Міністерство освіти і науки України
Національний університет водного господарства
та природокористування

Кафедра обчислювальної техніки

04-04-204

МЕТОДИЧНІ ВКАЗІВКИ

для практино-семінарських занять та самостійної роботи
з дисципліни
"Захист інформації"
студентами спеціальності
029 "Інформаційна, бібліотечна та архівна справа
(Документознавство та інформаційна діяльність) "
Частина І. Боротьба з комп'ютерними вірусами

Рекомендовано
науково-методичною комісією
спеціальності 029
"Інформаційна, бібліотечна та архівна справа
(Документознавство та
інформаційна діяльність) "
Протокол № 5
від 15 березня 2017 р.

Рівне 2017

Методичні вказівки для практино-семінарських занять та самостійної роботи з дисципліни "Захист інформації" студентами спеціальності 029 "Інформаційна, бібліотечна та архівна справа (Документознавство та інформаційна діяльність)". Частина І. Боротьба з комп'ютерними вірусами. / П. В. Ольшанський, – Рівне: НУВГП, 2017, – 36 с.

Упорядник П. В. Ольшанський, старший викладач кафедри обчислювальної техніки.

Відповідальний за випуск
Б.Б. Круліковський, кандидат технічних наук, доцент, завідувач кафедри обчислювальної техніки.

ЗМІСТ

1. Класифікація комп'ютерних вірусів

Комп'ютерним вірусом називається програма, яка здатна несанкціоновано і малопомітно «розмножуватись», тобто дописувати свої копії до інших програм або пристроїв (дискет, жорстких дисків, мережевих дисків, оперативної пам'яті).

Перший вірус з'явився в 1981 році на комп'ютерах Apple. Зараз (березень 2017 р.) налічується 30 881 129 видів вірусів. Постійно йде гостра боротьба між невгамовними авторами нових вірусів, діяльність яких в багатьох країнах кваліфікується як злочин, і розробниками систем пошуку, захисту і попередження можливої появи нових типів вірусів. Все різноманіття старих і нових типів вірусів можна розділити на великі групи за різними ознаками :

1) за руйнівним ефектом,
2) за місцем проникнення (механізмом поширення),
3) за способом використання оперативної пам'яті,
4) за особливостями алгоритмів.

1.1. За руйнівним ефектом

Крім здатності розмножуватись, більшість вірусів після замаскованого проникнення в комп'ютер через деякий час викликають ще певні дії, які прямо не пов'язані з механізмом їх розмноження, а залежать від доброї чи злої волі їх автора. За цим вторинним ефектом (за шкідливістю) віруси можна розділити на три групи:

— нешкідливі або малошкідливі, які не псують програм чи дисків, а нагадують про свою життєдіяльність текстовими повідомленнями, музикою, графічними відеоефектами - їх називають вірусами-жартами;

— небезпечні- перешкоджають нормальній роботі, захоплюють оперативну пам'ять, дисковий простір, шифрують каталоги і таблиці розміщення файлів, сповільнюють і ускладнюють виконання програм чи команд;

— особливо небезпечні - віруси-бомби - псують програми, інформацію на дискетах, вінчестерах, в CMOS, виводять з ладу операційну систему, роблять комп'ютер нероботоздатним.

Потрібно відмітити, що навіть нешкідливі віруси, в яких не закладені шкідливі ефекти, зменшують вільний простір на дисках, внаслідок можливих помилок і не передбачених змін обставин можуть викликати катастрофічні наслідки. Деякі віруси «коректно» поводять себе в старих версіях операційних систем але псують диски і програми в нових.

В окрему групу потрібно виділити легендарні міфічні віруси руйнівної дії, про які часто згадують в популярній пресі і навіть спеціальній літературі, і хоч можливість їх існування і поширення теоретично не відкидається, однак в реальному житті, на щастя, ще не зареєстровані.

Серед них варто згадати:

1) Віруси, які викликають теплове перегрівання і руйнування ділянок мікросхем з допомогою зациклення обчислювальних процесів і перевантаження окремих електронних елементів (подібний принцип використовується і для багатогодинного випробовування нових комп’ютерів тестуючими програмами).

2) Вірус, який викликає руйнування (падіння) головок вінчестера, викликаючи резонансний режим роботи періодичним звертанням до певних секторів.

3) Вірус ”666”, який з допомогою чергування кадрів негативно впливає на самопочуття людини, яка працює за дисплеєм.

4) Віруси, які негативно впливають на підсвідомість з допомогою прихованих кадрів телевізійного зображення.

Сюди можна віднести так звані “корисні” віруси, можливість існування яких обгрунтовувалась Д.Коеном і навіть деякі приклади наводились в літературі :

1) Віруси-архіватори, які стискають програми, звільняючи місце на дисках.

2) Віруси-імунізатори, які попереджують зараження програм іншими вірусами, залишаючи мітки (ознаки), які робить справжній (шкідливий) вірус.

3) Віруси-вакцини - варіанти небезпечних вірусів з вилученим механізмом руйнування, розмноження яких перешкоджає поширенню справжнього вірусу;

4) Віруси-антивіруси, які борються з результатами роботи небезпечних вірусів, повертаючи інфіковані програми до початкового вигляду;

З технічних причин розповсюдження вказаних типів вірусів в поширених операційних системах типу MS DOS, OS2, UNICS, MS Windows дуже і дуже проблематичне.

1.2. За місцем проникнення(механізмом поширення)

За використанням специфічних елементів файлової структури для проникнення і відповідних механізмів розмноження розрізняють :

1) Програмні файлові віруси, які дописують свої копії до програм на машинній мові, тобто до файлів з розширеннями .COM, .EXE (також .SYS, .OVL , .DRV і деяких інших). Віруси самі найчастіше поширюються у вигляді складної але порівняно невеликої програми в машинних двійкових кодах, яка дописуються до .COM чи .EXE файлів і робить спробу непомітно розмножуватись (дописувати свої копії до інших програм) в той момент, коли інфікована програма починає виконуватись. Найчастіше переносяться разом з іграми малодосвідченими користувачами.

2) Бутові (від Boot- завантажувач), дописують свої копії до дискет і жорстких дисків.

На магнітних дискетах інформація записується двійковими числами намагнічуванням окремих ділянок магнітної поверхні . Під час форматування магнітна поверхня дискети розмічається на концентричні кола -доріжки, які розбиваються на суцільні ділянки для запису- сектори..

При стандартному форматуванні 5,25-дюймових дискет об'ємом 360 кілобайтів утворюється 40 доріжок на 9 секторів з кожної сторони, 3,5-дюмових об'ємом 1,44 мегабайтів - 80 доріжок на 18 секторів з кожної сторони, розмір сектора на дискеті 512 байтів.

