Міністерство освіти і науки, молоді та спорту України

Тернопільський національний педагогічний університет

імені Володимира Гнатюка

Кафедра інформатики

та методики її викладання

«Видалення вірусів без допомоги антивірусних програм»

Виконала

Студентка 1-го курсу

Крицька Г.В.

Науковий керівник:

Галан В. І.

Тернопіль – 2014

Зміст

[Вступ 3](#_Toc379489103)

[Розділ 1. Загальне поняття про віруси 4](#_Toc379489104)

[Розділ 2. Ознаки появи вірусів 5](#_Toc379489105)

[Розділ 3. Метод видалення вірусу 6](#_Toc379489106)

[Розділ 4. Практична частина 7](#_Toc379489107)

[Висновок 8](#_Toc379489108)

[Список використаних джерел: 9](#_Toc379489109)

Вступ

Комп'ютерні віруси. Що це таке і як з цим боротися? На цю тему написано десятки книг і сотні статей, боротьбою з комп'ютерними вірусами [професійно](http://ua-referat.com/%D0%9F%D1%80%D0%BE%D1%84%D0%B5%D1%81%D1%96%D1%8F) займаються сотні (або тисячі) фахівців в десятках (а може бути, сотнях) компаній. Здавалося б, тема ця не настільки складна і актуальна, щоб бути об'єктом такої пильної уваги. Однак це не так. Комп'ютерні віруси були і залишаються однією з найбільш поширених причин втрати інформації. Відомі випадки, коли віруси блокували роботу організацій і підприємств. Більше [того](http://ua-referat.com/%D0%A2%D0%BE%D0%B3%D0%BE), кілька років тому був зафіксований [випадок](http://ua-referat.com/%D0%92%D0%B8%D0%BF%D0%B0%D0%B4%D0%BE%D0%BA), коли комп'ютерний вірус став причиною загибелі людини - в одному з госпіталів [Нідерландів](http://ua-referat.com/%D0%9D%D1%96%D0%B4%D0%B5%D1%80%D0%BB%D0%B0%D0%BD%D0%B4%D0%B8) пацієнт отримав летальну дозу морфію з тієї причини, що комп'ютер був заражений вірусом і видавав невірну інформацію.

Незважаючи на величезні зусилля конкуруючих між собою антивірусних фірм, [збитки](http://ua-referat.com/%D0%97%D0%B1%D0%B8%D1%82%D0%BA%D0%B8), принесені комп'ютерними вірусами, не падають і досягають астрономічних величин в сотні мільйонів доларів щорічно. Ці оцінки явно занижені, оскільки відомо стає лише частину подібних інцидентів.

При цьому слід мати на увазі, що антивірусні програми і "залізо" не дають повної гарантії захисту від вірусів. Приблизно так само погано йдуть справи на іншій стороні тандему "людина-комп'ютер". Як користувачі, так і професіонали-програмісти часто не мають навіть навичок "самооборони", а їхні уявлення про вірус часом є настільки поверхневими, що краще б їх (подань) і не було.

Трохи краще йдуть справи у країнах, де і літератури побільше (видається аж три щомісячні журналу, присвячених вірусам і захист від них), і вірусів менше (оскільки "ліві" китайські ком пакт-диски особливо на ринок не надходять), і антивірусні компанії ведуть себе активніше (проводячи, наприклад, спеціальні конференції та семінари для фахівців і користувачів).

У нас же, на жаль, все це не зовсім так. І одним з найменш "опрацьованих" пунктів є література, присвячена проблемам боротьби з вірусами. На сьогоднішній день що є в продажу друкована продукція антивірусного штибу або давно застаріла, або написана непрофесіоналами, або авторами типу Хижняка, що набагато гірше.

Досить неприємним моментом є й випереджальна робота Російського комп'ютерного "андеграунду": тільки за два роки було випущено більше десятка електронних номерів журналу вірусописьменників "Infected Voice", з'явилося кілька станцій BBS і WWW-сторінок, орієнтовані на поширення вірусів та супутньої інформації.

