ВИКОРИСТАННЯ ІДЕНТІФІКАЦІЙНИХ КАРТ ПРОЦЕСІВ ДЛЯ ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Гавриленко С.Ю., Шевердін І.В.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

На даний час існує велика кількість кібератак. Навіть така розвинута країна як США, не має єдиної системи захисту від кібератак що призводять до величезних збитків [1]. Для України також загрозу становлять вірусні атаки, котрі загрожують цілісності держави. Як правило жертвами масштабних кібератак є не тільки приватні структури, банки, заправки, магазини, але і державні організації.

Експерти у області комп’ютерної безпеки відзначають, що обсяги комп’ютерних вірусів та шкідливого програмного забезпечення ростуть із загрозливою швидкістю.

Одним з найважливіших етапів розробки антивірусного програмного забезпечення є побудова алгоритму аналізу процесів операційної системи. Актуальним стає питання у правильному підборі оптимальних алгоритмів аналізу подій у системі.

У даній роботі розглянуті основні принципи побудови системи антивірусного захисту на базі багаторівневого аналізу карт процесів ОС. Кожна система створює тисячі системних подій, котрі породжені окремим процесом, данні події можливо об’єднати у чотирьохрівневу карту для кожного процесу. Всі події розділено на чотири основні категорії, а саме робота процесу з системним реєстром, файловою системою, комунікація з іншими процесами, інтернет комунікація. Як результат, кожна із категорії має свій рівень.

Аналізуючи вплив вірусів на систему за рахунок аналізу системних подій було виділено вісім основних параметрів, котрі характеризують подію – це Process Name, Result, Image Path, Event Class, Company, Version, Authentication ID, Category. Параметри розділено на дві категорії, котрі описують стан системи та конкретну подію. Базуючись на параметрах подій операційної системи побудовано набір асоціативних правил системи виявлення комп’ютерних вірусів.

Експериментальним шляхом встановлено, що аналіз багаторівневих карт дозволяє зменшити час та підвищити точність виявлення зміни системи [2]. Використовуючи даний підхід для кожного окремого процесу, отримано механізм детермінації процесу. Результатом аналізу є опис поведінки процесу у вигляді сигнатури подій. Це дозволяє зменшити час аналізу ідентичних процесів в комп’ютерних системах.

Література:

1. У США підрахували втрати економіки від кібератак [Електронний ресурс]. – Режим доступу до ресурса: https://korrespondent.net/business/economics/3943657-v-ssha-podschytaly-potery-ekonomyky-ot-kyberatak