УДК 519.6

Кондратенко Н. Р.
Немировська Д. О.

Використання графів у виявленні кіберзагроз у соціальних мережах

Вінницький національний технічний університет

Анотація

Стаття містить загальну інформацію щодо використання графів у виявленні кіберзагроз соціальних мереж.

Ключові слова: соціальні мережі, кіберзагроза, граф.

Abstract

The article contains general information on the use of graphs in the detection of cyber threats to social networks.

Keywords: social networks, cyber threat, graph.

Соціальні мережі є невід'ємною частиною сучасного життя. Вони дозволяють людям спілкуватися, ділитися інформацією, розважатися та навчатися. Крім того, мають великий вплив на суспільство. Вони дозволяють підвищувати свою видимість та популярність, просувати свої товари та послуги, залучати та обслуговувати клієнтів, збирати та аналізувати дані, співпрацювати з партнерами та колегами, навчатися та вчити інших, досліджувати та вирішувати проблеми, створювати та поширювати контент, організовувати та відвідувати заходи тощо. Однак, разом зі значними перевагами, соціальні мережі несуть і ризики – кіберзагрози.

Кіберзагроза – наявні та потенційно можливі фактори, що ставлять під загрозу інтереси людини, суспільства та держави через порушення доступності, повноти, цілісності, достовірності, автентичності режиму доступу до інформації, що необхідна для коректної роботи критичних об'єктів національної інформаційної інфраструктури[1]. Це один з найбільших викликів, з якими стикаються користувачі соціальних мереж. Кіберзагрози можуть мати різні форми та цілі, але їх спільною ознакою є те, що вони використовують соціальні мережі як канал для поширення або виконання шкідливих дій. Це може бути крадіжка даних, шантаж, шпигунство, саботаж, пропаганда, тероризм тощо. Такі атаки можуть завдати значної шкоди не тільки окремим користувачам, але й цілим організаціям, суспільствам та державам. За інформацією від провідної американської компанії з питань кібербезпеки Palo Alto Networks, існує 10 основних типів кіберзагроз у соціальних мережах(для компаній): хробаки, фішинг, трояни, витоки даних, скорочені посилання, ботнети, постійні загрози, підробка міжсайтових запитів, видавання себе за іншу особу та довіра[2]. Для виявлення та запобігання більшості цих загроз дедалі частіше використовуються методи та алгоритми аналізу графів.

Графи - це математичні структури, що містять вершини та ребра, які їх з'єднують. Вони можуть бути використані для моделювання соціальних мереж, де вершини представляють користувачів, а ребра - їх взаємодії. Ці взаємодії можуть включати дружбу, обмін повідомленнями, спільні інтереси та інше. Соціальна мережа у вигляді графі буде мати математичний вигляд G = (V, E), де V - це вершини, E - ребра, а N - кількість вершин. Щільність графа, яка визначається як відношення кількості ребер до максимально можливої кількості ребер, є надзвичайно корисною для аналізу. Інші характеристики мережі можуть бути визначені за допомогою різних параметрів, таких як кількість шляхів певної довжини, мінімальна кількість ребер, які потрібно видалити, щоб розбити граф на окремі частини, та інше. Центральність вершини, яка вимірює її важливість в мережі, може бути визначена за допомогою різних метрик. Наприклад, ступінь центральності визначається кількістю ребер, які прилягають до вершини. Дана інформація може вказувати на популярність або комунікабельність користувача, його активність у групах. Близькість центральності вимірює, наскільки легко інформація може поширюватися від одного користувача до інших. Вона визначається як обернена величина нормалізованої суми всіх відстаней від даної вершини до всіх інших вершин. Такий параметр дозволяє оцінити, наскільки близько користувач до всіх інших користувачів мережі[3]. Однією з

найпоширеніших метрик центральності є посередництво центральності. Вона визначається як частка найкоротших шляхів між усіма парами вершин, які проходять через дану вершину. Посередництво центральності показує, наскільки важливий учасник для забезпечення зв’язності мережі. Якщо учасник має високу центральність, то він може контролювати потік інформації в мережі, а також бути потенційною мішенню для кібератак. Іншою популярною метрикою центральності є власна векторна центральність. Вона враховує не тільки кількість зв’язків учасника, але й якість цих зв’язків. Власна векторна центральність вершини пропорційна сумі власних векторних центральностей вершин, з якими вона з’єднана. Це означає, що учасник має більшу власну векторну центральність, якщо він пов’язаний з іншими учасниками, які також мають багато зв’язків. Власна векторна центральність дозволяє визначити, хто є лідерами думок або авторитетами в мережі[4].

Застосування аналізу графів у кібербезпеці дозволяє виявляти небезпечні структури та аномалії в цьому віртуальному просторі. Одним із ключових напрямків використання графів у кібербезпеці є виявлення аномалій. Алгоритми аналізу графів можуть ідентифікувати незвичайні або підозрілі зв'язки між користувачами, що може свідчити про спроби атак або використання соціальних мереж для поширення шкідливого вмісту. Наприклад, за допомогою графових алгоритмів можна виявити масові розсилки фішингових повідомлень або групи користувачів, які спільно взаємодіють для поширення шкідливих програм. Аналіз графів також може допомагати в ідентифікації фейкових акаунтів та їхніх зв'язків, що є частою практикою для кіберзлочинців. Графи можуть вказувати на ключові вузли або користувачів, які мають великий вплив у соцмережі. Це може бути використано для раннього виявлення потенційно небезпечних областей та їхнього подальшого моніторингу. Якщо певний користувач стає центральною фігурою в графі та розвиває непередбачувані зв'язки, це може слугувати сигналом про можливу кіберзагрозу.

На основі результатів аналізу графів можна розробити та впровадити ефективні заходи безпеки. Це може включати автоматизовані системи сповіщення про підозрілі активності, блокування акаунтів чи груп, що викликають аномалії, а також вдосконалення систем відслідковування та аналізу для попередження майбутніх загроз.

Висновок

Застосування графів у виявленні кіберзагроз у соцмережах відкриває нові можливості для ефективного контролю та захисту від кібербезпеки. Аналіз структури графів дозволяє виявляти патерни, що можуть свідчити про кіберзагрози, та реагувати на них невідкладно. З використанням цих інструментів можна забезпечити безпеку користувачів та підтримувати стійкість соцмереж проти різноманітних кіберзагроз.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. https://goal-int.org/ponyattya-ta-zmist-kiberzagroz-na-suchasnomu-etapi/
2. https://www.computerworld.com/article/2753616/top-10-social-networking-threats.html
3. https://arxiv.org/ftp/arxiv/papers/1805/1805.06680.pdf
4. https://www.bing.com/

Кондратенко Наталія Романівна – професор кафедри Захисту інформації, Вінницький національний технічний університет, м. Вінниця, Україна, e-mail: kondrn2014@gmail.com

Немировська Дар’я Олександрівна – студентка групи 1БКС-22б, Факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, Україна, e-mail: nemyrovskadaria@gmail.com

Kondratenko Nataliia Romanivna - Professor, Department of Information Security, Vinnytsia National Technical University, Vinnytsia, Ukraine, e-mail: kondrn2014@gmail.com

Nemyrovska Daria Oleksandrivna - student of group 1BKS-22b, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, Ukraine, e-mail: nemyrovskadaria@gmail.com