

ВІРУСИ ТА АНТИВІРУСИ

Зміст

Що таке вірус

Історія виникнення вірусів

Суспільний аспект

Ознаки зараження вірусом

Класифікації вірусів

Середовище перебування

Способи зараження комп'ютера

Функціональні можливості

Особливості алгоритму

Хибні думки про віруси

Що таке антивірус

Використання антивірусів

Класифікація антивірусів

Типи антивірусних програм

Що таке вірус

Вірус – це програма, яка заважає роботі комп'ютера (знищує або перетворює значення даних вінчестера, системної області, мережі).

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.

Історія виникнення вірусів

В кінці 1989 р. в пресі з'явилось 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 завантаження 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).

Суспільний аспект

Для одних віруси являються 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 других — 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 по призванню, це значить, може бути і комп'ютерний лікар по призванню. Для деяких віруси служать приводом пофілософствувати, на теми створення і розвитку комп'ютерного життя. 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 щоденна головна біль і турбота, причина збоїв в роботі комп'ютера і ворог номер один.

Суспільний аспект

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 де-факто являються міжнародними стандартними документами, а макровіруси не пишуть тільки лінії. 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.

Суспільний аспект

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 точку. 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.

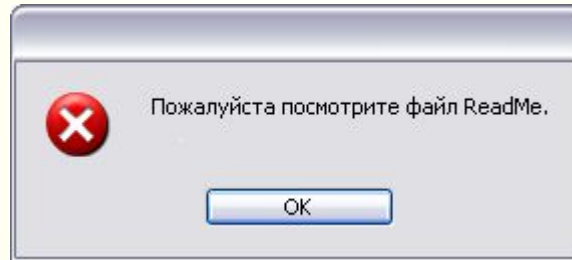
Ознаки зараження вірусом

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

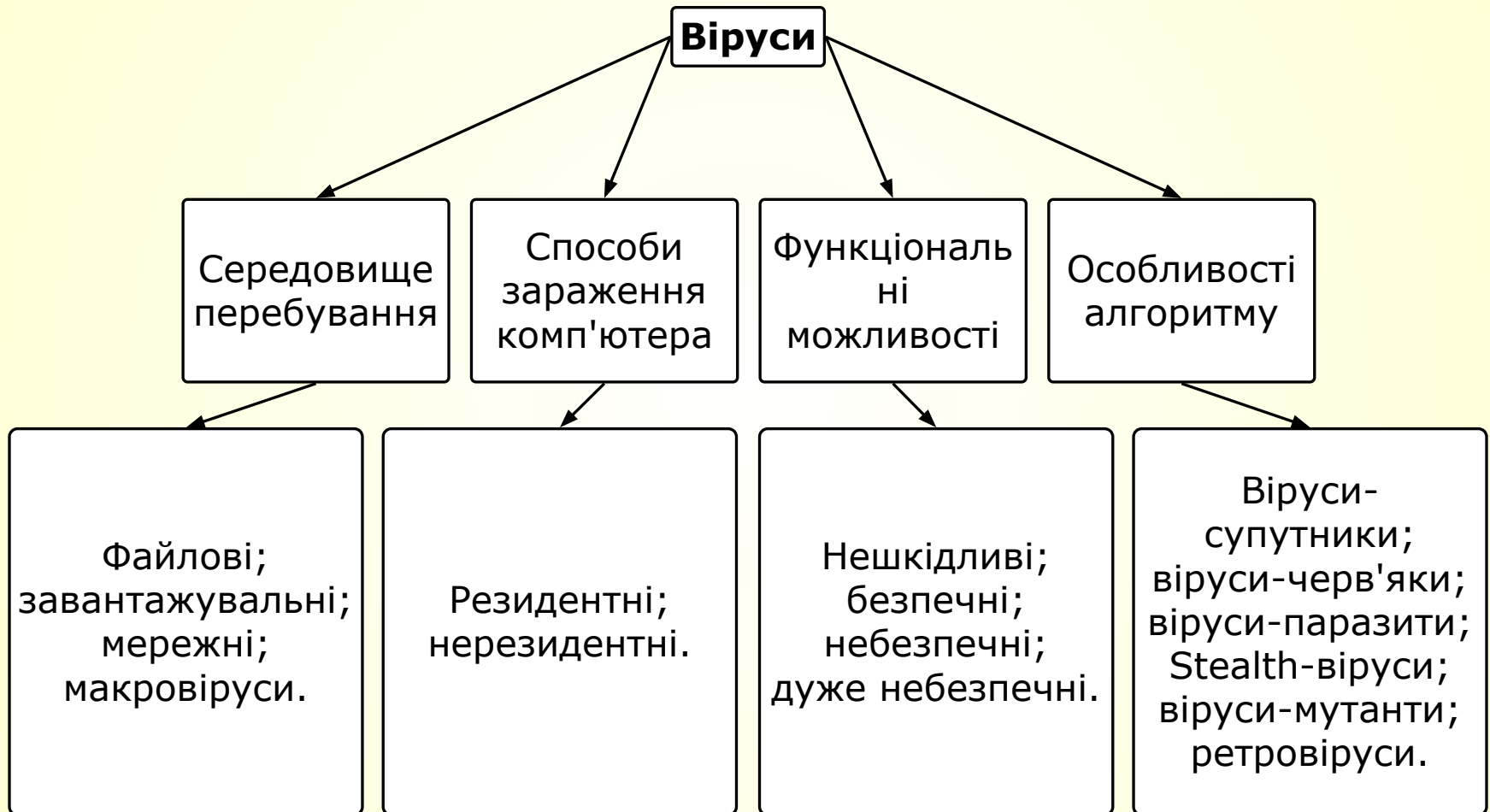
1. Зникнення файлів.
2. Форматування HDD.
3. Неспроможність завантажити комп'ютер.
4. Неспроможність завантажити файли.
5. Незрозумілі системні повідомлення, звукові ефекти і т. д.

