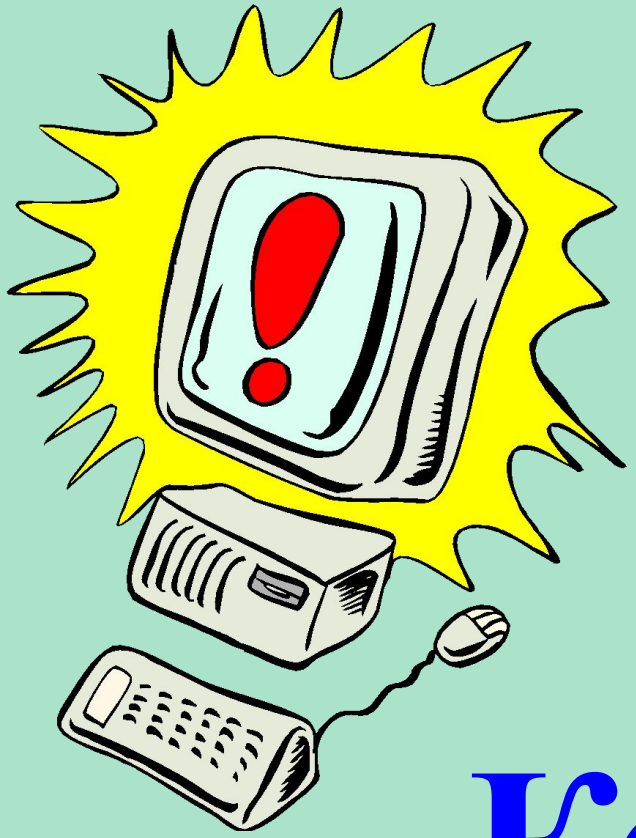


Комп'ютерні віруси

Зміст:

1. Що таке комп'ютерний вірус?
2. Історія комп'ютерних вірусів
3. Класифікація комп'ютерних вірусів
4. Методи виявлення і видалення комп'ютерних вірусів

Що таке комп'ютерний вірус?

Пояснень, що таке комп'ютерний вірус, можна навести декілька. Найпростіше дамо на прикладі клерка, що працює виключно з паперами. Уявімо собі акуратного клерка, який приходить на роботу в контору і кожен день виявляє у себе на столі стопку аркушів паперу зі списком завдань на день. Клерк бере верхній лист, читає вказівки начальства, пунктуально їх виконує, викидає в кошик для паперів "відпрацьований" лист і переходить до наступного аркушу.

Припустимо, що якийсь зловмисник потайки прокрадається в контору і підкладає в стопку із завданнями аркуш, на якому написано наступне: "Переписати цей лист два рази і покласти копії в стопку завдань сусідів". Що зробить клерк? Двічі перепише лист, покладе його сусідам на стіл, знищить оригінал і перейде до виконання наступного листа з стопки, тобто продовжить виконувати свою справжню роботу. Що зроблять сусіди, будучи такими ж акуратними клерками, виявивши нове завдання? Те ж, що і перший: перепишуть його по два рази і роздадуть іншим клеркам. Разом в конторі бродять вже чотири копії первинного документа, які й далі будуть копіюватися і передаватися на інші столи.

Приблизно також працює і комп'ютерний вірус, тільки стопками паперів-вказівок є програми, а клерком - комп'ютер. Як і клерк, комп'ютер акуратно виконує всі команди програми (листи завдань), починаючи з першої. Якщо ж перша команда звучить як - "скопіюй мене в дві інші програми", то комп'ютер так і зробить, і команда-вірус потрапить в дві інші програми. Коли комп'ютер перейде до виконання цих заражених програм, вірус тим же способом буде розходитися все далі і далі по всьому комп'ютеру.

У наведеному вище прикладі про клерка і його контору лист-вірус не перевіряє, заражена чергова папка завдань чи ні. У цьому випадку до кінця робочого дня контора буде завалена такими копіями, а клерки тільки і будуть що переписувати один і той же текст і роздавати його сусідам. Адже перший клерк зробить дві копії, чергові жертви вірусу - уже чотири, потім 8, 16, 32, 64 і т.д., тобто кількість копій кожного разу буде збільшуватися в два рази.

Якщо клерк на переписування одного листа витрачає 30 секунд і ще 30 секунд на роздачу копій, то через годину по конторі буде "бродити" більше 1 000 000 000 000 000 000 копій вірусу! Швидше за все звичайно ж не вистачить паперу, і поширення вірусу буде зупинено по настільки банальної причини.

Як це не смішно (хоча учасникам цього інциденту було зовсім не смішно), саме такий випадок стався в 1988 р в Америці: кілька глобальних мереж передачі інформації виявилися переповненими копіями мережевого вірусу (вірус Морріса), який розсилав себе від комп'ютера до комп'ютера. Тому "правильні" віруси роблять так: "Переписати цей лист два рази і покласти копії в стопку завдань сусідів, якщо у них ще немає
цього листа".
Проблема вирішена - "перенаселення" немає, але кожна стопка містить по копії вірусу,
при цьому клерки ще встигають
справлятися і з звичайною роботою.

"А як же знищення даних?" - Запитаєте ви. Все дуже просто - достатньо написати на аркуші приблизно наступне:

1) Переписати цей лист два рази і покласти копії в стопку завдань сусідів, якщо у них ще немає цього листа.?

2) Переглянути календар і, якщо сьогодні п'ятниця, яка потрапила на 13-е число, викинути всі документи в сміттєву корзину.

Подібну інструкцію добре виконує відомий вірус Jerusalem (інша назва - Time).

До речі, на прикладі клерка дуже добре видно, чому в більшості випадків не можна точно визначити, звідки в комп'ютері з'явився вірус. Всі клерки мають однакові (з точністю до почерку) КОПІЇ, але оригінал-то з почерком зловмисника вже давно в кошику!

Ось таке просте пояснення роботи вірусу. Плюс до нього хотілося б навести дві аксіоми, які, як це не дивно, не для всіх є очевидними.

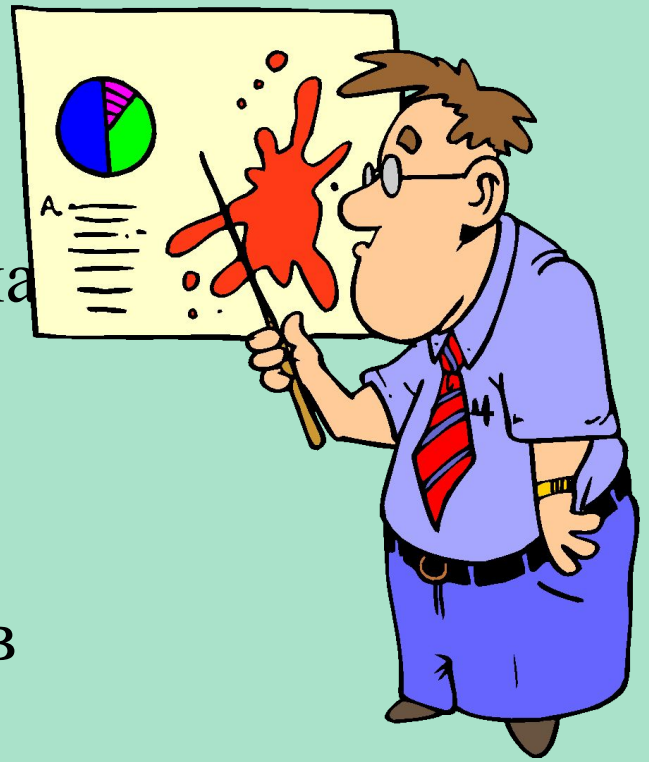
По-перше: віруси не виникають самі собою - їх створюють дуже злі і недобрі програмісти-хакери і розсилають потім по мережі передачі даних або підкидають на комп'ютери знайомих. Вірус не може сам собою з'явитися на вашому комп'ютері: або його підсунули на дискетах або на компакт-диску, або ви його випадково "завантажили" з комп'ютерної мережі передачі даних.

По-друге: комп'ютерні віруси заражають тільки комп'ютер і нічого більше, тому не треба боятися - через клавіатуру і мишу вони не передаються.

Комп'ютерний вірус -

- це спеціально написана програма, зазвичай невелика за розмірами, здатна самостійно дописувати себе до інших програм (заражати їх), і проводити різні небажані дії.

комп'ютерний вірус



Термін "комп'ютерний вірус" з'явився пізніше, офіційно вважається, що його вперше ужив співробітник Лехайского університету (США) Ф.Коен в 1984 р на 7-й ***конференції з безпеки інформації***, проходила в США. З тих пір пройшло чимало часу, гострота проблеми вірусів багаторазово зросла, однак строгого визначення, що ж таке комп'ютерний вірус, так і не дано, незважаючи на те що багато хто намагався це зробити неодноразово.

Програма, всередині якої знаходиться вірус, називається

«зараженої»

Коли така програма починає роботу, то спочатку управління отримує вірус.

Після того, як вірус виконає потрібні йому дії, він передає управління тій програмі, в якій він знаходиться, і вона працює так само, як зазвичай.

Тому представляється можливим сформулювати тільки обов'язкова умова для того, щоб деяка послідовність виконуваного коду була вірусом.

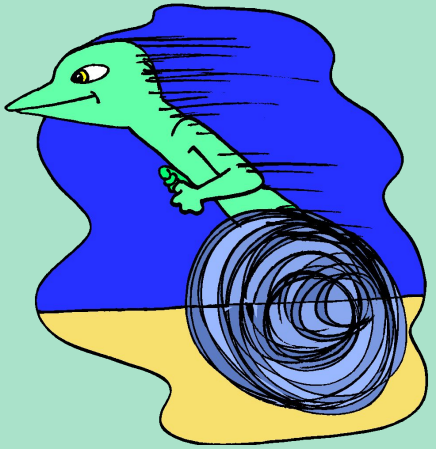
Обов'язкове (необхідне) властивість комп'ютерного вірусу - можливість створювати свої дублікати (не завжди збігаються з оригіналом) і впроваджувати їх в обчислювальні мережі і / або файли, системні області комп'ютера та інші виконувані об'єкти. При цьому дублікати зберігають здатність до подальшого поширення.

