Урок 13 ***інформатика 9*** ***Калініченко М.М.***

Тема: Комп'ютерні віруси. Призначення, принципи дії. Класифікація антивірусних програм. Практична робота № 5 «Захист комп'ютера від вірусів».

Навчальна мета: Познайомити учнів з класифікацією вірусів та антивірусних програм. Допомогти учням засвоїти роботу з антивірусними програмами, познайомити їх з відомими вірусами та профілактикою щодо зараження ними

Розвивальна мета: Розвиток пізнавальних інтересів, уміння вести діалог та розвиток уміння працювати з великим об'ємом інформації.

Виховна мета: Виховання інформаційної культури учнів, що вчаться, уважності, акуратності, дисциплінованості, посидючості.

***Тип уроку*:** Комбінований урок

Структура уроку

I. Організаційний момент
II. Етап орієнтації
III. Етап проектування
IV. Етап навчальної діяльності
V. Робота за ПК
VI. Контрольно-оцінювальний етап
VII. Домашнє завдання

Хід уроку

I. Організаційний момент

Доброго ранку, діти! Хто сьогодні відсутній?

II. Етап орієнтації

Сьогодні ми будемо вивчати тему: «Комп'ютерні віруси. Призначення, принципи дії. Класифікація антивірусних програм. Практична робота № 5 «Захист комп'ютера від вірусів».»
Мета сьогоднішнього уроку якомога найкраще познайомитися навчитися працювати з ОС.

III. Етап проектування

1. Комп'ютерні віруси.
2. Призначення, принципи дії.
3. Класифікація антивірусних програм.
4. Практична робота № 5 «Захист комп'ютера від вірусів».
5. Підсумок уроку

IV. Етап навчальної діяльності

Комп'ютерні віруси. Історія та класифікація вірусів та троянських програм.

Вірус — де спеціально написана, як правило, невелика за розмірами програма, до може записувати (впроваджувати) свої копії (можливо, змінені) в інші комп'ютерні програми, системну область диска і т. д.

Признак класифікації вірусів	Опис
За об'єктами зараження	**Файлові** – заражують виконувані файли, а також допоміжні програми, що завантажуються при виконанні інших програм
	Завантажувальні – заражують сектор завантаження диска
	Макровіруси – заражують документи та об'єкти, що містять макроси
За зовнішнім виглядом	**Звичайні** – код вірусу можна побачити на диску
	Невидимі (Stealth-віруси) – використовують особливі засоби маскування, і при перегляді код вірусу не видно
	Поліморфні – код вірусу видозмінюється
За результатами діяльності	**Безпечні** – не виконують ніяких дій, окрім свого розповсюдження і видачі різних повідомлень або інших ефектів (перевантаження комп'ютера і т. д.)
	Небезпечні – призводять до втрати інформації і руйнування обчислювальної системи

Коли заражена програма починає свою роботу, то спочатку управління одержує вірус. Вірус знаходить і «заражує» інші програми або об'єкти, а також може сам виконати які-небудь шкідливі дії. Після цього вірус передає управління тій програмі, в якій він знаходиться, і зовні її робота має такий самий вигляд, як і робота незараженої.
Основна відмітна характеристика комп'ютерного вірусу - здатність до самопоширення. Подібно біологічному вірусу для життя й розмноження він активно використає зовнішнє середовище - пам'ять комп'ютера, операційну систему. Збільшення швидкості передачі інформації, обсягів і значимості оброблюваних в обчислювальних мережах даних відкриває перед вирусописателями усе більше широкі можливості - поширення по усім світі написаних програм займає лічені дні або навіть годинники. Сотні мегабайт оперативної пам'яті дозволяють виконувати практично будь-які дії непомітно від користувача. Спектр можливих цілей, таких як паролі, карткові рахунки, ресурси вилучених комп'ютерів представляє величезне поле для діяльності. Ускладнення операційних систем веде до появи всі нових дір, які можуть бути використані для проникнення на вилучений комп'ютер.
Оскільки відмінною рисою вірусів у традиційному змісті є здатність до розмноження в рамках одного комп'ютера, розподіл вірусів на типи відбувається у відповідності зі способами розмноження. Сам процес розмноження може бути умовно розділений на кілька стадій:

1. Проникнення на комп'ютер
2. Активація вірусу
3. Пошук об'єктів для зараження
4. Підготовка вірусних копій
5. Впровадження вірусних копій

Віруси проникають на комп'ютер разом із зараженими файлами або іншими об'єктами (завантажувальними секторами дискет), ніяк, на відміну від хробаків, не впливаючи на процес проникнення. Отже, можливості проникнення повністю визначаються можливостями зараження й класифікувати віруси по цих стадіях життєвого циклу окремо змісту немає.
Для активації вірусу необхідно, щоб заражений об'єкт одержав керування. На даній стадії розподіл вірусів відбувається по типах об'єктів, які можуть бути заражені:

