Міністерство освіти і науки, молоді та спорту України

Тернопільський національний педагогічний університет

імені Володимира Гнатюка

Кафедра інформатики та методики її викладання

Профілактика та лікування. Антивіруси

Виконала: Гайда Наталія

Миронівна

Науковий керівник: Вельгач Андрій Володимирович

Тернопіль – 2014

ВСТУП

В даний час комп'ютер міцно увійшов у повсякденне життя. Його можливості використовуються на роботі, при проведенні дозвілля, в побуті та інших сферах життя людини. Кількість інформації, яку люди довіряють своєму «електронному другові», з кожним днем зростає, тому рано чи пізно кожен задається питанням: «Як забезпечити надійне збереження даних?»

Сьогодні неможливо зустріти користувача персонального комп'ютера, який не чув би про комп'ютерні віруси. В Інтернеті такі шкідливі програми існують у величезній кількості. Найнеприємніше, що багато розповсюджувачі вірусів успішно застосовують у своїй практиці передові досягнення IT-індустрії. У результаті те, що має служити на благо користувачів, в кінцевому підсумку може обернутися для них великими проблемами.

**Актуальність роботи** полягає в тому що, шляхів поширення вірусів існує безліч. Вірус може потрапити на комп'ютер користувача разом з дискетою, піратським компакт-диском або з повідомленням електронної пошти. Щоб не стати жертвою цієї напасті, кожному користувачеві слід добре знати принципи захисту від комп'ютерних вірусів. Адже немає ніякої надії на те, що з приходом нового тисячоліття віруси зникнуть.

З давніх часів відомо, що до будь-якої отрути рано чи пізно можна знайти протиотруту. Такою протиотрутою у комп'ютерному світі стали програми, які називаються антивірусними. Тому на будь-якому сучасному комп'ютері повинна бути обов'язково встановлена антивірусна програма.

**Об'єктом мого дослідження,** є комп'ютер, заражений вірусом. Оскільки проблему, коли комп'ютер працює, але заражений вірусами можна вирішити завантаживши антивірусне програмне забезпечення, тому я досліджувала ще й сучасні антивірусні програми.

 **Предметом мого дослідження** є проблема вибору та методика використання антивірусної програми.

**Метою** моєї наукової роботи є опис функціонування зараженого вірусами комп'ютера та підбір антивірусних програм, принципів їх роботи, переваги і недоліки. Також описати, яким чином і з якого боку будь-який користувач комп'ютера можуть очікувати неприємності, пов'язані з різними комп'ютерними вірусами. Більше того, я постараюся найбільш повно і зрозуміло розповісти про найбільш розповсюджений способи захисту інформації.

КРИТЕРІЇ АНТИВІРУСНИХ СИСТЕМ

Стабільність і надійність роботи. Цей параметр, без сумніву, є визначальним - навіть найкращий антивірус виявиться абсолютно марним, якщо він не зможе нормально функціонувати на вашому комп'ютері, якщо в результаті будь-якого збою в роботі програми процес перевірки комп'ютера не пройде до кінця. Тоді завжди є ймовірність того, що якісь заражені файли залишилися непоміченими.

Розміри вірусної бази програми (кількість вірусів, які правильно визначаються програмою). З урахуванням постійної появи нових вірусів база даних повинна регулярно оновлюватися що толку від програми, не бачить половину нових вірусів і, як наслідок, створює помилкове відчуття "чистоти" комп'ютера. Сюди ж слід віднести і можливість програми визначати різноманітні типи вірусів, і вміння працювати з файлами різних типів (архіви, документи). Важливим також є наявність резидентного монітора, що здійснює перевірку всіх нових файлів "на льоту" (тобто автоматично, у міру їх запису на диск).

Швидкість роботи програми, наявність додаткових можливостей типу алгоритмів визначення навіть невідомих програмі вірусів (евристичне сканування). Сюди ж слід віднести можливість відновлювати заражені файли, не стираючи їх з жорсткого диска, а лише видаливши з них віруси. Важливим є також відсоток помилкових спрацьовувань програми (помилкове визначення вірусу в "чистому" файлі).

Багатоплатформність (наявність версій програми під різні операційні системи). Звичайно, якщо антивірус використовується тільки вдома, на одному комп'ютері, то цей параметр не має великого значення. Але ось антивірус для великої організації просто зобов'язаний підтримувати всі розповсюджені операційні системи. Крім того, при роботі в мережі важливим є наявність серверних функцій, призначених для адміністративної роботи, а також можливість роботи з різними видами серверів.

