УДК 004.056.57 + 004.492

О.Ю. Новотарський

МЕТОД ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Вінницький національний технічний університет

Анотація

В даній науковій роботі описуються найпоширеніші методи пошуку вірусів за допомогою антивірусних програм. Проведено аналіз кожного з методів, а також запропоновано власний алгоритм пошуку вірусів в операційних системах.

Ключові слова: *Сигнатура, аномалія, евристика, комп'ютерний вірус, операційні системи*.

Abstract

In the present research work describes the most common methods to find viruses by using antivirus programs. The analysis of the advantages and disadvantages of each method, and proposed its own search algorithm viruses in operating systems.

Keywords: *Signature, anomaly, heuristics, computer virus, operating system.*.

Вступ

Безпека програмного забезпечення є властивістю програмного забезпечення функціонувати без прояву різноманітних негативних наслідків для конкретної комп'ютерної системи. Під рівнем безпеки програмного забезпечення (ПЗ) розуміється ймовірність того, що при заданих умовах у процесі його експлуатації буде отриманий функціонально придатний результат. Нині відомі десятки тисяч комп'ютерних вірусів, які поширюються через мережу Інтернет по всьому світу [1]. Необізнані користувачі ПК помилково завантажують програмні додатки з вірусами, що може призвести до непоправної шкоди операційній системі та іншим програмним додатках [2].

Задачею антивірусних програм є знаходження комп'ютерних вірусів, а також небажаних (шкідливих) програм загалом та відновлення заражених (модифікованих) такими програмами файлів, а також для профілактики — запобігання зараження (модифікації) файлів чи операційної системи шкідливим кодом.

Метою наукової роботи є створення власного алгоритму для покращення методів пошуку вірусів за допомогою антивірусних програм.

Для досягнення мети необхідно розв'язати такі задачі:

– Проаналізувати методи пошуку вірусів за допомогою антивірусних програм

– Розробити власний алгоритм пошуку вірусів який покращить процес пошуку вірусів в операційних системах.

Результати аналізу відомих методів пошуку вірусів

Проаналізувавши методи пошуку вірусів за допомогою антивірусних програм стає зрозумілим чому антивірусні програми не є надійними на 100%. Кожен метод пошуку вірусів є не надійним, так як в кожного метода є низка недоліків. [3].

Було проаналізовано такі методи пошуку вірусів, а саме:

– Виявлення, засноване на сигнатурах - даний метод дозволяє визначати конкретну атаку з високою точністю і малою часткою помилкових викликів. Метод є беззахистним перед поліморфними вірусами і зміненими версіями того ж вірусу, а також вимагає регулярного і вкрай оперативного оновлення.

– Виявлення аномалій – на відміну від методу відповідності визначенню вірусу в словнику, метод підозрілої поведінки дає захист від абсолютно нових вірусів і мережевих атак, яких ще немає ні в одній базі вірусів або атак. Однак програми, побудовані на цьому методі, можуть видавати також велику кількість помилкових попереджень, що робить користувача дуже чутливим до попереджень.

– Виявлення, засноване на емуляції – У деяких випадках, емуляція дозволяє досить ефективно протистояти таким технологіям як поліморфізм шкідливих програм, що досягається за рахунок оцінки здійснюваних дій, але не програмного коду. Безсумнівним недоліком емуляції є високе споживання системних ресурсів, що негативно позначається на продуктивності комп'ютера.

Відповідно актуально об'єднати переваги підходів до виявлення вірусів для покращення виявлення вірусів та зменшення кількості хибних спрацювань.

Алгоритм пошуку вірусів

Суть алгоритму заснована на методі пошуку вірусів за допомогою сигнатур але з різним ступенем кореляції. Алгоритм на основі сигнатур вважає файл ураженим, якщо сигнатура співпадає з кодом файлу на 100%, але це не надійний спосіб, так як файл може бути ураженим вірусом але співпадати з сигнатурою на 90%. Якщо зменшити ступінь кореляції, то тоді покращиться пошук вірусів в файлах.

