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).

Віктор САСЬКО;
Дмитро ЛАНДЕ, д.т.н., професор

ПОБУДОВА ПРИЧИНО-НАСЛІДКОВОЇ МЕРЕЖІ ДЛЯ ВИЯВЛЕННЯ І РАНЖУВАННЯ СЦЕНАРІЇВ ДІЯЛЬНОСТІ

Анотація. Розглянуто рішення для побудови причино-наслідкової мережі, шляхом застосування двонаправленого алгоритму, що удосконалило вже існуючі методи аналізу та прогнозування майбутніх кібератак, формування звітів на основі цієї інформації, за допомогою сервісу генеративного штучного інтелекту.

Summary. The article considers a solution for building a causal network by applying a bidirectional algorithm, which improved the existing methods of analyzing and predicting future cyberattacks, generating reports based on this information, using a generative artificial intelligence service.

Ключові слова: причино-наслідкова мережа, ранжування, штучний інтелект, кібератаки.

Сучасний віртуальний світ на цей час стає однією із можливих загроз людству. Кібератаки стають все частішими, більш витонченими та складними. Тому побудова причино-наслідкової мережі для виявлення та ранжування сценаріїв кібератак є надзвичайно важливою.

Аналіз вже існуючих робіт з цієї тематики вказує на тенденції в зміні причин кібератак. Виходячи з цього, прийнято рішення відобразити результати роботи у форматі причино-наслідкової мережі, що допоможе виявляти та ранжирувати потенційні сценарії діяльності, які можуть призвести до кібератак.

Для досягнення наших цілей у дослідженні, на поточному етапі досліджень використовувалися дані, що були отримані від системи генеративного штучного інтелекту (СГШІ) chatgpt.

Для цього було сформовано запит, що дозволяє отримати інформацію про окремі кібератаки, включаючи їх причини та наслідки у форматі “Причина; Наслідок”.

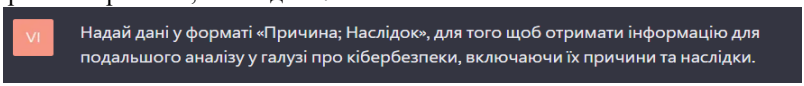

Рис.1. Промт для отримання інформації про причини кібератак.

Після збору даних, за допомогою СГШІ було проведено їх нормалізацію, щоб забезпечити спільність даних та зручність їх для подальшого аналізу. Цей крок дозволив виявити загальні та унікальні аспекти різних кібератак та їх взаємодію.

У подальшому здійснюється обробка цих даних для побудови структурованого набору інформації.

Для аналізу структурованих даних було застосовано двонаправлений алгоритм, що дозволяє виявити зв'язки між різними подіями та факторами. На основі цього аналізу і було побудовано причино-наслідкову мережу, яка графічно відображає взаємодію між різними елементами кібератак та їхніми причинами.

Наш підхід допомагає у виявленні ризиків та розробці стратегій кіберзахисту для захисту інформаційних активів та систем. За допомогою причино-наслідкової мережі, ми можемо помітити тенденції та основні причини кібератак, що допоможе нам у протидії та підвищенню рівня кіберзахисту.

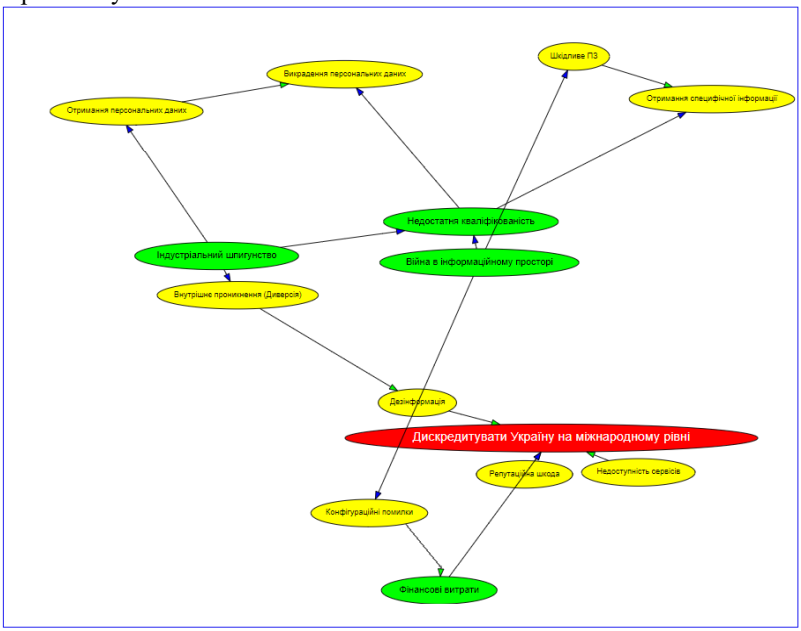

Рис. 2. Причино-наслідкова мережа кібератак.

Висновки. Формування причино-наслідкової мережі на основі даних, наданих системою chatgpt, виявляється ефективним інструментом для аналізу та ранжування причин і наслідків кібератак. Використання цього підходу сприяє покращенню стратегій кібербезпеки та забезпечує належний захист від подібних загроз, що є ключовим в контексті підвищення рівня кіберзахисту.