Характеристика антивірусних програм

Антивірусні програми поділяються на:

**Програми-детектори** забезпечують пошук і виявлення вірусів в оперативній пам'яті і на зовнішніх носіях, і при виявленні видають відповідне повідомлення. Розрізняють детектори універсальні і спеціалізовані.

Універсальні детектори в своїй роботі використовують перевірку незмінності файлів шляхом підрахунку та порівняння з еталоном контрольної суми. Недолік універсальних детекторів пов'язаний з неможливістю визначення причин викривлення файлів.

Спеціалізовані детектори здійснюють пошук відомих вірусів по їх сигнатурі (повторюваному ділянці коду). Недолік таких детекторів полягає в тому, що вони нездатні виявляти всі відомі віруси.

Недоліком таких антивірусних програм є те, що вони можуть знаходити тільки ті віруси, які відомі розробникам таких програм.

**Програми-доктора (фаги)**, не тільки знаходять заражені вірусами файли, але і "лікують" їх, тобто видаляють з файлу тіло програми вірусу, повертаючи файли в початковий стан. На початку своєї роботи фаги шукають віруси в оперативній пам'яті, знищуючи їх, і тільки потім переходять до "лікування" файлів. Серед фагів виділяють поліфаги, тобто програми-доктори, призначені для пошуку і знищення великої кількості вірусів.

Враховуючи, що постійно з'являються нові віруси, програми-детектори і програми-доктори швидко застарівають, і потрібне регулярне оновлення їх версій.

**Програми-ревізори** відносяться до найнадійніших засобів захисту від вірусів. Ревізори запам'ятовують початковий стан програм, каталогів і системних областей диска тоді, коли комп'ютер не заражений вірусом, а потім періодично або за бажанням користувача порівнюють поточний стан з вихідним. Виявлені зміни виводяться на екран відеомонітора. Як правило, порівняння станів проводять відразу після завантаження операційної системи. При порівнянні перевіряються довжина файла, код циклічного контролю (контрольна сума файла), дата і час модифікації, інші параметри.

**Програми-фільтри (сторожа)** представляють собою невеликі резидентні програми, призначені для виявлення підозрілих дій при роботі комп'ютера, характерних для вірусів. Такими діями можуть бути:

спроби корекції файлів з розширеннями СОМ і ЕХЕ;

зміна атрибутів файлів;

прямий запис на диск по абсолютному адресою;

запис у завантажувальні сектори диска.

завантаження резидентного програми.

При спробі будь-якої програми здійснити вказані дії "сторож" посилає користувачеві повідомлення і пропонує заборонити або дозволити відповідну дію. Програми-фільтри досить корисні, оскільки здатні виявити вірус на ранній стадії його існування до розмноження. Однак вони не "лікують" файли і диски. Для знищення вірусів потрібно застосувати інші програми, наприклад фаги. До недоліків програм-сторожів можна віднести їх "настирливість" (наприклад, вони постійно видають попередження про будь-якій спробі копіювання виконуваного файла), а також можливі конфлікти з іншим програмним забезпеченням.

**Вакцини (іммунізатори)** - це резидентні програми, що запобігають зараження файлів. Вакцини застосовують, якщо відсутні програми-доктори, "лікуючі" цей вірус. Вакцинація можлива тільки від відомих вірусів. Вакцина модифікує програму або диск таким чином, щоб це не відбивалося на їх роботі, а вірус буде сприймати їх зараженими і тому не впровадити. В даний час програми-вакцини мають обмежене застосування.

Істотним недоліком таких програм є їх обмежені можливості щодо запобігання зараження від великої кількості різноманітних вірусів.

Eset NOD32 (Словаччина)

NOD 32 AntivirusSystem від EsetSoftware забезпечує добре збалансований бездоганний захист персональних комп'ютерів і корпоративних систем, що працюють на платформах Microsoft Windows 95/98/ME/NT/2000/2003/XP, UNIX / Linux, Novell, MS DOS, а також для поштових серверів Microsoft Exchange Server, LotusDomino і інших. Головною перевагою NOD32 є його швидка робота, неймовірне низьке споживання системних ресурсів і не раз доведена здатність ловити 100% вірусів.

