Міністерство освіти і науки України

Тернопільський національний педагогічний університет

Імені Володимира Гнатюка

Кафедра інформатики

та методики її викладання

***“Комп’ютерні віруси і антивіруси”***

Підготував:  
студент групи Ф-11  
Гой Віталій Володимирович

Науковий керівник:

Грод Інна Миколаївна

Тернопіль-2016

# Зміст

[Вступ 3](#_Toc452025864)

[1. Прояв комп'ютерних вірусів 4](#_Toc452025865)

[2. Методи захисту від комп'ютерних вірусів 5](#_Toc452025866)

[3. Антивірусні програми 7](#_Toc452025867)

[Висновок: 17](#_Toc452025868)

[Список літератури 18](#_Toc452025869)

# Вступ

Якщо у вас дуже повільно працює комп’ютер, то викликати дану проблему можуть віруси. Віруси потрапляють в комп’ютер ззовні, тобто з флешок, дисків і, звичайно ж, з Інтернету. Як правило, віруси маскуються і тому візуально їх дуже важко виявити і, природно, знешкодити. Головна мета більшості вірусів — паралізувати роботу комп’ютера. Найчастіше віруси впроваджуються у встановлені на комп’ютері програми і звідти починають поглинати ресурси комп’ютера, через що він починає дуже повільно працювати. В даному випадку рекомендуємо провести повну перевірку комп’ютера антивірусом. Якщо антивірус не знайшов підозрілих об’єктів або їх було занадто багато, то радимо додатково скористатися однією їх безкоштовних антивірусних сканерів, які будуть відмінним доповненням до стаціонарного антивірусу.

# 1. Прояв комп'ютерних вірусів

Комп'ютерні віруси –— комп'ютерна програма, яка має здатність до прихованого самопоширення. Одночасно зі створенням власних копій віруси можуть завдавати шкоди: знищувати, пошкоджувати, викрадати дані, знижувати або й зовсім унеможливлювати подальшу працездатність операційної системи комп'ютера

При зараження комп'ютера вірусом дуже важливо своєчасно його знайти. І тому слід ознайомитися з основними ознаками появи вірусів:

· мерехтіння екрана.

· повільна робота комп'ютера.

· поява на екрані непередбачуваного повідомлення.

· блокування введення з клавіатури.

· зміна розмірів файла, дати створення програм.

· значне збільшення файлів на диску.

· часті зависання і збої у роботі комп'ютера.

· знищення файлів чи часткове руйнація.

· блокування записи на жорсткий диск.

Особливо небезпечним і для користувача є така дія вірусу, як форматування жорсткого диска, що може спричинити до швидкої втрати всієї що зберігається там інформації. Оскільки від проникнення вірусу не застрахований жоден користувач, можна скоротити можливі наслідки від присутності на комп'ютері вірусу. І тому необхідно дотримуватися деяких правил:

· Кожен свій носій, коли він «побував» іншою комп'ютери, слід перевірити будь-якою антивірусною програмою. Програми такі,що можуть не, лише знайти вірус, а й «вилікувати» носій.

· Аналогічні перевірки необхідно влаштовувати для файлів, отриманих через мережу.

· Антивірусні програми необхідно періодично оновлювати, оскільки вони швидко старіють.

· Працюючи з електронною поштою не відкривати файли якщо тема листи і саме лист порожні, видаляти все підозрілі файли.

# 2. Методи захисту від комп'ютерних вірусів

Хоч би яким не був би вірус, користувачеві треба зазначити основні засоби захисту від комп'ютерних вірусів. Для захисту від вірусів можна використовувати:

· спільні кошти захисту, які корисні, і як страховка від фізичного псування дисків, неправильно працюючих програм чи хибних дій користувача;

· профілактичних заходів, дозволяють зменшити ймовірність зараження вірусом;

· спеціалізовані програми захисту від вірусів.

Загальні засоби захисту інформації мають дві основи різновиду:

· копіювання інформації – створення копій файлів і системних областей дисків;

· розмежування доступу запобігає несанкціоноване використання інформації, захисту від змін програм, тож даних вірусами, неправильно які працюють з програмами.

Попри те що, спільні кошти захисту дуже важливі захисту від вірусів, проте їх недостатньо. Необхідно застосування спеціалізованих програм захисту від вірусів. Ці програми можна розділити сталася на кілька видів: детектори, доктора, ревізори, фільтри, вакцини чииммунизатори.

