DOI 10.15276/imms.v16.no1.52
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol.16 (2026), No. 1, pp. 52-57

МАТЕМАТИКА В КІБЕРБЕЗПЕЦІ

І.І. Борисенко, Л.М. Тимошенко, І.С. Вінковська

Національний університет «Одеська політехніка»
1, Шевченка пр., Одеса, 65044, Україна
Email: borisenko.i.i@op.edu.ua

Кількість користувачів мережі Інтернет зростає експоненціально кожного року. В той же час кожного дня з'являються десятки тисяч кіберзлочинців, які, використовуючи слабкі місця інформаційної системи, здатні викрадати дані, тому тема протистояння кібератакам є та буде актуальною зараз і, напевне, ще не одне десятиріччя. Сучасні технології з використанням математичного аналізу даних дозволяють протидіяти протиправним діям в мережі та характеризують наш сучасний етап розвитку. Кібербезпека – комплекс заходів, який спрямований на здійснення захисту різноманітних інформаційних систем та мереж від кібератак. Здійснення охорони даних базується на передових технологіях та методах захисту інформації, які в свою чергу базуються на фундаментальних знаннях математики. Саме такі розділи математики як логіка, комбінаторика, матричний аналіз, а особливо теорія графів, або графові технології, мають великий вплив та значення серед усієї кількості математичних методів. Стрункa система спеціальних термінів і позначень математики дозволяє просто і доступно описувати складні і тонкі речі як геометрично (графи), так і алгебраїчно (мариці). Аналіз наукових праць дозволив визначити основні напрями застосування властивостей, характеристик графів та графових алгоритмів в інформаційній та кібернетичній безпеці. Серед них виділено дослідження, пов'язані із застосуванням графів в інформаційних системах та у програмуванні, з моделюванням, аналізом та застосуванням графів атак, з криптографічними та стеганографічними перетвореннями, з побудовою дерева рішень у задачах прийняття рішень в умовах ризику і невизначеності. Увагу вчених і науковців привернули і інші математичні напрями. Цифрове зображення, яке в стеганографії обирається як контейнер, математично представляється матрицею. Повідомлення, яке вбудовується в контейнер, і не являється зображенням, можна представити в матричному вигляді, або виконати його препроцесінг, застосовуючи алгоритми роботи з послідовностями. Отже, широке застосування математики в інформаційній та кібербезпеці, математичний підхід до розробки нових та модифікації існуючих застосунків кібербезпеки робить обґрунтованим вибір та актуальність даного дослідження.

Ключові слова: математичні методи, кібербезпека, графові алгоритми, криптографія, стеганографія.

Вступ. У сучасному світі теорія графів є однією з актуальних та ефективних, серед математичних технологій, оскільки сфера її застосування охоплює різні області діяльності людства, зокрема у інформаційній та кібернетичній безпеці.

Аналіз наукової літератури свідчить про наявність глибокої зацікавленості вчених до проблеми використання графових технологій у кібербезпеці. Сформувалися наступні напрями застосування теорії графів:

- криптографічні перетворення за допомогою теорії графів;
- графи в стеганографії;
- графи в інформаційній системі та у програмуванні;
- моделювання;
- аналіз та застосування графів атак.

І це ще не повний перелік.

Не меншою популярністю та затребуваністю, особливо в стеганографії, користується лінійна алгебра, матричний аналіз та операції над послідовностями. А саме:

- використання систем алгебраїчних рівнянь [1,2];
- використання спектрального та сингулярного розкладу матриць [3-5];
- створення крипто-стеганографічних шифрів [6].

Постановка задачі. *Метою* роботи є аналіз та дослідження існуючих математичних методів, використання їх в області захисту інформації, визначення шляхів подальшого їх розвитку та використання в кібербезпеці.

Рамки роботи обмежені описом основних напрямків застосування графових технологій та матричного аналізу в інформаційній та кібернетичній безпеці.

Розглянемо питання щодо застосування графів в інформаційних системах.

