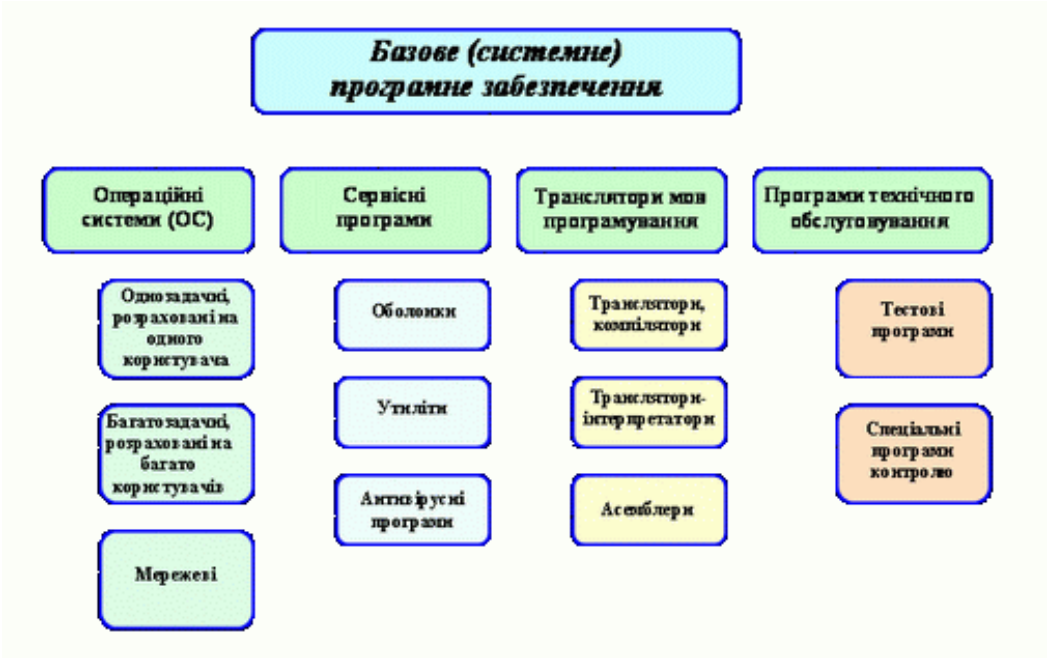
Тема 26: Захист програмного забезпечення.

Основне завдання сервісних програм - підтримка порядку в комп'ютері.

Сервісне програмне забезпечення:

- Діагностичні програми.
- Антивірусні програми.
- Програми, що обслуговують диски.
- Програми архівації даних.
- Програми, що обслуговують мережі.

Базове програмне забезпечення (base software) - мінімальний набір програмних засобів, що забезпечують роботу комп'ютера.



Сервісне програмне забезпечення *(програми обслуговування)* - програми та програмні комплекси, які розширюють можливості базового програмного забезпечення та організують більш зручне середовище роботи користувача.

До категорії сервісного програмного забезпечення *службові програми (утиліти).*

Утиліти (від англ. Utilize - використовувати) - це допоміжні або службові програми, що забезпечують оптимізацію використання ресурсів обчислювальної машини, надають користувачеві ряд додаткових послуг.

До утиліт відносяться також і засоби забезпечення комп'ютерної безпеки (резервне копіювання, антивірусне ПЗ).

Частина утиліт входить до складу ОС, а інша частина функціонує автономно.

Комп'ютерні віруси

Вважається, що поширення комп'ютерних вірусів почалося в середині 80-х років з появою ігрових програм. Незважаючи на прийняті в багатьох країнах закони про боротьбу з комп'ютерними злочинами і розробку спеціальних програмних засобів захисту від вірусів, кількість нових вірусів постійно росте. Це вимагає від користувача персонального комп'ютера знань про природу вірусів, способи зараження вірусами і захисту від них.

Що таке **комп'ютерний вірус**? Одне з найвідоміших тлумачень належить В.Е.Фігурнову: *«Це спеціально написана невелика за розмірами програма, яка може*

приписувати себе до інших програм (тобто заражати їх), а також виконувати різні небажані дії на комп'ютері» .

Класифікація вірусів

Віруси можна розділити на класи за такими основними ознаками:

- *середовище існування;*
- *тип операційної систем;*
- *особливості алгоритму роботи;*
- *деструктивні можливості*.

За середовищем існування віруси можна розділити на: *файлові, завантажувальні, мережеві.*

Файлові віруси різними способами впроваджуються у виконувані файли, або створюють файли-двійники, або використовують особливості організації файлової системи.

Завантажувальні віруси порушують роботу завантажувальний сектор диска (boot-сектор).

Мережеві віруси використовують для свого поширення протоколи або команди комп'ютерних мереж і електронну пошту.

