01, 02.10.24 **9 клас** **Вчитель: Артемюк Н.А.**

Тема. Шкідливе програмне забезпечення та боротьба з ним

Очікувані результати заняття

Після цього заняття потрібно вміти:

- називати основні типи шкідливих програм;
- пояснювати принцип дії шкідливих програм певного типу.

Поміркуйте

- що входить до програмного забезпечення комп'ютера?
- які види програмного забезпечення ви знаєте? Наведіть приклади.
- які типи файлів ви знаєте?
- що таке виконувані файли?

Ознайомтеся з інформацією

Комп'ютерний вірус - це невелика програма, що написана програмістом високої кваліфікації, здатна до саморозмноження й виконання різних деструктивних дій.

Віруси діють тільки програмним шляхом. Вони, як правило, приєднуються до файлу або проникають всередину файлу. У цьому випадку кажуть, що файл заражений вірусом. Вірус потрапляє в комп'ютер тільки разом із зараженим файлом. Для активізації вірусу потрібно завантажити заражений файл, і тільки після цього вірус починає діяти самостійно. Деякі віруси під час запуску зараженого файлу стають резидентними (постійно знаходяться в оперативній пам'яті комп'ютера) і можуть заражати інші файли та програми, що завантажуються. Інші різновиди вірусів відразу після активізації можуть спричиняти серйозні пошкодження, наприклад, форматувати жорсткий диск.

Дія вірусів може проявлятися по різному: від різних візуальних ефектів, що заважають працювати, до повної втрати інформації. Більшість вірусів заражують виконавчі програми, тобто файли з розширенням .EXE та .COM, хоча останнім часом все більшої популярності набувають віруси, що розповсюджуються через сервіси обміну повідомленнями.

Класифікація вірусів

1. *завантажувальні віруси* або *BOOT-віруси*: заражають boot-сектори дисків. Дуже небезпечні, можуть призвести до повної втрати всієї інформації, що зберігається на диску;
2. *файлові віруси:* заражають файли. Поділяються на:
    1. віруси, що заражують програми (файли з розширенням .EXE і .COM);
    2. макровіруси: віруси, що заражують файли даних, наприклад, документи Word або робочі книги Excel;
    3. віруси-супутники: використовують імена інших файлів;
    4. віруси сімейства DIR: спотворюють системну інформацію про файлові структури;
3. *завантажувально-файлові віруси:* здатні вражати як код boot-секторів, так і код файлів;

4. *віруси-невидимки* або *STEALTH-віруси*: фальсифікують інформацію прочитану з диска так, що програма, якій призначена ця інформація отримує невірні дані. Ця технологія, яку, інколи, так і називають Stealth-технологією, може використовуватися як в BOOT-вірусах, так і у файлових вірусах;
5. *ретровіруси:* заражують антивірусні програми, намагаючись знищити їх або зробити непрацездатними;
6. *віруси-хробаки:* заражують невеликі повідомлення електронної пошти, так званим заголовком, який по своїй суті є всього навсього лише Web-адресою місцезнаходження самого вірусу. При спробі прочитати таке повідомлення вірус починає зчитувати через глобальну мережу Internet своє 'тіло', яке після завантаження починає свою деструктивну дію. Дуже небезпечні, так як виявити їх дуже важко у зв'язку з тим, що заражений файл фактично не містить коду вірусу.

З прикладами вірусних програм можна ознайомитися на сайті **Української антівірусної лабораторії**, на сторінці **Вірусна енциклопедія** за адресою https://zillya.ua/virus/all.

Перегляньте відео

https://youtu.be/Ic7RgwANz1k

Запитання до відео

- Коли та як з’явився перший комп’ютерний вірус?
- Як може відбуватись зараження комп’ютера вірусом?

Виконайте вправу

https://wordwall.net/uk/resource/24900246

Завдання

Перегляньте інформацію та зробіть конспект за темою уроку

Джерело

Мій клас