КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.27.757
УДК 004.56

Гайдук Олег Васильович
старший викладач кафедри інженерії програмного забезпечення та кібербезпеки
Державний торговельно-економічний університет, Київ, Україна
ORCID ID: 0000-0003-4740-7759
o.hayduk@knute.edu.ua

Звєрєв Володимир Павлович
к.т.н., старший науковий співробітник
Доцент кафедри інженерії програмного забезпечення та кібербезпеки
Державний торговельно-економічний університет, Київ, Україна
ORCID ID: 0000-0002-0907-0705
zvieriev_vp@knute.edu.ua

Гулак Геннадій Миколайович
д.т.н., професор, професор кафедри інформаційної та
кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0001-9131-9233
h.hulak@kubg.edu.ua

КОРЕЛЯЦІЙНИЙ АНАЛІЗ ТИПІВ КІБЕРІНЦИДЕНТІВ В КОНТЕКСТІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ МІЖНАРОДНИХ КОМУНІКАЦІЙ

Анотація. У цій статті досліджується роль кореляційного аналізу стандартизованих типів кіберінцидентів в рамках тематики інформаційних технологій забезпечення кібербезпеки міжнародних комунікацій. У роботі застосовано кореляційний аналіз деяких типів знеособлених кіберінцидентів в Україні для визначення взаємозв'язків між ними, за усталеними категоріями і типами, з червня 2022 по лютий 2024 років. Теплова карта кореляцій використана для візуалізації отриманих результатів і подальшого аналізу закономірностей у динаміці загроз. Особлива увага приділяється можливості застосування теплових карт для візуального представлення кореляцій між різними типами кіберінцидентів. Цей підхід дозволяє ефективно аналізувати великі обсяги даних і виявляти складні взаємозв'язки, які можуть бути неочевидними при традиційному аналізі. Стаття зосереджується на методології обробки даних про інциденти з використанням статистичних методів для оцінки взаємозв'язків. Кореляційний аналіз виконується за допомогою коефіцієнта кореляції Пірсона, і результати представлені у формі теплових карт, що надають змогу визначити як сильні, так і слабкі кореляції між категоріями інцидентів. Такий підхід виявляє багатофакторні кіберзагрози і сприяє розумінню можливих механізмів їх спільного поширення та впливу. На основі отриманих даних формулюються рекомендації для покращення стратегій кібербезпеки міжнародних комунікацій та кібердипломатії, зокрема через розробку та впровадження комплексних заходів захисту, які враховують виявлені кореляції. Здійснений також аналіз перспектив подальших досліджень у цій сфері, спрямованих на оптимізацію інформаційних технологій кібербезпеки для міжнародних комунікацій.

Ключові слова: кібербезпека; кібердипломатія; міжнародні комунікації; кореляційний аналіз; теплові карти; інформаційні технології; соціальні мережі; соціальна інженерія; інформаційна безпека держави; кіберінциденти; статистичний аналіз; коефіцієнт кореляції Пірсона; аналіз кіберзагроз.

ВСТУП

Постановка проблеми. В сучасних умовах цифрової трансформації міжнародних комунікацій та зростання обсягів оброблюваної інформації питання кібербезпеки набуває критичного значення. Кіберзагрози стають все більш складними та

взаємопов'язаними, що ускладнює їх виявлення та протидію. Визначення кореляцій між різними типами кіберінцидентів є важливим кроком до розуміння закономірностей їх виникнення та розвитку складних кібератак, розробки ефективних заходів захисту [**Error! Reference source not found.**].

Кореляція — це статистичний метод, який використовується для аналізу взаємозв'язку між двома або більше змінними. Вона дозволяє визначити, наскільки зміни однієї змінної супроводжуються змінами іншої. Кореляція може бути позитивною, коли змінні змінюються в одному напрямку, негативною коли збільшення однієї змінної спричиняє зменшення іншої або відсутньою, коли взаємозв'язок між змінними не простежується [**Error! Reference source not found.**]. Найпоширенішими методами оцінки кореляції є коефіцієнт Пірсона, Спірмена та Кендалла. Кореляційний аналіз допомагає знаходити закономірності в даних, але не визначає причинно-наслідкові зв'язки [**Error! Reference source not found.**].

Одним із підходів до аналізу зв'язків між кіберінцидентами є застосування методів кореляційного аналізу та візуалізація отриманих результатів у вигляді теплових карт. Такий метод дозволяє не лише виявити найбільш тісно взаємопов'язані загрози, але й оцінити тенденції їх спільної появи [**Error! Reference source not found.**].