Існує велика кількість сполучень - наприклад, *файлово-завантажувальні віруси* , що заражають як файли, так і завантажувальні сектори дисків. Такі віруси, як правило, мають досить складний алгоритм роботи, часто застосовують оригінальні методи проникнення в систему. Інший приклад такого сполучення - *мережний макровірус* , який не тільки заражає документи, але і розсилає свої копії по електронній пошті.

Серед ***особливостей алгоритму роботи вірусів*** виділяють і:

- *резидентність,*
- *самошифрування і поліморфічность,*
- *використання нестандартних прийомів.*

Резидентний вірус при інфікуванні комп'ютера залишає в оперативній пам'яті свою резидентну частину, яка потім перехоплює звертання операційної системи до об'єктів зараження і впроваджується в них. Резидентні віруси знаходяться в пам'яті і є активними аж до вимикання комп'ютера або перезавантаження операційної системи.

Нерезидентні віруси не заражають пам'ять комп'ютера і зберігають активність обмежений час. Резидентними можна вважати макровіруси, оскільки вони постійно присутні в пам'яті комп'ютера. При цьому роль операційної системи бере на себе відповідний редактор, а поняття «перезавантаження операційної системи» трактується як вихід з редактора.

Самошифрування і поліморфічность використовуються практично всіма типами вірусів для того, щоб максимально ускладнити процедуру детектування вірусу.

Полиморфні віруси - це віруси, що не мають сигнатур, тобто що не містять жодного постійної ділянки коду. У більшості випадків два зразки того самого поліморфні вірусу не матимуть жодного збігу. Це досягається шифруванням основного тіла вірусу і модифікаціями програми-розшифровщика.

За особливостями алгоритму віруси важко класифікувати через велику їх різноманітності.

За деструктивними можливостями віруси можна розділити на:

1. *нешкідливі*, тобто ніяк що не впливають на роботу комп'ютера, крім зменшення вільної пам'яті на диску в результаті свого поширення;

2. *безпечні*, тобто не заважають роботі комп'ютера. Їх вплив обмежується зменшенням вільної пам'яті на диску і графічними, звуковими та іншими ефектами;

3. *небезпечні віруси*, які можуть привести до серйозних збоїв у роботі комп'ютера. В алгоритм їх роботи закладено процедури, які можуть привести до втрати програм, знищити дані, стерти необхідну для роботи комп'ютера інформацію, записану в системних областях пам'яті, і навіть, сприяти виведенню з ладу рухомих частин механізмів - вводити в резонанс і руйнувати голівки деяких типів жорстких дисків. Існують інші підходи в класифікації вірусів.

Найпростіші віруси змінюють вміст файлів і можуть бути легко виявлені і знищені. Можна відзначити *віруси-хробаки*, які поширюються по комп'ютерних мережах. Відомі *віруси-невидимки*, так звані *стелс-віруса*, які дуже важко виявити і знешкодити, оскільки вони перехоплюють звернення операційної системи до уражених файлів і секторів дисків і підставляють замість свого тіла незаражені ділянки диска. Найбільш важко знайти *віруси-мутанти*, що містять алгоритми шифрування-розшифрування, завдяки яким копії одного і того ж вірусу не мають ні одного однакового ланцюжка байтів. Є й так звані *квазівірусні*, або *«троянські»* програми, які хоч і не здатні до самопоширення, але дуже небезпечні, оскільки, маскуючись під корисну програму, руйнують завантажувальний сектор і файлову систему дисків.

На практиці віруси поділяють на три класи:

1. *Програми, які «заражають» інші програми*, модифікуючи їх таким чином, щоб «заражені» містили копію вірусу. Такий вірус може вважатися чимось на зразок доданого до програми модуля.

2. *Хробаки* - це програми, які можуть самостійно переноситися від одного комп'ютера до іншого, а, отже, «розмножуватися».

3. *Троянські коні* - це самостійні програми, які маскуються під корисні.

Програми виявлення і захисту від вірусів

Для виявлення, видалення і захисту від комп'ютерних вірусів розроблено декілька видів спеціальних програм, які дозволяють виявляти і знищувати віруси. Такі програми називаються ***антивірусними*** . Відповідно до виконуваних функцій розрізняють такі види антивірусних програм:

- *програми-детектори;*
- *програми-доктора або фаги;*
- *програми-ревізори;*
- *програми-фільтри;*
- *програми-вакцини, або іммунізатори.*

Програми-детектори здійснюють пошук характерної для конкретного вірусу сигнатури в оперативній пам'яті й у файлах і при виявленні видають відповідне повідомлення. Програми-детектори дозволяють виявляти файли, заражені одним з декількох відомих вірусів.