Програми – детектори дозволяють знайти файли, заражені вірусів. При виявленні, в якомусь файлі на екран виводиться відповідне повідомлення. Багато детектори мають режими лікування чи знищення заражених файлів. Недоліком таких програм і те, що можуть виявляти ті віруси, які відомі розробникам таких програм.

Програми – доктора (фаги) як знаходять заражені вірусами файли, а й «лікують» їх, тобто. видаляють з файла тіло програми вірусу, повертаючи файли у початковий стан. Середфагов виділяютьполифаги, призначені на допомогу пошуку і знищення великої кількості вірусів. Найвідоміші їхAidstest,Doctor Web, NortonAntiVirus.

Програми – ревізори – це програми, які аналізують поточний стан файлів і системних областей диска і порівнюють його з туристичною інформацією, збереженої до цього часу одному з файлів даних ревізора. Порівняння станів зазвичай виробляють відразу після завантаження ОС. У цьому перевіряється довжина файлів, їх час створення та інші параметри. Виявлені зміни виводяться на екран. Аналізуючи повідомлення програми – ревізора, користувач може вирішити, чим викликане зміни. Широко поширена програмаAdinf.

Програми – фільтри – це резидентні програми, які сповіщають користувача про спробах будь-якої програми записатися на диск чи відформатувати його, також оповіщає про інші підозрілих діях. До переваг програмних засобів можна віднести універсальність стосовно, як до відомим, і невідомим вірусам. До вад – часту видачу запитів за проведення будь-якої операції

Програми – вакцини – церезидентние програми,предотвращающие зараження файлів. Вакцини застосовують, якщо відсутні програми – доктора. Вакцинація можливе тільки відомі вірусів.

# 3. Антивірусні програми

>Антивирусна програма – частина програмного забезпечення, що встановлюється на комп'ютер, щоб шукати на дисках й у вхідних файлах комп'ютерні віруси й видаляти їх для виявлення. Програми виявляють віруси пропонуючи вилікувати файли, а при неможливості видалити. Бажано, щоб антивірусна програма виявляла будь-який вірус, причому з максимально високою ймовірністю.

Антивірусні програми залежно від розробника застосовують різні способи виявлення вірусів. Та більшість переглядає файли чи пам'ять комп'ютера, аби виявити присутність відомого вірусу, дізнаючись його за характерною частини коду.

Можливість отримати старий вірус порівняно невелика, але щодня з'являються нові віруси. Задля підтримки ефективності антивірусної програми рекомендується оновлювати антивірусні програми чи його бази даних про віруси. При виборі антивірусної програми необхідно враховувати як відсоток виявлення вірусів, а й виявляти нові віруси, кількість вірусів у антивірусної базі, частоту її відновлення, наявність додаткових функцій.

Нині серйозний антивірус мусить уміти розпізнавати щонайменше 25000 вірусів. Чимало їх ми вже припинила своє існування. Існує безліч антивірусних програм. Розглянемо найвідоміші їх.

>AIDSTEST

У нашій країні, як було зазначено вище, особливої популярності придбали антивірусні програми, поєднують у собі функції детекторів та докторів конкретних. Найвідомішою є програмаAIDSTESTД.Н. Лозинського. Україна має на кожномуIBM-совместимом персональному комп'ютері є одне з версій програмних засобів. Один із останніх версія виявляє більш 8000 вірусів.

>Aidstest для свого нормально функціонувати вимагає, щоб у пам'яті буврезидентних антивірусів, блокуючих запис в програмні файли, тому вони мають вивантажити, або, вказавши опцію вивантаження самоїрезидентной програмі, або скористатися відповідної утилітою.

Після запускуAidstest перевіряє себе оперативну пам'ять на наявність відомих йому вірусів і знешкоджує їх. У цьомупарализуются лише функції вірусу, пов'язані з розмноженням, інші побічні ефекти можуть залишатися. Програма по закінченні знешкодження вірусу у пам'яті видає запит про перезавантаженні. Слід обов'язково наслідувати цієї поради, якщо оператор ПЕОМ перестав бути системним програмістом, які займаються вивченням властивостей вірусів. До чого слід перезавантажитися кнопкоюRESET, бо за «теплою перезавантаженні» деякі віруси можуть зберігатися. До того ж, краще запустити автомобіль іAidstest ззащищенной від записи дискети, бо за запуску з зараженого диска вірус може записатись у пам'ять резидентом і перешкоджати лікуванню.