Особливу роль для роботи з дискетами відіграє службова інформація, записана в початкових секторах. В початковому секторі під час форматування записується невелика програма-завантажувач (BR-Boot Record), яка містить мітку , дані про формат - геометричні параметри дискети і про файли операційної системи (для системних дискет). Декілька наступних секторів містять інформацію про кореневий каталог (назви файлів, довжина, дата і час створення, атрибути) і FAT-таблицю розміщення файлів, в якій відмічаються ланцюжки секторів, зайняті кожним файлом.

Принцип зберігання інформації на жорстких дисках аналогічний . Інформація записується на магнітних поверхнях, нанесених на алюмінієві чи керамічні диски, які об'єднуються на одній осі в єдиний пакет. Для читання і запису для кожної поверхні використовується одна або декілька магнітних головок.. Група доріжок, які розташовані на відповідних поверхнях різних дисків і з якими операції запису і зчитування здійснюється одночасно, називають циліндром. Щільність запису і швидкість обертання дуже високі. Розмір сектора (стандартний) 1024 байти. Початкова системна область жорсткого диска аналогічна розглянутій вище для дискет. Поскільки жорсткі диски розбивають на декілька розділів, які називають логічними дисками, то в початковій системній області крім

інформації, розглянутої вище для дискет, записується Master Boot Record (MBR) з таблицею розділів жорсткого диска.

Логічна організація дисків може відрізнятись від фізичної. Група секторів, з якими операційна система працює, як єдиним цілим, (розташовані, як правило, на протилежних сторонах чи одному циліндрі) називається кластером.

Будь-яка операція з дискетою починається із читання Boot-сектора і саме цей елемент системи використовують для свого поширення бутові віруси. Вони заміняють оригінальний завантажувач , або дописують туди свій початок (голову), а друга частина вірусу (хвіст) записується у вільних секторах. Щоб заблокувати звертання до цих секторів, вони позначаються в таблиці розміщення файлів як дефектні («псевдодефектні» сектори).

Під час читання інфікованої дискети вірусна програма-завантажувач проникає в оперативну пам'ять і заражає системні сектори вінчестера і всі дискети, з якими користувач працює.

3) Файлово-бутові - складні типи вірусів, мають подвійний механізм розмноження, що значно прискорює їх поширення, часто використовують алгоритми шифрування, стелс- технологію, майже всі резидентні.

4) Мережеві віруси - розмножуються в мережах , враховуючи особливості мережевих систем, і з часом блокують їх роботу, що призводить до значних простоїв і втрат робочого часу великих колективів і прирівнюється до диверсії чи шкідництва. В комп'ютерних мережах з операційною системою MS DOS не набули поширення;

5) Екзотичні віруси використовують для свого поширення нетрадиційні способи: дописуються до текстових файлів (.TXT , .DOC), до програм на якійсь мові програмування (.PAS, .C,.ASM), до командних файлів (.BAT) або використовують для свого розмноження особливості роботи поширених програм (архіваторів, драйверів, текстових редакторів);

поширюються мляво, тому великої небезпеки не складають, а цікаві більше з теоретичної точки зору. Іноді бувають спалахи активності деяких видів, наприклад, внаслідок масового обміну документів, створених редактором WORD 6/7 , з 1995 року активно поширюються .DOC-віруси, які використовують макрокоманди цього редактора.

6) «Психологічні» віруси - розраховані на цікавість користувача. Відомий вірус «Різдв'яна ялинка», який стрімко поширився по більшості країн Європи, був звичайною програмою і не мав власного вірусного механізму поширення.

Близькими до вірусів є програми-«троянські коні» - замасковані під поширені програми «шкідники», а також вбудовані в звичайні програми системи захисту, які «дрімають» до певного моменту часу або події (внесення недозволених змін, порушення авторських прав, використання без дозволу - ліцензії та ін.). Внаслідок власної недосконалості чи помилок (неправильний аналіз обладнання, зміна конфігурації обладнання чи версії операційної системи, пошкодження вірусами) або внаслідок збігу обставин можуть робити проблематичними надійну роботу і використання програмного забезпечення.

1.3. За способом використання оперативної пам'яті

1) Резидентні віруси, які закріплюються в оперативній пам'яті і звідти роблять спроби на протязі всього сеансу роботи (до виключення чи перевантаження комп'ютера) дописувати свої копії до файлів чи дисків ; деякі навіть «переживають» перевантаження операційної системи.

2) Нерезидентні віруси менш активні, бо «стартують» тільки в момент початку чи завершення роботи інфікованої програми, або під час виконання операцій з файлами .

1.4. За особливостями алгоритмів

1) Компаньйони- віруси, які не змінюють файли. Створюють для EXE-файлів супутники з розширеннями .COM, які першими виконуються і поширюють вірус. ?

2) Віруси- «черв'яки» - проникають в пам'ять комп'ютера з мережі, знаходять адреси інших комп'ютерів і посилають свої копії. В мережах IBM-комп'ютерів не поширені.

3) Паразитуючі - під час поширення обов'язково змінюють сектори дисків або файлів;

4) Студентські - примітивні віруси , як правило з помилками, внаслідок чого псують файли і диски, часто виникають внаслідок незначної переробки старих вірусів із знайденої в Internet'і літературі. ?

5) Віруси-невидимки – під час перевірки зараженого файлу вірус з нього втікає (ховається в іншому місці на диску), заміняючи себе частиною оригінальної програми, а після перевірки повертається назад; за аналогією з американськими літаками-невидимками їх часто називають стелс-вірусами (Stealth).

6) Поліморфні віруси – багатоваріантні зашифровані самозмінювані віруси – «мутанти», які в процесі розмноження модифікуються, що ускладнює їх розпізнавання і знешкодження; використовують для свого поширення всі можливі шляхи (файли , диски, оперативну пам'ять) – дуже небезпечні і найбільш життєздатні. Найважче піддаються лікуванню - вимагають спеціальної для кожного вірусу програми трасування і розшифровки.

2. Найбільш поширені типи вірусів

2.1. Віруси-жарти

Хоч повністю нешкідливих вірусів в принципі бути не може, бо всі віруси засмічують пам'ять, диски і канали зв'язку, заважають нормальній роботі інших програм, змінюють їх код, втручаються в роботу операційної системи, досить велика група відзначається коректним механізмом розмноження і «гуманним» супутнім ефектом. Вони не псують програм чи дисків, а нагадують про свою життєдіяльність текстовими повідомленнями, музикою, чи відеоефектами . Часто віруси-жарти лякають повідомленнями про форматування дискет чи жорстких дисків, імітують несправність апаратури.

Музичні віруси. Найбільш відомими є велике сімейство (декілька поколінь) болгарських вірусів Yankey Doodle - о 17.00 грають відому мелодію- гімн США (загадковий прояв антипатріотизму). Для важчого виявлення це відбувається з імовірністю 1/8. За останній час з'явились віруси, які грають гімни Росії, України,Білорусії.

