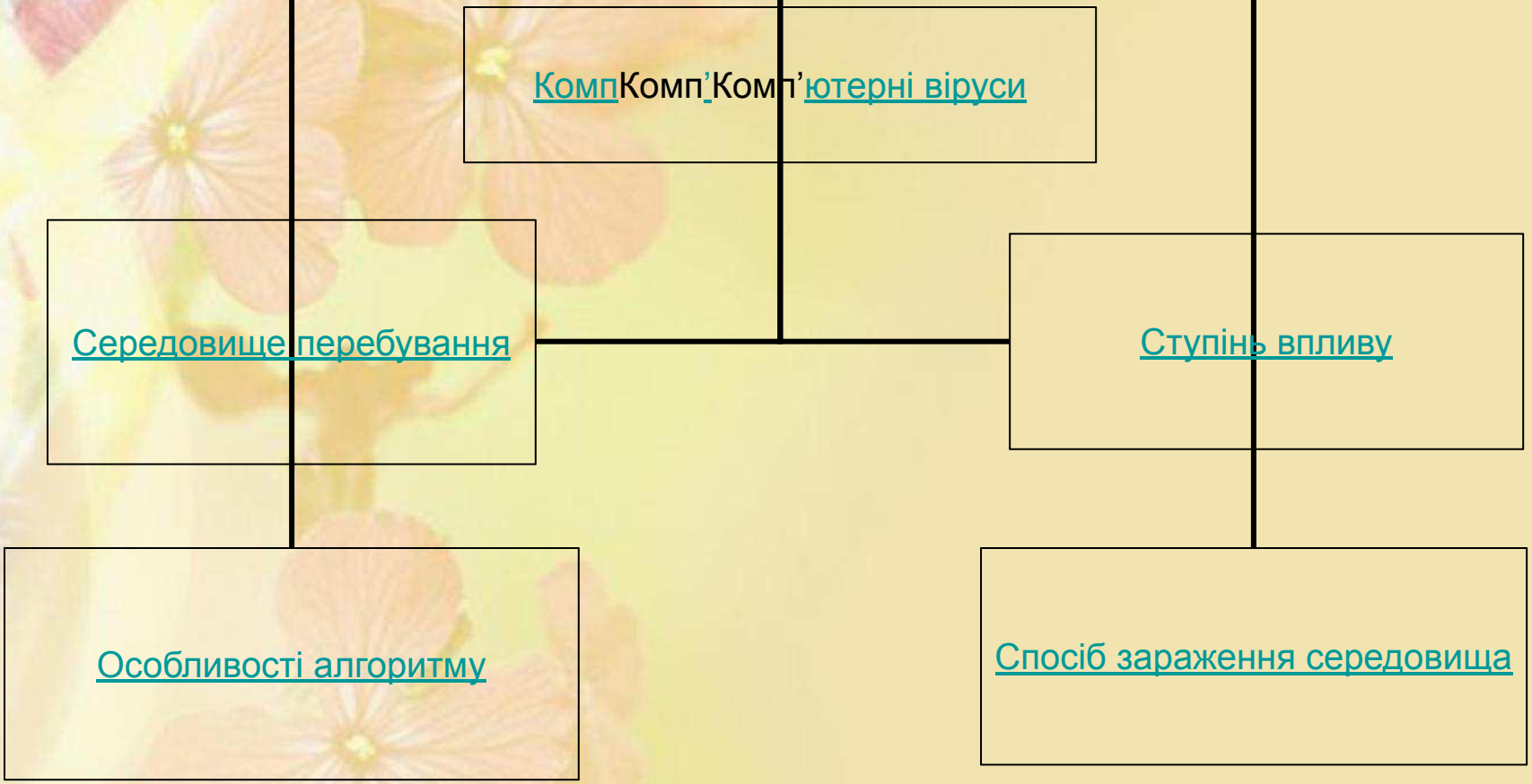
Антивірусні програмні засоби

ЗМІСТ

Для детальної інформації натисніть на розділ який вас цікавить

Класифікація комп’ютерних вірусів




Середовище перебування
Файлові
Завантажувальні
Файлово-завантажувальні
Мережні


Ступінь впливу
Безпечні
Дуже небезпечні
Небезпечні


Особливості алгоритму
Найпростіші (паразитичні)
Віруси реплікатори
Віруси-мутанти
Троянські програми


Спосіб зараження середовища
Резидентні
Нерезидентні

- 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.