Інсталяція вірусів

Оскільки вірус не може встановитись і почати працювати самостійно, для цього він пропонує відкрити певний файл або перезавантажити операційну систему. Це може виглядати так:



Класифікації вірусів



Середовище перебування вірусів

Файлові – ті, що додаються до файлів з розширенням exe, com.

Завантажувальні – ті, що додаються до boot-сектора.

Мережні – ті, що поширюються по комп'ютерній мережі.

Макровіруси – ті, що заражають файли Microsoft Office.

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.

Функціональні можливості вірусів

Нешкідливі – ті, що не впливають на роботу комп'ютера (наприклад, збільшують розмір файла).

Безпечні – ті, що заважають роботі, але не пошкоджують інформацію (наприклад, дають якісь повідомлення, перезавантажують комп'ютер тощо).

Небезпечні – ті, що пошкоджують інформацію файлів, зумовлюючи «зависання» комп'ютера.

Дуже небезпечні – ті, що зумовлюють втрату програм, знищення інформації із системних областей, форматування жорсткого диска.

Особливості алгоритму вірусів

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 зміненням змістом дискових секторів і файлів.

Особливості алгоритму вірусів

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.

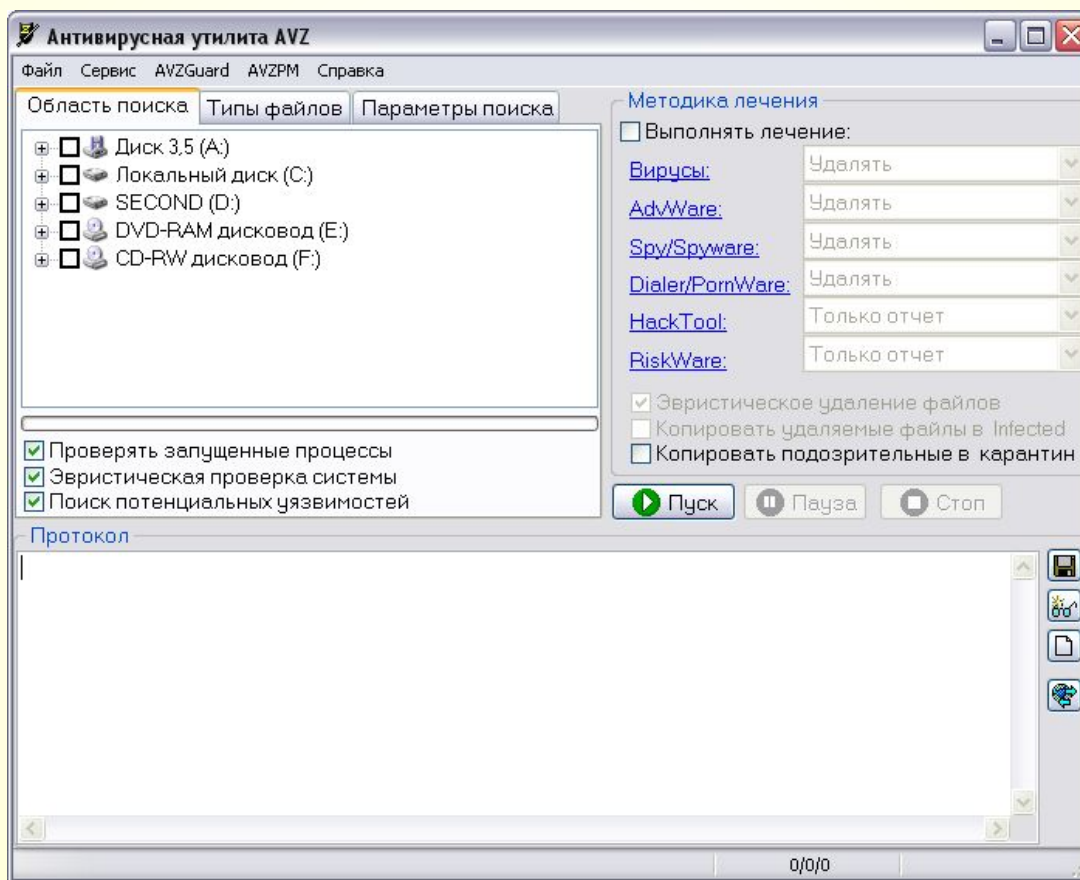
Деякі віруси абсолютно не шкідливі. Є віруси, котрі не знищують інформацію, але вони збільшують навантаження на процесор і змінюють програмний код без відома користувача.

