Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(освітній рівень)

на тему: "Використання OSINT-технологій при розкритті шахрайств, учинених в кіберпросторі"

Виконав: студент (ка)

Спеціальності:
125 «Кібербезпека та захист інформації»
(шифр і назва напряму підготовки, спеціальності)

Габорець Ольга Андріївна
підпис (прізвище та ініціали)

Керівник Муж В. В.
підпис (прізвище та ініціали)

Нормоконтроль Тимощук Д. І.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н. В.
підпис (прізвище та ініціали)

Рецензент Яцишин В. В.
підпис (прізвище та ініціали)

м. Тернопіль – 2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп`ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека та захист інформації
(шифр і назва спеціальності)

Студенту Габорець Ользі Андріївні
(прізвище, ім'я, по батькові)

1. Тема роботи Використання OSINT-технологій при розкритті шахрайств, учинених в кіберпросторі

Керівник роботи Муж Валерій Вікторович, кандидат юридичних наук, доцент кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «22» 11 2024 року № 4/7-1120

2. Термін подання студентом завершеної роботи 18.12.2024

3. Вихідні дані до роботи Наукові публікації, монографії, нормативно-правові акти .

4. Зміст роботи (перелік питань, які потрібно розробити)
Проаналізувати наукові джерела, нормативно-правові акти щодо поняття кіберзлочинів та їх класифікація.
Систематизувати теоретичні аспекти шахрайств у кіберпросторі: види, особливості та методи здійснення.
Розглянути загальну характеристику OSINT та особливості використання OSINT-технології у боротьбі з кіберзлочинами.
Дослідити методологію використання OSINT-технологій для збору інформації в кіберпросторі.
Розробити практичні кейси використання OSINT-технологій при розкритті шахрайств, учинених в кіберпросторі.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Титульна сторінка. Актуальність дослідження. Мета та завдання. Об'єкт і предмет дослідження. Кіберзлочини: поняття та класифікація. Сутність шахрайств у кіберпросторі. OSINT-технології: загальна характеристика. Методологія застосування OSINT-технологій для збору інформації в кіберпросторі. Методологія використання OSINT для розкриття шахрайств. Практичне значення одержаних результатів. Апробація результатів магістерської роботи. Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., к.т.н., доцент		
Безпека в надзвичайних ситуаціях	Клепчик В.М., проректор з адміністративно-господарської роботи та будівництва		

7. Дата видачі завдання 20.09.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	20.09 – 22.09	Виконано
2.	Проведення аналізу наукових джерел щодо поняття кіберзлочинів, їх класифікація та визначення актуальності дослідження	23.09 – 03.10	Виконано
3.	Формулювання мети, завдань, об’єкта та предмета дослідження	04.10 – 08.10	Виконано
4.	Систематизація теоретичних аспектів шахрайств у кіберпросторі: види, особливості та методи здійснення	09.10 – 17.10	Виконано
5.	Оформлення розділу «Теоретичні основи розкриття шахрайств у кіберпросторі»	18.10-22.10	Виконано
6.	Аналіз загальної характеристики OSINT та використання OSINT-технології у боротьбі з кіберзлочинами. Дослідження методології використання OSINT-технологій для збору інформації в кіберпросторі	23.10 – 01.11	Виконано
7.	Оформлення розділу «Особливості використання OSINT-технологій у розкритті шахрайств, учинених в кіберпросторі»	02.11 – 05.11	Виконано
8.	Розробити практичні кейси використання OSINT-технологій при розкритті шахрайств, учинених в кіберпросторі	06.11 – 11.11	Виконано
9.	Оформлення розділу «Практичні аспекти використання OSINT-технологій у розкритті шахрайств, учинених в кіберпросторі»	12.11-20.11	Виконано
10.	Оформлення розділу «Охорона праці та безпека в надзвичайних ситуаціях»	21.11 – 25.11	Виконано
11.	Оформлення кваліфікаційної роботи	26.11 – 07.12	Виконано
12.	Нормоконтроль	08.12 – 10.12	Виконано
13.	Перевірка на плагіат	12.12 – 14.12	Виконано
14.	Попередній захист кваліфікаційної роботи	20.12	Виконано
15.	Захист кваліфікаційної роботи	28.12.2024	

Студент _____ Габорець О.А.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Муж В.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Використання OSINT-технологій при розкритті шахрайств, учинених в кіберпросторі // ОР «Магістр» // Габорець Ольга Андріївна // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБмд-61 // Тернопіль, 2024 // С. 80, рис. – 3, табл. – - , кресл. – - , додат. – 1.