1. Завантажувальні віруси - віруси, що заражають завантажувальні сектори постійних і змінних носіїв. Приклади. Шкідлива програма Virus.Boot.Snow.a записує свій код в MBR жорсткого диска або в завантажувальні сектори дискет. При цьому оригінальні завантажувальні сектори шифруються вірусом. Після одержання керування вірус залишається в пам'яті комп'ютера (резидентність) і перехоплює переривання INT 10h, 1Ch й 13h. Іноді вірус проявляє себе візуальним ефектом - на екрані комп'ютера починає падати сніг. Інший завантажувальний вірус Virus.Boot.DiskFiller також заражає MBR вінчестера або завантажувальні сектори дискет, залишається в пам'яті й перехоплює переривання - INT 13h, 1Ch й 21h. При цьому, заражаючи дискети, вірус форматує додаткову доріжку з номером 40 або 80 (залежно від обсягу дискети він може мати 40 або 80 доріжок з номерами 0-39 або 0-79 відповідно). Саме на цю нестандартну доріжку поза полем звичайної видимості вірус записує свій код, додаючи в завантажувальний сектор лише невеликий фрагмент - головну частину вірусу. При зараженні вінчестера Virus.Boot.DiskFiller розташовує свій код безпосередньо за MBR, а в самому MBR міняє посилання на активний завантажувальний сектор, указуючи адресу сектора де він розташований.

2.Файлові віруси -віруси, що заражають файли. Ця група додатково ділиться на три, залежно від середовища в якій виконується код: Властиво файлові віруси - ті, які безпосередньо працюють із ресурсами операційної системи. Приклади. Найвідоміший файловий вірус всіх часів і народів

- Virus.Win9x.CIH, відомий також як "Чорнобиль". Маючи невеликий розмір - близько 1 кб - вірус заражає PE-файли (Portable Executable) на комп'ютерах під керуванням операційних систем Windows 95/98 таким чином, що розмір заражених файлів не міняється. Для досягнення цього ефекту вірус шукає у файлах "порожні" ділянки, що виникають через вирівнювання початки кожної секції файлу під кратні значення байт. Після одержання керування вірус перехоплює IFS API, відслідковуючи виклики функції звертання до файлів і виконують заражання файлу. 26 квітня спрацьовує деструктивна функція вірусу, що полягає в стиранні Flash BIOS і початкових секторів жорстких дисків. Результатом є нездатність комп'ютера завантажуватися взагалі (у випадку успішної спроби стерти Flash BIOS) або втрата даних на всіх жорстких дисках комп'ютера. З останніх шкідливих програм, що володіють вірусною функціональністю, можна відзначити Email-Worm.Win32.Bagle.p (а також його модифікації .q й .r). Будучи в першу чергу хробаком з основним каналом поширення через електронну пошту, Bagle.p містить також функцію зараження EXE-файлів шляхом дописування в їхній кінець поліморфного коду вірусу. Макровіруси - віруси, написані мовою макрокоманд й, що виконують у середовищі якого-небудь додатка. У переважній більшості випадків мова йде про макроси в документах Microsoft Office. Приклади. Одними з найбільш руйнівних макровірусів є представники сімейства Macro.Word97.Thus. Ці віруси містять три процедури Document_Open, Document_Close й Document_New, якими підмінює стандартні макроси, що виконуються при відкритті, закритті й створенні документа, тим самим забезпечуючи зараження інших документів. 13 грудня спрацьовує деструктивна функція вірусу - він видаляє всі файли на диску C:, включаючи каталоги й підкаталоги. Модифікація Macro.Word97.Thus.aa крім зазначених дій при відкритті кожного зараженого документа вибирає на локальному диску випадковий файл і шифрує перші 32 байта цього файлу, поступово приводячи систему в непрацездатний стан. Макровіруси здатні заражати не тільки документи Microsoft Word й Excel. Існують шкідливі програми орієнтовані й на інші типи документів: Macro.Visio.Radiant заражає файли відомої програми для побудови діаграм -Visio, Virus.Acad.Pobresito - документи AutoCAD, Macro.AmiPro.Green - документи популярного раніше текстового процесора Ami Pro.

Скріпт-віруси - віруси, що виконують у середовищі певної командної оболонки: раніше - bat-файли в командній оболонці DOS, зараз частіше VBS й JS - скріпти в командній оболонці Windows Scripting Host (WSH). Приклади. Virus.VBS.Sling написаний мовою VBScript (Visual Basic Script). При запуску він шукає файли з розширеннями .VBS або .VBE і заражає їх. При настанні 16-го червня або липня вірус при запуску видаляє всі файли з розширеннями .VBS й .VBE, включаючи самого себе.

