РОЗРОБКА МЕТОДИКИ ДІАГНОСТИКИ КОМП'ЮТЕРНИХ СИСТЕМ

Піддубний О.В., Дженюк Н.В.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

Сучасні методи пошуку та виявлення троянських програм, які ґрунтуються на алгоритмах сигнатурного аналізу, контрольних сум та евристичного аналізу, мають певні недоліки. Дослідження методів показало, що алгоритми, на яких вони базуються, не вирішують задачі ефективного пошуку нових троянських програм, оскільки не адаптовані до розпізнавання за їх життєвим циклом. Алгоритми, на яких базуються сучасні методи демонструють низьку ймовірність розпізнавання та виявлення нових ТП.

Для усунення недоліків сучасних методів розроблено новий інтелектуальний метод пошуку троянських програм в персональних комп'ютерах, який базується на використанні алгоритмів нечіткої логіки та штучних імунних систем. Для реалізації інтелектуального методу пошуку троянських програм розроблено нові алгоритми, суть яких полягає у відслідковуванні системних подій разом із виконанням нечіткого логічного висновку щодо підозрілості об'єкта та перевірці файлів на факт їх підміни троянськими версіям за допомогою алгоритму негативного відбору.

Проведене дослідження алгоритму негативного відбору доводить ефективність розробленого методу стосовно його швидкодії та високої ймовірності виявлення аномалій.

Розроблений алгоритм має два режими: автономний (створення «свого» та генерація детекторів) та оперативний (сканування ПК). Швидкодія роботи алгоритму в автономному режимі залежить від часу для виконання дій:

Вибору файлів, які підлягають контролю щодо виявлення факту їх підміни троянськими версіями, та для створення їх бінарного представлення.

Генерації кожного шаблону детекторів mr.

Розширення кожного дійсного шаблону до повністю визначеної послідовності.

Оновлення шаблонів при створенні кожного детектора.

Час виконання оперативного режиму, при якому виконується безпосереднє виявлення факту підміни, залежить від кількості файлів, що підлягають перевірці та кількості детекторів, згенерованих під час роботи автономного режиму.

Результати дослідження розроблених алгоритмів показали можливість виявлення нових троянських програм з ймовірністю в 70-95 %, що дасть змогу їх застосувати в програмній реалізації системи пошуку троянських програм в персональних комп'ютерах.

Реалізація методу забезпечить здійснення пошуку та ідентифікації відомих та нових троянських програм в персональному комп'ютері, які не вимагатимуть побудови баз сигнатур, застосування евристичного аналізатора та використання контрольних сум.