>Aidstest тестує своє тіло на наявність відомих вірусів, і навіть по спотворень у своїй коді судить про своє зараження невідомим вірусом. У цьому можливі випадки удаваної тривоги, наприклад при стискуванні антивірусуупаковщиком. Програма немає графічного інтерфейсу, і режими її задаються з допомогою ключів. Вказавши шлях, можна перевірити не весь диск, а окремий підкаталог.

Як показало практика, найоптимальніший режим для щоденної роботи задається ключами /g (перевірка всіх файлів, Не тільки з розширеннямEXE,COM,SYS) і />s (повільна перевірка). Збільшення часу при таких опціях мало відчутно, зате можливість виявлення значно вище.

При звичайному тестуванні годі було ставити ключ />f (виправлення заражених програм, тож стирання що підлягали відновленню), і з ключем />q (видавати запит про видалення файла), оскільки будь-яка програма, зокрема і антивірусна, не застрахована від власних помилок. Ключ />f варто використовувати тоді, колиAidstest, і навіть інші антивіруси свідчить про наявність в якомусь файлі. У цьому слідперезапустить комп'ютер ззащищенной від записи дискети, оскільки система то, можливо зараженерезидентним вірусом, і тоді лікування буде неефективним, або навіть просто небезпечним. При виявленні вірусу вценном файлі слід переписати його за дискету, а ще краще – електронну, диск де він спробувати вилікувати з допомогою вказівкиAidstest-у опції />f. Якщо спроба не увінчається успіхом, треба видалити все заражені копії файла і перевірити диск знову. Якщо файлі міститься важливу інформацію, яку прати шкода, можна заархівувати файл і почекати виходу нової версіїAidstest чи іншого антивірусу, здатної лікувати цей тип вірусу. Для прискорення процесу можна направити заражений файл за зразок Лозинському.

До сформування в файлі протоколу роботи програмиAidstest служить ключ />p. Протокол виявляється за потрібне, коли користувач не встигає переглянути імена заражених файлів. Для підтримки антивірусного програмно – апаратного комплексуSheriff (далі розглянутий докладніше), служить ключ />z.

>DOCTOR WEB

Останнім часом різко зростає популярність інший антивірусної програми –Doctor Web.Dr. Web як і, як іAidstest належить до класу детекторів – докторів, та на відміну від нього, має так званий «евристичний аналізатор» – алгоритм, дозволяє виявляти невідомі віруси. «Лікувальна павутиння», як перекладається з англійської назва програми, стала відповіддю вітчизняних програмістів на наваласамомодифицирующихсявирусов-мутантов. Останні при розмноженні модифікують своє тіло отже іншого жодної характерною ланцюжка байт, котра була присутня в вихідної версії вірусу.Dr. Web може бути антивірусом нової генерації протиAidstest та її аналогами.

Управління режимами як і вAidstest здійснюється з допомогою ключів. Користувач може вказати програмі, тестувати як усе диск, і окремі підкаталоги чи групи файлів, або ж відмовитися від перевірки дисків і тестувати лише оперативну пам'ять. Натомість можна тестувати або тільки базову пам'ять, або, ще й, ще й розширену (вказується з допомогою ключа /H). Як можна іAidstestDoctor Web може створювати звіт на роботу (ключ />P), завантажуватизнакогенераторКириллици (ключ /R), підтримує роботи зпрограммно-аппаратним комплексомSheriff (ключ /Z).

Але, звісно, головною особливістю «>Лечебной павутиння» служить наявність евристичного аналізатора, який підключається ключем /P.S.Баланса між швидкістю і якістю можна домогтися, вказавши ключу рівень евристичного аналізу: 0 – мінімальний, 1 – оптимальний, 2 – максимальний; у своїй, природно, швидкість зменшується паралельно зі збільшенням якості. До того жDr. Web дозволяє тестувати файли, вакцинованіCPAV, і навіть упакованіLZEXE,PKLITE,DIET. І тому слід зазначити ключ /U (у своїй розпакування файлів проведуть на поточному устрої) чи /U диск: (де диск: – пристрій, де буде здійснюватися розпакування), якщо дискета, з якою запущеноDoctor Web захищена від записи. Багато програм упаковані у такий спосіб, хоча користувач може і підозрювати звідси. Якщо ключ /U не встановлено, тоDoctor Web може пропустити вірус, заліз в запаковану програму.