Основні проблеми антивірусної індустрії

Які ж можуть бути проблеми у антивірусних програм, за винятком звичайного маркетингового протиборства? Є віруси і є антивіруси, які їх ловлять. І на перший погляд, антивірус давно став звичайним споживчим товаром, який практично нічим не відрізняється від конкуруючих продуктів і який купують або за більш гарний дизайн, або тому, що даний продукт був вдало розрекламований, або з якої-небудь ще зовсім не технічної причини. Тобто антивірус давно повинен стати тим «commodity», продуктом масового споживання, на зразок пральних порошків, зубних щіток або автомобілів.

На жаль (або ура!) - Це не зовсім так, і часто вибір антивірусного рішення грунтується не на його дизайні, ціною або вдалій рекламі, а на технічних характеристиках, які сильно відрізняються в різних антивірусних продуктах.

Основне питання - від яких саме комп'ютерних загроз захищає дане рішення і наскільки якісна надаваний захист. *Антивірус має захищати від усіх видів шкідливих програм,* і чим він краще це робить, тим спокійніше живе його користувач і довше і міцніше спить системний адміністратор. І хто цього не розуміє теоретично, дуже скоро усвідомлює всю глибину проблеми практично - коли раптом кудись починають витікати гроші з банківського рахунку, комп'ютер сам по собі починає дзвонити з якихось абсолютно «лівим» телефонних номерах, раптово і з незрозумілих причин різко збільшується вихідний трафік.

На жаль, далеко не всі антивірусні продукти, які можна виявити на полицях магазинів або в мережі, дають захист, близьку до 100%. Більшість продуктів не гарантує навіть 90%-вий рівень захисту! У цьому і полягає основна проблема антивірусних компаній на сьогоднішній день.

***Проблема № 1***

Кількість і різноманітність шкідливих програм неухильно зростає рік за роком. Рейтинг мережевих небезпек 2008 показана в табл.1. У результаті багато антивірусні компанії просто не в змозі встигнути за цим потоком, вони програють у вірусній «гонці озброєнь», а користувачі цих програм виявляються захищені далеко не від усіх сучасних комп'ютерних загроз. На жаль, продукти далеко не всіх антивірусних компаній можна назвати дійсно антивірусними.

При цьому років п'ять чи десять тому можна було сказати, що захищати від усіх нових вірусів і троянських програм не треба - адже більшість з них так ніколи і не потрапляють в комп'ютери користувачів, оскільки були написані підлітками-хуліганами з метою самоствердження або просто з цікавості, і захищати треба тільки від тих небагатьох вірусів (ITW-in-the-wild), які все ж таки дісталися до комп'ютерів-жертв. Зараз же це не так. Переважна більшість (понад 75%) шкідливих програм зараз створюються комп'ютерним кримінальним андеграундом з метою зараження необхідної кількості комп'ютерів в мережі, а число нових вірусів і троянських програм обчислюється сотнями щодня.

Дані вірусні зразки поставляються в лабораторію з декількох джерел: від автоматичних «липучок» (honeypots - спеціально розроблених комплексів збору шкідливих файлів в мережі), від заражених користувачів, від адміністраторів локальних мереж, від інтернет-провайдерів і від інших антивірусних компаній. Незважаючи на маркетингову рубку на відведеній ринковому просторі (як це відбувається на всіх без винятку ринках), антивірусні компанії співпрацюють один з одним. При виявленні нового небезпечного швидко поширюється хробака антивірусні компанії практично моментально сповіщають своїх колег-конкурентів і висилають зразок (штам) вірусу. А не рідше разу на місяць більшість антивірусних компаній відсилають колегам свій місячний «вилов». Також йде обмін інформацією в спеціалізованих конференціях, закритих від сторонніх очей.

Отже, новий зразок нововиявленного вірусу або троянця виявлений в мережі або на зараженому комп'ютері. Що це означає? А рівно те, що ймовірність підчепити цю комп'ютерну «вошу» далеко не нульова, і не виключено, що в мережі вже десятки, сотні, а може, й тисячі вже заражених користувачів. А якщо новий «шкідник» є мережним хробаком, то рахунок жертв може піти і на мільйони. Тобто антивірусним компаніям необхідно моментально випускати оновлення проти всіх знову виявлених вірусів і троянців. І в цьому полягає друга проблема.

