**Діана Данилюк**
студентка 1 курсу спеціальності «Ветеринарна медицина»
Науковий керівник: **Цвігун І.А.**
д.е.н., доцент, завідувач кафедри інформаційних технологій
Подільський державний аграрно-технічний університет
м. Кам`янець-Подільський

# КЛАСИФІКАЦІЯ ШКІДЛИВИХ ПРОГРАМ

Шкідлива програма - комп'ютерна програма або переносний код, призначений для реалізації загроз інформації, що зберігається в комп'ютерній системі, або для прихованого нецільового ресурсів системи, або іншої дії, що перешкоджає нормальному функціонуванню комп'ютерної системи.

Для шкідливих комп’ютерних програм характерно:

- швидке розмноження шляхом приєднання своїх копій до інших програм, копіювання на інші носії даних, пересилання копій комп’ютерними мережами;
- автоматичне виконання деструктивних дій, які вносять дезорганізацію в роботу комп’ютера:
- знищення даних шляхом видалення файлів певних типів або форматування дисків;
- внесення змін у файли, зміна структури розміщення файлів на диску;
- зміна або повне видалення даних із постійної пам’яті;
- зниження швидкодії комп’ютера, наприклад за рахунок заповнення оперативної пам’яті своїми копіями;
- постійне (резидентне) розміщення в оперативній пам’яті від моменту звернення до ураженого об’єкта до моменту вимкнення комп’ютера, і ураження все нових і нових об’єктів;
- примусове перезавантаження операційної системи;
- блокування запуску певних програм;

•збирання і пересилання копії даних комп'ютерними мережами, наприклад пересилання кодів доступу до секретних даних;

•використання ресурсів уражених комп'ютерів для організації колективних атак на інші комп'ютери в мережах;

•виведення звукових або текстових повідомлень, спотворення зображення на екрані монітора тощо.

За рівнем небезпечності дій шкідливі програми розподіляють на:

•**безпечні** – проявляються відео та звуковими ефектами, не змінюють файлову систему, не ушкоджують файли і не виконують шпигунські дії;

•**небезпечні** – призводять до перебоїв у роботі комп'ютерної системи: зменшують розмір доступної оперативної пам'яті, перезавантажують комп'ютер тощо;

•**дуже небезпечні** – знищують дані з постійної та зовнішньої пам'яті, виконують шпигунські дії тощо.

**За принципами розповсюдження і функціонування** шкідливі програми розподіляють на (рис. 1):

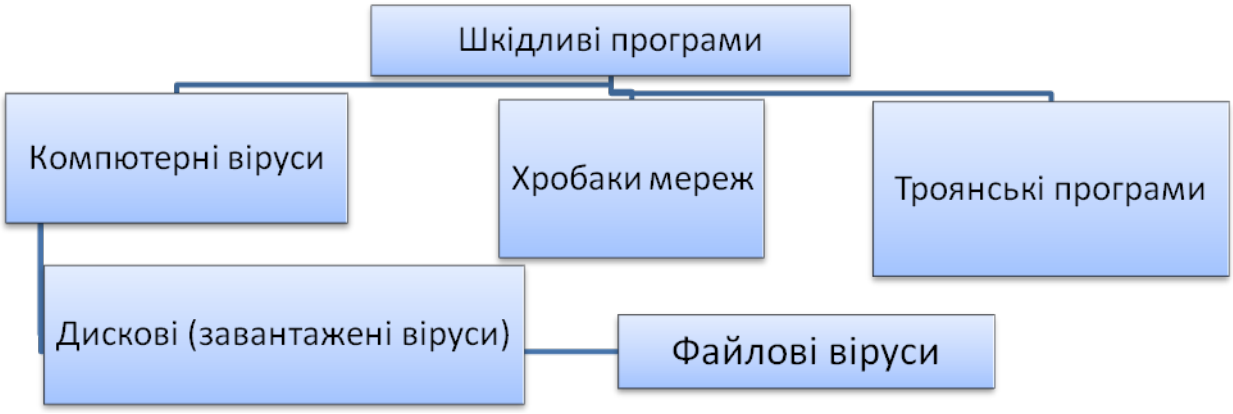


Рис.1. Схема класифікації шкідливих програм за принципами розповсюдження і функціонування

• ***комп'ютерні віруси*** – програми, здатні саморозмножуватися і виконувати несанкціоновані деструктивні дії на ураженому комп'ютері. Серед них виділяють:

•дискові (завантажувальні) віруси – розмножуються копіюванням себе в службові ділянки дисків та інших змінних носіїв, яке відбувається під час спроби користувача зчитати дані з ураженого носія;

•файлові віруси – розміщують свої копії у складі файлів різного типу. Як правило, це файли готових до виконання програм із розширенням імені exe або com. Однак існують так звані макровіруси, що уражують, наприклад, файли текстових документів, електронних таблиць, баз даних тощо;

•***хробаки (черв'яки) комп'ютерних мереж*** – пересилають свої копії комп'ютерними мережами з метою проникнення на віддалені комп'ютери. Більшість черв'яків поширюються, прикріпившись до файлів електронної пошти, електронних документів тощо. З ураженого комп'ютера хробаки намагаються проникнути на інші комп'ютери, використовуючи список електронних поштових адрес або іншими способами. Крім розмноження, черв'яки можуть виконувати деструктивні дії, які характерні для шкідливих програм;

•***троянські програми***– програми, що проникають на комп'ютери користувачів разом з іншими програмами, які користувач «отримує» комп'ютерними мережами. Шкідливі програми він отримує «в подарунок», так як у свій час захисники Трої отримали в подарунок від греків дерев'яного коня, всередині якого розміщалися грецькі воїни. Звідси й назва цього виду шкідливих програм. Як і інші шкідливі програми, троянські програми можуть виконувати зазначені вище деструктивні дії, але в основному їх використовують для виконання шпигунських дій.

Значна частина шкідливих програм у початкові періоди зараження не виконують деструктивних дій, а лише розмножуються. Це так звана пасивна фаза їхнього існування. Через певний час, у визначений день або по команді з комп'ютера в мережі шкідливі програми починають виконувати деструктивні дії – переходять в активну фазу свого існування.

Серед вірусів виділяють ті, що використовують спеціальні способи приховування своїх дій і знаходження в операційній системі комп'ютера:

•***поліморфні (мутанти)*** – віруси, які при копіюванні змінюють свій вміст так, що кожна копія має різний розмір; їх важче визначити, використовуючи пошук за відомою довжиною коду вірусу;

•***стелс*** (англ. stealth – хитрість, викрут, stealth virus – вірус (невидимка) – віруси, що намагаються різними засобами приховати факт свого існування в операційній системі. Наприклад, замість дійсного об’єкта, ураженого вірусом, антивірусній програмі надається для перевірки його неуражена копія.

## Список використаних джерел

1. Алексєєв О.П. Інформатика.Київ: «Солон», 2002. 280 с.

2. Безруков М.М. Комп'ютерні віруси. Москва: Наука, 1991. 312 с.

3. Горнец М.М. Організація ЕОМ і систем: навчальних посібник. Москва: Академія, 2006. 320 с.

4. Руденко В.Д. та ін. Базовий курс інформатики; за заг. ред. В.Ю.Бикова: Київ: Вид. група BHV. Кн. 1: Основи інформатики, 2005. 320 с.

5. Руденко В.Д. та ін. Базовий курс інформатики; за заг. ред. В.Ю.Бикова. Київ: Вид. група BHV. Кн. 2: Інформаційні технології, 2006. 368 с.