*Глосарій (словник термінів) до теми:*

***Поняття комп’ютерного вірусу. Антивірусні програми***

**Комп’ютерний вірус** - невелика програма, здатна до саморозмноження і виконання деструктивних дій.

**Пасивна фаза** вірусу – вірус перебуває в стані спокою, не чинить ніяких шкідливих дій. (тривалість від декількох секунд до декількох років)

**Активна фаза** вірусу – вірус проявляє себе, чинить шкідливі дії.

**Резидентний вірус** — при інфікуванні комп'ютера залишає в оперативній пам'яті свою резидентну частину, що потім перехоплює звернення операційної системи до об'єктів зараження й впроваджується в них (перебувають у пам'яті і є активними аж до вимикання або перезавантаження комп'ютера).

**Нерезидентні** **віруси** — не заражають пам'ять комп'ютера і є активними обмежений час. Деякі віруси залишають в оперативній пам'яті невеликі резидентні програми, які не поширюють вірус.

**Звичайні віруси** — код вірусу можна побачити на диску.

**Поліморфні** – код вірусу видозмінюється.

**Невидимі** **віруси** — використовують особливі засоби маскування і при перегляді коду вірусу не видно.

**«Компаньйони-віруси»** — це віруси, що не змінюють файли. Алгоритм роботи цих вірусів полягає в тому, що вони створюють для ЕХЕ-файлів файли-супутники, що мають те саме ім'я, але з розширенням .СОМ

**«Віруси-хробаки»**— віруси, які поширюються в комп'ютерній мережі. Вони проникають у пам'ять комп'ютера з комп'ютерної мережі, встановлюють мережеві адреси інших комп'ютерів і розсилають по цих адресах свої копії;

**«Макро-віруси»** — віруси цього сімейства використовують можливості макро-мов, вбудованих у системи обробки даних (текстові редактори, електронні таблиці й т.д.).

**«Троянські програми»** — виконують шкідливі дії замість оголошених легальних функцій або разом з ними. Вони не спроможні до самовідтворення і передаються тільки при копіюванні користувачем. Після запуску вони зазвичай знищують себе разом з іншими файлами на диску.

**Детектори** – антивірусні програми, які перевіряють оперативну або зовнішню пам'ять на наявність вірусу за допомогою розрахованої контрольної суми або сигнатури (частина коду, що повторюється) і складають список ушкоджених програм.

**Фаги** – антивірусні програми, які виявляють та знешкоджують вірус (фаг) або кілька вірусів.

**Ревізори** – антивірусні програми, що контролюють можливі засоби зараження комп'ютера, тобто вони можуть виявити вірус, невідомий програмі.

**Монітори** – антивірусні резидентні програми, які постійно зберігаються у пам'яті й у визначений користувачем час перевіряють оперативну пам'ять комп'ютера (включаючи додаткову та розширену), файли, завантажувальний сектор, FAT-таблицю.