**Комп’ютерні віруси**

1. ***Що таке комп’ютерний вірус***
2. ***Класифікація вірусів***
3. ***Ознаки зараження вірусом***
4. ***Шляхи проникнення вірусів на комп'ютер***
5. ***Запобіжні заходи***

[](https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B8%D0%B9_%D0%B2%D1%96%D1%80%D1%83%D1%81)**Що таке комп’ютерний вірус**

Комп'ютерний вірус - різновид комп'ютерних програм або шкідливий код, відмінною особливістю якого є здатність до розмноження (самореплікація). На додаток до цього віруси можуть без відома користувача виконувати інші довільні дії, в тому числі завдають шкоди користувачеві і/або комп'ютеру.

Навіть якщо автор вірусу не програмував шкідливих ефектів, вірус може призводити до збоїв комп'ютера через помилки, неврахованих тонкощів взаємодії з операційною системою і іншими програмами. Крім того, віруси зазвичай займають деяке місце на накопичувачах інформації і відбирають деякі інші ресурси системи. Тому віруси відносять до шкідливих програм.

Некомпетентні користувачі помилково відносять до комп'ютерних вірусів і інші види шкідливих програм - програми-шпигуни та інше. Відомі десятки тисяч комп'ютерних вірусів, які поширюються через Інтернет по всьому світу.

**Класифікація вірусів**

Нині існує чимало різновидів вірусів, що розрізняються за основним способом розповсюдження і функціональності. Якщо спочатку віруси поширювалися на дискетах та інших носіях, то зараз домінують віруси, що розповсюджуються через Інтернет. Зростає і функціональність вірусів, яку вони переймають від інших видів програм.

В даний час не існує єдиної системи класифікації і іменування вірусів (хоча спроба створити стандарт була зроблена на зустрічі CARO у 1991 році). Прийнято розділяти віруси:

* по заражених об'єктах (файлові віруси, завантажувальні віруси, скриптові віруси, макровіруси, віруси, що вражають вихідний код);
* по уражаємим операційним системам і платформам (DOS, Microsoft Windows, Unix, Linux);
* за технологіями, використовуваними вірусом (поліморфні віруси, стелс-віруси, руткіти);
* за мовою, на якій написано вірус (асемблер, високорівнева мова програмування, скриптова мова та ін);
* по додатковій шкідливої ​​функціональності (бекдори, кейлоггери, шпигуни, ботнети та ін).

**Ознаки зараження вірусом**

Існує ряд ознак, які можуть слугувати ознакою зараження вірусом: поява на екрані непередбачених повідомлень і запитів, зображень і звукових сигналів; мимовільний запуск програм без участі користувача; спроби невідомих програм підключитися до Інтернету без відома користувача і т. п. Про ураження вірусом через пошту може свідчити те, що друзі та знайомі користувача говорять про повідомлення від нього, які він не відправляв; наявність в поштовій скриньці великої кількості повідомлень без зворотної адреси і заголовків. Однак ці ознаки не завжди є наслідком присутністю вірусів. Наприклад, у випадку з поштою заражені повідомлення можуть розсилатися із зворотною адресою користувача з інших комп'ютерів.

Серед непрямих ознак можна назвати часті зависання і збої в роботі комп'ютера, уповільнена (порівняно з початковим поведінкою) робота комп'ютера при запуску програм, неможливість завантаження операційної системи, зникнення файлів і каталогів чи спотворення їх вмісту, часте звернення до жорсткого диску (часто блимає лампочка на системному блоці), браузер Internet Explorer «зависає» чи поводиться несподіваним чином (наприклад, вікно програми неможливо закрити). Але основною причиною для подібних симптомів є все ж таки не віруси, а збої в апаратному забезпеченні, конфлікти між програмами і баги («жучки», дефекти) у них.

**Шляхи проникнення вірусів на комп'ютер**

Віруси розповсюджуються, копіюючи своє тіло і забезпечуючи його подальше виконання: впроваджуючи себе у виконуваний код інших програм, замінюючи собою інші програми, прописуючись в автозапуск та інше. Вірусом або його носієм можуть бути не тільки програми, що містять машинний код, але і будь-яка інформація, що містить автоматично виконувані команди - наприклад, пакетні файли і документи Microsoft Word і Excel, що містять макроси. Крім того, для проникнення на комп'ютер вірус може використовувати уразливості в популярному програмному забезпеченні (наприклад, Adobe Flash, Internet Explorer, Outlook), для чого розповсюджувачі впроваджують його в звичайні дані (картинки, тексти і т. д.) разом з експлоїтом, що використовує вразливість.

**Запобіжні заходи**

На даний момент існує безліч антивірусних програм, що використовуються для запобігання попадання вірусів в ПК. Однак немає гарантії, що вони зможуть впоратися з новітніми розробками. Тому слід дотримуватися деяких запобіжних заходів, зокрема:

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