Історія комп'ютерних вірусів

Кінець 1960-х - початок 70-х років: "**кролик**" (the rabbit) - програма клонировала себе, займала системні ресурси і таким чином знижувала продуктивність системи.

Перша половина 70-х років: під ОС Tenex створений вірус **The Creeper**, що використав для свого поширення глобальні комп'ютерні мережі. Вірус був в змозі самостійно увійти в мережу через модем і передати свою копію віддаленій системі. Для боротьби з цим вірусом була створена програма **Reeper** - перша відома антивірусна програма.

Історія комп'ютерних вірусів



Початок 80-х років: комп'ютери стають все більш і більш популярними, результат цього - велика кількість різноманітних «троянських коней» - програм, які при запуску наносять системі якої-небудь шкоди.

1981 рік: епідемія завантажувального вірусу Elk Cloner на комп'ютерах Apple II. Вірус записувався в завантажувальні сектори дискет, до яких йшло звернення. Виявляв він себе вельми багатогранно - перевертав екран, змушував блимати текст на екрані і виводив різноманітні повідомлення.

Історія комп'ютерних вірусів

1986 рік: епідемія першого IBM PC-вірусу Brain. Вірус, що заражає 360 Кб дискети, практично миттєво розійшовся по всьому світу. Причина такого «успіху» - швидше за все, в неготовності комп'ютерного суспільства до зустрічі з таким явищем, як комп'ютерний вірус. Вірус був написаний в Пакистані братами Basit і Amjad Farooq Alvi, залишили у вірусі текстове повідомлення, що містить їх імена, адресу та номер телефону. Як стверджували автори вірусу, що були власниками компанії з продажу програмних продуктів, вони вирішили з'ясувати рівень піратського копіювання в їхній країні. На жаль, їх експеримент вийшов за межі Пакистану. Цікаво, що цей вірус був також і першим «стелс» -віруси - при спробі читання зараженого сектора він «підставляє» його незаражених оригінал.

Історія комп'ютерних вірусів

1987 рік: появу вірусу **Vienna** і ще кілька вірусів для IBM PC. Це знамениті в минулому **Lehigh**, що заражає тільки COMMAND.COM, **Suriv**-1 (інша назва - April1st), що заражає COM-файли, **Suriv**-2, що заражає (вперше) EXE-файли, і Suriv-3 заражає як COM-, так і EXE-файли. У грудні 1987 року трапилася перша відома повальна епідемія мережного вірусу **Cristmas Tree**, написаного на мові REXX і поширював себе в операційному середовищі VM / CMS. 9 грудня вірус був запущений в мережу в Західній Німеччині і через чотири дні 13 грудня паралізував мережу IBM Vnet. При запуску вірус виводив на екран зображення різдвяної ялинки і розсилав свої копії всім користувачам мережі.

Історія комп'ютерних вірусів

1988 рік: в п'ятницю 13 травня відразу кілька фірм та університетів різних країн світу познайомилися з вірусом **Jerusalem** - цього дня вірус знищував файли при їх запуску. Це, мабуть, один з перших MS-DOS-вірусів, що став причиною справжньої епідемії: повідомлення про заражених комп'ютерах надходили з Європи, Америки та Близького Сходу. Назва, до речі, вірус отримав за місцем одного з інцидентів - університету в Єрусалимі.

Цього року була створена нова антивірусна програма - Dr.Solomon's Anti-Virus Toolkit, що є на сьогоднішній день одним з найпотужніших антивірусів.

Історія комп'ютерних вірусів

1989 рік: виявлено новий вірус Datacrime, який мав вкрай небезпечне прояв - з 13 жовтня по 31 грудня він форматувати вінчестер.
Слід відзначити той факт, що 1989 був початком повальної епідемії комп'ютерних вірусів в Росії - все ті ж віруси Cascade, Jerusalem, Vienna заполонили комп'ютери наших співвітчизників.

В кінці 1989 року в Росії Е.В. Касперскім була розроблена перша версія антивіруса AVP (AntiViral Toolkit Pro). .

Історія комп'ютерних вірусів

1990 рік: цей рік приніс кілька досить помітних подій. Перше з них - поява поліморфік-вірусів **Chameleon** (інша назва - V2P1, V2P2, V2P6). До цього моменту антивірусні програми для пошуку вірусів користувалися так званими «масками» - шматками вірусного коду. Після виявлення вірусів Chameleon розробники антивірусів були змушені шукати інші методи детектування вірусів.

Друга подія– поява болгарського «заводу з виробництва вірусів»: величезна кількість нових вірусів мало болгарське походження. У липні стався інцидент з комп'ютерним журналом **PC Today** (Великобританія). Він містив гнучкий диск, заражений вірусом **DiskKiller**. Було продано більше 50 000 екземплярів журналу.

Історія комп'ютерних вірусів

1991 рік: популяція комп'ютерних вірусів безперервно зростає, досягаючи вже кількох сотень. У квітні вибухнула справжня епідемія файлово-завантажувального поліморфік-вірусу **Tequila**. Росію ця подія практично не торкнулися.

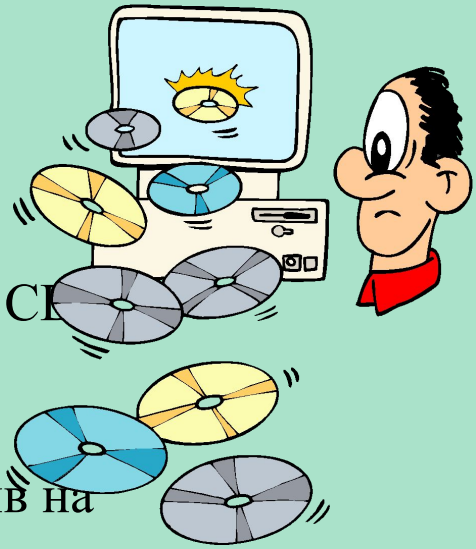
Літо 1991: епідемія вірусу **Dir_II**, який використав принципово нові способи зараження файлів (link-вірус). В цілому 1991 був досить спокійним - отаке затишшя перед бурею, що вибухнула в 1992.

Історія комп'ютерних вірусів

1992 рік: перший **поліморфік-генератор MtE**, на його базі через деякий час з'являється відразу кілька поліморфік-вірусів. Перший вірус для Windows, що заражає виконувані файли цієї ОС, відкрив нову сторінку в вирусописательстве.

1993 рік: з'являється все більше вірусів, що використовують досить незвичайні способи зараження файлів, проникнення в систему і т.д.

Історія комп'ютерних вірусів



1994 рік: все більшого значення набуває проблема вірусів на CD-дисках. Швидко ставши популярними, ці диски і виявилися одним з основних шляхів поширення вірусів.
Зафіксовано відразу декілька інцидентів, коли вірус потрапляв на майстер-диск при підготовці партії CD-дисків. В результаті на комп'ютерний ринок були випущені досить великі тиражі (десятки тисяч) заражених CD-дисків. Природно, що про їх лікуванні говорити не доводиться - їх треба просто знищувати.

У червні почалася повальна епідемія вірусу OneHalf, досі є найпоширенішим в Росії.
Вересень: «***ЗАРАЗА***» - епідемія файлово-завантажувального вірусу, що використовує вкрай незвичайний спосіб впровадження в MS-DOS. Жоден антивірус не виявився готовим до зустрічі з подібного типу монстром.

Історія комп'ютерних вірусів

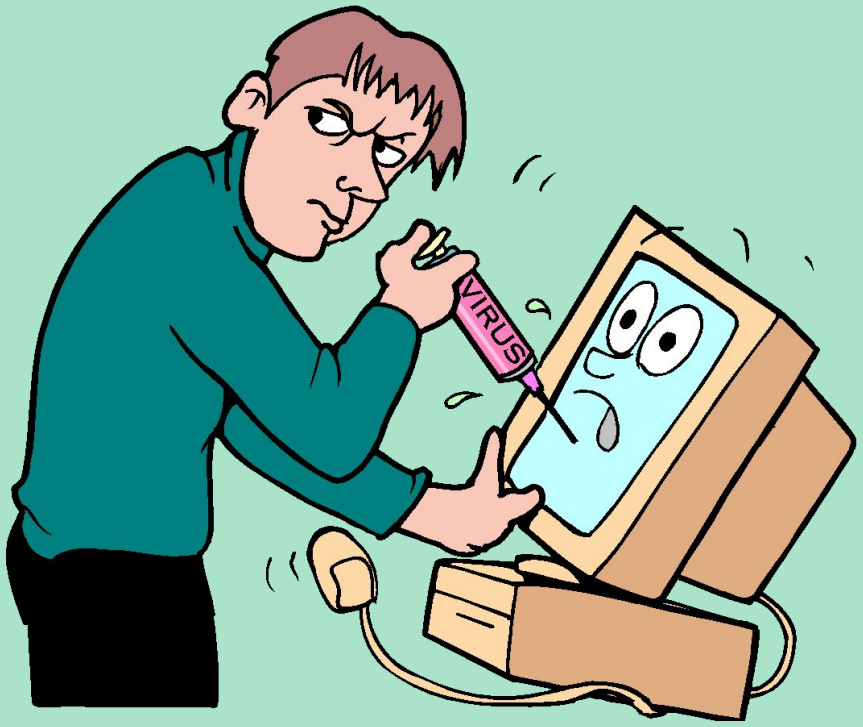
1995 рік: стався інцидент з Microsoft: на диску, що містить демонстраційну версію Windows 95. Копії цього диска були розіслані бета-тестерами, один з яких не полінувався перевірити диск на віруси.

Серпень : один з поворотних моментів в історії вірусів і антивірусів - в «живому вигляді» виявлений перший вірус для Microsoft Word (**Concept**). Буквально за місяць вірус «облетів» всю земну кулю, заповнив комп'ютери користувачів MS-DOS і міцно зайняв перше місце в статичних дослідженнях.

