НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ ПРОБЛЕМ РЕЄСТРАЦІЇ ІНФОРМАЦІЇ НАН УКРАЇНИ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА БЕЗПЕКА

МАТЕРІАЛИ XXIII МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

ВИПУСК 23

Київ – 2023

Рекомендовано до друку Вченою радою
Інституту проблем реєстрації інформації НАН України
(протокол № 11 від 26 грудня 2023 р.)

Інформаційні технології та безпека. Матеріали XXIII Міжнародної науково-практичної конференції ІТБ-2023. – Київ: Інжиніринг. – 202 с. ISBN: 978-966-2344-96-7

До збірника увійшли матеріали доповідей, представлених на XXIII Міжнародній науково-практичній конференції «Інформаційні технології та безпека» (ІТБ-2023, 30 листопада 2023 року, м. Київ, Україна).

У збірнику представлені матеріали, присвячені питанням створення і впровадження інформаційних технологій, актуальним проблемам забезпечення інформаційної та кібербезпеки, протидії інформаційним операціям і кібертероризму, інтелектуальним технологіям підтримки прийняття рішень, проведенню аналітичних досліджень на основі сучасних методів інтелектуального аналізу даних.

Для фахівців в області інформаційних технологій, інформаційної і кібернетичної безпеки, а також для аспірантів і студентів старших курсів вищої школи відповідних спеціальностей.

ISBN 978-966-2344-96-7

ЗМІСТ

ДОСЛІДЖЕННЯ МЕРЕЖ СУБ'ЄКТІВ КІБЕРБЕЗПЕКИ ЗАСОБАМИ ГЕНЕРАТИВНОГО ШТУЧНОГО ІНТЕЛЕКТУ

Дмитро Ланде[1,2], Анатолій Фегер[1], Леонард Страшной[3]
[1] Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна
[2] Інститут проблем реєстрації інформації НАН України, Київ, Україна
[3] University of California, Los Angeles, USA
dwlande@gmail.com, feher.anatolii@gmail.com, lstrashnoy@gmail.com

В роботі запропонована методика екстрагування понять – назв хакерських угрупувань і їх контекстуальних зв'язківіз текстів повідомлень мережевих джерел, що стосуються предметної області кібербезпеки, засобами генеративного штучного інтелекту, формування мереж їх взаємозв'язків і змістовного аналізу цих мереж. Досліджуються мережі хакерських угрупувань, що активізувались напередодні і спочатку повномасштабних воєнних дій в Україні і в Ізраїлі. Підкреслюється наявність спільних хакерських угрупувань. Для створення реалізації запропонованих підходів використовуються засоби OSINTі системи генеративного штучного інтелекту ChatGPT, а також засоби програмного забезпечення для моделювання, аналізу та візуалізації графів – Gephi.

Ключові слова:OSINT, система генеративного штучного інтелекту,ChatGPT,екстрагування понять, мережа понять, кібербезпека.

Постановка проблеми

У сфері кібербезпеки важливими об'єктами дослідження є хакерські угрупування, деструктивне програмне забезпечення, аналітичні групитощо. Утаких групах об'єктів, як злочинні хакерські угрупування, можуть активізуватись відомі або виникати нові центри та об'єкти, що потребують особливої уваги фахівців із кібербезпеки. Таким чином,актуальним є завдання постійного моніторингу інформації у межах визначеної предметної області.

Необхідна для цього завдання інформація широко представлена у соціальних мережах, форумах, в мережі Інтернет, до контенту якої, зокрема, документів, розміщених на веб-сайтах, може бути застосована технологія розвідки у відкритих джерелах (Open Source INTelligence, OSINT) [1]. Можливість масового моніторингу відкритих джерел інформації з метою пошуку цільового контенту, людей і подій приводить до необхідності застосування технологій Big Data, які успішно розвиваються на цей час [2]. Крім того, досягається різке скорочення часу доступу. Для здійснення дієвої аналітики результатів добування інформації пропонується застосування засобів генеративного штучного інтелекту (ГШІ) [3], зокрема, системи ChatGPT, яка дозволяє отримувати результати змістовних запитів (промптів) через API.

Метацієї роботи – створення і апробування методики визначення злочинних хакерських угрупувань, що діють напередодніі спочатку широкомасштабних широких воєнних дій, та зв‘язків між ними на базі аналізу ресурсів веб-простору, а також формування на основі системи ГШІта аналітична обробка мереж виявлених об’єктів кібербезпеки. Для досягнення цієї мети вирішується низка завдань, зокрема, добування і первинної обробки інформації, витягу із неї необхідних сутностей шляхом застосування ГШІ, встановлення зв’язків між ними, формування і аналіз мереж.

Опис методики

Особливістю наведеної методики є поєднання OSINTі систем ГШІ. Основні етапи (ланцюжки) методики включають:

1) добування інформації шляхом звернення до системи контент-моніторингу (складової OSINT)із експертними запитами;

2) екстрагування понять і зв’язків між нимишляхом звернення до системи ГШІ із змістовними промптами;

3) фільтрація отриманих понять із залученням експертів;

4) формування мережі хакерських угрупувань;

5) аналіз і візуалізація цієї мережі.