Вірус Christmas.1694 виводить на екран різдв'яні поздоровлення і грає новорічну мелодію. Вірус Girls освідчується в коханні і грає мелодію «Yesterday». Вірус Holms.6161 грає мелодію з фільму «Шерлок Холмс». Вірус GoodBye.839 грає мелодію «Goodbye, America» рок-групи «Наутілус Помпіліус».

Потрібно пам'ятати, що не всі музичні віруси є жартами, - деякі крім програвання музики викликають негативні наслідки. Наприклад, вірус Funeral періодично грає похоронний марш і перевантажує операційну систему.

Віруси з відеоефектами. Flip - перевертає зображення на екрані, Mirror -транспонує зображення, Macaroni- трусить екран, Metallica-

складний відеоефект, внаслідок якого зображення пливе і скручується, Rotor -в тексті на екрані створює враження обертання символів / I \ | -- послідовним їх чергуванням. Дуже гарний відеоефект викликає вірус Snow - плавний снігопад. Вірус Cascade (Falling Letters-«Буквопад»)- ефект осипання букв на екрані. Ping-Pong - ефект стрибаючої кульки, яка відбивається від символів і меж екрана.

Віруси з повідомленнями. Більшість вірусів містять в своєму коді рядки тексту, залишенні їх авторами з різних міркувань, часто після проникнення в комп'ютер віруси посилають їх на екран чи прінтер.
Поскільки антивірусні діагностичні програми розпізнають відомі віруси за такими текстовими вставками, то повідомлення в тілі вірусів часто зашифровані їх авторами.

Зустрічаються повідомлення у вигляді віршів, псевдографіки, лозунгів, які можна назвати дадзибао чи граффіті комп'ютерної доби. Вірус Чукча виводить гумористичний текст, StoryTeller - досить довгий англійський текст -розповідь, CPSU - моральний кодекс будівника комунізму, сімейство CivilDefence - різні лозунги і вірші на тему серпневих подій в Москві 1991 р.

2.2. Віруси руйнівної дії

Головною функцією (завданням) вірусів є непомітне розмноження і проникнення на якомога більшу кількість комп'ютерів, тому більшість авторів вірусів прикладають зусилля для маскування процесу розмноження і не допускають псування програм, на яких вірус паразитує. Однак внаслідок помилок, чи недосвідченості автора, чи виходу з під контролю під час тестування і відладки - переважна частина вірусів наносить відчутну шкоду, втрати робочого часу для ліквідації наслідків інфекції, а також відволікає багато часу і зусиль для постійного контролю і запобігання можливого проникнення.

Крім некваліфіковано написаних вірусів, які безнадійно псують програми і диски внаслідок помилок в алгоритмах, багато вірусів з «коректним» механізмом поширення мають небезпечний супутній ефект, закладений в них авторами-терористами з людиноненависницькими чи геростратівськими комплексами або просто паталогічною відсутністю почуття відповідальності.

Вірус «Атомний вибух» нищить інформацію на вінчестері, причому чим ближче до «епіцентру» (таблиці розміщення файлів), тим більше пошкоджених секторів.

Vienna.1014 в листопаді форматує вінчестер.

Blackmonday інфікує .COM та .EXE файли. Щопонеділка форматує вінчестер.

Killer.964 знищує файли з ролшириннями INI, SFP, SFL, LOD, WID, FON, CDR, MEM, PRG, DBT, FRM.

DiskFull.1871 - зашифрований вірус, в залежності від лічильника витирає сектори дисків і виводить повідомлення : Disk Full. Press any key to continue.

Дуже небезпечне сімейство вірусів, які викликають "зникнення" жорсткого диска при завантаженні з неінфікованої дискети. Для цього вони шифрують або переносять таблицю розділів жорсткого диска (найбільш важливий елемент файлової системи). Поки вірус знаходиться в оперативній пам’яті , все здається нормальним, тому що вірус інформує DOS про розташування таблиці або містить її в своєму коді. Якщо завантажитись з незараженої дискети, то DOS не знайде таблицю розділів, так як не буде вірусу, який інформує про її розташування. В результаті при спробі звертання до жорсткого диска з’явиться повідомлення "Invalid drive specification" або подібне.

Така поведінка властива для бутових вірусів Crazy Boot, Frankenstein, Neuroquila і Stoned.Empire.Monkey.

DirFiller.1409 - стелс-вірус,- шифрує кореневий каталог диска C:

Один з найбільш небезпечних і в свій час поширений One Half - резидентний поліморфний файлово-бутовий вірус. Код віруса зашифрований і розсіяний по зараженому файлу. При завантаженні з інфікованого жорсткого диска шифрує два останніх циліндри диска, при наступному - ще два, і так далі, поки не дійде до першого циліндра.

Коли кількість зашифрованих даних перевищить половину диска, вірус повідомляє:

Dis is one half.

Press any key to continue...

Після завантаження в оперативну пам'ять вірус розшифровує і знову зашифровує сектори, так що користувач не помічає того, що його дані зіпсовані. Але після лікування MBR старими антивірусними програмами-поліфагами всі дані в зашифрованих секторах втрачаються і вінчестер потрібно переформатовувати. Зашифровані багатьма новими вірусами диски коректно лікуються і розшифровуються новими версіями DrWeb.

Аналогічно до One Half діють віруси Annoying.4060, Bad_Head, Byway, CPW, Crazy Boot, Da'Boys, Die Hard, Emmie.2702, Emmie.2823, Emmie.3097, Fairz, Frankenstein, Neuroquila, Sat_Bug.Natas, Urkel. Не можна відновлювати зашифровані жорсткі диски стандартними поліфагами або засобами Norton Disk Doctor чи іншими утилітами. Потрібно знайти якомога новіші версії антивірусних програм і по документації до них визначити найкращу для знешкодження наслідків шифрування конкретного типу вірусу.

2.3. Файлові програмні віруси

Поширені типи файлових вірусів дописуються до документів Word (див. Макровіруси), до пакетних BAT-файлів (відомо декілька BAT-вірусів київського походження) і переважна більшість відомих типів (приблизно 90%)- до програм на машинній мові (в машинних двійкових кодах). Програмні віруси можуть проникати у файли системних драйверів з розширенням імені SYS, в тому числі IO.SYS та MSDOS.SYS, і виконувані двійкові файли (EXE, COM) включачи нові типи EXE-файлів (NEW EXE) і NLM-файли, виконувані в операційних системах типу MS-Windows, OS/2, Novell Netware та ін.

