30.09.22 9 клас

Тема. Шкідливе програмне забезпечення та боротьба з ним. Антивірусні та антишпигунські програми

Мета: ознайомитися з основними типами шкідливих програм та навчитися пояснювати принцип їх дії; навчитися застосовувати антивірусну програму для захисту комп'ютерного пристрою від інформаційних загроз, налаштовувати параметри антивірусної програми.

Повторюємо

дайте відповіді на запитання (усно)

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

Перегляньте відеоурок за посиланням:

https://youtu.be/Ic7RgwANz1k

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.

Антивірус - це програма, яка виявляє й знешкоджує комп'ютерні віруси. Антивірусні програми можуть виявляти та знищувати лише відомі віруси, при появі нового комп'ютерного вірусу захисту від нього не існує до тих пір, поки для нього не буде розроблено свій антивірус. Однак, багато сучасних антивірусних пакетів мають у своєму складі спеціальний програмний модуль, який називається евристичний аналізатор, і який здатний досліджувати вміст файлів на наявність коду, характерного для комп'ютерних вірусів. Це дає змогу вчасно виявляти та попереджати про небезпеку зараження новим вірусом.

Розрізняють такі **типи антивірусних програм**:

1. *програми-детектори*: призначені для знаходження заражених файлів одним із відомих вірусів. Деякі програми-детектори можуть також лікувати файли від вірусів або знищувати заражені файли. Існують спеціалізовані (тобто призначені для боротьби з одним вірусом) детектори та поліфаги (можуть боротися з багатьма вірусами);
2. *програми-лікарі*: призначені для лікування заражених дисків і програм. Лікування програми полягає у вилученні із зараженої програми тіла вірусу. Також можуть бути як поліфагами, так і спеціалізованими;
3. *програми-ревізори*: призначені для виявлення зараження вірусом файлів, а також знаходження ушкоджених файлів. Ці програми запам'ятовують дані про стан програми та системних областей дисків у нормальному стані (до зараження) і порівнюють ці дані у процесі роботи комп'ютера. В разі невідповідності даних виводиться повідомлення про можливість зараження;
4. *лікарі-ревізори*: призначені для виявлення змін у файлах і системних областях дисків й у разі змін повертають їх у початковий стан.
5. *програми-фільтри*: призначені для перехоплення звернень до операційної системи, що використовуються вірусами для розмноження і повідомляють про це користувача. Останній має можливість дозволити або заборонити виконання відповідної операції. Такі програми є резидентними, тобто вони знаходяться в оперативній пам'яті комп'ютера.
6. *програми-вакцини*: використовуються для обробки файлів і boot-секторів із метою попередження зараження відомими вірусами (в останній час цей метод використовується все частіше).

Антивірусні програми

- Avira
- Dr.Web
- Kaspersky
- McAfee
- NOD32
- Panda Software
- Symantec США
- Український Національний Антивірус
- ZoneAlarm AntiVirus

Завдання

- знайдіть інформацію про антивірусні програми зі списку “Антивірусні програми”
- користуючись знайденою інформацією та власним досвідом, складіть список рекомендацій для захисту комп’ютера від шкідливих програм, оформіть свій список у текстовому документі на власному диску та надайте посилання для читання вчителю на HUMAN або на електронну пошту **Balag.elizaveta@gmail.com**

- пройдіть тестування за посиланням: https://naurok.com.ua/test/join?gamecode=6253581