Приурочено до 125-ї річниці створення
Національного технічного університету України
“Київський політехнічний інститут імені Ігоря Сікорського”

МАТЕРІАЛИ
VI науково-практичної конференції курсантів (студентів), аспірантів, докторантів та молодих учених
“АКТУАЛЬНІ ПИТАННЯ ЗАСТОСУВАННЯ СПЕЦІАЛЬНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ”

23 листопада 2023 року

Київ – 2023

УДК 621

Матеріали VI науково-практичної конференції курсантів (студентів), аспірантів, докторантів та молодих учених "Актуальні питання застосування спеціальних інформаційно-комунікаційних систем". Київ : ІСЗЗІ КПІ ім. Ігоря Сікорського, 2023. 394 с.

У матеріалах VI науково-практичної конференції курсантів (студентів), аспірантів, докторантів та молодих учених "Актуальні питання застосування спеціальних інформаційно-комунікаційних систем" опубліковано тези доповідей, в яких висвітлюються питання дослідження, аналізу й узагальнення нових теоретичних і практичних результатів у сферах кібербезпеки та кіберзахисту, інформаційної безпеки держави, інформаційних технологій та електронних комунікацій, а також залучення здобувачів вищої освіти до активної наукової діяльності.

РЕЦЕНЗЕНТИ:

Олександр ПУЧКОВ	К.філос.н., професор
Сергій КОНЮШОК	К.т.н., доцент
Владислав ГОЛЬ	К.т.н., професор
Вадим РОМАНЕНКО	К.т.н., доцент
Дмитро МОГИЛЕВИЧ	Д.т.н., професор
Ігор СУБАЧ	Д.т.н., доцент
Ярослав ЗІНЧЕНКО	К.т.н., с.н.с.

Рекомендовано до друку Вченою радою ІСЗЗІ КПІ ім. Ігоря Сікорського (протокол № 4 від 22.11.2023).

Артем ПЕДУНОВ;
Дмитро ЛАНДЕ, д.т.н., професор

ОБ'ЄДНАННЯ БЛИЗЬКИХ ЗА ЗМІСТОМ ВУЗЛІВ ПРИ ФОРМУВАННІ МЕРЕЖІ КІБЕРНЕТИЧНИХ ВРАЗЛИВОСТЕЙ

Анотація Робота розглядає процедуру удосконалення мережі кібернетичних вразливостей шляхом поєднання вузлів, близьких за змістом понять, за допомогою генеративного штучного інтелекту. Сформовано відповідний промпт та показано покращення показників мережі шляхом об'єднання близьких за змістом вузлів.

Summary. The work examines the procedure for improving the network of cybernetic vulnerabilities by combining nodes - concepts close in content with the help of generative artificial intelligence. A corresponding prompt is formed and improvement is shown by combining nodes corresponding to concepts close in content.

Ключові слова: кібернетичні вразливості, генеративний штучний інтелект, поєднання вузлів, промпт, характеристики мережі

На цей час за допомогою генеративного штучного інтелекту (ГСШ) можливе формування мереж предметних галузей, що раніше вимагало великих ресурсних і часових витрат. Зокрема, за адресою https://bigsearch.space/datasets/cyber_security_vulnerability.txt знаходить-ся датасет, присвячений вразливостям кібербезпеки, який дозволяє приймати важливі рішення в у цій галузі. Разом з цим, цей датасет містить ряд вузлів-понять, які є за своєю сутністю змістовними синонімами. Поєднання таких синонімічних ланцюжків, зміна їх однаковими сутностями має зробити мережу більш лаконічною, зрозумілою користувачу-експерту.

Тому актуальність роботи полягає в необхідності оптимізації мереж, що створюються за допомогою ГСШ.

Основна мета роботи полягає в об'єднанні вузлів-понять для створення систематизованої структури, спрямованої на підвищення загального рівня сприйняття предметної області.

Мережу, що розглядається, було створено шляхом виконання промптів до системи chatgpt типу "Reason Prompt: Name 10 reasons for the concept of "Weak encryption" as part of the concept of "cyber security vulnerability". Each reason must contain no more than three words. In the format "reason; Weak encryption". Each entry on a separate line" (https://ssrn.com/abstract=4464477). У результаті було сформовано мережу, яка поряд з великими перевагами (актуальний і повний склад понять,

доступне візуальне відображення), має недолік, вона містила деяку кількість практично однакових за змістом понять, що інколи знижує сприйняття мережі, ускладнює процес підтримки прийняття рішень. Структуру цієї мережі наведено на Рис. 1. Мережа містить 162 вузли і 176 зв'язків, дуже малу щільність 0,013.

Шляхом виконання промпту до системи chatgpt вигляду

"Replace each concept in the list of pairs of concepts with a shorter concept that is close in meaning, and output it in the same format in English (in pairs, through ;). The list consists of pairs of concepts:

Weak encryption; cyber security vulnerability

Malware infections; cyber security vulnerability…"

Була отримана узагальнена мережа, наведена на Рис. 2, яка містить лише 110 вузлів і значно більшу щільність 0,047. Основні вузли-концепти цієї мережі: "SECURITY VULNERABILITY", "SECURITY WEAKNESS", "MALICIOUS SOFTWARE", "INSIDER RISKS", "LACK OF UPDATES", "SOCIAL MANIPULATION", "DATA BREACHES", "DECEPTIVE MESSAGES", "CONFIGURATION FLAWS", "CYBERSECURITY VULNERABILITY", "ENCRYPTION FLAW".

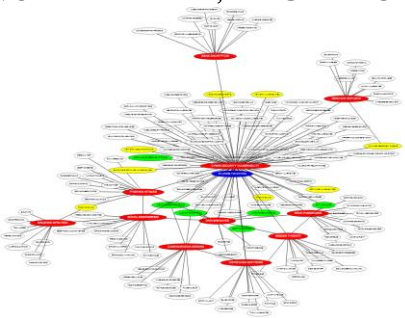

Рис. 1. Вихідна мережа

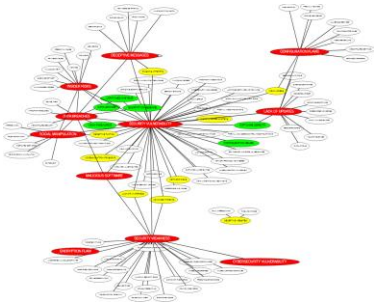

Рис. 2. Удосконалена мережа

Висновки. Слід відзначити, що розроблена методика консолідації вузлів у мережі предметної області вразливостей кібербезпеки, надає оптимізацію використання ресурсів, а саме, зменшення кількості вузлів сутностей, що розглядаються, збільшення щільності мережі, явним виділенням наявних кластерів. Цей підхід дозволяє створити систематизовану структуру, яка сприяє кращій візуалізації, зрозумілості структури мережі, що сприяє підвищенню рівня підтримки прийняття рішень в галузі кібербезпеки. Важливість алгоритму використовується до швидко змінюючихся умов кіберпростору забезпечує стійкість та захист від сучасних кіберзагроз.