Ключові слова: OSINT, OSINT-технології, кіберзлочини, шахрайство, кіберпростір, кібербезпека, розслідування, електронні докази, соціальна інженерія, фішинг.

Кваліфікаційна робота на тему «Використання OSINT-технологій при розкритті шахрайств, учинених в кіберпросторі» є науково-практичним дослідженням, спрямованим на вдосконалення методів протидії шахрайствам у цифровому середовищі із застосуванням OSINT (Open Source Intelligence). У рамках дослідження здійснено комплексний аналіз сучасних викликів у кіберпросторі, визначено ключові види шахрайств, серед яких фішинг, соціальна інженерія, криптографічні маніпуляції та використання шкідливого програмного забезпечення.

Особливу увагу приділено розробці практичних підходів до використання OSINT-інструментів, включаючи авторську методику для ідентифікації цифрових слідів, збору електронних доказів, профілювання злочинців і документування шахрайських дій. Це дозволяє значно підвищити ефективність розслідувань у кіберзлочинів та сприяє вдосконаленню процесу протидії кіберзагрозам.

ABSTRACT

Use of OSINT Technologies in Uncovering Cyber Fraud // Thesis of educational level "Master"// Olha Haborets // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБмд-61 // Ternopil, 2024 // P. 80, figs. – 3, tables –, diagrams – , appendices – 1.

Keywords: OSINT, OSINT technologies, cybercrimes, fraud, cyberspace, cybersecurity, investigation, electronic evidence, social engineering, phishing.

The qualification thesis titled "Use of OSINT Technologies in Uncovering Cyber Fraud" is a scientific and practical research aimed at improving methods for combating fraud in the digital environment using OSINT (Open Source Intelligence). The research includes a comprehensive analysis of contemporary challenges in cyberspace and identifies key types of fraud, such as phishing, social engineering, cryptographic manipulations, and the use of malicious software.

Particular attention is devoted to the development of practical approaches for utilizing OSINT tools, including an original methodology for identifying digital traces, collecting electronic evidence, profiling offenders, and documenting fraudulent activities. This significantly enhances the efficiency of cybercrime investigations and contributes to the advancement of countering cyber threats.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

OSINT	—	Open Source Intelligence
КПК України	—	Кримінальний процесуальний кодекс України
ЦПК України	—	Цивільний процесуальний кодекс України
ЗУ	—	Закон України
КК України	—	Кримінальний кодекс України
СБУ	—	Служба безпеки України
НПУ	—	Національної поліції України
ШПЗ	—	Шкідливе програмне забезпечення
ШІ	—	Штучний інтелект

ВСТУП

Актуальність теми. Шахрайство в кіберпросторі належить до найбільш динамічних і небезпечних форм кіберзлочинності, що набули особливої актуальності в умовах глобальних викликів, таких як пандемія COVID-19 та військова агресія російської федерації проти України. Активне використання мережі Інтернет і сучасних інформаційних технологій сприяє створенню унікальних умов для маніпуляцій, обману та незаконного збагачення. Це зумовлює необхідність розроблення новітніх, ефективних підходів до протидії зазначеному явищу.

Ключовою особливістю шахрайства в кіберпросторі є відсутність географічних обмежень, що дозволяє зловмисникам реалізовувати злочинні дії з будь-якої точки світу за допомогою технологій анонімізації та інструментів соціальної інженерії. Така специфіка суттєво ускладнює процеси виявлення, документування та розслідування зазначених злочинів, що значно знижує ефективність традиційних методів боротьби. Крім того, швидке поширення цифрових платформ, зокрема соціальних мереж, онлайн-торгівлі та дистанційних сервісів, створює сприятливі умови для розширення шахрайських схем.

