Міністерство освіти і науки України
Хмельницький національний університет

ЗБІРНИК НАУКОВИХ ПРАЦЬ

за матеріалами XIV Всеукраїнської науково-практичної конференції
«Актуальні проблеми комп'ютерних наук АПКН-2022»

18-19 листопада 2022

Хмельницький 2022

УДК 004:37:001:62

Збірник наукових праць за матеріалами XIV Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2022». Хмельницький – 2022. – 331с.

У збірнику наукових праць подані перспективні практичні розробки аспірантів, студентів та здобувачів в області сучасних інформаційних технологій. Розглянуто актуальні проблеми комп'ютерних наук, комп'ютерної інженерії, прикладної математики й інженерії програмного забезпечення, приведено ряд робіт по впровадженню інформаційних технологій у виробництво та управління. Висвітлено перспективні розробки сучасних систем пошуку, обробки й захисту інформації, медійних та комунікаційних системи.

УДК 004:37:001:62

Матеріали конференції відтворені з авторських оригіналів. При макетуванні можливі незначні зміни компоновки контенту авторських оригіналів.

Участь у конференції та складові всіх її етапів (розгляд праць, макетування, публікація збірника наукових праць та видача сертифікатів) є безкоштовними для всіх учасників. Оргкомітет конференції висловлює подяку учасникам конференції та сподівається на подальшу співпрацю.

З питань проведення конференції та подальшого обміну інформацією звертатись на e-mail конференції: *apkt.khnu@gmail.com*

АКТУАЛЬНІ ПРОБЛЕМИ КОМП'ЮТЕРНИХ НАУК - 2022

XIV Всеукраїнська науково-практична конференція

Метою конференції є висвітлення актуальних проблем комп'ютерних наук, інформатики та інформаційних технологій.

СЕКЦІЇ КОНФЕРЕНЦІЇ:

1. Комп'ютерні науки та прикладні інформаційні технології.
2. Комп'ютерна інженерія та системи захисту інформації.
3. Математичне моделювання та інженерія програмного забезпечення
4. Телерадіокомунікації, медійні та комунікаційні системи.
5. Проблеми впровадження інформаційних технологій у виробництво та управління.

Робочі мови конференції: українська, англійська

ОРГКОМІТЕТ:

СИНЮК О. М. голова оргкомітету, проректор Хмельницького національного університету з наукової роботи, доктор технічних наук, професор

САВЕНКО О. С. заступник голови оргкомітету, декан факультету Інформаційних технологій ХНУ, доктор технічних наук, професор

БАРМАК О. В. заступник голови оргкомітету, завідувач кафедри Комп'ютерних наук ХНУ, доктор технічних наук, професор

ГОВОРУЩЕНКО Т. О. завідувач кафедри Комп'ютерної інженерії та інформаційних систем ХНУ, доктор технічних наук, професор

ВИСОЦЬКА О. В. доктор технічних наук, завідувач кафедри Радіоелектронних та біомедичних комп'ютеризованих засобів і технологій Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут», професор

ЛАВРОВ Є. А. доктор технічних наук, професор (Сумський державний університет)

ТІМОФЄЄВА Л. В. відповідальна за студентську науково-дослідну роботу ХНУ

МАЗУРЕЦЬ О. В. секретар конференції, к.т.н., доцент кафедри Комп'ютерних наук ХНУ

МОЛЧАНОВА М. О. секретар конференції, викладач кафедри Комп'ютерних наук ХНУ

КОНТАКТНА ІНФОРМАЦІЯ:

e-mail для листування: *apkt.khnu@gmail.com*

УДК 004.4

Ланде Д.В., Болюх М.О., Нагорний Д.О.

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

OSINT ДЛЯ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ІНЦИДЕНТІВ КІБЕРБЕЗПЕКИ ТА КІБЕРАТАК

Розглянуто рішення для автоматизації OSINT, яке б включало збір, обробку та аналіз інформації, витяг концептів (понять) визначення взаємозв'язку цих концептів, відображення подій на географічній карті, аналіз та прогнозування майбутніх кіберінцидентів, формування звітів на основі цієї інформації. Цей напрям є актуальним, враховуючи практичну відсутність автоматизованих засобів OSINT на оперативно-технічному рівні забезпечення кібербезпеки у сукупності з відсутністю єдиних підходів до проведення розвідки з відкритих джерел.

Solutions for automating OSINT are considered, which would include the collection, processing and analysis of information, the extraction of concepts (concepts) of determining the relationship of these concepts, displaying events on a geographical map, analyzing and predicting future cyber incidents, and generating reports based on this information. This direction is relevant, given the practical absence of automated OSINT tools at the operational and technical level of cybersecurity, combined with the lack of unified approaches to conducting intelligence from open sources.

У теперішній час у світі існує багато технологій OSINT [1-4], але більшість з них потребує залучення великих обчислювальних і людських ресурсів, закупівлі коштовного програмного забезпечення, що приводить до великих часових і фінансових витрат.

Практична відсутність автоматизованих засобів OSINT на оперативно-технічному рівні забезпечення кібербезпеки у сукупності з відсутністю єдиних підходів до проведення розвідки з відкритих джерел призводить до збільшення часу реагування на кіберінциденти та зниження ефективності роботи відповідних аналітичних підрозділів.

Виходячи з цих обставин, методика розслідування і прогнозування кіберінцидентів на базі застосування відкритих джерел інформації і вільно доступного програмного забезпечення з відкритим кодом, що забезпечує розслідування кіберінцидентів, які вже відбулися, збір аналітичних даних щодо них, накопичення відповідної аналітичної інформації для майбутнього застосування методів та технологій машинного навчання, своєчасне детектування кібератак, що здійснюються на цей час, дослідження та прогнозування майбутніх кібератак, є актуальною науковою задачею.

