1. Комп'ютерні та інформаційні технології

ОГЛЯД СУЧАСНИХ МЕТОДІВ І ЗАСОБІВ БОРОТЬБИ ЗІ ШКІДЛИВИМ ПО Й ПРОГРАМНИМИ ВІРУСАМИ.

Федоров І.О.
Науковий керівник – проф. каф. СПЗ д.т.н. Крісілов В.А.

На даний момент у комп'ютерній мережі Інтернет існує більше 300000 програмних вірусів і шкідливого ПЗ, з яким покликане боротися різноманітне антивірусне програмне забезпечення.[1]

Ціль даної доповіді складається в короткому огляді й виявленні переваг та недоліків існуючих методів і засобів, а також їх можливих сполучень для боротьби зі шкідливим ПЗ й програмними вірусами.

На даний момент існують наступні сучасні методи й засоби захисту: сигнатурний пошук, евристичний аналіз, кріптоанализ, аналіз контрольних сум, аналіз редуцированої маски, статистичний аналіз, емуляція. [2]

Базовим методом, який використовується у сучасному антивірусному ПЗ, є сигнатурний аналіз, здійснюючий пошук унікальних сигнатур у програмному коді , на предмет виявлення в ньому коду програмних вірусів і шкідливого ПЗ. У зв'язку з їхньою зростаючою складністю даний метод об`єднується із кріптоаналізом , статистичним аналізом, аналізом редуцированої маски для визначення й розшифровки програмних вірусів, що самошифруються, а також виявлення резидентних вірусів. Сигнатурний аналіз може об`єднуватися з евристичним аналізом, та емулятором команд і функцій операційної системи для визначення невідомих програмних вірусів і шкідливого ПЗ, а також боротьби з усіма відомими програмними вірусами й шкідливим ПЗ. Аналіз контрольних сум є модифікацією сигнатурного аналізу.

1 Гошко С. В. Энциклопедія по захисту від вірусів Солон 2005.
2 Доля А.В Антивірусні "двіжки" http://www.fcenter.ru/online.shtml?articles/software/utilities/12214