ИССЛЕДОВАНИЕ МЕТОДОВ ПОСТРОЕНИЯ ЭВРИСТИЧЕСКИХ АНАЛИЗАТОРОВ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ С ИСПОЛЬЗОВАНИЕМ АЛГОРИТМА СУГЕНО

канд. техн. наук, доц. С.Ю. Гавриленко, студ. Е.А. Вельбивец, Национальный технический университет "Харьковский политехнический институт", г. Харьков

Работа эвристического анализатора основывается на наборе эвристик (предположений, статистическая значимость которых подтверждена опытным путем), содержащих характерные признаки вредоносного исполняемого кода. Важным преимуществом эвристического анализа является проактивный метод работы – возможность обнаружения новых вирусов, которые еще не были добавлены в базу вирусов. Недостатком такого метода является большое количество ложных срабатываний. Работа эвристического анализатора основывается на теории искусственного интеллекта. В данной работе использован механизм нечеткого вывода.

Для обнаружения вредоносного ПО были взяты WinAPI функци, которые характерны для вирусов определенного типа (например LoadLibrary, GetProcessAddress, SetWindowHookEx), т.к. только выполнение API-функций может оказать негативное влияние на компьютер, чего нельзя сказать об операциях пересылок, арифметических операциях и т.д. В системе нечеткого вывода лингвистическими переменными являются WIN-API функции, используемые вирусами, которые имеют три терма: Safely, Undefined, Dangerous – характеризующие уровень безопасности программы в зависимости от количества вызовов данных WIN-API функций. В правилах данной системы реализован полный перебор всех комбинаций термов лингвистических переменных. Результатом работы данной системы является определение степени безопасности программы, а также определение типа вируса. Выходная переменная имеет значения Safely, Undefined, тип вируса или Dangerous, когда тип не удалось определить однозначно. Поиск и подсчет количества вызываемых функций производится путем вычисления количества адресов, которые содержат адреса вызовов функций в загруженных программой DLL библиотеках. Преимуществом данной системы является проактивный анализ, т.к. не обязательно чтобы были обнаружены абсолютно все характерные для вируса WIN-API функции. Недостатком данной системы являются возможные ложные срабатывание и трудоемкость добавления нового вируса в базу, т.к. необходимо корректировать уже существующие правила для правильности распознавания вируса или степени опасности программы.