



**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
УКРАЇНИ "КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ
ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО"**



**НАВЧАЛЬНО-НАУКОВИЙ
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ**



**THEORETICAL AND APPLIED
CYBERSECURITY**

**Перша Всеукраїнська
науково-практична конференція,
присвячена 100-річному ювілею
академіка В.М. Глушкова
Матеріали конференції**



Київ – 2023

Перелік використаних джерел

1. Alexander E. Farrell, Hisham Zerriffi, Hadi Dowlatabadi Energy infrastructure and security. Annual Review of Environment and Resources. 2004. Vol. 29 P. 421-469.
2. I. Andrea, C. Chrysostomou and G. Hadjichristofi Internet of Things: Security vulnerabilities and challenges, IEEE Symposium on Computers and Communication (ISCC), Larnaca, Cyprus. 2015, pp. 180-187.

ІЄРАРХІЧНЕ ФОРМУВАННЯ ПРИЧИННО-НАСЛІДКОВИХ МЕРЕЖ НА ОСНОВІ CHATGPT

Д.В. Ланде¹, Л.Л. Страшной²

¹ІНН ФТІ КПІ ім. Ігоря Сікорського

²The University of California, Los Angeles (UCLA)

Ця робота присвячена опису методики формування причинно-наслідкових (каузальних) мереж шляхом багаторазового звернення до системи ChatGPT, а також візуалізації та аналізу цих мереж за допомогою системи Gephi. Методика базується на використанні системи ChatGPT, попередньо генеративного навченого на великих текстових корпусах перетворювача, який використовує можливості штучного інтелекту для виконання промтів користувачів. Методика охоплює засоби аналізу та візуалізації сформованих мереж за допомогою програми Gephi. У статті показано можливість побудови причинно-наслідкових мереж концептів на основі використання Chat GPT, що дозволяє вирішувати завдання, які раніше вимагали залучення великих ресурсів (людських та тимчасових). У методиці інтегруються засоби інтелектуальної текстової аналітики та аналізу мереж, а також їхня візуалізація.

Ключові слова: ChatGPT, Каузальні мережі, Моделі предметної області, Штучний інтелект, Візуалізація графів, Кібербезпека

Вступ

Останнім часом великі лінгвістичні моделі, такі як ChatGPT набувають все більшого поширення в багатьох областях. Найпоширеніші застосування - це машинний переклад, реферування текстів, узагальнення різного рівня, наприклад, формулювання питань до навчальних матеріалів. Зокрема, ChatGPT від OpenAI – це Генеративний Попередньо навчений Трансформер (GPT), який використовує обробку природної мови для виконання промтів користувачів, використовуючи широкі можливості області штучного інтелекту [1].

Величезні можливості в екстрагуванні основних понять, іменних сутностей дозволяють використовувати ChatGPT у фактографічних системах, зокрема, в медицині, економіці [2]. Інтелектуальні чати інтегруються із зовнішніми системами, такими як геоінформаційні [2], системи аналізу та візуалізації графів, мереж [3]. Зокрема, авторами у роботі [4] показано, як і формувати мережі зв'язків персонажів літературних творів, мережі предметних областей зі зв'язками типу «загальне-приватне».

Ця робота присвячена опису методики формування причинно-наслідкових (каузальних) мереж шляхом багаторазового звернення до системи ChatGPT, а також візуалізації та аналізу цих мереж за допомогою системи Gephi (gephi.org) – найпопулярнішої програми візуалізації графових структур із вільною ліцензією [5]. Для завантаження даних у середу Gephi цілком підходить формат CSV, тому всі запити до ChatGPT будуть супроводжуватись вимогою до формату.

Сформовані причинно-наслідкові мережі забезпечать можливість переходу до сценарного аналізу. Основна проблема, що виникає під час проведення сценарного аналізу на основі каузальних мереж полягає саме у створенні таких систем, що у традиційних випадках потребує великих ресурсних витрат, залучення експертів.

Формування мережі на базі простого ієрархічного звернення до ChatGPT

Нехай нас, наприклад, цікавить проблематика витоку даних, навіщо попросимо у ChatGPT видати відомі їй причини цього явища. Тобто, центральним вузлом майбутньої мережі має стати поняття "data leakage". Успішне відпрацювання такого запиту визначить другий рівень ієрархії - поняття пов'язані з витоком даних - її причини. Після цього для кожного такого поняття також вимагають безліч причин, що вплинули на нього. Такий процес може тривати нескінченно, але в роботі зупинимося на трьох рівнях. Незважаючи на ієрархічне формування такої каузальної мережі, отримана мережа загалом не буде строго ієрархічною структурою.