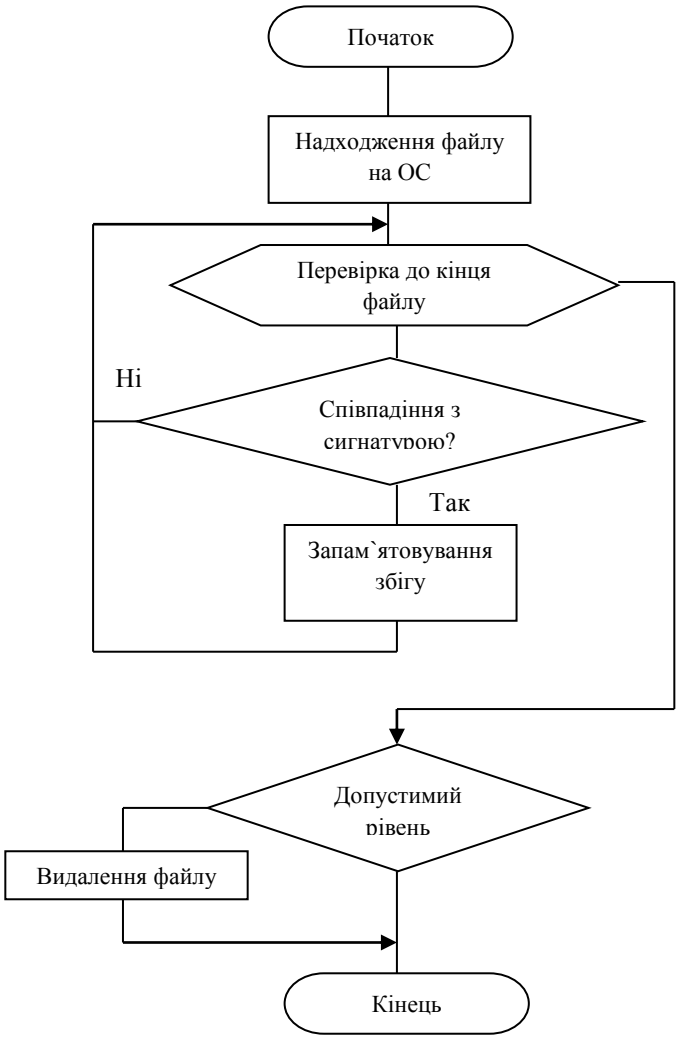

Рис. 1. Структура операційного пристрою

Як видно з Рис. 1, запропонований алгоритм покращує сигнатурний метод пошуку вірусів та зменшує кількість хибних спрацювань евристичного методу.

Висновки

Внаслідок аналізу методів пошуку вірусів було виявлено актуальну задачу удосконалення методики евристичного пошуку вірусів

Перелік використаних джерел

1. Анин Б.Ю. Защита компьютерной информации. – СПб.: БХВ-Петербург, 2000. – 384 с.
2. Терський С. В. Виявлення, засноване на сигнатурах/ С. В. Терський ; Нац. ун-т "Львів. політехніка". – Львів : Вид-во Нац. ун-ту "Львів. політехніка", 2010. – 320 с. : іл. – Бібліогр.: с. 275–298.
3. Виявлення, засноване на емуляції / Нац. ун-т "Львів. політехніка" ; [відп. ред. К. Р. Третяк]. – Львів : Вид-во Нац. ун-ту "Львів. політехніка", 2008. – Вип. 70. – 88 с.

Олексій Юрійович Новотарський – студент факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет.

Науковий керівник: ***Юрій Володимирович Баришев***– канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет.

Oleksiy Y. Novotarskiy - student of the Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University.

Supervisor: ***Yurii Baryshev*** – Cand. Sc. (Eng), Associated Professor of Information Protection Chair, Vinnytsia National Technical University, Khmelnytske shosse 95, Vinnytsia, Ukraine.