В умовах зазначених викликів особливої актуальності набуває застосування OSINT-технологій (розвідки на основі відкритих джерел), які забезпечують можливість збору, аналізу та використання публічно доступної інформації для ідентифікації, розкриття та протидії кіберзагрозам. Використання цих технологій відкриває нові перспективи для підвищення ефективності заходів із розкриття шахрайства у кіберпросторі та мінімізації його наслідків.

Мета і задачі дослідження. Мета дослідження полягає у розробці теоретичних основ та практичних рекомендацій щодо використання OSINT-технологій у розкритті шахрайств, учинених в кіберпросторі.

Завданнями дослідження є:

– Аналіз поняття кіберзлочинів та їх класифікації.

– Визначення сутності шахрайств у кіберпросторі, їх видів, особливостей та методів здійснення.

– Аналіз сучасних OSINT-інструментів.

– Розробка практичних рекомендацій щодо методології використання OSINT-технологій для збору інформації в кіберпросторі.

– Розробка методології використання OSINT-технологій для розкриття шахрайств, учинених у кіберпросторі.

Об’єкт дослідження є шахрайства, вчинені у кіберпросторі.

Предмет дослідження є методи та інструменти використання OSINT-технологій для розкриття шахрайств у кіберпросторі.

Наукова новизна одержаних результатів кваліфікаційної роботи. Вперше проведено комплексний аналіз використання OSINT-технологій у розкритті шахрайств, учинених в кіберпросторі, що дозволило сформувати систематизований підхід до їх використання для збору, аналізу та використання інформації з відкритих джерел.

Удосконалено класифікацію шахрайств у кіберпросторі шляхом врахування сучасних соціально-економічних умов, глобалізації цифрових платформ та особливостей шахрайських схем в умовах воєнного стану.

Запропоновано авторську методологію використання OSINT-технологій для ідентифікації цифрових слідів та збору електронних доказів, що підвищує ефективність розслідувань кіберзлочинів.

Практичне значення одержаних результатів. Розроблені методики використання OSINT-технологій можуть бути використані у роботі уповноважених суб’єктів для підвищення ефективності розслідування шахрайств у кіберпросторі. Результати дослідження впроваджено в освітній процес Донецького державного університету внутрішніх справ (Акт впровадження результатів науково-дослідної роботи в освітній процес Донецького державного університету внутрішніх справ від 18.12.2024 року) у межах викладанні таких освітніх компонентів: «Пошук інформації з відкритих джерел (OSINT) працівниками кримінальної поліції» та «Інформаційно-аналітичне забезпечення підрозділів кримінальної поліції».

Апробація результатів магістерської роботи. Основні результати проведених досліджень обговорювались на: науково-педагогічному підвищенні кваліфікації «Цифровізація вищої освіти та цифрова грамотність», (м. Львів, Україна – м. Торунь, Польща), круглому столі «Взаємодія державних органів та громадськості у сфері протидії кримінальним правопорушенням у центральних регіонах України», (м. Кропивницький, Україна), міжвідомчому науково-практичному круглому столі «Актуальні проблеми кібербезпеки в Україні в умовах воєнного стану», (м. Київ, Україна), міжнародній науково-практичній конференції «Теоретико-прикладні проблеми кримінального процесу та криміналістики в умовах воєнного стану» (м. Кам'янець-Подільський, Україна).

Апробація результатів магістерської роботи також проведена на базі Донецького державного університету внутрішніх справ: Акт впровадження результатів науково-дослідної роботи в освітній процес Донецького державного університету внутрішніх справ від 18.12.2024 року та Акт впровадження результатів науково-дослідної роботи в науково-дослідну діяльність Донецького державного університету внутрішніх справ від 18.12.2024 року.

Публікації. Основні результати кваліфікаційної роботи опубліковано у працях конференції (див. Додаток А).

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ РОЗКРИТТЯ ШАХРАЙСТВ У КІБЕРПРОСТОРІ

1.1 Поняття кіберзлочинів та їх класифікація

Розвиток людства характеризується глобалізацією інформаційних потоків та віртуалізацією способів спілкування фізичних та юридичних осіб. При цьому констатуємо те, що особи, які вчиняють різні кримінальні правопорушення не залишили поза увагою впровадження в суспільні відносини інформаційно-комунікаційних технологій.