Аналіз останніх досліджень і публікацій. Кореляційний аналіз є одним з основних методів оцінки взаємозв'язку між змінними у кібербезпеці, особливо на міждержавному рівні і в міжнародних комунікаціях. Дослідження Фахіма Суфі (Fahim Sufi) з Університету Монаш (Monash University) в Мельбурні, Австралія [**Error! Reference source not found.**] описує багатогранний характер кібератак на об'ємі даних у 225 країнах протягом 2022–2023 років. Ця робота охопила вісім типів кіберінцидентів, зокрема спам, програми-вимагачі, локальне зараження, експлойт, фішинг, мережеві атаки, сканування на вимогу та веб-загрози. Автор наголошує, що використання кореляційного аналізу дозволило виявити неочевидні закономірності між різними типами атак що виникають одночасно або у певній послідовності. Наприклад результати виявили значні кореляції між такими типами атак, як сканування на вимогу та зараження шкідливим програмним забезпеченням з коефіцієнтом більше 0,9. Такий високий кореляційний зв'язок може свідчити, в тому числі, про спільну спрямованість цих атак на компрометацію користувачів. Інше дослідження (Ömer Sen, Dennis van der Velde та інших) [1] вказує на необхідність більш широкого розуміння кореляцій між різними типами атак для виявлення найбільш масштабних і складних кібератак, що може свідчити про використання зловмисниками багатофакторних атакуючих сценаріїв. Автори підкреслюють доцільність використання автоматизованих підходів до кореляційного аналізу даних про різні типи кіберінцидентів з багатьох джерел, оскільки це дозволить швидко виявляти такі взаємозв'язки та ефективніше завчасно прогнозувати можливі сценарії атак.

При аналізі великих обсягів даних кіберінцидентів виникає проблема значного розкиду значень, що ускладнює інтерпретацію кореляційних залежностей. Для вирішення цієї проблеми широко застосовується логарифмічне перетворення [6], яке дозволяє нормалізувати розподіл даних та зменшити вплив аномальних значень. Логарифмічне згладжування даних покращує виявлення трендів та допомагає уникнути спотворення результатів при аналізі частоти кіберінцидентів.

Методи візуалізації даних відіграють ключову роль у розумінні складних взаємозв'язків у кіберзагрозах. Одним із найбільш ефективних методів є теплові карти, що дозволяють представити рівень кореляції між змінними у графічному вигляді. Як зазначає Бібор Сабо (Bibor Szabo) [7], кореляційні теплові карти є важливим дослідницьким інструментом візуалізації та спрощення аналізу багатовимірних даних.

Кореляційні теплові карти подають інформацію у візуально привабливому вигляді та одразу показують, які змінні корелюють, до якої міри і в якому напрямку, а також попереджають дослідника про потенційні проблеми мультиколінеарності.

Огляд літератури свідчить, що використання кореляційного аналізу, логарифмічного перетворення та теплових карт є ефективними методами для вивчення закономірностей у сфері кібербезпеки. Попередні дослідження підтверджують важливість аналізу взаємозв'язків між кіберінцидентами для прогнозування загроз та розробки ефективних заходів безпеки.

Мета статті. Мета цієї статті полягає у вивченні застосування кореляційного аналізу та теплових карт у забезпеченні кібербезпеки міжнародних комунікацій. Ці інструменти можуть допомогти в ідентифікації та візуалізації складних взаємозв'язків між різними типами кіберінцидентів, забезпечуючи глибше розуміння потенційних загроз і покращення стратегій протидії. Ця робота має на меті показати, як використання передових статистичних та аналітичних методів може сприяти створенню більш ефективних і науково обґрунтованих підходів до кібербезпеки на міждержавному рівні та кібердипломатії.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Наказом № 570 Адміністрації Держспецзв'язку від 03.07.2023 р. передбачено збір, аналіз та реагування на багато типів кіберінцидентів [8]. Використання в дослідженні інцидентів з цього переліку важливо з точки зору уніфікації і стандартизації. Для аналізу кореляційних зв'язків між різними типами кіберінцидентів було використано дані, які підходять до цієї класифікації і зібрані з внутрішніх корпоративних систем моніторингу кіберзагроз у період з червня 2022 року по лютий 2024 року. Аналізовані дані містять загальну кількість 24 тисячі знеособлених подій з інформацією про частоту виникнення п'ятнадцяти основних типів кіберінцидентів, зокрема:

1. Спроби авторизації/входу в систему;
2. Розповсюдження ШПЗ;
3. Шахрайський сайт;
4. Несанкціонований доступ до інформації;
5. Шкідливе підключення;
6. Фішинг;
7. Зараження ШПЗ;
8. Сканування;
9. Саботаж/шкідливі дії;
10. Несанкціонована модифікація;
11. Сніфінг;
12. Компрометація системи;
13. Атака на відмову в обслуговуванні;
14. Компрометація облікового запису;
15. Спроба експлуатації вразливості.

Щоденні дані агреговані за місяцями, що дозволяє аналізувати динаміку змін та взаємозв'язки між інцидентами протягом зазначеного періоду. Як видно із візуалізації за деякими типами інцидентів (рис. 1), різні типи кіберінцидентів мають дуже різні кількості випадків, що утруднює їх коректне представлення на спільному графіку.

