

# Шкідливі програми, їх типи, принципи дії і боротьба з ними



# Шкідлива програма —

комп'ютерна програма або переносний код, призначений для реалізації загроз даним, що зберігаються в інформаційній системі, або для прихованого нецільового використання ресурсів системи, або іншої дії, що перешкоджає нормальному функціонуванню інформаційної системи.



# Комп'ютерні віруси —

це спеціальні програми в машинних кодах або фрагменти програм, здатні без відома та згоди користувача розмножуватися й розповсюджуватися на інші програми шляхом копіювання свого коду у файли, що зберігаються в системі.



# «Симптоми» зараження комп'ютера вірусом:

- ✓ часті зависання і збої в роботі комп'ютера;
- ✓ повільна робота комп'ютера при запуску програм;
- ✓ неможливість завантаження операційної системи;
- ✓ зникнення файлів і папок або спотворення їхнього вмісту;
- ✓ часте звернення до жорсткого диска (часто блимає лампочка на системному блоці);
- ✓ браузер зависає або поводиться несподіваним чином (наприклад, вікно програми неможливо закрити).



**Мережеві віруси** для свого розповсюдження використовують можливості комп'ютерних мереж.



**Хробаки** — це один з різновидів шкідливих вірусів, що розмножуються та псують дані, збережені на комп'ютері.



## **«Троянський кінь»**

розповсюджуються шляхом обману,  
вони запускаються під виглядом  
іншої програми для отримання  
важливих даних.



# КОМП'ЮТЕРНІ ВІРУСИ ЗА ОБ'ЄКТАМИ ЗАРАЖЕННЯ

Файлові

Макровіруси

Завантажувальні

Віруси структури  
файлової системи



# Класифікація за зовнішнім ВИГЛЯДОМ:

- звичайні;
- невидимі (Stealthвіруси) ;
- поліморфні.

# Засоби захисту та безпечної роботи на комп'ютері

# Брандмауери (або міжмережеві екрани) —

окремі пристрої чи спеціальні програми, які для захисту створюють бар'єр між комп'ютером і мережею.



# Антивіруси

призначені для виявлення та лікування програм і файлів, що заражені комп'ютерним вірусом, а також для запобігання зараженню файлів вірусами.





# АНТИВІРУСНІ ПРОГРАМИ

Сканери

Ревізори

Монітори

Вакцини

Лікарі

# Резервна копія —

копія окремих файлів, групи файлів або всього диска, що збережена на іншому носії, для наступного відновлення в разі руйнувань, псування або втрати даних на основному носії.



## Типи резервних копій:

- резервна копія операційної системи;
- резервна копія логічного диска (розділу);
- резервна копія окремих файлів і папок.

# **Яких правил доцільно дотримуватися для безпечної роботи в інтернеті?**

- необхідно використовувати надійні джерела програмного забезпечення для свого комп'ютера, купувати його лише в офіційних продавців;
- перевіряти за допомогою антивірусних програм файли, які надходять ззовні (з дисків, Інтернету) до вашого комп'ютера;
- обмежити доступ сторонніх осіб до комп'ютера;
- регулярно створювати резервні копії важливих даних;
- періодично перевіряти комп'ютер на наявність вірусів з використанням нових версій антивірусних програм;
- не відкривати вкладення електронної пошти, які були надіслані від невідомих вам адресатів;
- не завантажувати з Інтернету файли з розширенням exe з неперевірених сайтів.



# **Способи боротьби зі спамом:**

- Не варто без необхідності публікувати адресу електронної пошти на веб-сайтах чи в групах новин.
- Не потрібно реєструватися на підозрілих сайтах. Якщо деякий корисний сайт вимагає реєстрації, можна вказати спеціально для цього створену адресу.
- Ніколи не відповідати на спам і не переходити за посиланнями, які містяться в ньому. Цим ви тільки підтвердите, що користуєтеся своєю електронною адресою й будете одержувати ще більше спаму.
- Вибираючи ім'я для своєї електронної пошти, варто, за можливості, щоб воно було довгим й незручним для вгадування.