Міністерство освіти і науки, молоді та спорту України

Тернопільський національний педагогічний університет  
імені Володимира Гнатюка

Кафедра інформатики та

методики її викладання

Реферат на тему:  
 «Форматування диска та відновлення інформації з резервних копій»

Виконала:

Стирчак Ю.Р.

Науковий керівник:

Галан В.І.

Тернопіль 2014

[Вступ](#_Toc379470039) 4

[Розділ 1 Комп’ютерні віруси](#_Toc379470040) 5

[Коротко про комп'ютерний вірус . 3](#_Toc379470041)

[Ознаки зараження вірусами: 3](#_Toc379470042)

[Розділ 2 Практичне вирішення проблеми 5](#_Toc379470043)

[Форматування жорсткого диску для видалення вірусів. 5](#_Toc379470044)

[Відновлення 6](#_Toc379470045)

[Образ системи](#_Toc379470046) 8

[Висновок](#_Toc379470047) 11

[Список використаних джерел: 12](#_Toc379470048)

**Анотація**

В даній роботі розповідається про проблеми комп'ютерних вірусів та способи їх вирішення. Є багато способів вберегти ПК від зараження такі як: встановлення антивірусних програм, часте сканування комп'ютера, і як останній варіант сканування комп'ютера зробивши резервне копіювання файлів.В роботі коротко описано про комп'ютені віруси,їх типи, а також способи їх видалення. Детальніше ж описано останній метод-форматування жорсткого диску при резервному копіюванні файлів.

Ключові слова:

Комп’ютерний вірус, форматування, жорсткий диск, DOS, контрольна точка відновлення, резервні копії, образ системи, BIOS.

Вступ

Комп'ютери стали справжніми [помічниками](http://ua-referat.com/%D0%9F%D0%BE%D0%BC%D1%96%D1%87%D0%BD%D0%B8%D0%BA%D0%B8) людини і без них вже не може обійтися ні комерційна [фірма](http://ua-referat.com/%D0%A4%D1%96%D1%80%D0%BC%D0%B0), ні [державна](http://ua-referat.com/%D0%94%D0%B5%D1%80%D0%B6%D0%B0%D0%B2%D0%B0) організація. Однак у зв'язку з цим особливо загострилася проблема захисту інформації. [Віруси](http://ua-referat.com/%D0%92%D1%96%D1%80%D1%83%D1%81%D0%B8), що набули широкого поширення в комп'ютерній техніці, розбурхали весь світ. Багато користувачів комп'ютерів стурбовані чутками про те, що за допомогою комп'ютерних вірусів [зловмисники](http://ua-referat.com/%D0%97%D0%BB%D0%BE%D0%B2%D0%BC%D0%B8%D1%81%D0%BD%D0%B8%D0%BA%D0%B8) зламують [мережі](http://ua-referat.com/%D0%9C%D0%B5%D1%80%D0%B5%D0%B6%D1%96), грабують [банки](http://ua-referat.com/%D0%91%D0%B0%D0%BD%D0%BA%D0%B8), крадуть інтелектуальну власність. Сьогодні масове застосування [персональних](http://ua-referat.com/%D0%9F%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB_21) комп'ютерів, на жаль, виявилося пов'язаним з появою самовідтворюються програм-вірусів, що перешкоджають нормальній роботі комп'ютера, руйнують файлову структуру дисків і завдають шкоди зберiгається в комп'ютері інформації. Все частіше в засобах масової інформації з'являються повідомлення про різного роду піратських витівках комп'ютерних хуліганів, про появу все більш досконалих, саморозмножуються програм. Незважаючи на прийняті в багатьох [країнах](http://ua-referat.com/%D0%9A%D1%80%D0%B0%D1%97%D0%BD%D0%B0) закони про боротьбу з комп'ютерними злочинами і розробку спеціальних програмних засобів захисту від вірусів, кількість нових програмних вірусів постійно росте. Це вимагає від користувача персонального комп'ютера знань про природу вірусів, способи зараження вірусами і захисту від них.

