Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА
на тему:
«Метод виявлення потенційного кіберпорушника з використанням штучного інтелекту»

Виконав: студент 2-го курсу, групи 2БС-22м

спеціальності 125 – Кібербезпека

_____Андрій МАРУСІЙ

Керівник: к. т. н., доцент каф. ЗІ

_____ Віталій ЛУКІЧОВ

Рецензент: к. т. н. доцент каф. ПЗ

_____ Олена КОВАЛЕНКО

«13» 12 2023р.

Допущено до захисту

Завідувач кафедри ЗІ
д. т. н., проф.
Володимир ЛУЖЕЦЬКИЙ
«14» 12 2023 р.

Вінниця ВНТУ – 2023 рік

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації
Рівень вищої освіти ІІ-й (магістерський)
Галузь знань 12 Інформаційні технології
Спеціальність 125 Кібербезпека
Освітня програма – Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ
Завідувач кафедри ЗІ,
д. т. н., проф.
Володимир ЛУЖЕЦЬКИЙ
«19» 09 2023 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Марусію Андрію Андрійовичу

1. Тема роботи: «Метод виявлення потенційного кіберпорушника з використанням штучного інтелекту»,
   керівник роботи: Лукічов Віталій Володимирович, к.т.н., доцент каф. ЗІ,
   затверджені наказом ректора ВНТУ від 18 вересня 2023 року №247.
2. Строк подання студентом роботи 14 грудня 2023 р.
3. Вихідні дані до роботи:
   - Дані автора роботи;
   - OSINT - інструменти.
   - Моделі штучного інтелекту.
4. Зміст текстової частини: Вступ. 1. Аналіз методів та засобів виявлення потенційних кіберпорушників. 2. Теоретичні основи виявлення кіберпорушників. 3. Методологія виявлення кіберпорушників з використання штучного інтелекту. 4. Метод виявлення кіберпорушників з використанням штучного інтелекту 5. Економічна частина. Висновки. Перелік використаних джерел. Додатки.
5. Перелік ілюстративного матеріалу: Актуальність, мета та задачі МКР (плакат А4). Метод шифрування даних (плакат А4). Алгоритм роботи засобу (плакат А4). Результати інтеграційного тестування (плакат А4). Висновки з виконаної роботи (плакат А4).

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанти	Підпис, дата	
		завдання видав	виконання прийняв
1	Віталій ЛУКІЧОВ., к.т.н., доцент каф. ЗІ	19.09	21.09
2	Віталій ЛУКІЧОВ., к.т.н., доцент каф. ЗІ	19.09	22.09
3	Віталій ЛУКІЧОВ., к.т.н., доцент каф. ЗІ	19.09	26.10
4	Ольга РАТУШНЯК., к.т.н., доцент каф. ЕПВМ	19.09	17.10

7. Дата видачі завдання 1 вересня 2023 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи	Прим
1	Аналіз завдання. Вступ	01.09.2023 – 10.09.2023	
2	Аналіз інформаційних джерел за напрямком магістерської кваліфікаційної роботи	10.09.2023 – 15.09.2023	
3	Розробка рішень	16.09.2023 – 22.09.2023	
4	Практична реалізація, моделювання, експериментування, результати	23.09.2023 – 29.09.2023	
5	Розробка розділу економічного обґрунтування доцільності розробки	30.09.2023 – 24.11.2023	
6	Оформлення пояснювальної записки	25.11.2023 – 30.11.2023	
7	Попередній захист та доопрацювання МКР	28.11.2023 – 01.12.2023	
8	Представлення МКР до захисту	11.12.2023 – 14.12.2023	
9	Захист МКР	14.12.2023 – 21.12.2023	

Студент _____ Андрій МАРУС

Керівник роботи _____ Віталій ЛУКІЧ

АНОТАЦІЯ

УДК 004.056

Марусій А.А. Метод виявлення потенційного кіберпорушника з використанням штучного інтелекту. Комплексна магістерська кваліфікаційна робота зі спеціальності 125 – Кібербезпека, освітня програма – Безпека інформаційних і комунікаційних систем. Вінниця: ВНТУ, 2023. 87 с.

На укр. мові. Бібліогр.: 17 назв; рис.: 8; табл. 6.

Комплексна магістерська кваліфікаційна робота присвячена розробці методу виявлення кіберпорушників у соціальних мережах. Досліджено існуючі аналоги та програмні реалізації систем виявлення загроз для обґрунтування вибору власних методів та розробки необхідних схем і алгоритмів. Здійснено програмну реалізацію розробленої системи та проведено відповідне тестування на коректність функціонування.

Ілюстративна частина складається з 7 плакатів з демонстрацією схеми алгоритму роботи системи та прикладами її використання.

В економічному розділі оцінено витрати на розробку.

Ключові слова: захищена система, виявлення кіберпорушників, соціальні мережі, кібербезпека.

АНОТАЦІЯ

UDC 004.056

Marusii A.A. A method of identifying a potential cyber offender using artificial intelligence. Comprehensive master's qualification work on specialty 125 - Cybersecurity, educational program - Security of information and communication systems. Vinnytsia: VNTU, 2023. 87 p.

In Ukrainian language. Bibliographer: 17 titles; fig.: 8; tabl.: 6.

The comprehensive master's thesis is devoted to the development and implementation of a secure system for detecting cybercriminals in social networks. The existing analogues and software implementations of threat detection systems were studied to justify the choice of own methods and the development of the necessary schemes and algorithms. The software implementation of the developed system was carried out and appropriate testing was carried out for the correct functioning.

The illustrative part consists of 7 posters with a demonstration of the algorithm scheme of the system and examples of its use.

Development costs are estimated in the economic section.

Keywords: protected system, detection of cyber criminals, social networks, cyber security.

ЗМІСТ

ВСТУП

У сучасному світі кібербезпека є одним з найважливіших пріоритетів для організацій будь-якого масштабу. Зростаюча кількість кібератак, які вчиняються з використанням все більш витончених методів, вимагає від організацій розробки ефективних методів захисту своїх інформаційних систем. Одним із ключових завдань кібербезпеки є виявлення кіберпорушників.

На сьогоднішній день існує безліч методів виявлення кіберпорушників. Однак ці методи часто мають обмеження. Так, деякі методи можуть бути неефективними для виявлення нових типів кібератак. Інші методи можуть бути занадто повільним для своєчасного виявлення кіберпорушників. Штучний інтелект (AI) має потенціал для вирішення цих проблем. AI може бути використаний для розробки ефективніших і швидших методів виявлення кіберпорушників. Розробка методу виявлення кіберпорушника з використанням AI є актуальним дослідженням, яке може мати значний вплив на кібербезпеку.

Об’єктом дослідження є процес розслідування кіберінцидентів.

Предмет дослідження є методи виявлення кіберпорушників, інструменти OSINT та інструменти штучного інтелекту.

Метою підвищення ефективності процесу розслідування кіберінцидентів. Для досягнення мети потрібно виконати наступні завдання:

- виконати аналіз засобів для виявлення потенційних кіберпорушників
- проаналізувати відомі методи кіберозслідувань;
- розробити моделі системи;
- розробити програмний засіб в ядрі якого є штучний інтелект;
- виконати експериментальне дослідження методу.

Новизна дослідження: Відсутність подібних методів станом на 2023 рік.

Практичне значення Якісному методі пошуку кіберпорушників, який за допомогою ШІ підвищує ефективність кіберрозслідувань.

1 ТЕОРЕТИЧНІ ОСНОВИ ВИЯВЛЕННЯ КІБЕРПОРУШНИКІВ

1.1 Поняття кіберзагрози та класифікації кіберзагроз

Кіберзагроза або загроза кібербезпеці визначається як зловмисна дія, спрямована на викрадення чи пошкодження даних або порушення цифрового добробуту та стабільності підприємства. Кіберзагрози включають широкий спектр атак, починаючи від витоку даних, комп'ютерних вірусів, відмови в обслуговуванні та багатьох інших векторів атак. У цьому підрозділі розглядається визначення кіберзагроз, типи кіберзагроз і деякі типові приклади загроз.

Все, що може завдати серйозної шкоди комп'ютерній системі, мережам або іншим цифровим активам організації чи особи, є кіберзагрозою. Згідно з Techopedia, кіберзагрози перетворюють потенційні вразливості на реальні атаки на системи та мережі. Загрози кібербезпеці можуть включати все: від троянів, вірусів, хакерів до бекдорів. У більшості випадків більш доречним є термін «змішана кіберзагроза», оскільки одна загроза може включати кілька експлойтів [1]. Наприклад, хакер може використати фішингову атаку, щоб отримати інформацію та зламати мережу.

Кіберзагрози також стосуються потенційних кібератак, спрямованих на отримання несанкціонованого доступу, порушення, викрадення або пошкодження IT-активів, інтелектуальної власності, комп'ютерної мережі чи будь-якої іншої форми конфіденційних даних. Загрози можуть надходити від довірених користувачів із підприємства та віддалених місць від невідомих зовнішніх сторін.

Не буде перебільшенням сказати, що загрози кібербезпеці впливають на кожен аспект нашого життя. Фактично кіберзагрози можуть призвести до відключення електроенергії, виходу з ладу військового обладнання або порушення секретів національної безпеки. Вони можуть порушити комп'ютерні та телефонні мережі або паралізувати системи, зробивши дані недоступними . Вони також можуть спричинити крадіжку конфіденційних, цінних даних, таких як медичні записи та інша особиста інформація споживачів і співробітників у всьому світі.

Загрози кібербезпеці за своєю природою постійно розвиваються. Команди корпоративної безпеки повинні постійно бути в курсі та випереджати всі нові загрози в домені, які можуть вплинути на їхній бізнес. Ось список поширених кіберзагроз, з якими організації стикаються найчастіше.

Зловмисне програмне забезпечення – це загальний термін, який описує будь-яку програму чи файл, які мають намір порушити роботу системи, чи комп'ютера, чи завдати шкоди їм [2]. Зловмисне програмне забезпечення проникає в мережу через вразливість, як правило, коли користувач натискає вкладення електронної пошти або небезпечне посилання, яке встановлює небезпечне програмне забезпечення. До різних типів шкідливого програмного забезпечення належать:

- Троян — це різновид зловмисного програмного забезпечення, яке маскується під законне програмне забезпечення, але під час виконання робить шкідливі дії.
- Віруси та хробаки — це частина шкідливого коду, яка встановлюється без відома користувача. Ці віруси можуть розмножуватися та поширюватися на інші системи, просто приєднуючись до комп'ютерних файлів. Хробаки також саморозмножуються, як і віруси, але їм не потрібно приєднуватися до іншої програми для розмноження.
- Програми-вимагачі – це тип зловмисного програмного забезпечення, яке шифрує інформацію жертви та вимагає плату за ключ розшифровки. Навіть якщо ви заплатите викуп, це не обов'язково гарантує, що ви зможете відновити зашифровані дані.
- Програмне забезпечення ботнету спеціально розроблене для зараження величезної кількості пристроїв, підключених через Інтернет. Кілька ботнетів містять мільйони скомпрометованих машин, кожна з яких використовує незначну кількість процесорної потужності [3]. Через це надзвичайно складно виявити ботнети, навіть коли вони запущені.

- Шпигунське програмне забезпечення — це форма шкідливого програмного забезпечення, яке використовується для незаконного моніторингу комп’ютерної діяльності користувача та збору особистої інформації.
- Трояни віддаленого доступу або RAT встановлюють бекдори на цільових системах. Вони забезпечують віддалений доступ, а також адміністративний контроль для зловмисних користувачів.
- Бекдори дозволяють віддалений доступ до систем і комп'ютерів без відома користувачів.
- Атаки з отруєнням системи доменних імен (DNS) компрометують DNS для перенаправлення веб-трафіку на шкідливі сайти [4]. Вони не зламують уражені сайти компрометують DNS для перенаправлення веб-трафіку на шкідливі сайти. Вони не зламують уражені сайти.
- Розподілені атаки типу «відмова в обслуговуванні» або DDoS-атаки заповнюють сервери, системи та мережі веб-трафіком, щоб виснажити ресурси або пропускну здатність і спричинити їх збій. Через це система не може виконати жодного законного запиту.
- Під час прийому форм зловмисний код JavaScript вставляється в платіжні онлайн-форми для збирання даних карток клієнтів

Хоча можливі багато типів кібератак, типові методи та тактики атак противника можна згрупувати в матриці, яка включає такі категорії:

- Початковий доступ включає методи, які використовуються для закріплення в мережі, як-от цілеспрямований фішинг , недоліки конфігурації в загальнодоступних системах або використання вразливостей.
- Командування та контроль (C&C) – це один із найважливіших аспектів будь-якої кібератаки. За допомогою C&C зловмисники можуть керувати зараженими системами, отримувати доступ до інформації та завдавати шкоди. Зловмисник намагається уникнути виявлення, використовуючи

порти, які рідко використовуються для зв'язку з системами [5]. Існує багато інших методів C&C, які використовують зловмисники. Наприклад, вони можуть використовувати мережі анонімного доступу (Tor), хмарну інфраструктуру або навіть соціальні мережі для зв'язку з зараженими системами.

- Збір включає тактики, які використовували супротивники для збору та консолідації інформації, на яку вони націлювалися, як частину своїх цілей.
- Настійливість (persistence) – це методи, які дозволяють зловмиснику зберігати доступ до цільової системи, навіть після зміни облікових даних та перезавантаження. Наприклад, зловмисник може створити планований завдання, яке запускає його код при перезавантаженні або у певний час. Настійливість – це важливий аспект будь-якої кібератаки. За допомогою настійливості зловмисники можуть гарантувати, що вони зможуть отримати доступ до системи навіть після того, як їхня початкова атака буде виявлена та нейтралізована. Існує багато інших методів настійливості, які використовують зловмисники. Наприклад, вони можуть використовувати шкідливі програми, які можуть інфікувати завантаження системи або драйвери пристроїв [6]. Це може зробити їх важкими для видалення або усунення.

Ухил від захисту – це методи, які використовують зловмисники, щоб уникнути виявлення. Вони включають в себе:

- Приховування шкідливого коду в довірених папках і процесах: Зловмисники можуть ховати шкідливий код у папках і процесах, які вважаються безпечними. Це може зробити його важче виявити для програмного забезпечення безпеки.
- Відключення програмного забезпечення безпеки: Зловмисники можуть використовувати різні методи для відключення програмного забезпечення безпеки, наприклад, модифікуючи налаштування безпеки або інфікуючи

систему шкідливою програмою, яка може відключати програмне забезпечення безпеки.

- Замаскування шкідливого коду: Зловмисники можуть використовувати різні методи для замаскування шкідливого коду, наприклад, зашифровуючи його або маскуючи його під законний код. Це може зробити його важче виявити для програмного забезпечення безпеки.
- Виконання (execution) – це методи, які використовуються для запуску коду на цільовій системі. Наприклад, зловмисник може запустити сценарій PowerShell для завантаження додаткових інструментів зловмисника або сканування інших систем.
- Виявлення (discovery) – це методи, які використовуються зловмисниками для отримання інформації про мережі та системи, які вони планують використовувати для досягнення своїх тактичних цілей.
- Доступ до облікових даних (credential access) – це методи, які використовуються на мережах і системах для крадіжки імен користувачів і паролів для повторного використання.
- Вплив (impact) – це методи, які використовують зловмисники для впливу на доступність даних, систем та мереж. Це включає атаки на відмову в обслуговуванні, програмне забезпечення для видалення даних або дисків.
- Бічний рух (lateral movement) – це тактика, яка дозволяє зловмисникам переміщатися з однієї системи на іншу в мережі. Деякі поширені техніки включають зловживання протоколом віддаленого робочого столу або методами аутентифікації користувачів за допомогою хешів [7].

1.2 Методи виявлення кіберзагроз.

Раннє виявлення та втручання є метою всіх методів виявлення загроз. Коли трапляються зломи мережі, їх швидке виявлення може допомогти командам безпеки мінімізувати втрату даних і зменшити шкоду.

Розвідка про кіберзагрози – це процес ідентифікації, аналізу та розуміння загроз, які були спрямовані на організацію в минулому, зараз намагаються

отримати несанкціонований доступ і, ймовірно, зроблять це в майбутньому. Аналітики можуть використовувати будь-яку інформацію про загрози всередині своєї організації або від груп безпеки, які публікують публікації в Інтернеті, щоб застосувати їх до власних даних. Наприклад, якщо злам стався в іншій організації, вони можуть опублікувати ці індикатори компрометації (IOC) в Інтернеті, щоб будь-хто міг використовувати їх і потенційно виявити подібні шаблони у своїх власних даних безпеки. Подібно до того, як уряди збирають дані про спроби іноземного супротивника зламати їхній захист, виявлення загроз може допомогти зміцнити захист і нейтралізувати поточні загрози безпеці. Розвідка про загрози прагне зрозуміти наступне:

- Методи, якими користуються зловмисники;
- Уразливості в мережі, системах і додатках компанії;
- Ідентифікація зловмисників, які прагнуть скомпрометувати мережі.

Ця інформація допомагає підвищити готовність до кібербезпеки та зусилля щодо пом’якшення загроз, одночасно інформуючи керівників компаній і зацікавлених сторін про потенційні ризики та наслідки, якщо зловмисники досягнуть успіху.

Аналіз моделей поведінки внутрішніх користувачів може допомогти мисливцям за загрозами позначити відхилення, які можуть вказувати на те, що облікові дані користувача зламано. Ці дані можуть включати такі речі, як типи інформації, до якої користувачі отримують регулярний доступ, який час доби кожен користувач зазвичай активний у мережі та звідки вони працюють. Наприклад, керівник корпорації найвищого рівня, який зазвичай працює в робочі години з домашнього офісу в Сіетлі, навряд чи ввійде в корпоративну мережу о 2:30 ночі в Брюсселі [8]. Встановлюючи базову лінію для того, як виглядає звичайна поведінка, аналітики безпеки можуть краще виявляти аномалії, які потребують подальшої перевірки.

Як бджола до меду, деякі цілі занадто солодкі, щоб погані актори їх ігнорували. Пастка для зловмисників — це техніка виявлення загроз, яка діє як

спецоперація, розроблена, щоб виманити хакерів із тіні, щоб групи кібербезпеки могли виявити їхню присутність. Команди встановлюють пастки, створюючи фальшиві цілі, такі як області, які, здається, містять мережеві служби, або недостатньо захищені облікові дані, які, схоже, можуть бути використані для доступу до областей, що містять конфіденційні дані. Після доступу ці пастки для зловмисників діють як провід, сповіщаючи команди безпеки про те, що хтось активно перевіряє систему та потрібне втручання.

Полювання за загрозами — це відкрито проактивний підхід до виявлення загроз, коли аналітики безпеки активно шукають загрози, що насуваються, або ознаки того, що зловмисники вже отримали доступ до ключових систем. Перевіряючи мережу організації, кінцеві точки та технології безпеки, мисливці за загрозами прагнуть виявити зловмисників, які успішно уникли поточного кіберзахисту.

Інструменти та методи виявлення загроз постійно вдосконалюються, щоб протистояти постійно мінливим загрозам безпеці мережі та даних. Хоча потреби безпеки кожної організації унікальні, ці технології виявлення загроз належать до арсеналу кібербезпеки кожної організації.

Об’єднуючи дані по всій мережі організації, технологія подій безпеки збирає події, включаючи автентифікацію, доступ до мережі та журнали з критичних систем, в одне місце. Це спрощує такі завдання, як порівняння даних загальносистемного журналу з потенційними проблемами за допомогою каналу бази даних загроз для більш ефективного аналізу журналів подій і викорінення ймовірних кіберзагроз. Технологія подій безпеки дозволяє аналітикам безпеки отримати повне уявлення про всі свої кінцеві точки, включаючи брандмауери, пристрої та програми IDS/IPS, сервери, комутатори, журнали ОС, маршрутизатори та інші програми [9].

Технологія мережевих загроз відстежує трафік у мережі організації, між іншими надійними мережами та в Інтернеті, щоб активно сканувати підозрілі дії, які можуть свідчити про наявність зловмисної діяльності. Ця технологія скорочує

час реакції на виявлення загроз і реакцію, що робить її критичним інструментом для протидії зростаючій кількості системних атак хакерів.

