РОЗРОБКА ЕЛЕМЕНТІВ СИСТЕМИ АНАЛІЗУ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА ОСНОВІ МЕТОДУ ГРУПОВОГО ВРАХУВАННЯ АРГУМЕНТІВ

Горносталь О.О., Челак В.В., Гавриленко С.Ю.
Национальный технический университет «Харьковский политехнический институт», г. Харьков

У сучасному світі кожен день з’являються нові комп’ютерні віруси, які завдають шкоди мільйонам комп’ютерів. При цьому для їх виявлення та видалення використовується антивірусне програмне забезпечення. Воно має розпізнавати комп’ютерні віруси не лише за їх кодом та командами, а й за їх поведінкою, тобто за діями, які вони виконують.

У ході проведеного дослідження були розглянуті тестові набори якісних характеристик різних шкідливих програм. Для кожного тестового набору послідовностей було виконано наступні операції:

– записати критерії (відповідають за наявність певних характеристик) усіх зразків у вигляді матриці;

– розрахувати стандартні показники (максимінний критерій, критерій азартного гравця, нейтральний критерій, критерій добутку та критерій Севіджа);

– проаналізувати отримані дані;

– створити нові критерії, використовуючи операцію середнього арифметичного для пар вже наявних критеріїв;

– повторити описану операцію потрібну кількість кроків.

Були отримані елементи системи аналізу шкідливого програмного забезпечення на основі методу групового врахування аргументів. Результати розробки дозволяють проводити дослідження потенційно небезпечних (підозрілих) програм, маючи інформацію про наявність чи відсутність у них певних характеристик.

Література:

1. Стрижов В.В. Методы выбора регрессионных моделей / В.В. Стрижов, Е.А. Крымова. – М.: ВЦ РАН, 2010. – 60 с. **2.** Madala H.R. Inductive Learning Algorithms for Complex System Modeling / H.R. Madala, A.G. Ivakhnenko. – 1994, CRC Press. **3.** Лесковец Ю. Анализ больших наборов данных / Ю. Лесковец, А. Раджараман. – М.: ДМК, 2016. – 498 с.