## МЕТОД МІНІМАЛЬНОЇ ДОВІРИ ДЛЯ ВИДІЛЕННЯ ШКІДЛИВИХ ПРОЦЕСІВ ТА ВІДНОВЛЕННЯ ДАНИХ В ОПЕРАЦІЙНИХ СИСТЕМАХ WINDOWS

*канд. техн. наук, доц. С.Ю. Гавриленко, аспірант І.В. Шевердін, Національний технічний університет "Харківський політехнічний інститут", м. Харків*

Основною задачею антивірусного програмного забезпечення є знаходження потенційно шкідливих процесів [1]. Для забезпечення системного захисту необхідно миттєво аналізувати міліони системних подій. Рішення даної задачі не є тривіальним, тому що необхідно виділити критерії шкідливих подій та процесів. Помилка у вирішенні даного питання може бути фатальною у зв’язку з вірогідністю пошкодження системних файлів та компонент.

Для рішення даної проблеми розглянуто метод "мінімальної довіри". Для розуміння цього методу виділимо декілька результатів силогізму. По перше, в ізольованій системі вірусів не може бути. По друге, нова поведінка, котра забезпечується новим процесом є потенційно вірусною. По третє, кожна подія у системі ділиться на дію та результат цієї дії.

Базуючись на цьому, запропоновано програмну ізоляцію для кожного процесу. В ізольованому середовищі процес не може зробити зміни у системі, він буде виконувати дію тільки з копіями файлів. Після виконання можливо проаналізувати результат та виконати поєднання його з джерелом. Якщо неможливо працювати з копією, то необхідно забезпечити збереження всіх змін, для можливості відновлення стану файлу в випадку вірусної активності.

Запропонований метод програмної ізоляції кожного процесу дозволить виявити шкідливе програмне забезпечення та відновити дані, базуючись на трьох правилах та існуючих методах, принципах обробки та об’єднання даних.

**Список літератури: 1.** Антивірусна програма [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Антивірусна_програма.