

Комп'ютерні віруси



Комп'ютерний вірус - це 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.

- Потрапляючи на комп'ютер, вірус може створювати свої копії, поширюватися, впроваджуючи себе в інші програми, або замінювати їх.
- Комп'ютерні віруси можуть призвести до псування або видалення інформації, передачі конфіденційних або персональних даних злоумисникам по мережі Інтернет. Можливі збої в роботі програм або самої операційної системи (аж до приведення операційної системи в повну непрацездатність).

Класифікація вірусів

- **Файлові віруси**—проникають у файли, що виконуються (exe, com, bat), у системні файли, файли драйверів (sys, drv, vxd), файли бібліотек (DLL), а також у ряд інших типів файлів. Після вкорінення файлові віруси починають розмножуватися під час кожного запуску файла.
- **Завантажувальні віруси** – заражають завантажувальний сектор диска (Boot сектор) або сектор, що містить програму системного завантажувача вінчестера (Master Boot Record). Такий вірус заміщає собою програму в завантажувальному секторі, внаслідок цього потрапляє до оперативної пам'яті й перехоплює керування відразу під час завантаження операційної системи.
- **Файлово-завантажувальні віруси** можуть проникати як у файли, такі в завантажувальні сектори. До таких вірусів належать, зокрема, стелс-віруси і найнебезпечніші екземпляри поліморфних вірусів.
- **Макровіруси** проникають у файли документів (пакет Microsoft Office) й інші файли, підготовлені в додатках, що мають свою мову макрокоманд. Формально ці віруси є файловими, але заражають вони не файли, що виконуються, а файли даних. Небезпека макровірусів не стільки в їхній руйнівній дії, скільки в поширеності документів, підготовлених у популярних системах Word і Excel.
- **Мережні віруси** поширюються по комп'ютерній мережі. Особливість цих вірусів полягає в тому, що вони заражають тільки оперативну пам'ять комп'ютерів і не записуються на носії інформації.



Основними ознаками зараження комп'ютера вірусом є:

- 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.

Щоб уникнути зараження вірусами, слід дотримуватися деяких правил:

- ❑ Не працювати під привілейованими обліковими записами без крайньої необхідності.
- ❑ Не запускати незнайомі програми з сумнівних джерел.
- ❑ Намагатися блокувати можливість несанкціонованої зміни системних файлів.
- ❑ Відключати потенційно небезпечний функціонал системи (наприклад autorun носіїв у MS Windows, приховування файлів, їх розширень і пр.).
- ❑ Не заходити на підозрілі сайти, звертати увагу на адресу в адресному рядку браузера.
- ❑ Користуватися тільки довіреними дистрибутивами.
- ❑ Постійно робити резервні копії важливих даних і мати образ системи з усіма налаштуваннями для швидкого розгортання.
- ❑ Виконувати регулярні оновлення часто використовуваних програм та безпеки системи.



Дякую за увагу!