УДК 004.056

Афанасьєва Д. С., студентка 1 курсу спеціальності 122 «Комп'ютерні науки»
Ніколюк П. К., д.ф.-м.н., професор, професор кафедри комп'ютерних технологій

ЗАСТОСУВАННЯ ТЕОРІЇ ГРАФІВ У КІБЕРНЕТИЧНІЙ БЕЗПЕЦІ

Донецький національний університет імені Василя Стуса, м. Вінниця

Поява мережі Інтернет спричинила утворення величезної кількості людей, які користуються нею. На жаль, кожного дня з'являються десятки тисяч кіберзлочинців, які, використовуючи слабкі місця системи, здатні викрадати дані, тому дана тема є та буде актуальною для нас завжди. 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 систем та мережі від кібератак. Для здійснення охорони даних також необхідні фундаментальні знання дискретної математики. Саме розділ теорія графів, або графові технології, має великий вплив та значення серед усієї кількості математичних методів, адже завдяки ним можна вирішити проблеми майже в кожній відомій вам дисципліні. Але, на жаль, ця тема є однією з найскладніших для застосування та розуміння.

Граф – це певна дискретна структура, яка складається з вершин та зв'язків (ребер), які з'єднують ці вершини. Якщо розглядати графи з алгебраїчної точки зору, то вони можуть бути представлені матрицями чи списками суміжності. Ці елементи є ефективним засобом перетворення великого обсягу інформації в зрозумілу візуальну форму без втрати інформативності. Відповідно до принципів побудови, типів вершин виділяють різні типи графів: неорієнтовні, орієнтовні, з петлями, ейлерові, гамільтонові, змішані, порожні тощо. Окрім цього, графи можна подати як лінійні структури даних, наприклад, таблиці чи масиви, в яких сусідні елементи можуть бути пов'язані відношеннями. [1]

Сучасне програмування також неможливо уявити без використання графових алгоритмів, які допомагають автоматизувати процес.

Розглянемо приклад застосування графів для блокування фішингу в мережі. Фішинг (з англ. phishing — видобування) – вид кібершахрайства, коли відбувається створення вебресурсів, які схожі на надійні організації, з метою отримання даних акаунтів чи платіжних систем користувача. Часто використовується масова розсилка електронних листів з проханням увійти на сайт, аби отримати ідентифікаційну інформацію. Аби знешкоджувати злочинців, відбувається пошук потенційних доменів шахраїв, адже вони пов'язані кількома сутностями:

1) a name server – сервер, який реалізує службу для отримання відповідей на запит в мережі;
2) a registar – комерційна компанія, яка займається бронюванням доменів в мережі Інтернет;
3) an IP address – унікальний числовий запис, що присвоюється кожному пристрою для використання в мережі протоколу зв'язку. [2]

На основі отриманих даних створюється граф мережевих даних, який допомагає виявляти потенційні домени шахраїв та блокувати їх. (рис. 1) [2]

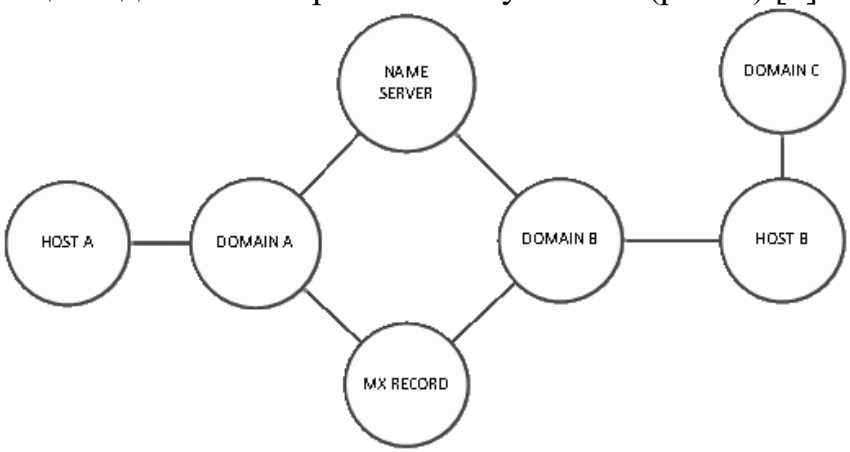

Рисунок 3. Модель графа мережевих даних, створений компанією Cisco

Також графи використовують й у доволі нестандартний спосіб. Аби удосконалювати системи, потрібно знаходити слабкі місця в ній та прибирати їх. Для таких цілей відбувається моделювання кібератаки на систему з використанням графа атак (спеціальний метод, який здатен знаходити уразливості та опрацьовувати їх взаємодію).

До графів атак відносять: умовно-орієнтовний граф залежностей, граф залежних експлойтів та граф з перерахування станів. Їх застосовують під час розслідування комп'ютерних атак, прогнозування можливих дій кіберзлочинців та виявлення слабких місць системи захисту. [1]

Іноді для безпеки даних потрібно виконати шифрування у вигляді послідовностей бінарних чисел різної довжини. Цей процес називається криптографією перетворень, яку зручно здійснювати та візуалізовувати за допомогою бінарних дерев-графів. [1]

Отже, застосування теорії графів для візуального зображення даних безпеки дозволяє створювати систему обліку та розвідки, яка може бути використана для аналізу можливих кібератак в майбутньому та вже наявних вразливостей системи. Також вони дають змогу розробляти моделі мережевих даних для пошуку кіберзлочинців.

Список літератури

1) Математичні моделі в кібербезпеці: графи та їх застосування в кібербезпеці: https://csecurity.kubg.edu.ua/index.php/journal/article/view/288/248

2) Cyber security: how to use graphs to do an attack analysis URL: https://linkurious.com/blog/cyber-security-use-graphs-attack-analysis/

3) Graph Theory: A Mathematical Approach to Activating Security Data: https://mytechdecisions.com/network-security/graph-theory-mathematical-approach-activating-security-data/