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.

Що таке антивірус

Антивірус – це програма, призначена для захисту від спеціально створених програм пошкодження інформації – вірусів.



Використання антивірусів

Попередній аналіз відомих вірусів дозволяє виділити послідовності кодів, характерних для кожного з них. Принцип роботи антивірусних сканерів 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 сканерів можна назвати DrWeb, AVP, Aidstest, McAfee Virus Scan, Norton Antivirus, IBM Anti-Virus та інш.

Досить ефективними є також антивірусні програми-ревізори, в тому числі так звані CRC-сканери. Зараження файла 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.

Використання антивірусів

Не існує універсального засобу боротьби з вірусами. Але потрібно знати і виконувати хоча б основні правила анти вірусного захиту, 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.

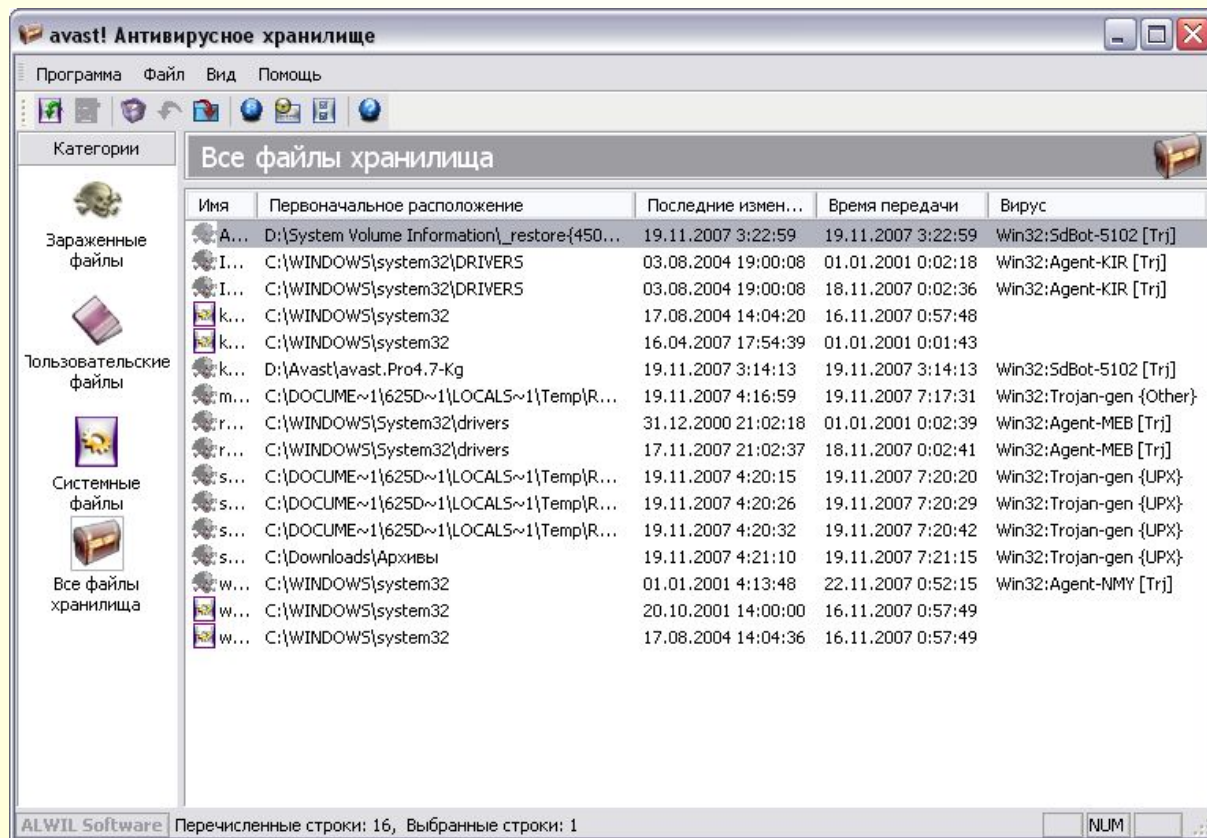
Необхідно регулярно оновлювати антивірусні програми. Якщо не планується завантаження саме з дискети, при ввімкненні або перезавантаженні комп'ютера ні в якому разі не можна залишати дискети в дисководі.