Метою роботи є опис теоретичних засад і методології проведення OSINT для виявлення та запобігання інцидентів кіберзбезпеки та кібератак.

Розвідка за відкритими джерелами (англ. OSINT - Open source intelligence) - один з напрямів розвідки, який включає пошук, вибір та добування розвідува-льної інформації, отриманої з загальнодоступних джерел (не обов'язково комп'ютерних або мережевих), а також аналіз цієї інформації. Роль OSINT визначається низкою аспектів, серед яких оперативність надходження, обсяг, якість, ясність, легкість подальшого використання, вартість отримання та ін.

Для вирішення сформульованого наукового завдання, запропоновано нову методику, яка передбачає виконання наступних дій:

1) Визначення проміжку часу [T1, T2], коли було здійснено кіберінцидент. Цю інформацію можна отримати в офіційних джерелах, звітах щодо кібератак, повідомленнях мережевих ЗМІ та ін.

2) Отримання, на скільки це можливо, найбільшого за кількістю масиву посилань на повідомлення з веб-ресурсів мережі Інтернет, що відноситься до вказаного кіберінциденту у часовому інтервалі [T1–C, T2+C], де C – константа, наприклад, яка відповідає 30 добам. Для цього можна використовувати глобальні мережеві пошукові системи, такі як Google, Google News, Bing та ін.

3) Отримання повних текстів всіх повідомлень, що відповідають посиланням та проведення їх попередньої обробки та нормалізації.

4) Агрегування отриманих повідомлень за часом їхньої появи в мережі Інтернет, побудова часового ряду динаміки публікацій за тематикою визначеного кіберінциденту.

5) Дослідження отриманого часового ряду, згладжування його, проведення вейвлет-аналізу, отримання скейлограми, виявлення аномалій, періодичності і т.і., порівняння з відомими шаблонами інформаційних операцій та кіберінцидентів.

6) Отримання з текстів концептів – поіменованих сутностей, географічних назв (топонімів), імен і прізвищ персон і назв організацій. Відображення на географічній карті топонімів, що відповідають вибраному кіберінциденту.

7) Побудова мережі цих сутностей, виявлення груп найбільш зв'язаних (кластерний аналіз).

8) Побудова дайджестів з повідомлень, що відображають найбільш важливі різні аспекти визначеного кіберінциденту.

Для дослідження кіберінцидентів, що відбуваються у цей час необхідно виконати майже всі перелічені кроки (крок 2 за умови, що T2 невідоме), після цього виконати прогнозування часового ряду, наприклад, за методом Сорнетте [5, 6], щоби передбачити майбутню поведінку кіберінциденту.

Застосування запропонованої методики продемонстровано на прикладі трьох відомих кібератак 2021 та 2022 років, а саме:

– кібератаки на Colonial Pipeline - застосування шкідливого ПЗ для виводу з ладу американської трубопровідної системи Colonial Pipeline (6-12 травня 2021 року);
– кібератаки на завод з очищення стічних вод у Флориді (5 лютого 2021 року) [7];

– кібератаки на урядові сайти України (14 січня 2022 року) [8].

Отже, практичне значення отриманих результатів полягає в наданні користувачам оперативно-тактиічного рівня дієвої інформаційної технології, яка реалізована у вигляді набору готових для використання інструментальних засобів контент-моніторингу і аналізу Інтернет-простору з питань кібербезпеки та є придатною до як автономного використання, так і застосування в якості компоненти у складі систем підтримки прийняття рішень щодо інформаційної та кібернетичної безпеки в ситуаційних центрах різного рівня.

Дані отримані в процесі обробки за допомогою наведених програмних застосунків є джерелом інформації для розслідування кібератак та їх прогнозування шляхом виділення шаблонів їхньої реалізації. Їхнє застосування на практиці дозволяє легко будувати графічні звіти, для подальшого аналізу та прийняття оперативних та обґрунтованих рішень.

Перелік посилань

1. D. Lande, and E. Shnurko-Tabakova, "OSINT as a part of cyber defense system", Theoretical and Applied Cybersecurity, no. 1, pp. 103-108, 2019, doi: 10.20535/tacs.2664-29132019.1. 169091.
2. B. Akhgar, P. S. Bayerl, and F. Sampson, Open Source Intelligence Investigation. From Strategy to Implementation: Springer International Publishing AG, 2016.
3. N. Memon, and R. Reda Alhajj, Counterterrorism and Open Source Intelligence, Wien, Austria: Springer-Verlag, 2011.
4. Lande D.; Subach I.; Puchkov A. System of Analysis of Big Data from Social Media Information & Security: An International Journal 47, no. 1 (2020): 44-61. DOI: doi.org/10.11610/isij.4703
5. Sornette, D. Why Stock Markets Crash: Critical Events in Complex Financial Systems. Princeton University Press (2004), https://doi.org/10.23943/princeton/9780691175959.001.0001.
6. D. Sornette, How to predict the collapse of financial markets. Critical events in complex financial systems, Litres, 2017.
7. Outdated computer system exploited in Florida water treatment plant hack // [Електронний ресурс]. — Режим доступу: https://abcnews.go.com/US/outdated-computer-system-exploited-florida-water-treatment-plant/story?id=75805550
8. Офіційний сайт України вночі атакували хакери // [Електронний ресурс]. — Режим доступу: https://www.epravda.com.ua/news/2022/01/26/681800/