Virus.WinHLP.Pluma.a - вірус, що заражає файли допомоги Windows. При відкритті зараженого файлу допомоги виконується вірусний скрипт, що використовуючи нетривіальний метод (по суті, уразливість в обробці скріптів) запускає на виконання вже як звичайний файл Windows певний рядок коду, що міститься у скрипті. Запущений код робить пошук файлів довідки на диску й впроваджує в їхню область System скріпт автозапуску. Пошук жертв На стадії пошуку об'єктів для зараження зустрічається два способи поводження вірусів. 1. Одержавши керування, вірус робить разовий пошук жертв, після чого передає керування асоційованому з ним об'єкту (зараженому об'єкту). Приклад. Звичайно при освоєнні нової платформи спочатку з'являються віруси саме цього типу. Так було з появою вірусів під DOS, під Windows 9x, під Windows NT, під Linux. Наприклад, таким вірусом є Virus.Multi.Pelf.2132 - один з деяких представників мультиплатформових вірусів. Цей вірус здатний заражати як PE-файли, так і файли у форматі ELF (формат файлів, що виконують, під Linux). При запуску вірус робить у поточному (під обома операційними системами) і вищестоящих каталогах (під Windows) файлів форматів, що заражають, (PE й ELF), визначаючи дійсний формат файлу по його структурі. Після зараження знайдених файлів вірус завершує роботу й повертає керування запущеному файлу. 2. Одержавши керування, вірус так чи інакше залишається в пам'яті й робить пошук жертв безупинно, до завершення роботи середовища, у якій він виконується Приклад.

Virus.DOS.Anarchy.6093 також є мультиплатформенным у тому розумінні, що він здатний заражати DOS COM- і EXE-файли, а також документи Microsoft Word 6/7. При цьому вірус може активуватися при запуску як у середовищі DOS, так й у середовищі Windows 95. Після запуску вірус перехоплює переривання INT 21h, а в середовищі Windows додатково вносить зміни в драйвер VMM32.VXD (Virtual Memory Manager) з метою перехоплення звертань до файлів. При запуску або відкритті COM-, EXE й DOC -файлу вірус заражає його. Крім цього, у файловому варіанті вірус є поліморфним (див. нижче), і в будь-якому варіанті має stealth-функціональність (див. нижче) Віруси другого типу в часи однозадачной DOS було прийнято називати резидентними. З переходом на Windows проблема залишитися в пам'яті перестала бути актуальної: практично всі віруси, що виконують у середовищі Windows, так само як й у середовищі додатків MS Office, є вірусами другого типу. І навпроти, скрипт-вирусы є вірусами першого типу. Відповідно, атрибут резидентний застосуємо тільки до файлових DOS вірусам. Існування нерезидентних Windows вірусів можливо, але на практиці вони є рідкісним винятком. Окремо має сенс розглянути так називані stealth-віруси - віруси, які перебуваючи постійно в пам'яті, перехоплюють звертання до зараженого файлу й на ходу видаляють із нього вірусний код, передаючи у відповідь на запит незмінену версію файлу. У такий спосіб ці віруси маскують своя присутність у системі. Для їхнього виявлення антивірусним засобам потрібна можливість прямого звертання до диска в обхід засобів операційної системи. Найбільше поширення Stealth-віруси одержали в часи DOS.

Процес підготовки копій для поширення може істотно відрізнятися від простого копіювання. Автори найбільш складних у технологічному плані вірусів намагаються зробити різні копії максимально несхожими для ускладнення їхнього виявлення антивірусними засобами. Як наслідок, складання сигнатури для такого вірусу вкрай утруднене або зовсім неможливо. При створенні копій для маскування можуть застосовуватися наступні технології:

• Шифрування — вірус складається із двох функціональних шматків: властиво вірус і шифратор. Кожна копія вірусу складається із шифратора, випадкового ключа й властиво вірусу, зашифрованого цим ключем. • Метаморфізм — створення різних копій вірусу шляхом заміни блоків команд на еквівалентні, перестановки місцями шматків коду, вставки між значущими шматками коду "сміттєвих" команд, які практично нічого не роблять. Сполучення цих двох технологій приводить до появи наступних типів вірусів.

• Шифрований вірус - вірус, що використає просте шифрування з випадковим ключем і незмінний шифратор. Такі віруси легко виявляються по сигнатурі шифратора.

• Метаморфний вірус - вірус, що застосовує метаморфізм до всього свого тіла для створення нових копій.

• Поліморфний вірус - вірус, що використає метаморфний шифратор для шифрування основного тіла вірусу з випадковим ключем. При цьому частина інформації, використовуваної для одержання нових копій шифратора також може бути зашифрована. Наприклад, вірус може реалізовувати кілька алгоритмів шифрування й при створенні нової копії міняти не тільки команди шифратора, але й сам алгоритм. Поліморфні віруси можна ділити на класи за рівнем поліморфізму, що бажають докладніше познайомитися із цим питанням можуть знайти корисну інформацію в [1]. Пік популярності поліморфних вірусів довівся на часи DOS, проте, і пізніше поліморфізм використався в безлічі вірусів, продовжує використатися поліморфізм і сьогодні. Впровадження вірусних копій може здійснюватися двома принципово різними методами: • Впровадження вірусного коду безпосередньо в заражає об’єкт
• Заміна об'єкта на вірусну копію. Об'єкт, що заміщає, як правило, перейменовується Для вірусів характерним є переважно перший метод.