Якщо є підозра на зараження, слід якнайшвидше починати лікування (знищення вірусів у пам'яті, в завантажувальних секторах і у файлах). Рекомендується навіть завантажитися з системної дискети (звичайно, сама ця дискета гарантовано не повинна містити вірусів) і запустити антивірусну програму саме з цієї дискети.

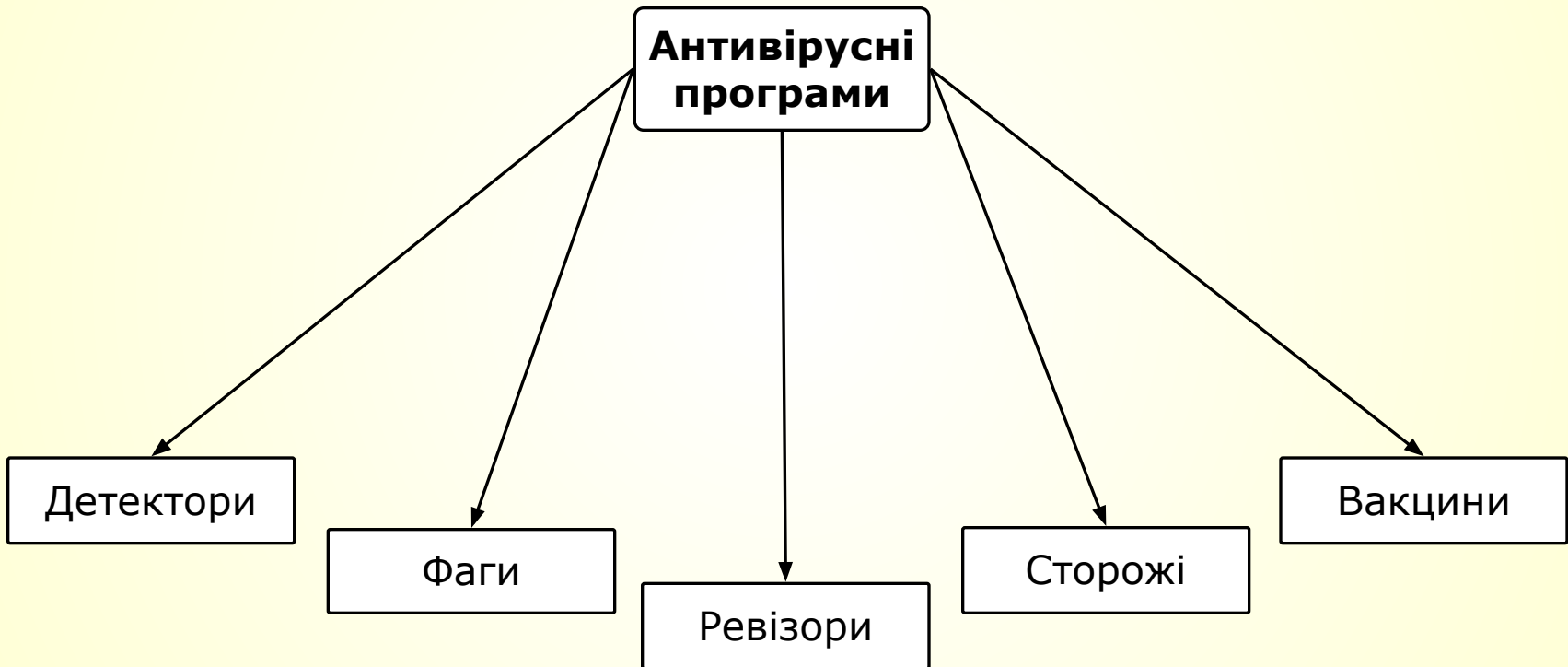
Під час роботи з файлами в текстових редакторах збереження файлів у форматі RTF дозволяє запобігати їх зараженню вірусами.