Приклад

Для отримання інформаційного масиву публікацій щодо кібербезпеки було визначено необхідний період(місяць до і місяць після початку широкомасштабних воєннихдій) та опрацьовано тематичні запити до системиOSINT:

1. Війна в Україні

1.1. (кібератак~/3/украї) | (хакер~/3/атак~/2/украї) | (кибератак~/3/украин) | (хакер~/3/атак~/2/украин)

1.2. (hack~/3/ukrain) | (cyber~attack~/3/ukrain) | (cyberattack~/3/ukrain)

2. Війна в Ізраїлі

2.1. (кібератак~/3/ізра) | (хакер~/3/атак~/2/ізра) | (кибератак~/3/израил) | (хакер~/3/атак~/2/израил)

2.2. (hack~/3/israel) | (cyber~attack~/3/israel) | (cyberattack~/3/israel)

Для кожного з отриманих документів було застосовано такий промпт до системи ChatGPT, результати якого надходять до програм через API та агрегуються для подальшого формування мереж:

Промпт: Приведи список назв хакерських груп з тексту без пояснень у вигляді переліку. Текст: …

На останньому етапі здійснюєтьсяаналізвідібраної мережі тавізуалізація сформованих мереж із застосуванням системи Gephi [4] (Рис. 1, 2).

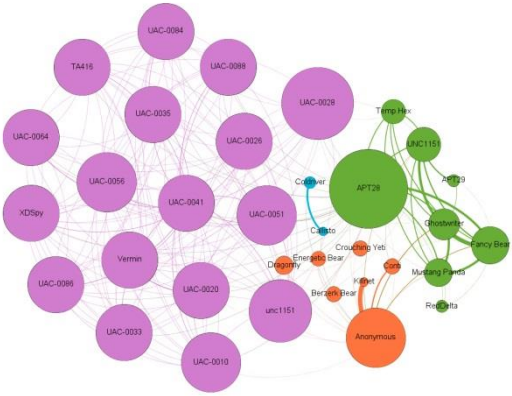

Рисунок1 – Фрагмент мережі злочинних хакерських угрупувань, пов’язаних із російсько-українською війною

Для подальшої кластеризації і візуалізації в рамках системи Gephi обчислюється модульність окремих вузлів – іменних сутностей, на основі якої здійснюється виявлення груп в мережах (кластерів).

Висновки

Запропоновано методику виявлення злочинних хакерських угрупуваньіз документів системи OSINT із застосування системи генеративного штучного інтелекту, яка враховує приховані знання, внесені експертним мережевим середовищем.Результати контент-моніторингу інтернет-ресурсів та проведеного кластерного аналізу вказують наодночаснуактивність у двох війнах хакерських угрупувань, що відносяться до спецслужб рф, а саме: Killneti APT29 (CozyBear).

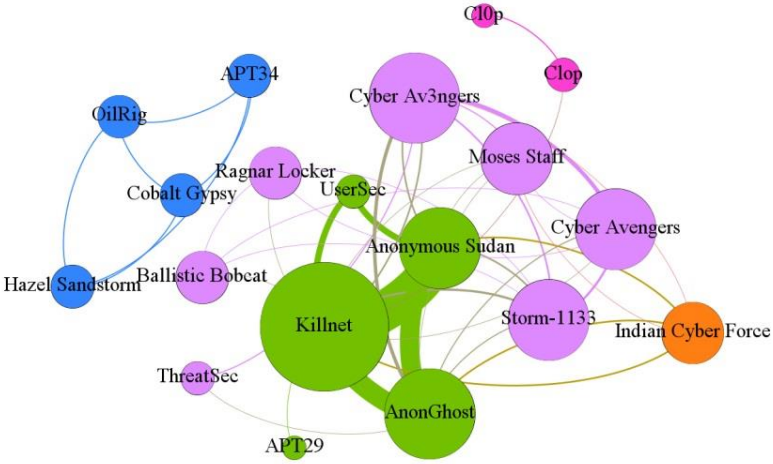

Рисунок 2 – Фрагмент мережі злочинних хакерських угрупувань, пов’язаних із війною в Ізраїлі

Перелік посилань

1. D. Lande, O. Puchkov, I. Subach, M. Boliukh, D. NahornyiOSINT

investigationtodetectandpreventcyberattacksandcybersecurityincidents // InformationTechnologyandSecurity, 2021. Vol 9 (2). –pp. 209-218.DOI: doi.org/10.20535/2411-1031.2021.9.2.249921.

2. Dmytro Lande,Ellina Shnurko-Tabakova. OSINT as a part of cyber defense system. Theoretical and Applied Cybersecurity, 2019. – Iss. 1. –pp. 103-108.

3. Dmytro Lande, Leonard Strashnoy.GPT Semantic Networking: A Dream of the Semantic Web - The Time is Now. - Kyiv: Engineering, 2023. - 168 p. ISBN 978-966-2344-94-3

4. Cherven K. Mastering Gephi Network Visualization. – PacktPublishing, 2015. – 378 p. ISBN 78-1-78398-734-4.

МЕТОДИ ТА МОДЕЛІ ПОБУДОВИ АДАПТИВНИХ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ

Додонов О.Г., Никифоров О.В., Путятін В.Г.
Інститут проблем реєстрації інформації НАН України, Київ, Україна

Предметна область досліджень щодо створення адаптивних автоматизованих систем управління (АСУ), територіально розподілених інформаційних комп'ютерних систем полягає у розробці адаптивних моделей та методів з:

- програмування функціонування: опис структури та поведінки системи, прогнозування значень її параметрів;
- цільового управління: формування підмножини контрольованих параметрів, зон їх контролю залежно від вимог до стійкості функціонування системи;
- поточного управління: контроль поточного стану та діагностування порушень працездатності.

В основному, для вирішення наукових задач в цієї галузі, використовується онтологічний підхід при застосуванні науково-методичного апарату алгебри систем [1], концептуального або конструктивного проєктування [2] та ступенів множин [3].

Відомо кілька прикладів успішного розв'язання задач побудови адаптаційних механізмів систем.

Так в [4] створено автоматичну адаптацію алгоритмів обробки інформації до змін умов, задач і цілей системи шляхом трансформації зв'язаних онтологій (онтології алгоритмів залежно від онтології предметної області). Створення практичних