Можливе дописування вірусу у файли даних, але внаслідок помилки вірусу, або як прояв його агресивних властивостей. Відомі віруси , які інфікують файли з текстами програм на мовах високого рівня , бібліотечні чи об'єктні модулі. Вони для свого поширення вимагають спеціального програмного середовища (компіляторів, інструментальних програм). Їх відносять до класу екзотичних, бо на практиці не зустрічаються і цікаві лише з теоретичного погляду.

Проникнення вірусів у SYS-файл

Віруси, проникаючи в SYS-файл, дописують свої коди до тіла файлу і модифікують адреси програм стратегії (Strategy) та переривання (Interrupt) драйвера. При ініціалізації зараженого драйвера вірус перехоплює відповідний запит операційної системи, передає його драйверу, чекає відповіді на цей запит, коригує його і залишається в оперативній пам'яті разом з драйвером в одному блоці пам'яті. Такий вірус може бути дуже небезпечним та живучим, бо проникає в оперативну пам'ять при завантаженні DOS раніше більшості програм, в тому числі антивірусних.

Можливий інший варіант інфікування , коли вірус модифікує його заголовок так, що DOS розглядає інфікований файл як ланцюжок із двох (або більше) драйверів.

Аналогічно вірус може записати свої команди на початку драйвера, а якщо у файлі розміщено декілька драйверів, то і в середину файлу.

Проникнення вірусу в COM і EXE-файли

Виконувані двійкові файли мають формати COM або EXE, які відрізняються заголовком і способом запуску програм на виконання. Розширення імені файлу (".COM" або ".EXE") не завжди відповідає дійсному формату файлу, що , правда, ніяк не впливає на роботу програми. Файли COM і EXE заражаються по-різному, тому вірус повинен відрізняти файли одного формату від іншого. Віруси вирішують цю задачу двома шляхами: одні аналізують розширення імені файлу (".COM", ".EXE"), другі - заголовок файлу.

В більшості випадків вірус інфікує файл коректно, тобто за інформацією в тілі вірусу можна повністю відновити заражений файл. Але віруси, як і більшість програм, часто містять непомітні з першого погляду помилки. Тому цілком коректно написаний вірус може непоправно зіпсувати файл під час його зараження. Наприклад, віруси, які розрізняють типи файлів за розширеннями імені (.COM, .EXE), дуже небезпечні, бо псують файли, у яких розширення імені не відповідає внутрішньому формату.

Файлові віруси при розмноженні дописуються в тіло інфікованого файлу: на початок, в кінець або середину. Існує декілька можливостей проникнення вірусу в середину файлу: він може бути скопійований в таблицю адрес EXE-файлу (BootExe), в область стека файлу COMMAND.COM (Lehigh), може "розсунути" файл або переписати частину файлу в його кінець, а свої команди у звільнене місце (April1st.Exe, Phoenix). Крім того, копіювання вірусу в середину файлу може бути результатом помилки вірусу - в цьому випадку файл буде непоправно

зіпсований. Можливі інші способи,наприклад, вірус "Mutant" застосовує стискання (архівацію) деяких ділянок файлу.

Проникнення вірусу на початок файлу

Відомі три способи дописування вірусу на початку файлу. Перший спосіб полягає в тому, що вірус переписує початок інфікованого файлу в його кінець, а сам копіюється в звільнене місце. При зараженні файлу другим способом вірус створює в оперативній пам'яті свою копію, дописує до неї інфікований файл і зберігає отриману комбінацію на диску. При зараженні третім способом вірус записує свої команди на початку файлу, не зберігаючи оригінального початку файлу. Зрозуміло, що програма при цьому перестає працювати і не відновлюється. Деякі віруси, що розмножуються першим і другим способом, дописують блок інформації також і в кінець файлу (наприклад, вірус Jerusalem за цим блоком відрізняє заражені файли від незаражених).

Проникнення вірусу на початок файлу відбувається переважно при зараженні COM-файлів. EXE-файли заражаються таким методом в результаті помилки вірусу, або при використанні алгоритму вірусу Pascal (руйнується початок файлу).

Проникнення вірусу в кінець файлу

Найбільш поширеним способом поширення вірусу є дописування вірусу в кінець файлу. При цьому вірус змінює початок файлу таким чином, щоб першими виконуваними командами програми, яка зберігається у файлі, були команди вірусу. В COM-файлі у більшості випадків це досягається зміною його перших трьох байтів на команду безумовного переходу на тіло вірусу. EXE-файл о переводиться у формат COM-файлу і потім заражається як COM-файл, або модифікується заголовок файлу. В заголовку EXE-файлу змінюється значення стартової адреси (CS:IP) і значення довжини виконуваного модуля (файлу), рідше- регістри-

покажчики стека (SS:SP), контрольна сума файлу. Крім того довжини файлів перед зараженням можуть збільшуватись до значення, кратного параграфу (16 байтів).

Алгоритм роботи файлового програмного вірусу

Вірус, після передачі йому керування , здійснює такі дії (для конкретного вірусу список може бути розширений, пункти можуть мінятись місцями):

1) відновлює програму (але не файл) до початкового вигляду (наприклад , у COM-програми відновлюється декілька перших байтів, у EXE-програми обчислюється істинна стартова адреса, у драйвера відновлюється значення адрес програм стратегії і переривання);

2) якщо вірус резидентний, то він перевіряє оперативну пам'ять на присутність своєї копії і інфікує пам'ять комп'ютера, якщо копія вірусу не знайдена;

якщо вірус нерезидентний, то він шукає незаражені файли в активному та інших каталогах логічних дисків, а потім заражає знайдені файли;

3) виконує супутній руйнівний ефект (якщо він передбачений для даного вірусу);

4) виконує графічні або звукові ефекти (супутні функції резидентного вірусу можуть включатись через деякий час після активізації в залежності від часу, конфігурації системи, внутрішніх лічильників або інших умов);

5) повертає керування основній програмі.

Метод відновлення програми до початкового вигляду залежить від способу зараження файлу.

2.4. Бутові віруси

Вражають завантажуючий (Boot) сектор дискети і Boot-сектор або Master Boot Record (MBR) жорсткого диска. При інфікуванні диска вірус в більшості випадків переносить оригінальний Boot-сектор (або MBR) в інший сектор диска (наприклад , в перший вільний). Якщо довжина вірусу більше розміру сектора, то в заражений сектор поміщається перша частина вірусу, решта - в інших секторах. Потім вірус копіює системну інформацію із оригінального завантажувача в свій код та переносить його в нульовий завантажуючий сектор (для MBR такою інформацією являється Disk Partition Table, для Boot-сектора дискет - BIOS Parameter Block).

Існує декілька способів розміщення на диску копії оригінального незараженого завантажуючого сектора і продовження вірусу: в сектори вільних кластерів логічного диска, в невикористовувані або рідко використовувані системні сектори, в сектори, розташовані за межами інфікованого диска. Якщо продовження («хвіст») вірусу разміщується у вільних секторах диска (для пошуку цих секторів вірусу потрібно аналізувати таблицю розміщення файлів - FAT), то, як правило, вірус відмічає у FAT ці кластери як дефектні (так звані псевдодефектні кластери). Цей спосіб використовується вірусами Brain, Ping-Pong та ін.