Файлові

- Убудовуються у виконувані файли (найбільш поширений тип вірусів), або створюють файли-двійники (компаньйон-віруси), або використовують особливості організації файлової системи (link віруси)

Завантажувальні

- Записують себе або в завантажувальний сектор диска (bootсектор), або сектор, який містить системний завантажник вінчестера (Master Boot Record), або змінюють покажчик на активний bootсектор

Файлово-завантажувальні

- Заражають як файли, так і завантажувальні сектори дисків.

Мережні

- Поширюються комп'ютерними мережами.

Безпечні віруси

- Вплив обмежується зменшенням вільної пам'яті на диску та графічними, звуковими й іншими ефектами.

Небезпечні віруси

- Можуть призвести до серйозних збоїв у роботі комп’ютера.

Дуже небезпечні

- В алгоритм роботи явно закладено дії, що можуть спричинити втрату програм, знищити дані тощо.

Найпростіші віруси (паразитичні)

- Змінюють уміст файлів і секторів диска; їх можна достатньо легко виявити і знищити.

Віруси-реплікатори

- Так називані хробаки, що поширюються комп'ютерними мережами.

Віруси мутанти

- Містять алгоритми шифрування-розшифрування.

Квазивірусні, або «троянські програми»

- Не спроможні до саморозповсюдження, проте дуже небезпечні, оскільки, маскуючись під корисну програму, руйнують завантажувальний сектор і файлову систему дисків.

Резидентний вірус

- 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.

Нерезидентний вірус

- Зберігають активність обмежений час.

Віруси невидимки - стелсвіруси

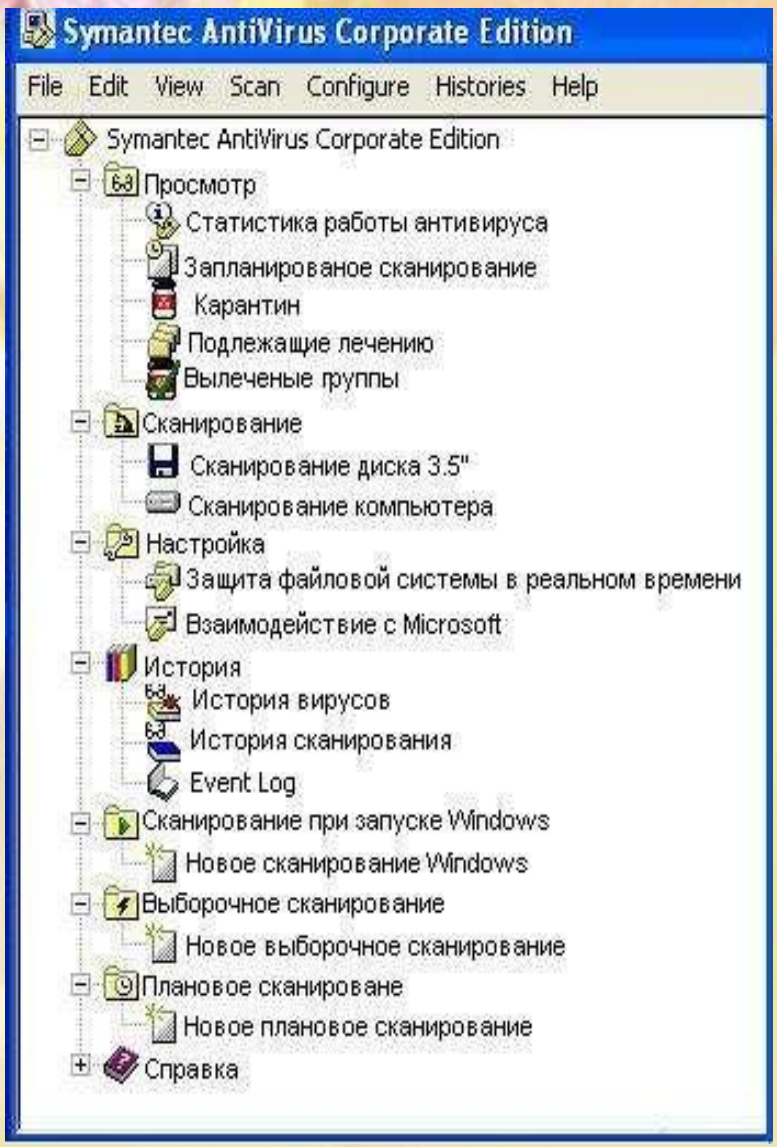
- Перехоплюють обертання ОС до уражених файлів і секторів дисків та підставляють замість свого тіла незаражені ділянки диска.