Історія комп'ютерних вірусів

1996 рік: два досить помітних події - з'явився перший вірус для Windows 95 (**Win95.Boza**) і почалася епідемія вкрай складного поліморфік -віруси **Zhengix** в Санкт-Питербурге.? Березень: перша епідемія вірусу для Windows 3.x (**Win.Tentacle**).? Липень: **Laroux** - перший вірус для Microsoft Excel, до того ж спійманий в «живому вигляді».

Історія комп'ютерних вірусів



1997 рік: макровіруси перебралися в Office 97, тому з'явилися віруси, орієнтовані тільки на документи Office 97.
Квітень : ***Homer*** – перший мережевий вірус-хробак, що використовує для свого розмноження File Transfer Protocol (ftp).?
Червень: поява першого самошифруються вірусу для Windows 95.

Історія комп'ютерних вірусів

2000 рік: поява і епідемія в Росії вірусу «***I love You***».

Класифікація комп'ютерних вірусів:

Віруси можна розділити на класи за такими основними ознаками :

1. ***середовище проживання;***
2. ***спосіб зараження середовища проживання);***
3. ***особливості алгоритму роботи;***
4. ***деструктивні можливості.***

Залежно від **довкілля** віруси можна розділити на:

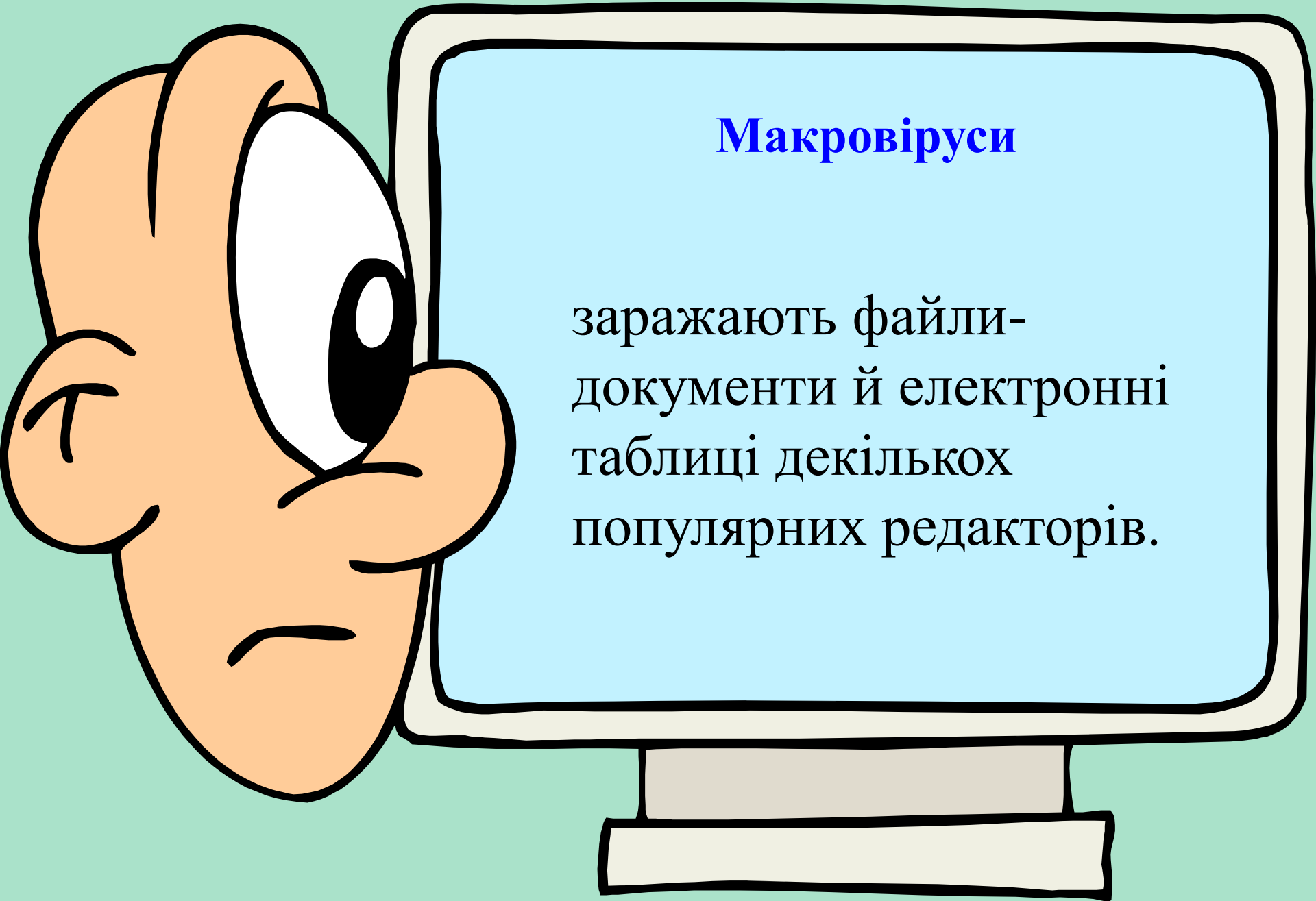
- ***файлові;***
- ***завантажувальні;***
- ***макровіруси;***
- ***мережеві.***

файлові віруси

або різними способами впроваджуються у виконувані файли (найбільш поширений тип вірус), або створюють файли-двійники (віруси-компаньйони), або використовують особливості організації файлової системи (link-віруси).

Завантажувальні віруси

записують себе або в завантажувальний сектор диска (boot-сектори), або в сектор, що містить системний завантажувач вінчестера (Master Boot Record), або змінюють покажчик на активний boot-сектор.



Макровіруси

заражають файли-документи й електронні таблиці декількох популярних редакторів.

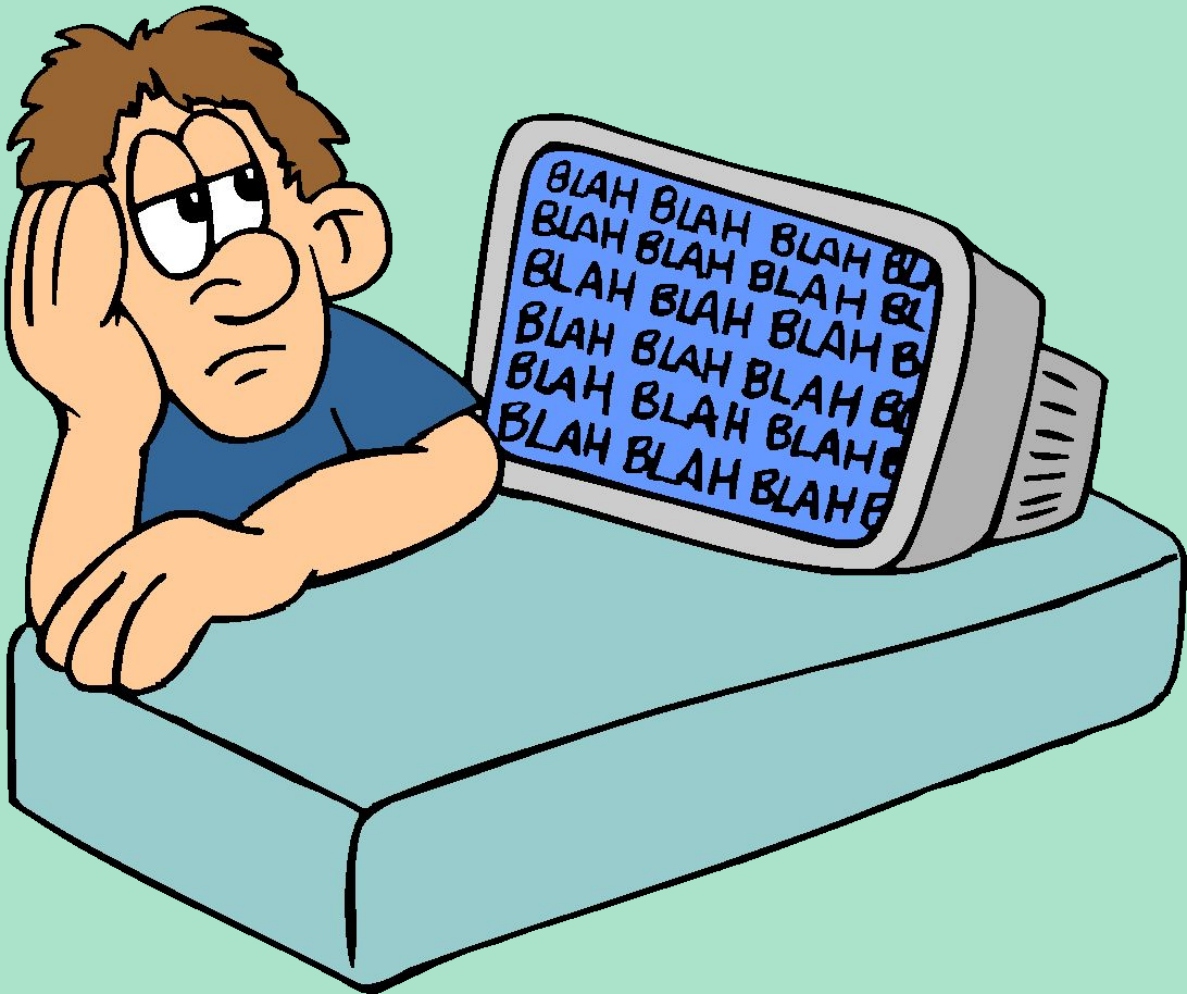
Мережеві віруси

використовують для свого поширення протоколи або команди комп'ютерних мереж і електронної пошти.

Існує велика кількість сполучень, наприклад **файловий-завантажувальні віруси**, заражающие як файли, так і завантажувальні сектори дисків. Такі віруси, як правило, мають досить складний алгоритм роботи, часто застосовують оригінальні методи проникнення в систему, використовують «стелс» і поліморфік-технології.