Віруси сімейства Stoned використовують інший метод - розташовують старий нульовий сектор в невикористовуваному або рідко використовуваному секторі. На вінчестері це один із секторів, розташованих між MBR та першим Boot-сектором, а на дискеті - один з останніх секторів кореневого каталога.

Рідше використовується метод збереження продовження вірусу за межами диска, поки що зустрічається тільки при зараженні дискет. Для цього вірусу приходиться форматувати на дискеті додаткову доріжку

(метод нестандартного форматування), наприклад, 41-у доріжку на дискеті з об'ємом 360 кілобайт.

Існують інші методи розміщення вірусу на диску, наприклад, віруси сімейства Azusa містять у своєму тілі стандартний завантажувач MBR і при зараженні записують його замість оригінального MBR без його збереження.

Алгоритм роботи бутового вірусу

Відомі бутові віруси завжди резидентні. Вони проникають в пам'ять комп'ютера під час завантаження з інфікованого диска. При цьому системний завантажувач зчитує вміст першого сектора диска, з якого відбувається завантаження, заносить зчитану інформацію в пам'ять і передає на неї (тобто на вірус) керування. Після цього починають виконуватись команди вірусу, який:

1) зменшує розмір вільної пам'яті (два байти за адресою 0040:0013);
2) зчитує з диска своє продовження (якщо воно є);
3) переносить себе в іншу область пам'яті (наприклад, в самі старші адреси пам'яті);
4) встановлює необхідні вектори переривань;
5) здійснює, якщо вони є, додаткові дії;
6) копіює в пам'ять оригінальний Boot-сектор і передає на нього керування.

Далі бутовий вірус поводить себе так само, як і резидентний файловий вірус - перехоплює звертання операційної системи до дисків і інфікує їх, в залежності від деяких умов виконує деструктивні дії або викликає звукові чи відеоефекти.

2.5. Стелс-віруси.

Стелс (Stealth) -віруси (віруси-невидимки) -перехоплюють звертання DOS до інфікованих файлів або секторів дисків і "підставляють" замість себе незаражені ділянки інформації. Крім того такі віруси при звертанні до файлів використовують оригінальні алгоритми для

"обманювання" резидентних антивірусних програм. До стелс-вірусів відносяться віруси Frodo, Fish#6, Brain та багато інших.

2.6. Поліморфні шифровані віруси

Найбільш складні типи вірусів. Складаються з двох частин: основної, зашифрованої криптографічним методом з допомогою змінного ключа, та порівняно невеликої багатоваріантної програми - розшифровщика. Деякі поліморфні віруси складаються із десятків частин, розсіяних по файлах або дисках. Під час активізації віруса розшифровуюча частина збирає разом і розшифровує команди віруса, після чого знову зашифровує з іншим ключем і записує в новий файл чи диск основну частину і модифікований варіант самої себе. Ключ для шифрування визначається випадковим чином з допомогою лічильників чи системного годинника. Багатоваріантність кодів розшифровуючої частини забезпечується таблицями еквівалентних замін, з допомогою яких одні і тіж дії виконуються різними ланцюжками команд. Внаслідок цього поліморфні віруси не мають постійної довжини і ланцюжків байтів. Два екземпляри одного типу вірусу практично ніколи не співпадають.

Незважаючи на складний алгоритм, поліморфні віруси активно поширюються.

Для ускладнення виявлення і знешкодження в алгоритмах багатьох поліморфіків передбачені спеціальні команди і режими роботи для унеможливлення стеження за їх роботою (трасування) і розшифровки алгоритмів (дизасемблювання) .

Алгоритми поліморфних вірусів дуже нагадують алгоритми, які використовують для захисту програм від копіювання чи несанкціонованого доступу. Аналогічно алгоритми для знешкодження цих вірусів нагадують методи, якими користуються хакери-кракери для проникнення в чужі програми і системи захисту.

До шифрованих належать віруси сімейства MtE, Mutant, Chameleon, Bomber, OneHalf та багато інших.

2.6. Макровіруси

Для свого поширення використовують макрокоманди, які відіграють роль «внутрішньої» мови програмування в багатьох редакторах, електронних таблицях та інших поширених програмних продуктах і використовуються для створення нових складних команд- макросів, перепрограмування клавіш, для побудови демонстраційних програм, для створення складних документів, для розвитку основної програми шляхом побудови нових функцій та об'єктів тощо.

Якщо раніше макровіруси відносились до класу екзотичних, то останнім часом в зв'язку з масовим обміном документів, створених в текстовому редакторі Word 6/7, який в переважній кількості країн на різних платформах комп'ютерів став стандартом де-факто, почалась масова епідемія цього класу вірусів (Colors, Concept, DMV, Nuclear). Крім того відомі віруси, які використовують макрокоманди Write, WordPad, Excel.

Перші макровіруси WinWord з'явились влітку 1995 року. Мова WordBasic, яка є підмножиною Visual Basic, досить проста і щоденна поява нових макровірусів (зараз їх налічується більше 1000 видів) стала серйозною проблемою. Це відчутно сповільнює роботу і наносить великі збитки.

Віруси сімейства WinWord інфікують файли з розширеннями .DOC та .DOT. Зараження системи відбувається під час редагування інфікованого DOC-файлу. Після зараження віруси записуються у всі нові створювані DOC-файлы.

Характерні прояви вірусів сімейства WinWord :

1) Неможливість конвертування зараженного документу Word в інший формат.

2) Неможливість запису документу в інший каталог/на інший диск командою "Save As".

3) Заражені файли мають формат Template. При зараженні віруси WinWord конвертують файли з формату Word Document в Template.

Віруси для Word можуть інфікувати комп'ютери на різних платформах, на яких встановлений текстовий редактор, сумісний з Microsoft Word версії 6 або 7.

Захиститись від вірусів WinWord можна з допомогою системного макросу DisableAutoMacros, який забороняє автоматичний запуск макросу AutoOpen під час відкриття файлів.

Механізм розмноження макровірусів.

Під час відкривання документу Word перевіряє його на присутність макросу AutoOpen. Якщо такий макрос існує , то Word виконує його. Якщо документ інфікований, то Word викликає заражений макрос AutoOpen (якщо це не заборонено системним макросом DisableAutoMacros), і, таким чином, запускає код вірусу.