Важливою функцією є контроль зараженнятестируемих файліврезидентним вірусом (ключ /V). При скануванні пам'яті немає стовідсоткової гарантії, що «Лікувальна павутиння» знайде все віруси, які перебувають там. Отож, при завданні функції /VDr. Web намагається перешкодити які залишилисярезидентним вірусам, заразититестируемие файли.

Тестування вінчестераDr.Web-ом займає набагато більше часу, ніжAidstest-ом, тому кожен користувач може ми собі дозволити витрачати стільки часу на щоденну перевірку всього жорсткого диска. Таким користувачам можна порадити ретельніше (з опцією />S2) перевіряти принесені ззовні дискети. Якщо інформація на дискеті перебуває у архіві (а останнім часом програми розвитку й дані переносяться з машини на машину лише у такому вигляді; навіть фірми-виробники програмного забезпечення, наприкладBorland, пакують своєї продукції), слід розпакувати їх у окремий каталог на жорсткому диску відразу ж, одразу ж, запуститиDr. Web, поставивши йому як параметра замість імені диска повний шлях до цьогоподкаталогу. І все-таки потрібно б разів у два тижні виробляти повну перевірку «вінчестера» на віруси із завданням за максимальний рівень евристичного аналізу.

Як у разі зAidstest при початковому тестуванні годі вирішувати програмі лікувати файли, у яких вона знайде вірус, оскільки не можна виключити, що послідовність байт, затвердженаантивирусе за шаблон може зіткнутися здорової програмі. Якщо з завершенні тестуванняDr. Web видасть повідомлення у тому, що знайшов віруси, потрібно запустити його з опцією />P (Якщо цяопція була зазначена) у тому, щоб подивитися, який файл заражений. Після цього необхідно скопіювати файл на дискету чи електронний диск і спробувати видалити, вказавши «>Лечебной павутинні» ключ /F. При невдалому лікуванні слід вступити як і, як і аналогічній ситуації, описаної вище для програмиAidstest.

MICROSOFTANTIVIRUS

До складу сучасних версій MS-DOS (наприклад, 7.10) входить антивірусна програма MicrosoftAntivirus (>MSAV). Цей антивірус може працювати у режимахдетектора-доктора і ревізора.

>MSAV має дружній інтерфейс у стиліMS-Windows, природно, підтримується миша. Добре реалізована контекстна допомогу: підказка є до будь-якого пункту меню, до будь-якої ситуації.Универсально реалізований доступом до пунктах меню: при цьому можна використовувати клавіші управління курсором, ключові клавіші (>F1-F9), клавіші, відповідні одній з літер назви пункту, і навіть миша. Прапорці установок у пункті менюOptions можна встановлювати як клавішПРОБЕЛ, і клавіш ENTER.Серьезним незручністю під час використання програми і те, що вона таблиці з цими про файлах над одному файлі, а розкидає за всіма директоріям.

Після запуску програма завантажує власнийзнакогенератор й читає дерево каталогів поточного диска, після чого відбуває о головне меню. Незрозуміло, навіщо читати дерево каталогів відразу під час запуску: адже користувач може і захотіти перевіряти поточний диск. У головному меню можна змінити диск (>Select newdrive), вибрати між перевіркою без видалення вірусів (>Detect) і зі своїми видаленням (>Detect&Clean). Після запуску перевірки диска (як і режимі видалення, і ж без нього) програма спочатку сканує пам'ять на наявність відомих їй вірусів. У цьому виводиться індикація зробленого як кольорової смужки і відсотка виконаної роботи. Після сканування пам'ятіMSAV приймається за перевірку безпосередньо диска. За першої перевірціMSAV створює у кожному директорії, що міститьисполнимие файли, файлиCHKLIST.MS, у яких записує інформацію розмір, дати, часу,атрибутах, і навіть контрольну суму контрольованих файлів. При наступних перевірках програма порівнюватиме файли з туристичною інформацією вCHKLIST.MS-файлах. Якщо змінилися величину і дата, то програма повідомить звідси користувачеві й запросить про подальші дії: оновити інформацію (Update), встановити дату та палестинці час у відповідність із даними вCHKLIST.MS (>Repair), продовжити, не звертаючи увагу зміни у даному файлі (>Continue), перервати перевірку (>Stop). Якщо змінилася контрольна сума, тоMSAV виведе таку ж вікно, лише замість пунктуRepair буде пунктDelete (видалити), оскільки програма неспроможна відновити вміст файла. При виявленні вірусу якDetect&Clean програма віддалить цей вірус. Перевірку диска в обох режимах можна призупинити, або повністю перервати, натиснувшиESC (чи F3) і відповівши на запитання програми. Під час сканування диска виводиться інформацію про виконану роботу: відсоток опрацьованих каталогів і відсоток опрацьованих файлів нинішнього року каталозі. Цю інформацію видається також наочно, як кольорової смужки, як і за перевірці пам'яті. Наприкінці перевіркиMSAV видає звіт як таблиці, у якій повідомляється про кількість перевірених жорстких дисків і гнучких дисків, про кількість перевірених, інфікованих і вилікуваних файлів. З іншого боку, виводиться час сканування.