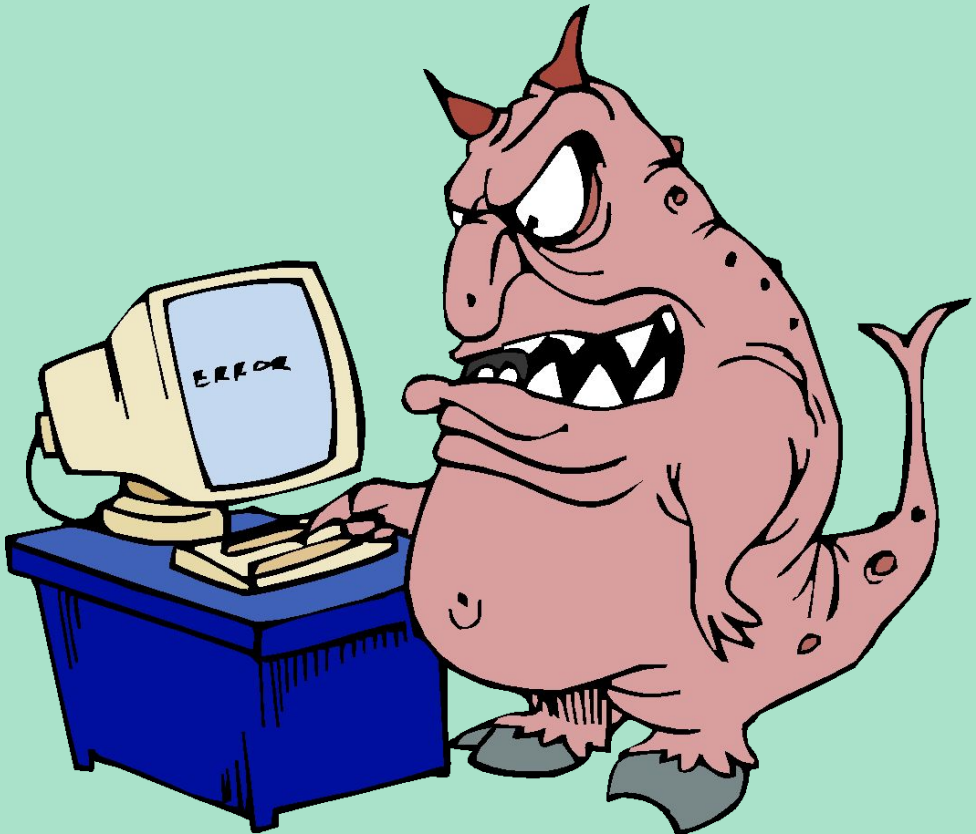
Інший приклад такого сполучення - **мережний макровірус**, який не тільки заражає редаговані документи, а й розсилають свої копії по електронній пошті.

Заражається **операційна система** є другим рівнем розподілу вірусів на класи. Кожен файловий чи мережний вірус заражає файли який-небудь однієї або декількох ОС.



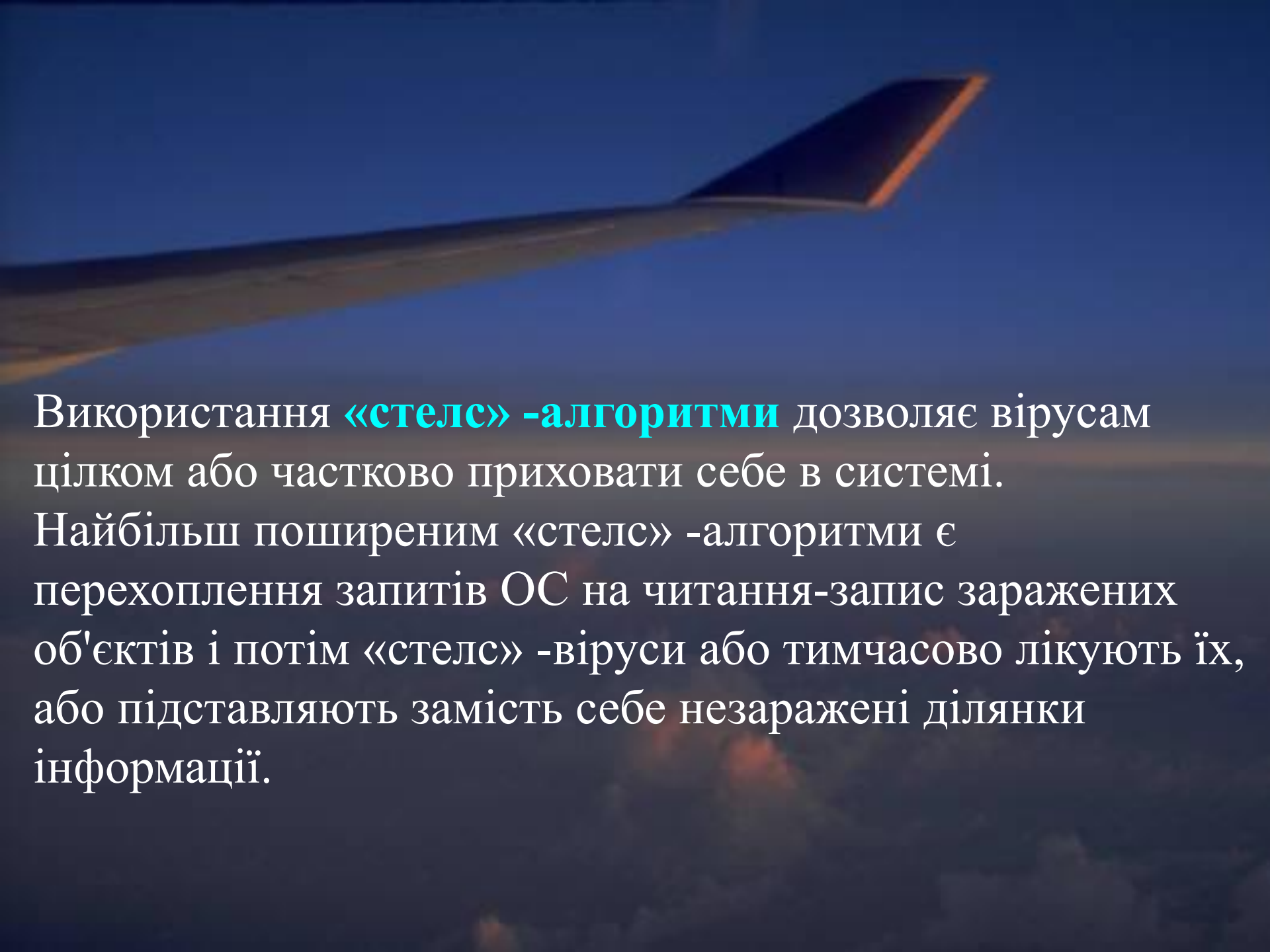
Серед **особливостей алгоритму роботи** вірусів виділяються наступні:

- ***резидентність***;
- ***використання «стелс» -алгоритми***;
- ***самошифрування і поліморфічность***;
- ***використання нестандартних прийомів***.



Резидентний вірус

при інфікуванні комп'ютера залишає в оперативній пам'яті свою резидентну частину, яка потім перехоплює звернення ОС до об'єктів зараження і впроваджується в них. Ці віруси знаходяться в пам'яті і є активними аж до вимикання комп'ютера або перезавантаження ОС.

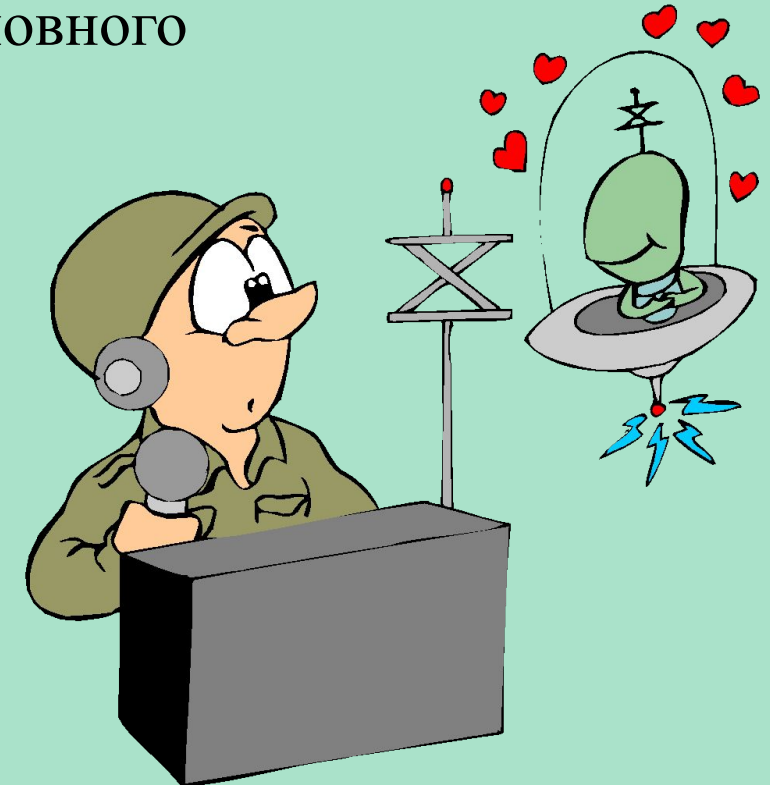


Використання **«стелс» -алгоритми** дозволяє вірусам цілком або частково приховати себе в системі. Найбільш поширеним «стелс» -алгоритми є перехоплення запитів ОС на читання-запис заражених об'єктів і потім «стелс» -віруси або тимчасово лікують їх, або підставляють замість себе незаражені ділянки інформації.

Самошифрування і поліморфічность використовуються практично всіма типами вірусів для того, щоб максимально ускладнити процедуру виявлення вірусу.

Полиморфик-віруси досить важко піддаються виявленню; вони не мають сигнатур, тобто не містять жодного постійної ділянки коду. У більшості випадків два зразки того самого поліморфік-вірусу не будуть мати жодного збігу.

Це досягається шифруванням основного тіла вірусу і модифікаціями програми-расшифровщика.



