

РОЗРОБКА СИГНАТУРНОГО АНАЛІЗАТОРА

*канд. техн. наук, проф. С.Ю. Гавриленко, студ. Д.Н. Сасенко,
Національний технічний університет "Харківський політехнічний
інститут", м. Харків*

Найбільша частина всіх комп'ютерних злочинів приходить на комп'ютерні віруси. Інформаційні технології стрімко розвиваються, віруси модифікуються, їх кількість неухильно зростає, тому вирішити остаточно дану проблему неможливо. Саме тому актуальною темою є розробка ефективних методів протидії комп'ютерним вірусам.

В роботі розглянуто та обґрунтовано необхідність розробки і вдосконалення статичного аналізу виконуючих файлів з метою полегшення та уточнення подальшого аналізу для виявлення шкідливого файлу.

Запропоновано створення web-сервісу, що здійснює аналіз підозрілих файлів на предмет виявлення шкідливого програмного забезпечення (рис.).

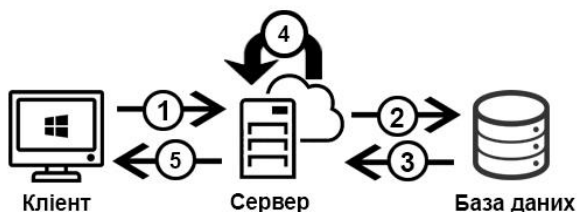


Рис. – Загальна схема сигнатурного аналізатору.

На рис. прийняті такі позначення: 1 – відправка файлу до серверу; 2 – перевірка файлу на наявність в базі даних; 3 – відправлення результату пошуку на сервер; 4 – виконання сигнатурного аналізу при відсутності інформації в базі даних; 5 – відправлення результату аналізу користувачу.

В основі роботи сервісу є аналіз PE-структури завантаженого файлу, а саме: кількість секцій, ентропія, тип компілятора, пакувальника, лінкери, визначення точки входу (entrypoint), наявність сертифікату, наявність запису в автозавантаження, хеш-сума (MD5), перелік використаних API функцій.

За результатами приймається рішення про наявність вірусу. В випадку визначення даного програмного забезпечення як шкідливого, формується сигнатура нового типу вірусу.