Важливо підкреслити, що наведені типи кіберінцидентів мають безпосередній зв'язок із такими факторами, як соціальні мережі, соціальна інженерія та загальна інформаційна безпека держави. Соціальні мережі й медіа-платформи сьогодні слугують одним із найпотужніших каналів поширення будь-яких інформаційних чи програмних

впливів. Зокрема, соціальна інженерія — комплекс методик, спрямованих на отримання конфіденційних відомостей або доступу до системи за допомогою маніпулювання свідомістю та емоціями користувачів, — дедалі частіше реалізується через платформи соціальних мереж. Шахрайські сайти, фішинг, компрометація облікових записів та інші типи інцидентів активно використовують вірусний характер онлайн-комунікацій для підвищення масштабів атак. Крім того, за допомогою соціальних мереж зловмисники можуть організовувати та координувати більш складні атаки, зокрема поєднуючи спроби експлуатації вразливостей, сканування і несанкціонований доступ з психологічними прийомами впливу. У контексті інформаційної безпеки держави ці загрози стають особливо небезпечними, оскільки атаки, що опираються на соціальний інжиніринг і масове поширення дезінформації або шкідливого контенту, можуть сприяти дестабілізації інформаційного простору, створенню паніки та підриву довіри громадян до державних інституцій. Можна стверджувати, що значна частина кіберінцидентів, описаних у попередньому переліку, може бути посилена саме через взаємодію з платформами соціальних мереж і відповідні техніки соціальної інженерії, що, у свою чергу, становить серйозний виклик для національної інформаційної безпеки.

Маючи на меті дослідити кореляцію основних типів кіберінцидентів, особливо важливо зрозуміти їхні часові і кількісні максимальні і мінімальні показники, вектори змін та розподіл випадків за періодами. Однак, значна варіативність кількостей подій створює складнощі для стандартного аналізу, що вимагає більш складних інструментів для обробки та інтерпретації даних. Таким чином, вступний огляд даних за допомогою простої візуалізації, як показано на рис. 1, є критично важливим для встановлення базового розуміння загальних тенденцій та відхилень у наведених типах кіберінцидентів перед проведенням більш детального кореляційного аналізу.

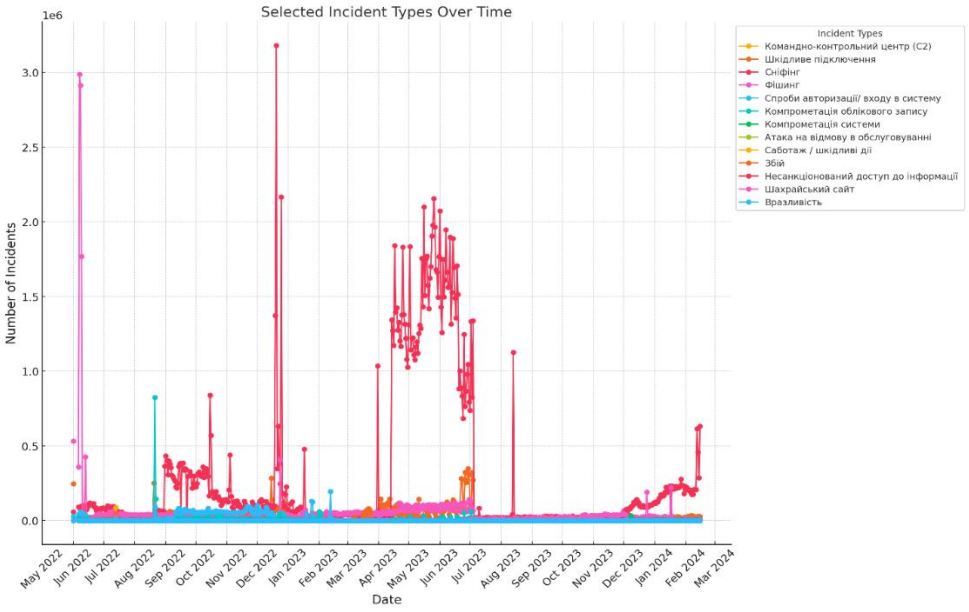


Рис. 1. Частота типів кіберінцидентів 2022–2024 рр.

Тому для коректного представлення аналізу частоти кіберінцидентів, із значною варіативністю даних, включаючи наявність аномальних пікових значень, ми застосовували логарифмічне перетворення**.** Використання логарифмічної шкали для згладжування даних, дозволило забезпечити коректніше візуальне представлення кореляцій. Перетворення виконувалося за такою формулою:

ISSN 2663 - 4023

$$X' = \log(X + 1)$$

де X — початкове значення частоти кіберінциденту, X' — перетворене значення, додавання 1 використовується для уникнення логарифмування нульових значень.

Графік, який ми створили на рис. 2, відображає кількість інцидентів за різними типами на логарифмічній шкалі протягом часу. Він покликаний ілюструвати тренди та зміни в кількості інцидентів, хоча і не встановлює статистичних взаємозв'язків або кореляцій між ними.

