

*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

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 Об'єднання близьких за змістом вузлів при формуванні мережі кібернетичних вразливостей.....	373
Артем ПЕДУНОВ; Олександр ШАПОВАЛ Перспективи використання штучного інтелекту у системах міжмережєвих екранів.....	375
Костянтин ПЕЛЮХОВСЬКИЙ; Василь ЦУРКАН Ознаки підроблення url-адрес вебзастосунків	376
Вікторія ПОЛІЩУК; Артем МИКИТЮК Аналіз бази даних кіберінцидентів	377
Ihor PROTSYSHYN; Ihor YAKOVIV Hierarchical model of cyber threat intelligence objects	379
Дарина САВЧУК; Вячеслав РЯБЦЕВ Функціонал та режими застосування модулю “інфотека” інформаційної системи підтримки професійного навчання.....	380
Віктор САСЬКО; Дмитро ЛАНДЕ Побудова причино-наслідкової мережі для виявлення і ранжування сценаріїв діяльності.....	382
Дмитро СВЕШНІКОВ; Віктор СВЕЦЬКИЙ Автоматизована оцінка якості псевдовипадкових послідовностей на основі графічних тестів	384
Ярослав СЛОБОДЯНЮК; Артем МИКИТЮК Характеристики системи моніторингу та реагування на ddos-атаки	385
Дмитро УЛОЖЕНКО; Дмитро ШАРАДКІН Використання нейронних мереж для виявлення кібератак.....	387
Ivan FESENKO; VasyI TSURKAN Detection of photo fake authenticity based on their metadata.....	388
Марія ХАЛІМОНЕНКО; Олександр УСПЕНСЬКИЙ Багаторівнева система автентифікації користувачів вебсервера	389
Богдан ЧАЛЕНКО; Вячеслав РЯБЦЕВ Автоматизація індивідуального планування навантаження викладачів у інформаційній системі модульної архітектури.....	390
Михайло ШЕЛЕЛЬО; Вікторія ПОЛІЩУК; Дмитро ЛАНДЕ Інтелектуальна технологія виявлення і візуалізації мережі хакерських угруповань.....	392

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 угруповань на основі документів, зібраних з мережових 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 угруповання, мережа, генеративний штучний інтелект, аналіз, кібербезпека.

У сучасному світі, де кібербезпека стає надзвичайно важливою складовою національної безпеки, виявлення та моніторинг діяльності хакерських угруповань 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, отримуємо тематичний інформаційний масив за тематичним запитом до пошукової системи:

(хакер | кібер | груп) & ізраїль

Наступним етапом є виділення із сформованого масиву інформації назв хакерських угруповань 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 угруповань 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 угруповань, відповідальних за кібератаки на Ізраїль.

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

Створи зв'язки між злочинними хакерськими угрупованнями 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:

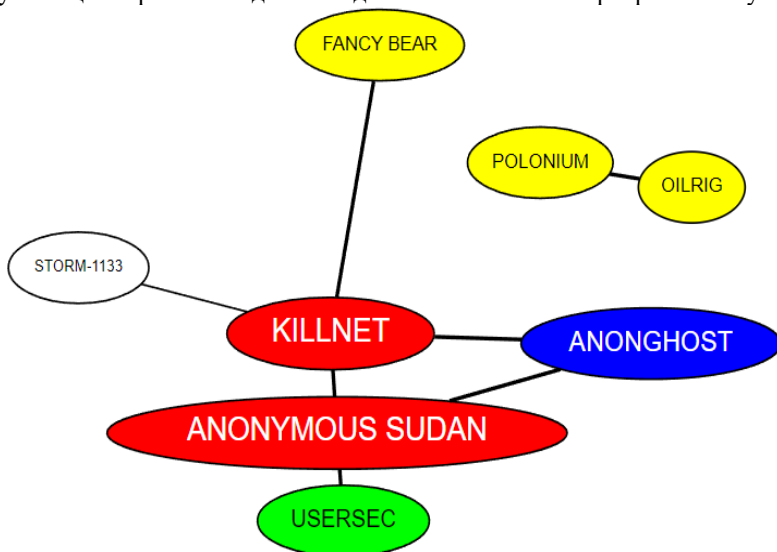


Рисунок 1 – Мережа хакерських угруповань.

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

Висновки. Робота розкриває інтелектуальну технологію виявлення і візуалізації мережі хакерських угруповань, 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 угруповань.