УДК 004.056.57

А. О. Радецька
В. А. Каплун

ЗАСІБ ДЛЯ ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Вінницький національний технічний університет

Анотація

Досліджено поняття комп'ютерних вірусів, їх класифікацію та схарактеризовано особливості методів захисту від нього. Розроблено програмний додаток, який реалізує захист від шкідливого програмного забезпечення без застосування спеціалізованого антивірусного програмного забезпечення.

Ключові слова: *шкідливе програмне забезпечення, комп'ютерні інфекції, захист програм від вірусів.*

Abstract

The concept of computer viruses, their classification and features of methods of protection against it are studied. Developed a software application that implements protection against malicious software without the use of specialized antivirus software.

Keywords*: malware, computer infections, virus protection.*

Вступ

Забезпечення інформаційної безпеки систем є одним з першорядних питань. У сучасному суспільстві особливо значну роль відіграє захист інформації, так як інтернет кишить вірусами і навіть найпростіші з них можуть завдати серйозної шкоди комп'ютеру і даним, що зберігаються на ньому. Ці загрози можуть мати найрізноманітніший характер – порушувати роботу системи шляхом знищення важливих системних файлів, красти важливу інформацію, паролі, документи. Це призводить до сумних наслідків – від переустановлення системи до втрати важливих даних або грошей.

Метою роботи є розробка програмного засобу, який дозволяє швидко здійснювати перевірку файлів на наявність шкідливого та небезпечного коду, не застосовуючи для цього коштовне і велике за обсягом спеціалізоване антивірусне програмне забезпечення.

Результати дослідження

Комп'ютерним вірусом називається програма, зазвичай мала за розміром (від 200 до 5000 байт), яка самостійно запускається, багаторазово копіює свій код, приєднуючи його до кодів інших програм («розмножується») і заважає коректній роботі комп'ютера та (або) руйнує інформацію (програми і дані), що зберігається на дисках [1].

Відомі програмні віруси можна класифікувати за такими ознаками [2]: середовище існування; спосіб зараження; вплив; особливості алгоритму.

У залежності від середовища перебування віруси можна розділити на такі групи: мережеві; файлові; завантажувальні; файлово-завантажувальні.

За способом зараження віруси поділяються на резидентні та нерезидентні.

За ступенем впливу віруси можна розділити на такі види:

- безпечні, не заважають роботі комп'ютера, але зменшують обсяг вільної оперативної пам'яті і пам'яті на дисках, дії таких вірусів виявляються в яких-небудь графічних або звукових ефектах;
- небезпечні віруси, які можуть призвести до різних порушень в роботі комп'ютера;
- дуже небезпечні, вплив яких може привести до втрати програм, знищення даних.

За особливостями алгоритму віруси важко класифікувати через їх велику різноманітності.

Способи протидії комп'ютерним вірусам можна розділити на кілька груп: профілактика вірусного зараження і зменшення можливої шкоди від такої зараження; методика використання антивірусних програм, в тому числі знешкодження і видалення відомого вірусу; способи виявлення і видалення невідомого вірусу.

Найбільш ефективні в боротьбі з комп'ютерними вірусами є антивірусні програми.

Відомо, що антивірусні програми поділяються на такі категорії: програми-детектори; програми-доктори; програми-ревізори; програми-фільтри; програми-вакцини.

Існує кілька основних методів пошуку вірусів, які застосовуються антивірусними програмами [3].

Антивірусні програми, як правило, мають великий обсяг, займають немалу частку процесорного часу і можуть реалізовувати всі одночасно такі методи пошуку шкідливого програмного забезпечення, як сканування; евристичний аналіз; виявлення змін; резидентні монітори.

Але часто вірусні програми приховуються під назвами інших програм, маскуються під вигляд корисних утиліт, і користувач не може візуально визначити, шкідлива ця програма чи ні. Не маючи спеціалізованого антивірусного забезпечення, виявити наявність таких шкідливих програм не можливо. Саме тоді і може стати у нагоді розроблений програмний засіб.

Розробка і реалізація додатку

Розроблено програмного засобу, що реалізує перевірку файлів та додатків на наявність в них замаскованого вірусного програмного коду. Розробка програми була здійснена за допомогою мови програмування Java в середовищі IntelliJ IDEA.

Програма перевіряє не всю інформацію на комп'ютері користувача, не інформацію з окремого логічного диску, а лише певні файли, на які вказує користувач.

Перевірка відбувається таким чином. Користувач повинен обрати файл (або файли) для перевірки. Далі буде здійснено визначення його сигнатури та її порівняння із базою даних. У базі зберігаються сигнатури найбільш поширених зразків шкідливого програмного забезпечення. Для визначення сигнатури файлу планується використання алгоритму хешування MD5.

