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).

Каріна БОНДАРЕНКО;
Дмитро ЛАНДЕ, д.т.н., професор

МЕТОД ПОБУДОВИ Й АНАЛІЗУ МЕРЕЖІ СУБ'ЄКТІВ ПРОТИСТОЯНЬ У КІБЕРПРОСТОРІ

Анотація. У даній роботі розглянуто побудову та аналіз мережі злочинних хакерських угрупувань, їх інструментарію та вразливостей на базі відібраних в Інтернеті документів за допомогою сервісу генеративного штучного інтелекту.

Summary. This paper considers the construction and analysis of a network of criminal hacker groups, their tools and vulnerabilities based on documents selected on the Internet using the generative artificial intelligence service.

Ключові слова: мережа, хакерські угрупування, штучний інтелект.

Фахівці в галузі інформаційної та кібернетичної безпеки завжди мають бути орієнтовані на основні поняття та об'єкти в цій сфері. Проте, оскільки кібербезпека постійно еволюціонує, постійно з'являються нові поняття та об'єкти. У цій галузі такими об'єктами можуть бути хакерські групи, шкідливі програми, різновиди кібератак, вразливості та багато іншого.

Дана робота допоможе у майбутньому успішно слідкувати за кіберзлочинними угрупуваннями та їх інструментарієм. З кожною появою нового угрупування будуть отримані формалізовані дані, які допоможуть підвищити рівень обізнаності спеціалістів з кіберзахисту, а в подальшому підвищить рівень захищеності інформаційних систем.

Також побудова та аналіз мережі допомагають кібербезпецістам виявляти потенційні загрози, вчасно реагувати на кібератаки та розробляти ефективні стратегії захисту. Ця візуалізація дозволяє аналізувати структуру ієрархії злочинних груп, їх інструментарію, атак і виділяти ключові фігури в їхньому складі.

Невід'ємною складовою інформаційної та кібернетичної безпеки є методологія та набір технологій розвідки відкритих джерел (OSINT), спрямований на виявлення та видобування цих прихованих знань, їх узагальнення та подальший аналіз. У цій роботі представлена методика видобування понять з текстів документів, доступних в мережі, які стосуються кібербезпеки, зокрема хакерських угрупувань, що діють в усьому світі та беруть активну участь в сучасних кіберконфліктах, а також їхніх інструментів та вразливостей. Для досягнення такого результату була вирішена низка завдань, зокрема, збір інформації, її

обробка, витяг необхідних даних, встановлення відповідних зв'язків, а у подальшому формування мережі.

Для початку за допомогою генеративного штучного інтелекту потрібно знайти інформацію про найбільш відомі хакерські угрупування світу та зберегти це у відповідний файл, який у подальшому буде аналізуватися chatpdf (Рис.1). Далі отримана інформація буде записана у файл з розширенням CSV за допомогою функцій для бібліотек мови Python.

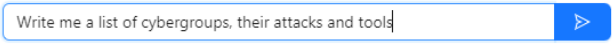

Рис. 1 - Промт для отримання інформації про хакерські угрупування.

Надалі отримані дані використовуються для побудови мережі у власноруч написаній програмі на мові Python (Рис.2).

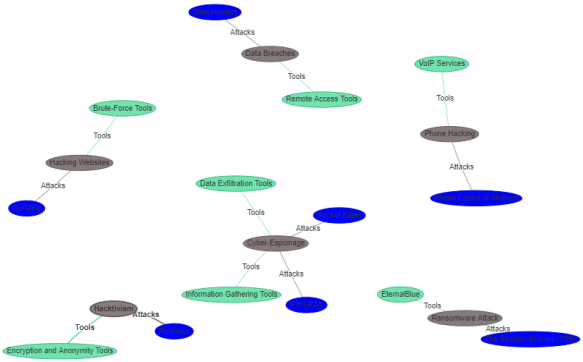

Рис. 2 - Мережа суб'єктів протистоянь у кіберпросторі

Назви угрупувань позначаються синім кольором. При натисканні будь-якого вузла відкривається Google-сторінка з відповідним запитом.

Висновки. Отримані відповіді з даного дослідження мають велике значення та важливість. Ключовими аспектами являються, зокрема, підвищення обізнаності в галузі кібербезпеки, тобто інформація, яку було отримано, стане важливим ресурсом для спеціалістів у галузі кіберзахисту, допомагаючи їм краще розуміти сучасні загрози та захищати інформаційні системи. Також описана методологія відкриває шлях для подальших наукових досліджень в галузі кібербезпеки. Ця робота служить фундаментом для розвитку більш ефективних інструментів та методів відстеження та аналізу кіберзагроз.