Виявлення загроз кінцевої точки та реагування на неї — це рішення безпеки кінцевої точки, яке реалізує безперервний моніторинг і збір даних кінцевої точки за допомогою можливостей автоматичного реагування та аналізу на основі правил. Ця технологія дає змогу відстежувати та збирати дані про діяльність у режимі реального часу з кінцевих точок, наприклад машин користувачів, які можуть вказувати на наявність потенційної загрози. Озброївшись цими даними, команди можуть швидко ідентифікувати шаблони загроз, згенерувати автоматичну відповідь, яка видаляє або містить загрози, і повідомляти персонал служби безпеки для подальшого втручання. Технологія виявлення загроз кінцевої точки також надає поведінкову або криміналістичну інформацію, щоб допомогти у розслідуванні виявлених загроз.

1.4 Переваги та недоліки використання ШІ у кібербезпеці.

Щоб допомогти командам безпеки впоратися з цими нескінченними атаками, ШІ стає важливим союзником. Здатність штучного інтелекту аналізувати величезні масиви даних, виявляти закономірності та приймати розумні рішення в режимі реального часу зробила його кардинальним у боротьбі проти кіберзагроз. Оскільки базові моделі продовжують розвиватися, ШІ є рішенням, яке компаніям, безумовно, варто розглянути щодо впровадження, коли справа доходить до боротьби з цими ризиками та загрозами.

ШІ може аналізувати величезні обсяги даних у режимі реального часу, виявляючи аномалії та потенційні загрози з високою точністю. Це пояснюється тим, що штучний інтелект може вивчати закономірності в даних, які не можуть отримати люди, і може ідентифікувати загрози, які можуть бути пропущені традиційними інструментами безпеки. Наприклад, штучний інтелект можна використовувати для аналізу мережевого трафіку для виявлення підозрілих моделей, таких як велика кількість підключень з однієї IP-адреси.

ШІ може автоматизувати обробку інцидентів, мінімізуючи збитки та забезпечуючи швидке відновлення. Це тому, що штучний інтелект може швидко виявляти загрози та реагувати на них без втручання людини. Наприклад, штучний інтелект можна використовувати для автоматичного розміщення заражених пристроїв у карантині або для скасування змін, внесених зловмисником.

ШІ може виявляти підозрілі дії користувачів, захищаючи від внутрішніх загроз. Це пояснюється тим, що штучний інтелект може навчатися нормальній поведінці користувача та визначати відхилення від цієї поведінки. Наприклад, штучний інтелект можна використовувати, щоб виявити, чи намагається користувач отримати доступ до конфіденційних даних із несанкціонованого місця.

ШІ може обробляти дані розвідки про загрози, щоб передбачати й запобігати потенційним загрозам. Це пояснюється тим, що штучний інтелект може дізнаватися про відомі загрози та використовувати ці знання для виявлення потенційних загроз, які ще невідомі. Наприклад, штучний інтелект можна використовувати, щоб передбачити, які системи, швидше за все, стануть мішенню для конкретного суб’єкта загрози.

ШІ може виявляти відхилення від нормальної поведінки, ідентифікуючи атаки нульового дня. Це тому, що штучний інтелект може навчитися нормальній поведінці та визначити відхилення від цієї поведінки. Наприклад, штучний інтелект можна використовувати для виявлення ненормальної поведінки системи, що може бути ознакою атаки нульового дня [10].

ШІ може аналізувати електронні листи та URL-адреси, щоб відрізнити спроби фішингу від законних повідомлень. Це пояснюється тим, що штучний інтелект може дізнатися про характеристики фішингових електронних листів і URL-адрес і використовувати ці знання для виявлення спроб фішингу. Наприклад, штучний інтелект можна використовувати, щоб виявити, чи надходить електронний лист від підозрілого відправника, чи URL-адреса вказує на шкідливий веб-сайт.

Традиційні методи виявлення загроз певною мірою ефективні, але вони стикаються з кількома проблемами та обмеженнями. Однією з важливих проблем є

величезний обсяг даних, який генерують сучасні мережі та системи, що ускладнює аналітикам вручну ідентифікувати потенційні загрози в режимі реального часу. Крім того, кіберзагрози стають все більш витонченими і можуть легко уникнути систем виявлення на основі правил. Традиційні методи можуть не відставати від технологій атак, що швидко розвиваються, роблячи організації вразливими до прогресивних загроз. Більше того, хибно-позитивні та хибно-негативні результати можуть погіршити точність виявлення загроз, що призведе до втрати часу та ресурсів на розслідування інцидентів, що не становлять загрози, або втрати реальних загроз.

Системи виявлення загроз на основі ШІ використовують алгоритми машинного навчання, щоб подолати обмеження традиційних методів. Ці системи можуть аналізувати величезні обсяги даних у режимі реального часу, виявляючи шаблони та аномалії, які можуть означати потенційні порушення безпеки. Алгоритми штучного інтелекту можуть навчатися на історичних даних і адаптуватися до нових загроз, що робить їх високоефективними у виявленні раніше невідомих векторів атак. Здатність виявляти незвичайні шаблони та поведінку, навіть без чітких правил, дозволяє системам на основі ШІ виявляти атаки нульового дня та інші складні загрози, які традиційні методи можуть пропустити [11].

Приклади з реального світу, як штучний інтелект виявляє кіберзагрози:

- Виявлення вторгнень у мережу. Системи виявлення вторгнень на основі штучного інтелекту можуть контролювати мережевий трафік, ідентифікувати підозрілі дії та вторгнення з різних векторів атак, як-от зловмисне програмне забезпечення, спроби фішингу та атаки грубої сили.
- Аналіз поведінки. Алгоритми штучного інтелекту можуть аналізувати поведінку користувачів і виявляти відхилення від звичайних шаблонів, дозволяючи виявляти внутрішні загрози або зламані облікові записи.
- Розширене виявлення зловмисного програмного забезпечення: штучний інтелект може розпізнавати раніше невідомі шаблони та поведінку зловмисного програмного забезпечення, сприяючи ранньому виявленню та локалізації.

Штучний інтелект відіграє вирішальну роль в аналітиці безпеки, обробляючи та аналізуючи великі обсяги даних, отриманих із різних джерел, таких як журнали, мережевий трафік, дії користувачів і події кінцевих точок. Алгоритми можуть швидко просіювати ці дані, щоб виявити потенційні інциденти безпеки, аномалії та тенденції. Цей автоматизований аналіз значно зменшує робоче навантаження на аналітиків і дозволяє швидше реагувати на нові загрози.

Аналітика на основі штучного інтелекту може виявити потенційні вразливості та слабкі місця в системі безпеки організації шляхом постійного моніторингу та оцінки IT-середовища. Алгоритми можуть виявляти помилки конфігурації, застаріле програмне забезпечення та неправильні конфігурації, які можуть створити прогалини в безпеці. Зіставляючи дані з багатьох джерел, аналітика штучного інтелекту може надати цілісне уявлення про систему безпеки та визначити пріоритетність критичних вразливостей, дозволяючи командам безпеки вирішувати їх проактивно [12].

Тематичні дослідження аналітики безпеки на основі ШІ:

- Автоматизація реагування на інциденти: аналітика безпеки на основі штучного інтелекту може автоматизувати реагування на інциденти, виявляючи загрози, оцінюючи їх серйозність і запускаючи відповідні відповіді. Це допомагає стримувати загрози до їх ескалації, скорочуючи час реакції та мінімізуючи потенційну шкоду.
- Полювання на загрози: алгоритми штучного інтелекту можуть допомогти аналітикам безпеки в пошуках загроз, позначаючи підозрілі шаблони та виділяючи потенційні індикатори загроз, роблячи полювання ефективнішим і ефективнішим.
- Прогнозна безпека: аналізуючи історичні дані, аналітика безпеки на основі штучного інтелекту може передбачити потенційні загрози безпеці та вразливості, дозволяючи організаціям вживати превентивних заходів для зміцнення свого захисту.

Традиційне реагування на інциденти – це ручний процес, який може зайняти багато часу та бути схильним до помилок. Зазвичай це включає такі кроки:

- Виявлення : виявлення того, що стався інцидент.
- Локація : ізоляція уражених систем і запобігання подальшому пошкодженню.
- Розслідування : встановлення першопричини інциденту.
- Усунення : виправлення вразливості, яка призвела до інциденту.
- Відновлення : відновлення уражених систем до початкового стану.

Реагування на інциденти, кероване ШІ, автоматизує та прискорює багато з цих кроків. Це може допомогти організаціям скоротити час відповіді та мінімізувати шкоду.

ШІ можна використовувати для автоматизації та прискорення виявлення інцидентів різними способами. Наприклад, штучний інтелект можна використовувати для моніторингу мережевого трафіку на наявність шкідливих дій. Його також можна використовувати для аналізу поведінки користувачів на ознаки компрометації. Після виявлення інциденту ШІ можна використовувати для автоматизації процесу стримування [13]. Це може включати ізоляцію уражених систем і блокування шкідливого трафіку. ШІ також можна використовувати для автоматизації процесу відновлення. Це може включати відновлення пошкоджених систем до початкового стану та впровадження заходів пом’якшення наслідків для запобігання майбутнім інцидентам.

Штучний інтелект (ШІ) показав великі надії на посилення кібербезпеки, але він також має власний набір проблем і ризиків, які необхідно вирішити. Оскільки ШІ стає все більш поширеним у практиці кібербезпеки, організації повинні знати про такі потенційні підводні камені.

Алгоритми штучного інтелекту настільки хороші, наскільки хороші дані, на яких вони навчаються, і якщо ці дані містять упередження, система штучного інтелекту може зберегти та посилити ці упередження. Наприклад, якщо історичні дані, які використовуються для навчання моделі кібербезпеки штучного інтелекту, мають упередження щодо певних типів загроз або зловмисників, вони можуть не помічати нові загрози з різних джерел. Забезпечення різноманітності та

інклюзивності навчальних даних і регулярний аудит систем штучного інтелекту на наявність упереджень є ключовими кроками для зменшення цього ризику.

Крім того, системи штучного інтелекту мають обмеження в розумінні контексту та наміру, що може призвести до помилкових позитивних або негативних результатів. Це обмеження може призвести до помилкової ідентифікації законної діяльності як зловмисної або навпаки. Фахівці з кібербезпеки повинні бути пильними в інтерпретації результатів, створених штучним інтелектом, і підтверджувати їх за допомогою людського досвіду.

З розвитком технологій штучного інтелекту кіберзловмисники можуть використовувати їх у своїх інтересах. Наприклад, зловмисники можуть використовувати штучний інтелект для розробки та виконання складніших атак, які обходять традиційні засоби захисту кібербезпеки. Діпфейки та синтетичний контент, створені штучним інтелектом, також можуть бути використані для обману користувачів і проникнення в заходи безпеки. Крім того, важливі постійний моніторинг і оновлення моделей ШІ, щоб випередити потенційне зловмисне використання.

Кібербезпека, керована штучним інтелектом, викликає етичні проблеми, зокрема щодо конфіденційності користувачів і стеження. Збір і аналіз величезних обсягів даних для виявлення загроз може порушувати права особи на конфіденційність. Встановлення правильного балансу між безпекою та конфіденційністю має вирішальне значення, щоб уникнути порушення етичних принципів.

Прозорість і зрозумілість алгоритмів штучного інтелекту також важливі для завоювання довіри користувачів. Користувачі та зацікавлені сторони повинні розуміти, як ШІ приймає рішення та чому вживаються певні дії. Для забезпечення відповідального використання штучного інтелекту в практиці кібербезпеки слід розробити етичні принципи [14].

1.4 Постановка задачі

В сучасному інформаційному середовищі, де кібербезпека стає найважливішим аспектом забезпечення безпеки даних та інформаційних систем,

розробка ефективних методів пошуку та слідкування за потенційними кіберпорушниками за допомогою систем штучного інтелекту (ШІ) є вельми актуальним завданням. Мета даного проекту полягає в створенні інноваційного підходу до виявлення та моніторингу діяльності зловмисників в інформаційних системах, забезпечуючи високий рівень кібербезпеки. Так як поле кіберпорушень є надзвичайно велике, тому варто виділити, що даний метод працюватиме саме для виявлення порушників, що працюють у соціальних мережах. Це важливо особливо в умовах боротьби з тероризмом, кібервійнах, розголошені секретної інформації чи поширені забороненого матеріалу через соціальні мережі, або месенджери.

1.5 Висновки з розділу

Кіберзлочинність - це серйозна проблема, яка може призвести до значних фінансових збитків, порушення конфіденційності та інших проблем. Існує багато різних форм кіберзлочинності, включаючи кібертероризм, кібервійну, фінансову крадіжку, кібершахрайство, телемаркетингове шахрайство та копіювання веб-сайтів.

Кіберпорушники використовують комп'ютерні технології для досягнення своїх злочинних цілей. Вони можуть атакувати комп'ютерні системи та мережі, щоб отримати доступ до даних, вкрасти гроші або завдати шкоди. Вони також можуть використовувати шкідливе програмне забезпечення для поширення дезінформації, шантажу або здійснення інших незаконних дій. Поставлення завдання на розробку нової методі виявлення та слідкування за потенційними кіберпорушниками Вирішення цієї задачі допоможе покращити процеси розслідувань кіберінцидентів у мережі.

2. МЕТОД ВИЯВЛЕННЯ ПОТЕНЦІЙНОГО КІБЕРПОРУШНИКА З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

2.1 Збір даних для розслідування з відкритих джерел.

OSINT або Open-Source Intelligence відіграє вирішальну роль у всіх видах розслідувань. Якщо розслідування означає перехід від запитання до відповіді, OSINT часто можна використовувати для пошуку відповіді. OSINT - це те, що відомо як одне з джерел розвідувальних даних або дисциплін збору розвідувальних даних. Незважаючи на те, що термін «розвідувальна інформація з відкритим кодом» використовується вже більше трьох десятиліть, до цього дня не існує стандартизованого визначення для нього. Іншими словами, OSINT – це розвідувальні дані, зібрані шляхом збору та аналізу загальнодоступної інформації та даних для цілей розслідування. Джерела даних OSINT, зібрані в Інтернеті, можуть охоплювати майже все, що ви можете знайти в Інтернеті, від IP-адреси до публічних державних записів. У широкому розумінні OSINT-збирання може навіть охоплювати виконання пошуку в Google або читання на загальнодоступному форумі про те, як виправити витік труби.

Незважаючи на те, що дані OSINT, зібрані з Інтернету, наразі використовуються в багатьох галузях, що сприяє їх популяризації, існують більш «традиційні» джерела OSINT, такі як друковані книги, газети та журнали, теле- та радіопередачі, фотографії та багато іншого.

Технології OSINT застосовуються різними слідчими та аналітиками в різних галузях — аналітиками операцій з кібербезпеки, правоохоронними органами, розслідувачами шахрайства, мисливцями за загрозами, дослідниками, журналістами-розслідувачами та багатьма іншими.

Це означає, що OSINT можна використовувати для широкого діапазону випадків використання, особливо тих, які покладаються на дослідження в Інтернеті або включають їх. Давайте розглянемо найпоширеніші випадки використання OSINT.

Фахівці з безпеки та етичні хакери використовують OSINT для виявлення потенційних слабких місць у мережі, вразливостей і зовнішніх загроз. Від пошуку невиправленого програмного забезпечення чи незахищених уразливостей Інтернету речей до моніторингу підпільних злочинних балачок, OSINT надає величезну кількість даних та інформації для допомоги в реагуванні на інциденти, усуненні пошкоджень, аналізі загроз, захисті бренду, тестуванні на проникнення, відбитку мережі та інших розслідуваннях .

За даними Statista, у 2020 році понад 3,6 мільярда людей у всьому світі користувалися соціальними мережами, а до 2025 року ще один мільярд стане користувачами соціальних мереж. Велика кількість контенту та інформації, створюваної та поширеної на платформах соціальних мереж, природним чином стала формою розвідки з відкритим кодом:

- Соціальні дії, як-от публікації, фотографії, закріплення місцезнаходження, коментарі та відповіді на запрошення на події;
- Особиста інформація, як-от імена, псевдоніми, дата народження, адреси електронної пошти, історія освіти та кар’єри тощо;
- Міжособистісні зв’язки, такі як друзі, сім’ї, підписники та підписники;
- Тематичні групи, спільноти та членство.

Слідчі можуть прочесати сліди кіберзлочинців у соціальних мережах, щоб виявити потенційних спільників і скласти карту пов’язаної мережі кіберзлочинців. Вони також можуть відстежити дії зниклої людини в соціальних мережах, щоб визначити місцезнаходження зниклої людини востаннє, можливих підозрюваних і спосіб життя жертви.

Фахівці з розслідування шахрайства та спеціалісти з управління ризиками можуть використовувати OSINT для керування та виявлення порушень інтелектуальної власності (ІВ), а також шахрайських, контрафактних і несанкціонованих продуктів, що продаються через Інтернет. Вони також можуть використовувати OSINT для зменшення ризику організації, виявлення потенційних інцидентів збитків і допомоги у відшкодуванні збитків.

Діапазон і глибина OSINT майже безмежні, оскільки його також можна використовувати для інших випадків використання, таких як фішинг , відмивання криптовалюти , належна обачність, глибокі та темні розслідування Інтернету тощо. Усе залежить від того, які OSINT-інструменти та джерела даних ви тримаєте у своїй кишені, а також від того, як ви інтерпретуєте та зв'язуєте інформацію, яку маєте під рукою.

Оскільки обмеження OSINT закінчуються там, де немає доступу до Інтернету, отримати масу даних так само легко, як і загубитися в кролячій норі, або, в деяких випадках, бути приголомшеним морем «шуму» та величезний обсяг інформації.

Оскільки вручну збирати, прочісувати та консолідувати доступну OSINT-інформацію часто потрібно багато часу та енергії, багато OSINT-практиків, експертів, спільнот і компаній розробили різні інструменти та фреймворки для автоматизації або спрощення процесів збору та аналізу даних, або генерувати підібрані звіти розвідки та бази даних. Майже з упевненістю можна сказати, що для кожного типу OSINT-даних існує інструмент або веб-сайт, яким можна скористатися. І це показує OSINT Framework.

Коли ви починаєте досліджувати практики OSINT у своїх розслідуваннях, ви почнете більше чути про термін «OSINT Framework». OSINT Framework – це найбільше сховище інструментів для збору OSINT-інформації та розслідувань. Він сортує ресурси за 32 категоріями залежно від типу даних, які шукають дослідники: публічні записи, соціальні мережі, зображення, відео, цифрова валюта, темна мережа, архіви тощо. У кожній категорії ви можете знайти безкоштовні та платні інструменти, за допомогою яких можна знайти відповідні дані.

Одними з найбільш часто використовуваних інструментів розвідки з відкритим кодом, як не дивно, є пошукові системи, оскільки веб-дослідження є значною частиною OSINT.

Google і Bing, ймовірно, є найбільш використовуваними пошуковими системами, і досвідчені практики OSINT знають про використання розширених функцій пошуку під назвою « Google Dorks », щоб звузити результати пошуку до

певних типів файлів, веб-сайтів, рядків та IP-адрес. Існують також подібні пошукові оператори, « Bing Dorks », для пошукової системи Bing. Однак на цьому сфера пошукових систем не закінчується. Слідчі також використовують менш популярні пошукові системи, такі як Yandex, DuckDuckGo і Baidu, щоб досліджувати більше результатів. Існують також пошукові системи, розроблені для певних доменів, наприклад:

- Метапошукові системи: наприклад, AnswerThePublic.com;
- Пошукові системи коду: наприклад, GitHub або PublicWWW;
- Академічні та публікаційні пошукові системи;
- Пошукові системи новин.

Інструменти аналізу посилань чудово підходять для OSINT-досліджень, оскільки вони розроблені для автоматичного пошуку та візуального відображення зв’язків даних. Хоча деякі джерела даних OSINT, такі як VirusTotal і CipherTrace , також пропонують функцію візуалізації даних, інструменти аналізу посилань йдуть далі. Вони часто інтегруються з кількома джерелами даних і можуть об’єднувати різні дані на одному графіку, таким чином усуваючи проблеми з перемиканням між вкладками та інструментами.

