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).

Данило БУБЛЕЙ;
Дмитро ЛАНДЕ, д.т.н., професор

ІНТЕГРАЦІЯ СПОСОБІВ ПОБУДОВИ МЕРЕЖ КІБЕРНЕТИЧНИХ УРАЗЛИВОСТЕЙ

Анотація. Досліджується процес інтеграції різних мереж кібернетичних вразливостей, сформованих з урахуванням різних сценаріїв кібернетичних атак та оборони. Ця тема важлива для розуміння складу і природи кіберзагроз.

Summary. The process of integrating various networks of cyber vulnerabilities, formed considering different scenarios of cyber attacks and defense, is under investigation. This topic is essential for understanding the complexity and nature of cyber threats.

Ключові слова: кібернетичні вразливості, мережеві моделі предметної області, інтеграція мереж, кіберзагрози, кібербезпека, генеративний штучний інтелект, захист мережі, захист даних.

Захист від кібернетичних загроз стає життєво важливим завданням для кожного користувача і підприємства. Зараз ми стикаємося з різноманітними атаками, включаючи віруси, фішинг, кібертероризм, кібершпигунство тощо. Ці загрози можуть призвести до фінансових втрат, порушення конфіденційності особистих даних, або навіть загрожувати національній безпеці. Необхідно виділяти найбільш небезпечні та найбільш зустрічні загрози, оскільки саме такий спектр вразливостей може принести найжахливішу шкоду.

Використовуючи chatgpt, для побудови зв’язків, вдалось з'ясувати найчастіші зв’язки між поняттями в галузі кібербезпеки. Ідеєю роботи було застосування повторних запитів (промтів) до системи генеративного штучного інтелекту (ГШІ), з кожним разом отримуючи нові реалізації. Зібравши достатню кількість інформації, було проведено аналіз і візуалізацію зв’язків між результатами виконання промтів. Виявлено, які теми та поняття найчастіше зустрічаються в інформаційному просторі, що дозволило нам підготуватися до надання більш точної та актуальної інформації.

На Рис. 1 можна побачити, що поняття, зображені білим кольором, досить незначні, жовтим кольором – більш суттєві, а червоним кольором – найнебезпечніші або найбільш вагомі поняття.

У розглянутому випадку, у жовтих еліпсах розташовані такі поняття, як Безпека, VPN, Політика безпеки, Захист мережевого трафіку. Вже за ними можна зрозуміти що безпосередньо безпека є дуже

важливим аспектом, та має велику кількість зв'язків, але вочевидь поняття у червоному еліпсі (Захист) свідчить про велику вагу цього поняття в інформаційному просторі, важливість захисту від потенційних загроз та спроби ліквідувати вразливості.

Хоча вже з цієї первинної мережі вже можна визначити напрямок необхідних дій в області кіберзахисту, однак шляхом створення додаткових мереж за подібними промптами і поєднання (інтеграції) цих мереж було сформовано узагальнену мережу, яка дозволила виявити більш широкий спектр понять і зв'язків. При візуалізації узагальненої матриці також розширився спектр значимості окремих понять (з'явились зелені та сині кольори), мережа стала щільнішою.

Синім кольором на Рис. 2 стали такі поняття: Захист даних, Захист мережі, Інтеграція безпеки, Мережева інтеграція, а червоним залишається Захист. Це свідчить про те, що безпека завжди залишається однією з основних тем в цифровому світі.

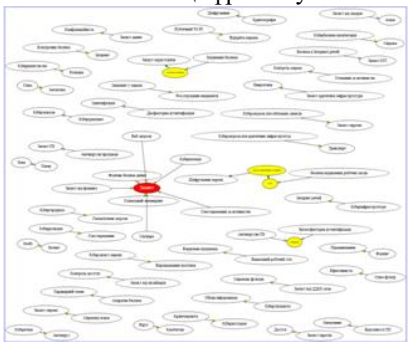

Рисунок 1 – Фрагмент первинної мережі

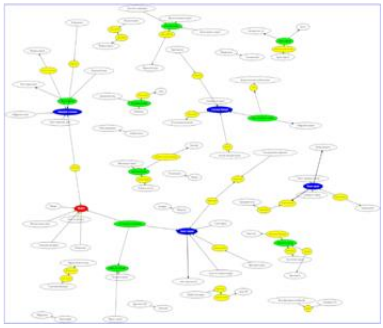

Рисунок 2 – Фрагмент повної мережі

На підставі аналізу нашої роботи можна визначити, що дослідження та інтеграція різних сценаріїв кібернетичних вразливостей в наш час є не лише корисними, але й необхідними для ефективної кібербезпеки. Безпека завжди залишається в основі цифрового світу, і інтеграція мереж вразливостей розширює наше розуміння загроз.

Висновки. Дослідження та інтеграція різноманітних сценаріїв кібернетичних вразливостей дозволяють краще розуміти сучасні загрози та шляхи організації відповідної протидії. Інтегруючи різні мережі вразливостей, створюється більш повний та реалістичний образ кіберзагроз, що допоможе розробляти комплексні стратегії захисту.