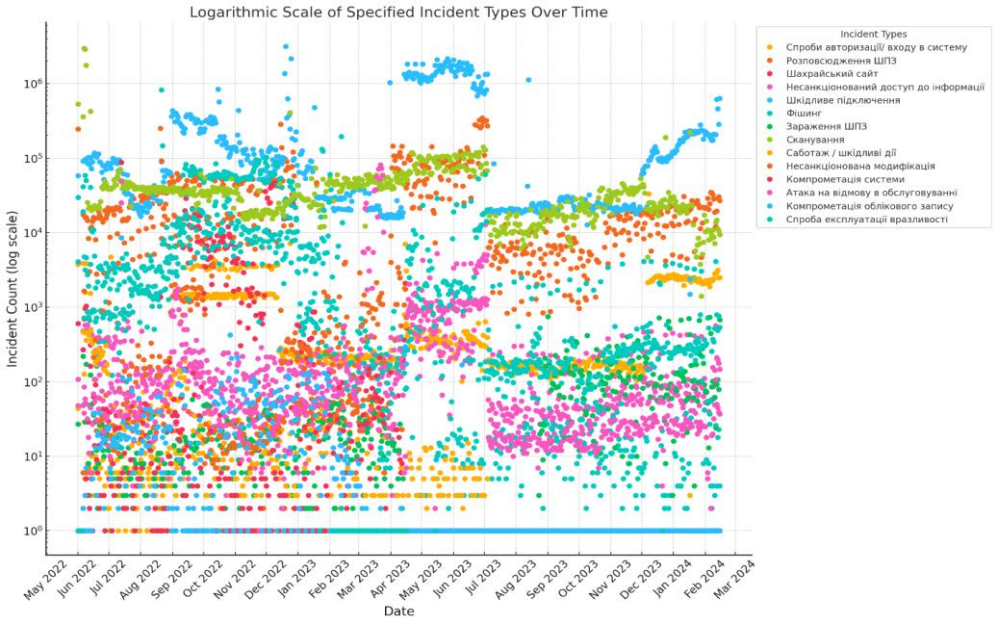
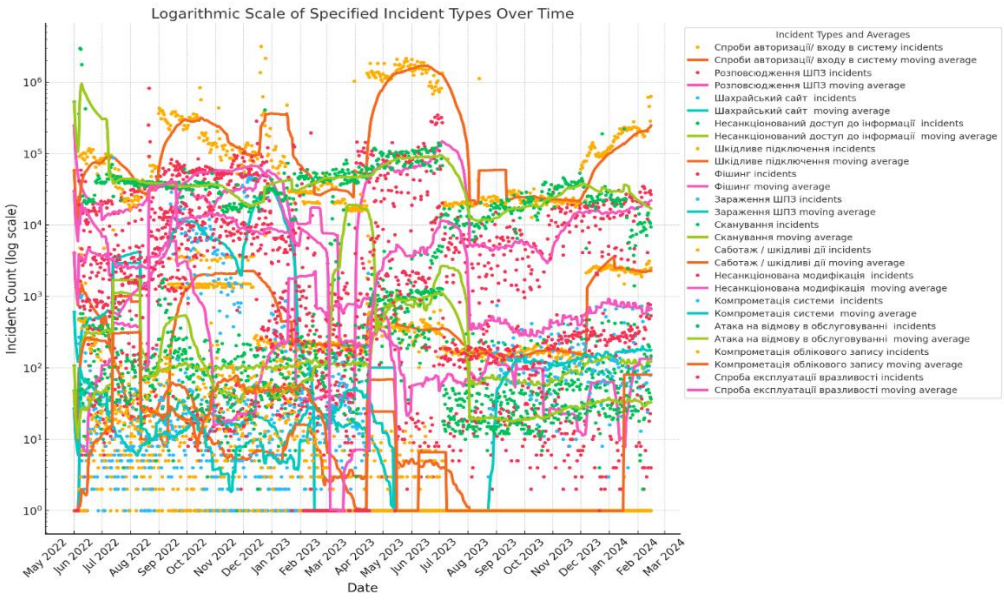


Рис. 2. Логарифмічне представлення частоти типів кіберінцидентів 2022–2024 рр.

Цей підхід дозволяє вирівняти вплив високочастотних та рідкісних інцидентів, зменшуючи спотворення в подальшому кореляційному аналізі. Разом із цим, ми маємо справу з процесами, що змінюються експоненційно і мають великий розкид даних, тому наступна візуалізація на рис. 3 відображає середнє логарифмованих значень.



№ 3 (27), 2025
ISSN 2663 - 4023

Рис. 3. Середнє логарифмованих значень

Криві середніх значень логарифму даних (moving average) на графіку дозволяють «згладити» дані, які мають великий діапазон значень або містять викиди і співставити їх з іншими даними, роблячи розподіл більш симетричним, графічно візуалізувавши певні кореляції.

Разом із цим, зазначені підходи лише частково дозволили побачити певні види кореляції між різними типами кіберінцидентів. Тому для оцінки взаємозв'язків між різними типами кіберінцидентів було обрано кореляційний коефіцієнт Пірсона, який широко використовується для оцінки лінійного зв'язку між двома змінними. Він визначається за формулою:

$$r = \frac{\sum(X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum(X_i - \bar{X})^2} \cdot \sqrt{\sum(Y_i - \bar{Y})^2}}$$

де X_i, Y_i — значення змінних (частота кіберінцидентів), $\bar{X}, \bar{Y}$ — середні значення змінних, r — коефіцієнт кореляції, який приймає значення в діапазоні [-1; 1]: $r = 1$ означає повну позитивну кореляцію, $r = -1$ означає повну негативну кореляцію, $r = 0$ означає відсутність лінійної залежності.