За **діструктівним** можливостям віруси можна розділити на:? - Нешкідливі, тобто ніяк що 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 і графічним, звуковим та іншими ефектами;

- Небезпечні віруси, які можуть призвести до серйозних збоїв у роботі комп'ютера;

- Дуже небезпечні– в алгоритм їх роботи свідомо закладені процедури, які можуть викликати втрату програм, знищити дані, стерти необхідну для роботи комп'ютера інформацію, записану в системних областях пам'яті, і навіть, як говорить одна з неперевірених комп'ютерних легенд, сприяти швидкому зносу рухомих частин механізму - вводити в резонанс і руйнувати голівки деяких типів вінчестерів.

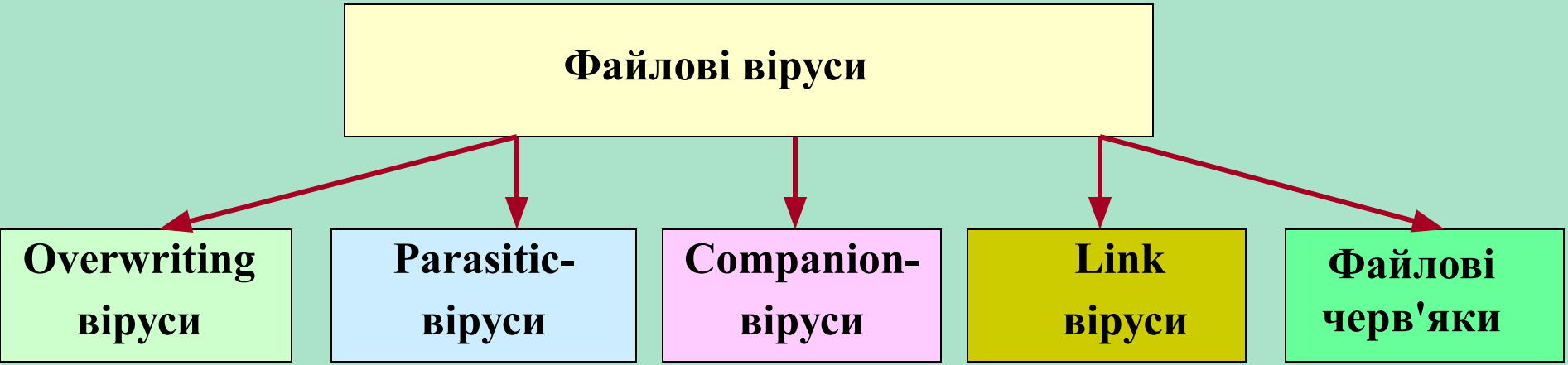
Файлові віруси

До даної групи відносяться віруси, які при своєму розмноженні тим або іншим способом використовують файлову систему якої-небудь (або будь-яких) ОС.

Файлові віруси можуть впроваджуватися практично у всі виконувані файли всіх популярних ОС. На сьогоднішній день відомі віруси, вражають всі типи виконуваних об'єктів стандартної DOS: командні файли (BAT), що завантажуються драйвери (SYS, в тому числі спеціальні файли IO.SYS і MSDOS.SYS) і виконувані двійкові файли (EXE, COM). Існують віруси, що вражають виконувані файли інших ОС - Windows 3.x, Windows 95 / NT, OS / 2, Macintosh, Unix, включаючи VxD-драйвери Windows 3.x і Windows 95.

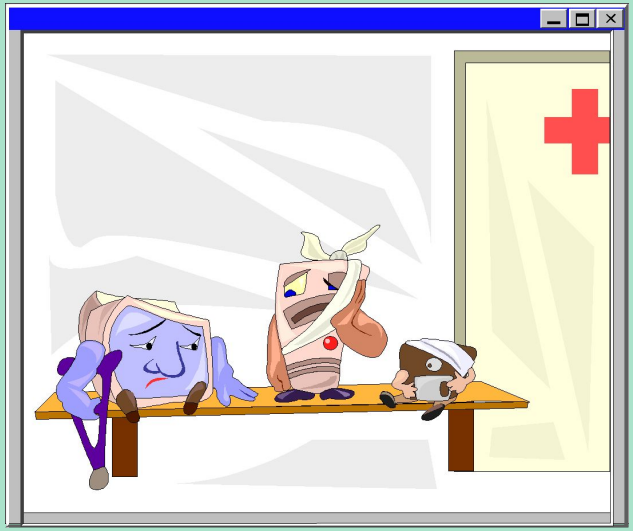
Файлові віруси

За способом зараження файлів віруси діляться на:



Overwriting-віруси

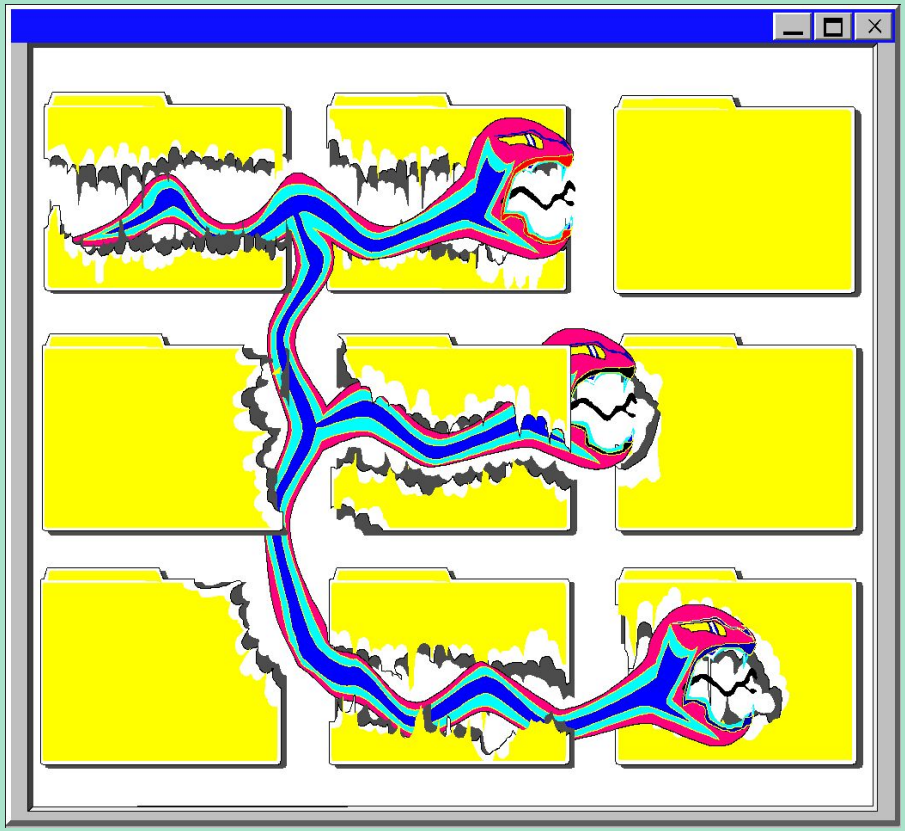
Даний метод зараження є найбільш простим: вірус записує свій код замість коду заражає файли, знищуючи його вміст. Природно, що при цьому файл перестає працювати і не відновлюється. Такі віруси дуже швидко виявляють себе, так як ОС і додатки досить швидко перестають працювати. Чи не відомо жодного випадку, коли подібного типу віруси були б виявлені "в живому вигляді" і стали причиною епідемії.



До різновиду overwriting-вірусів належать віруси, що записуються замість DOS-заголовка NewEXE-файлів. Основна частина файлу при цьому залишається без змін і продовжує нормально працювати в відповідне ОС, однак DOS-заголовок виявляється зіпсованим.

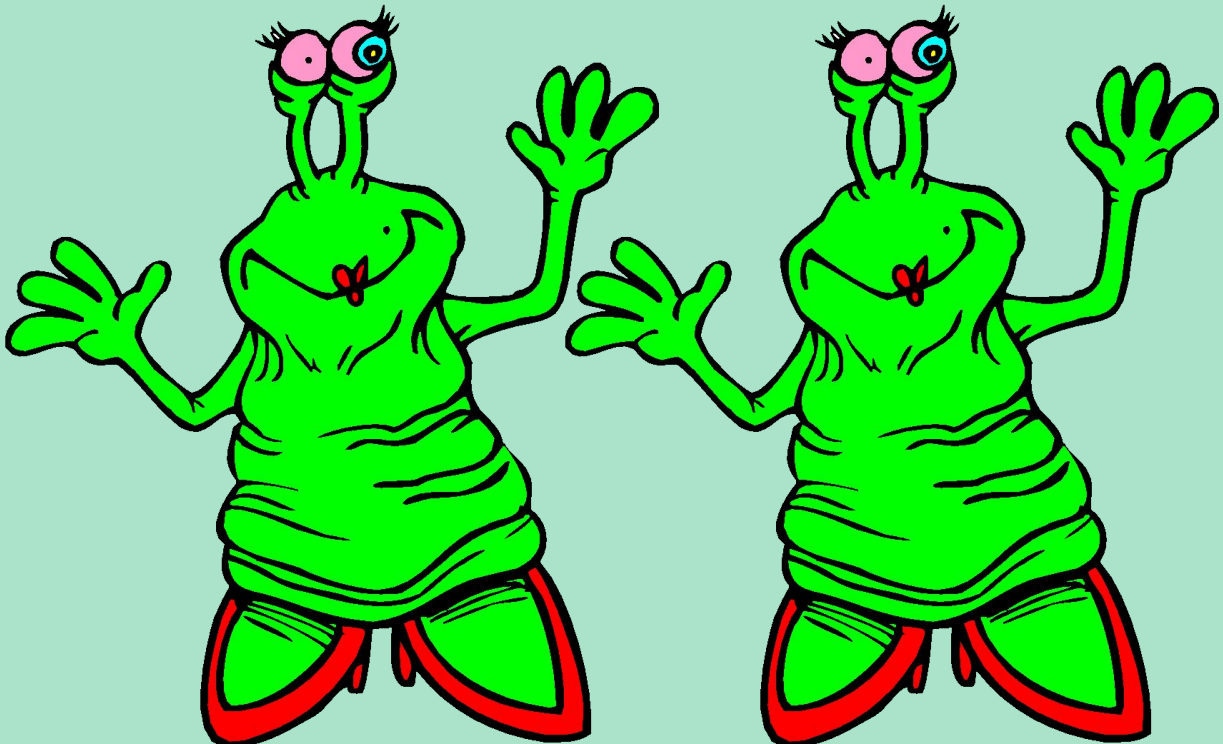
Parasitic-віруси

До паразитичним відносяться всі файлові віруси, які при поширенні своїх копій обов'язково змінюють вміст файлів, залишаючи сам файли при цьому повністю або частково працездатними. Основними типами таких вірусів є віруси, що записуються в початок файлів (prepending), в кінець файлів (appending) і в середину файлів (inserting). У свою чергу, впровадження вірусів в середину файлів відбувається різними ми методами - шляхом перенесення частини файлу в його кінець або впровадження у свідомо невикористовувані дані файлу (cavity-віруси).