2.2 Узагальнений опис методів та засобів кіберрозслідувань

Хоча методи можуть відрізнятися залежно від типу кіберінциденту, який розслідується, а також від того, хто проводить розслідування, більшість цифрових інцидентів підпадають під деякі загальні методи, які використовуються під час процесу розслідування.

Перевірка минулого : створення та визначення передісторії інциденту за допомогою відомих фактів допоможе встановити відправну точку, щоб визначити, з чим вони стикаються та скільки інформації вони мають під час обробки початкового звіту про інцидент.

Збір інформації: одна з найважливіших речей, яку повинен зробити будь-який дослідник кібербезпеки, це зібрати якомога більше інформації про кіберінцидент. Це була автоматизована атака чи цілеспрямований злочин з боку людини? Чи була якась відкрита можливість для цього нападу? Який обсяг і вплив? Чи може цю атаку здійснити будь-хто або певні люди з певними навичками? Хто потенційні підозрювані? Які цифрові злочини були скоєні? Де можна знайти докази? Чи маємо ми доступ до таких джерел доказів? Ці та інші запитання є цінними міркуваннями під час процесу збору інформації.

Багато національних і федеральних агентств використовують опитування та звіти про спостереження, щоб отримати докази кіберінцидентів. Спостереження включає не лише камери безпеки, відео та фотографії, а й спостереження за електронними пристроями, які детально описують, що використовується і коли, як це використовується, а також усю цифрову поведінку.

Одним із найпоширеніших способів збору даних від кіберінцидентів є налаштування приманки, яка виступатиме в якості жертви, збираючи докази, які пізніше можна буде використовувати проти атак.

Інструменти розслідування кіберінцидентів включають багато утиліт, залежно від технік, які ви використовуєте, і фази, через яку ви проходите. Однак знайте, що більшість із цих інструментів призначені для аналізу даних, коли у вас є докази.

Існують тисячі інструментів для кожного типу кіберінцидентів, тому це не вичерпний список, а короткий огляд деяких із найкращих ресурсів, доступних для виконання криміналістичної діяльності.

SIFT — це колекція інструментів, створена, щоб допомогти групам реагування на інциденти та дослідникам-криміналістам вивчати цифрові криміналістичні дані в кількох системах. Він підтримує різні типи файлових систем, як-от FAT 12/16/32, а також NTFS, HFS+, EXT2/3/4, UFS1/2v, vmdk, swap, RAM dta та дані RAW.

Коли справа доходить до підтримки зображень доказів, вона ідеально працює з файлами окремих необроблених зображень, AFF (Advanced Forensic Format), EWF

(Expert Witness Format, EnCase), AFM (AFF із зовнішніми метаданими) та багатьма іншими.

Серед інших важливих функцій: 64-розрядна базова система Ubuntu LTS 16.04, найновіші інструменти криміналістики, перехресна сумісність між Linux і Microsoft Windows, можливість інсталювати як окрему систему та обширна документація, яка відповідає всім вашим потребам у криміналістиці. Найкраще те, що він є відкритим і абсолютно безкоштовним.

Написаний Браяном Керрієром і відомий як TSK, The Sleuth Kit — це колекція інструментів на базі Unix і Windows з відкритим кодом, яка допомагає дослідникам аналізувати образи дисків і відновлювати файли з цих пристроїв.

Його функції включають повну підтримку синтаксичного аналізу для різних файлових систем, таких як FAT/ExFAT, NTFS, Ext2/3/4, UFS 1/2, HFS, ISO 9660 і YAFFS2, що дає змогу аналізувати майже будь-який образ або диск для Windows-, операційні системи на базі Linux та Unix.

Доступний з командного рядка або використовується як бібліотека, The Sleuth Kit є ідеальним союзником для будь-якої людини, яка цікавиться відновленням даних із файлових систем і необроблених образів дисків.

CAINE — це не проста програма чи пакет для розслідування кіберзлочинів, це повний дистрибутив Linux, який використовується для цифрового криміналістичного аналізу. Він працює з Live CD і може допомогти вам витягнути дані, створені в кількох операційних системах, таких як Linux, Unix і Windows.

Вилучення файлової системи, пам’яті чи мережевих даних CAINE може зробити все це, об’єднавши найкраще програмне забезпечення для експертизи, яке працює як на інтерфейсі командного рядка, так і на основі графічного інтерфейсу.

Він містить такі популярні цифрові програми для розслідування інцидентів, як The Sleuth Kit, Autopsy, Wireshark, PhotoRec, Tinfoleak та багато інших.

PALADIN — це завантажувальний дистрибутив Linux на основі Ubuntu, розроблений SUMURI. PALADIN Toolbox допомагає оптимізувати численні завдання, справді пропонуючи «достаток інструментів» — понад 30+ категорій із понад 100 інструментами, включаючи The Sleuth Kit і Autopsy. Ця справжня

лабораторія на диску доступна як у 64-, так і в 32-бітній версіях, що робить його одним із найпопулярніших пакетів у своєму роді. Використовується правоохоронними, військовими, федеральними, державними та корпоративними агентствами, PALADIN є ідеальним союзником для будь-якого розслідувача комп'ютерних злочинів.

Широко використовуваний у комп'ютерній криміналістиці та реагуванні на інциденти, ProDiscover Forensic має можливості, необхідні для обробки кожного аспекту розслідування. Цей цифровий криміналістичний продукт допомагає швидко й ефективно виявляти файли, збирати, обробляти, захищати й аналізувати дані, а також створювати звіти про докази.

Набір продуктів ProDiscover пропонує слідчим широкий спектр інструментів діагностики та доказів для дослідження доказів і вилучення відповідних артефактів розслідування. Його функції включають широку автоматизацію, хмарну криміналістику, криміналістику пам'яті, попередній перегляд файлів без зміни даних на диску, включаючи метадані, і аналіз даних на рівні сектора.

Відома як DFF, Digital Forensics Framework — це програмне забезпечення з відкритим вихідним кодом для комп'ютерної криміналістики, яке дозволяє фахівцям із цифрової криміналістики виявляти та зберігати системні дії в операційних системах Windows і Linux.

Це дозволяє дослідникам отримувати доступ до локальних і віддалених пристроїв, таких як знімні диски, локальні диски, файлові системи віддаленого сервера, а також реконструювати віртуальні диски VMware. Що стосується файлових систем, він може витягувати дані з FAT12/16/32, EXT 2/3/4 і NTFS як для активних, так і для видалених файлів і каталогів. І навіть допомагає перевіряти та відновлювати дані з карт пам'яті, включаючи мережеві з'єднання, локальні файли та процеси.

Bulk Extractor — одна з найпопулярніших програм, яка використовується для вилучення важливої інформації з даних цифрових доказів. Він працює, витягуючи такі функції, як URL-адреси, адреси електронної пошти, номери кредитних карток і багато іншого з образів дисків ISO і каталогів або просто файлів, включаючи

зображення, відео, офісні та стиснені файли. Це інструмент, який служить не тільки для вилучення даних, але й для аналізу та збору. І однією з його найкращих переваг є широка підтримка майже будь-якої платформи ОС, включаючи Linux, Unix, Mac і Windows, усе без проблем.

Написаний на Perl, цей криміналістичний інструмент, розроблений Філом Харві, є утилітою на основі командного рядка, яка може читати, записувати та маніпулювати метаданими з кількох мультимедійних файлів, таких як зображення та відео. ExifTool підтримує вилучення EXIF із зображень і відео (загальних і спеціальних метаданих), таких як GPS-координати, ескізи зображень, тип файлу, дозволи, розмір файлу, тип камери тощо. Це також дозволяє зберігати результати в текстовому форматі або простому HTML.

Методи розслідування кіберзлочинів передбачають поєднання технічних і нетехнічних методів для збору доказів та ідентифікації підозрюваних. Одним із найважливіших методів розслідування кіберзлочинів є цифрова криміналістика.

Цифрова криміналістика передбачає збір, збереження та аналіз цифрових доказів. Цифрова експертиза може включати відновлення видалених файлів, аналіз метаданих і вивчення журналів мережевого трафіку. Інструменти цифрової криміналістики можуть включати такі програми, як EnCase, FTK і Autopsy.

Окрім цифрової криміналістики, розслідувачі кіберзлочинів можуть використовувати різні інші методи для збору доказів і ідентифікації підозрюваних. Ці методи можуть включати проведення інтерв'ю зі свідками, перегляд записів камер спостереження та аналіз фінансових записів для відстеження потоків грошей.

Слідчі також можуть використовувати методи соціальної інженерії для збору інформації про підозрюваних, наприклад, видавати себе за потенційних жертв або використовувати підроблені профілі в соціальних мережах для отримання доступу до інформації.

Ще один важливий метод, який використовується в розслідуванні кіберзлочинів, це співпраця. У розслідуваннях кіберзлочинів часто беруть участь кілька відомств і організацій, і слідчим важливо працювати разом, щоб обмінюватися інформацією та ресурсами. Це може включати співпрацю з

правоохоронними органами, урядовими установами або приватними компаніями, які спеціалізуються на кібербезпеці. Співпраця може допомогти слідчим виявляти закономірності, відслідковувати підозрюваних і ділитися передовим досвідом.

2.3 Узагальнений опис методу

Методологія розглядається на різних етапах, включаючи збір даних, їх обробку та використання різноманітних алгоритмів для ефективного виявлення кіберпорушників.

Перший етап методу - збір даних - передбачає систематичний збір інформації про канали у соціальних мережах, які відповідають визначеним критеріям для виявлення кіберзагроз. Для досягнення цієї мети використовуються різні техніки, такі як сканування мереж за ключовими словами, використання API соціальних мереж та інструментів моніторингу.

Google надає розширений пошук для покращення ефективності роботи з даними. Функції розширеного пошуку можна використовувати на спеціальній сторінці розширеного пошуку або за допомогою спеціальних слів-операторів, які вводяться в пошуковий рядок.

На сторінці розширеного пошуку Google можна використовувати простий пошук без операторів. Також можна задати формат файлу, який вас цікавить, обмежити пошук на певному сайті або області сайту, вибрати період часу, який вас цікавить. Пошук за словосполученням допомагає знайти конкретну фразу, де ключові слова йдуть підряд. Кавички використовуються для усунення непотрібних посилань, які не пов'язані з вашим запитом. Кавички також допомагають знайти номери телефонів з різними варіантами написання або адреси електронної пошти.

Комплексний пошук без слів допомагає виключити непотрібний результат з пошукової видачі. Це виконується за допомогою оператора мінус перед словом, яке потрібно виключити. Наприклад, якщо ви шукаєте людину за ім'ям і прізвищем і

приблизно знаєте місци проживання, ви можете виключити інші локації і отримати результати без них.

Логічний оператор "або" допомагає економити час і отримувати всі результати, якщо у вас є кілька варіантів написання ключового слова, які треба перевірити. На сторінці пошукової видачі є спеціальне меню, в якому також можна вибрати інструменти пошуку, які є на сторінці розширеного пошуку.

Оператор "site" дозволяє обмежити пошук на певному сайті або доменній зоні, якщо ви цікавитеся лише сайтами певної країни. Також можна шукати в доменній зоні другого рівня, наприклад, тільки на господарських українських сайтах або на конкретному сайті. Можна також шукати в певній частині сайту, скопіювавши його URL-адресу. Використовуючи ці оператори, можна отримати доступ до конкретних документів або інформації, яка зберігається у відкритій частині сервера.

Оператор "file type" допомагає знайти ключові слова не на сторінках, а в файлах певного формату. Наприклад, формату PDF. Якщо додати обмеження пошуку за певним сайтом, можна знайти документи, які зберігаються на відкритій частині сервера Центральної виборчої комісії. Оператор "file type" також можна комбінувати з оператором "site" для обмеження пошуку на українських державних сайтах. Іншими корисними форматами оператора "file type" є файли Excel з електронними таблицями, текстові документи та файли презентацій Microsoft Word (розширення файлу P5). Розширення файлу можна доповнювати та коригувати вручну прямо в рядку пошуку.

Ідентифікатори — це конкретні ключові слова або фрази, унікальні для окремої особи чи компанії. Ці ідентифікатори можуть містити такі речі, як номери телефонів, адреси електронної пошти, реєстраційні номери транспортних засобів або реєстраційні номери в державних базах даних. Використовуючи ці ідентифікатори в онлайн-пошуку, ви можете звузити результати та легше знайти відповідну інформацію.

Якщо у вас є лише номер телефону, ви можете використовувати його для ідентифікації компанії чи особи. Просто використовуйте пошуковий оператор

«лапки» та спробуйте різні варіанти номера телефону. Це допоможе вам знайти відповідну інформацію та ідентифікувати компанію чи особу, пов’язану з цим номером телефону.

Реєстраційні номери можуть бути надійними ідентифікаторами. Наприклад, реєстраційний номер літака, також відомий як бортовий номер, можна використовувати для ідентифікації власника або оператора літака. Використовуючи пошуковий оператор «лапки» з бортовим номером, ви можете знайти інформацію про літак на сайтах і форумах, де любителі авіації діляться своїми фотографіями. Це може допомогти вам дізнатися більше про літак, у тому числі про його оператора.

Адреси електронної пошти також можна використовувати як ідентифікатори в онлайн-пошуку. Якщо адресу електронної пошти було проіндексовано пошуковими системами на інших веб-сайтах і сторінках, ви можете скористатися пошуковим оператором «лапки», щоб знайти більше інформації про особу чи компанію, пов’язану з цією адресою електронної пошти. Це може бути особливо корисним під час пошуку корпоративних адрес електронної пошти, оскільки оператор пошуку «*» можна використовувати для представлення будь-якого символу перед символом «@».

В Україні номер ЄДРПОУ (Єдиний державний реєстр підприємств та організацій України) є корисним ідентифікатором для пошуку інформації про компанії та організації. Якщо ви не знаєте номер ЄДРПОУ, ви можете просто додати до назви організації в пошуковому рядку ключове слово «ЄДРПОУ», а потім знову спробувати пошук з номером ЄДРПОУ в лапках. Це допоможе вам знайти більш конкретну інформацію про компанію чи організацію, яку ви шукаєте.

Основні електронні реєстри України працюють під егідою Міністерства Юстиції та останнім часом стали набагато зручнішими для використання на сайті Міністерства. Їх легко знайти та вибрати для себе необхідну інформацію.

Державний реєстр прав на нерухоме майно містить всю інформацію про нерухомість та її власників в Україні, а також про права на нерухомість та заборони відчужувати власність. Основною метою роботи з ним є встановлення зв'язку між

держслужбовцями та дорогою нерухомістю, яка могла бути придбана корупційним шляхом.

Однак, крім внутрішнього пошуку в соціальних мережах, можна використовувати і пошук Google. Необхідно обмежити пошук Google на цьому сайті та попросити його знайти для вас потрібні ключові слова. Наприклад, профілі людей, на яких присутні словосполучення "адміністрація президента РФ". Також стосується і імені людини, яку ви шукаєте. Скористайтеся кавичками, і Google надасть вам посилання на сторінки в LinkedIn, де фігурує це ім’я. Це можна робити і з усіма іншими соціальними мережами. Недалік полягає в тому, що із-за великого обсягу Google все-таки не бачить велику кількість релевантних повідомлень для кириличної зони соціальних мереж. В цьому випадку в пошуковій роботі дуже пригодяться інструменти Яндекса.

Яндекс.Люди і Яндекс.Поіск по блогам індексують профілі людини по імені та сім'ї одночасно у всіх популярних соціальних мережах. А також дозволяється фільтрувати результати за віком, місцем проживання і так далі. Шукати ключові слова в постах і коментарях зручно через Яндекс.Поіск по блогам. Секрет полягає в тому, щоб відразу ж вибрати розширений пошук, який дає можливість створити фільтр.

Крім того, серед інструментів пошуку Яндекса є багато цікавих операторів, які краще перевірити самостійно. Процес пошуку інформації в соціальних медіа завжди творчий. Необхідно пробувати різні підходи. Однак, окремі секрети все же існують.

Також є можливість створити профіль людини за номером її телефону або URL-адресою адреси у Facebook. Facebook думає, що якщо у вас є номер телефону людини та його електронна адреса, він може надати вам інформацію про нього. Це зручно, якщо ви не знаєте, як саме людина пише своє ім'я.

Один з основних аспектів роботи з пошуком у соціальних мережах - кросплатформений пошук. Багато людей одночасно присутні на кількох соціальних мережах, і в різних соцмережах вони виставляють різну інформацію про себе. Тому завжди бажано виявити всі соціальні профілі людини, які він зареєстрував.

Наприклад, із соціальної мережі ВКонтакте завжди можна отримати дату народження людини, навіть якщо він не вказав її у своєму профілі. Її можна знайти, використовуючи фільтр за датою народження. Велике значення має також URL-адреса конкретного соціального профілю. Чем більш він унікальний, тим більша ймовірність того, що нікнейм, який є його частиною, буде зустрічатися ще. Для цього використовуйте розширений пошук Google за полем URL-адреси.

Додаткову інформацію можуть давати і месенджери, такі як Вайбер і WhatsApp. Досить провести пошук по нікнейму у людини в цих месенджерах або за номером його телефону.

Другий етап методу спрямований на систематичну обробку та документування зібраної інформації з метою ефективного визначення ознак та особливостей кіберпорушників у соціальних мережах. Цей етап включає в себе ряд ключових аспектів, які сприяють відкриттю та аналізу потенційних загроз.

Azure Blob Storage — це рішення Microsoft для зберігання об’єктів у хмарі. Blob Storage оптимізовано для зберігання величезних обсягів неструктурованих даних. Неструктуровані дані – це дані, які не відповідають певній моделі даних або визначенню, наприклад текстові або двійкові дані.

Blob-сховище призначене для:

- Подача зображень або документів безпосередньо в браузер.
- Зберігання файлів для розподіленого доступу.
- Потокове відео та аудіо.
- Запис у файли журналу.
- Зберігання даних для резервного копіювання та відновлення, аварійного відновлення та архівування.
- Зберігання даних для аналізу локальною службою або службою, розміщеною в Azure.

Користувачі або клієнтські програми можуть отримувати доступ до об’єктів у сховищі BLOB через HTTP/HTTPS з будь-якої точки світу. Об’єкти в Blob Storage доступні через REST API Azure Storage , Azure PowerShell , Azure CLI або

клієнтську бібліотеку Azure Storage. Клієнтські бібліотеки доступні для різних мов, зокрема:

- .NET
- Java
- Node.js
- Python

Клієнти також можуть безпечно підключатися до Blob Storage за допомогою протоколу SSH File Transfer Protocol (SFTP) і монтувати контейнери Blob Storage за допомогою протоколу Network File System (NFS) 3.0.

Існує ряд рішень для переміщення наявних даних до сховища BLOB-об’єктів:

- AzCopy — це простий у використанні інструмент командного рядка для Windows і Linux, який копіює дані до та з Blob Storage, між контейнерами або обліковими записами зберігання. Щоб отримати додаткові відомості про AzCopy, перегляньте передачу даних за допомогою AzCopy v10 .
- Бібліотека Azure Storage Data Movement — це бібліотека .NET для переміщення даних між службами Azure Storage. Утиліта AzCopy створена з бібліотекою переміщення даних. Щоб отримати додаткові відомості, перегляньте довідкову документацію для бібліотеки переміщення даних.
- Azure Data Factory підтримує копіювання даних до та з Blob Storage за допомогою ключа облікового запису, спільного підпису доступу, принципала служби або керованих ідентифікаторів для ресурсів Azure. Щоб отримати додаткові відомості, перегляньте статтю Копіювання даних до або з Azure Blob Storage за допомогою Azure Data Factory .
- Blobfuse — це драйвер віртуальної файлової системи для Azure Blob Storage. Ви можете використовувати BlobFuse для доступу до існуючих даних блоку blob у вашому обліковому записі Storage через файлову систему Linux. Для отримання додаткової інформації див. Що таке BlobFuse? - BlobFuse2 (попередній перегляд) .

- Служба Azure Data Box доступна для передачі локальних даних у Blob Storage, коли великі набори даних або мережеві обмеження роблять завантаження даних через мережу нереальним. Залежно від розміру даних ви можете надіслати запит на Azure Data Box Disk , Azure Data Box або Azure Data Box Heavy пристрої від Microsoft. Потім ви можете скопіювати свої дані на ці пристрої та надіслати їх назад до Microsoft для завантаження в Blob Storage.
- Служба імпорту/експорту Azure надає можливість імпортувати або експортувати великі обсяги даних у ваш обліковий запис зберігання та з нього за допомогою наданих вами жорстких дисків.

