## *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. Під час досліджень, проведених, однією з американських асоціацій по боротьбі з комп'ютерними вірусами, за сім місяців 1988 р. комп'ютери, які належали фірмам-членам асоціації, піддавались дії 300 масових вірусних атак, які знищили близько 300 тис. комп'ютерних систем, на відтворення яких було затрачено багато часу і матеріальних затрат.

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. Збиток, який наноситься комп'ютерними вірусами, зростає, а їх небезпечність для таких важливих систем, як оборона, транспорт, зв'язок, поставила проблему комп'ютерних вірусів в ряд тих, котрі як правило знаходяться під пристальним наглядом органів державної безпеки.

Розроблений в Пакистані, в 1986 році, вірус отримав назву PAKISTANI BRAIN. Він повністю замінює вміст стартового сектора і використовує 6 доповнюючих секторів, які відмічені в FAT диску, як дефектні. Заражені дискети отримують нове ім'я COPYRIGHT@BRAIN. Наслідками зараження цим вірусом можуть бути: уповільнене завантвження ОС, часткова втрата даних.

Біля 5% виявлених заражень припадає на ALAMEDA VIRUS, який також відноситься до цієї групи. Цей вірус заміщує вміст завантажуючого сектора, переписуючи і зберігаючи в ньому оригінал в першому вільному секторі на диску. Механізм і наслідки зараження цим вірусом ті, що і в PAKISTANI BRAIN. ISRAELI VIRUS заражає файли типу com, exe. Втілюючись в них, вірус збільшує їх розмір на 1813 байт (інколи, посилаючись на віруси цієї групи, їм дають назви: вірус — 1813, вірус — 1704 і тощо).

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.

На сході були пошкоджені комп'ютерні центри таких великих закладів, як Масачусетський технологічний інститут. Гарвардський, Пітсбургський, Меріленський 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**.

***Комп'ютерним вірусом*** називають певну сукупність виконуваного машинного коду, яка може створювати свої копії (що не обов'язково співпадають з оригіналом) і вміщувати їх у файли, системні області комп'ютерів, комп'ютерні мережі.

**Вірус** — це своєрідна програма, яка, на відміну від звичайних програм, ніколи не зберігає себе у вигляді окремих файлів, а також може виконувати різні небажані дії на комп'ютері.

частину матеріалу взято із сайту http://virusy.org.ua

## *Суспільний аспект*

Для одних віруси є бізнесом. Причому не тільки для їх авторів, але і для тих, хто з цими вірусами бореться. Бо процвітання компаній, які випускають антивірусні програми не є несподіванкою ні для кого.

Для інших — це хоббі. Хоббі — збирання вірусних колекцій і хоббі — написання вірусів. З останнього, до речі, починав видатний Ігор Данілов.

Для третіх — створення вірусів просто спосіб показати свою зухвалість і незалежність, в деяких колах подібна діяльність просто необхідна для підняття свого престижу.

Ще для когось віруси це витвір; зустрічаються ж лікарі за призванням, це значить, може бути і комп’ютерний лікар за призванням.

Для інших віруси — це також стаття кримінального кодексу. В Росії, наприклад, тільки за написання вірусів засуджують до 5 років ув’язнення, правда, з моменту нововведення в дію ні однієї справи по даній статті заведено не було.

А для багатьох користувачів комп’ютерів віруси — це щоденний головна біль і турбота, причина збоїв в роботі комп’ютера і ***ворог номер один***.

Ситуація з вірусами корінним чином змінилась декілька років тому. Якщо до того моменту кожний був зайнятий безпекою свого комп’ютера і своїх даних, то із збільшенням кількості машин, з появою корпоративних ліній, виходом в Internet проблема постала по-новому. Раніше віруси пробирались на робочі місця з піратського диска, а точніше — дискети.

Професіоналізація піратства супроводжувалась переходом до компакт-дисків і практично усунула небезпеку зараження вірусами через піратські програми.

