**\*Назва навчального закладу\***

**Факультет \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

***Кафедра \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

**Реферат**

**з курсу**

**«Комп’ютерні мережі»**

## ТЕМА: хмарні технології

Студент \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Група \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Факультет \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Викладач: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Київ 2023**

Зміст

[Вступ 3](#_Toc152261667)

[Джерела вірусів 4](#_Toc152261668)

[Ознаки зараження комп'ютера вірусом: 4](#_Toc152261669)

[Класифікація вірусів 5](#_Toc152261670)

[Типи антивірусних програм: 7](#_Toc152261671)

[ADINF 8](#_Toc152261672)

[AVP 8](#_Toc152261673)

[Висновок: 9](#_Toc152261674)

[Використана література 11](#_Toc152261675)

# Вступ

**Комп'ютерний вірус** - це невелика програма, що написана програмістом високої кваліфікації, здатна до саморозмноження й виконання різних деструктивних дій. На сьогоднішній день відомо понад 50 тис. Комп'ютерних вірусів. Існує багато різних версій стосовно дати народження першого комп'ютерного вірусу. Однак більшість фахівців сходяться на думці, що комп'ютерні віруси, як такі, вперше з'явилися у 1986 році, хоча історично виникнення вірусів тісно пов'язане з ідеєю створення самовідтворюючих програм.

Одним із "піонерів" серед комп'ютерних вірусів вважається вірус "Brain", створений пакистанським програмістом на прізвище Алві. Тільки у США цей вірус вразив понад 18 тис. комп'ютерів. На початку епохи комп'ютерних вірусів розробка вірусоподібних програм носила чисто дослідницький характер, поступово перетворюючись на відверто вороже протистояння користувачів та безвідповідальних, і навіть кримінальних "елементів". В ряді країн карне законодавство передбачає відповідальність за комп'ютерні злочини, в тому числі за створення та розповсюдження вірусів.

Віруси діють тільки програмним шляхом. Вони, як правило, приєднуються до файлу або проникають всередину файлу. У цьому випадку кажуть, що файл заражений вірусом. Вірус потрапляє в комп'ютер тільки разом із зараженим файлом. Для активізації вірусу потрібно завантажити заражений файл, і тільки після цього вірус починає діяти самостійно. Деякі віруси під час запуску зараженого файлу стають резидентними (постійно знаходяться в оперативній пам'яті комп'ютера) і можуть заражати інші файли та програми, що завантажуються. Інші різновиди вірусів відразу після активізації можуть спричиняти серйозні пошкодження, наприклад, форматувати жорсткий диск.

Дія вірусів може проявлятися по різному: від різних візуальних ефектів, що заважають працювати, до повної втрати інформації. Більшість вірусів заражують виконавчі програми, тобто файли з розширенням .EXE та .COM, хоча останнім часом все більшої популярності набувають віруси, що розповсюджуються через систему електронної пошти. Слід зауважити, що комп'ютерні віруси здатні заражати лише самі комп'ютери. Тому абсолютно абсурдними є різні твердження про вплив комп'ютерних вірусів на користувачів комп'ютерів.

# Джерела вірусів

* дискета, на якій знаходяться заражені вірусом файли;
* комп'ютерна мережа, в тому числі система електронної пошти та Internet;
* жорсткий диск, на який потрапив вірус в результаті роботи з зараженими програмами;
* вірус, що залишився в оперативній пам'яті після попереднього користувача.

#### Звідси випливає, що зараження комп'ютера не відбудеться, якщо:

* на комп'ютері переписуються тексти програм, документів, файли даних системи управління базами даних (СУБД), таблиць табличних процесорів і т. д. (ці файли не є програмами);
* виконується копіювання файлів з однієї дискети на іншу, в разі копіювання зараженого файлу його копія також буде заражена.

# Ознаки зараження комп'ютера вірусом:

* зменшення обсягу вільної оперативної пам'яті;
* сповільнення завантаження та роботи комп'ютера;
* незрозумілі (без причин) зміни у файлах, а також зміни розмірів та дати останньої модифікації файлів;
* помилки при завантаженні операційної системи;
* неможливість зберігати файли в потрібних каталогах;
* незрозумілі системні повідомлення, музикальні та візуальні ефекти і т.д.

#### Коли вірус переходить в активну фазу можливі такі ознаки:

* зникнення файлів;
* форматування жорсткого диска;
* неспроможність завантаження файлів або операційної системи.

