ЕВРИСТИЧНИЙ АНАЛІЗАТОР КОМП'ЮТЕРНИХ ВІРУСІВ НА ОСНОВІ МЕТОДА МАМДАНІ

канд. техн. наук, доц. С.Ю. Гавриленко, студ. Д.М. Саєнко,
Національний технічний університет "Харківський політехнічний інститут", м. Харків

Найбільша частка всіх комп'ютерних злочинів [1] припадає на комп'ютерні віруси. На даному етапі розвитку інформаційних технологій приріст вірусів дуже великий. Розвиток неможливо зупинити, але з ним можливо намагатися боротися.

Для боротьби з вірусами було обрано евристичний аналіз [2]. Механізм прийняття рішення в евристичних аналізаторах базується на використанні теорії штучного інтелекту, наприклад на основі методів нечіткої логіки та алгоритмів нечіткого виведення, теорії нейронних мереж.

Розроблено програмну модель та проведено тестування. Алгоритм роботи програмної моделі полягає в отримуванні таблиці імпорту з виконуючого файлу та збереженні отриманого результату в текстовому файлі з бібліотеками та функціями.

Отримана інформація надалі поступає на вхід аналізатора. Після відкриття аналізатор відразу створює масив з бібліотеками та функціями які були використані в проаналізованому файлі. Отримана інформація групується за трьома ознаками: загальна кількість використаних бібліотек, кількість підозрілих бібліотек, кількість підозрілих функцій, та поступає на вхід евристичного аналізатора комп'ютерних вірусів на основі метода Мамдані.

Правильність роботи розробленої програмної моделі перевірено за допомогою Fuzzy Logic від MATLAB [3].

Отримані результати підтвердили можливість практичної реалізації та використання розроблених засобів евристичного пошуку комп'ютерних вірусів на основі метода Мамдані.

Список літератури: 1. *Семенов С.Г.* Захист інформації в комп'ютерних системах та мережах: навч. посіб. / *С.Г. Семенов, А.О. Подорожняк, О.І. Баленко, С.Ю. Гавриленко.* – Х.: НТУ "ХПІ", 2014. – 251 с. **2.** *Анатолий Ализар*. Эвристика эффективнее, чем обновление антивирусных баз. [Электронный ресурс] − Режим доступу: http://www.compdoc.ru /secur/virus/heuristics/. **3.** *Штовба С.Д.* Проектирование нечетких систем средствами MATLAB / *С.Д. Штовба*. – М.: Горячая линия-Телеком, 2007. – 288 с.