Після завантаження документів до сховища BLOB-об’єктів можна розпочати третій крок методу. Алгоритми ШІ застосовуються для автоматичного виділення ключових слів, тем та ідентифікації основних патернів у текстовому контенті. Система використовує методи обробки природної мови для ефективного аналізу великої кількості інформації та створення структурованого текстового корпусу.

За допомогою ШІ реалізується автоматична категоризація зібраної інформації на основі визначених тематичних ключових слов. Це дозволяє створювати категорії та маркувати дані, що сприяє покращенню організації та доступності інформації для подальшого аналізу.

2.4 Архтектура та розгортання інструменту ШІ

Щоб визначити потенційних кіберпорушників, на заключному етапі використовується інструмент на основі штучного інтелекту (ШІ), який використовує алгоритми машинного навчання для ідентифікації ознак, що можуть свідчити про потенційну кіберзлочинність. Серед таких ознак можуть бути:

- Частота використання певних веб-сайтів або програм:

Аналіз того, як часто користувач відвідує конкретні веб-ресурси або використовує певні програми, що може вказувати на особливі інтереси чи дії.

- Пошук певної інформації:

  Вивчення запитань і пошукових запитань користувача для виявлення тем та ключових слів, які можуть бути пов'язані з кіберзлочинністю.

- Обмін файлами певного типу:

  Визначення типів файлів, які користувач часто обмінює, і виявлення можливих загроз або небезпек.

- Спілкування з певними людьми:

  Аналіз комунікаційного кругу користувача та виявлення можливих зв'язків з особами, які можуть бути пов'язані із злочинною діяльністю.

Інструмент використовує ці ознаки для побудови моделі, яка може визначати потенційних кіберпорушників. Модель навчається на наборі даних, який включає інформацію про відомих кіберзлочинців.

Зазначаю, що це рішення використовує кілька підходів, які дозволяють побудувати досвід, схожий на ChatGPT, використовуючи шаблон Retrieval Augmented Generation. Воно використовує Azure OpenAI Service для доступу до моделі ChatGPT (gpt-3.5-turbo) та Azure AI Search для індексації та пошуку даних.

Ключові функції цього рішення включають:

- Інтерфейси чату та запитань
- Вивчає різні варіанти, щоб допомогти користувачам оцінити достовірність відповідей за допомогою цитувань, відстеження вихідного вмісту тощо.

- Показує можливі підходи до підготовки даних, швидкої побудови та оркестровки взаємодії між моделлю (ChatGPT) і ретривером (AI Search)
- Налаштування безпосередньо в UX, щоб налаштувати поведінку та експериментувати з параметрами
- Відстеження та моніторинг продуктивності за допомогою Application Insights

Також, важливо відзначити, що це рішення враховує етичні та юридичні аспекти використання ШІ для виявлення потенційних кіберпорушників. Забезпечується конфіденційність та захист особистої інформації користувачів згідно з відповідними законодавчими вимогами.

Розширені можливості цього рішення включають інтерфейси чату та запитань, які сприяють зручній взаємодії з користувачем. Вивчення різних варіантів допомагає користувачам визначити достовірність відповідей за допомогою цитувань та відстеження вихідного вмісту. Засоби навчання на власному датасеті з відомими кіберзлочинцями покращують ефективність моделі та роблять її більш адаптованою до конкретного контексту.

Налаштування у користувацькому інтерфейсі дозволяє адміністраторам та модераторам легко впроваджувати зміни в параметрах та експериментувати з різними конфігураціями для оптимізації результатів. Крім того, важливою частиною рішення є відстеження та моніторинг продуктивності за допомогою Application Insights, що дозволяє стежити за роботою і вчасно реагувати на будь-які аномалії чи відхилення.

Це комплексне рішення покликане сприяти виявленню потенційних кіберпорушників через аналіз їхньої активності та взаємодії в онлайн середовищі, забезпечуючи при цьому високий рівень надійності та захисту приватності користувачів.

Для успішного розгортання інструменту вам необхідно відповідати певним вимогам та мати необхідні ресурси. Ось детальний опис вимог:

- Обліковий запис Azure .
- Підписка на Azure з увімкненим доступом до служби Azure OpenAI . Ви можете подати запит на доступ за допомогою цієї форми . Якщо ваш запит на доступ до служби Azure OpenAI не відповідає критеріям прийнятності , ви можете використовувати натомість загальнодоступний API OpenAI .
- Дозволи облікового запису Azure :
  - Ваш обліковий запис Azure повинен мати такі Microsoft.Authorization/roleAssignments/write дозволи, як «Адміністратор керування доступом на основі ролей» , «Адміністратор доступу користувачів » або «Власник» . Якщо у вас немає дозволів на рівні підписки, вам потрібно надати RBAC для наявної групи ресурсів і розгорнути в цій існуючій групі .
  - Обліковому запису Azure також потрібні Microsoft.Resources/deployments/write дозволи на рівні підписки.

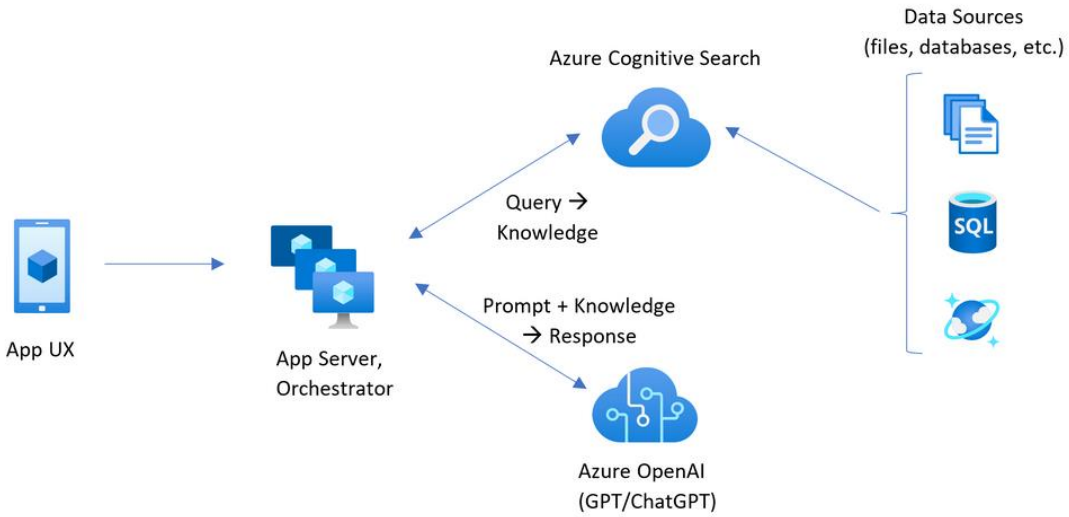


Рисунок 2.1 – Архітектура сервісів Azure

Архітектура (рис 2.1), представлена на зображенні, є хмарної архітектурою, яка використовується для створення інтелектуального пошуку. Ця архітектура складається з наступних компонентів:

- Джерело даних: Цей компонент відповідає за збір даних, які будуть використовуватися для створення інтелектуального пошуку. Джерела даних можуть бути різними, такими як файли, бази даних, веб-сайти або соціальні мережі.
- Індексатор: Цей компонент відповідає за створення індексу даних, який буде використовуватися для пошуку. Індекс містить інформацію про структуру даних, яка буде використовуватися для швидкого пошуку.
- Пошук: Цей компонент відповідає за виконання запитів пошуку. Пошук використовує індекс для пошуку даних, які відповідають запиту.
- Знання: Цей компонент містить додаткові знання, які можуть бути використані для поліпшення результатів пошуку. Знання можуть включати інформацію про домен, такі як тезауруси або словники.
- Запит + Знання: Цей компонент об'єднує запит користувача з додатковими знаннями. Це дозволяє отримати більш релевантні результати пошуку.
- Відповідь: Цей компонент відповідає за надання результатів пошуку користувачеві. Відповідь може бути представлена в різних форматах, таких як текст, графіка або відео.

У представленій архітектурі, інтелектуальний пошук створюється за допомогою хмарної служби Azure Cognitive Search. Ця служба надає всі необхідні

компоненти для створення інтелектуального пошуку, включаючи індексатор, пошук і знання. Azure OpenAI використовується для створення додаткових знань, які можуть бути використані для поліпшення результатів пошуку. Azure OpenAI надає доступ до різних моделей штучного інтелекту, які можуть бути використані для різних цілей, таких як розпізнавання тексту, переклад або генерація тексту. App UX і App Server відповідають за взаємодію з користувачем. App UX відповідає за відображення інтерфейсу користувача, а App Server відповідає за обробку запитів користувача.

Щоб розпочати роботу з проєктом, спочатку требпотрібно переконатись в наявності встановлення всіх необхідних інструментів.

CLI розробника Azure (азд) — це відкрите програмне забезпечення, яке допомагає розробникам створювати, налаштовувати та керувати ресурсами Azure. Цей інструмент надає набори команд, які можна використовувати для виконання різних завдань, таких як:

- Створення та налаштування віртуальних машин
- Створення та налаштування баз даних
- Створення та налаштування веб-сайтів
- Створення та налаштування конвеєрів CI/CD

Python 3.9, 3.10 або 3.11 - це високорівнева мова програмування загального призначення, яка використовується для розробки широкого спектру програм, включаючи веб-додатки, десктопні програми, ігрові програми та наукові розрахунки. Python і менеджер пакунків pip мають бути на шляху в Windows, щоб сценарії налаштування працювали. Також потрібно переконатися, що запускається python –version з консолі. В Ubuntu може знадобитися запустити, sudo apt install python-is-python3щоб створити посилання pythonна python3.

Node.js 14+ - це платформа для розробки веб-додатків і служб, яка заснована на JavaScript. Вона використовує ядро V8 JavaScript, яке забезпечує високу продуктивність і масштабованість. Node.js використовується для розробки широкого спектру веб-додатків, включаючи односторінкові додатки, чат-боти, ігрові сервери та потокові медіа-сервіси. Node.js 14+ є важливою версією, яка включає ряд нових функцій і поліпшень, які можуть зробити розробку веб-додатків більш продуктивною, безпечною і масштабованою.

Git - це розподілена система керування версіями, яка дозволяє відстежувати історію розробки програмного забезпечення і спільно працювати над складними проектами з будь-якої точки світу. Git працює шляхом створення ієрархії каталогів, які називаються репозиторіями. Кожен репозиторій містить історію змін, внесених у код. Ці зміни називаються комітами. Git дозволяє відстежувати зміни в коді, створюючи послідовність комітів. Кожен коміт містить інформацію про дату, час, автора коміту та зміни, внесені в код. Git також дозволяє спільно працювати над проектами, створюючи відгалуження від репозиторію. Відгалуження - це копія репозиторію, яка може бути використана для розробки нових функцій або виправлення помилок.

Powershell 7+ (pwsh) – лише для користувачів Windows. Також важливо переконатись, що запускається pwsh.exe з терміналу PowerShell. Якщо це не вдасться, ймовірно, потрібно оновити PowerShell.

Інтерфейс чату програми є статичною веб-програмою Blazor WebAssembly . Цей інтерфейс — це те, що приймає запити користувачів, направляє запити до серверної частини програми та відображає згенеровані відповіді. Якщо працювати з клієнтськими програмами на мобільних пристроях або комп’ютері, .NET MAUI також буде хорошим варіантом для цього компонента.

- Сервер програми — це мінімальний API ASP.NET Core . Серверна частина містить статичну веб-програму Blazor і те, що організовує взаємодію між різними службами. Послуги, які використовуються в цій програмі, включають:
- Azure Cognitive Search – індексує документи з даних, що зберігаються в обліковому записі Azure Storage. Це робить документи доступними для пошуку.
- Служба Azure OpenAI – надає моделі ChatGPT для створення відповідей. Крім того, Semantic Kernel використовується в поєднанні зі службою Azure OpenAI Service для організації більш складних робочих процесів ШІ.
- Azure Redis Cache – кешує відповіді. Це зменшує затримку під час створення відповідей на схожі запитання та допомагає керувати витратами, оскільки вам не потрібно робити інший запит до служби Azure OpenAI.

Тепер, коли ви знаєте компоненти, з яких складається ця програма, давайте подивимося, як вони працюють разом у контексті чату. Перш ніж почати спілкуватися в чаті зі своїми документами, потрібна мати базу знань, до якої можна зробити запит. Цією базою в нашому випадку буде зібрана за допомогою OSINT методів інформація. У каталозі даних програми розташовуються набори PDF-документів. Щоб завантажити їх у Azure Storage та індексувати в Azure Cognitive Search, створено консольну програму C# (рис 2.2).

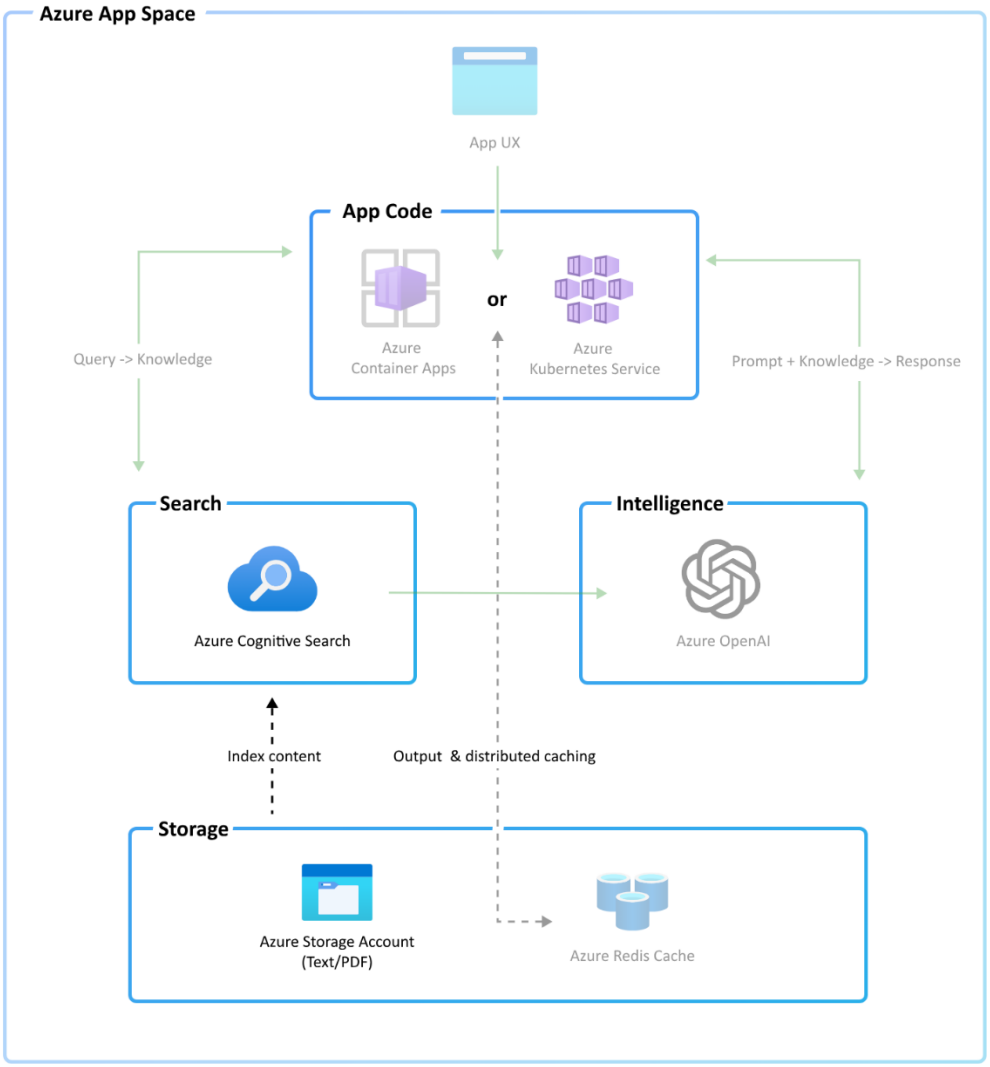


Рисунок 2.2 –Простір сервісів Azure

Консольна програма C# виконує такі дії:

- Використовує Azure Form Recognizer для вилучення тексту з кожного документа.
- Розбиває документи на менші уривки. (нарізка)
- Створює новий документ PDF для кожного з уривків.
- Завантажує уривок до облікового запису сховища Azure.
- Створює індекс у Azure Cognitive Search.
- Додає документи до індексу когнітивного пошуку Azure.

Запит до бази знань починається з того, що користувач вводить запитання у веб-програмі Blazor. Потім запит користувача направляється до ASP.NET Core Minimal Web API (рис 2.3).

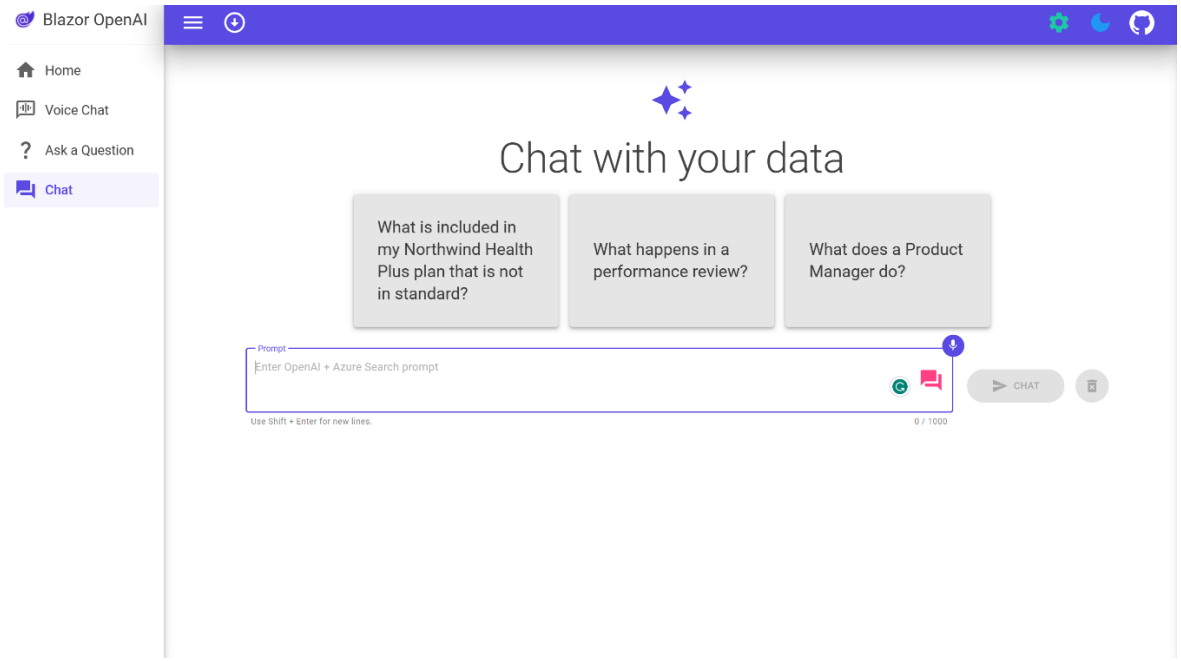


Рисунок 2.2 – Веб інтерфейс користувача

Всередині веб-інтерфейсу API chat кінцева точка обробляє запит:

api.MapPost("chat", OnPostChatAsync);

Щоб обробити запит, використовується шаблон, відомий як Retrieval Augmented Generation, який робить наступне:

- Запитує в базі знань відповідні документи
- Використовує відповідні документи як контекст для створення відповіді

База знань запитується за допомогою когнітивного пошуку Azure. Хоча когнітивний пошук Azure не розуміє природну мову, надану користувачем. Щоб це виправити потрібно використовувати ChatGPT, щоб допомогти перекласти природну мову в запит. Використовуючи Semantic Kernel, створено метод, який

визначає шаблон запиту та додає історію чату та запитання користувача як додатковий контекст для створення запиту Azure Cognitive Search.

```
private ISKFunction CreateQueryPromptFunction(ChatTurn[] history)
{
    var queryPromptTemplate = """
        Below is a history of the conversation so far, and a new question asked by the user that needs to be answered by searching in a knowledge base.
        Generate a search query based on the conversation and the new question.
        Do not include cited source filenames and document names e.g info.txt or doc.pdf in the search query terms.
        Do not include any text inside [] or <<>> in the search query terms.
        If the question is not in English, translate the question to English before generating the search query.
        Chat History:
        {{$chat_history}}
        Question:
        {{$question}}
        Search query:
        """;
    return _kernel.CreateSemanticFunction(queryPromptTemplate,
        temperature: 0,
        maxTokens: 32,
        stopSequences: new[] { "\n" });
}
```

Потім цей метод використовується для створення підказки для створення запиту.

```
var queryFunction = CreateQueryPromptFunction(history);
```

```
var context = new ContextVariables();
context["chat_history"] = history.GetChatHistoryAsText();
context["question"] = userQuestion;
```

Коли запускається функція семантичного ядра, вона надає складену підказку моделі Azure OpenAI Service ChatGPT, яка генерує запит..

```
var query = await _kernel.RunAsync(context, cancellationToken, queryFunction);
```

Після створення запиту скористаємось клієнтом Azure Cognitive Search, щоб зробити запит індексу, що містить документи.

```
var documentContents = await _searchClient.QueryDocumentsAsync(query.Result, overrides, cancellationToken);
```

Приклади в підказці слугують вказівками для моделі для створення відповіді. Це відоме, як кількакратне навчання.

```
private ISKFunction CreateAnswerPromptFunction(string answerTemplate, RequestOverrides? overrides) =>
    _kernel.CreateSemanticFunction(answerTemplate,
        temperature: overrides?.Temperature ?? 0.7,
        maxTokens: 1024,
        stopSequences: new[] { "<|im_end|>", "<|im_start|>" });
ISKFunction answerFunction;
var answerContext = new ContextVariables();
answerContext["chat_history"] = history.GetChatHistoryAsText();
answerContext["sources"] = documentContents;
```

```
answerContext["follow_up_questions_prompt"] = ReadRetrieveReadChatService.FollowUpQuestionsPrompt;
answerFunction = CreateAnswerPromptFunction(ReadRetrieveReadChatService.AnswerPromptTemplate, overrides);
prompt = ReadRetrieveReadChatService.AnswerPromptTemplate;
```

Коли запускається функція семантичного ядра, вона надає скомпоновану підказку для моделі Azure OpenAI Service ChatGPT, яка генерує відповідь.

```
var ans = await _kernel.RunAsync(answerContext, cancellationToken, answerFunction);
```

Після деякого форматування відповідь повертається до веб-програми та відображається. Щоб підвищити довіру до відповідей, відповідь включає цитати, повну підказку, яка використовується для створення відповіді, і допоміжний вміст, що містить документи з результатів пошуку.