Companion-віруси

До категорії компаньйон-вірусів належать віруси, що не змінюють заражаємо файлів. Алгоритм роботи цих вірусів полягає в тому, що для заражає файли створюється файл-двійник, причому при запуску зараженого файлу управління отримує саме цей двійник, т. Е. Вірус.



Link-віруси

Link-віруси, як і компаньйон-віруси, не змінюють фізичного вмісту файлів, однак при запуску зараженого файлу змушують ОС виконай свій код. Цієї мети вони досягають модифікацією необхідних полів файлової системи.

На сьогоднішній день відомий єдиний тип link-вірусів - вірус сімейства **Dir_II**. При зараженні системи вони записують своє тіло в останній кластер логічного диска. При зараженні файлу віруси коректують лише номер першого кластера файлу, розташований у відповідному секторі каталогу.
Новий початковий кластер файлу буде вказувати на кластер, що містить тіло вірусу. Таким чином, при зараженні файлів і довжина і вміст кластерів з цими файлами не змінюються, а на всі заражені файли на одному логічному диску буде припадати тільки одна копія вірусу.

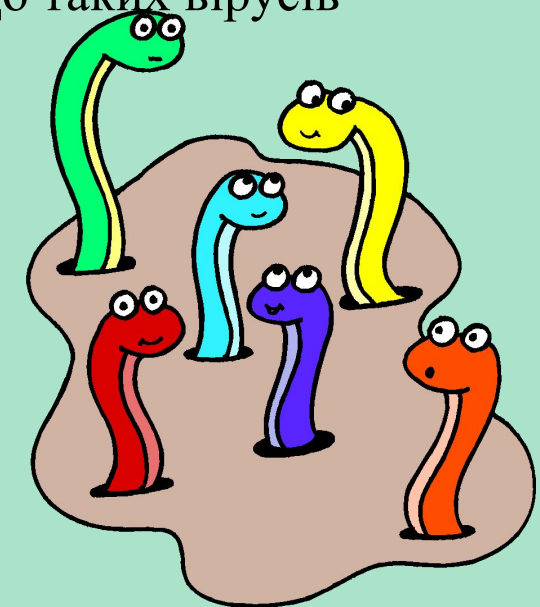
До зараження дані каталогу зберігають адресу першого кластера файлу.? Після зараження дані каталогу вказують на вірус, т. Е. При запуску файлу управління отримують не файли, а вірус.

Файлові черв'яки

Файлові черв'яки (worms) є в деякому сенсі різновидом компаньйон-вірусів, але при цьому жодним чином не пов'язують свою присутність з яким-небудь виконуваним файлом. При розмноженні вони всього лише копіюють свій код в будь-які каталоги дисків в надії, що ці нові копії будуть коли-небудь запущені користувачем. Іноді ці віруси дають своїм копіям "спеціальні" імена, щоб підштовхнути користувача на запуск своєї копії, наприклад **INSTALL.EXE** або **WINSTART.BAT**.

Існують віруси-черв'яки, що використовують досить незвичайні прийоми, наприклад, записуючі свої копії в архіви (ARJ, ZIP та ін.). До таких вірусів відносяться "**ArjVirus**" і "**Winstart**".

Не слід плутати файлові віруси-черв'яки з мережевими хробаками. Перші використовують тільки файлові функції якої-небудь операційної системи, другі ж при своєму розмноженні користуються мережними протоколами.



Алгоритм роботи файлового вірусу

Отримавши управління, вірус робить наступні дії :
(Наводимо список найбільш загальних дій вірусу при його виконанні; для конкретного вірусу список може бути доповнений, пункти можуть помінятися місцями і значно розширитися):

- Резидентний вірус перевіряє оперативну пам'ять на наявність своєї копії і інфікує пам'ять комп'ютера, якщо копія вірусу не знайдена; резидентний вірус шукає незаражені файли в поточному і (або) кореневому каталогах, в каталогах, зазначених командою PATH, сканує дерево каталогів логічних дисків, а потім заражає виявлені файли;

Алгоритм роботи файлового вірусу

Отримавши управління, вірус робить наступні дії :

- виконує, якщо вони є, додаткові функції: деструктивні дії, графічні чи звукові ефекти і т. д. (додаткові функції резидентного вірусу можуть викликатися через деякий час після активізації залежно від поточного часу, конфігурації системи, внутрішніх лічильників вірусу або інших умов; в цьому випадку вірус при активізації обробляє стан системних годин, встановлює свої лічильники і т. д.);

Алгоритм роботи файлового вірусу

- повертає управління основній програмі (якщо вона є). Паразитичні віруси при цьому або відновлюють програму (але не файл) в початковому вигляді (наприклад, у COM-програми відновлюється кілька перших байтів, у EXE-програми обчислюється істинний стартовий адресу, драйвера відновлюються значення адрес програм стратегії і переривання), або лікують файл, виконують його, а потім знову заражають. Компаньон-віруси запускають на виконання свого "господаря", віруси-черв'яки і overwriting-віруси повертають управління DOS.

Завантажувальні віруси

Завантажувальні віруси заражають завантажувальний (boot) сектор гнучкого диска в **boot-сектор** або **Master Boot Record** (MBR) вінчестера. Принцип дії завантажувальних вірусів заснований на алгоритмах запуску ОС при включенні або перезавантаженні комп'ютера: після необхідних тестів встановленого обладнання (пам'яті, дисків і т. Д.) Програма системної завантаження зчитує перший фізичний сектор завантажувального диска і передає управління на A :, C: або CD -ROM, залежно від параметрів, встановлених BIOS Setup.

Завантажувальні віруси

При зараженні дисків завантажувальні віруси підставляють свій код замість якої-небудь програми, що одержує управління при завантаженні системи. Принцип зараження, таким чином, однаковий у всіх описаних вище способах: вірус "змушує" систему при її перезапуску вважати в пам'ять і віддати управління не оригінальному коду завантажувача, а коду вірусу.

Завантажувальні віруси

Зараження дискет здійснюється єдиним відомим способом: вірус записує свій код замість оригінального коду boot-сектора дискети. Вінчестер заражається трьома можливими способами: вірус записується або замість коду MBR, або замість коду boot-сектора завантажувального диска (зазвичай диска C :), або модифікує адресу активного boot-сектора в Disk Partition Table, розташований в MBR вінчестера.

Алгоритм роботи завантажувального вірусу

Практично всі завантажувальні віруси резидентні. Вони впроваджуються в пам'ять комп'ютера при завантаженні з інфікованого диска. При цьому системний завантажувач зчитує вміст першого сектора диска, з якого проводиться завантаження, поміщає зчитану інформацію в пам'ять і передає на неї (т. Е. На вірус) управління. Після цього починають виконуватися інструкції вірусу, який:

- як правило, зменшує обсяг вільної пам'яті (слово за адресою 0040: 0013), копіює в звільнилося місце свій код і зчитує з диска своє продовження (якщо воно є). Надалі деякі віруси чекають завантаження DOS і відновлюють це слово в його первісному значенні. В результаті вони виявляються розташованими за межами DOS, а як окремі блоки DOS-пам'яті;

Алгоритм роботи завантажувального вірусу

- перехоплює необхідні вектори переривань (зазвичай - INT 13H), зчитує в пам'ять оригінальний boot-сектор і передає на нього управління.

Надалі завантажувальний вірус поводиться так само, як резидентний файловий: перехоплює звернення ОС до дисків і інфікує їх, залежно від деяких умов здійснює деструктивні дії або викликає звукові або відеоефекти.

Макровіруси

Макровіруси (macro viruses) є програмами на мовах (макромови), вбудованих в деякі системи обробки даних (текстові редактори, електронні таблиці і т. Д.). Для свого розмноження такі віруси використовують можливості макромов і за їх допомогою переносять себе з одного зараженого файлу
(документа або таблиці) в інші.

Найбільшого поширення набули макровіруси для **Microsoft Word, Excel і Office 97**.

Макровіруси

Для існування вірусів у конкретній системі необхідна наявність вбудованого в систему макромови з можливостями:
1) прив'язки програми на макромові до конкретного файлу;
2) копіювання макропрограми з одного файлу в інший;
3) отримання управління макропрограми без втручання користувача (автоматичні або стандартні макроси).

Даним умовам задовольняють редактори **Microsoft Word, Office 97 і AmiPro**, а також електронна таблиця **Excel**. Ці системи містять собі макромови (**Word - Word Basic, Excel і Office 97 - Visual Basic**), а також:1) макропрограммы привязаны к конкретному файлу (**AmiPro**) или находятся внутри файла (**Word, Excel, Office 97**);
2) макромова дозволяє копіювати файли (AmiPro) або переміщати як підпрограми в службові файли системи і редаговані файли (Word, Excel, Office 97);
3) при роботі з файлом за певних умов (відкриття, закриття і т. д.) викликаються макропрограми (якщо такі є), які визначені спеціальним чином (AmiPro) або мають стандартні імена (Word, Excel, Office 97).

Макровіруси

Ця особливість макромов призначена для автоматичної обробки даних у великих організаціях або в глобальних мережах і дозволяє організувати так званий "автоматизований документообіг". З іншого боку, можливості макромов таких систем дозволяють вірусу переносити свій код в інші файли і заражати їх.