Розділ 1. Загальне поняття про віруси

Комп’ютерний вірус – спеціально написана невелика за розміром програма (тобто деяка сукупність виконуваного коду, призначена для заподіяння руйнівних дій ). Вона може «приписувати» себе до інших програм («заражати» їх ), створювати свої копії і вбудовувати їх у файли, системну ділянку комп’ютера тощо,а також виконувати різноманітні небажані дії.

Комп’ютерні віруси класифікуються на :

1. Мережні які поширюються комп’ютерними мережами.

2. Файлові які вбудовуються у виконувані файли (найбільш поширений тип вірусів), або створюють файли – двійники (компаньйон – віруси ), або використовують особливості організації файлової системи (link віруси )

3. Завантажувальні які записують себе або в завантажувальний сектор диска (bootсектор),або сектор, який містить системний завантажник вінчестера (Master Boot Record ), або змінюють покажчик на активний bootсектор

4. Файлово – завантажувальні які завантажують як файли, так і завантажувальні сектори дисків

5. Резидентний вірус який у разі інфікування комп’ютер залишає в оперативній пам’яті свою резидентну частину, що потім перехоплює обертання ОС до об’єктів зараження і вбудовується в них. Цей вид віруса міститься в пам’яті і є активним аж до вимикання комп’ютера або перезавантаження ОС

6. Нерезедентний вірус який зберігає свою активність обмежений час

7. Безпечні віруси яких вплив обмежується зменшенням вільної пам’яті на диску та графічними, звуковими й іншими ефектами

8. Небезпечні які можуть призвести до серйозних збоїв у роботі комп’ютера

9. Дуже небезпечні в яких в алгоритм роботи явно закладено дії, що можуть спричинити втрату програм, знищити дані тощо

10. Найпростіші віруси (паразитичні) які змінюють уміст файлів і секторів диска ; їх можна достатньо легко виявити і знищити

11. Віруси – реплікатори так звані хробаки, що поширюються комп’ютерними мережами

12. Віруси невидимки – стелсвіруси які перехоплюють обертання ОС до уражених файлів і секторів дисків та підставляють замість свого тіла незаражені ділянки диска

13. Віруси мутанти які містять алгоритм шифрування – розшифрування

14. Квазивірусні, або «троянські програми» які неспроможні до само розповсюдження, проте дуже небезпечні, оскільки, маскируючись під корисну програму, руйнують завантажувальний сектор і файлову систему дисків

Розділ 2. 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.

Розділ 3. Метод видалення вірусу

Для початку потрібно завантажити антивірус Касперського або NOD32, щоб провести глибоку перевірку жорсткого диска на наявність шкідливих програм. Бажано проводити процедуру в безпечному режимі, але попередньо використовувати процедуру: завантаження останньої успішної конфігурації. Швидше за все, це не вірус вивів з ладу комп’ютер, а простий збій в системі. Але не всі знають, як увійти в безпечний режим, це дуже просто: під час запуску комп’ютера натисніть на F8, з’явиться меню, де можна вибрати даний режим. Цей режим запускає роботу WINDOWS без основних програм і драйверів, що гарантує повну перевірку на віруси в стислі терміни. Проблема полягає в тому, що антивіруси не перевіряють багато файлів, які задіяні в роботі (програми). Нерідко перевірка не виявляє вірус, тому потрібно завантажити утиліту Dr webCureit, яка знаходиться у вільному доступі. Знову проведіть глибоку перевірку, на цей раз, швидше за все, віруси будуть виявлені. Далі потрібно провести очищення автоматичного завантаження, зайдіть в пуск і виберіть вкладку «виконати», потім наберіть слово «msconfig». З’явиться налаштування системи, зайдіть у розділ «автозавантаження». Галочкою будуть відзначені об’єкти, які могли бути заражені. У більшості випадків зараженими виявляються такі елементи:

C: WINDOWSINF \*. Exe /% windir% system328353.exe;

C: WINDOWSsecuritysmss.exe /% windir% system32smphost.exe.