3. ЕКСПЕРИМЕНТАЛЬНА ПЕРЕВІРКА МЕТОДУ

3.1Пошук інформації за деталями електронного листа

Яскравим прикладом може слугувати така подія, як отримання листа на електрону скриньку із прикріпленим файлом, де прикріпленим файлом виступає архів із шкідливим програмним забезпеченням. При розархівуванні здійснює 34 збирання заданих йому файлів та передає на сторонній сервер. На даний час такі випадки не є поодинокими. Відправниками таких листів можуть бути як новачки, які тільки пробують та тестують такі засоби, так і особи, які бажають здійснити хакерську атаку на організацію та заволодіти її даними.

Відправною точкою для розслідування такого типу інциденту слід вважати адресу електронної скриньки відправника та Ip-адресу відправника. Використовую методи OSINT можна перевірити чи адреси електронної скриньки немає у спам базах та можливих власників електронної адреси. Так, використовуючи інструменти, які були раніше згадані в роботі можна прослідкувати чи електронна адреса відправника незареєстрованна на вебресурсах, та чи не використовувалася для реєстрації у соціальних мережах.

Скачавши лист на свій персональний комп'ютер та відкривши його у текстовому редакторі, можна побачити Ip-адресу відправника або сервісу через який здійснювалась пересилки (рис 3.1).

Рисунок 3.1 – Приклад відкритого листа

Для відкриття листа було використано програмне забезпечення “Notepad++”. У 27 рядку файлу листа, що рис. 3.1 можна замітити Ip-адресу сервісу відправника: 192.174.84.252.

Використавши інструмент “whois”, а точніше скориставшись веб-ресурсом “https://whoer.net/ru/checkwhois” ми можемо дізнатися інформацію про хостинг-провайдера, який надає послуги по цьому Ip-адресу. На (рис 3.2) ми спостерігаємо, що інформація про відправника зберігатися фізично у компанії “SparkPost”, яка розміщує свої сервери на території Сполучених Штатів Америки у Штаті Огáйо (англ. Ohio), місто Дублін, індекс міста 43017.

Рисунок 3.2 – Інформація про відправника

Таким чином, використавши, тільки методи та інструменти OSINT ми дізналися через який сервіс здійснювалась розсилка повідомлення та де зберігається інформація про відправника. Зібрана інформація в подальшому, звісно, якщо ми будемо звертатися до правоохоронних органів, пришвидшить розслідування справити та дасть можливість оперативного реагування на такий випадок.

Так, не беручи до уваги те, що до повідомлення було прикріплений файл табез його аналізу, ми дізналися багато інформації від якої можна відштовхнутися

при дослідженні. Звісно, без детального аналізу файлу та принципу його дії не можна скласти повної картини кіберінциденту.

3.2 Пошук інформації по url адресі

Отримання посилання на фішинг веб-ресурс, як кіберінцидент, характеризується самим посиланням. Тобто ми маємо url від якої будемо відштовхуватися не беручу до уваги джерело отримання такого посилання. Найпопулярнішим фішинг посиланням в Україні можна рахувати це посилання на “OLX доставку” або самий веб-ресурс. Для дослідження ми будемо використовувати реальне фішинг посилання “https://olx.ua-pocchta.xyz/delivery.php?pay=1&q=4624029673”, яке було використане для отримання грошей від продавця. Вигляд веб-ресурс мав такий, як на (рис 3.3). Серед то, за що ми можемо зачепитися при розслідуванні такого типу кіберінциденту, насамперед, так це url посилання. Оскільки реквізити отримувача є вигаданими та не має змісту їх перевіряти. Тільки в кінці такого розслідування для повноти інформації можливо здійснити таку перевірку.

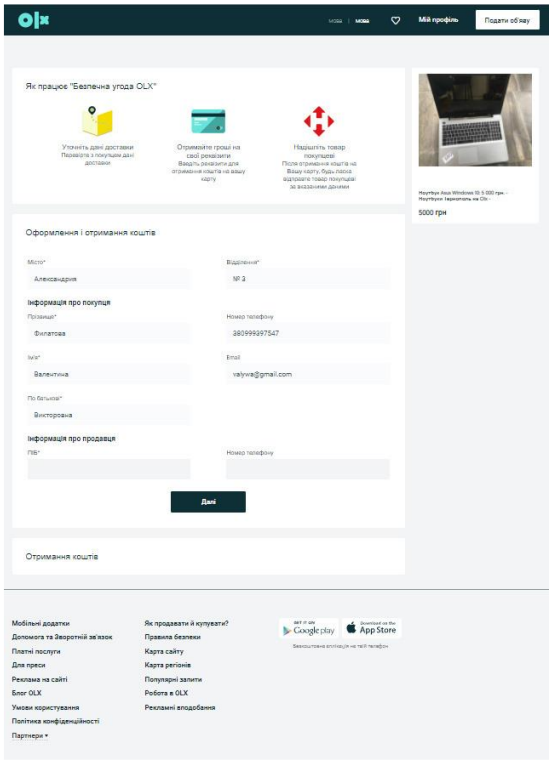


Рисунок 3.3 – Фішинг посилання

Тому, для початку скористаємося веб-ресурсом ”https://www.whoer.net/checkwhois” для перевірки фізичного розташування інформації про веб-ресурс. Із (рис 3.4) ми бачимо, що даний фішинговий сайт має Ip-адресу 135.125.21.210, що належить діапазону Ip-адрес, які обслугову cloud.4host.su, який в свою чергу орендує сервери в “OVH SAS”, яка є французькою компанією та фізично розміщення серверів має у Франції.

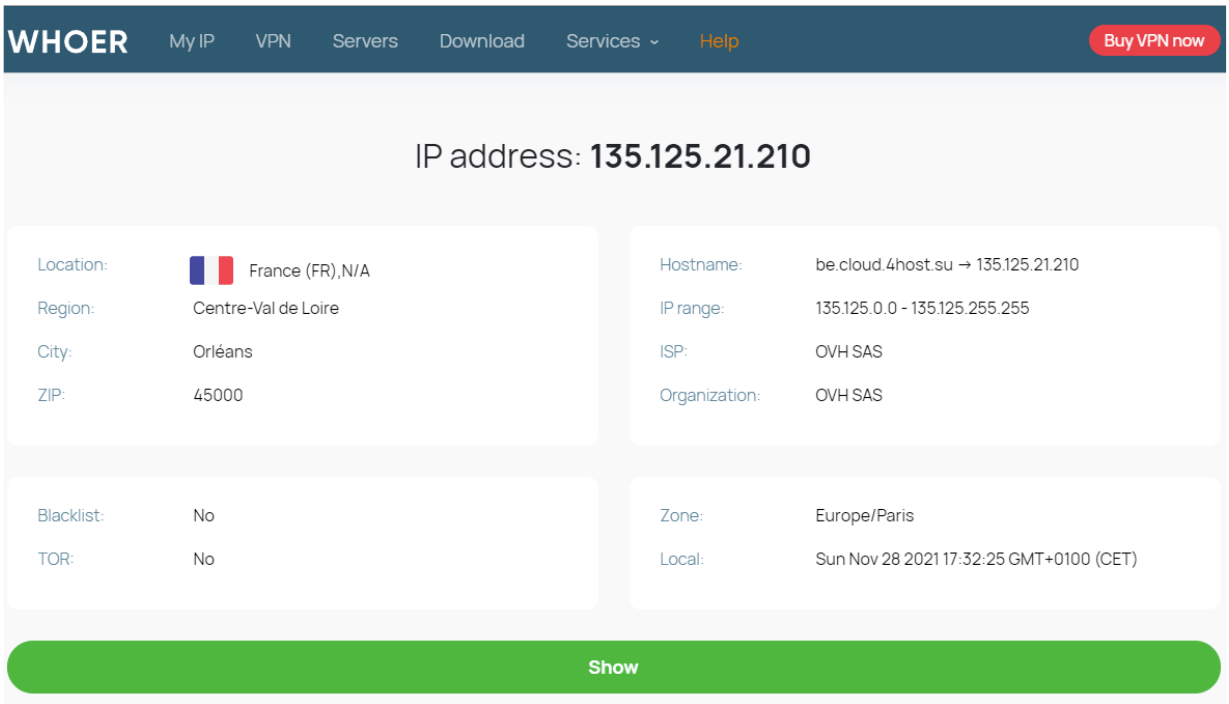


Рисунок 3.3 – Адреса фішингового сайту

3.3 Пошук інформації за адресою крипто-гаманця

При розслідувані кіберінцидента, в якому фігурує крипто гаманець можливо здійснити ідентифікацію особи власника гаманця. Засоби OSINT дозволяють здійснити аналіз інформації по крипто гаманцю. Крім цього, технологія Блокчейн дозволяє всім бажаючим переглянути стан гаманця та транзакції, які відбувалися із його використанням, знаючи лише адресу гаманця. Технології OSINT дозволяють більш комплексно підійти до питання пошуку такої інформації. Данні про власника крипто-гаманця стали не виключенням. Один із інструментів OSINT для здійснення пошуку інформації є Maltego, який був раніше згаданий в

роботі, дає змогу здійснювати аналіз крипто-гаманців та встановлювати зв'язки між ними, як це показано на (рис 3.4) та (рис 3.5).

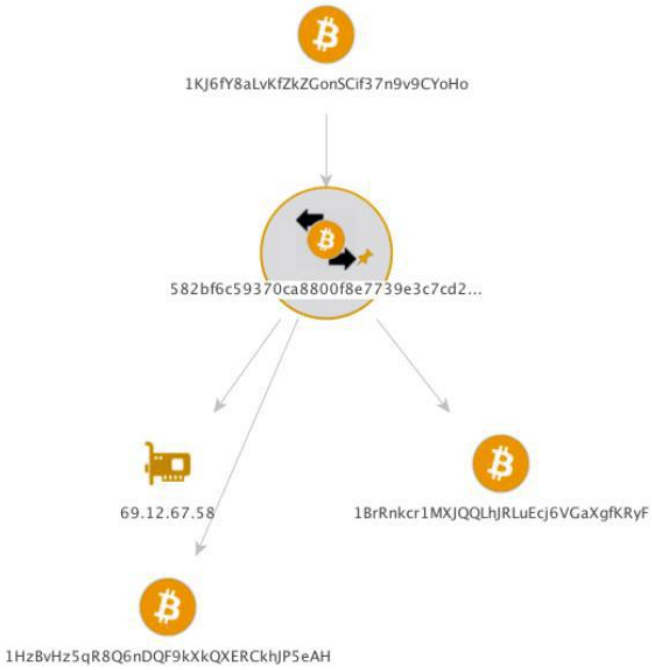


Рисунок 3.4 – Зв’язки криптогаманців

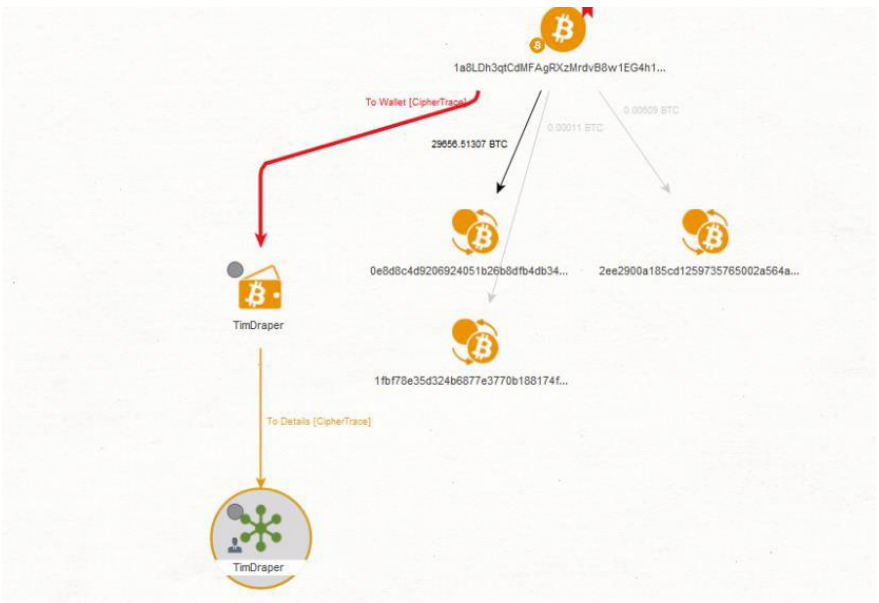


Рисунок 3.5 – Зв’язки криптогаманців

Крім цього, можна спробувати здійснити пошук гаманця у пошукових системах, типу Google, Yandex, Bing, Boardreader тощо. Нерідко буває так що такий гаманець міг вказуватися у реквізитах на одному із форумів у мережі Інтернет. Оскільки пошукові системи можуть індексувати такі сторінки, навіть якщо це так званий “хакерський форум”.

Також існує безліч веб-ресурсів для пошуку по крипто-гаманцях. Із найвідоміших це: “blockchain.com/explorer”, "blockchair.com/”, “etherchain.org”, "etherscan.io".

Технологій OSINT через їх різновидність та не шаблонність при пошуку інформації, які дають можливість підійти до питання із різних сторін, що в комплексі із іншими методами та способами розслідування дасть повну та об'єктивну інформацію про інцидент.

3.4 Імплементація засобів OSINT в СУІБ

Інформаційна безпека залежить від того, наскільки добре система може реагувати на виклики та загрози. При цьому все більшого значення набуває аналіз зовнішнього та внутрішнього середовища безпеки. Врахування взаємозалежності та мережевості цих базових компонентів безпеки створює передумови для успішного вирішення проблеми захисту інтересів.

Розвідка з відкритим кодом (OSINT) є однією з дисциплін розвідки. Включає пошук, відбір і збір данних з загальнодоступних джерел та їх аналіз. У розвідувальному співтоваристві термін «відкритий» відноситься до загальнодоступного джерела (на відміну від засекречених джерел та джерел обмеженого використання), він не відноситься до концепції відкритого джерела чи публічної розвідки.

Збір розвідувальноих данних в OSINT суттєво відрізняється від інших видів розвідувальних методів збору інформації. Основною проблемою роботи з розвідувальними методами є отримання інформації з джерела, який завжди

співпрацює. Основне завдання OSINT — знайти змістовні та надійні джерела з величезної кількості різноманітної інформації у кіберпросторі.

Отже, повернемось до суті методу (рис 3.6), вона полягає в наступному: для отримання необхідної інформації про проблему необхідно сформувати якнайбільше питань, згрупувати питання за характеристиками, встановити взаємозв'язки між групами та окремими проблемами, шукати інформацію з кожної проблеми, аналізувати джерела інформації. для об'єктивності, новизни, достовірності і т. д. відбирати найкращі джерела, систематизувати та упорядкувати інформацію.

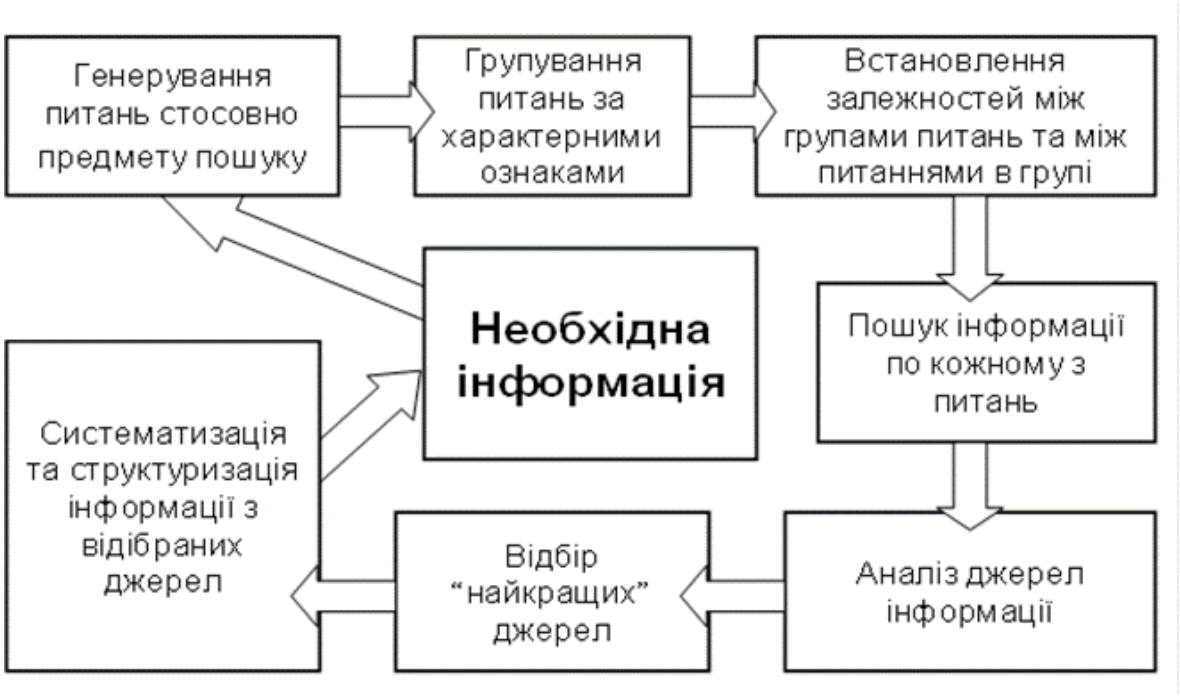


Рисунок 3.6 – Блок схема методу

Донедавна ринок пропонував велику кількість програмних продуктів для автоматизації етапів життєвого циклу системи управління інформаційними ризиками (СУІБ), всі вони роз'єднані, мають різні формати уявлення, використовують різні методології управління ризиками, оцінки безпеки інформаційних систем, ієрархію та класифікацію ресурсів. на основі різних джерел баз загроз і вразливостей та ін. У цьому контексті впровадження єдиного

автоматизованого інструменту є найбільш перспективним для реалізації системного підходу до управління інформаційними ризиками (IP).