Лікувальні програми або фаги , а також ***програми-вакцини*** не тільки знаходять заражені вірусами файли, але і «лікують» їх, тобто видаляють з файлу тіло програми-вірусу, повертаючи файл в початковий стан. На початку своєї роботи фаги

шукають віруси в оперативній пам'яті, знищують їх, і тільки потім переходять до лікування файлів. Враховуючи, що постійно з'являються нові віруси, програми-детектори і програми-доктори швидко застарівають і вимагають регулярного оновлення.

Програми-ревізори - це самі надійні засоби захисту від вірусів. Вони запам'ятовують початковий стан програм, каталогів і системних областей диска тоді, коли комп'ютер не заражений вірусом, а потім порівнюють поточний стан з вихідним. Виявлені зміни виводяться на екран. Зазвичай порівняння станів вони виконують після завантаження операційної системи. При порівнянні перевіряються довжина файлу, код циклічного контролю (контрольна сума), дата і час модифікації та інші параметри.

Програми-фільтри - це невеликі резидентні програми, призначені для виявлення характерних для вірусів дій при роботі комп'ютера. Такими діями можуть бути: спроби корекції файлів з розширенням *com, exe;* зміна атрибутів файлу; прямий запис на диск по абсолютному адресою; запис в завантажувальні сектори диску; завантаження резидентної програми та ін.

Існує досить багато програмних засобів антивірусного захисту. Сучасні антивірусні програми складаються з модулів:

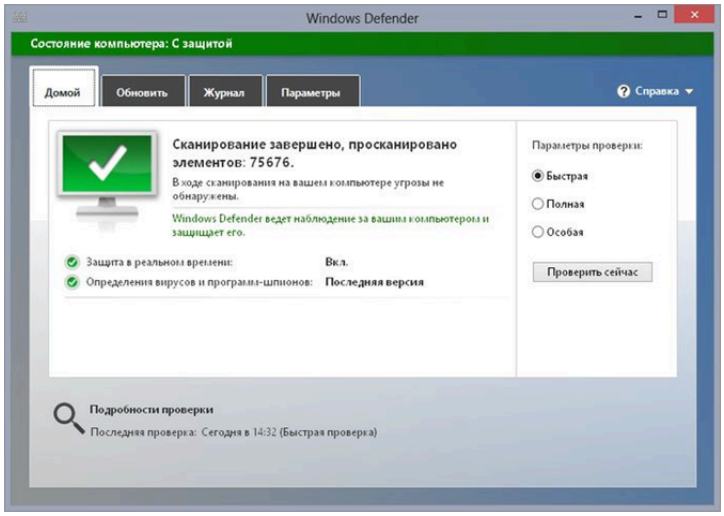
1. *Евристичний модуль* - для виявлення невідомих вірусів
2. *Монітор* - програма, яка постійно знаходиться в оперативній пам'яті ПК
3. *Пристрій управління* , яке здійснює запуск антивірусних програм і оновлення вірусної бази даних і компонентів
4. *Поштова програма* (перевіряє електронну пошту)
5. *Програма сканер* - перевіряє, виявляє і видаляє фіксований набір відомих вірусів в пам'яті, файлах і системних областях дисків
6. *Мережевий екран* - захист від хакерських атак

До найбільш ефективним і популярним антивірусним програмам ставляться: *Антивірус Касперського, AVAST* і багато інших.

Windows Defender - вбудований антивірус Windows

Windows Defender - це антивірусна програма, яка була розроблена компанією Microsoft. Сам Windows Defender представляє собою повноцінний антивірус, створений на базі Microsoft Security Essentials і здатний захистити від більшості сучасних загроз. Windows Defender можна було помітити в деяких версіях Windows 7, але там він виконував тільки пасивну роль захисту від вірусів і працював у вигляді антивірусного сканера. Щодо нової версії Windows 8, то тут він вже здатний працювати в реальному часі і виконувати активний захист комп'ютера. В Windows 8, Defender або українською мовою Захисник Windows запускається зразу ж після старту системи, що дає користувачам можливість використовувати його в якості основного захисту комп'ютера і при цьому обійтися без придбання інших антивірусних програм.

Windows Defender - не просто сканер системи, як інші подібні безкоштовні програми. До нього входить ряд модулів безпеки, що відслідковують підозрілі зміни в певних сегментах системи в режимі реального часу.


Windows Defender
Состояние компьютера: С защитой
Домой
Обновить
Журнал
Параметры
Справка
Сканирование завершено, просканировано элементов: 75676.
В ходе сканирования на вашем компьютере угрозы не обнаружены.
Windows Defender ведет наблюдение за вашим компьютером и защищает его.
Защита в реальном времени: Вкл.
Определения вирусов и программ-шпионов: Последняя версия
Параметры проверки:
Быстрая
Полная
Особая
Проверить сейчас
Подробности проверки
Последняя проверка: Сегодня в 14:32 (Быстрая проверка)