Запропонувавши ChatGPT відпрацювати деякий запит, отримаємо множину причин первинного поняття. Система ChatGPT може допомогти отримати зміст CSV-файлу (поля, відповідні іменам понять, розділені точкою з комою). Для цього можна застосувати, наприклад, такий запит до системи ChatGPT:

→List the causes of **data leakage** in cyber security. The reason is to use no more than three words. The results should be presented in the format "cause;**data leakage**". Each such entry - from a new line

Система видає відповідь приблизно такого вигляду:

human error; data leakage
weak passwords; data leakage
insider threats; data leakage
misconfigured systems; data leakage
phishing attacks; data leakage
unpatched software; data leakage
malware infection; data leakage
social engineering; data leakage
third-party access; data leakage
stolen devices; data leakage

Запити наступного рівня будуть ставитись до наведених у відповіді концептів і мати вигляд, що повністю відповідає первинному запиту, наприклад:

→List the causes of **human error** in cyber security. The reason is to

use no more than three words. The results should be presented in the format "cause; **human error**". Each such entry - from a new line

Об'єднані в одному CSV-файлі відповіді ChatGPT завантажуються для аналізу та візуалізації програми Gephi.

Завантаживши отримані дані до системи Gephi, вибираємо розмір вузлів, пропорційний ступеня (кількості суміжних зв'язків) і розділивши мережу на кластери за критерієм модулярності отримуємо наочний граф (Рис. 1).

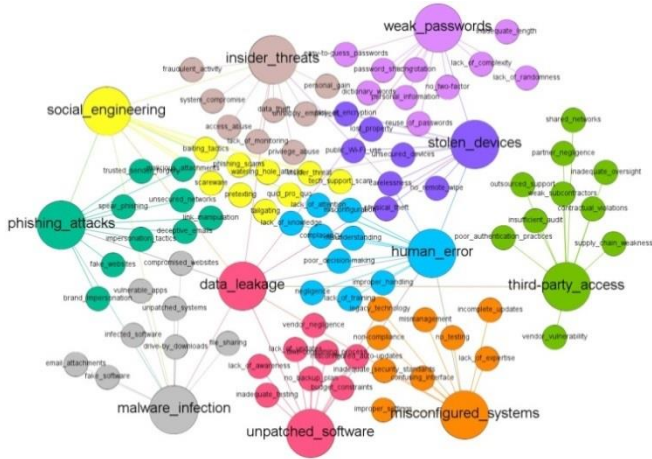


Рисунок 1. Спрямована первинна каузальна мережа, отримана шляхом найпростішого ієрархічного звернення до ChatGPT

Найбільш впливові вузли цієї мережі (найбільший Out-Degree), це: human error (5), social engineering (4), weak passwords(3), phishing attacks(2).

Очевидно, сформована мережа слабопов'язана, неповна, представлені в ній концепти можуть не точно відобразити причини та наслідки. Вважатимемо, що це мережа, отримана в результаті опитування лише одного штучного експерта.

Формування мережі на основі ієрархічного звернення рою віртуальних експертів до ChatGPT

Система ChatGPT у різні моменти під час обробки тексту може видавати різні варіанти відповідей, причому правильне, і з погляду людської логіки цілком «обґрунтовані». Кожну таку відповідь можна сприймати як відповідь деякого віртуального експерта [3]. Можна припустити, що узагальнюючи відповіді множини (рою) подібних експертів можна отримати більш повну та точну відповідь. Реалізуючи рій віртуальних експертів ми по кілька разів задаємо одні й ті самі запити, що розглядаються в минулому випадку, які стосуються як першого, так і другого рівня ієрархії. Після отримання відповідей від системи, об'єднуємо їх у загальний CSV-файл і передаємо для аналізу та візуалізації програмі Gephi. Завантаживши отримані дані до системи Gephi, отримуємо граф, поданий на Рис. 2. На практиці мережа може поповнюватися доти, доки не стане достатньо повною за оцінкою експерта-людини.