В вірусах сімейства WinWord макрос AutoOpen містить команди перенесення макросів вірусів область глобальних (загальних) макросів Word і під час запуску AutoOpen вірус заражає область глобальних макросів. Потім вірус змінює макрос FileSaveAs і перехоплює таким чином команду збереження файлу на диску. При виклику цієї команди вірус заражає збережений файл, для цього вірус конвертує файл у формат Template (що робить неможливими подальші зміни формату файлу, тобто конвертування в будь-який не-Template формат) і записує у файл свої макроси, включаючи AutoOpen. Таким чином вірус інфікує кожен DOC-файл, збережений командою "Save As".

Під час виходу з WinWord глобальні макроси (включаючи макроси вірусу) автоматично записуються в DOT-файл глобальних макросів (звичайно

таким файлом є NORMAL.DOT). Таким чином при наступному запуску WinWord вірус активізується в той момент, коли WinWord завантажує глобальні макроси, тобто зразу.

Для боротьби з макровірусами створено багато імунізаторів, які поширюються у вигляді .DOC - файлів і працюють за тою самою схемою, що і самі віруси - під час відкривання заміщають системні макроси своїми таким чином, щоб перешкодити розмноженню справжніх вірусів.

В зв'язку з використанням в нових макровірусах додаткових механізмів розмноження - через MS DOS із шифруванням і стелс-технологією, - використання захисних .DOC-файлів для боротьби з макровірусами є недостатнім.

Найкращих результатів (але далеко не стовідсоткових) у виявленні і знешкодженні макровірусів досягає програма DrWeb.

Перший вірус для Word, пійманий "в живому вигляді" отримав назву **WinWord.Concept (або WW6Macro).** Вірус складається з п'яти макросів: AAAZAO, AAAZFS, AutoOpen, PayLoad, FileSaveAs. В зараженому файлі присутні рядки:

see if we're already installed
iWW6IInstance
AAAZFS
AAAZAO
That's enough to prove my point

та багато інших . В зараженій системі у файлі WINWORD6.INI присутній рядок WW6I= 1

При першому запуску вірусу (тобто при першому перегляді зараженого файлу) з'являється MessageBox з цифрою 1 всередині .

WinWord.Nuclear інфікує файли-документів формату Microsoft Word і файли формату COM, EXE і NewEXE (Windows). В заражених

файлах-документах вірус міститься у вигляді зашифрованих макросів. Періодично запускає інший вірус, який інфікує COM, EXE и NewEXE - файли.

При зараженні COM, EXE і NewEXE файлів вірус дописується в їх кінець. Вірус в цих файлах не може інфікувати файли-документів.

Варіант вірусу в документах складається із дев'яти макросів: AutoExec, AutoOpen, FileSaveAs, FilePrint, FilePrintDefault, InsertPayload, Payload, DropSuriv, FileExit. Якщо макроси з такими іменами вже були визначені, то вони знищуються. В подальшому файли-документи заражаються при їх закритті (при виконанні макроса FileSaveAs). Вірус проявляється трьомаспособами:

1) запускає COM/EXE/NewEXE вірус,

2) добавляє рядки тексту під час друку документів (приблизно в кожен 12-й файл)

And finally I would like to say:
STOP ALL FRENCH NUCLEAR TESTING IN THE PACIFIC!

{І наприкінці я хотів би сказати :
Зупиніть всі французькі ядерні випробування в Тихому океані ! }

3) псує системні файли 5-го квітня.

Варіант вірусу в COM/EXE/NewEXE-файлах використовує стандартний алгоритм розмноження. Перевіряє імена файлів і вражає тільки файлы *.DL*, *.CO* и *.EX*. В COM/EXE/NewEXE-файлах вірус вторинного ефекту не проявляє. Містить рядки :

=Ph33r=

Qark/VLAD

3. Антивірусні програми

3.1. Класифікація

1. Сторожові програми - монітори слідкують за всіма підозрілими характерними для розмноження вірусів ситуаціями і повідомляють про них користувачеві.

Для розмноження бутових вірусів характерним є спроба запису в завантажуючий сектор системного диска. На більшості нових типів комп'ютерів в BIOS записана програма, яка контролює спробу запису в системну область вінчестера. Під час завантаження комп'ютера потрібно викликати **SETUP** (клавішами Del або Ctrl+Esc) і знайшовши пункт **Virus Warning** вибрати **Enabled** для її активізації чи **Disabled** для відключення контролю.

Для розмноження файлових вірусів характерні немотивовані звертання до дисків (дискет), спроби модифікації певних типів файлів, резидентне закріплення в оперативній пам'яті. Існують сторожові програми, які повідомляють про всі такі ситуації і вимагають дозволу користувача для продовження роботи. Поскільки такі ситуації виникають досить часто і під час роботи звичайних програм, то такі зупинки сповільнюють роботу і на практиці частіше використовують більш складні діагностичні монітори.

2. Ревізори дисків- програми, які складають таблиці для системних секторів і всіх файлів, які постійно зберігаються на жорстких дисках, а потім періодично перевіряють диски для виявлення підозрілих змін. Внаслідок інфікування можуть змінюватись довжина файлу, час і дата створення, системні атрибути. Деякі «хитрі» віруси запам'ятовують і після проникнення у файли відновлюють в таблиці розміщення файлів старі дані, крім того багато вірусів для важчого виявлення використовують більш складні стелс-алгоритми. Тому ревізори визначають з допомогою різних

функцій BIOS і DOS заявлену і дійсну довжину і для більш точного контролю для кожного файлу обчислюють контрольну суму.

Ревізори дисків швидко перевіряють всі диски і повідомляють про всі змінені файли. Потім користувач повинен визначити причину змін. Якщо змінився файл, з яким довго ніхто не працював, то це може свідчити про появу вірусу. Якщо однакові зміни відбулись з декількома різними файлами в різних каталогах чи дисках, то перш ніж піднімати тривогу, потрібно пересвідчитись чи не внесені вони програмами ScanDisk, NortonDiskDoctor, імунізаторами.

Якщо діагностичні програми повідомляють тільки про відомі типи вірусів, то з допомогою ревізорів можна зафіксувати появу ще не відомих. Ревізори не потрібно щомісяця оновлювати, як більшість інших антивірусних програм.

Для роботи в MS DOS рекомендується програма ADINF (автор - Д.Мостовой). Якщо на комп'ютері встановлені системи MS Windows 95/OSR2/NT, які під час завантаження і роботи змінюють велику кількість файлів і мають специфічну файлову структуру, то потрібно використовувати ревізор дисків, розрахований на конкретну версію операційної системи.

Після встановлення програми-ревізора рекомендується включити її виклик у самовиконуваний пакетний файл AUTOEXEC.BAT для щоденної перевірки всіх жорстких дисків.

3. Імунізатори-програми, які захищають файли і диски від зараження різними прийомами - вирівнюванням розмірів програм до розміру сегмента, записуючи мітки, які віруси залишають у заражених файлах для уникнення зациклення при повторному інфікуванні, заповненням вільних байтів бутового сектора захисними записами.