У менюOptions можнасконфигурировать програму з власним бажанням. Тут можна встановити режим пошукувирусов-невидимок (>Anti-Stealth), перевірки всіх, і навіть дозволити чи заборонити створювати таблиціCHKLIST.MS. До того ж можна поставити режим збереження звіту про виконану роботу в файлі. Якщо встановити опціюCreateBackup, та над видаленням вірусу з зараженого файла його копія буде збережено з розширенням \*.>VIR

Знаходячись у основному меню, можна переглянути список вірусів, відомих програміMSAV, натиснувши клавішу F9. У цьому виведеться вікно із назвами вірусів. Щоб подивитися докладнішу інформацію про вірус, потрібно підвести курсор для її імені Ілліча та натиснути ENTER. Можна швидко можливість перейти до цікавого для вірусу, набравши перші літери його від імені. Щодо вірус можна вивести на принтер, обравши відповідного пункту меню.

>ADINF (AdvancedDiskinfoscope)

>ADinf належить до класупрограмм-ревизоров. Антивірус має високий швидкість роботи, здатний успішно протистояти вірусам, які у пам'яті. Він дає змогу контролювати диск, читаючи його за секторам черезBIOS і використовуючи системні переривання DOS, що може перехопити вірус.

ПрограмаADinf отримала перший приз на Другому Всесоюзному конкурсі антивірусних програм, у 1990 року, і навіть другий приз на конкурсіBorlandContest'93.ADinf був єдинимантивирусом, який улітку 1991 року відшукав вірусDIR, побудований на принципово новий спосіб зараження і маскування.

Для лікуваннязараженних файлів застосовується модульADinfCureModule, не входить у пакетADinf іпоставляющийся окремо. Принцип роботи модуля – збереження невеличкий бази даних, яка описує контрольовані файли. Працюючи спільно, ці програми дозволяють знайти й видалити близько 97% файлових вірусів і 100% вірусів у завантажувальному секторі. Приміром, гучний вірусSatanBug був легко виявлено, ізараженние їм файли автоматично відновлено. Причому, навіть ті користувачі, які отрималиADinf іADinfCureModule кілька місяців до появи цього, змогли легко його позбутися.

На відміну з інших антивірусівAdvansedDiskinfoscope не вимагає завантаження з еталонною,защищенной від записи дискети. При завантаженні з вінчестера надійність захисту не зменшується.

>ADinf має добре виконаний дружній інтерфейс, який реалізований у графічному режимі. Програма працює безпосередньо звидеопамятью, минаючиBIOS, у своїй підтримуються все графічні адаптери. Наявність великої кількості ключів дозволяє користувачеві створити максимально зручну йому конфігурацію системи. Можна встановити, що саме треба контролювати: файли із наперед заданими розширеннями, завантажувальні сектора, наявність збійних кластерів, нові файли на наявністьStealth-вирусов, файли зі списку незмінних тощо. З власного бажанню користувач може заборонити перевіряти деякі каталоги (це потрібно, якщо каталоги є робітниками і над ними постійно відбуваються зміни). Є можливість змінювати спосіб доступу до диска (>BIOS,Int13h чиInt25h/26h), редагувати список розширень перевірених файлів, і навіть призначити кожному розширенню власнийвьюер, з допомогою якого буде проглядатися файли з цим розширенням. У традиціях сучасного програмного забезпечення реалізована роботу з мишею. Хоча це й вся продукція фірми «>ДиалогНаука»,ADinf підтримує програмно-апаратний комплексSheriff.