***Проблема № 2***

Видалення виявленого шкідливого коду із зараженої системи. Часто віруси і троянські програми роблять спеціальні дії, щоб приховати факт своєї присутності в системі, і / або вбудовуються в неї так глибоко, що завдання «виколупуванням кліща» стає досить нетривіальною. На жаль, інколи антивірусні програми не в змозі благополучно і без всяких побічних наслідків вилучити і заштопати рану.

Далі, будь-яке програмне забезпечення споживає ресурси комп'ютера. Антивіруси не виняток. Для того, щоб захищати комп'ютери, антивірусним програмам потрібно виробляти деякі дії: відкривати файли, читати з них інформацію, розкривати архіви для їх перевірки і т.п. І чим ретельніше перевіряються файли, тим більше від'їдається ресурсів комп'ютера (це як залізні двері: чим вона товщі, тим краще захищає, проте відкривати-закривати її стає тим складніше, чим більше тонн металу в неї закладено). У результаті з'являється проблема балансу: повноцінний захист або швидкість роботи.

***Проблема №3***

Доцільність споживання ресурсів. На жаль, проблема - як показує практика, всі «скорострільні» антивіруси дуже сильно «діряві» і пропускають віруси і троянські програми, як друшляк воду. Зворотне невірно: далеко не всі «загальмують» антивіруси захищають вас досить добре.

Для того щоб перевіряти файли «на льоту» і постійно захищати підопічний комп'ютер, антивірусним програмам доводиться досить глибоко проникати в ядро системи, причому проникати доводиться в одні і ті ж зони. Говорячи технічною мовою, антивіруси повинні встановлювати перехоплювачі системних подій глибоко всередині захищається системи і передавати результати своєї роботи антивірусному «движку» для перевірки перехоплених файлів, мережевих пакетів та інших потенційно небезпечних об'єктів.

Далеко не завжди в необхідну зону ядра операційної системи можна встановити два перехоплювача. У результаті - несумісність постійно працюють антивірусних «моніторів»; другий антивірусу або не вдається перехопити системні події, або спроба дублюючого перехоплення призводить до краху системи. У цьому полягає чергова антивірусна проблема.

Дії при зараженні комп'ютера вірусом:

Якщо ж на комп'ютері дійсно знайдений вірус, то треба зробити наступне.

**1.** Відразу ж вимкнути живлення, щоб вірус перестав поширюватися далі. Єдине, що можна зробити до виключення живлення, - це зберегти результати поточної роботи.

**2.** Увійти в SETUP і включити завантаження з диска А:.

**3.** Якщо відбулися які-небудь зміни, то необхідно відновити старі значення. Ні в якому разі не запускати жодної програми, яка знаходиться на жорсткому диску.

**4.** Необхідно завантажити з дискети (вона повинна бути захищена від запису) і запустити по черзі програми-детектори, що знаходяться на дискеті.

**5.** Якщо програма-детектор виявить файловий вірус, то можливі два варіанти дій. Якщо у вас встановлена програма-ревізор з лікуючим модулем, то відновлення файлів краще робити з її допомогою. Якщо таке програми немає. то необхідно скористатися для лікування одним з детекторів.

**6.** Після того як всі віруси видалені, необхідно заново перенести операційну систему на жорсткий диск (за допомогою команди SYS).

**7.** Необхідно перевірити цілісність файлової системи на вінчестері (за допомогою CHKDSK) і виправити всі пошкодження.

**8.** Необхідно ще раз перевірити жорсткий диск на наявність вірусів, якщо таких не виявилося, то можна перезавантажитися з вінчестера.

**9.** Необхідно відновити всі необхідні файли і програми з допомогою архіву - і для страховки, ще раз завантажившись з дискети, протестувати вінчестер.

**10.** Якщо все гаразд, то необхідно перевірити всі дискети, які могли виявитися зараженими вірусом і при необхідності пролікувати їх.

**11.** Після того як вірус дезактивований, ви можете продовжувати свою роботу. Крім перерахованих вище пунктів необхідно звертати особливу увагу на чистоту модулів, стиснутих файлів в архівах (ZIP, ARC, ICE, ARJ і т.д.) і даних в саморозпаковуючих файлах, створених утилітами типу ZIP2EXE. Якщо випадково упакувати файл заражений вірусом, то виявлення і видалення такого вірусу без розпакування файлу практично неможливо. У даному випадку типовою буде ситуація, при якій всі антивірусні програми, нездатні сканувати всередині упакованих файлів, повідомлять про те, що від вірусів очищено всі диски, але через деякий час вірус з'явиться знову.