Другий метод набагато частіше використається хробаками й троянами, а точніше троянськими компонентами хробаків, оскільки трояни самі по собі не поширюються. Приклад. Один з деяких поштових хробаків, що поширюються по поштовій книзі The Bat! - Email-Worm.Win32.Stator.a, крім усього іншого заражає деякі файли Windows за принципом вірусу-компаньйона. Зокрема, до заражають файлам, що, ставляться: mplayer.exe, winhlp32.exe, notepad.exe, control.exe, scanregw.exe. При зараженні файли перейменовуються в розширення .VXD, а вірус створює свої копії під оригінальними іменами файлів, що заражають. Після одержання керування вірус запускає відповідний перейменований оригінальний файл. Як варіант другого методу, у часи DOS застосовувався наступний прийом. При наборі імені файлу, що виконує, без вказівки розширення, DOS шукає один по одному спершу BAT, потім COM, і зрештою EXE-файл. Відповідно, вірусна копія створювалася в одному каталозі з EXE-файлом, дублюючи його ім'я й приймаючи розширення COM. Таким чином, при спробі запустити даний EXE-файл без явної вказівки розширення спочатку запускався вірус. Аналогічний прийом може використатися й в Windows-системах, але оскільки основна маса користувачів Windows рідко користуються запуском файлів з командного рядка, ефективність цього методу буде низкою. Віруси – хробаки На жаль, визначення хробака відсутній у державних стандартах і розпорядницьких документах, тому тут наведено лише інтуїтивне визначення, що дає подання про принципи роботи й виконуваних функцій цього типу шкідливих програм.

Хробак (мережний хробак) — тип шкідливих програм, що поширюються по мережних каналах, здатних до автономного подолання систем захисту автоматизованих і комп'ютерних мереж, а також до створення й подальшого поширення своїх копій, що не завжди збігаються з оригіналом, і здійсненню іншого шкідливого впливу.
Так само як для вірусів, життєвий цикл хробаків можна розділити на певні стадії:
1. Проникнення в систему
2. Активація
3. Пошук "жертв"
4. Підготовка копій
5. Поширення копій

На етапі проникнення в систему чирви діляться переважно по типах використовуваних протоколів:
• Мережні хробаки - чирви, що використають для поширення протоколи Інтернет і локальні мережі. Звичайно цей тип хробаків поширюється з використанням неправильної обробки деякими додатками базових пакетів стека протоколів tcp/ip
• Поштові хробаки - чирви, що поширюються у форматі повідомлень електронної пошти
• IRC-хробаки - хробаки, що поширюються по каналах IRC (Internet Relay Chat)
• P2P-хробаки - чирви, що поширюються за допомогою пірінгових (peer-to-peer) файлообмінних мереж
• IM-хробаки - хробаки, що використають для поширення системи миттєвого обміну повідомленнями (IM, Instant Messenger - ICQ, MSN Messenger, AIM й ін.)

Троян (троянський кінь) — тип шкідливих програм, основною метою яких є шкідливий вплив стосовно комп'ютерної системи. Трояни відрізняються відсутністю механізму створення власних копій. Деякі трояни здатні до автономного подолання систем захисту КС, з метою проникнення й зараження системи. У загальному випадку, троян попадає в систему разом з вірусом або хробаком, у результаті необачних дій користувача або ж активних дій зловмисника.
У силу відсутності в троянів функцій розмноження й поширення, їхній життєвий цикл украй короткий - усього три стадії:
• Проникнення на комп'ютер
• Активація

• Виконання закладених функцій
Це, саме собою, не означає малого часу життя троянів. Навпроти, троян може тривалий час непомітно перебувати в пам'яті комп'ютера, ніяк не видаючи своєї присутності, доти, поки не буде виявлений антивірусними засобами. Способи проникнення Завдання проникнення на комп'ютер користувача трояни вирішують звичайно одним із двох наступних методів.
1.Маскування — троян видає себе за корисний додаток, що користувач самостійно завантажує з Інтернет і запускає. Іноді користувач виключається із цього процесу за рахунок розміщення на Web-сторінці спеціального скріпта, що використовуючи діри в браузері автоматично ініціює завантаження й запуск трояна. Приклад. Trojan.SymbOS.Hobble.a є архівом для операційної системи Symbian (SIS-архівом). При цьому він маскується під антивірус Symantec і має ім'я symantec.sis. Після запуску на смартфоні троян підмінює оригінальний файл оболонки FExplorer.app на ушкоджений файл. У результаті при наступному завантаженні операційної системи більшість функцій смартфона виявляються недоступними .