Зараз з ліцензійним програмним забезпеченням все налагоджується, і ігри на робочому місці частково заборонені, але поки що Word і Excel являються міжнародними стандартними документами, а макровіруси не пишуть тільки ліниві. При достатньо активному документообороті, як з західними партнерами, так і всередині держави, макровіруси можуть повністю паралізувати роботу компанії, на заході вже таке практикувалось.

Друга проблема – Internet. Нема ніякої гарантії, що на файлових серверах не знаходяться віруси. Вихід один — захист. А тут, як звичайно постає проблема вибору — який антивірус краще.

По-перше, **вірус — це програма, і, в більшості випадків, шкодити вона може лише програмно, але ніяк не апаратно**. Це змінилось після поширення Flash-пам'яті в різних пристроях комп'ютера, яку вірус може стерти. Відновлення потребуватиме спеціального обладнання, що з практичної точки зору еквівалентно псуванню обладнання з подальшим ремонтом. Раніше зустрічались віруси, які могли

вивести з ладу монітор комп'ютера, проектуючи усе зображення в одну точу. Наразі в більшості сучасних моніторів стоїть програмний захист від таких дій.

Страшні казки ходять про віруси, які вбивають і зводять з розуму користувачів за допомогою виводу на екран небезпечної для людини кольорової гами, були і будуть казками. Проте віруси, які за допомогою системного динаміка видають доволі шкідливий ультразвук, були написані ще на початку 90-х. Далі — **вірус — це програма, спроможна до розмноження**. Існують віруси, котрі не займаються нічим, крім розмноження.

## *Ознаки зараження вірусом*

1. Зменшення вільної пам’яті.
2. Уповільнення роботи комп’ютера.
3. Затримки при виконанні програм.
4. Незрозумілі зміни в файлах.
5. Зміна дати модифікації файлів без причини.
6. Незрозумілі помилки Write-protection.
7. Помилки при інсталяції і запуску Windows.
8. Відключення 32-розрядного допуску до диску.
9. Неспроможність зберігати документи Word в інші каталоги, крім Template.
10. Погана робота дисків.

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

1. Зникнення файлів.
2. Форматування HDD.
3. Неспроможність завантажити комп’ютер.
4. Неспроможність завантажити файли.
5. Незрозумілі системні повідомлення, звукові ефекти і т. д.

## *Види та типи вірусів*

| ***Ознака класифікації вірусів*** | | ***Опис*** |
|---|---|---|
| ***За об'єктами зараження*** | ***Файлові*** | заражують виконувані файли, а також допоміжні програми, що завантажуються при виконанні інших програм з розширенням exe, com. |
| | ***Завантажувальні*** | заражують завантажувальний сектор диску (boot-сектор) |
| | ***Текстові (Макровіруси)*** | заражують текстові файли Microsoft Office, інші документи та об'єкти, що містять макроси |
| | ***Мережні*** | поширюються по комп'ютерній мережі |
| ***За зовнішнім виглядом*** | ***Звичайні*** | код вірусу можна побачити на диску |
| | ***Невидимі (Стелс-віруси)*** | використовують особливі засоби маскування і при перегляді код вірусу не видно |
| | ***Поліморфні*** | код вірусу видозмінюється |
| ***За результатами діяльності*** | ***Нешкідливі*** | не впливають на роботу комп'ютера (наприклад, збільшують розмір файла) |
| | ***Безпечні*** | не виконують ніяких дій, окрім свого розповсюдження,виведення різних повідомлень або інших дій (перезавантаження комп'ютера і тощо) |
| | ***Небезпечні*** | пошкоджують інформацію файлів, зумовлюючи «зависання» комп'ютера |

| | | |
|---|---|---|
| | ***Дуже небезпечні*** | зумовлюють втрату програм, знищення інформації із системних областей, форматування жорсткого диска |

***Способи зараження комп'ютера***

***Резидентні*** – ті, що вміщуються в оперативну пам'ять і додаються до всіх об'єктів (файлів, дисків), до яких звертається ОС.

