РАЗРАБОТКА СИСТЕМЫ ПРИНЯТИЯ РЕШЕНИЯ ОБНАРУЖЕНИЯ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Челак В.В., к.т.н., проф. Гавриленко С.Ю.
Национальный технический университет «ХПИ», Харьков

В докладе представлена система принятия решений (СПР), для обнаружения вредоносного программного обеспечения на основе вероятностного автомата.

СПР регулирует значения таблицы вероятностей переходов автомата и управляет функционированием автомата.

Текущая вероятность $P_{ij}\ (X,\ t)$ определяется следующим образом (1):

$$\mathrm{P_{ij}}\left(\mathrm{X,t}\right)=\left\{\begin{array}{c}0,\mathrm{S_{ij}^{A}}\left(\mathrm{X}\right)=\mathrm{S_{z}^{A}}\\ \mathrm{P_{ij}}\left(\mathrm{X,t-1}\right),\mathrm{S_{ij}^{A}}\left(\mathrm{X}\right)\neq\mathrm{S_{z}^{A}}\wedge\mathrm{S_{ij}^{H}}\left(\mathrm{X}\right)=\mathrm{S_{z}^{H}}\\ \mathrm{P_{ij}}\left(\mathrm{X,t-1}\right)+\mathrm{M},\mathrm{S_{ij}^{H}}\left(\mathrm{X}\right)\neq\mathrm{S_{z}^{H}}\end{array}\right\} \quad (1)$$

где $P_{ij}\left(X,t\right)$ – рассчитываемое значение вероятности переходов в таблице для *i*-го столбца и *j*-ой строки, $P_{ij}\left(X,t-1\right)$ – текущее значение таблицы вероятности, S_z^A все элементы множества состояний-предков, исключая текущий элемент, $\mathrm{S_{ij}^{A}}\left(\mathrm{X}\right)$ – элемент из множества предков, которому соответствует вероятность P_{ij} , S_z^H - множество наследников, включает все элементы кроме текущего ($S_{ij}^H\left(X\right)$), *M* – маркерное значение (принимает значения -1 до 1).

Полученные результаты тестирования предложенной системы, подтвердили возможность ее использования, как средства выявления вирусных атак в общей системе обнаружения вредоносного программного обеспечения.