На сьогоднішній день відомі чотири системи, для яких існують віруси, - Microsoft Word, Excel, Office 97 і AmiPro. У цих системах вірус отримують управління при відкритті або закритті зараженого файлу, перехоплюють стандартні файлові функції і потім заражають файли, до яких яким-небудь чином йде звернення. За аналогією з MS-DOS можна сказати, що більшість макровірусів є резидентними: вони активні не тільки в момент відкриття / закриття файлу, але до тих пір, поки активний сам редактор.

Макровіруси

Макровіруси, що вражають файли Word, Excel або Office 97, як правило, користуються одним з трьох прийомів : у вірусі або є присутнім автомакрос (автофункція), або перевизначений один із стандартних системних макросів (асоційований з яким-небудь пунктом меню), або макрос вірусу викликається автоматично при натисненні на яку-небудь клавішу або комбінацію клавіш. Існують також напіввіруси, які не використовують усіх цих прийомів і розмножуються, тільки коли користувач самостійно запускає їх на виконання.

Таким чином, якщо документ заражений, при його відкритті Word викликає заражений автоматичний макрос AutoOpen (чи AutoClose при закритті документу) і запускає код вірусу, якщо це не заборонено системній змінній DisableAutoMacros. Якщо вірус містить макроси із стандартними іменами, вони отримують управління при виклику відповідного пункту меню (File/Open, File/Close, File/SaveAs). Якщо ж перевизначений який-небудь символ клавіатури, то вірус активізується тільки після натиснення на відповідну клавішу.

Мережеві віруси

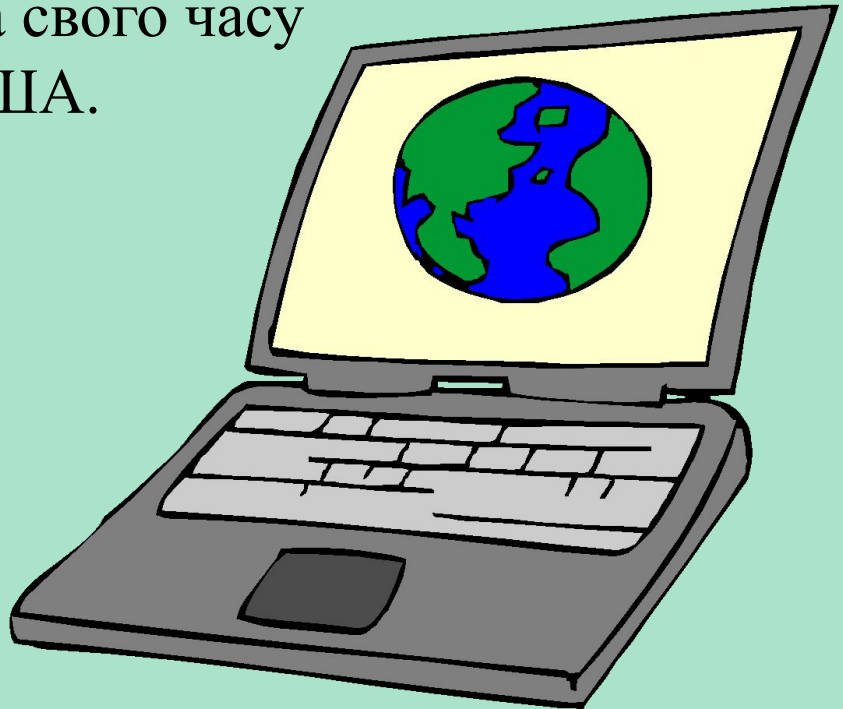
До мережевих відносяться віруси, які для свого поширення активно використовують протоколи і можливості локальних і глобальних мереж. Основним принципом роботи мережевого вірусу є можливість самостійно передати свій код на видалений сервер або робочу станцію. "Повноцінні" мережеві віруси при цьому мають ще і можливість запустити на виконання свої код на видаленому комп'ютері або, принаймні, "підштовхнути" користувача до запуску зараженого файлу.

Існує помилкова думка, що мережевим є будь-який вірус, що поширюється в комп'ютерній мережі. Але у такому разі практично усі віруси були б мережевими, навіть найбільш примітивні з них: адже звичайнісінький нерезидентний вірус при зараженні файлів не розбирається, мережевий (видалений) це диск або локальний. В результаті такий вірус здатний заражати файли в межах мережі, але віднести його до мережевих ніяк не можна.

Мережеві віруси

Найбільшої популярності набули мережеві віруси кінця 80-х, їх так само називають мережевими черв'яками (**worms**). До них відносяться вірус Моріса, віруси **Cristmas Tree і Wank Worm**. Для свого поширення вони використали помилки і недокументовані функції глобальних мереж того часу. Віруси передавали свої копії з сервера на сервер і запускали їх на виконання.

Епідемія вірусу Моріса захопила свого часу декілька глобальних мереж в США.

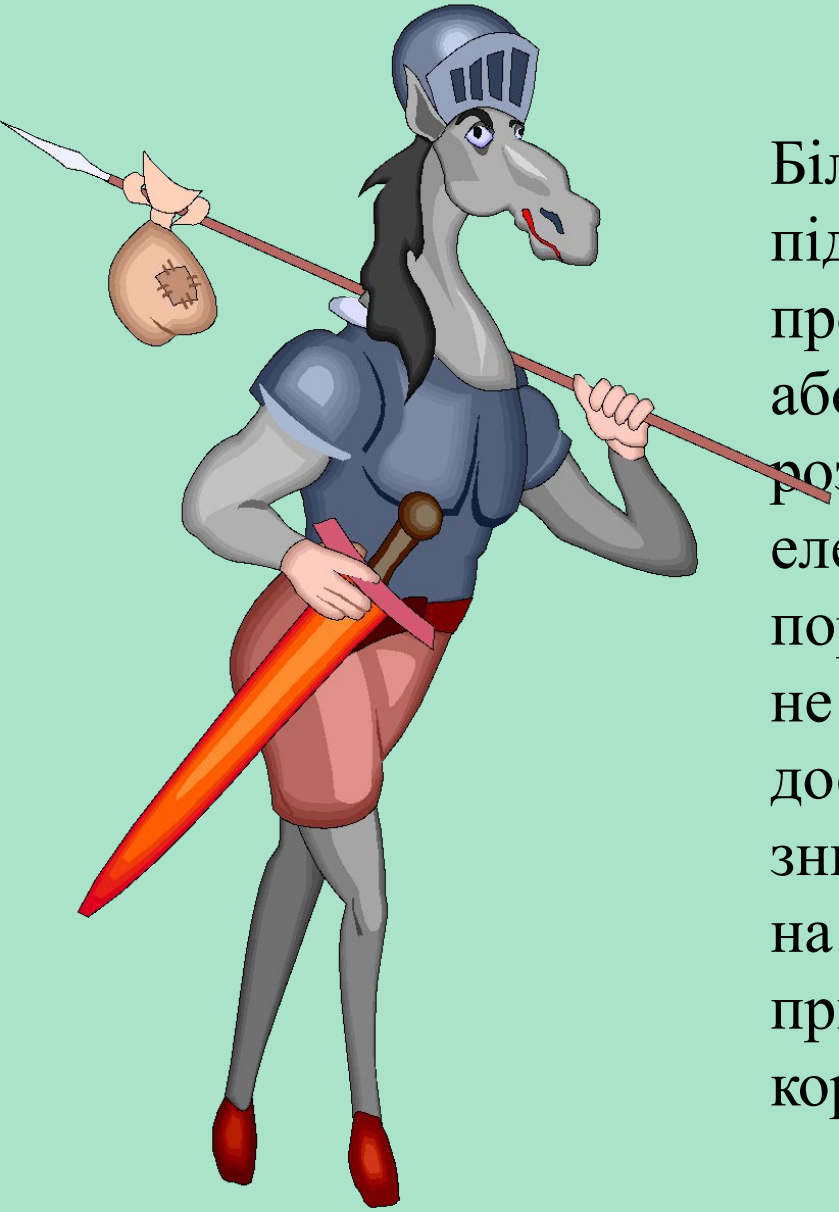


Інші несприятливі програми

До шкідливих програм окрім вірусів відносяться також "**троянські коні**" (логічні бомби), **intended**- віруси, конструктори вірусів і полиморфик-генераторы.

" **Троянський кінь** " - Це програма, завдає які-небудь руйнівні дії, т. Е. В залежності від певних умов або при кожному запуску нищівна інформацію на дисках, "що приводить" систему (до зависання) і т. П.

Інші несприятливі програми



Більшість відомих "троянських коней" підробляються під які-небудь корисні програми, нові версії популярних утиліт або доповнення до них. Дуже часто вони розсилаються по BBS- станціям або електронним конференціям. В порівнянні з вірусами "троянські коні" не набувають широкого поширення з досить простих причин: вони або знищують себе разом з іншими даними на диску, або демаскують свою присутність і знищуються постраждалим користувачем.

Інші несприятливі програми

Слід зазначити також "злі жарти" (**hoax**). До них відносяться програми, які не заподіюють комп'ютеру якої-небудь прямої шкоди, проте виводять повідомлення про те, що така шкода вже причинна, або буде причинний за яких-небудь умов, або попереджають користувача про неіснуючу небезпеку. До "злих жартів" відносяться, наприклад, програми, які "лякають" користувача повідомленнями про форматування диска (хоча ніякого форматування насправді не відбувається), визначають віруси в незаражених файлах (як це робить широко відома програма **ANTITIME**), виводять дивні вірусоподібні повідомлення (драйвер диска CMD640X від якогось комерційного пакету) і т. д. - варіанти залежать від почуття гумору автора такої програми. Мабуть, до "злих жартів" відноситься також рядок **CHOLEEPA** в другому секторі вінчестерів фірми Seagate. До цієї ж категорії жартів можна віднести свідомо неправдиві повідомлення про нові супервіруси. Такі повідомлення періодично з'являються в електронних конференціях і зазвичай вызы

"Стелс" -віруси

"Стелс" -віруси тими чи іншими способами приховують факт своєї присутності в системі. Відомі "стелс" -віруси всіх типів за винятком Windows-вірусів, файлові DOS-віруси і навіть макровіруси. Поява "стелс" -віруси, що заражають файли Windows, швидше за все справа часу.