***Нерезидентні*** – ті, що додаються до оперативної пам'яті і є активними лише короткий час.

***Особливості алгоритму***

***Віруси-супутники*** – віруси, які не змінюють файли, але створюють однойменні файли з розширенням com, що завантажуються першими.

***Віруси-черв'яки*** – віруси, що поширюються автоматично в комп'ютерній мережі за знайденою адресою в адресній книзі.

***Віруси-паразити*** – віруси, які розпізнаються за зміненим змістом дискових секторів і файлів.

***Stealth-віруси*** – ті, що фальсифікують інформацію, яка читається з диска. Вірус перехоплює вектор переривання int 13h і видає активній програмі хибну інформацію, яка показує, що на диску все гаразд. Цей засіб використовується як у файлових, так і в завантажувальних вірусах.

***Віруси-мутанти*** – віруси, що мають зашифрований програмний код.

***Ретровіруси*** – звичайні файлові віруси, які намагаються заразити антивірусні програми, щоб знищити їх або зробити недієздатними.

## *Хибні думки про віруси*

***Віруси самопоширюються.*** Віруси не можуть виконувати себе. Із цього виходить, що вони не поширюються самі. Вірус не може нічого зробити, перед тим як заражені програми не завантажаться або комп’ютер не перевантажиться з зараженого диску.

***Віруси можуть поширюватися між будь-якими комп’ютерами.*** В теорії можна написати вірус, котрий може функціонувати в різних ОС, але це завдання дуже важке. На практиці можна передбачити, що DOS-віруси неспроможні заразити такі комп’ютери, як, наприклад, Macintosh, Unix, Vax.

***Віруси можуть заразити захисні від запису диски.*** Віруси не можуть заразити захищені від запису диски. Однак диски можуть бути заражені, коли захист виключений.

***Деякі віруси абсолютно не шкідливі.*** Є віруси, котрі не знищують інформацію, але вони збільшують навантаження на процесор і змінюють програмний код без відома користувача.

***Тільки в піратських дисках знаходяться віруси.*** Часто віруси знаходяться в піратських копіях, але відомі випадки, коли комерційне ПЗ мало віруси.

***Віруси можуть руйнувати комп’ютери.*** Час від часу з’являються слухи про віруси, котрі руйнують монітор, або руйнують HDD, але ні разу це не підтвердилось.

## *Антивірусні програми. Використання антивірусів.*

Попередній аналіз відомих вірусів дозволяє виділити послідовності кодів, характерних для кожного з них. Антивірусні програми використовують принцип

роботи сканерів, який полягає в пошуку цих кодових послідовностей у файлах, завантажувальних секторах і оперативній пам'яті. Якщо сканер знаходить таку послідовність, він повідомляє про зараження. Така перевірка дозволяє виявляти лише відомі віруси і не допомагає проти невідомих. Тому, якщо сканер повідомляє про відсутність вірусів, це не означає, що їх насправді немає. Це зумовлює необхідність постійного оновлення **програм-сканерів** (нові версії деяких сканерів з'являються майже щотижня).

У сканерах використовується також алгоритми "евристичного сканування", які виявляють фрагменти програм, поведінка яких може бути подібною до поведінки вірусів. Дуже часто це дозволяє дійти висновку про зараження новими вірусами. У багатьох випадках антивірусні програми здатні "ліквідувати" заражені файли, вилучаючи з них вірусний код.

Серед найбільш відомих антивірусних програм-сканерів можна назвати DrWeb, AVP, Aidstest, McAfee Virus Scan, Norton Antivirus, IBM Anti-Virus та ін.

Досить ефективними є також антивірусні **програми-ревізори**, в тому числі так звані CRC-сканери. Зараження файлу вірусом призводить до зміни цього файла. Програма-ревізор контролює будь-які зміни файлів у разі їх виявлення повідомляє про можливість вірусного зараження. Відомою програмою-ревізором є ADINF.

### *Засоби боротьби з вірусами*

Не існує універсального засобу боротьби з вірусами. Але потрібно знати і виконувати хоча б основні правила антивірусного захисту, які істотно зменшують ризик зараження, а також можливі втрати від вірусів.