Відповідно до положень статті 2 Кримінального процесуального кодексу України від 13 квітня 2012 року № 4651-VI (далі – КПК України) завданнями кримінального провадження є захист особи, суспільства та держави від кримінальних правопорушень, охорона прав, свобод та законних інтересів учасників кримінального провадження, а також забезпечення швидкого, повного та неупередженого розслідування і судового розгляду з тим, щоб кожний, хто вчинив кримінальне правопорушення, був притягнутий до відповідальності в міру своєї вини, жоден невинуватий не був обвинувачений або засуджений, жодна особа не була піддана необґрунтованому процесуальному примусу і щоб до кожного учасника кримінального провадження була застосована належна правова процедура [1].

Дефініцією є те, що для вирішення завдань кримінального провадження, розпочатого за фактом вчинення кіберзлочину, правоохоронцями приділяється увага пошуку, виявленню, фіксації ти використанні доказів при досудовому розслідуванні та судовому розгляду кримінального провадження. Доказами в кримінальному провадженні є фактичні дані, отримані у передбаченому КПК України порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню [1].

Згідно з положеннями КПК України процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів [1]. При цьому, з метою

протидії кіберзлочинам, правоохоронцями велика увага приділяється пошуку та фіксації електронних доказів. Однак, в чинному КПК України відсутнє тлумачення поняття «електронний доказ». Для визначення понятійної сутності терміну «електронний доказ», використовуючи принцип аналогії права, необхідно звернутися до положень Цивільного процесуального кодексу України від 18 березня 2004 року № 1618-IV [2] (далі – ЦПК України). Згідно з положеннями статті 100 ЦПК України електронними доказами є інформація в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи, зокрема, електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), вебсайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі [2].

Відповідно до положень чинного ЦПК України електронні докази можуть зберігатися, зокрема, на портативних пристроях (картах пам’яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (в тому числі в мережі Інтернет) [2].

Отже, використання всесвітньої мережі Інтернет, сучасних комунікаційних та інших технологій стало одним із новітніх способів вчинення злочинів. Причетними до таких злочинів стають різні категорії правопорушників. Це і раніше судимі особи й організовані злочинні групи, що намагаються у такий спосіб приховати свою злочинну діяльність від правоохоронних органів, уникнути безпосереднього контакту з потерпілою особою чи правоохоронцями тощо. Як наслідок, можливість бути затриманими «на гарячому» знижується. Виступаючи в якості організаторів кримінальних правопорушень, зазначені особи активно залучають до їх вчинення осіб, які мають спеціальні знання в галузі інформаційних технологій (наприклад, для створення вебсайтів, блогів, телеграм-ботів, технічної підтримки їх функціонування та ін.), молодь з-поміж осіб, які мають бажання активно урізноманітнити своє життя, «спробувати все», у тому числі й вчинення кримінальних правопорушень. Як приклад – спілкування в Інтернеті із

покупцями, для зняття з карткових рахунків перерахованих ними грошових коштів та передачі їх організаторам злочинних оборудок тощо.

Злочинці використовують сучасні комунікаційні технології, зашифровані мережеві інтернет-ресурси, псевдоніми, кодові слова, дотримуються заходів конспірації, координують свої дії та здійснюють обмін інформацією за допомогою різних телекомунікаційних мереж і мобільних додатків (застосунків). Зазначені додатки мають властивості технології наскрізного шифрування, що дозволяє читати повідомлення лише учасникам листування (наприклад, WhatsApp) або мають функцію «секретний чат», повідомлення в якому видаляються автоматично залежно від часу, встановленого користувачем, та на серверах листування теж не зберігається (наприклад, Telegram). Зазначене суттєвим чином ускладнює виявлення та розслідування досліджуваних кримінальних правопорушень.