Розрахунок кореляційної матриці проводився у середовищі Python, використовуючи бібліотеку pandas. Для побудови кореляційної матриці спочатку було виконано очищення даних та перетворення їх до формату, придатного для аналізу. Дані включають кількість інцидентів для кожного типу, агрегованих по місяцях. Кореляційна матриця обчислена з використанням функції corr() бібліотеки Pandas, яка за замовчуванням використовує коефіцієнт Пірсона. Значення коефіцієнтів кореляції варіювалися від -1 до +1, де +1 вказує на ідеальну позитивну лінійну залежність, -1 на ідеальну негативну лінійну залежність, а 0 на відсутність лінійного зв'язку.

Для наочності результатів кореляційні коефіцієнти були візуалізовані у вигляді теплової карти (рис. 4) за допомогою бібліотеки Seaborn. На діагоналі матриці були встановлені значення NaN для візуального відокремлення ідентичних типів інцидентів, оскільки кореляція типу з самим собою не несе аналітичної цінності. Використання кольорової шкали 'plasma' допомогло виділити ступені кореляції за інтенсивністю кольору, полегшуючи інтерпретацію значень матриці. Цей методологічний підхід дозволив нам виявити ключові залежності між типами інцидентів, що сприятиме формуванню стратегії протидії комбінованим атакам.

Методологія побудови теплової карти:

1. Створення кореляційної матриці — використання pandas.corr() для обчислення коефіцієнтів Пірсона.
2. Видалення зайвих значень — усунення діагональних елементів, які мають значення 1 (самокореляція).
3. Візуалізація — використання seaborn.heatmap() для графічного представлення з кольоровою шкалою plasma.

Код на Python, який використовувався для створення теплової карти кореляцій між різними типами кіберінцидентів і кольоровою шкалою 'plasma':

```
import numpy as np
import matplotlib.pyplot as plt
import seaborn as sns
# Передбачається, що correlation_matrix_ordered - це ваша кореляційна
матриця,
```

```
# вже очищена від зайвих рядків та колонок і упорядкована за допомогою
кластеризації.
# Встановлення значень NaN на діагоналі матриці для того, щоб вони
відображались білим кольором на карті
np.fill_diagonal(correlation_matrix_ordered.values, np.nan)
# Створення теплової карти з використанням кольорової шкали 'plasma'
plt.figure(figsize=(15, 12))
heatmap = sns.heatmap(correlation_matrix_ordered, annot=True,
cmap='plasma', fmt=".2f",
                      cbar_kws={'label': 'Correlation Coefficient'})
plt.title('Heatmap of Cyber Incident Type Correlations')
plt.xlabel('Incident Type')
plt.ylabel('Incident Type')
# Показуємо графік
plt.show()
```

Цей код імпортує необхідні бібліотеки, налаштовує діагональні значення на NaN для відображення їх білим кольором на тепловій карті, застосовує кольорову шкалу ‘plasm’ для кращої візуалізації та відображає графік. Результатом роботи цієї програми є теплова карта (*heatmap*) — графічне представлення отриманих коефіцієнтів кореляції, що дозволяє наочно ідентифікувати найбільш тісно взаємопов’язані кіберзагрози рис. 4.