**Розділ 1**

**Комп’ютерні віруси**

Комп'ютерний вірус ([англ.](http://uk.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0_%D0%BC%D0%BE%D0%B2%D0%B0" \o "Англійська мова)*computer virus*)—комп'ютерна програма, яка має здатність до прихованого саморозмноження. Нині відомі десятки тисяч комп'ютерних вірусів, які поширюються через мережу Інтернет по всьому світу. Необізнані користувачі ПК помилково відносять до комп'ютерних вірусів також інші види.

Не існує єдиної системи класифікації та іменування вірусів (хоча спроба створити стандарт була зроблена на зустрічі CARO в 1991 році).

Прийнято розділяти віруси за:

* об'єктами, які вражаються ([файлові віруси](http://uk.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB%D0%BE%D0%B2%D0%B8%D0%B9_%D0%B2%D1%96%D1%80%D1%83%D1%81), [завантажувальні віруси](http://uk.wikipedia.org/wiki/%D0%91%D1%83%D1%82%D0%BE%D0%B2%D0%B8%D0%B9_%D0%B2%D1%96%D1%80%D1%83%D1%81), [анти-антивірусні віруси](http://uk.wikipedia.org/wiki/%D0%A0%D0%B5%D1%82%D1%80%D0%BE%D0%B2%D1%96%D1%80%D1%83%D1%81), [скриптові віруси](http://uk.wikipedia.org/wiki/%D0%A1%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B2%D0%B8%D0%B9_%D0%B2%D1%96%D1%80%D1%83%D1%81), [макро-віруси](http://uk.wikipedia.org/wiki/%D0%9C%D0%B0%D0%BA%D1%80%D0%BE-%D0%B2%D1%96%D1%80%D1%83%D1%81), [мережеві черв'яки](http://uk.wikipedia.org/wiki/%D0%9C%D0%B5%D1%80%D0%B5%D0%B6%D0%B5%D0%B2%D0%B8%D0%B9_%D1%87%D0%B5%D1%80%D0%B2%27%D1%8F%D0%BA)).
* способом зараження ([перезаписуючі віруси](http://uk.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D0%B5%D0%B7%D0%B0%D0%BF%D0%B8%D1%81%D1%83%D1%8E%D1%87%D0%B8%D0%B9_%D0%B2%D1%96%D1%80%D1%83%D1%81" \o "Перезаписуючий вірус), [віруси-компаньйони](http://uk.wikipedia.org/w/index.php?title=%D0%92%D1%96%D1%80%D1%83%D1%81-%D0%BA%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D1%8C%D0%B9%D0%BE%D0%BD&action=edit&redlink=1), [файлові хробаки](http://uk.wikipedia.org/w/index.php?title=%D0%A4%D0%B0%D0%B9%D0%BB%D0%BE%D0%B2%D0%B8%D0%B9_%D1%85%D1%80%D0%BE%D0%B1%D0%B0%D0%BA&action=edit&redlink=1), [віруси-ланки](http://uk.wikipedia.org/w/index.php?title=%D0%92%D1%96%D1%80%D1%83%D1%81-%D0%BB%D0%B0%D0%BD%D0%BA%D0%B0&action=edit&redlink=1), [паразитичні віруси](http://uk.wikipedia.org/w/index.php?title=%D0%9F%D0%B0%D1%80%D0%B0%D0%B7%D0%B8%D1%82%D0%B8%D1%87%D0%BD%D0%B8%D0%B9_%D0%B2%D1%96%D1%80%D1%83%D1%81&action=edit&redlink=1), [віруси, що вражають вихідний код программ](http://uk.wikipedia.org/w/index.php?title=%D0%92%D1%96%D1%80%D1%83%D1%81,_%D1%89%D0%BE_%D0%B2%D1%80%D0%B0%D0%B6%D0%B0%D1%94_%D0%B2%D0%B8%D1%85%D1%96%D0%B4%D0%BD%D0%B8%D0%B9_%D0%BA%D0%BE%D0%B4_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC&action=edit&redlink=1))