Саме тому зазначаємо те, що кіберпростір та шахрайство зокрема, що здійснюються в його межах, є об’єктом підвищеної уваги у сучасній правовій науці та практиці, зокрема у контексті забезпечення кібербезпеки та боротьби з кіберзлочинністю. Відповідно до предмета даного дослідження нам необхідно проаналізувати поняття «кіберзлочин», визнати сутність даного протиправного явища та надати авторське бачення їх класифікацію.

Отже, практика протидії правоохоронними органами злочинності свідчить про те, що одним із поширених кіберзлочинів є шахрайство [3], яке вчиняється за допомогою кіберпростору. Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» [4] (далі – ЗУ) «кіберпростір» визначається як середовище (віртуальний простір), що надає можливості для комунікацій і реалізації суспільних відносин, утворене через функціонування взаємопов’язаних комунікаційних систем та електронних комунікацій із використанням Інтернету та/або інших глобальних мереж передачі даних. «Кіберзлочин» (комп’ютерний злочин) – це суспільно небезпечне винне діяння, учинене у кіберпросторі чи з його використанням, відповідальність за яке передбачена кримінальним законодавством України або міжнародними договорами України.

На сьогодні не розроблено чітких рекомендацій чи інструкцій щодо визначення кримінальних правопорушень, учинених у кіберпросторі, як кіберзлочинів. Серед наукової спільноти та практиків відсутня єдність у підходах до цього питання, що ускладнює формування загальновизнаних критеріїв для віднесення протиправних діянь до зазначеної категорії. Як наслідок, відсутність систематизованого переліку таких злочинів унеможливлює забезпечення об'єктивної статистики щодо рівня кіберзлочинності. Науковцями пропонуються різні дефініції кіберзлочинів. Наприклад, кіберзлочини визначаються як кримінальні правопорушення, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), телекомунікаційних систем, комп'ютерних мереж і мереж електрозв'язку. Інший підхід розглядає кіберзлочинність як сукупність злочинів, що здійснюються в кіберпросторі зі застосуванням комп'ютерних систем, мереж або спрямованих проти них.

Стосовно наукових підходів до визначення понять «кіберзлочин» і «кіберзлочинність» слід зазначити, що більшість дослідників пов'язують їх із специфічним предметом злочину – комп'ютерними даними або технікою, способом вчинення (з використанням комп'ютерів і мереж) або місцем вчинення злочину – кіберпростором. Таким чином, кіберзлочинність охоплює широкий спектр кримінальних правопорушень, що значно ускладнює розробку системи їхньої класифікації. До таких злочинів належать діяння, спрямовані на отримання фінансової вигоди, злочини, пов'язані з використанням інформації, що зберігається у комп'ютерних системах, а також правопорушення, які порушують конфіденційність, цілісність і доступність цих систем [5, с. 46].

Кіберзлочинність можна визначити як сукупність злочинів, що здійснюються в кіберпросторі із застосуванням комп'ютерних систем, мереж або інших засобів доступу до кіберпростору, а також злочинів, спрямованих на комп'ютерні системи, мережі чи комп'ютерні дані або таких, що відбуваються в їх межах.

Стосовно наукових підходів до визначення понять «кіберзлочин» і «кіберзлочинність» слід пояснити, що вчені переважно пов'язують їх зі

специфічним предметом злочину – комп'ютером (комп'ютерною технікою) чи комп'ютерними даними та способом вчинення злочину – з використанням вищевказаних предметів для вчинення злочину або з певним місцем його вчинення, яким є кіберпростір [6, с. 156]. Особливості кіберпростору є відсутність фізичного контакту з потерпілими – фізичними та юридичними особами, представниками фінансових установ, а також анонімність, швидкість дій і низька вартість здійснення злочинів. Означене стало ключовими факторами, що сприяють зростанню зацікавленості злочинців можливостями, які надають сучасні інформаційні технології.

Таким чином, поняття «кіберзлочинність» охоплює широкий спектр кримінальних правопорушень, що значно ускладнює розробку системи їхньої типології чи класифікації. До кіберзлочинів належать діяння, спрямовані на отримання фінансової вигоди, злочини, пов'язані з використанням інформації, що зберігається у комп'ютерних системах, а також правопорушення, які порушують конфіденційність, цілісність і доступність цих систем.