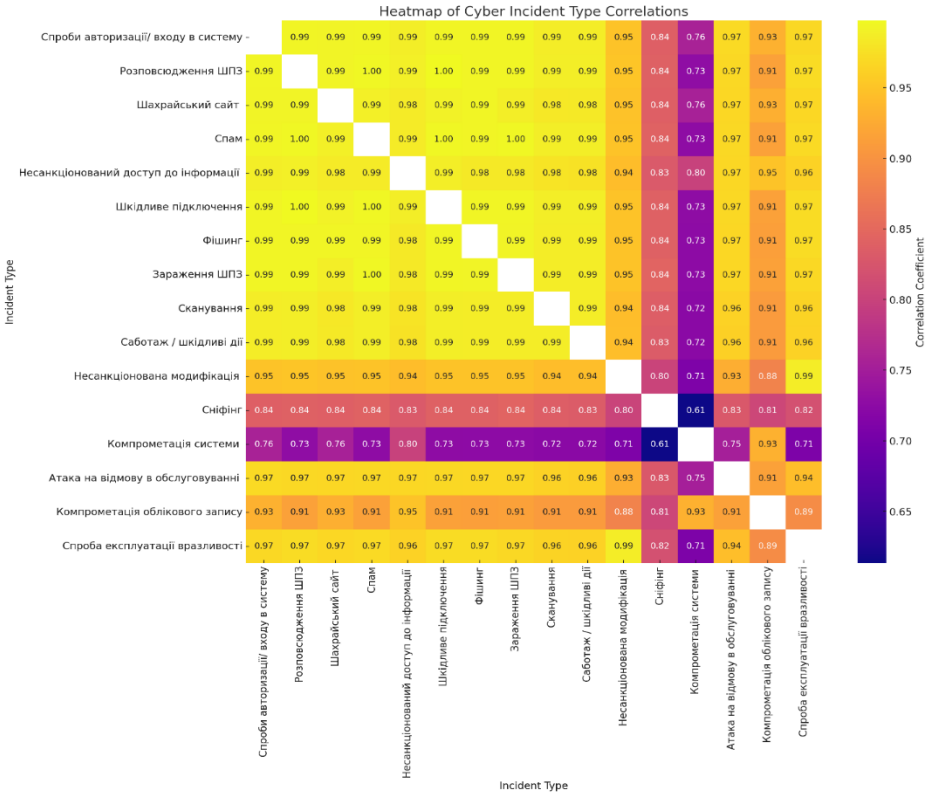


Рис. 4. Теплова карта

Аналізуючи теплову карту кореляцій між різними типами кіберінцидентів, ми можемо виявити декілька ключових взаємозв’язків, які можуть бути особливо цікавими для подальших досліджень та вжиття превентивних заходів у сфері кібербезпеки на національному та міжнародному рівнях. Розглянемо п’ять основних висновків, які прямо випливають із аналізу побудованої теплової карти.

1. Високі кореляції між подібними інцидентами: Такі як «Фішинг» та «Шахрайський сайт», «Розповсюдження ШПЗ» та «Зараження ШПЗ», які мають високі кореляційні коефіцієнти. Це вказує на те, що коли відбувається один тип інциденту, імовірно з’являться інші схожі або пов'язані інциденти.
2. Співвідношення технічних та соціальних інцидентів: Висока кореляція між такими типами інцидентів, як «Спам» та «Фішинг», може вказувати на використання комбінованих атак, де зловмисники використовують як технічні, так і соціальні методики.
3. Загальні вразливості та атаки: Тісний зв’язок між «Атаками на відмову в обслуговуванні» (DoS) і «Компрометацією системи» може свідчити про спільні вразливості у системах, що дозволяють зловмисникам виконувати обидва типи атак.
4. Широка кореляція «Командно-контрольних центрів (C2)»: Цей тип інциденту має високу кореляцію з багатьма іншими інцидентами, що може вказувати на їхнє використання як ключових компонентів у багатьох кібератаках.
5. Низькі кореляції унікальних або рідкісних інцидентів: Такі інциденти, як «Некоректна конфігурація», можуть мати низькі кореляційні значення з іншими інцидентами, що вказує на їх унікальний або незалежний характер.

Низька кореляція в компрометації системи з іншими типами кіберінцидентів може мати кілька пояснень, що відображають особливості цього типу інциденту та його взаємодії з іншими видами загроз. Розглянемо чотири основні потенційні причини такої низької кореляції:

1. Унікальні вектори атаки: Компрометація системи часто залежить від специфічних вразливостей або унікальних конфігурацій систем, які можуть не бути загальнопоширеними або легко повторюваними. Таким чином, інші типи інцидентів, які базуються на різних методах атаки, можуть не мати тісного зв’язку з компрометацією системи.
2. Індивідуальні цілі атак: Інциденти, що ведуть до компрометації системи, можуть бути цілеспрямованими або спрямованими на конкретні організації або індустрії. Це може обмежити кількість спостережуваних подій, а також їхню кореляцію з іншими типами інцидентів, які можуть бути більш загальними або випадковими.
3. Різноманітність методів виявлення: Компрометація системи може бути виявлена через різні засоби, включаючи аналіз поведінки, моніторинг мережевого трафіку або аудит системних журналів. Ця різноманітність може призводити до розбіжностей у виявленні та звітуванні, що впливає на кореляцію з іншими інцидентами, які можуть виявлятися стандартними методами.
4. Затримки у виявленні: Компрометація системи часто виявляється зі значною затримкою після самого інциденту, особливо якщо зловмисники вдаються до приховування своєї присутності. Це може знижувати кореляцію в часі з іншими інцидентами, які виявляються та реєструються негайно.

Для зменшення ризику компрометації системи та підвищення кореляції з можливими попереджувальними сигналами можна розглянути заходи з покращення засобів моніторингу та виявлення, а також розробку відповідних стратегій для більш ефективного реагування на попередні інциденти, які можуть передувати компрометації.

Проведений аналіз теплової карти кореляцій між різними типами кіберінцидентів дозволив виявити ключові закономірності у взаємодії атакуючих векторів та оцінити можливі ризики їхнього поширення. Високі кореляційні значення між окремими видами інцидентів, такими як «Фішинг» і «Шахрайський сайт» або «Розповсюдження ШПЗ» і «Зараження ШПЗ», свідчать про їхню часту спільну появу, що може бути результатом комбінованих атак або використання схожих механізмів компрометації систем.

Аналіз низьких кореляцій між деякими інцидентами, наприклад, «Компрометація системи» та іншими загрозами, свідчить про їхній унікальний характер або наявність окремих векторів атак, які не залежать від масових кібератак. Це вказує на необхідність вдосконалення засобів моніторингу та покращення міжсистемного обміну інформацією для виявлення прихованих взаємозв’язків.