Після проведення процесу порівняння сигнатур, виводиться вікно з інформацією про результат перевірки. Якщо у обраному файлі виявлено шкідливе програмне забезпечення, користувачу виводиться попередження про це, а також вказується тип та ім'я вірусу, яким заражений файл. У випадку, коли ж обраний для перевірки файл, не містить шкідливого програмного коду, виводиться повідомлення про те, що файл безпечний для використання.

Для перевірки ефективності роботи програми було використано базу вірусів з сайту Європейського інституту комп'ютерних антивірусних досліджень [4]. Наприклад, при тестуванні віруса *eicar.com* програмний засіб спрацював так, як показано на рисунку 1. Даний вірусний файл призначений спеціально для перевірки роботи антивірусних програм.

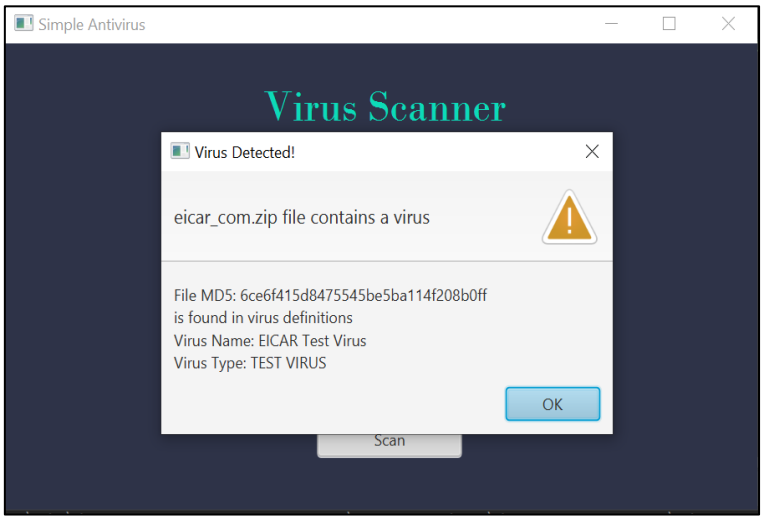

Рисунок 1 – Вигляд повідомлення при виявленні вірусного коду

Згідно з результатів тестування програми, можна зробити висновок, що розроблений програмний засіб працює коректно та виконує поставлену перед ним задачу – виявлення шкідливого програмного забезпечення на комп'ютері користувача.

Висновки

В результаті роботи було розроблено автономний засіб, що реалізує перевірку файлів на наявність комп’ютерних вірусів. Досліджено поняття комп’ютерний вірус та методи його класифікації. Ознайомлено з основними способами протидії комп’ютерним вірусам. Досліджено характеристики антивірусних програм та методики їх роботи.

Розроблена програма стане у нагоді користувачам, які бажають захистити свій комп’ютер від шкідливого програмного забезпечення. З її допомогою вони матимуть змогу перевірити будь-який файл на наявність прихованого вірусного програмного коду у будь-який момент часу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Что такое компьютерный вирус? Просто о сложном [Електронний ресурс] – Режим доступу: URL: https://ichip.ru/sovety/chto-takoe-kompyuternyjj-virus-prosto-o-slozhnom-223382- Назва з екрану.
2. Класифікація комп'ютерних вірусів. Принципи «зараження» комп'ютерним вірусом диска і пам'яті комп'ютера [Електронний ресурс] – Режим доступу: URL: https://vseosvita.ua/library/ponatta-pro-komputerni-virusi-klasifikacia-komputernih-virusiv-principi-zarazenna-komputernim-virusom-diska-i-pamati-komputera-306009.html- Назва з екрану.
3. Характеристики і класифікація антивірусних програм [Електронний ресурс] – Режим доступу: URL: https://studopedia.org/6-157206.html- Назва з екрану.
4. Eicar – EUROPEAN EXPERT GROUP FOR IT-SECURITY [Електронний ресурс] – Режим доступу: URL: https://www.eicar.org/- Назва з екрану.

Радецька Анастасія Олександпівна – студентка групи 1БС-18б, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: an.radetska@gmail.com

Каплун Валентина Аполінаріївна, ст. викл. кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, valuka8379@gmail.com.

Anastsiia O. Radetska– Department of Information Technology and Computer Engineering , Vinnytsya National Technical University, Vinnytsia.

Valentyna A. Kaplun – Lecturer of the Chair of Safety of Infomation and Communication Systems, NTU, Vinnytsia.