Для розробки та опису схеми інформаційних потоків в інформаційній системі зручно використовувати теорію графів. Будують інформаційну систему як орієнтований граф, який містить скінченну кількість вузлів – це компоненти інформаційної системи, та дуг, які відображають інформаційні потоки, тобто взаємозв’язки між ними. Опис схеми інформаційних потоків можна змоделювати за допомогою маршрутів графа, послідовно перерахувавши: джерело інформації, проміжну апаратура та отримувача інформації, а також вид інформації, яка передається. Суміжність компонентів інформаційної системи буде визначати матриця суміжності, а матриця інцидентності – зв’язок між компонентами та інформаційними потоками. На основі даних цих матриць можна передбачити засоби захисту інформації, наприклад, розмежування доступу до інформації [3].

Велика кількість наукових досліджень присвячена розробці та удосконаленню моделей атак у вигляді графів для задач моніторингу кібербезпеки з метою захисту інформації.

В роботі [3] представлена графово - матрична модель супротивника інформаційно-технологічної системи для розробки методу перевірки стійкості системи захисту інформації до передбачуваної загрози.

Будується матриця суміжності зваженого графа інформаційної системи, на головній діагоналі якої знаходиться вага вершин, інші елементи це 1, якщо вершини зв’язані ребром і 0 в противному разі.

Розглядається можливий спосіб моделювання атаки з використанням сукупної моделі інформаційно-технологічної системи й супротивника. Припускається, що здійснення впливу супротивника буде спрямовано безпосередньо на засоби захисту (листки в графі системи), і вплив здійснюється членами-виконавцями організації супротивника. Атака моделюється, вводячи новий зв'язок між вершиною, відповідною до активного члена-супротивника, і тим листком у графі інформаційної системи, який відповідає атакованому засобу захисту, що відобразиться у збуренні матриці суміжності сукупного графа.

У статті [7] розглядається комплексна модель кібератаки на основі теорії графів, яка поєднує класичні уявлення щодо моделювання складних атак з розширеннями, що враховують залежності уразливостей окремих компонентів системи та мережевий статус компонентів. Наведено приклад оцінювання сценарію атаки та зроблено висновки щодо можливості застосування моделі для прогнозування наслідків атаки.

У роботі [8], на відміну [7], використовується орієнтований граф і на його основі побудовано графову модель противника інформаційної системи та показано, як зручне укладання графа, отримане завдяки розбивці графа на класи еквівалентності та порядку, може відігравати принципово важливу роль у вирішенні задачі знищення або обмеження діяльності злочинної групи.

В роботі [9] вирішено задачу підвищення ефективності стеганосистеми шляхом розробки модифікації методу вбудовування повідомлення, запропонованого в [10].

Підвищення ефективності вдалося досягти завдяки запропонованому методу знаходження максимального паросполучення, як основи алгоритму вбудовування повідомлень на основі теорії графів.

Основна частина. Розглянемо приклад, як можна застосувати розвинуту в стеганографії теорію графів до алгоритмів, які вже мають практичне застосування, тобто як і надалі можна розвивати практичну теорію графів.

В роботі [11] пропонується стеганографічний алгоритм просторової області вбудовування в цифрове зображення. Основним принципом розробки є мінімізація впливів вбудованого повідомлення на контейнер. В основу алгоритму покладено порівняння бітових послідовностей контейнера та повідомлення, модифікація елементів контейнера виконується тільки у випадку, коли виявлено неспівпадіння відповідних бітів. Алгоритм дозволяє зменшити викривлення контейнера, зберегти статистики першого порядку та забезпечити стійкість до найбільш відомих статистичних атак.

Повідомлення і пікселі контейнера розбиваються на підпослідовності. Початок підпослідовностей контейнера, в які вбудовується повідомлення, фіксуються в ключі *K*. Але саме цю задачу можна вирішити за допомогою графа.

Розглянемо, яким чином можна фіксувати за допомогою графа підпослідовності контейнера, в які вбудована інформація, яку треба передати адресату. Окрім цього, пропонується дублювати інформацію, яку треба переслати. За рахунок клонування відліків інформації, що вбудовується, алгоритм підвищить свою стійкість не тільки до статистичних але і до інших видів атак таких як, наприклад, зашумлення стегоконтейнера, а в окремих випадках до геометричних атак, таких як поворот та обрізання.