* операційними системами і платформами, які вражаються ([DOS](http://uk.wikipedia.org/wiki/DOS), [Microsoft Windows](http://uk.wikipedia.org/wiki/Microsoft_Windows), [Unix](http://uk.wikipedia.org/wiki/Unix), [Linux](http://uk.wikipedia.org/wiki/Linux), інші)
* активністю ([резидентні віруси](http://uk.wikipedia.org/w/index.php?title=%D0%A0%D0%B5%D0%B7%D0%B8%D0%B4%D0%B5%D0%BD%D1%82%D0%BD%D0%B8%D0%B9_%D0%B2%D1%96%D1%80%D1%83%D1%81&action=edit&redlink=1), [нерезидентні віруси](http://uk.wikipedia.org/w/index.php?title=%D0%9D%D0%B5%D1%80%D0%B5%D0%B7%D0%B8%D0%B4%D0%B5%D0%BD%D1%82%D0%BD%D0%B8%D0%B9_%D0%B2%D1%96%D1%80%D1%83%D1%81&action=edit&redlink=1))
* технологіями, які використовуються вірусом (нешифровані/шифровані віруси, поліморфні віруси, стелс-віруси ([руткіт](http://uk.wikipedia.org/wiki/%D0%A0%D1%83%D1%82%D0%BA%D1%96%D1%82" \o "Руткіт) і [буткіт](http://uk.wikipedia.org/wiki/%D0%91%D1%83%D1%82%D0%BA%D1%96%D1%82)))
* деструктивними можливостями ([нешкідливі віруси](http://uk.wikipedia.org/w/index.php?title=%D0%9D%D0%B5%D1%88%D0%BA%D1%96%D0%B4%D0%BB%D0%B8%D0%B2%D0%B8%D0%B9_%D0%B2%D1%96%D1%80%D1%83%D1%81&action=edit&redlink=1), [безпечні віруси](http://uk.wikipedia.org/w/index.php?title=%D0%91%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%BD%D0%B8%D0%B9_%D0%B2%D1%96%D1%80%D1%83%D1%81&action=edit&redlink=1), [небезпечні віруси](http://uk.wikipedia.org/w/index.php?title=%D0%9D%D0%B5%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%BD%D0%B8%D0%B9_%D0%B2%D1%96%D1%80%D1%83%D1%81&action=edit&redlink=1), [дуже небезпечні віруси](http://uk.wikipedia.org/w/index.php?title=%D0%94%D1%83%D0%B6%D0%B5_%D0%BD%D0%B5%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%BD%D0%B8%D0%B9_%D0%B2%D1%96%D1%80%D1%83%D1%81&action=edit&redlink=1))
  + мовою, якою написаний вірус ([асемблер](http://uk.wikipedia.org/wiki/%D0%90%D1%81%D0%B5%D0%BC%D0%B1%D0%BB%D0%B5%D1%80), [високорівнева мова програмування](http://uk.wikipedia.org/w/index.php?title=%D0%92%D0%B8%D1%81%D0%BE%D0%BA%D0%BE%D1%80%D1%96%D0%B2%D0%BD%D0%B5%D0%B2%D0%B0_%D0%BC%D0%BE%D0%B2%D0%B0_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F&action=edit&redlink=1), [скриптова мова](http://uk.wikipedia.org/wiki/%D0%A1%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B2%D0%B0_%D0%BC%D0%BE%D0%B2%D0%B0), інші).