Для створення єдиного автоматизованого засобу СУІБ спочатку необхідно визначити основні напрямки автоматизації процесів управління інформаційною безпекою на всіх фазах циклу управління: планування, впровадження, перевірка, удосконалення стандартів серії ДСТУ. Процес планування повинен включати наступні етапи:

- Визначте перелік інформаційних ресурсів підприємства. Автоматизований інструмент допомагає зберегти дані про інформаційні ресурси та їх зміни, а також може спростити процес збору даних.
- Оцінка критичності інформації. Тут автоматизований інструмент може зберігати лише дані опитування.
- Оцінка безпеки інформаційних ресурсів. Інтеграція з базами даних про вразливості та інтегрованими базами даних загроз допомагає оптимізувати цей процес і забезпечити його повноту.

Також можлива інтеграція з різними сканерами уразливостей.

- Виявлення інформаційних ризиків. Вбудоване алгоритмічне рішення розраховує інформаційні ризики на основі введених даних. Результат виводиться у вигляді звіту.
- Обрання стратегії управління ризиками, визначення способів зниження ризиків. За допомогою автоматизованої технології ви можете гнучко та зручно моделювати різні варіанти реалізації захисту, оцінювати ефективність запланованих засобів та вибирати найкращу стратегію захисту.

Впровадження процедур IMS для підвищення безпеки включає їх впровадження в організаційні процеси. У цьому випадку автоматизований інструмент може збирати інформацію, спілкуватися між фахівцями IP і брати на себе роль планувальника завдань.

На цьому етапі основним завданням автоматизованого інструменту є збереження документів СУІР:

- нормативні документи (методичні вказівки, положення, інструкції);
- записи, що підтверджують виконання існуючих процедур в організації.

Це означає, що вся вимірювальна документація може зберігатися в центральному місці та надаватися зацікавленим сторонам (наприклад, внутрішнім або зовнішнім аудиторам) своєчасно, якщо це необхідно.

Огляд функціонування процесів ЦРТ необхідний для того, щоб переконатися, що вони працюють належним чином та ефективно, або, у разі невідповідності, щоб визначити, які покращення необхідні. Наприклад, на цьому етапі автоматизований інструмент може виконувати такі ролі:

Статистика та аналіз подій. Аналіз подій є основним критерієм ефективності та адекватності інформаційної безпеки організації, а також ефективності ЗУІБ загалом. Заходи щодо покращення відновлювальних заходів визначаються на основі інформації про інциденти.

Автоматизований інструмент може структуровано зберігати інформацію про всі ІР-інциденти, збирати їх статистику за різними параметрами та позначати об’єкти, які часто записуються як об’єкти інцидентів.

Збірник метрик для оцінки ефективності ІС. Результати та частота інцидентів інформаційної безпеки – найбільш очевидні метрики для оцінки її ефективності.

З іншого боку, автоматизований інструмент може здійснювати аналіз, таких данних, як вразливості, ефективність реалізованих заходів протидії, перелік ІР тощо.

На базі отриманих та проаналізованих метрик оцінки ефективності визначають подальші дії та складання плану їх реалізації. Зазвичай, коригувальні дії - це зміна процедур, документів, нових засобів захисту, тобто зміни у самій організації. Автоматизований інструмент допомагає відображати результати, зберігати дані та відстежувати зміни у захищеності інформаційних ресурсів укінці заключного етапу, весь прогрес повертається до етапу планування та циклічно

повторюється впродовж усього життєвого циклу системи управління інтелектуальною власністю.

Назви компаній і продуктів можуть з’являтися в Інтернеті мільйони разів на день. Організації можуть застосовувати більш активний підхід до управління ризиками бренду, впроваджуючи передові методи OSINT для оцінки глобальної репутації бренду.

Захист подій та місця проведення: шкідливі дії та дії не тільки можуть завдати фізичної шкоди відвідувачам, але й можуть завдати шкоди іміджу бренду в довгостроковій перспективі. Використання методів OSINT дає змогу брати участь у розвідувальних зусиллях для покращення безпеки подій і місць проведення до, під час і після подій. Це забезпечує безпечний досвід для клієнтів і зацікавлених сторін шляхом визначення потенційних загроз, надання уявлень про осіб або групи інтересів, а також моніторинг інших типів загроз, як-от кібератаки або небезпечні прогнози.

Настрої ринку: маркетингові групи хочуть знати, що говорять про їхній бренд в Інтернеті, особливо тому, що майже всі кампанії покладаються на розуміння цільових ринків. Методи OSINT дозволяють цим командам зрозуміти сприйняття клієнтів і ключових зацікавлених сторін шляхом послідовного моніторингу джерел PAI, щоб визначити відповідні розмови та зрозуміти їх вплив.

Зв’язки з громадськістю: подібно до розуміння настроїв ринку, менеджери зі зв’язків з громадськістю повинні добре уявляти, що говорять про їхню компанію та хто це говорить. Впровадження методів OSINT допомагає випереджати виникаючі PR-ситуації, щоб планувати потенційні сценарії, визначати відповідні розмови різними мовами, відстежувати методи OSINT, щоб отримати огляд на 360°, щоб швидко визначити проблеми, визначити належну відповідь і прийняти прямо наступний крок.

Кіберзагрози поширені в кожній галузі. Використання методів OSINT дає командам із кібербезпеки ще один спосіб попередити загрози як всередині, так і поза межами свого брандмауера.

Виявлення внутрішніх загроз: ні для кого не секрет, що корпоративні інсайдери становлять потенційну загрозу безпеці бізнесу. Впровадження методів OSINT надає вашій команді безпеки інструменти, необхідні для сповіщення про потенційно підозрілу поведінку. Рішення OSINT також забезпечують постійну пильність і постійний моніторинг, необхідні для виявлення цих загроз.

Захист ІТ-Компанії, які залежать від своїх патентів і торгових марок, повинні знати про потенційний витік ІВ в Інтернеті – особливо в глобальній електронній комерції. Методи OSINT дають підприємствам глибоке уявлення про можливу крадіжку ІР. Копання в РАІ може виявити місце крадіжки, джерело підроблених товарів, а також підприємства можуть вжити заходів, необхідних для пом’якшення втрат, притаманних крадіжці ІР.

Запобігання шахрайству: підроблені товари не тільки впливають на цінність бренду та прибуток, але й можуть мати негативний вплив на здоров’я населення залежно від продукту. Технології OSINT допомагають підприємствам впроваджувати моніторинг боротьби з шахрайством за допомогою інструментів для постійного міжмовного моніторингу незаконних веб-сайтів і ринків, точного визначення місцезнаходження виробників, відстеження грошових слідів тощо.

Деякі види загроз виходять за межі внутрішніх процесів і в глобальні операції. Безпека та здоров’я ключових працівників можуть бути під загрозою залежно від типу загроз. Використання методів OSINT допомагає підприємствам залишатися попереду потенційних операційних ризиків і пом’якшувати їх вплив.

Безперервність бізнесу: на безперервність бізнес-операцій можуть вплинути різноманітні природні та техногенні катастрофи. Ці катастрофи можуть легко вивести підприємства з ладу без належних запобіжних заходів. Методи OSINT дозволяють командам використовувати інформацію з надійних глобальних джерел для покращення обізнаності та прозорості ситуації. Безпека критичної інфраструктури: Критична інфраструктура підтримує підприємства та країни; тому розуміння будь-яких потенційних збоїв є критичним. Методи OSINT забезпечують систему раннього попередження, щоб передбачити та пом’якшити ризики, які можуть вплинути на інфраструктуру.

Захист керівників і співробітників: забезпечення безпеки всіх співробітників є головним пріоритетом для бізнесу. Методи OSINT покращують уявлення про потенційні загрози, щоб можна було виявити ранні попереджувальні ознаки ризику та вжити відповідних заходів.

Оскільки загрози стають все більш складними та різноманітними, збір розвідувальних даних має адаптуватися до ландшафту, що розвивається. Здатність штучного інтелекту виявляти аномалії та тонкі закономірності в даних матиме вирішальне значення для виявлення потенційних загроз, будь то кібербезпека, кримінальна діяльність чи навіть глобальні надзвичайні ситуації. Виявлення загроз у режимі реального часу та реагування на них будуть посилені швидкістю та точністю ШІ.

Замість того, щоб замінити людей-аналітиків, ШІ розширить їхні можливості. Інструменти штучного інтелекту допомагатимуть аналітикам, автоматизуючи повторювані завдання, забезпечуючи контекстно-насичену візуалізацію даних і пропонуючи шляхи для подальшого дослідження. Цей спільний підхід дозволить використати сильні сторони як людей, так і машин, що призведе до більш повних і глибоких розвідувальних звітів.

Майбутнє збору розвідданих також вимагає ретельного розгляду етичних наслідків. Оскільки системи штучного інтелекту стають більш здатними агрегувати та аналізувати персональні дані, досягнення балансу між безпекою та конфіденційністю стане першорядним. Забезпечення прозорої та підзвітної практики матиме вирішальне значення для підтримки громадської довіри та захисту прав особи.

Збір розвідданих часто включає дані з безлічі джерел — від соціальних мереж до супутникових зображень. Системи, керовані штучним інтелектом, будуть чудовими в інтеграції та об’єднанні різноманітних наборів даних, забезпечуючи цілісне уявлення про складні ситуації. Такий інтегрований підхід зменшить розрив інформації та підвищить точність оцінок розвідки.

Майбутній ландшафт розвідки характеризуватиметься посиленою співпрацею між різними секторами та агентствами. Платформи з підтримкою

штучного інтелекту сприятимуть обміну даними та інформацією, дозволяючи урядам, організаціям і установам об’єднувати свої колективні ідеї для більш повного аналізу розвідувальних даних.

Хоча ШІ сприятиме ефективності та автоматизації, людський дотик залишається незамінним у зборі розвідувальної інформації. Критичне мислення, розуміння контексту та нюансована інтерпретація – це навички, які машини не можуть відтворити. Майбутні спеціалісти з розвідки зосередяться на аналізі вищого рівня, використовуючи результати штучного інтелекту як цінні вхідні дані.

Майбутнє збору розвідданих є захоплюючим і трансформуючим. Можливості ШІ в обробці даних, розпізнаванні образів і прогнозному аналізі підвищать ефективність зусиль розвідки. Однак етичні міркування, співпраця та збереження людського досвіду залишатимуться на передньому плані. Коли ми впроваджуємо ці досягнення, синергія між ШІ та людським інтелектом сформує нову еру обґрунтованого прийняття рішень і стратегічного планування.

Перш ніж ми заглибимося в трансформаційну роль штучного інтелекту, давайте спершу дамо чітке розуміння Open Source Intelligence. OSINT означає процес збору, аналізу та використання інформації із загальнодоступних джерел, таких як веб-сайти, соціальні медіа-платформи, новинні статті тощо. Це важливий компонент сучасної розвідувальної роботи, який надає цінну інформацію для широкого спектру додатків, від кібербезпеки до бізнес-аналітики.

Поєднання штучного інтелекту та OSINT - це більше, ніж сума його частин. Симбіотичний зв’язок між цими двома сферами підсилює їхні сильні сторони, що призводить до комплексного процесу збору розвідувальних даних. Оскільки ШІ продовжує розвиватися, ось як він покращує середовище OSINT:

- Здатність штучного інтелекту аналізувати дані без людської упередженості призводить до підвищення точності та зменшення помилок. Аналітики можуть бути впевнені, що інформація, з якою вони працюють, є надійною, що дозволяє їм приймати обґрунтовані рішення.

- У швидкоплинному світі інтелекту своєчасність має вирішальне значення. Швидкість штучного інтелекту в обробці даних означає, що розуміння можна генерувати в режимі реального часу, що дає аналітикам перевагу в миттєвому реагуванні на виникаючі ситуації.
- Передбачувані можливості штучного інтелекту є благом для роботи розвідки. Виявляючи тенденції та екстраполюючи майбутні сценарії, аналітики можуть активно розглядати потенційні загрози та можливості, сприяючи стратегічному плануванню.

Штучний інтелект більше не є футуристичною концепцією, що обмежується науковою фантастикою; це відчутна реальність, яка змінює визначення всіх галузей. У сфері OSINT штучний інтелект надає незрівнянні переваги, які підвищують ефективність і точність вилучення інформації. Ось як AI трансформує OSINT:

- ШІ може швидко просіювати величезні обсяги даних із різноманітних джерел. Це стосується не лише тексту, а й зображень, відео та інших типів медіа. Це дозволяє аналітикам ефективно збирати інформацію з різних платформ і мов. Однією з найвидатніших переваг ШІ в OSINT є його здатність обробляти величезні обсяги даних за лічені хвилини. Традиційні ручні методи збору й аналізу даних бліднуть у порівнянні з майстерністю ШІ в обробці великих даних. Алгоритми штучного інтелекту можуть швидко сканувати численні веб-сайти, соціальні медіа-платформи, форуми та новинні статті, щоб зібрати відповідну інформацію — завдання, на виконання якого аналітикам-людинам потрібні години або навіть дні.
- Алгоритми штучного інтелекту створені для визначення закономірностей і зв’язків у даних, які аналітикам може бути складно помітити. Ці моделі можуть надати важливу інформацію про тенденції, взаємозв’язки та потенційні загрози. Здатність штучного інтелекту розпізнавати складні візерунки змінює правила гри в OSINT. Навчаючи моделі штучного інтелекту

на різноманітних наборах даних, аналітики можуть розробляти інструменти, які визначають тонкі зв'язки між фрагментами інформації. Це дозволяє глибше зрозуміти контексти, потенційні загрози та нові тенденції, які інакше могли б залишитися прихованими.

- NLP дозволяє системам ШІ розуміти та обробляти людську мову. Це важливо для таких завдань, як аналіз настроїв, розпізнавання об'єктів і узагальнення текстового вмісту з таких джерел, як соціальні мережі та новинні статті. Обробка природної мови — це підполе ШІ, яке дозволяє машинам розуміти, інтерпретувати та генерувати людську мову. В OSINT НЛП відіграє ключову роль у аналізі настроїв, вилученні ключових сутностей із тексту та навіть підсумовуванні довгих статей. Цей рівень лінгвістичного аналізу забезпечує цілісне уявлення про суспільні настрої та думки, що є цінним для прийняття обґрунтованих рішень.
- AI може автоматизувати завдання, які потребують багато часу та повторюються, наприклад моніторинг змін на веб-сайтах, відстеження розмов у соціальних мережах і створення звітів. Це звільняє людей-аналітиків, щоб зосередитися на більш складних аналітичних завданнях. Наприклад, штучний інтелект можна запрограмувати на відстеження змін на веб-сайтах, стеження за розмовами в соціальних мережах і складання вичерпних звітів — і все це в режимі реального часу. Ця нова ефективність дозволяє аналітикам зосередитися на завданнях вищого рівня, які потребують когнітивного мислення та аналізу.

Підводячи підсумок, можна сказати, що інтеграція штучного інтелекту в сферу інтелекту з відкритим кодом є зміною парадигми, яку не можна ігнорувати. Швидка й точна обробка інформації в поєднанні зі здатністю ШІ виявляти приховані закономірності робить його незамінним інструментом як для аналітиків, так і для дослідників. Оскільки ми орієнтуємося в постійно мінливий ландшафт інформаційних війн і цифрових складнощів, використання потенціалу штучного інтелекту в OSINT буде ключем до того, щоб залишатися попереду.

4 ЕКОНОМІЧНА ЧАСТИНА

Виконання наукових досліджень завжди передбачає отримання конкретних результатів і вимагає відповідних витрат. Отримані результати надають нові знання, які можуть бути застосовані для вдосконалення і/або розробки нових, більш продуктивних зразків техніки, процесів та програмного забезпечення.

Дослідження на тему "Метод виявлення потенційного кіберпорушника з використанням штучного інтелекту" відноситься до фундаментальних і дослідницьких наукових досліджень, спрямованих на вирішення наукових проблем, пов'язаних з практичним використанням. Основою таких досліджень є науковий ефект, що виражається у отриманні наукових результатів, які розширюють обсяг знань про природу, техніку та суспільство, розвивають теоретичну базу у відповідному науковому напрямку та виявляють нові закономірності, придатні для практичного використання.

Для виконання цієї роботи ми розглянемо такі етапи:

1. Здійснимо науковий аудит досліджень для визначення їх наукового рівня та значущості.
2. Розробимо план витрат на проведення наукових досліджень.

4.1 Оцінювання наукового ефекту

Основними ознаками наукового ефекту науково-дослідної роботи є новизна роботи, рівень її теоретичного опрацювання, перспективність, рівень розповсюдження результатів, можливість реалізації. Науковий ефект НДР на тему «Метод виявлення потенційного кіберпорушника з використанням штучного інтелекту» можна охарактеризувати двома показниками: ступенем наукової новизни та рівнем теоретичного опрацювання.

Таблиця 4.1 – Показники ступеня новизни науково-дослідної роботи виставлені експертами

Ступінь новизни	Характеристика ступеня новизни	Значення ступеня новизни, бали		
		Експерти (ПІБ, посада)		
		1	2	3
Принципово нова	Робота якісно нова за постановкою задачі іґрунтується на застосуванні оригінальних методів дослідження. Результати дослідження відкривають новий напрям в даній галузі науки і техніки. Отриманіпринципово нові факти, закономірності; розроблена нова теорія. Створено принципово новий пристрій, спосіб, метод	-	-	-
Нова	Отримана нова інформація, яка суттєво зменшує невизначеність наявних значень (по-новому або вперше пояснені відомі факти, закономірності, впроваджені нові поняття, розкрита структуразмісту). Проведено суттєве вдосконалення,доповнення і уточнення раніше досягнутих результатів	56	60	58
Відносно нова	Робота має елементи новизни в постановці задачі і методах дослідження. Результати дослідженнясистематизують і узагальнюють наявну інформацію, визначають шляхи подальших досліджень; впершезнайдено зв’язок (або знайдено новий зв’язок) між явищами. В принципі відомі положення розповсюджені на велику кількість об’єктів, в результаті чого знайдено ефективне рішення. Розроблені більш прості способи для досягнення відомих результатів. Проведена часткова раціональнамодифікація (з ознаками новизни)	-	-	-
Традиційна	Робота виконана за традиційною методикою. Результати дослідження мають інформаційний характер. Підтверджені або поставлені під сумнів відомі факти та твердження, які потребують перевірки. Знайдено новий варіант рішення, який не дає суттєвих переваг в порівнянні з існуючим	-	-	-
Не нова	Отримано результат, який раніше зафіксований в інформаційному полі, та не був відомий авторам	-	-	-
Середнє значення балів експертів		58,0		

Згідно середнього балу, отриманого від експертів, ступінь новизни визначається як високий, що свідчить про отримання нової інформації, яка значно зменшує невизначеність наявних знань. Це включає в себе пояснення відомих фактів чи закономірностей в новому світлі, вперше введені поняття, а також

розкриття структури змісту. Крім того, проведено значуще удосконалення, доповнення і уточнення раніше досягнутих результатів.

Таблиця 4.2 – Показники рівня теоретичного опрацювання науково-дослідноїроботи виставлені експертами

Характеристика рівня теоретичного опрацювання	Значення показника рівня теоретичного опрацювання, бали		
	Експерт (ПІБ, посада)		
	1	2	3
Відкриття закону, розробка теорії	-	-	-
Глибоке опрацювання проблеми: багатоаспектний аналіз зв’язків, взаємозалежності між фактами з наявністю пояснень, наукової систематизації з побудовою евристичної моделі або комплексного прогнозу	68	70	66
Розробка способу (алгоритму, програми), пристрою, отримання нової речовини	-	-	-
Елементарний аналіз зв’язків між фактами та наявною гіпотезою, класифікація, практичні рекомендації для окремого випадку тощо	-	-	-
Опис окремих елементарних фактів, викладення досвіду, результатів спостережень, вимірювань тощо	-	-	-
Середнє значення балів експертів	68,0		

Згідно середнього балу, отриманого від експертів, рівень теоретичного опрацювання науково-дослідної роботи визначається як глибоке. Це означає багатоаспектний аналіз проблеми, розгляд взаємозалежностей та зв'язків між фактами з врахуванням наявних пояснень. Також характеризується науковою систематизацією, яка включає в себе побудову евристичної моделі або комплексного прогнозу.