Завантажувальні "стелс"-вирусы для приховання свого коду використовують два основні способи. Перший з них полягає в тому, що вірус перехоплює команди читання зараженого сектора (INT 13h) і підставляє замість нього незаражений оригінал. Цей спосіб робить вірус невидимим для будь-якої DOS- програми, включаючи антивіруси, нездатні "лікувати" оперативну пам'ять комп'ютера. Можливе перехоплення команд читання секторів на рівні нижчому, ніж INT 13h.

"Стелс" -віруси

Другий спосіб спрямований проти антивірусів, що підтримують команди прямого читання секторів через порти контроллера диска. Такі віруси при запуску будь-якої програми (включаючи антивірус) відновлюють заражені сектори, а після закінчення її роботи знову заражають диск. Оскільки для цього вірусу доводиться перехоплювати запуск і закінчення роботи програм, то він повинен перехоплювати також DOS- переривання INT 21h.

"Стелс" -віруси

Більшість файлових "стелс"-вирусов використовують ті ж прийоми, що приведені вище: вони або перехоплюють DOS- виклики звернення до файлів (INT21h), або тимчасово лікують файл при його відкритті і заражають при закритті. Так само як і для завантажувальних вірусів, існують файлові віруси, що використовують для своїх "стелс"-функций перехоплення переривань нижчого рівня, - виклики драйверів DOS, INT 25h і навіть INT 13h. Повноцінні файлові "стелс"-вирусы, що використовують перший спосіб приховання свого коду, у більшості своїй досить громіздкі, оскільки їм доводиться перехоплювати велику кількість DOS- функцій роботи з файлами: відкриття-закриття, читання-запис, пошук, запуск, перейменування і так далі, причому необхідно підтримувати обидва варіанти деяких викликів (FCB/ASCII), а з появою Windows 95/NT необхідно також обробляти третій варіант - функція робота з довгий ім'я файл.

Полиморфик-віруси

Полиморфик-вірусами є ті, виявлення яких неможливе, або украй скрутно здійснити за допомогою так званих вірусних масок - ділянок постійного коду, специфічних для конкретного вірусу. Досягається це двома основними способами - шифруванням основного коду вірусу з непостійним ключем і випадковим набором команд того, що розшифровує або зміною самого виконуваного коду вірусу. Існують також інші, досить екзотичні приклади поліморфізму - DOS- вірус Bomber, наприклад, не зашифрований, проте послідовність команд, яка передає управління коду вірусу, є повністю поліморфною. Поліморфізм різної міри складності зустрічається у вірусах усіх типів - від завантажувальних і файлових DOS- вірусів до Windows- вірусів і навіть макровірусів.

Методи виявлення і видалення комп'ютерних вірусів

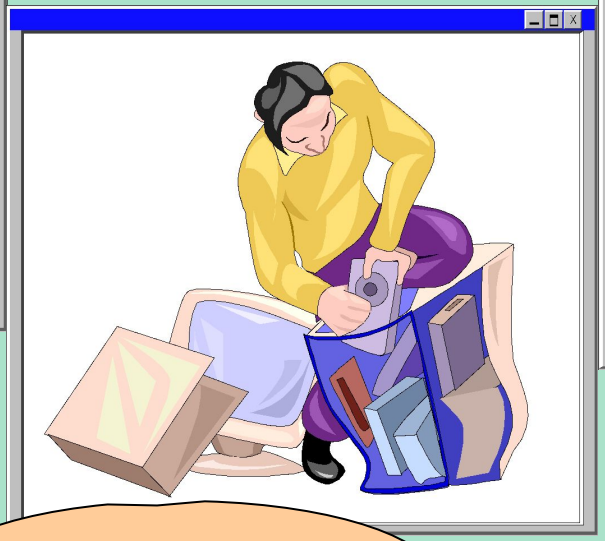
Профілактика зараження комп'ютера

Одним з основних методів боротьби з вірусами є, як і в медицині, своєчасна профілактика.

Комп'ютерна профілактика передбачає дотримання деяких правил, що дозволяють значно знизити ймовірність зараження вірусом і втрати даних. Тому, щоб визначити ці основні правила комп'ютерної гігієни, необхідно з'ясувати шляхи проникнення вірусу в комп'ютер і комп'ютерні мережі.

Звідки беруться віруси

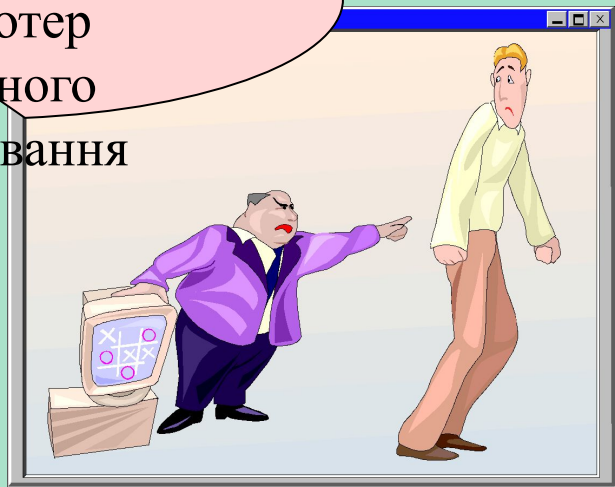
Глобальні мережі - електронна пошта



локальні мережі

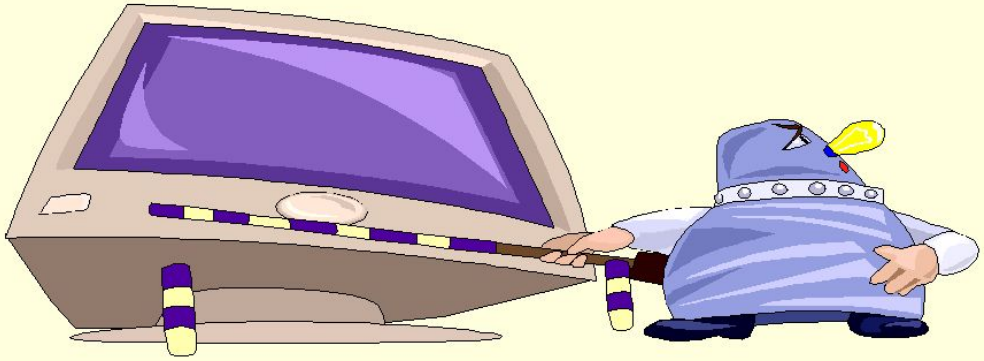
ремонтні служби

Персональний комп'ютер загального користування



Піратське програмне забезпечення

Основні правила захисту

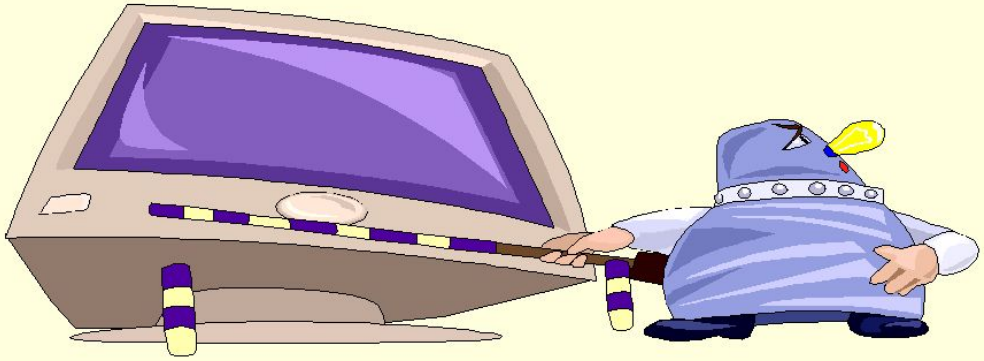


правило перше : вкрай обережно ставитеся до програм та документів Word / Excel 97, які отримуєте з глобальних мереж. Перед тим як відкрити документ обов'язково перевірте його на наявність вірусів.

правило друге : захист локальних мереж (обмеження прав користувачів, використання антивірусних програм, використання бездискових робочих станцій.

правило третє : використовуйте тільки добре зарекомендували себе джерела програм.

Основні правила захисту



правило четверте : намагайтеся не запускати неперевірені файли. Перед запуском нових програм обов'язково перевірте їх одним або декількома антивірусами.

правило п'яте : необхідно обмежувати коло осіб, допущених до роботи на конкретному комп'ютері. Як правило, найбільш часто схильні до зараження багатокористувацькі ПК.

Антивірусні програми

Найбільш ефективні в боротьбі з комп'ютерними вірусами антивірусні програми. Проте відразу хотілося б відзначити, що не існує антивірусів, що гарантують 100% захист від вірусів.

Який антивірус найкращий? Будь, якщо на вашому комп'ютері віруси не водяться і ви не користуєтеся вірусоопаснимі джерелами інформації.

Антивірусні програми

Якщо ж ви любитель іграшок, ведете активну переписку електронною поштою, то вам все-таки слід використовувати який-небудь антивірус. Який саме - вирішуйте самі, проте є декілька позицій, по яких різні антивіруси можна порівняти між собою.

Якість антивірусної програми визначається за такими позиціями, наведеними в порядку убування їх важливості:

Антивірусні програми

1. Надійність і зручність роботи

2. Якість виявлення вірусів всіх поширених типів. Відсутність «помилкових спрацьовувань». Можливість лікування заражених об'єктів.

2. Існування версій антивіруса під всі популярні платформи (операційні системи)

Антивірусні програми найбільш відомі

AIDSTEST – популярність можна пояснити лише крайнім консерватизмом вітчизняних користувачів. З необхідних антивірусним програмам якостей цій властиві лише надійність і непогана швидкість роботи. AIDSTEST абсолютно безсилий проти більшості сучасних вірусів.

AVP – один із самих надійних і потужних антивірусів в світі.

DrWeb – непогана програма, що має всі необхідні функції пошуку і лікування вірусів. До недоліків можна віднести дуже невелику базу даних (всього близько 3000 вірусів).

Удачі
в боротьбі з
комп'ютерними вірусами!