Штами вірусу можуть проникнути і в резервні копії ПЗ при оновленні цих копій причому архіви і резервні копії є основними постачальниками давно відомих вірусів. Вірус може роками сидіти в дистрибутивної копії будь-якого програмного продукту і несподівано проявитися при установці програм на новому комп'ютері.

Як уберегтися від вірусів

Дотримання наступних правил може багаторазово знизити ризик зараження. Ці правила прості і відомі багатьом користувачам, однак дотримуються їх, на жаль, не все:

* За можливістю уникайте комп'ютерів «загальногкористування», встановлених в студентських [аудиторіях](http://ua-referat.com/%D0%90%D1%83%D0%B4%D0%B8%D1%82%D0%BE%D1%80%D0%B8%D1%8F), на поштах і т.п.3а день таким комп'ютером користується безліч людей, і будь-хто може занести вірус зі своєю дискети або [компакт-диска](http://ua-referat.com/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BA%D1%82-%D0%B4%D0%B8%D1%81%D0%BA), тому записувати інформацію з такого копьютера на свою дискету категорично не рекомендується;
* при полученні з Інтернету або локальної мережі файлів додатків пакету Microsoft Office (наприклад, Word або [Excel](http://ua-referat.com/Excel)) в першу чергу перевірте їх надійної антивірусною програмою і тільки потім відкривайте. Такі файли можуть містити макровіруси;
* те ж саме відноситься і до інших скачаних з Інтернету файлів: дистрибутивам або виконуваним файлами додатків, архівів і д.р. Перед Виконанням їх необхідно обов'язково перевірити антивірусною програмою, не забувши попередньо оновити антивірусні бази;
* якщо використовувана антивірусна програма володіє можливістю постійного моніторингу, то при роботі в Інтернеті даний режим обов'язково повинен бути включений. Це допоможе вчасно виявити заражені файли, які намагаються проникнуть в комп'ютер;
* час від часу потрібно повністю сканувати комп'ютер на наявність вірусів за допомогою хорошої антивірусної програми. Періодичність сканування залежить від завантаження комп'ютера, а також від того, чи [працює](http://ua-referat.com/%D0%9F%D1%80%D0%B0%D1%86%D1%8E%D1%94) користувач з Інтернетом;
* при роботі із зовнішніми носіями інформації (наприклад, дискетами або компакт-дисками)

обов'язково перевіряйте їх антивірусною програмою на наявність вірусів. Особливо це стосується роботи з чужими або новими компакт-дисками або дискетами

* ні в якому разі не запускайте раптово з'явилися на *Робочому столі* значки. Багато вірусів (особливо мережеві «черв'яки») спеціально поміщають на *Робочий стіл* привабливий значок. При натисканні на такому значку вірус активізується і починає поширюватися по мережі;
* при роботі з файлами, розташованими в Інтернеті, не запускайте їх відразу. Збережіть потрібний файл на свій комп'ютер, перевірте його антивірусною програмою і тільки після цього відкрийте;
* після закінчення роботи в Інтернеті обов'язково відключіть шнур, що з'єднує комп'ютер з телефонною лінією. Якщо цього не зробити, то зловмисник може легко отримати доступ навіть до виключеного комп'ютера.

Висновок

Провівши дослідження комп’ютера, я стикнулась з проблемою «знищення вірусів». Основним методом вирішення проблеми було застосування антивірусної програми. Проблема була вирішена повністю, оскільки аналіз даних зараженого копм'ютера показав, що потрібно скачати антивірусне ПЗ (мною запропоноване ESET NOD32). Ідентифікувала походження вірусу- троян. Заражено 60 об'єктів. Якщо комп'ютер навіть не включається, то потрібно спробувати комбінацію клавіш F8 (відновлення останньої вдалої конфігурації) або ж повернутися до BIOS. В крайньому випадку потрібно оновлювати операційну систему. При розробці **антивірусної стратегії компанії** слід пам'ятати, що основними шляхами поширення комп'ютерних вірусів є програмне забезпечення, системи електронної пошти в локальних мережах, а також дискети, використовувані службовцями в їхніх домашніх комп'ютерах.

Користувач може вірити повідомленням про віруси, що розсилається спеціальними групами з організацій з комп'ютерної безпеки. Необхідно перевіряти джерело повідомлення. Відкриті ключі організацій зберігаються на їхніх інтернет-сторінках. Необхідно уникати повідомлень, що не пройшли процедуру ідентифікації. При виявленні нового вірусу необхідно повідомити про це в організацію з комп'ютерної безпеки. Довіртеся професіоналам.