Показник, який характеризує рівень наукового ефекту, визначаємо за формулою.

$$E_{нау} = 0,6 \cdot k_{нов} + 0,4 \cdot k_{теор},$$

де $k_{нов}$, $k_{теор}$ - показники ступеня новизни та рівня теоретичного опрацювання науково-дослідної роботи, $k_{ноя} = 58{,}0$, $k_{теор} = 68{,}0$ балів;

0,6 та 0,4 – питома вага (значимість) показників ступеня новизни та рівня теоретичного опрацювання науково-дослідної роботи.

$$E_{нау} = 0{,}6 \cdot k_{нов} + 0{,}4 \cdot k_{теор} = 0{,}6 \cdot 58{,}0 + 0{,}4 \cdot 68{,}00 = 62{,}00 \text{ балів.}$$

Таблиця 4.3 – Граничні значення показника наукового ефекту

Досягнутий рівень показника	Кількість балів
Високий	70…100
Середній	50…69
Достатній	15…49
Низький (помилкові дослідження)	1…14

Згідно з визначеним рівнем наукового ефекту проведеної науково-дослідної роботи на тему " Метод виявлення потенційного кіберпорушника з використанням штучного інтелекту". Отриманий рівень становить 62,00 бали, що відповідає середньому статусу. Таким чином, у даному випадку можна говорити про потенційну фактичну ефективність науково-дослідної роботи.

4.2 Розрахунок витрат на здійснення науково-дослідної роботи

Витрати, пов’язані з проведенням науково-дослідної роботи на тему «Метод виявлення потенційного кіберпорушника з використанням штучного інтелекту», під час планування, обліку і калькулювання собівартості науково-дослідної роботи групуємо за відповідними статтями.

4.2.1 Витрати на оплату праці

Стаття "Витрати на оплату праці" включає у себе витрати на виплату основної та додаткової заробітної плати різним категоріям працівників. Ці витрати включають в себе оплату праці керівників відділів, лабораторій, секторів і груп, наукових, інженерно-технічних працівників, конструкторів, технологів, креслярів, копіювальників, лаборантів, робітників, студентів, аспірантів та інших працівників, які безпосередньо зайняті виконанням конкретної теми.

Ці витрати обчислюються на основі посадових окладів, відрядних розцінок, тарифних ставок відповідно до чинних в організаціях систем оплати праці.

Основна заробітна плата дослідників

Витрати на основну заробітну плату дослідників (Зо) розраховуємо у відповідності до посадових окладів працівників, за формулою:

$$З_о = \sum_{i=1}^{k} \frac{M_{ni} \cdot t_i}{T_p},$$

де k – кількість посад дослідників залучених до процесу досліджень;

M_{ni} – місячний посадовий оклад конкретного дослідника, грн;

t_i – число днів роботи конкретного дослідника, дн.;

T_p – середнє число робочих днів в місяці, T_p=24 дні.

Зо = 19400,00 · 24 / 24 = 19400,00 грн.

Проведені розрахунки зведемо до таблиці.

Таблиця 4.4 – Витрати на заробітну плату дослідників

Найменування посади	Місячний посадовий оклад, грн	Оплата за робочий день, грн	Число днів роботи	Витрати на заробітну плату, грн
Керівник проекту	19400,00	808,33	24	19400,00
Науковий співробітник	19150,00	797,91	14	11170,74
Інженер-програміст 1-ї категорії	19050,00	793,75	24	19050,00
Лаборант	8750,00	364,58	15	5468,70
Всього				55089,44

Основна заробітна плата робітників. Витрати на основну заробітну плату робітників ($З_р$) за відповідними найменуваннями робіт НДР на тему «Метод захисту даних, отриманих за допомогою сенсорів 6G» розраховуємо за формулою:

$$З_р = \sum_{i=1}^{n} C_i \cdot t_i,$$

де Сі – погодинна тарифна ставка робітника відповідного розряду, за виконану відповідну роботу, грн/год;

ti – час роботи робітника при виконанні визначеної роботи, год.

Погодинну тарифну ставку робітника відповідного розряду Сі можна визначити за формулою:

$$C_i = \frac{M_M \cdot K_i \cdot K_c}{T_p \cdot t_{зм}},$$

де ММ – розмір прожиткового мінімуму працездатної особи, або мінімальної місячної заробітної плати (в залежності від діючого законодавства), приймемо Мм=6700,00 грн;

Кі – коефіцієнт міжкваліфікаційного співвідношення для встановлення тарифної ставки робітнику відповідного розряду (табл. 4.5).

Таблиця 4.5 – Величина витрат на основну заробітну плату робітників

Найменування робіт	Тривалість роботи, год	Розряд роботи	Тарифний коефіцієнт	Погодинна тарифна ставка, грн	Величина оплати на робітника грн
Встановлення допоміжного обладнання	8,50	2	1,10	63,34	538,36
Інсталяція програмного забезпечення	6,25	3	1,35	77,73	485,82
Калібрування сенсорів	5,20	5	1,70	97,88	508,99
Налаштування програмних застосунків	5,50	4	1,50	86,37	475,02
Підготовка дослідження	8,00	4	1,50	86,37	690,94
Формування бази даних результатів дослідження	14,00	2	1,10	63,34	886,70
Всього					3585,82

Кс – мінімальний коефіцієнт співвідношень місячних тарифних ставок робітників першого розряду з нормальними умовами праці виробничих

об’єднань і підприємств до законодавчо встановленого розміру мінімальної заробітної плати.

Тр – середнє число робочих днів в місяці, приблизно Тр = 24 дн;

tзм – тривалість зміни, год.

С1 = 6700,00 · 1,10 · 1,65 / (24 · 8) = 63,34 грн.

Зр1 = 63,34 · 8,50 = 538,36 грн.

Додаткова заробітна плата дослідників та робітників

Додаткову заробітну плату розраховуємо як 10 … 12% від суми основної заробітної плати дослідників та робітників за формулою:

$$З_{дод} = (З_{о} + З_{р}) \cdot \frac{Н_{дод}}{100\%},$$

де Ндод – норма нарахування додаткової заробітної плати. Приймемо 11%.

Здод = (55089,44 + 3585,82) · 11 / 100% = 6454,27 грн.

4.2.2 Відрахування на соціальні заходи

Нарахування на заробітну плату дослідників та робітників розраховуємо як 22% від суми основної та додаткової заробітної плати дослідників і робітників за формулою:

$$З_{н} = (З_{о} + З_{р} + З_{дод}) \cdot \frac{Н_{зп}}{100\%}$$

де $Н_{зп}$ – норма нарахування на заробітну плату. Приймаємо 22%.

$Зн = (55089,44 + 3585,82 + 6454,27) \cdot 22 / 100\% = 14328,49$ грн.

4.2.3 Сировина та матеріали

До статті «Сировина та матеріали» належать витрати на сировину, основні та допоміжні матеріали, інструменти, пристрої та інші засоби і предмети праці, які

придбані у сторонніх підприємств, установ і організацій та витрачені на проведення досліджень за темою «Метод виявлення потенційного кіберпорушника з використанням штучного інтелекту».

Витрати на матеріали на даному етапі проведення досліджень в основному пов’язані з використанням моделей елементів та моделювання роботи і досліджень за допомогою комп’ютерної техніки та створення експериментальних математичних моделей або програмного забезпечення, тому дані витрати формуються на основі витратних матеріалів характерних для офісних робіт.

Витрати на матеріали (М), у вартісному вираженні розраховуються окремо по кожному виду матеріалів за формулою:

$$M = \sum_{j=1}^{n} H_j \cdot Ц_j \cdot K_j \; - \sum_{j=1}^{n} B_j \cdot Ц_{вj} \,,$$

де Нj – норма витрат матеріалу j-го найменування, кг;

n – кількість видів матеріалів;

Цj – вартість матеріалу j-го найменування, грн/кг;

Кj – коефіцієнт транспортних витрат, (Кj = 1,1 … 1,15); Вj – маса відходів j-го найменування, кг;

Цвj – вартість відходів j-го найменування, грн/кг.

М1 = 2,0 · 225,00 · 1,11 – 0 · 0 = 499,50 грн.

Проведені розрахунки зведемо до таблиці.

Таблиця 4.6 – Витрати на матеріали

Найменування матеріалу, марка, тип, сорт	Ціна за 1 кг, грн	Норма витрат, кг	Величина відходів, кг	Ціна відходів, грн/кг	Вартість витраченого матеріалу, грн
Папір канцелярський офісний (А4)	225,00	2,0	-	-	499,50
Папір для заміток (А5)	116,00	4,0	-	-	515,04
Начиння канцелярське	195,00	3,0	-	-	649,35
Органайзер офісний	183,00	3,0	-	-	609,39
Картридж для принтера	950,00	1,0	-	-	1054,50
USB флеш накопичувач Transcend 16Gb JetFlash 700 (TS64GJF700)	200,00	1,0	-	-	222,00
Всього					3549,78

4.2.5 Накладні (загальновиробничі) витрати

До статті «Накладні (загальновиробничі) витрати».. До них належать: витрати, пов’язані з управлінням організацією; витрати на винахідництво та раціоналізацію; витрати на підготовку (перепідготовку) та навчання кадрів; витрати, пов’язані з набором робочої сили; витрати на оплату послуг банків; витрати, пов’язані з освоєнням виробництва продукції; витрати на науково-технічну інформацію та рекламу та ін.

Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуємо як 100…150% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%},$$

де Ннзв – норма нарахування за статтею «Накладні (загальновиробничі) витрати», приймемо Ннзв = 130%.

Внзв = (55089,44 + 3585,82) · 130 / 100% = 76277,83 грн.

Витрати на проведення науково-дослідної роботи на тему «Метод виявлення потенційного кіберпорушника з використанням штучного інтелекту» розраховуємо як суму всіх попередніх статей витрат за формулою:

$$B_{заг} = З_о + З_р + З_{дод} + З_н + М + К_в + B_{спец} + B_{прг} + A_{обл} + B_в + B_{св} + B_{сп} + I_в + B_{нзв}. \quad (4.17)$$

$B_{заг}$= 55089,44 +3585,82 +6454,27 +14328,49 +3549,78+4867,52+34965,00 +0 + 5684,88+247,06+11735,05 +17602,57 +35205,15 +76277,83 = 269592,86 грн.

Загальні витрати ЗВ на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів розраховується за формулою:

$$ЗВ = \frac{B_{заг}}{\eta},$$

де η – коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи, приймемо η =0,95.

ЗВ = 269592,86 / 0,95 = 283781,95 грн.

4.3 Розрахунок витрат на здійснення науково-дослідної роботи

Оцінка та підтвердження ефективності виконання науково-дослідної роботи фундаментального або пошукового характеру представляє собою складний процес,

який часто ґрунтується на експертних оцінках і, отже, має високий рівень вірогідності.

Для обґрунтування доцільності проведення науково-дослідної роботи на тему "Метод виявлення потенційного кіберпорушника з використанням штучного інтелекту" використовується спеціальний комплексний показник, який враховує важливість, результативність роботи, можливість впровадження отриманих результатів у виробництво та обсяг витрат на виконання робіт.

Комплексний показник КР рівня науково-дослідної роботи представляє собою зважену комбінацію різноманітних метрик та показників. Він використовується для оцінки та порівняння рівня науково-дослідної активності або продуктивності науково-дослідницьких груп, організацій, країн чи інших суб'єктів. Такий комплексний показник може враховувати різні аспекти дослідницької діяльності та намагається відобразити їх узагальненим числовим значенням. Він може бути розрахований за визначеною формулою:

$$K_P = \frac{I^n \cdot T_C \cdot R}{B \cdot t},$$

де I – коефіцієнт важливості роботи. Приймемо I= 4;

n – коефіцієнт використання результатів роботи. Приймемо n=2;

ТС – коефіцієнт складності роботи. Приймемо ТС=3;

В – вартість науково-дослідної роботи, тис. грн. Приймемо В =283781,95 грн;

t – час проведення дослідження. Приймемо t = 0,08 років, (1 міс.).

R – коефіцієнт результативності роботи. Приймемо R=4;

Визначення показників I, n, ТС, R, В, t здійснюється експертним шляхом або на основі нормативів.

$$K_P = \frac{I^n \cdot I_C \cdot K}{B \cdot t} = 4^2 \cdot 3 \cdot 4 / 283{,}7 \cdot 0{,}08 = 8{,}45.$$

Якщо КР=1, то науково-дослідну роботу на тему «Метод виявлення потенційного кіберпорушника з використанням штучного інтелекту» можна вважати ефективною з високим науковим, технічним і економічним рівнем.

Таким чином, у даному розділ було проведено економічне тестування та витрати на проведення науково-дослідної роботи на тему «Метод виявлення потенційного кіберпорушника з використанням штучного інтелекту» складають 283781,95 грн. Відповідно до проведеного аналізу та розрахунків рівень наукового ефекту проведеної науково- дослідної роботи на тему «Метод захисту даних, отриманих за допомогою сенсорів 6G» є середній, а дослідження актуальними, рівень доцільності виконання науково-дослідної роботи КР=1, що свідчить про потенційну ефективність з високим науковим, технічним і економічним рівнем.

ВИСНОВКИ

В результаті проведеного дослідження методів виявлення потенційного кіберпорушника з використанням штучного інтелекту визначено основний об'єкт уваги - процес виявлення та протидії можливим кібератакам. Предметом дослідження стали методи та стратегії виявлення порушників в кіберпросторі. Мета даної магістерської роботи полягала в оптимізації існуючих методів виявлення кіберпорушників в умовах штучного інтелекту.

Для досягнення цієї мети був проведений аналіз існуючих методів виявлення кіберзагроз та вдосконалення їх шляхом використання штучного інтелекту. Розроблено власні методи та стратегії виявлення, спрямовані на підвищення ефективності захисту від кіберпорушників. Експериментальне дослідження виявлення потенційних загроз дозволило оцінити ефективність запропонованих методів та стратегій.

Новаторським результатом дослідження став розроблений метод виявлення кіберпорушника з використанням штучного інтелекту, спрямований на розв'язання актуальних завдань забезпечення кібербезпеки. Цей метод має велике практичне значення, забезпечуючи високий рівень безпеки та надійності виявлення кіберзагроз.

Відповідно до проведеного аналізу та розрахунків, рівень наукового ефекту проведеної науково-дослідної роботи на тему «Метод виявлення потенційного кіберпорушника з використанням штучного інтелекту» становить 8,45(середній рівень), а витрати 283781,95 грн, що свідчить про потенційну ефективність роботи з високим науковим, технічним і економічним рівнем.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Dinesh Kumar Saini, Krishan Kumar, Punit Gupta. Security Issues in IoT and Cloud Computing Service Models with Suggested Solutions. April 2022. URL: https://www.hindawi.com/journals/scn/2022/4943225/ (accessed: 15.10.2023)
2. Krešimir Popović; Željko Hocenski. Cloud computing security issues and challenges. URL: https://ieeexplore.ieee.org/abstract/document/5533317 (accessed: 15.10.2023)
3. Олексій Палій. Аналіз загроз кібербезпеці комп'ютерних ігор жанру RPG. Науково-технічна конференція факультету інформаційних технологій та комп'ютерної інженерії ВНТУ. 2022 р. 2 с. URL: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2022/paper/view/15765/13281 (дата звернення: 10.06.2022)
4. Олексій Палій, Ігор Віщун. Рух квадрокоптеру за траєкторією, заданою контрольними точками. Науково-технічна конференція факультету машинобудування та транспорту ВНТУ. 2022 р. 3 с. URL: https://conferences.vntu.edu.ua/index.php/all-fmt/all-fmt-2022/paper/view/15370/12925 (дата звернення: 10.06.2022)
5. Nakita Mc Cool. What is GitHub?. 2023. URL: https://codeinstitute.net/global/blog/github-might-benefit-using (accessed: 15.10.2023)
6. Erica Mixon, Ivy Wigmore. What is Google Drive?. 2022. URL: https://www.techtarget.com/searchmobilecomputing/definition/Google-Drive (accessed: 15.10.2023)
7. Ellen Cushing, How Slack Upended the Workplace. November 2021. URL: https://www.theatlantic.com/magazine/archive/2021/11/slack-office-trouble/620173/ (accessed: 15.10.2023)
8. John Brandon. Why Microsoft Teams is so much better than zoom for collaboration. URL: https://www.forbes.com/sites/johnbbrandon/2021/01/17/why-microsoft-teams-is-

so-much-better-than-zoom-and-slack-for-collaboration/?sh=5a64bc705cd7 (accessed: 15.10.2023)

9. Idilio Drago, Marco Mellia, Anna Sporotto, Ramin Sadre, Aiko Pras. Inside dropbox: understanding personal cloud storage services. November 2012 URL: https://dl.acm.org/doi/abs/10.1145/2398776.2398827 (accessed: 15.10.2023)
10. Hari Narayn. Get Online with SharePoint Online. September 2023 URL: https://link.springer.com/chapter/10.1007/978-1-4842-9726-1_1 (accessed: 15.10.2023)
11. Muhammed-Amr Abd El-Migid. A Trello power-up to capture and monitor emotions of Agile teams. URL: https://www.sciencedirect.com/science/article/abs/pii/S016412122100279X (accessed: 15.10.2023)
12. Noah Buhlmann, Mohammad Ghafari. How do developers deal with security issue reports on Github? April 2022. URL: https://dl.acm.org/doi/abs/10.1145/3477314.3507123 (accessed: 15.10.2023)
13. Darren Quick. Google Drive: Forensic analysis of data remnants. April 2021. URL: https://www.sciencedirect.com/science/article/abs/pii/S1084804513002051 (accessed: 15.10.2023)
14. Joel Witts. How Secure Is Slack For Your Business? 29 March 2023. URL: https://expertinsights.com/insights/how-secure-is-slack-for-your-business/ (accessed: 15.10.2022)
15. Jason Stagnitto. Dropbox Security 2023: The Good, the Bad and the Ugly. URL: https://www.cloudwards.net/dropbox-security/ (accessed: 15.10.2023)
16. Risks and Vulnerabilities: Is SharePoint Secure? URL: https://www.mrsharepoint.guru/is-sharepoint-secure/ (accessed: 15.10.2023)
17. Nikolay Pankov. Trello data leak. URL: https://www.kaspersky.com/blog/trello-data-leaks/39497/ (accessed: 15.10.2023).

ДОДАТОК А

ПРОТОКОЛ ПЕРЕВІРКИ МАГІСТЕРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Метод виявлення потенційного кіберпорушника з використанням штучного інтелекту

Автор роботи: Марусій Андрій Андрійович

Тип роботи: магістерська кваліфікаційна робота

Підрозділ кафедра захисту інформації ФІТКІ
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність – 80,2 %. Схожість – 19,8 %.