**Ознаки зараження вірусами**:

1. Зменшення вільної пам'яті
2. Уповільнення роботи комп'ютера
3. Затримки при виконанні програм
4. Незрозумілі зміни в файлах
5. Зміна дати модифікації файлів без причини
6. Незрозумілі помилки Write-protection
7. Помилки при інсталяції і запуску Windows
8. Відключення 32-розрядного допуску до диску
9. Неспроможність зберігати документи Word в інші каталоги, крім Template
10. Погана робота дисків
11. Файли невідомого походження

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

1. Зникнення файлів
2. Форматування [HDD](http://uk.wikipedia.org/wiki/HDD)
3. Неспроможність завантажити комп'ютер
4. Неспроможність завантажити файли
5. Незрозумілі системні повідомлення, звукові ефекти

Здебільшого, все це в минулому. Зараз основні ознаки—самовільне відкривання браузером деяких сайтів (рекламного характеру), підозріло підвищений інтернет-трафік та повідомлення від друзів, що ваші листи електронної пошти до них містили вірус.



**Розділ 2**

**Практичне вирішення проблеми**

Практична частина почалася з того,що увімкнувши комп’ютер далися у знаки всі віруси. Їх було надто багато. Перш за все ми встановили антивірусну програму Avast, яка змогла знайти але не змогла знешкодити деякі віруси. Більшість наступних програм не запускалися взагалі. Після цього ми запустили Doctor Web у безпечному режимі. Таким чином більшість вірусів були знешкодженні. Та був ще і запасний варіант.

**Форматування жорсткого диску для видалення вірусів.**

Очистити диск в Microsoft Windows досить легко: треба зайти в папку Мій комп’ютер, клікнувши правою кнопкою миші по назві томи, викликати контекстне меню, в якому вибрати останній пункт—Властивості. Думаю, багато хто вже здогадуються, як форматувати жорсткий диск Windows: знадобиться всього лише натиснути на кнопку Очистка диска, щоб почати її. Те ж можна зробити через консоль командою format. У папці Службові програми даної операційної системи знаходиться Дискова утиліта—програма-диспетчер для роботи з вінчестером. Її необхідно запустити, і в який з’явився в лівій частині вікна списку вибрати потрібний тому чи диск. Зробивши це, від користувача вимагається натиснути кнопку Стерти. Знову ж, таким методом неможливо очистити той розділ, на якому знаходиться власне система. Тут знову доведеться вдаватися до допомоги CD або DVD-дисків.

Є деякі нюанси, що стосуються того як відформатувати жорсткий диск через DOS, основний серед яких—потреба у володінні командами даної системи. Другий момент — MS-DOS не «бачить» томів, записаних у форматі NTFS. Взагалі, користуватися DOS зручніше з завантажувального диска, ніж встановлювати її на жорсткий. При необхідності, диск з нею можна вставити в дисковод, попередньо виставивши в BIOS завантаження з зовнішнього носія. Функціонал DOS нітрохи не поступається сучасним системам: повністю відформатувати диск або його розділ можна однією командою format, що має кілька параметрів.

**Відновлення**

Відновлення—це процес відновлення комп’ютера до заводських параметрів. Відновлення системи дає змогу повернути системні файли комп’ютера до попереднього стану. У такий спосіб можна скасувати зміни, внесені до комп’ютера, не впливаючи на особисті файли, наприклад електронну пошту, документи або фотографії.

Іноді інсталяція програми або драйвера може спричинити неочікувані зміни в системі комп’ютера або привести до непередбачуваної поведінки Windows. Зазвичай видалення програми або драйвера виправляє помилку. Якщо після видалення помилка залишилася, можна спробувати відновити систему комп’ютера до попереднього стану, коли все працювало належним чином.

Існує два способи відновити систему комп’ютера:

❑з носія для відновлення;

❑з розділу відновлення.Коли потрібно виконувати відновлення?

❑Якщо комп’ютер працює нестабільно.

❑Якщо комп’ютер інфіковано вірусом.