Вузли графа – це стартові відліки підпослідовностей контейнера, в які вбудоване повідомлення, ребра – показують, з якої вершини графа потрібно перемістити в іншу, а саме ту вершину, щоб одержати зв’язне повідомлення.

Оскільки є клони кожного відліку повідомлення, то граф буде представляти собою не ланцюг, а дерево – рис.1.

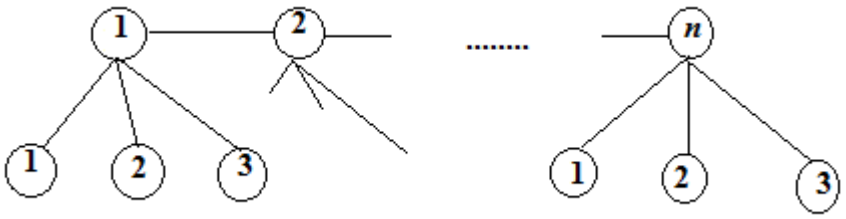

Рис. 1. Граф-дерево розміщення повідомлення

При декодуванні повідомлення, якщо ланцюг графа 1-2-…-*n* не дає зв’язного тексту (шум в каналі зв’язку або навмисно накладений шум, як атака на стегоконтейнер, інші види атак), то є можливість використати листи графа 11, 12 або 13 і так далі *n*1, *n*2, *n*3.

Дублювання окремих блоків інформації дещо перевантажує контейнер, але дає можливість протистояти атакам, які вносять збурення в контейнер, навіть помітні оку, наприклад, накладання шуму достатньо високого рівня, або ж геометричним атакам.

Характеристики алгоритмів, що оперують із графами, зазвичай дуже чутливі до способу їх представлення.

Однією з найбільш простих схем зберігання графа [12] є *таблиця зв'язків* - двовимірний масив, який має n рядків і m стовпців, де m — максимальна степінь вершин в графі $G=(X,E)$. Список суміжності $i-$го вузла зберігається в $i-$ рядку.

Дана схема зберігання надзвичайно проста при реалізації, доступ до списку суміжності чергового вузла — доступ до відповідного рядка матриці, модифікація графа приводить до зміни елементів відповідних рядків матриці без порушення

загальної структури (якщо при модифікації не змінюється m). Однак ця схема може бути надзвичайно неефективною, якщо велика кількість вузлів графа має степінь, меншу (значно), ніж вершина з максимальною степінню, оскільки її (схеми) вимоги до пам'яті визначаються як mn «збережених» елементів.

Найбільш зручною з погляду можливостей проведення модифікацій графа є схема, що використовує *поле зв'язків*. Дана схема містить три одновимірні масиви A, A_s, A_{ind}, перші два з яких мають довжини $2|E|$, останній — $|X|$. Значенням покажчика $A_{ind}(i)$ є початок списку суміжності $i-$го вузла в масиві A. Якщо $A(k)$ — це черговий сусід $i-$го вузла, то $A_s(k)$ — покажчик розташування наступного його сусіда в масиві A. Від'ємне значення $A_s(k)$ говорить про закінчення списку суміжності вузла, що розглядається.

Загальна довжина масивів при такому способі представлення графа — $4|E|+|X|$, що значно більше, ніж у першій схемі. Однак модифікація графа вимагає лише незначних змін у вже сформованій частині масивів.

Другий аспект використання математики в кібербезпеці – це розвиток матричного аналізу в стеганографії (спектральний і сингулярний розклад (SVD) матриці контейнера, в якості якого обирається зображення), який ґрунтовно і докладно представлено в [3].

Наприклад, в роботі [13] оцінюється збурення контейнера, при його стеганоперетвореннi, через оцінку збурень сингулярних чисел його SVD.

В роботі [5] досліджується і обґрунтовується зв'язок чутливості стегоповідомлення і збурень власних векторів матриці контейнера.