# Класифікація вірусів

1. завантажувальні віруси або BOOT-віруси: заражають boot-сектори дисків. Дуже небезпечні, можуть призвести до повної втрати всієї інформації, що зберігається на диску;
2. файлові віруси: заражають файли. Поділяються на:
   1. віруси, що заражують програми (файли з розширенням .EXE і .COM);
   2. макровіруси: віруси, що заражують файли даних, наприклад, документи Word або робочі книги Excel;
   3. віруси-супутники: використовують імена інших файлів;
   4. віруси сімейства DIR: спотворюють системну інформацію про файлові структури;
3. завантажувально-файлові віруси: здатні вражати як код boot-секторів, так і код файлів;
4. віруси-невидимки або STEALTH-віруси: фальсифікують інформацію прочитану з диска так, що програма, якій призначена ця інформація отримує невірні дані. Ця технологія, яку, інколи, так і називають Stealth-технологією, може використовуватися як в BOOT-вірусах, так і у файлових вірусах;
5. ретровіруси: заражують антивірусні програми, намагаючись знищити їх або зробити непрацездатними;
6. віруси-хробаки: заражують невеликі повідомлення електронної пошти, так званим заголовком, який по своїй суті є всього навсього лише Web-адресою місцезнаходження самого вірусу. При спробі прочитати таке повідомлення вірус починає зчитувати через глобальну мережу Internet своє 'тіло', яке після завантаження починає свою деструктивну дію. Дуже небезпечні, так як виявити їх дуже важко у зв'язку з тим, що заражений файл фактично не містить коду вірусу.

Якщо не вживати заходів для захисту від комп'ютерних вірусів, то наслідки зараження можуть бути дуже серйозними. В ряді країн карне законодавство передбачає відповідальність за комп'ютерні злочини, в тому числі за впровадження вірусів. Для захисту інформації від вірусів використовуються загальні та програмні засоби.

До загальних засобів, що допомагають запобігти зараженню та його руйнівних наслідків належать:

* резервне копіювання інформації (створення копій файлів і системних областей жорстких дисків);
* уникнення користування випадковими й невідомими програмами. Найчастіше віруси розповсюджуються разом із комп'ютерними вірусами;
* перезавантаження комп'ютера перед початком роботи, зокрема, у випадку, якщо за цим комп'ютером працювали інші користувачі;
* обмеження доступу до інформації, зокрема фізичний захист дискети під час копіювання файлів із неї.

До програмних засобів захисту належать різні антивірусні програми (антивіруси). Антивірус - це програма, яка виявляє й знешкоджує комп'ютерні віруси. Слід зауважити, що віруси у своєму розвиткові випереджають антивірусні програми, тому навіть у випадку регулярного користування антивірусів немає 100% гарантії безпеки. Антивірусні програми можуть виявляти та знищувати лише відомі віруси, при появі нового комп'ютерного вірусу захисту від нього не існує до тих пір, поки для нього не буде розроблено свій антивірус. Однак, багато сучасних антивірусних пакетів мають у своєму складі спеціальний програмний модуль, який називається евристичний аналізатор, і який здатний досліджувати вміст файлів на наявність коду, характерного для комп'ютерних вірусів. Це дає змогу вчасно виявляти та попереджати про небезпеку зараження новим вірусом.

# Типи антивірусних програм:

1. програми-детектори: призначені для знаходження заражених файлів одним із відомих вірусів. Деякі програми-детектори можуть також лікувати файли від вірусів або знищувати заражені файли. Існують спеціалізовані (тобто призначені для боротьби з одним вірусом) детектори та поліфаги (можуть боротися з багатьма вірусами);
2. програми-лікарі: призначені для лікування заражених дисків і програм. Лікування програми полягає у вилученні із зараженої програми тіла вірусу. Також можуть бути як поліфагами, так і спеціалізованими;
3. програми-ревізори: призначені для виявлення зараження вірусом файлів, а також знаходження ушкоджених файлів. Ці програми запам'ятовують дані про стан програми та системних областей дисків у нормальному стані (до зараження) і порівнюють ці дані у процесі роботи комп'ютера. В разі невідповідності даних виводиться повідомлення про можливість зараження;
4. лікарі-ревізори: призначені для виявлення змін у файлах і системних областях дисків й у разі змін повертають їх у початковий стан.
5. програми-фільтри: призначені для перехоплення звернень до операційної системи, що використовуються вірусами для розмноження і повідомляють про це користувача. Останній має можливість дозволити або заборонити виконання відповідної операції. Такі програми є резидентними, тобто вони знаходяться в оперативній пам'яті комп'ютера.
6. програми-вакцини: використовуються для обробки файлів і boot-секторів із метою попередження зараження відомими вірусами (в останній час цей метод використовується все частіше).

Слід зауважити, що вибір одного "найкращого" антивірусу є вкрай помилковим рішенням. Рекомендується використовувати декілька різних антивірусних пакетів одночасно. Вибираючи антивірусну програму слід звернути увагу на такий параметр, як кількість розпізнаючих сигнатур (послідовність символів, які гарантовано розпізнають вірус). Другий параметр - наявність евристичного аналізатора невідомих вірусів, його присутність дуже корисна, але суттєво уповільнює час роботи програми. На сьогоднішній день існує велика кількість різноманітних антивірусних програм. Розглянемо коротко найбільш поширені в Україні.

