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).

© ІСЗЗІ КПІ ім. Ігоря Сікорського

Михайло ШЕЛЕЛЬО;
Вікторія ПОЛІЩУК;
Дмитро ЛАНДЕ, д.т.н., професор

ІНТЕЛЕКТУАЛЬНА ТЕХНОЛОГІЯ ВИЯВЛЕННЯ І ВІЗУАЛІЗАЦІЇ МЕРЕЖІ ХАКЕРСЬКИХ УГРУПУВАНЬ

Анотація. Розглянуто інтелектуальну технологію виявлення і візуалізації мережі злочинних хакерських угрупувань на основі документів, зібраних з мережевих джерел, за допомогою сервісу генеративного штучного інтелекту. Основний акцент роботи став на визначенні ключових етапів побудови мережі та аналізі зв'язків в ній.

Summary. The article considers an intelligent technology for detecting and visualising a network of criminal hacker groups based on documents collected from network sources using a generative artificial intelligence service. The main focus of the work was on identifying the key stages of network construction and analysing the links in it.

Ключові слова: хакерські угрупування, мережа, генеративний штучний інтелект, аналіз, кібербезпека.

У сучасному світі, де кібербезпека стає надзвичайно важливою складовою національної безпеки, виявлення та моніторинг діяльності хакерських угрупувань має вирішальне значення. Інтелектуальна технологія виявлення і візуалізації мережі буде розглядатися на прикладі хакерських атак на Ізраїль, що розпочалися з жовтня 2023 року і тривають досі.

На першому етапі технології здійснюється добування інформації. Для цього за допомогою системи контент-моніторингу infostream, що забезпечує одержання й обробку вхідного потоку інформації з вебсайтів Інтернету, отримаємо тематичний інформаційний масив за тематичним запитом до пошукової системи:

(*хакер* | *кібер* | *груп*) & *ізраїль*

Наступним етапом є виділення із сформованого масиву інформації назв хакерських угрупувань та кількість їх згадок. Головний принцип розпізнавання іменних сутностей базується на використанні англійських слів і словосполучень, які розпочинаються з великої літери. У результаті пошуку вдалося знайти 29 назв хакерських угрупувань та кількість згадок кожного з них.

На 3-му етапі, за допомогою генеративного штучного інтелекту (ГШІ) Microsoft Bing було здійснене сортування та фільтрація зібраної інформації. В результаті цього було сформовано масив, який включав 8

злочинних хакерських угрупувань, відповідальних за кібератаки на Ізраїль.

Після цього, на 4-му етапі, здійснюється формування мережі відібраних злочинних хакерських угрупувань. Для досягнення цього завдання було використано запит (промпт) для встановлення зв'язків між виділеними поняттями:

Створи зв'язки між злочинними хакерськими угрупуваннями для побудови мережі у форматі csv: "Name_1;Name_2".

На останньому етапі інтелектуальної технології здійснюється візуалізація оброблених даних за допомогою власної програми на Python:

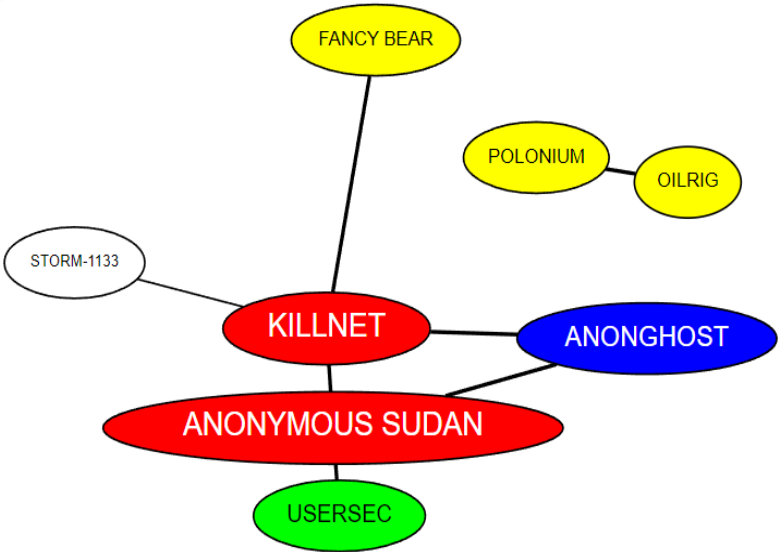

Рисунок 1 – Мережа хакерських угрупувань.

Результати використання інтелектуальної технології для виявлення та візуалізації мережі показують, що серед основних хакерських угрупувань, які здійснювали атак на Ізраїль, виділяються Killnet та Anonymous Sudan, більшість з яких мають російський слід.

Висновки. Робота розкриває інтелектуальну технологію виявлення і візуалізації мережі хакерських угрупувань, що може бути використана для аналізу активності цих груп у контексті кібербезпеки. Дослідження хакерських атак на Ізраїль можна розглядати прикладом застосування технології ГШІ, а також допомагає розкрити зв'язки злочинних кібернетичних угрупувань.