При інсталяціїADinf до системи є можливість змінити ім'я основного файлаADINF.EXE й ім'я таблиць, у своїй користувач може поставити будь-яке ім'я. Це дуже корисна функція, позаяк у останнім часом з'явилося багато вірусів, «>охотящихся» заантивирусами (наприклад, є вірус, який змінює програмуAidstest що вона замість заставки фірми «>ДиалогНаука» пише: «Лозинський – пень»), зокрема і позаADinf.

>Полезной функцією є можливість роботи з DOS, виходячи з програми. Це корисно, коли не треба запустити зовнішній антивірус на лікування файла, якщо в користувача немає лікуючого блокуADinfCureModule.

Ще один цікавий функція – заборона роботи і системи для виявлення змін диску. Ця функція корисна, коли, використовуючи терміналами працюють користувачі, які мають ще великого досвіду спілкування з комп'ютером. Такі користувачі, це через незнання чи з халатності, можуть проігнорувати повідомленняADinf та продовжити роботу, як у що ж не бувало, що може спричинити до важким наслідків.

Якщо ж встановлено ключ –Stop в рядку викликуAdinfAUTOEXEC.BAT, то, при виявленні змін диску програма зажадає покликати системного програміста, обслуговуючого даний термінал, і якщо користувач натиснеESC чи ENTER, то системаперезагрузится і всі повториться знову.

Принцип роботиADinf грунтується зберігається в таблиці копіїMASTER-BOOT іBOOT секторів, список номерів збійних кластерів, схему дерева каталогів і інформацію про контрольованих файлах. З іншого боку, програма запам'ятовує і кожному запуску перевіряє, посутньо не змінився чи доступний DOS обсяг оперативної пам'яті (що трапляється при зараження більшістю завантажувальних вірусів), кількість встановлених вінчестерів, таблиці параметрів вінчестера у сфері зміннихBIOS.

За першого запуску програма запам'ятовує обсяг оперативної пам'яті, знаходить і запам'ятовує адресу оброблювача перериванняInt13h вBIOS, який використовуватися попри всі наступних перевірках, і будує таблиці для перевірених дисків. У цьому перевіряється, показував чи вектор переривання13h вBIOS перед завантаженням DOS.

При наступних запускахADinf перевіряє обсяг оперативної пам'яті, доступною DOS, перемінніBIOS, завантажувальні сектора, список номерів збійних кластерів (бо окремі віруси, записавшись в кластер, позначають його, яксбойний, щоб їхзатерли інші дані, і навіть не виявили примітивні антивіруси). До того ж антивірус шукає новостворені і знищені підкаталоги, нові, віддалені, перейменовані,перемещенние і змінилися файли (перевіряється зміна довжини і контрольної суми). ЯкщоADinf знайде, що, змінився файл зі списку незмінних, або у файлі відбулися зміни без зміни дати й часу, і навіть наявність в файла дивній дати (число більше 31, місяць більше 12 чи рік довший поточного) або часі (хвилин більше 59, годин більше 23 чи секунд більше 59), він видасть попередження у тому, що можна зараження вірусом.

Якщо виявлено зміниBOOT-секторов, можна як діалогу порівняти системні таблиці, хто був доі після зміни, і з бажанню відновити колишній сектор. Після поновлення змінений сектор зберігається у файлі на диску на подальше аналізу. Нові збійні кластери (вірніше інформації про неї вFAT) можуть з'явитися після запуску будь-якої утиліти,лечащей диск (наприклад,NDD) чи завдяки діям вірусу. ЯкщоAdinf видав повідомлення, а користувач не запускала ніяких подібних утиліт, то, швидше за все в комп'ютер видерся вірус. З отриманням такого повідомлення слід продовжити перевірку, уважно стежачи над усіма повідомленнями про зміни файлів і завантажувальних секторів. Якщо системі справді вірус, то такі повідомлення не змусять на себе довго чекати (бо коли її вірусу перебуватиме у «>сбойном» кластері, йому будь-коли передасться управління).