Не варто також приписувати всі ваші неприємності діям вірусу. Говорити ж про дію невідомого вірусу, а тим більше вдаватися до радикальних заходів слід тільки тоді, коли не залишається жодних сумнівів. Варто спочатку спробувати відновити файли, і, тільки якщо це не вдається, видалити їх.

Не існує антивірусів, що гарантують стовідсоткову захист від вірусів. Таких систем не існує, оскільки на будь-який алгоритм антивіруса завжди можна запропонувати контр алгоритм вірусу, невидимого для цього антивіруса. Більш того, неможливість [існування](http://ua-referat.com/%D0%86%D1%81%D0%BD%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F) абсолютного антивіруса була доведена [математично](http://ua-referat.com/%D0%9C%D0%B0%D1%82%D0%B5%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0) на основі теорії кінцевих [автоматів](http://ua-referat.com/%D0%90%D0%B2%D1%82%D0%BE%D0%BC%D0%B0%D1%82), автор [докази](http://ua-referat.com/%D0%94%D0%BE%D0%BA%D0%B0%D0%B7%D0%B8)-Фред Коен.

Необхідно стежити за тим, щоб антивірусні програми, використовувані для перевірки, були найновіших версій. Якщо до програм підставляються оновлення, то необхідно перевірити їх на «свіжість». Зазвичай [вихід](http://ua-referat.com/%D0%92%D0%B8%D1%85%D1%96%D0%B4) нових версій антивірусів анонсується, тому досить відвідати відповідні вузли WWW, ftp або BBS.

«Національність» антивірусів в більшості випадків не має значення, оскільки на сьогоднішній день [процес](http://ua-referat.com/%D0%9F%D1%80%D0%BE%D1%86%D0%B5%D1%81) еміграції вірусу в інші країни та імміграції антивірусних програм обмежується тільки швидкістю Internet, тому як віруси, так і антивіруси не визнають кордонів.

Незважаючи на великі зусилля як теоретичного, так і практичного характеру щодо вирішення проблеми захисту інформації, його сучасний стан дуже далекий від будь-якого надійного розв'язання. Віруси роблять неможливим нормальне функціонування програм і комп'ютера, тому, безперечно, для лікування програм, знищення вірусів і профілактики постійно потрібні нові антивірусні програми.

Список використаної літератури

1. Донцов Д. Як захистити комп'ютер від помилок, вірусів, хакерів. Почали!-Санкт-Петербург: «Пітер», 2008
2. Касперський Е. Комп'ютерні віруси в MS-DOS.-М.: «Едель», 1992
3. Сичов Ю.М. Інформаційна безпека: навчальний посібник, посібник з вивчення дисципліни, практикум, тести, навчальна программа.-М.: «Алла», 2007
4. Фігурне В.Е. IBM PC для користувача від початківця - до досвідченого. Повністю перероблене сьомого ізданіе.-М.: «Аст», 2002
5. Філін С.О. Інформаційна безпека: Навчальний посібник.-М.: «Альфа-Прес», 2006
6. Ярочкін В.І. Інформаційна безпека: [Підручник](http://ua-referat.com/%D0%9F%D1%96%D0%B4%D1%80%D1%83%D1%87%D0%BD%D0%B8%D0%BA) для [студентів](http://ua-referat.com/%D0%A1%D1%82%D1%83%D0%B4%D0%B5%D0%BD%D1%82) вузов.-3-е изд.-М.: «Трікста», 2005
7. Дії при зараженні, основні проблеми, як уберегтись від вірусів (Електронний ресурс):

Ua-referat.com/Методика\_використання\_антивірусних\_програм

ЗМІСТ

[ВСТУП 2](#_Toc379456793)

[КРИТЕРІЇ АНТИВІРУСНИХ СИСТЕМ 3](#_Toc379456794)

[Характеристика антивірусних програм 4](#_Toc379456795)

[Eset NOD32 (Словаччина) 6](#_Toc379456796)

[Основні проблеми антивірусної індустрії 6](#_Toc379456797)

[Дії при зараженні комп'ютера вірусом: 11](#_Toc379456798)

[Як уберегтися від вірусів 12](#_Toc379456799)

[Висновок 14](#_Toc379456800)

[Список використаної літератури 16](#_Toc379456801)