Одним з варіантів маскування може бути також впровадження зловмисником троянського коду в код іншого додатка. У цьому випадку розпізнати троян ще складніше, тому що заражений додаток може відкрито виконувати які-небудь корисні дії, але при цьому тайкома завдавати шкоди за рахунок троянських функцій. Розповсюджений також спосіб впровадження троянів на комп'ютери користувачів через веб-сайти. При цьому використається або шкідливий скріпт, що завантажує й запускає троянську програму на комп'ютері користувача, використовуючи уразливість у веб-браузері, або методи соціальної інженерії - наповнення й оформлення веб-сайту провокує користувача до самостійного завантаження трояна. При такому методі впровадження може використатися не одна копія трояна, а поліморфний генератор, що створює нову копію при кожнім завантаженні. Застосовувані в таких генераторах технології поліморфізму звичайно не відрізняються від вірусних поліморфних технологій.
Клавіатурні шпигуни - трояни, що постійно перебувають у пам'яті й дані, що зберігають всі, вступники від клавіатури з метою наступної передачі цих даних зловмисникові. Звичайно в такий спосіб зловмисник намагається довідатися паролі або іншу конфіденційну інформацію.
Викрадачі паролів - трояни, також призначені для одержання паролів, але не використають спостереження за клавіатурою. У таких троянах реалізовані способи добування паролів з файлів, у яких ці паролі зберігаються різними додатками. Приклад. Trojan-PSW.Win32.LdPinch.kw збирає відомості про систему, а також логіни й паролі для різних сервісів і прикладних програм - месенджерів, поштових клієнтів, програм дозвонуи. Часто ці дані виявляються слабко захищені, що дозволяє трояну їх одержати й відправити зловмисникові по електронній пошті. Утиліти вилученого керування - трояни, що забезпечують повний вилучений контроль над комп'ютером користувача. ' Існують легальні утиліти такої ж властивості, але вони відрізняються тим, що повідомляють про своє призначення при установці або ж постачені документацією, у якій описані їхні функції. Троянські утиліти вилученого керування, навпроти, ніяк не видають свого реального призначення, так що користувач і не підозрює про те, що його комп'ютер підконтрольний зловмисникові. Найбільш популярна утиліта вилученого керування - Back Orifice. Приклад. Backdoor.Win32.Netbus.170 надає повний контроль над комп'ютером користувача, включаючи виконання будь-яких файлових операцій, завантаження й запуск інших програм, одержання знімків екрана й т.д.

Люки (backdoor) - трояни які надають зловмисникові обмежений контроль над комп'ютером користувача. Від утиліт вилученого керування відрізняються більше простим пристроєм й, як наслідок, невеликою кількістю доступних дій. Проте, звичайно одними з дій є можливість завантаження й запуску будь-яких файлів по команді зловмисника, що дозволяє при необхідності перетворити обмежений контроль у повен. Приклад. Останнім часом backdoor-функціонал став характерною рисою хробаків. Наприклад, Email-Worm.Win32.Bagle.at

використає порт 81 для одержання вилучених команд або завантаження троянів, що розширюють функціонала хробака. Є й окремі трояни типу backdoor. Троян Backdoor.win32.Wootbot.gen використає IRC-канал для одержання команд від "хазяїна". По команді троян може завантажувати й запускати на виконання інші програми, сканувати інші комп'ютери на наявність вразливостей і встановлювати себе на комп'ютери через виявлені вразливості.

•Анонімні smtp-сервера й проксі - трояни, що виконують функції поштових серверів або проксі й, що використаються в першому випадку для спам-розсилань, а в другому для замітання слідів хакерами. Приклад. Трояни із сімейства Trojan-Proxy.Win32.Mitglieder поширюються з різними версіями хробаків Bagle. Троян запускається хробаком, відкриває на комп'ютері порт і відправляє авторові вірусу інформацію про IP-адресу зараженого комп'ютера. Після цього комп'ютер може використатися для розсилання спаму.

•Утиліти дозвону - порівняно новий тип троянів, що представляє собою утиліти dial-up доступу в Інтернет через дорогі поштові служби. Такі трояни прописуються в системі як утиліти дозвону за замовчуванням і спричиняють величезні рахунки за користування Інтернетом. Приклад. Trojan.Win32.Dialer.a при запуску здійснює дозвон в Інтернет через платні поштові служби. Ніяких інших дій не робить, у тому числі не створює ключів у реєстрі, тобто навіть не реєструється як стандартна програма дозвону й не забезпечує автозапуск.