Застосування логарифмічного перетворення дозволило усунути вплив викидів і забезпечити більш точну інтерпретацію змін у динаміці інцидентів. Запропонований підхід до аналізу кореляцій у поєднанні з методами статистичної оцінки дозволяє краще зрозуміти структуру загроз та їхній взаємний вплив, що є важливим для формування ефективних стратегій кібербезпеки.

Отримані результати можуть бути використані для прогнозування можливих сценаріїв атак та розробки превентивних заходів із мінімізації ризиків, а також для покращення координації між суб’єктами кіберзахисту. Подальші дослідження можуть бути спрямовані на використання методів машинного навчання та мережевого аналізу для автоматизації виявлення закономірностей у великих масивах даних про кіберінциденти.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Отримані результати можуть бути використані для вдосконалення методів кіберзахисту, оскільки виявлення висококорельованих кіберзагроз є базою у створенні комплексних стратегій реагування. Наприклад, висока кореляція між фішингом і шахрайськими сайтами дозволяє прогнозувати ланцюгові атаки та впроваджувати захист від фішингу як один із ключових елементів безпеки.

В роботі підкреслюється значення кореляційного аналізу та візуалізації через теплові карти в аналізі кіберінцидентів, особливо у контексті забезпечення безпеки міжнародних комунікацій та кібердипломатії. Виявлені взаємозв'язки між різними типами кіберінцидентів можуть вказувати на спільні причини чи послідовності подій, що має важливе значення для розробки міжнародних стратегій кібербезпеки. Результати дослідження відкривають можливості для кібердипломатії, дозволяючи краще розуміти, як кіберзагрози можуть впливати на міждержавні відносини та міжнародну стабільність. Отримані результати можуть бути корисними для розробки автоматизованих систем кібермоніторингу, що враховують взаємозв’язки між загрозами та допомагають прогнозувати майбутні атаки.

Аналіз також виявив деякі обмеження, включаючи кількість даних і відсутність аналізу нелінійних зв’язків, що може обмежити загальну універсальність висновків. Це підкреслює необхідність подальших досліджень, зокрема використання розширених методів машинного навчання для глибшого розуміння динаміки кіберзагроз. Розширення бази даних та включення більш комплексних аналітичних інструментів можуть в майбутньому допомогти в розробці більш ефективних міжнародних стратегій протидії кіберзагрозам, зміцнюючи глобальну кіберстійкість та сприяючи міжнародній безпеці.

За результатами даного дослідження, що вивчало взаємозв'язки між різними кіберінцидентами через кореляційний аналіз, наступним етапом у наукової роботи може стати застосування теорії ігор та теорії графів для моделювання міжнародних кібервзаємодій. Цей підхід може виявити стратегічні можливості для формування більш ефективних відповідей на кіберзагрози, оскільки теорія ігор дозволяє аналізувати рішення, що приймаються раціональними учасниками в умовах конфлікту та співпраці, а теорія графів може структурувати та візуалізувати складні мережі кібервзаємодій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Sen, Ö., van der Velde, D., Wehrmeister, K. A., Hacker, I., Henze, M., & Andres, M. (2022). On using contextual correlation to detect multi-stage cyber attacks in smart grids. *Sustainable Energy, Grids and Networks, 32,* 100821. https://doi.org/10.1016/j.segan.2022.100821
2. Cohen, J., Cohen, P., West, S. G., & Aiken, L. S. (2013). *Applied Multiple Regression/Correlation Analysis for the Behavioral Sciences.* https://doi.org/10.4324/9780203774441.
3. Janse, R. J., Hoekstra, T., Jager, K. J., Zoccali, C., Tripepi, G., Dekker, F. W., & van Diepen, M. (2021). Conducting correlation analysis: important limitations and pitfalls. *Clin Kidney J. 14(11),* 2332–2337. https://doi.org/10.1093/ckj/sfab085
4. Gnatyuk, S., Berdibayev, R., Sydorenko, V., Zhyharevych, O., & Smirnova, T. (2023). System of Event Correlation and Cybersecurity Incident Management at Critical Infrastructure Facilities. *Electronic Professional Scientific Publication "Cybersecurity: Education, Science, Technique", 3(19),* 176–196. https://doi.org/10.28925/2663-4023.2023.19.176196
5. Sufi, F. (2021). A New Time Series Dataset for Cyber-Threat Correlation, Regression and Neural-Network-Based Forecasting. *Information, 15,* 199. https://doi.org/10.3390/info15040199
6. Yadav, G., Yadav, D. K., Chandra Mouli, P.V.S.S.R. (2022). Statistical measures for Palmprint image enhancement. *Machine Learning for Biometrics, Academic Press,* 65–85. https://doi.org/10.1016/B978-0-323-85209-8.00010-9
7. Szabo, B. (2020). *How to Create a Seaborn Correlation Heatmap in Python?* Electronic Publication Medium. https://medium.com/@szabo.bibor/how-to-create-a-seaborn-correlation-heatmap-in-python-834c0686b88e
8. On Approval of Methodical Recommendations for Cybersecurity Entities to Respond to Various Types of Events in Cyberspace, Order of the Administration of the State Service of Special Communication and Information Protection of Ukraine dated № 570 (2023) (Ukraine). https://zakon.rada.gov.ua/rada/show/v0570519-23#Text

