РЕФЕРАТ

Магістерська дисертація: __ с., __ рис., __ табл., __ джерел.

Здійснено порівняльний аналіз різних підходів розробки системи виявлення вторгнень як складової частини запропонованої системи моделювання зараження мережі та протидії процесу зараження.

Метою запропонованої системи є моделювання реальних загроз безпеці комп'ютерної мережі та створення системи протидії цим загрозам.

Предметом дослідження є побудування теоріко-ігрової моделі протидії системи виявлення вторгнень процесу атаки на мережу.

Об'єктом дослідження є створення системи виявлення вторгнень на основі даних нормальної та аномальної роботи мережі.

Система виявлення вторгнень навчається на даних нормальної роботи мережі деякий час, формуючи декілька кластерів, які характеризують нормальну роботу правильно налаштованої мережі. Для виявлення загроз навчена система перевіряє наскільки близькі поточні дані до одного з кластерів, що дозволяє виявити аномалії по відхиленню значення нових вимірів від середнього відносно даних, на яких вона навчалась.

Реалізація даної системи моделювання була імплементована та протестована на відкритому наборі реальних даних комп'ютерної мережі. Алгоритм GNG показав значно кращі результати ніж IGNG у представленій реалізації. Ефективність кластерізації системою виявлення вторгнень майже не залежить від кількості спостерігаємих параметрів. Швидкість та якість роботи системи моделювання дій атакуючого та системи виявлення вторгнень є задовільною. Подальше дослідження може включати в себе використання більш досконалих алгоритмів кластерізації, імплементації багатопоточності у систему виявлення вторгнень, використання даних, зібраних за допомогою honeypot, у навчанні системи виявлення, та оптимізації моделюючої системи шляхом додавання рефлексії до моделі при виборі часу роботи.

Подальше дослідження може включати використання більш досконалих моделей для виділення тексту, а також розробка більш складних метрик для оцінки результатів подібних моделей.

КІБЕРЗАГРОЗА, МУЛЬТИАГЕНТНІ СИСТЕМИ, СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ, МОДЕЛЮВАННЯ СЦЕНАРІЇВ, НЕЙРОННИЙ ГАЗ, КЛАСТЕРІЗАЦІЯ