•Модифікатори настроювань браузера - трояни, які міняють стартову сторінку в браузері, сторінку пошуку або ще які-небудь настроювання, відкривають додаткові вікна браузера, імітують натискання на банери й т.п. Приклад. Trojan-Clicker.JS.Pretty звичайно втримується в html-сторінках. Він відкриває додаткові вікна з певними веб-сторінками й обновляє їх із заданим інтервалом.

•Логічні бомби - частіше не стільки трояни, скільки троянські складових хробаків і вірусів, суть роботи яких полягає в тому, щоб за певних умов (дата, час доби, дії користувача, команда ззовні) зробити певну дію: наприклад, знищення даних. Приклад. Virus.Win9x.CIH, Macro.Word97.Thus Збиток від вірусів

Призначення, принципи дії, класифікація антивірусних програм.

Засоби захисту від вірусів поділяються на такі групи, як детектори, фаги, ревізори, охоронці, вакцини.

Детектори (сканери). Їх метою є постановка діагнозу, лікуванням буде займатися інша антивірусна програма або професійний програміст – “вірусолог”.

Фаги (поліфаги). Програми спроможні найти і знищити вірус (фаги) або декілька вірусів (поліфаги). Сучасні версії, як правило, проводять евристичний аналіз файлів – вони досліджують файли на предмет коду, характерного для віруса.

Ревізори. Цей тип антивірусів контролює всі (відомі на момент випуску програми) можливі способи зараження комп’ютерів. Таким чином, можливо знайти вірус, створений вже після виходу програми-ревізора.

Охоронці. Резидентні програми, постійно знаходяться в пам’яті комп’ютера і контролюють всі операції.

Вакцини. Використовуються для обробки файлів і завантажувальних секторів з метою попередження зараження відомими вірусами (в останній час цей метод використовується все частіше). Як відомо, ні один з даних типів антивірусів не забезпечує 100% захисту комп’ютера, і їх бажано використовувати в зв’язку з іншими пакетами. Вибір тільки одного, “найкращого” антивіруса вкрай помилковий.

Тепер про деякі характеристики антивірусних пакетів. Перше, на що треба звернути увагу, це

кількість розпізнаваючих сигнатур – послідовність символів, гарантовано виявляючих вірус. Треба помітити, що виробники використовують різні системи підрахунку сигнатур : якщо в одних різні версії або близькі по характеристиках версії вірусів рахуються за одну сигнатуру, то другі підраховують всі варіації. Найкращі із пакетів розпізнають біля 10 тисяч вірусів, що декілька менше загального числа існуючих сьогодні шкідливих програм. Другий параметр – наявність евристичного аналізатора невідомих вірусів, його присутність дуже корисна, але суттєво уповільнює час роботи програми.

Попробуємо розібратися з тими антивірусами, котрі зараз можна реально знайти на українському ринку або в INTERNET. Мова піде про комплексні антивірусні пакети, які забезпечують максимальний рівень захисту вашої інформації.

Серед російських розробників найбільш відомими є комплект від “ДіалогНауки” і AntiViral Toolkit Pro by Eugene Kaspersky від НТЦ КАМІ. Почнемо з продуктів “ДіалогНауки”, оскільки ці програми вже стали деяким стандартом, і подавляюча більшість комп’ютерів в нашій країні укомплектовано саме їх антивірусами.

Антивірусній комплект від “ДіалогНаука”

На початку 90-х достатньо було мати в себе цю програму і думати, що комп’ютер в повній безпеці : питання було лише в постійному її обновленні. Але часи змінюються, і тепер, крім Aidstest, не завадило б мати ще якісь програми.

Aidstest являється поліфагом. Це значить, що він може знаходити і знищювати відомі йому віруси. Програма розпізнає приблизно 2 тисячі вірусів. Поскільки він використовує сигнатурний пошук, то не може справлятися з поліморфними вірусами. Він не може також перевіряти упаковані файли і файли захищені вакциною, не має евристичного аналізу.

“ДіалогНаука” включає Aidstest в свій антивірусний комплект, як безкоштовний додаток.

Сильний антивірус з сильним алгоритмом знаходження вірусів. Він також, як і Aidstest, є поліфагом, однак, DrWEB може “читати” упаковані файли і архіви, файли даних в форматах Word і Excel, розброює поліморфні віруси, котрі в останній час, отримують все більше простору. Достатньо сказати, що епідемію дуже небезпечного віруса OneHalf зупинив саме DrWeb. Евристичний аналізатор DrWeb, досліджуючий програми в пошуці участків коду, характерних для вірусів, дозволяє знайти біля 90% невідомих вірусів. При завантаженні програми першим ділом DrWeb перевіряє самого себе на цілістність, після чого тестує ОЗП – в залежності від настройки, 640Kb або 1024Kb (включаючи HMA). Бажано перевіряти всю пам’ять – в цьому випадку процес перевірки триває більше, але справа в тому, що вже давно існують віруси спроможні завантажуватись в верхню пам’ять. Алгоритм роботи цього антивіруса заключається в тому, що він емулює процесор (створює програмну модель комп’ютера). Нові версії з’являються нечасто. По висновку останнього тестування журналом “Virus Bulletin” DrWeb вперше зайняв 3 місце серед 24 антивірусів.