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023

Oleh Haiduk
Senior Lecturer at the Department of Software Engineering and Cybersecurity
State University of Trade and Economics, Kyiv, Ukraine
ORCID ID: 0000-0003-4740-7759
o.hayduk@knute.edu.ua

Volodymyr Zverev
Candidate of Technical Sciences, Senior Researcher
Associate Professor of the Department of Software Engineering and Cybersecurity
State University of Trade and Economics, Kyiv, Ukraine
ORCID ID: 0000-0002-0907-0705
zvieriev_vp@knute.edu.ua

Hennadii Hulak
Doctor of Technical Sciences, Professor, Professor of the Department of
Information and Cyber Security named after Professor Volodymyr Buryachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0001-9131-9233
h.hulak@kubg.edu.ua

CORRELATIONAL ANALYSIS OF CYBER INCIDENT TYPES IN THE CONTEXT OF INFORMATION TECHNOLOGIES FOR INTERNATIONAL COMMUNICATIONS SECURITY

Abstract. This article explores the role of correlation analysis of standardized types of cyber incidents within the context of information technology for securing international communications. The study applies correlation analysis to various types of anonymized cyber incidents in Ukraine to identify relationships between them, across established categories and types, from June 2022 to February 2024. A heatmap of correlations is used to visualize the results and further analyze the patterns in the dynamics of threats. Particular attention is paid to the possibility of using heatmaps to visually represent correlations between different types of cyber incidents. This approach allows for effective analysis of large data volumes and the identification of complex relationships that may be obscure in traditional analysis. The article focuses on the methodology of processing incident data using statistical methods to assess relationships. Correlation analysis is performed using the Pearson correlation coefficient, and the results are presented in the form of heatmaps, which allow identifying both strong and weak correlations between incident categories. This approach reveals multifactorial cyber threats and aids in understanding potential mechanisms of their joint spread and impact. Based on the obtained data, recommendations are formulated for improving the strategies of international communications cybersecurity and cyber diplomacy, particularly through the development and implementation of comprehensive protection measures that take into account the identified correlations. An analysis of the prospects for further research in this area is also conducted, aimed at optimizing information technologies for cybersecurity in international communications.

Keywords: cybersecurity; cyber diplomacy; international communications; correlation analysis; heatmaps; information technology; social networks; social engineering; state information security; cyber incidents; statistical analysis; Pearson correlation coefficient; cyber threat analysis.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Sen, Ö., van der Velde, D., Wehrmeister, K. A., Hacker, I., Henze, M., & Andres, M. (2022). On using contextual correlation to detect multi-stage cyber attacks in smart grids. *Sustainable Energy, Grids and Networks*, *32*, 100821. https://doi.org/10.1016/j.segan.2022.100821
2. Cohen, J., Cohen, P., West, S. G., & Aiken, L. S. (2013). *Applied Multiple Regression/Correlation Analysis for the Behavioral Sciences*. https://doi.org/10.4324/9780203774441.

3. Janse, R. J., Hoekstra, T., Jager, K. J., Zoccali, C., Tripepi, G., Dekker, F. W., & van Diepen, M. (2021). Conducting correlation analysis: important limitations and pitfalls. *Clin Kidney J. 14(11),* 2332–2337. https://doi.org/10.1093/ckj/sfab085
4. Gnatyuk, S., Berdibayev, R., Sydorenko, V., Zhyharevych, O., & Smirnova, T. (2023). System of Event Correlation and Cybersecurity Incident Management at Critical Infrastructure Facilities. *Electronic Professional Scientific Publication "Cybersecurity: Education, Science, Technique", 3(19),* 176–196. https://doi.org/10.28925/2663-4023.2023.19.176196
5. Sufi, F. (2021). A New Time Series Dataset for Cyber-Threat Correlation, Regression and Neural-Network-Based Forecasting. *Information, 15,* 199. https://doi.org/10.3390/info15040199
6. Yadav, G., Yadav, D. K., Chandra Mouli, P.V.S.S.R. (2022). Statistical measures for Palmprint image enhancement. *Machine Learning for Biometrics, Academic Press,* 65–85. https://doi.org/10.1016/B978-0-323-85209-8.00010-9
7. Szabo, B. (2020). *How to Create a Seaborn Correlation Heatmap in Python?* Electronic Publication Medium. https://medium.com/@szabo.bibor/how-to-create-a-seaborn-correlation-heatmap-in-python-834c0686b88e
8. On Approval of Methodical Recommendations for Cybersecurity Entities to Respond to Various Types of Events in Cyberspace, Order of the Administration of the State Service of Special Communication and Information Protection of Ukraine dated № 570 (2023) (Ukraine). https://zakon.rada.gov.ua/rada/show/v0570519-23#Text