❑Якщо в комп’ютері виникли проблеми, які не вдається вирішити шляхом виправлення несправностей.

❑Якщо диск C: на комп’ютері помилково відформатовано.

**Створення контрольної точки відновлення**

Контрольна точка відновлення - це відображення збереженого стану системних файлів комп’ютера. Контрольну точку відновлення можна використовувати для відновлення системних файлів комп’ютера до попереднього стану. Засіб відновленням системи автоматично створює контрольні точки відновлення щотижня та тоді, коли засіб виявляє початок внесення змін у комп’ютер, наприклад інсталяцію програми або драйвера. Резервні копії образу системи, які зберігаються на жорстких дисках, також можна використовувати для відновлення системи, так само як контрольні точки відновлення, створені функцією захисту системи. Навіть якщо резервні копії образу системи містять системні файли й особисті відомості, відновлення системи не вплине на файли даних.

* Створення контрольної точки відновлення
* Щоб відкрити вікно "Система", натисніть кнопку **Пуск**Зображення кнопки «Пуск», клацніть правою кнопкою миші **Комп’ютер**, а потім–**Властивості**.
* В області ліворуч клацніть **Захист системи**.Потрібен дозвіл адміністратораЯкщо буде запропоновано ввести пароль адміністратора або підтвердити видалення, введіть пароль або надайте підтвердження.
* Виберіть вкладку **Захист системи**, а потім клацніть **Створити**.
* У діалоговому вікні **Захист системи** введіть опис і клацніть **Створити**.

**Образ системи**

Образ системи-це точна копія диска. За промовчанням образ системи включає диски, необхідні для запуску Windows. Він також містить файли, програми та настройки системи Windows, а також ваші файли, програми та настройки. Образ системи можна використати, щоб відновити вміст комп’ютера, якщо жорсткий диск чи комп’ютер вийде з ладу. Відновлення комп’ютера з образу системи–це повне відновлення; не можна вибрати окремі елементи для відновлення, і всі поточні файли, програми та настройки системи замінюються вмістом образу системи.

Хоча цей тип резервного копіювання містить особисті файли, рекомендуємо періодично створювати резервні копії файлів за допомогою архівації Windows, щоб у разі потреби можна було відновити окремі файли та папки. Під час настроювання архівації Windows можна дозволити Windows вибирати елементи, резервну копію яких потрібно створити, разом з образом системи, або ви можете вибрати елементи, резервну копію яких потрібно створити, а також вказати, чи слід включати образ системи.

Відновлення даних за допомогою контрольної точки відновлення

Точка відновлення дає змогу відновити системні файли комп’ютера до попереднього стану, за якого було створено цю контрольну точку. Зазвичай точка відновлення створюється автоматично, наприклад у разі інсталювання драйвера програмного забезпечення. Але рекомендовано створювати точку відновлення вручну у вікні панель керування перед інсталюванням програмного забезпечення або драйверів на комп’ютер.

Висновок

В даній роботі я розглянула випадок зараження комп’ютера вірусам і способи вирішення цієї проблеми, так як це актуально в теперішній час. Одним із способів було форматування жорсткого диску та відновлення інформації з резервних копій. У своїй роботі я дослідила загальні поняття про комп’ютерні віруси, принципи їх класифікації, процес загального копіювання, контрольні точки відновлення. Та запасний варіант-форматування жорсткого диску при збереженні всіх даних використовувати не прийшлося, так як на допомогу прийшли антивірусні програми.

Список використаних джерел:

<http://windows.microsoft.com/uk-ua/windows/what-is-system-restore#1TC=windows-7>

<http://windows.microsoft.com/uk-ua/windows7/what-is-a-system-image>

Посібник з відновлення системи резервного копіювання та виправлення несправностей

<http://download.sony-europe.com/pub/manuals/RecoTS/2011Q1_TRG_UA.pdf>

<http://a-yak.com/yak-vidformatuvati-zhorstkij-disk/>