Антивірусні програми

Антивірусні програми

- Антивірусні програми — програми для виявлення, видалення і захищення від комп'ютерних вірусів.
- Розроблювачі антивірусів змушені передбачати практично всі основні типи антивірусних програм, які стосовно нинішніх питань безпеки правильно було б назвати компонентами або складовими, ніж самостійними додатками.

Шпаргалка по Symantec



Види антивірусних програм

- Програми детектори або сканери
- Програми монітори
- Програми лікарі або фаги
- Програми ревізори
- Програми фільтри або “сторожі”
- Програми вакцини, або імунізатори

Програми детектори або сканери

- Основний елемент будь-якого антивірусу здійснює пасивний захист. За запитом ко ристувача або заданим розпорядком провадить перевірку файлів у вибраній ділянці) системи. Шкідливі об'єкти виявляє шляхом пошуку й порівняння програмного коду вірусу. Приклади програмних кодів містяться в заздалегідь установлених сиг натурах (наборах, характерних послідовностей байтів для відомих вірусів).

Програми детектори або сканери

(продовження)

- Серед недоліків цих програм — беззахисність перед вірусами, що не мають постійного програмного коду й здатні видозмінюватися зі збереженням основних функцій. Також сканери не можуть протидіяти різновидам того самого вірусу, що вимагає від користувача постійного оновлення антивірусних баз. Та найбільш уразливе міс це - нездатність виявляти нові й невідомі віруси.

Програми монітори

- У сукупності зі сканерами створюють базовий захист комп'ютера. На основі наявних сигнатур здійснюють перевірку поточних процесів у режимі реального часу.
- Виконують попередню перевірку при спробі перегляду або запуску файлу. Розрізняють файлові монітори, для поштових клієнтів, що використовують протоколи POP3, IMAP, NNTP і SMTP, і спеціальні монітори для окремих додатків. Основна їхня перевага - здатність виявляти віруси безпосередньо на ранній стадії активності.

Програми лікарі або фаги

- Знаходять заражені вірусами файли та «лікують» їх, тобто видаляють із файла тіло програми віруса, повертаючи файли до вихідного стану. Спочатку фаги знаходять і знищують віруси в оперативній пам'яті, і тільки потім переходять до «лікування» файлів. Серед фагів виділяють поліфаги, тобто програми-лікарі, призначені для пошуку і знищення великої кількості вірусів. З огляду на те, що постійно з'являються нові віруси, програми-детектори і програми-доктори швидко застарівають, і потрібно регулярне відновлення їх версій.

Програми ревізори

- Зберігають в окремій базі дані про стан критичних на певний момент для роботи ділянок системи. Згодом порівнюють поточні файли із зареєстрованими раніше, в такий спосіб виявляючи будь-які підозрілі зміни. Перевага — низькі апаратні вимоги і висока швидкість роботи.