В зв'язку з величезною кількістю поширених типів вірусів і постійною появою нових, повністю файли і диски від проникнення вірусів таким способом нереально.

Імунізацію файлів і дискет проти деяких поширених типів вірусів можна виконати програмою Norton AntiVirus. Рекомендується також імунізувати редактор Word від макровірусів з допомогою AVPWW.DOC або DrWebWW.DOC.

4. Діагностичні програми - монітори і сканери дисків

Кожен вірус має в своєму коді характерне тільки для себе сполучення символів, команд, яке називають маскою і використовують для пошуку відомих типів вірусів у файлах і завантажуючих секторах. Для прискорення пошуку враховується місце проникнення різних типів вірусів (початок, середина чи кінець файлу, BR, MBR), супутні ефекти, маскувальні властивості.

Найбільш складною проблемою є виявлення поліморфних вірусів, які практично не мають повторюваних символів завдяки багатоваріантності та шифруванню більшої частини їхнього коду і мають алгоритми, які унеможливлюють їх трасування.

Для виявлення і ідентифікації цих вірусів програмою AVTK Dr Solomon використовується той факт, що всі вони резидентні і під час перебування в оперативній пам'яті перебувають в розшифрованому вигляді.

Діагностичні антивірусні програми складаються у вигляді сканерів, які використовуються для періодичної перевірки дисків на всі (чи якомога більшу кількість) поширених типів вірусів, або у вигляді резидентних програм-моніторів, які постійно знаходяться в оперативній пам'яті і перевіряють всі програми, які виконуються і всі нові диски (дискети), які підключаються.

Всі нові програми і дискети, з якими працюють не на одному комп'ютері, потрібно обов'язково перевіряти діагностичними програмами.

Повна і ретельна перевірка великих жорстких дисків займає чимало часу, але рекомендується проводити її щоденно вранці чи під час обідньої перерви.

5. Лікуючі програми - фаги. Програмісти, які пишуть прості віруси - це, як правило, погані програмісти. Тому навіть якщо руйнівний ефект автором не передбачений, внаслідок помилок або недосконалості алгоритму після проникнення вірусу в системні сектори комп'ютера чи враження файлів відбуваються непоправні втрати інформації. Єдиним способом надійного збереження програм і документів від пошкодження вірусами є їх постійне дублювання на дискетах, мережевих дисках або нових типах магнітних, електронних і оптичних дисків.

У випадку зараження потрібно витерти інфіковані файли і замінити їх «чистими» резервними копіями.

На практиці часті випадки, коли резервні копії інфікованих програм чи документів відсутності. В цьому випадку потрібно обов'язково проконсультуватись із спеціалістом і вибрати розраховану на даний тип вірусу лікуючу програму. Лікуючі програми - фаги «вбивають» вірус в тілі файлу, «викушуючи» його повністю або лише активну частину і повертають, якщо це можливо, файл до початкового вигляду. Для успішного лікування фаги повинні точно враховувати спосіб проникнення вірусу і конкретний алгоритм зміни вірусом файлів, на яких він паразитує.

В зв'язку з великою кількістю вірусів найбільш поширені програми-поліфаги, які розраховані на знешкодження великої кількості типів вірусів. При цьому з рекламною метою для збільшення кількості знешкоджуваних досить часто для лікування нових типів вірусів використовують старі

алгоритми. Знешкодження вірусу відбувається не повністю,- відновлені програми не працюють, або працюють з помилками.

Тому для особливо цінної інформації рекомендується перед лікуванням інфікованих файлів зробити окрему копію на дискеті, щоб після можливого невдалого лікування звернутись до спеціалістів за допомогою.

6. Евристичні аналізатори_- програми для пошуку шифрованих і невідомих типів вірусів.

Шукають віруси не за шаблонами, а з допомогою перевірки можливих місць проникнення на характерні для вірусів прояви і зміни. Для пошуку невідомих програмних файлових вірусів аналізуються коди і алгоритми COM і EXE-файлів. Підозрілими характерними для вірусів діями є використання недокументованих функцій DOS, перевірка каталогів і пошук файлів певних типів, заміна системних переривань своїми, характерними для шифрованих вірусів є використання великої кількості логічних операцій і прийомів, які ускладнюють трасування і відладку програм під час виконання.

Ефективність правильного визначення присутності вірусів евристичними аналізаторами коливається в межах від 40% до 60%, досить часто підозра лягає на неінфіковані файли. У випадку повідомлення про підозрілі файли, перш ніж піднімати тривогу, потрібно перевірити їх ще раз більш новими версіями антивірусних програм. Досить часто під підозру попадають системні програми, відладчики, антивірусні програми, системи захисту.

3.2. Короткий огляд поширених програм

Коли з'явились перші віруси, для кожного типу складались окремі програми для знешкодження. В наш час, коли кількість поширених типів вірусів оцінюється числом 8-14 тисяч і щодня з'являється декілька нових , для успішного захисту і боротьби використовують в основному багатофункціональні антивірусні програми і комплексні програмні пакети.

1) Діагностично-лікуюча програма-сканер **Aidstest** (автор Д.Лозінський)- найкраща для лікування старих типів вірусів і у випадках одночасного зараження декількома вірусами;

Перевірка і лікування дискет виконується командою

AIDSTEST A:/F/G/Q

2) Діагностично-лікуюча програма-сканер з евристичним аналізатором **DrWeb** (автор І.Данилов) - одна з найкращих програм за результатами різних тестів для пошуку поліморфних і макровірусів. Розшифровує каталоги на дисках після враження вірусами типу OneHalf.

3) **Norton Antivirus** - імунізатор, поліфаг-монітор. Для лікування складних типів вірусів рекомендує звертатись до фірми Symantec.

4) Діагностична програма -сканер **Microsoft Antivirus** входив в комплект програм операційних систем MS DOS і MS Windows. Для діагностики і знешкодження нових типів файлів потрібно підключати нову вірусну базу даних.

5) **ViruScan** відомої англійської фірми McAfee - поліфаг- сканер, одна з найкращих програм за наслідками тестувань останніх років.

6) **AntiVirus ToolKit Dr Solomon** - пакет антивірусних засобів для MS Windows 95 , включає ревізор дисків, діагностичний сканер і резидентний монітор, евристичний аналізатор і енциклопедію з описом близько 300 вірусів.

7) **ADINF**(«Диалог-наука», Д.Мостовой) - один з найкращих ревізорів дисків, крім того знаходить стелс-віруси.

Для роботи на комп'ютерах з MS Windows в зв'язку з особливостями їх файлової системи, довгими іменами файлів і полібутовою системою потрібно використовувати відповідні нові версії антивірусних програм.

