ФІЗИКО-МАТЕМАТИЧНІ НАУКИ

Баландіна Н.М.
старший викладач,
Національний університет «Одеська юридична академія»

ДЕЯКІ ОСОБЛИВОСТІ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ КІБЕРІНФОРМАЦІЙНИХ ОПЕРАЦІЙ

Під математичним моделюванням розуміють процес встановлення відповідності даному реальному об'єкту деякого математичного об'єкта, званого математичною моделлю, і дослідження цієї моделі, що дозволяє отримувати характеристики розглянутого реального об'єкта [1, с. 180]. Інформаційна операція є складовою так званих гібридних війн і її наявність є ознакою виникнення і проявлення ймовірних так званих економічних війн або військових загроз [2, с. 158]. При цьому в інформаційній безпеці та кібербезпеці прикладами інформаційних операцій є кібератаки, кібершпигунство, кіберінциденти, кібервійна, інформаційна війна і т. д.

Особливістю математичного моделювання інформаційних операцій варто вважати порівняльну простоту інтерпретації одержуваних результатів. Такі поняття як «кібератака», «кіберзагроза», «модель порушника», «сценарії атаки», «захист інформації» і т. д. сприймаються на інтуїтивному рівні навіть без знайомства з точними визначеннями. А це дозволяє робити подібний аналіз актуальних ситуацій предметом широкого обговорення.

При моделюванні інформаційних операцій обчислювальний експеримент дає змогу скоротити операції з уточнення обмежень, підбору вихідних даних, вибору правил функціонування компонентів моделі тощо. У цьому випадку з'являється можливість урахування випадків, які важко реалізуються на практиці, використовуючи реальні дані лише для ідентифікації параметрів математичної моделі. Разом з тим математичне моделювання має свої обмеження, реальний світ виявляється складним для моделювання з достатнім рівнем деталізації й точності, тобто більш-менш достовірні математичні моделі настільки

складні та багатопараметричні, що не піддаються аналізу та оцінкам точними методами [3, с. 35].

Нині є досить багато можливостей для ефективної комп'ютерної обробки даних, що дає змогу, з одного боку, готувати набори вхідних параметрів на підставі аналізу результатів статистичних досліджень, а з іншого – вирішувати формалізовані задачі з достатнім ступенем точності та у припустимий час. Все це дає підстави думати, що найближчим часом математичне моделювання стане основним інструментальним засобом планування інформаційних операцій та протидії їм [4, с. 209].

Якщо за елемент інформаційної безпеки брати не загрози несанкціонованого знімання інформації – атаки, а загрози – можливості отримання інформації уразливості, із застосовуваними нами допущеннями з використанням теорії на основі марковських випадкових процесів, то є можливість визначити структуру системи з необхідним рівнем інформаційної безпеки ще на підготовчому етапі [5, с. 48]. Крім того, в математичному моделюванні кіберінформаційних операцій використовується модель порушника для оцінювання рівня загроз, виявлення слабких місць в системі, прогнозування атаки/послідовності атак, а також сценаріїв відновлення системи після успішно проведеної атаки [6, с. 24].

Отже, математична модель описує реальний об'єкт, але з певним наближенням. Однак для ефективного математичного моделювання кіберінформаційних операцій необхідно обрати влучний підхід для правильної інтерпретації вхідних даних. При цьому для моделювання інформаційних операцій математичними методами характерним є складність отримання вірної математичної моделі яка б враховувала елементи інформаційної безпеки в реальному часі.

Список використаних джерел:

1. Давідіч Ю.О. Конспект лекцій з дисципліни «Моделювання транспортних систем» (для магістрів усіх форм навчання спеціальності 275 – Транспортні технології) / Ю.О. Давідіч, Г.І. Фалецька; Харків. нац. ун-т. міськ. госп-ва ім. О.М. Бекетова. – Харків: ХНУМГ ім. О.М. Бекетова, 2019. – 71 с.

2. Дудатьєв А. Моделі для організації протидії інформаційним атакам. *Захист інформації.* 2015. Т. 17. № 2. С. 157–162.

3. Горбулін В.П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія / В.П. Горбулін, О.Г. Додонов, Д.В. Ланде. – К.: Інтертехнологія, 2009. – 164 с.

4. Якименко Н.М. Важливість дослідження та моделювання інформаційних операцій в умовах інформаційної війни та кібервійни: матеріали Всеукраїнської науково-технічної конференції (м. Кропивницький, 23-25 листопада 2016 р.). 2016. С. 207–209.

5. Лаптєв О.А. Модель інформаційної безпеки на основі марковських випадкових процесів. *Зв'язок.* 2018. № 6. С. 45–49.

6. Кіреєнко О. Рекомендації щодо розробки моделі порушника інформаційної безпеки із загальною та спеціалізованою інформацією. Безпека інформації. 2019. Т. 25, № 1. С. 24–29.