## ADINF

Антивірус-ревізор диска ADINF (Avanced DiskINFoscope) дозволяє знаходити та знищувати, як існуючі звичайні, stealth- і поліморфні віруси, так і зовсім нові. Антивірус має в своєму розпорядженні лікуючий блок ревізору ADINF - Adinf Cure Module - який може знешкодити до 97% всіх вірусів. Цю цифру наводить "ДіалогНаука", виходячи з результатів тестування, котре відбувалося на колекціях вірусів двох визнаних авторитетів в цій області - Д.Н.Лозинського й фірми Dr.Solomon's (Великобританія).

ADINF завантажується автоматично у разі вмикання комп'ютера і контролює boot-сектор і файли на диску (дата й час створення, довжина, контрольна сума), виводячи повідомлення про їх зміни. Завдяки тому, що ADINF здійснює дискові операції в обхід операційної системи, звертаючись до функцій BIOS, досягаються не тільки можливість виявлення активних stealth-вірусів на рівні переривання Int 13h, але і висока швидкість перевірки диску. Якщо знайдено boot-вірус, то ADINF просто відновить попередній завантажувальний сектор, котрий зберігається в його таблиці.

Якщо вірус є файловим, то тут на допомогу приходить лікуючий блок Adinf Cure Module, який на основі звіту основного модуля про заражені файли порівнює нові параметри файлів із попередніми, які зберігаються в спеціальних таблицях. При виявленні розбіжностей ADINF відновлює попередній стан файлу, а не знищує тіло вірусу, як це роблять поліфаги.

## AVP

Антивірус AVP (AntiVirus Program) відноситься до поліфагів, у процесі роботи перевіряє оперативну пам'ять, файли, в тому числі архівні, на гнучких, локальних, мережних і CD-ROM дисках, а також системні структури даних, такі як завантажувальний сектор, таблицю розділів і т.д. Програма має евристичний аналізатор, котрий, за твердженнями розробників антивірусу здатний знаходити майже 80% усіх вірусів. Програма AVP є 32-розрядним додатком для роботи в середовищі операційних систем Windows 98, NT і 2000, має зручний інтерфейс, а також одну з найбільших у світі антивірусну базу. Нові бази антивірусів до AVP з'являються приблизно один раз у тиждень і їх можна отримати з Internet. Ця програма здійснює пошук і вилучення найрізноманітніших вірусів, у тому числі:

* поліморфних, або вірусів, що самошифруються;
* стелс-вірусів, або вірусів-невидимок;
* нових вірусів для Windows;
* макровірусів, що заражають документи Word і таблиці Excel.

Крім того, програма AVP здійснює контроль файлових операцій у системі у фоновому режимі, виявляє вірус до моменту реального зараження системи, а також визначає невідомі віруси за допомогою евристичного модуля.

# Висновок:

Комп'ютерні віруси стали невід'ємною частиною сучасного інформаційного суспільства, породжуючи величезні загрози для безпеки і конфіденційності інформації. Вони можуть призвести до серйозних проблем, таких як втрата даних, порушення приватності, а також значних економічних збитків. З цього приводу, важливо вживати заходів для запобігання і поширення захворювань в комп'ютерних мережах.

Одним із найефективніших заходів захисту є регулярне оновлення антивірусного програмного забезпечення та встановлення важливих патчів безпеки. Крім того, користувачам слід бути обережними при відкритті електронних листів, завантаженні файлів та відвідуванні ненадійних веб-сайтів, оскільки багато вірусів поширюються через соціальну інженерію.

Важливо пам'ятати, що в сфері кібербезпеки немає повної гарантії захисту, і тому постійно покращувати стратегії та технічні рішення для виявлення і видалення нових загроз. Широке розуміння ризиків, ретельне навчання персоналу та використання сучасних методів захисту є важливими елементами боротьби з комп'ютерними вірусами у сучасному інформаційному середовищі.

# Використана література

1. Курс користувачів персональним комп’ютером. Автори : Г.В.Саєнко та Т.Б.Волобуєва. 2006 рік.
2. Практичний курс інформатики. Автори : В.Д.Руденко; О.М.Макарчук; М.О.Патланжоглу.
3. Караванова Т. П. Розвиток творчості учнів при вивченні інформатики: Авторська програма погли­бленого вивчення інформатики.—Чернівці: ОНМІПО, 2006.—44с.
4. Рудненко В.Д.,Макарчук О.М., Патланжоглу М.О.Практичний курс інформатики / За ред. Мадзігона В.М. - К.:Фенікс, 2007. -304 с.
5. Глушаков С.В. ,Персональний комп'ютер. Учебний курс.-Харків:Фомо;М.:ООО.Фирма "Издательство Аст",2004.-499с.
6. Гордієнко Г.В. Входження України у всесвітню систему інформації. // Нова політика. - 1999 р. - №5 – С. 64-67.
7. Демінський С.О. Гроші в Мережі. // Політика і культура. - 2001. - №5 (88) / 13-19 лютого. - С. 34-36.
8. Демонополізація “Інтернету”. // Молода дипломатія. - 2000. - №4 (18). – 17 с.
9. Інформаційна тривога. // Пробудись. - 1998. - 8 січня. – С. 3-12.