Це показує завантаження шкідливого об’єкта. Перевірте, чи дійсно ви встановлювали дані програми? Якщо немає — приберіть з них галочки. Найбільш небезпечний вірус під назвою svchost.exe, тому що він має властивість шифровки під всілякі служби вашого комп’ютера. У диспетчері завдань таких служб близько шести, тому видаліть цей файл в режимі автозавантаження, якщо він відображається. Пам’ятайте, що svchost.exe не повинен відображатися в автозавантаженні ні в якому разі.

Далі потрібно очистити інші об’єкти. Найчастіше шкідливі програми потрапляють в папку, де зберігаються файли для відновлення WINDOWS. Зрозуміло, всю папку доведеться видалити. Очистіть папку під назвою temp і всі тимчасові файли з мережі інтернет. Щоб провести всю роботу максимально швидко, скористайтеся програмою Ccleaner.

Розділ 4. Практична частина

Отже, проблема нашої команди полягала в тому, щоб очистити комп’ютер від всіх вірусів, що на ньому знаходились.

В першу чергу ми встановили антивірус Avast та запустили сканування жорсткого диску. Вірусні програми досить обтяжували роботу сканера, через що доводилось періодично перезавантажувати систему.

Тоді ви вирішили використати наступні антивірусні програми

які дали позитивні результати.

Під час першого сканування програмою Kaspersky Antivirus ми знайшли та видалили вірус Trojan remover.Win32.

Після видалення цього вірусу робота пішла краще.

Висновок

Отже, в даній роботі я розглянула питання про видалення вірусу у випадку, коли немає можливості зробити це за допомогою антивірусної програми.

З проблемою необхідності видалення комп'ютерних вірусів рано чи пізно стикалося більшість користувачів. На помилках вчаться, і сьогодні люди вважають за краще встановлювати антивірус завчасно, замість того, щоб боротися з наслідками зараження комп'ютера. Запобігти зараженню, безумовно, простіше, ніж видаляти вірус і усувати наслідки його діяльності, але що робити, якщо вірус вже потрапив до вас в комп'ютер?
Перше і головне правило - не піддаватися паніці і не робити необдуманих дій. Багато вірусів можна видалити навіть без використання антивірусних програм (наприклад, autorun.inf на флешці). Ми розглянемо найчастіші види заражень комп'ютера і дізнаємося, як видалити вірус у кожному конкретному випадку.
Видалення комп'ютерних вірусів найчастіше зводиться до установки на заражений комп'ютер програми для видалення вірусів (або антивірусної програми), повного сканування системи і процедури лікування комп'ютерних вірусів. Анотація

У цьому рефераті я використала такі поняття як вірус та ознаки вірусів .

#  Анотація

У цьому рефераті я використала такі поняття як вірус та ознаки вірусів .

Також тут детально розглянуто найпоширеніший та найбільш поширений метод видалення вірусів.

# Ключові слова

Комп’ютерний вірус, антивірус Касперського , NOD32, Trojan remover.Win32, Ccleaner.

Список використаних джерел:

Інформатика: Навчальний посібник для 10-11 кл. Зарецька І.Т. Колодяжний Б.Г

Журнал “Компьютерное обозрение” №35(108) за 10 жовтня 1997 рік.

Тхір І.Л, Галушка ВП. Юзьків А.В.Посібник користувача ПК.

<http://www.kurs-pk.com/windows/virus/virus1.html>

[http://yak-prosto.com/yak-vidaliti-virus-vruchnu/](http://vk.com/away.php?to=http%3A%2F%2Fyak-prosto.com%2Fyak-vidaliti-virus-vruchnu%2F)

[http://www.callgenius.com.ua/resursi/119-vidalennya-v..](http://vk.com/away.php?to=http%3A%2F%2Fwww.callgenius.com.ua%2Fresursi%2F119-vidalennya-virusiv)