Аналіз звіту подібності (відмітити потрібне):

√ 1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

√ 2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

√ 3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ Валентина КАПЛУН
(підпис)

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ Андрій МАРУСІЙ
(підпис)

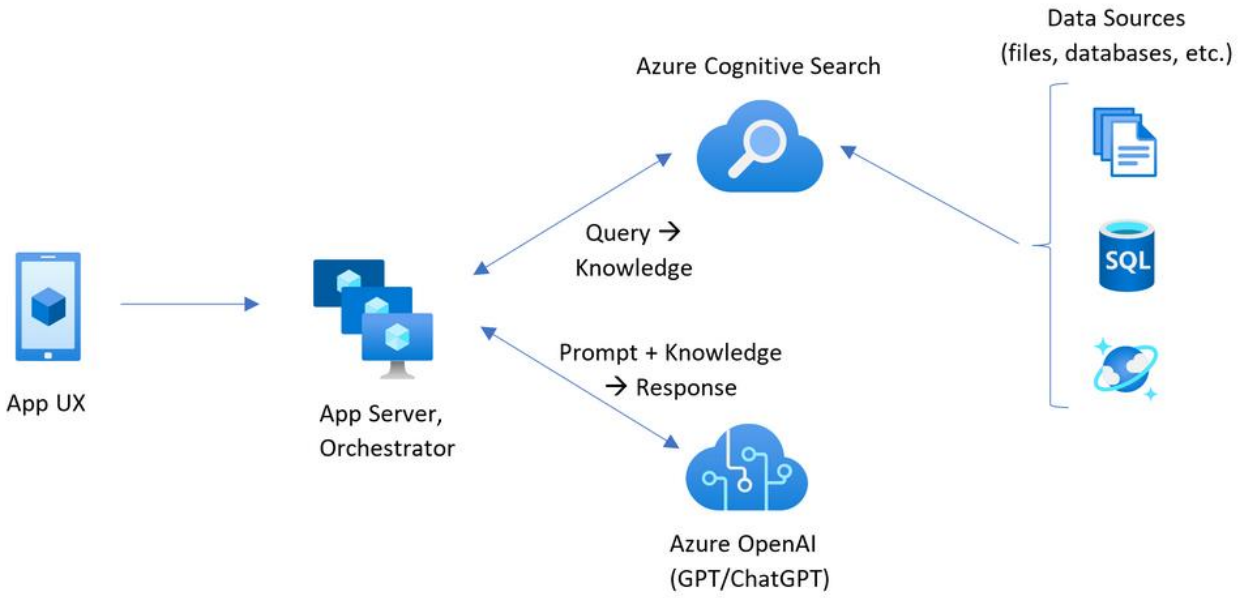
Керівник роботи _____ Віталій ЛУКІЧОВ

ІЛЮСТРАТИВНА ЧАСТИНА

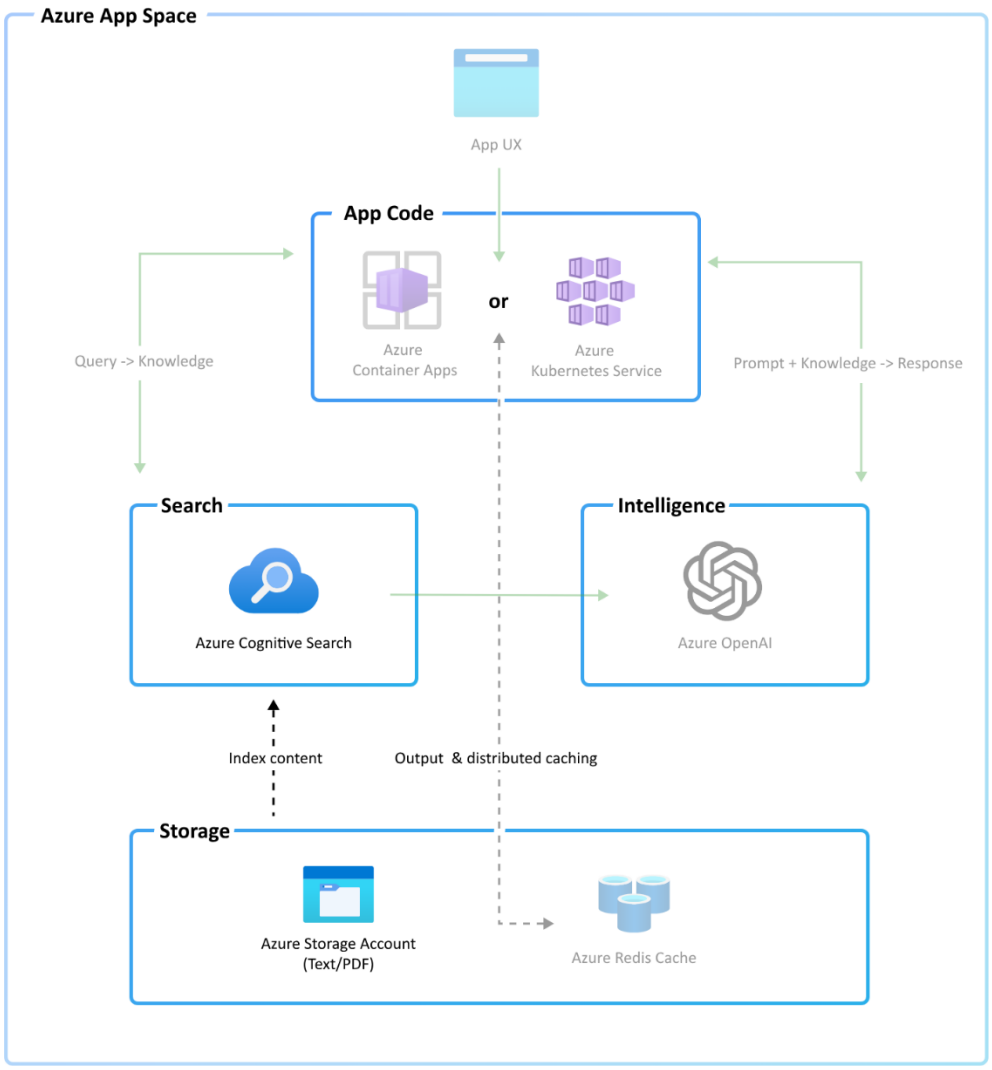
Метод виявлення потенційного кіберпорушника з використанням штучного інтелекту

(Назва магістерської кваліфікаційної роботи)

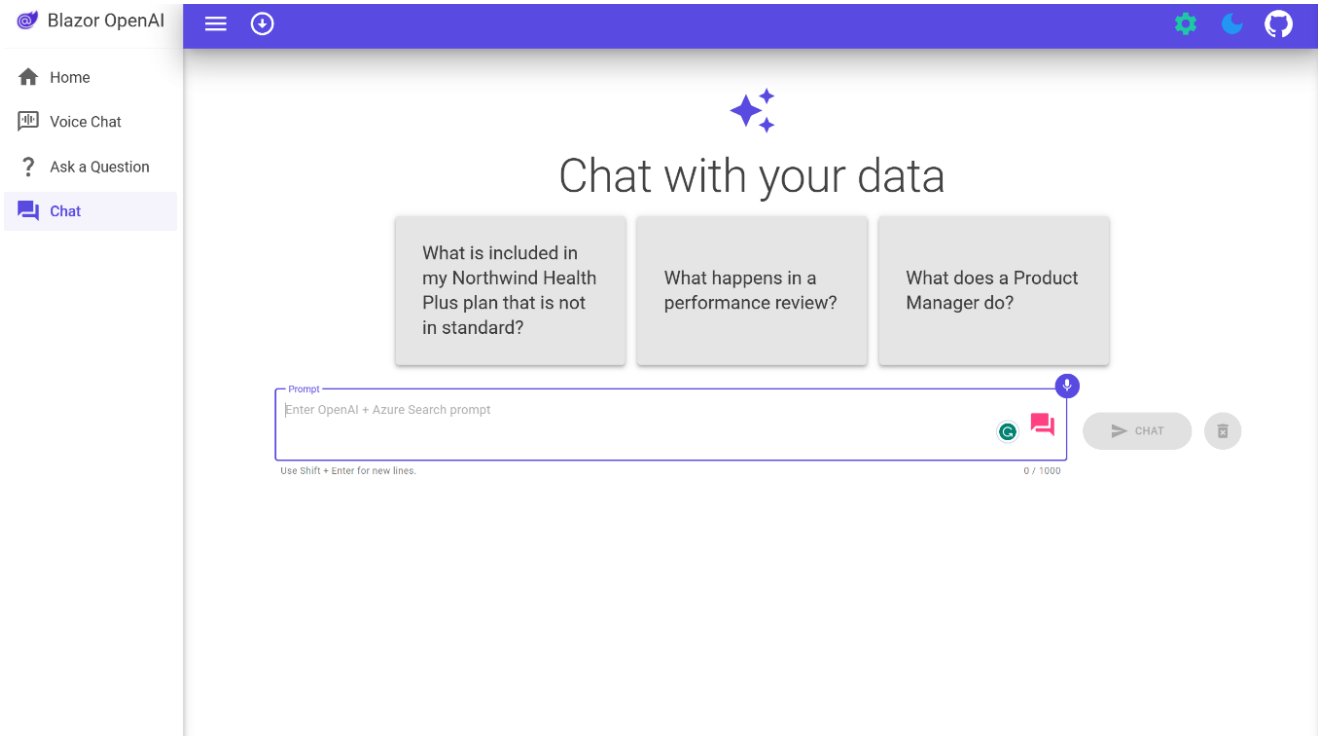
Архітектура сервісів Azure



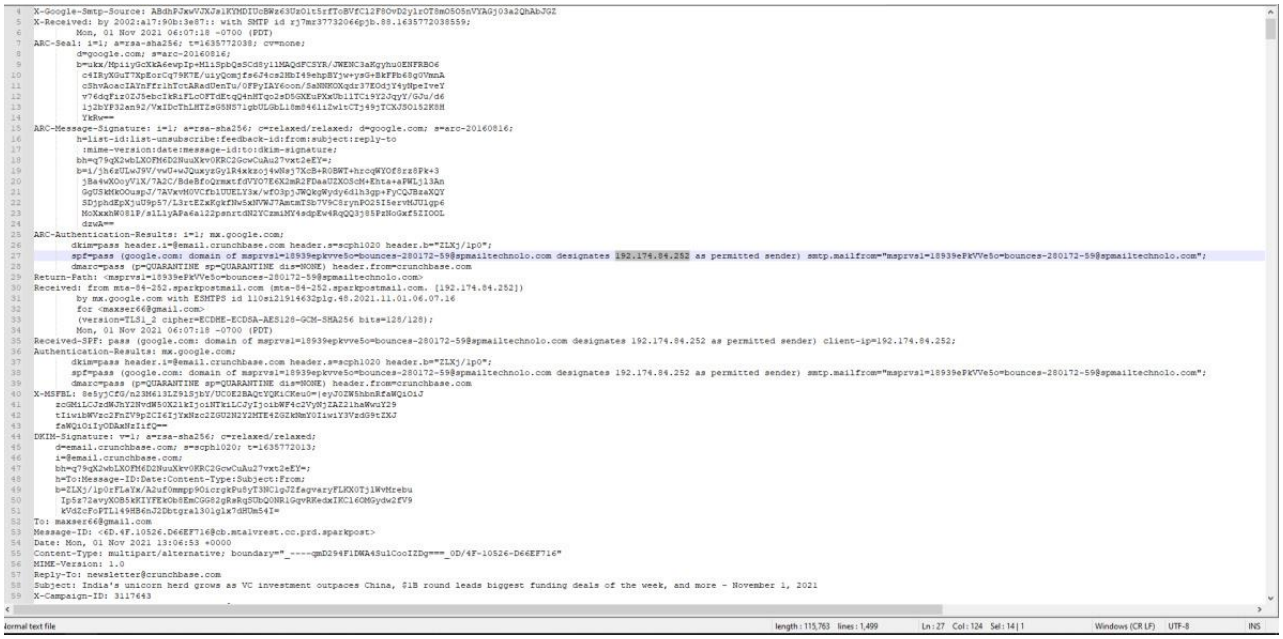
Простір сервісів Azure



Веб-інтерфейс користувача



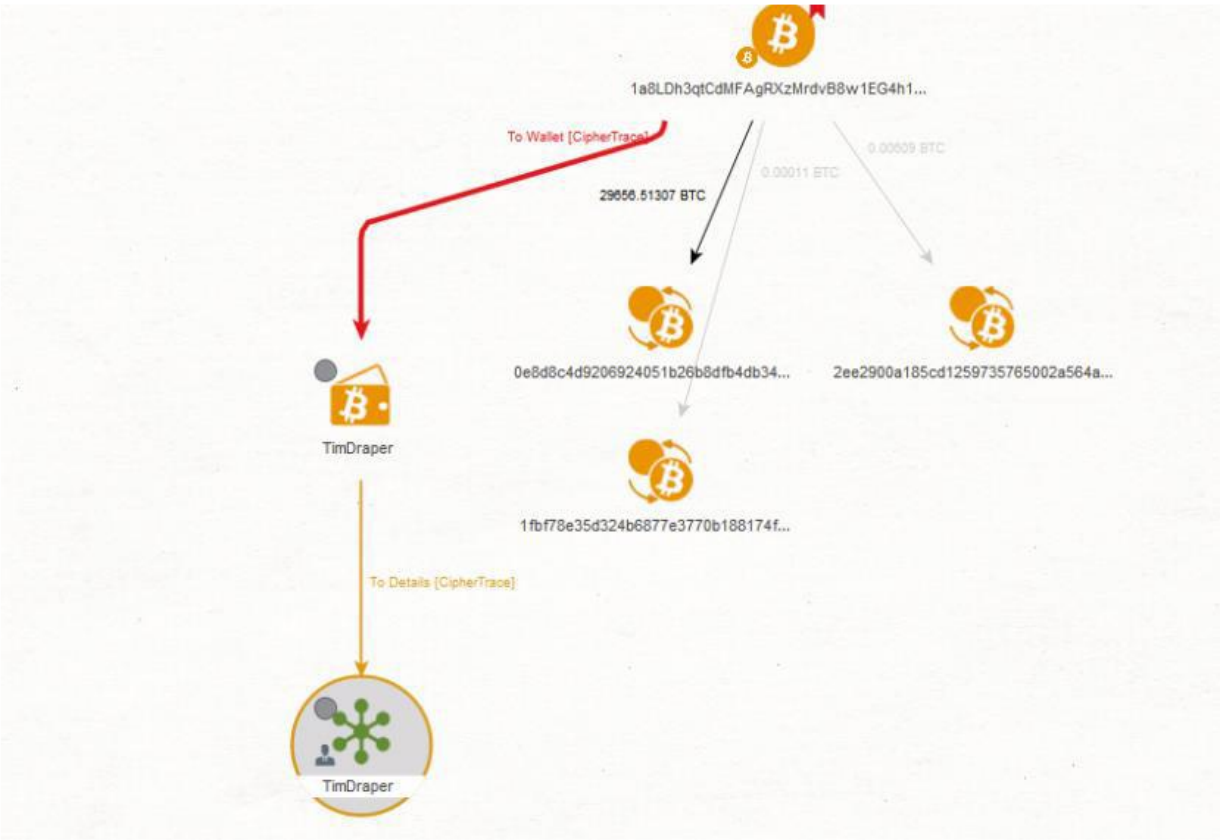
Приклад відкритого листа



```
X-Google-Smtp-Source: ABdhPJxwVJXJs1KYMDIUoBWz63Uz0lt5rfToBVfC12F8OvD2ylrOT8mO5O5nVYAGj03a2QhAbJGZ
X-Received: by 2002:a17:90b:3e87:: with SMTP id rj7mr37732066pjb.88.1635772038559;
        Mon, 01 Nov 2021 06:07:18 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1635772038; cv=none;
        d=google.com; s=arc-20160816;
        b=ukx/MpiiyGcXkA6ewpIp+M1iSpbQaSCd8yllMAQdFCSYR/JWENC3aKgyhu0ENFBO6
         c4IRyX0uT7XpEorCq79K7E/uiyQomjfs6J4csZHbI49ehpBYjw+ysG+BkFFb6SqOVmnA
         cSbvAcacIAYbFfrihTotARadUenTu/0FPyIAY6om/SaNNKOXqdz37EOdjY4yHpIvwY
         v76dqFizOJJ5ebcIkRiFLoOFTdEtqQ4nHTqo2sD5GKEuPXx0blITCi9YJJqyY/GJu/d6
         1j2bYP32an92/VwIDcThLHTZs6NS71gbULl8m846liZwltCTj49jTCXJSO152K8H
         YkKv==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=list-id:list-unsubscribe:feedback-id:from:subject:reply-to
         :mime-version:date:message-id:to:dkim-signature;
        bh=q79qX2wbLXOfM6D2NuuXkv0KRC2GcwCuAu27vxt2eEY=;
        b=1/jh6fULwJ9V/vwU+wJQuxyzGy1R4akzoj4wNaj7XcB+RGBWT+hrcqWYOf8rz8Pk+3
         jBa4wXOoyV1X/7A2C/BdeBfoQrmxtfdVYO7E6X2mR2FDaaUZXO5cM+Ehta+aFWLj13An
         GgUSkMkOOuspJ/7AVwvH0VCfb1UUELY3k/wfO3pjJWQkgWydy6dlh3gp+FyCQJBzaXQY
         SDjphdEpXjuU9p57/L3rtEZxKgkfNw5xNVWJ7AmtmTSb7V9C8rynPO2SI5erv6tJUlgp6
         NoXmXMW081P/slLiyAPa6al22psnrtdN2YCzmiMY4sdpEw4RqQQ3j85FzNoGxf5ZIOOL
         dzwA==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@email.crunchbase.com header.s=scph1020 header.b="ZLXj/1p0";
       spf=pass (google.com: domain of msprvs1=18939epkvve5o=bounces-280172-59@spmailtechnolo.com designates 192.174.84.252 as permitted sender) smtp.mailfrom="msprvs1=18939ePkVVe5o=bounces-280172-59@spmailtechnolo.com";
       dmarc=pass (p=QUARANTINE sp=QUARANTINE dis=NONE) header.from=crunchbase.com
Return-Path: <msprvs1=18939ePkVVe5o=bounces-280172-59@spmailtechnolo.com>
Received: from mta-84-252.sparkpostmail.com (mta-84-252.sparkpostmail.com. [192.174.84.252])
        by mx.google.com with ESMTPS id l10si21914632plg.48.2021.11.01.06.07.16
        for <maxser66@gmail.com>
        (version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
        Mon, 01 Nov 2021 06:07:18 -0700 (PDT)
Received-SPF: pass (google.com: domain of msprvs1=18939epkvve5o=bounces-280172-59@spmailtechnolo.com designates 192.174.84.252 as permitted sender) client-ip=192.174.84.252;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@email.crunchbase.com header.s=scph1020 header.b="ZLXj/1p0";
       spf=pass (google.com: domain of msprvs1=18939epkvve5o=bounces-280172-59@spmailtechnolo.com designates 192.174.84.252 as permitted sender) smtp.mailfrom="msprvs1=18939ePkVVe5o=bounces-280172-59@spmailtechnolo.com";
       dmarc=pass (p=QUARANTINE sp=QUARANTINE dis=NONE) header.from=crunchbase.com
X-MSFBL: 8etyjCfG/nZM613LZ9l5jbY/UCOLEBAQcYQMiCKeuC=|eyJ0ZWSnbnRfaWQiOiJ
    zGMiLCJzdWJhY2NvdW50X2lkIjoiNTkiLCJyIjoibWF4c2VyMjZAZ21haWwuY29
    tIiwibWVzc2FnZV9pZCI6IjYxNzc2ZGU2N2Y2MTE4ZGZkNmY0IiwiY3Vzdd9tZXJ
    faWQiOiIyODAxNzIifQ==
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
    d=email.crunchbase.com; s=scph1020; t=1635772013;
    i=@email.crunchbase.com;
    bh=q79qX2wbLXOfM6D2NuuXkv0KRC2GcwCuAu27vxt2eEY=;
    h=To:Message-ID:Date:Content-Type:Subject:From;
    b=ELXj/1p0rFLaYk/AJuf0mmpp9OicrgkPu5yT3NC1gJZfagvaryFLKX0TjlWvMrebu
     Ip5z72avyXOB5kKIYFEkOb8EmCGG82gReqSUbQONRlGqvRKedxIKC16MGydw2fV9
     kVdZcFoPIL149HB6nJ2Dbtgra130ig1k7dHUm54I=
To: maxser66@gmail.com
Message-ID: <6D.4F.10526.D66EF716@cb.mtalvrest.oc.prd.sparkpost>
Date: Mon, 01 Nov 2021 13:06:53 +0000
Content-Type: multipart/alternative; boundary="_----qmD294F1DWA4SulCooIZDg===_0D/4F-10526-D66EF716"
MIME-Version: 1.0
Reply-To: newsletter@crunchbase.com
Subject: India's unicorn herd grows as VC investment outpaces China, $1B round leads biggest funding deals of the week, and more - November 1, 2021
X-Campaign-ID: 3117643
```

Адреса фішингового сайту

Зв’язки криптогаманців



Блок схема методу