

МОДЕЛІ АНОМАЛЬНОГО СТАНУ ДЛЯ ВИЯВЛЕННЯ КІБЕРАТАК В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Актуальність даної роботи полягає в тому, що несанкціоновані дії на ресурси інформаційних систем впливають на оточуюче середовище і породжують в ньому певні аномалії. Таке середовище зазвичай слабоформалізоване, нечітко визначене і для виявлення атак, що породили аномалії, в такому середовищі потрібно використовувати ефективні моделі і методи. Формалізувати і ефективно обробити інформацію в такому середовищі дозволяють методи і моделі теорії нечітких множин. У зв'язку з цим актуальним завданням при розробці засобів, що розширюють можливості сучасних СВВ є створення, на основі теорії нечітких множин, моделей, методів і систем виявлення аномалій, породжених мережевими кібератаками.

Наукова новизна полягає в наступному: на основі базової моделі параметрів, універсальної моделі еталонів і моделі евристичних правил розроблено метод виявлення аномалій, породжених діями неавторизованої сторони, який дозволяє на основі експертного підходу і сформованих нечітких поточних параметрів створювати засоби ідентифікації несигнатурного типу кібератак;

Дана робота має на меті розробку моделей і засобів ідентифікації аномального стану, для розширення можливостей системи виявлення несигнатурних типів кібератак в комп'ютерних мережах. Для досягнення поставленої мети необхідно вирішити такі основні завдання: дослідити сучасний стан розвитку теоретичної та практичної бази, що використовується для виявлення атак в комп'ютерних системах; розробити базову модель параметрів і універсальну модель еталонів для відображення та виміру аномального стану в оточуючому середовищі, характерного для певного типу кібератак в комп'ютерних мережах.

На основі базової моделі параметрів, універсальної моделі еталонів та моделі евристичних правил було розроблено метод виявлення аномалій породжених кібератаками в комп'ютерних мережах.

На основі отриманих результатів експлуатації даної моделі можна сказати, що дослідження сучасного стану теоретичної та практичної бази, яка використовується для виявлення атак в комп'ютерних системах, показали недосконалість відповідних засобів безпеки щодо їх можливостей ідентифікувати в нечітко визначеному слабоформалізованому середовищі несигнатурного і нових типів кібератак. Використання методів і моделей нечітких множин для побудови засобів виявлення аномалій, породжених атакуючими діями, дозволить удосконалити існуючі системи виявлення вторгнень і шляхом контролю активності в оточуючому середовищі ідентифікувати небезпечні аномальні стани.

Науковий керівник – д.т.н., проф., В.В. Козловський