Ще одне суттєве використання математики – це застосування в криптографії таких інструментів як модулярні обчислення, теореми Ейлера та Ферма, застосування еліптичних кривих для створення цифрових підписів, використання однонаправлених функцій для хешування паролів та інші.

Розглянемо як можна відомий криптографічний шифр транспозиції модифікувати за допомогою математичних операцій над перестановками та адаптувати його до стеганографії. Оскільки транспозиційний шифр не змінює частоту окремих літер, він все ще сприйнятливий до частотного аналізу, хоча транспозиція дійсно усуває інформацію з пар літер. Тому подальший розвиток цього виду шифру є актуальним.

Для будь-яких перестановок μ і g визначена операція їх добутку $\mu \circ g$, а також операція перестановки оберненої до даної μ^{-1}.

Для реалізації алгоритму, що пропонується, потрібно вміти розв'язувати рівняння, елементами якого є перестановки. Розглянемо рівняння:

$$\mu \circ x = g \tag{1}$$

Оскільки існує така перестановка x для якої виконується рівність (1) і вона єдина, то розв'язком рівняння (1) є:

$$x = \mu^{-1} \circ g \tag{2}$$

До безпосереднього процесу вбудовування повідомлення потрібно виконати препроцесінг і самого повідомлення і контейнера, в якості якого виступає цифрове зображення в градаціях сірого, або ж синя складова кольорового зображення, оскільки зорова система людини менш чутлива до синього кольору.

Елементи повідомлення кодуються цифрами, які належать деякій множині $M = \{1, 2, ..., k\}$. Елементи контейнера послідовно групуються у блоки розміром $1x\ n$. При вбудовуванні повідомлення використовується деякий допоміжний масив *masiv*, в якому знаходиться k перестановок довжини n. Всі перестановки занумеровані. При вбудовуванні елемента повідомлення з кодом i в масиві *masiv* знаходимо перестановку з номером i, перемножуємо її на ключ μ, одержуємо перестановку g. Масив *masiv* не

містить перестановки, добуток якої з ключем μ дає тотожну перестановку. Блоки контейнера, які складаються з однакових елементів, випускаються. Елементи інших блоків переставляються згідно перестановці g тільки в тому випадку, якщо для будь-якої пари елементів, які обмінюються місцями, різниця їх значень не перевищує деяке число d.

Запропонований алгоритм не являється «сліпим», тому для декодування повідомлення потрібна наявність контейнера.

Щоб декодувати повідомлення треба розбити матрицю контейнера та стеганоконтейнера на блоки того самого розміру, що і при вбудовуванні. Порівняти відповідні блоки контейнера та стего, якщо вони співпали, то це означає, що в блок повідомлення не вбудовувалося. У противному разі треба обчислити перестановку μ^{-1}, обернену до ключа μ, та обчислити добуток $h = \mu^{-1} \circ g$. Одержану перестановку h знайти в масиві *masiv*. Порядковий номер, який відповідає h, є кодом елемента вбудованого повідомлення.

Висновок. Математика – це наука, яка дає широке розмаїття інструментів за допомогою яких можна створювати все нові, більш ефективні, методи захисту інформації. Тому її значення та застосування у різних напрямках наукових досліджень, зокрема у сфері інформаційної та кібернетичної безпеки, буде розвиватися і надалі.

В роботі проведено аналіз та дослідження деяких існуючих математичних методів та запропоновано два нових алгоритми, як практична реалізація можливостей математики для модифікації вже існуючих методів.

Розглянуті підходи до застосування теорії графів, матричного аналізу, дискретної математики в інформаційній та кібернетичній безпеці можуть бути впроваджені під час вивчення дисципліни «Математичні основи кібербезпеки», «Основи криптографії», «Основи стеганографії» та інших дисциплін для студентів спеціальності 125 Кібербезпека, а також при підготовці фахівців у процесі науково-дослідної роботи або курсової чи дипломної роботи.