Після перевіркиADinf видає зведену таблицю,сообщающую про зміни на диску. По таблиці можна переміщатися стрілками і переглядати докладну інформацію, натиснувши ENTER на сюжеті, який пункті. Існує можливість початку кожному пункту з допомогою «швидких» клавіш.Изменившиеся файли можна переглянути у "класичному режимі (>шестнадцатеричний розвантажити /ASCII-коди) з допомогою вбудованоговьюера, котрий читає диск черезBIOS. Можна ще скористатися зовнішнімвьюером, попередньо вказавши щодо нього шлях. Залучивши зовнішній редактор, можна відредагувати змінився файл.

Але не зовсім звично виглядає форма, у якійADinf повідомляє про виявлених підозрілих змінах: замість видачі повідомлення про конкретних змінах виводить червоне вікно з переліком всіх можливих і позначає галочкою пункти, відповідні змін, що стався зараз. Якщо після отримання такого повідомлення натиснутиESC, то програма запросить про подальші дії: оновити інформацію про диску, не оновлювати її, лікувати (за наявності лікуючого модуляADinfCureModule) чи записати протокол. Для лікування можна скористатися зовнішнімантивирусом, завантаживши його з вікна на роботи з DOS, яке викликається комбінацією клавішALT+V.

Якщо не ставляться до розряду підозрілих, то після видачі таблиці змін можна натиснутиESC. У цьому програма запитає, чи потрібно оновлювати даних про диску в таблицях або потрібно, і навіть чи потрібно створювати файл в звіті про виконану роботу. Після вибору однієї з пунктів програма виконуєзатребованное дію і завершує своєї роботи.

Антивірус Касперського

Створено для перевірки електронної пошти, захисту поштових систем.Виполняет перевірку всіх повідомлень, що пропливали поштовий сервер, видаляє віруси з електронної пошти доти, як вони досягнуть адресата. При виявленні вірусів у файлах вкладень програма видаляє їх і пересилає саме повідомлення, і навіть попередження виявлення вірусу на заздалегідь поставлене адресу. Це дозволяє адміністратору визначати джерело вірусів та інших шкідливих програм. Антивірус Касперського може перевіряти як вкладені файли, а й вбудовані до них об'єкти, упаковані архіви файлів і вміст вкладених поштових повідомлень рівня вкладеності.

Переваги програми:

· можливість перевірки особистих і публічних папок;

· автоматичне відновлення антивірусних баз даних через Інтернет;

· зміна списку захищуваних ящиків без перезавантаження серверу;

· вбудована система розсилки попереджень випадки вірусних атак;

· зручна систему управління, відновлення іконфигурирования програми.

# Висновок:

Отже, віруси – це ж серйозна проблема, до якої треба підходити обережно та розважливо.

Відомі ситуації, коли віруси блокували роботу організацій та підприємств.

Для запобігання появи вірусів вашому ПК використовуйте засоби захисту.

У цьому слід пам'ятати, що антивірусні програми розвитку й «залізо» не дають повної гарантії захисту від вірусів. Приблизно так само кепські справи з другого боку тандема «людина-комп'ютер». Як користувачі, іпрофессіонали-программісти часто вже не мають навіть навичок «самооборони», як і ставлення до віруса часом є настільки поверхневими, що краще їх (уявлень) і не.

Попри величезних зусиль які конкурують між собою антивірусних фірм, збитки, принесені комп'ютерними вірусами, не падають і досягають астрономічних величин на сотні мільйонів років щорічно. Ці оцінки явно занижені, оскільки відомо стає лише частину подібних інцидентів.

# Список літератури

1. Алексєєв, О.П. Інформатика / О.П. Алексєєв. – вид. «Солон» 2002. – 280 з.

2. Безруков, М.М. Комп'ютерні віруси / М.М. Безруков. – М.: Наука, 1991. – 312 з.

3.Острейковский, В.А. Інформатика / В.А.Острейковский. – вид. «Вищу школу», 2001. – 245 з.

4. Інформатика. Базовий курс: навчальних посібників для вузів / під ред. С.В.Симоновича – СПб.: Пітер, 2001. – 640 з.

5.Горнец, М.М. Організація ЕОМ і систем: навчальних посібників / М.М.Горнец, О.Г. Рощин, В.В.Соломенцев. – М.: Академія, 2006. – 320 з.ГрифУМО.