Програма може працювати у діалоговому режимі, має дуже зручний інтерфейс, який можна настроювати.

Для запуску програми необхідно ввести у командний рядок DOS команду :

Диск :\ Шлях \ drweb.exe

Після натискання клавіші ENTER на екрані з’явиться головне вікно. У верхній частині вікна зображується меню: Dr.Web, Тест, Настройки, Дополнения, Помощь.

Призначення меню :

Dr.Web – використовується для отримання інформації про програму, тимчасового виходу в DOS та завершення роботи програми.

Тест – дозволяє запустити програму в режимі перевірки та лікування файлів.

Настройки – використовується для наладки інтерфейса програми та зміни режимів її роботи.
Дополнения – забезпечує підмикання зовнішніх файлів – баз даних, які мають інформацію про нові віруси.
Помощь – призначена для отримання довідкової інформації.
Режим пошуку вірусів вмикається вибором команди тестування в меню Тест, або натискуванням клавіші F5. При цьому на екрані над головним вікном з'являється діалогова панель Путь для тестирования. У рядку введення цієї панелі потрібно указати диск, каталог (каталоги) або групи файлів, де потрібно шукати віруси.
Тестування починається після натискування кнопки OK діалогової панелі. Для тестування з лікуванням потрібно натиснути Ctrl+F5.
(ADinf Cure Module)
Антивірус- ревізор диску (Advanced Diskinfoscope) дозволяє знайти, як звичайні, stealth – і поліморфні віруси, як вже відомі, так і зовсім свіжі. Антивірус має в своєму розпорядженні лікуючий блок ревізору Adinf – Adinf Cure Module – може знешкодити до 97% всіх вірусів. Цю цифру приводить "ДіалогНаука", виходячи з результатів тестування, котре відбувалося на колекціях вірусів двох визнаних авторитетів в цій області – Д.Н.Лозонського і фірми Dr.Solomon's (Великобританія). Adinf запускається автоматично з початку робочого дня і контролює завантажувальний сектор і файли на диску (Дата і час створення, довжина, контрольна сума), виводячи повідомлення про їх зміни. Дякуючи тому, що Adinf читає диск, обходячи ОС – напряму звертаючись до функцій BIOS, досягаються не тільки можливості знаходження активних stealth – вірусів на рівні перерви Int13h, але і висока швидкість перевірки диску, Adinf дозволяє робити перевірку під час завантаженні ОС, з HDD, а не тільки з дискет. Якщо вірус знайдений, то є два способи вирішення проблеми. Перший : якщо цей вірус завантажувальний, то Adinf просто відновить попередній завантажувальний сектор, котрий зберігається в його таблиці. Другий спосіб : якщо вірус є файловим, то тут вам на допомогу прийде лікуючий блок Adinf Cure Module. Метою його роботи є те, що ревізор Adinf передає модулю звіти про заражені файли, і той, зіставляє маючи в таблиці інформацію про старі характеристики файла з новими, відновлюючи старий стан файла, а не знищує тіло віруса, як це роблять поліфаги.
Цей антивірус по пулярності не набагато поступається комплекту від "ДіалогНаука". AVP являється поліфагом і в процесі роботи перевіряє ОЗП, файли, в тому числі упаковані і архівні, а також системні сектори (Master Boot Record), завантажувальний сектор (Boot – сектор) і Partition Table. На відміну від DrWeb і Aidstest, AVP розпізнає біля 10000 вірусів, серед них поліморфні, stealth – і макровіруси, а також "Троянські програми". Така різниця пояснюється тим, що "ДіалогНаука" незначні варіації одного вірусу приймає за одну сигнатуру, а КАМІ – різними вірусами. Програма має евристичний сканер, котрий, за затвердженням розробників антивіруса із КАМІ, знаходить біля 80% всіх вірусів. Нові бази антивірусів до AVP з'являються приблизно один раз в тиждень.
Нижче показуємо таблицю з результатами тестування по 14 антивірусних програмах.
Itw Boot Itw File Itw Over-all Standart Polymorphic Macro
Sophos Sweep 100% 100% 100% 99,7% 100% 100%
Dr Solomon's AVTK 100% 100% 100% 100% 98,4% 98,9%
DialogueScience DrWeb 94,4% 99,2% 97,2% 97,8% 100% 99,5%
EsaSS ThunderBYTE 100% 100% 100% 97,8% 93,5% 97,8%
IBM AntiVirus 100% 100% 100% 99,7% 92,3% 96,2%
McAfee VirusScan 100% 99,6% 99,7% 98,0% 90,1% 99,5%