Архів вірусів

Щоб при повторному зараженні вірусом комп'ютер швидше його знаходив і впізнавав, антивірусні програми зберігають віруси в спеціальних "сховищах".



Класифікація антивірусів



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.

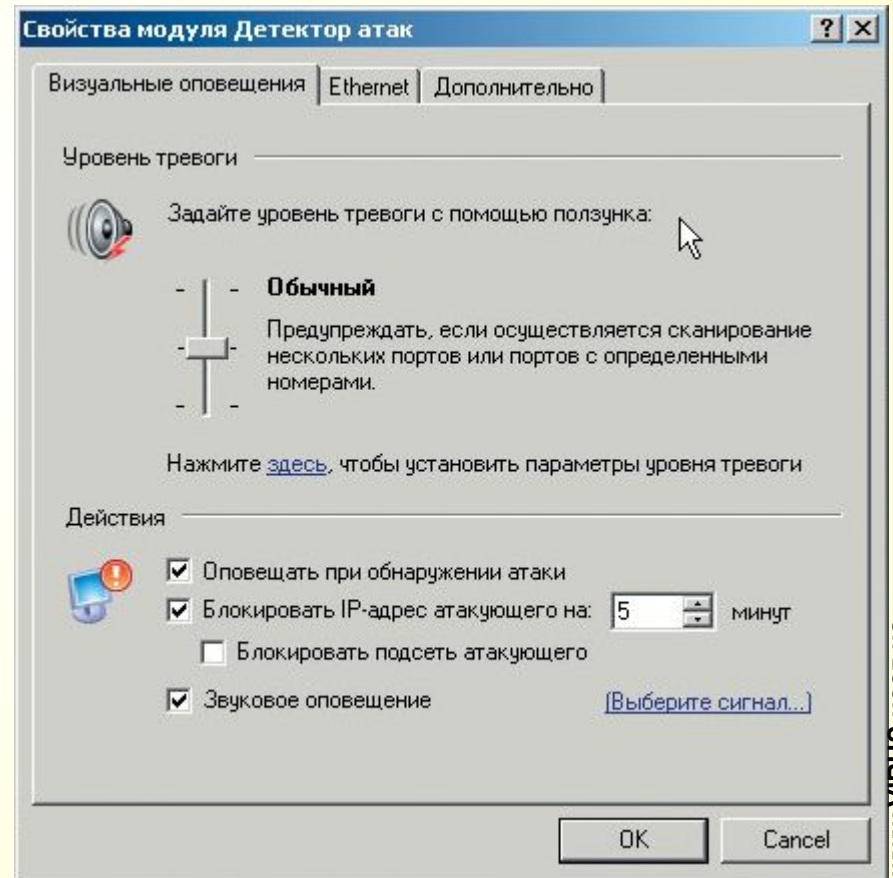
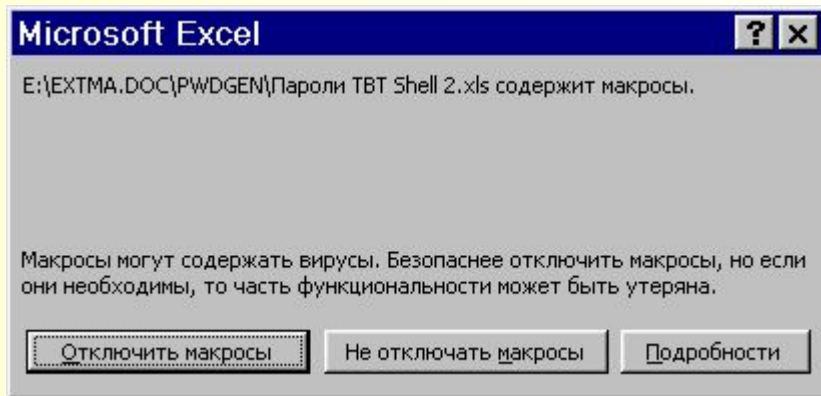
Типи антивірусних програм

Сторожі – 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.

Засоби захисту Windows

Microsoft передбачив можливість вірусних атак і створив ряд засобів, які мали б їм протидіяти. Так вони проявляються:



**Дякуємо
за увагу!**