Список літератури

1. Кобозева А.А., Коломийчук А.В. Стеганографический метод, основанный на решении систем линейных алгебраических уравнений. *Праці УНДІРТ*. 2006. №1(45). С. 104–108.
2. Борисенко И.И., Кобозева А.А. Практическая реализация стеганографического метода, основанного на решении системы линейных алгебраических уравнений. *Праці УНДІРТ*. 2006. №3(47). С. 78–83.
3. Кобозева А.А, Хорошко В.А. Анализ информационной безопасности. К.: ГУИКТ, 2009. 251 с.
4. Кобозева А.А. Применение сингулярного и спектрального разложения матриц в стеганографических алгоритмах. *Вісник Східноукр. нац. ун-ту ім. В.Даля.* 2006. №9(103). Ч.1. С.74–82.
5. Нариманова Е.В., Кобозева А.А. Оценка чувствительности стегосообщений к возмущающим воздействиям. *Системні дослідження та інформаційні технології*. 2008. №3. С. 52–65.
6. Борисенко И.И., Трифонова Е.А. Система передачи секретных данных основанная на криптостеганографической технике. *Сучасний захист інформації*. 2020. №1. С. 58–61.
7. Моделювання кібератак засобами теорії графів/ В.А. Савченко та ін. *Сучасний захист інформації*. 2019. №4(40). С. 6–11.
8. Борисенко И.И. Еще один подход к моделированию противника информационной системы с использованием теории графов. *Информатика и математические методы в моделировании*. 2012. №1. С. 70–76.

9. Борисенко І.І., Вінковська І.С. Теорія графів як основа методів вбудовування інформації. *Математика та математичні методи в моделюванні*. 2025. Том 15, №1. С. 39–47.
10. Hetzl S., Mutzel P. A graph-theoretic approach to steganography. *Proc. Communication and Multimedia security.* 2005. P.119–128.
11. Борисенко І.І. Застосування методів порівняння послідовностей в стеганографічних перетвореннях цифрових зображень. *Сучасна спеціальна техніка*. 2014. №2. С. 110–115.
12. Харари Ф. Теория графов. М.: Мир. 1973. 300 с.
13. Борисенко И.И. Оценка возмущения контейнера при его стеганопреобразовании. *Високі технології в машинобудуванні*. 2015. №1. С. 27–32.

MATHEMATICS IN CYBERSECURITY

I.I. Borysenko, L.M.Timoshenko, I.S. Vinkovska

National Odesa Polytechnic University
1, Shevchenko Ave, Odesa, 65044, Ukraine
Email: borisenko.i.i@op.edu.ua

The number of Internet users is growing exponentially every year. At the same time, tens of thousands of cybercriminals emerge every day, who, exploiting the weaknesses of information systems, are capable of stealing data. Therefore, the topic of countering cyberattacks is and will remain relevant now and, most likely, for decades to come. Modern technologies using mathematical data analysis make it possible to counter illegal activities online and characterize our current stage of development. Cybersecurity is a set of measures aimed at protecting various information systems and networks from cyberattacks. The protection of data is based on advanced technologies and information security methods, which in turn are based on fundamental mathematical knowledge. It is precisely branches of mathematics such as logic, combinatorics, matrix analysis, and especially graph theory, or graph technologies, that have a significant influence and importance among all mathematical methods. The structured system of specialized mathematical terms and notations allows complex and subtle concepts to be described simply and accessibly, both geometrically (graphs) and algebraically (matrices). The analysis of scientific works made it possible to identify the main directions for applying the properties, characteristics of graphs, and graph algorithms in information and cyber security. Among them, research related to the use of graphs in information systems and programming, modeling, analysis and application of attack graphs, cryptographic and steganographic transformations, and building decision trees in decision-making tasks under conditions of risk and uncertainty was highlighted. The attention of scientists and researchers was also drawn to other mathematical areas. A digital image chosen as a container in steganography is mathematically represented by a matrix. A message embedded in the container, which is not an image, can be represented in matrix form, or preprocessed using algorithms for working with sequences. Thus, the extensive use of mathematics in information and cybersecurity, and the mathematical approach to developing new and modifying existing cybersecurity applications, makes the choice and relevance of this research justified.
Keywords: mathematical methods, cybersecurity, graph algorithms, cryptography, steganography.