**Тема: "Комп′ютерні віруси та програми антивіруси"**

Вірус - це комп′ютерна програма, яка виконує несанкціоновані дії у комп′ютері.

**За результатами впливу на комп′ютер** віруси поділяються на безпечні та небезпечні. Безпечні віруси уповільнюють роботу комп′ютеру, ведуть до зависань, виводять на екран свої повідомлення але не руйнують файлову систему. Небезпечні віруси можуть повністю зруйнувати інформацію на дисках.

**За способами зараження** віруси бувають файлові, завантажувальні і мережні.

**Файлові** приєднуються до тіла програми (до виконавчого файлу) і при завантаженні програми в оперативну пам′ять крім означених несанкціонованих дій вони створюють в ОЗП свої копії, яки будуть заражати будь-який програмний файл, завантажений в оперативну пам′ять в поточному сеансі роботи.

**Завантажувальні** віруси заражають завантажувальний запис – невелику програму, яка знаходиться на 0-й доріжці першого сектору системного диску і завантажується в оперативну пам′ять при вмиканні комп′ютеру.

**Мережні** віруси потрапляють на комп′ютер через комп′ютерну мережу Internet. До мережних вірусів відносять хробаків і троянських коней.

**Хробаки** після потрапляння на комп′ютер надають контроль над зараженим комп′ютером користувачу в комп′ютерній мережі, який його активізував.

**Троянські коні** (віруси-вандали) – це віруси, яки замасковані під звичайні програми і після активізації у зараженому комп′ютері відразу починають руйнацію файлової системи.

**За спосібом організації** віруси бувають: звичайні, поліморфні, невидимки (stelth), макровіруси.

**Звичайні** – вони приєднуються до тіла програми, збільшуючи її розмір.

**Поліморфні** –вони завдяки спеціальним алгоритмам кодування і шифрації змінюють кодові сигнатури свого тіла. Не існує двох абсолютно однакових копій такого вірусу.

**Вірус-невидимка (stelth-вірус)** – при спробі програми-антивірусу визначити тип вірусу по його кодовим сигнатурам такий вірус замість своїх сигнатур підставляє незаражені сигнатури зараженої програми.

**Макровірус** заражає документи редактору Word. Такий вірус створюється на мові Visual Basic Aplication (VBA) у вигляді звичайного макросу – невеликої підпрограми, яка при розкритті документу може проводити його автоматичне опрацювання.

Вірус "Чорнобиль" (WIN95.CIH) – небезпечний файловий звичайний вірус. Він спрацьовує 26 квітня (дата вибуху на Чорнобильській АЕС). Він руйнує всі exe-файли, а також намагається перезаписати BIOS і форматує перший Мб жорсткого диску (в ньому розміщені FAT-таблиці файлової системи).

Вірус "One half" (одна половина) – небезпечний файловий вірус. Форматує одну половину вінчестера.

"Восток – дело тонкое" – небезпечний вірус.

Melisa – макровірус, руйнує інформацію документа редактора Word.

**Програми-антивіруси**

Існує два методи пошуку вірусних програм: 1) по вірусним сигнатурам і 2) по результатам дій вірусної програми (емпіричний пошук)

До цих програм відносять детектори (ревізори), лікарі (фаги), сканери і фільтри.

**Детектори (ревізори)** мають у своєму складі базу даних вірусних сигнатур, за порівнянням з якими відбувається встановлення типу вірусу. Необхідно постійно оновлювати антивірусні бази вірусних сигнатур.

**Лікарі (фаги) –** лікують програми від вірусів. В останній час з′явилися антивірусні програми з властивостями детекторів і лікарів – **поліфаги. (AVP Касперського), DrWeb (Доктор Weber)**

**Сканери** - запам′ятовують стан всіх файлів і системних областей системи (їхні контрольні суми) і реагують на будь-яку нештатну зміну цих даних.

**Фільтри** – завантажуються в ОЗП резидентно і на самому першому етапі завантаження будь-якої програми перевіряють її на наявність тих звертань до операційної системи, які використовують віруси. Недолік таких програм: велике уповільнення роботи комп′ютеру. Проте її слід використовувати при роботі з мережею Internet/

**Засоби боротьби з вірусами:**

1. Регулярно перевіряти жорсткі диски свого комп′ютеру.
2. Перевіряти будь-яки чужі гнучкі диски та Flash-пам'ять USB.
3. Використовувати тільки ліцензійне ПЗ.
4. Постійно оновлювати антивірусні бази вірусних сигнатур.
5. На залишати гнучкі диски у дисководі.
6. При роботі у мережі Internet застосовувати антивіруси-фільтри.
7. У випадку застосування файлової системи FAT під час форматування диску переносити другу копію FAT-таблиці у останні сектори диску (це захист від вірусу "Чорнобиль")