Найбільш впливові вузли цієї мережі (найбільший Out-Degree), це:

Human error (7), social engineering (4), weak passwords(3), phishing attacks(2), unpatched systems(2), insider threats(2).

Як бачимо, кількість важливих концептів збільшилася порівняно з попереднім випадком.

Формування мережі на основі узагальнення ієрархічного звернення рою віртуальних експертів до ChatGPT

Сформований у попередньому прикладі граф, маючи відносно велику повноту концептів, водночас може містити неточну інформацію, помилково видану ChatGPT при обробці окремих запитів. З припущення, що ймовірність появи тих самих помилок щодо невелика, можна винести з розгляду при побудові мережі концепти, які зустрічаються рідше заданого порогу.

У наведеному нижче випадку (Рис. 3) не розглядалися концепти, які зустрічалися рідше 2 разів.

Найбільш впливові вузли цієї мережі (найбільший Out-Degree), це:

Human error (5), social engineering (3), phishing attacks(2), unpatched systems(2).

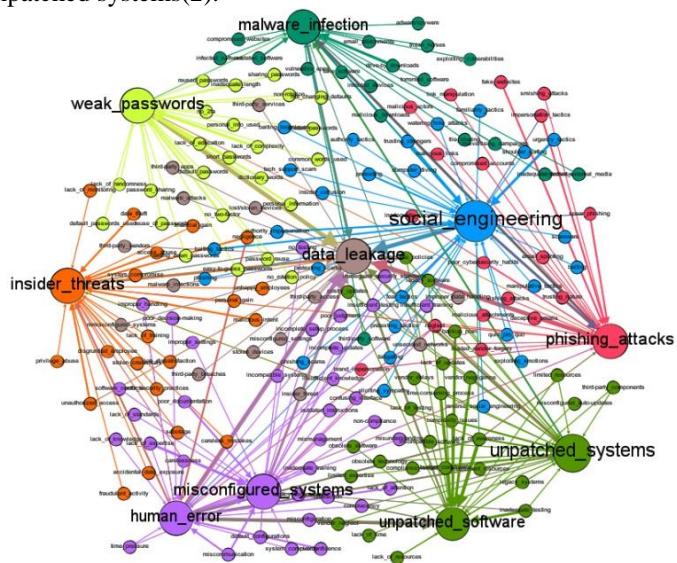


Рисунок 2. Спрямована повна каузальна мережа, отримана шляхом ієрархічного звернення рою віртуальних експертів до ChatGPT

Висновки

На підставі експертних оцінок можна зробити висновок, що первинна каузальна мережа, отримана шляхом найпростішого ієрархічного звернення до ChatGPT, охоплює найбільшу кількість концептів, які відносно слабо пов'язані (мережа близька до ієрархічної), але завдяки повноті може бути непоганою «сировиною для подальшої аналітичної обробки».

Статистично оброблена друга мережа, каузальна мережа, отримана шляхом ієрархічного звернення рою віртуальних експертів до ChatGPT, є більш точною, ніж первинна мережа і, нарешті, третя мережа, отримана шляхом узагальнення ієрархічного звернення рою віртуальних експертів до ChatGPT, що має найбільший середній свідчить про найбільшу взаємодію окремих концептів, що впливають на ціль у цій причинно-наслідковій мережі. Мабуть, така мережа є найбільш прийнятною для подальшого застосування сценарного аналізу.

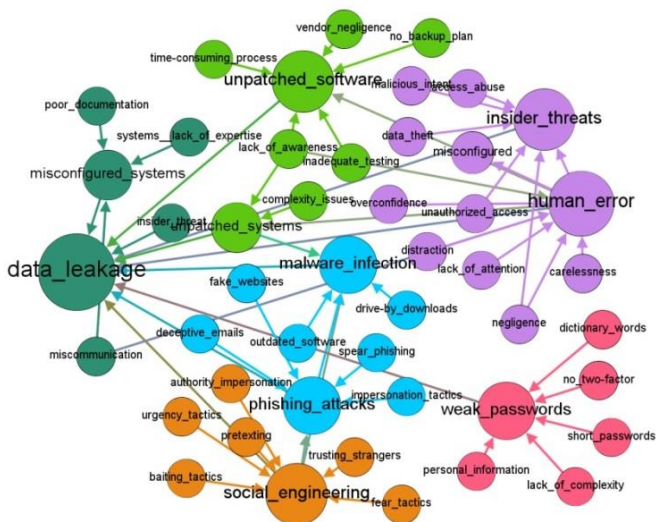


Рисунок 3. Направлена каузальна мережа, отримана шляхом узагальнення ієрархічного звернення рою віртуальних експертів до ChatGPT