ALWIL AVAST! 100% 99,3% 99,6% 100% 88,5% 95,8%
KAMI AVP 100% 99,7% 99,8% 94,4% 95,2% 90,3%
Norman Virus Control 100% 100% 100% 92,2% 87,4% 99,1%
EliaShim ViruSafe 95,6% 99,3% 97,9% 100% 88,5% 84,7%
Cybec VET 100% 81,0% 88,2% 88,9% 95,1% 97,3%
Iris AntiVirus 100% 99,7% 99,8% 99,0% 86,4% 82,7%
Cheyenne InnocuLAN 98,9% 98,0% 98,3% 99,3% 86,4% 82,2%
Symantec Norton AntiVirus 100% 99,7% 99,8% 84,4% 83,6% 94,3%

Профілактики зараження вірусами. Робота в середовищі антивірусної програми.

Ознаки появи вірусів

При зараженні комп'ютера вірусом важливо його знайти. Для цього треба знати про основні ознаки прояву вірусів. До них можна зарахувати такі:
— припинення роботи або неправильна робота програм, що раніше функціонували успішно;
— повільна робота комп'ютера;
— неможливість завантаження операційної системи;
— зникнення файлів і каталогів або перекручування їхнього вмісту;
— зміна дати і часу модифікації файлів;
— зміна розмірів файлів;
— несподіване значне збільшення кількості файлів на диску;
— істотне зменшення розміру вільної оперативної пам'яті;
— виведення на екран непередбачених повідомлень або зображень;
— подача непередбачених звукових сигналів;
— часті зависання і збої у роботі комп'ютера.
Слід зазначити, що перелічені вище явища необов'язково викликаються присутністю вірусу, а можуть бути наслідком інших причин. Тому правильна діагностика стану комп'ютера завжди утруднена.

Заходи щодо попередження зараження:

- використання надійних джерел програмного забезпечення;
- перевірка інформації, що надходить ззовні;
- установлення захисту від запису на знімних дисках з файлами;
- обмеження доступу до комп'ютера сторонніх осіб;
- регулярне створення резервних копій.

Отже, враховуючи все вищеописане, зрозуміло, що основними напрямками захисту від комп'ютерних вірусів є:
- запобігання надходженню вірусів;
- запобігання вірусній атаці, якщо вірус все-таки поступив на комп'ютер;
- запобігання руйнівним наслідкам, якщо атака все-таки сталася.

Виходячи з цього, можна виділити такі основні напрямки профілактики розповсюдження комп’ютерних вірусів:
1. Проведення регулярних апаратних заходів захисту інформації від розповсюдження комп’ютерних вірусів шляхом створення образу жорсткого диска на зовнішніх носіях (наприклад, на USB-, або DVD-дисках). Цей же засіб може захистити від втрати даних при апаратних збоях і при випадковому форматуванні жорсткого диска.
2. Проведення регулярних програмних методів захисту інформації шляхом встановлення антивірусних програм та сканування цією програмою жорстких дисків у пошуках комп'ютерних вірусів. Сканування звичайно виконується автоматично при увімкненні комп'ютера та при розміщенні зовнішнього диска в пристрої для читання. При скануванні потрібно мати на увазі, що антивірусна програма шукає вірус шляхом порівняння коду сканованої програми з кодами відомих їй вірусів, які зберігаються в базі даних. Якщо база даних застаріла, а вірус є новим,

скануюча програма його не виявить. Для надійної роботи потрібно регулярно оновлювати антивірусну програму. Бажана періодичність оновлення один раз на два тижні.
3. Контроль за зміною розмірів та інших атрибутів файлів. Комбіновані віруси на етапі розмноження змінюють параметри заражених файлів. Тому контролююча програма може виявити їх діяльність і попередити користувача.
4. Контроль за зверненнями до жорсткого диска тієї чи іншої програми. Оскільки найбільш небезпечні операції, пов'язані з роботою комп'ютерних вірусів, так чи інакше звернені на модифікацію даних, записаних на жорсткому диску, антивірусні програми чи так звані файрволи можуть контролювати звернення до нього і попереджати користувача про підозрілу активність.

V. Робота за ПК

Практична робота № 5

1. Запустити антивірусну програму
2. Обрати Сканувати ПК та вибрати всі локальні диски
3. Виконати сканування ПК
4. Очистити віруси, якщо такі маєте
5. Змінити ключ на антивірусну програму
6. Обновити антивірусну програму
7. Згорнути програму в трей

VI. Контрольно-оцінювальний етап

Вчитель оцінює роботу на уроці.

На наступному уроці нас чекає вивчення теми «Архіватори та операції з архівами. Запис на оптичні носії. Форматування та копіювання дисків. Практична робота № 6 «Архівування та розархівування даних».»

VII. Домашнє завдання

1. § 24.1 – 24.8 2. пит.. 2, 3,4,5,6 с. 270 3. Вивчити теорію