Програми ревізори

(продовження)

- Ревізорові взагалі не потрібна антивірусна база, сприйняття й знаходження відбуваються тільки на рівні незмінності вихідних файлів. Це дозволяє ефективно відновлювати систему, пошкоджену діяльністю шкідливих модулів. Недолік полягає в неможливості оперативно реагувати на появу вірусу в системі. Під час перевірки також виключаються нові файли, що дозволяє вірусам, які заражають тільки заново створювані файли, залишитися.

Програми фільтри або “сторожі”

- Являють собою невеличкі резидентні програми, призначені для виявлення підозрілих дій при роботі комп'ютера, характерних для вірусів (а саме: спроба корекції файлів із розширеннями COM і EXE; зміна атрибутів файлів; прямий запис на диск за абсолютною адресою; запис у завантажувальні сектори диска; завантаження резидентної програми).

Програми фільтри або “сторожі”

(продовження)

- При спробі програми зробити зазначені дії «сторож» посилає користувачу повідомлення і пропонує заборонити або дозволити відповідну дію. Програми-фільтри дуже корисні, оскільки здатні виявити вірус на початковій стадії існування його до розмноження. Проте вони не «лікують» файли і диски, для знищення вірусів потрібно застосувати інші програми, наприклад фаги.

Програми вакцини, або імунізатори

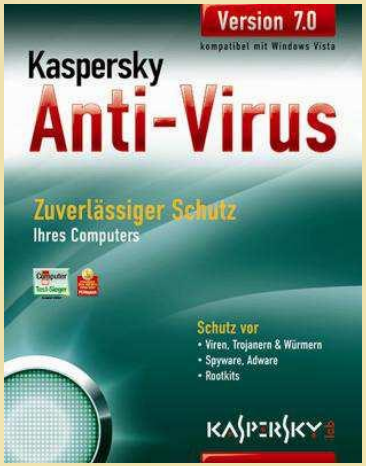
- Імітують зараження файлів певними вірусами, внаслідок чого справжні віруси зіштовхуються зі своїми «побратимами» і припиняють спроби зараження. Сьогодні цей тип програм практично не використовується.

Протидія комп’ютерним вірусам

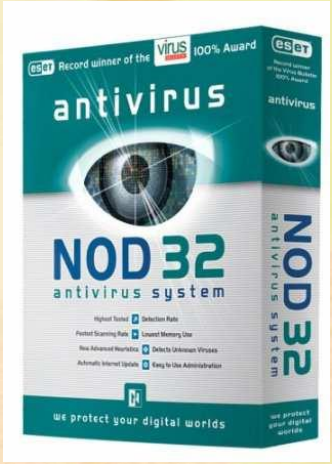
- Профілактика вірусного зараження й зменшення передбачуваної шкоди від такого зараження
- Методика використання антивірусних програм, у тому числі знешкодження й видалення відомого вірусу.

- Установити на комп’ютері сучасні антивірусні програми й постійно оновлювати їх версії.
- Перед зчитуванням з дискет інформації, записаної на інших комп’ютерах, завжди перевіряти ці дискети на наявність вірусів; перенесені на свій комп’ютер файлів в архівіруваному вигляді перевіряти відразу після розархівування на жорсткому диску, обмежуючи ділянку перевірки тільки щойно записаними файлами; періодично перевіряти на наявність вірусів жорсткі диски комп’ютера, запускаючи антивірусні програми для тестування файлів, пам’яті й систематичних ділянок.
- Завжди захищати свої дискети від запису під час роботи на інших комп’ютерах, якщо на них не буде проводитись запис інформації.
- Дистрибутивні копії програмного забезпечення необхідно купувати в офіційних продавців.
- Періодично зберігати на зовнішньому носії файли, з якими ведеться робота

Антивірусні програми



Антивірусні програми



Вікна антивірусних програм (Касперського та NOD32)