Незважаючи на суттєвий вигрaш у ресурсах (як тимчасових, так і людських), важливо зазначити, що як сам процес побудови каузальних мереж, так і інтерпретація результатів, вимагають від дана сайнсиста досвіду в предметній галузі, що вивчається, і як і раніше необхідно

спостереження з боку людини для забезпечення достовірності та точності результатів.

Перелік використаних джерел

1. St. Wolfram. "What Is ChatGPT Doing ... and Why Does it Work?". – Wolfram Media, Inc. March 9, 2023. 112 p.
2. Brady D. Lund, Ting Wang, Nishith Reddy Mannuru, Bing Nie, Somipam Shimray, Ziang Wang. ChatGPT and a new academic reality: Artificial Intelligence-written research papers and the ethics of the large language models in scholarly publishing. JASIST, 2023. / Volume74, Issue5. Pages 570-581. DOI: <https://doi.org/10.1002/asi.24750>
3. Tamilla Triantoro. Graph Viz: Exploring, Analyzing, and Visualizing Graphs and Networks with Gephi and ChatGPT (March 30, 2023). ODSC Community.
4. Lande, Dmitry and Strashnoy, Leonard, Concept Networking Methods Based on ChatGPT & Gephi (April 17, 2023). SSRN. Available at <http://dx.doi.org/10.2139/ssrn.4420452>
5. Ken Cherven. "Mastering Gephi Network Visualization". – Packt Publishing, 2015. 378 p.

АНАЛІЗ МЕРЕЖЕВОГО ПРОТОКОЛУ ДЛЯ ВИЯВЛЕННЯ ОЗНАК АТАК НА КРИТИЧНУ ІНФРАСТРУКТУРУ

Таран В. Є., Коломицев М. В.

Навчально-науковий Фізико-технічний інститут КПІ ім.

Ігоря Сікорського, Київ, Україна

viktoriiatar1@gmail.com, box144.85@gmail.com

Один з найважливіших компонентів для надійної роботи Інтернету - це протокол мережевої інфраструктури Border Gateway Protocol (BGP). Використовуючи BGP, відбувається обмін повідомленнями про маршрутизацію, що дозволяє сигналізувати про наявні активні та несправні маршрути. Проте, під час катастрофічних подій великого масштабу, таких як військові дії або кібервійна,

ЗМІСТ

	Стор.
<i>Л.Б. Алексейчук, О.М. Новіков</i>	3
Логіко-ймовірнісне моделювання ризиків кібербезпеки об'єкту критичної інфраструктури	
<i>Д.Р. Друзь, С.А. Смирнов</i>	7
Адаптивна стратегія розподілу ресурсу для захисту інформації	
<i>В.Ю. Зубок</i>	11
Кіберстійкість критичної інформаційної інфраструктури в умовах енергетичної кризи	
<i>Е.В. Абдуллаєва, Л.Ю. Гальчинський</i>	17
Аналіз вразливостей та форензика мережі ethereum: забезпечення безпеки та цілісності блокчейну	
<i>Д.О. Шатковська, І.В. Стьопочкіна</i>	21
Механізми моніторингу кібербезпеки об'єктів енергетичної інфраструктури	
<i>Д.В. Ланде, Л.Л. Страшиной</i>	24
Ієрархічне формування причинно-наслідкових мереж на основі ChatGPT	
<i>В.Є. Таран, М.В. Коломицев</i>	31
Аналіз мережевого протоколу для виявлення ознак атак на критичну інфраструктуру	
<i>А. С. Живодьоров, Ю. Г. Даник</i>	35
Виявлення і протидія підміні базової станції в мережах мобільного зв'язку 5G	
<i>М. Маманчук, Д. Прогонов</i>	42
Локалізація позицій стегобітів, вбудованих до зображень-контейнерів з використанням адаптивних стеганографічних методів HUGO та wow	
<i>В. Ustyenko, A. Wróblewska, O. Pustovit</i>	45
Quadratic multivariate transformations in terms of Extremal Graph Theory as implemented encryption tools	