Більшість «старих» ДОСівських вірусів під час роботи комп'ютера в MS Windows не активні, але активізуються і розмножуються в сеансах MS

DOS, тому для їх виявлення і знешкодження потрібно перезавантажити комп'ютер в режимі емуляції MS DOS і використовувати варіанти антивірусних програм для роботи в MS DOS.

4. Прийоми для захисту дисків і комп'ютерів від вірусів

Одним з основних методів боротьби з вірусами, як і в медицині, є своєчасна профілактична робота. Дотримуючись простих правил, можна значно зменшити імовірність інфікування вірусом і втрати інформації.

Якщо флешки використовуються тільки для зчитування з них файлів на різних комп'ютерах, вони обов'язково повинні захищатись механічно від запису (заклеюванням прорізів або слайдером).

Для постійного контролю за можливим проникненням вірусів потрібно вибрати і встановити програму-ревізор дисків і діагностичну програму - сканер дисків, узгоджені з версією операційної системи.

Для запобігання втрат інформації потрібно зробити резервні копії всіх оригінальних програм і цінних документів на захищених від запису носіях і зберігати їх в сейфі.

Для знешкодження наслідків вірусної інфекції потрібно підготувати для кожної версії OS, які встановлені на різних комп'ютерах, «чисті» системні диски з антивірусними програмами, орієнтованими на дану версію.

Для можливості відновлення пошкодженої інформації на жорстких дисках і в CMOS з допомогою Нортонівської утиліти Rescue для кожного комп'ютера підготувати і періодично оновлювати «рятівні» диски. З допомогою таких аварійних дисків можна швидко відновити дані про конфігурацію, які зберігаються в енергонезалежній пам'яті CMOS, завантачуючий сектор, таблицю розділів і таблиці розміщення файлів для конкретного жорсткого диска.

Всі нові диски і програми повинні проходити вхідний контроль. Для цього на кожному (або спеціально визначеному) комп'ютері потрібно

встановити нові версії антивірусних програм і постійно їх оновлювати. На кожному робочому місці потрібно підготувати короткі вичерпні інструкції.

Не можна запускати неперевірені файли, в тому числі отримані з мереж. Бажано використовувати тільки програми, отримані з надійних джерел. Бажано, щоб під час роботи з новими програмами в пам'яті резидентно знаходився антивірусний монітор.

Необхідно обмежувати коло людей, допущених до роботи на конкретному комп'ютері. Найбільш часто підлягають зараженню персональні комп'ютери колективного використання в школах, інститутах.

Характерним для нових операційних систем і прикладних програм є одночасне відкривання і робота з великою кількістю файлів. У випадку «зависання» комп'ютера, несподіваного вимкнення чи аварійного перевантаження інформація про розміри і розміщення файлів в каталогах не співпадає з дійсною. Тому наслідком таких випадків є поява і накопичення численних помилок на дисках, які з часом роблять операційну систему недієздатною.

Перед вимкненням комп'ютера обов'язково потрібно закривати всі працюючі програми. Для усунення помилок і підтримання порядку на жорстких дисках потрібно щоденно перевіряти всі розділи програмами ScanDisk або NortonDiskDoctor відповідної версії. Ці програми часто першими повідомляють про вірусоподібні зміни в завантажуючих секторах, таблицях розміщення файлів, змінах дат чи розмірів файлів.

Завдання для самостійної роботи

Пропонується виконати послідовніть дій, яку необхідно періодично проводити на кожному робочому місці, обладнаному персональним комп'ютером для попередження втрат інформації внаслідок проникнення вірусів, троянських програм чи некваліфікованих користувачів.

1. Контроль за вірусоподібними змінами.

Перевірити (надалі виконувати регулярно) час і дату. В OS MS DOS це можна зробити командами DATE і TIME. Однією з причин неправильних показів системного годинника може бути діяльність вірусів.

Уточнити версію операційної системи командою. Порівняти довжину і час створення системних файлів на різних комп'ютерах з однаковими версіями.

Скласти таблицю довжин для системних та EXE- файлів, встановлених на даному комп'ютері. Зміна довжини чи часу і дати цих файлів з великою ймовірністю свідчить про появу вірусів.

2. Перевірка всіх дисків антивірусними програмами.

Познайомитись з антивірусними програмами, встановлених на даному комп'ютері. Звернути увагу на дату їх написання. Перевірити всі дискети і розділи жорсткого диска діагностичними програмами.

Встановиту одну з нових версій антивірусних програм або додаткові інформаційні файли для вже встановленої. Підготувати коротку вичерпну інструцію для користувачів.

3. Перевірка файлової структури всіх розділів жорстких дисків.

Познайомитись з програмами ScanDisk і NortonDiskDoctor, з допомогою яких виявляються і виправляються помилки в каталогах і таблицях розміщення файлів на дискетах і жорстких дисках.

4.Підготовка системного та рятівного дисків.

Підготувати системну флешку (лазерний диск), записати декілька антивірусних програм, захистити від запису і тримати в надійному місці для можливого використання у випадку зараження комп'ютера вірусами чи пошкодження системних файлів на вінчестері.

З допомогою утиліти RESCUE підготувати аварійний компакт-диск для кожного комп'ютера з важливою системною інформацією, яка дає можливість відновити файлову структуру після руйнівної дії вірусів чи краху системи з інших причин (вимкнення напруги, випадкове знищення).

5. Профілактика макро-вірусів.

Якщо на комп'ютері встановлений текстовий редактор Word, перевірити яка захисна система для нього встановлена. При можливості встановити більш нову версію, викликаючи документ-імунізатор типу AVPWW.DOC або DRWEBWW.DOC.

Контрольні запитання

1. Дати визначення комп'ютерного віруса.
2. Порівняти діяльність комп'ютерних і біологічних вірусів. Знайти спільні риси і відмінності.
3. Назвати особливості, за якими класифікуються комп'ютерні віруси.
4. Як класифікуються віруси за супутнім ефектом ?
5. Які супутні ефекти викликають віруси-жарти ?
6. Які руйнівні дії характерні для небезпечних вірусів?
7. Які шляхи (механізми) використовують віруси для розмноження ?

8. Як модифікують інфіковану програму файлові віруси?
9. Пояснити особливості зберігання інформації на дискетах і жорстких дисках.
10. Якими способами поширюються бутові віруси.
11. Чим відрізняється спосіб поширення резидентних і нерезидентних вірусів?
12. Проілюструвати особливості алгоритмів складних типів вірусів на прикладі поліморфних і стелс-вірусів.
13. Назвати основні типи антивірусних програм.
14. Які антивірусні програми використовуються для профілактики вірусного зараження?
15. Які програми використовуються для подолання наслідків руйнівної дії вірусів?
16. Які програми використовуютьс для пошуку нових і шифрованих типів вірусів?
17. Які прийоми використовуються для профілактики вірусної інфекції?