Насамперед слід робити резервні копії своїх даних. Це дозволить відновити інформацію не тільки у випадку пошкодження вірусами, а й у разі механічного псування дисків і т.п.

Нові файли, які заносяться до комп'ютера, повинні перевірятися антивірусною програмою, особливо це стосується програм, які будуть запускатися на виконання файлів текстових процесорів та електронних таблиць.

Необхідно регулярно оновлювати антивірусні програми.

Якщо є підозра на зараження, слід якнайшвидше починати лікування (знищення вірусів у пам'яті, в завантажувальних секторах і у файлах). Рекомендується навіть завантажитися з системного диску (звичайно, який не повинен містити вірусів) і запустити антивірусну програму саме з цього диску.

Антивірусні програми групи **детекторів** виявляють файли, які заражені одним із відомих цим програмам вірусів.

Антивірусні програми групи **лікарів** (або фагів) «лікують» заражені програми або диски, вилучаючи з них код вірусу, тобто відновлюючи програму в тому стані, в якому вона була до зараження вірусом.

Антивірусні програми групи **ревізорів** спочатку запам'ятовують відомості про стан програм і системних областей дисків, а після роботи з цими програмами порівнюють їхній стан з початковим. При виявленні невідповідності повідомляють про неї.

Антивірусні програми групи **фільтрів** завантажуються резидентно в оперативну пам'ять, перехоплюють ті звернення до системи, які використовуються вірусами для розмноження та нанесення шкоди і повідомляють про них.

| | | |
|---|---|---|
| Антивірус avast! Free |  | Швидкий і ефективний безкоштовний антивірус Аваст: хмарні технології, захист в режимі реального часу від вірусів, програм-шпигунів і інших погроз, веб-захист WebRep для браузерів, автоматична пісочниця. |
| Kaspersky Internet Security |  | Основні компоненти : Файловий антивірус; Поштовий антивірус; Веб-Антивірус; Хмарна мережа Kaspersky Security Network; Контроль активності програм; Моніторинг активності; Мережний екран; Захист від мережевих атак; Анти-Спам; Анти-Банер; Захист введення з клавіатури; Батьківський контроль. |
| Avira Free Antivirus |  | Ефективний захист в режимі реального часу і за запитом від шкідливих програм: вірусів, троянів, інтернет-хробаків, програм-шпигунів і рекламного ПО, захищає від складних у виявленні загроз – руткітів, фільтрує дані і файли, передані через Інтернет по протоколу HTTP , захищаючи від шкідливих веб-сайтів і завантажень, запобігає онлайн-відстеження вашої діяльності в Інтернеті, оцінює безпеку всіх сайтів в результатах пошуку. |
| Dr.Web |  | Антивірус Dr.Web визначає і видаляє поштові і мережеві черв'яки, файлові віруси, троянські програми, стелс-віруси, поліморфні, безтілесні і макровіруси, віруси, що вражають документи MS Office, скрипт-віруси, шпигунське ПЗ (Spyware), програми-викрадачі паролів, програми -дозвонщики, рекламне ПО (Adware), утиліти хакерів, потенційно небезпечне ПО і будь-які інші небажані коди. |
| Антивирус ESET NOD32 6 |  | Усунення всіх типів загроз, включаючи віруси, руткіти і шпигунське ПО. Можливості "хмарного" сканування для швидкої перевірки комп'ютера, високий рівень захисту та перевірка USB-флешок, CD та DVD-дисків при підключенні. |
| Panda ActiveScan |  | Вдосконалений онлайн-сканер, оснований на принципі Колективного розуму (сканування "в хмарах") і здатний виявляти шкідливі програми.<br>Онлайн-антивірус від Panda Security сканує і визначає віруси, інтернет-черв'яки і троянські програми у всіх системних пристроях, на жорстких дисках, в стислих файлах, в електронній пошті. ActiveScan також виявляє програми-шпигуни (Spyware) і наступні типи шкідливих програм: дозвонювачі, хакерські утиліти, руткіти, жартівливе ПО. |