Відповідно, особливістю шахрайств, учинених у кіберпросторі, є їхній цифровий характер, що створює нові виклики для правоохоронної діяльності. До таких викликів належать складнощі у встановленні цифрових слідів, аналізі їх взаємозв'язків та ідентифікації суб'єктів злочинної діяльності. Відсутність фізичних кордонів у кіберпросторі дозволяє злочинцям діяти з будь-якої точки світу, використовуючи технології забезпечення анонімності, що суттєво ускладнює розслідування.

Отже, наразі в Кримінальному кодексі України (далі – КК України) відсутній чіткий перелік статей, які однозначно можна віднести до кіберзлочинів. Як у національному, так і в міжнародному законодавстві, досі немає уніфікованого підходу до визначення критеріїв, за якими протиправні дії класифікуються як кіберзлочини [7, с. 116].

Кримінальна відповідальність за кіберзлочини передбачена різними розділами та статтями КК України. Передусім кримінально-правовий обсяг поняття «кіберзлочинність» складають злочини, передбачені статтями:

– 361 («Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв'язку»);

– 361-1 («Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут»);

– 361-2 («Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї»);

– 363 («Порушення правил експлуатації електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку, чи правил захисту інформації, яка в них оброблюється»);

– 363-1 («Перешкоджання роботі електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв’язку»).

При цьому з низки різних кримінальних правопорушень, кваліфікуючою ознакою є використанням інформаційно-телекомунікаційних систем чи технологій. Для прикладу доведення до самогубства особи через погрозу розповсюдити інформацію за допомогою інформаційно-телекомунікаційних технологій, злочини у сфері моральності, торгівля людьми, створення порнографічного контенту, при незаконному обігу наркотиків, зброї, вибухівки та боєприпасів тощо.

Також кримінальна відповідальність за кіберзлочини передбачена ч. 3 ст. 190 «Шахрайство», тобто за шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки; ст. 200 «Незаконні дії з документами на переказ, платіжними картками та іншими

засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення».

Крім того, про комп'ютери, комп'ютерні програми та інші спеціальні пристрої як засоби вчинення злочинів зазначено у ст. 163 «Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер»; ст. 176 «Порушення авторського права і суміжних прав» КК України.

Таким чином, ключовою, системоутворюючою категорією кіберзлочинів є правопорушення, пов'язані з використанням електронно-обчислювальних машин (комп'ютерів), інформаційних систем, комп'ютерних мереж та мереж електрозв'язку. Відповідно сукупність кіберзлочинів чинним законодавством визнається як кіберзлочинність [8].

Загалом у структурі кіберзлочинності в Україні домінують злочини, пов'язані з несанкціонованим втручанням у роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК України) [6, с. 161].

Під час класифікації кіберзлочинів доцільно враховувати міжнародні нормативно-правові акти, зокрема Конвенцію Ради Європи про кіберзлочинність, яка була прийнята в Будапешті 23 листопада 2001 року зазначена Конвенція є базовим документом для уніфікації підходів до визначення та протидії таким злочинам. Ця Конвенція, ратифікована Законом України від 07.09.2005 р. № 2824-IV [9], класифікує правопорушення в кіберсфері на чотири основні групи, до яких згодом Додатковим протоколом було додано ще п'яту. Класифікація, запропонована Конвенцією, вважається еталонною, оскільки саме на її основі сформовано більшість міжнародних і регіональних нормативно-правових документів, а також наукових підходів до визначення кіберзлочинів.

Отже, Будапештська Конвенція Ради Європи про кіберзлочинність 2001 року [10], яка є основоположним документом у сфері боротьби з кіберзлочинністю, разом із Додатковим протоколом, що стосується криміналізації дій расистського та ксенофобного характеру, вчинених із

використанням комп'ютерних систем, пропонує умовну класифікацію кіберзлочинів. Ця класифікація поділяє кіберзлочини на кілька категорій [11]:

1) правопорушення проти конфіденційності, цілісності та доступності комп’ютерних даних і систем (так звані «CIA-злочини»), зокрема:

– незаконний (несанкціонований) доступ, наприклад, шляхом злому, обману та іншими засобами;

– нелегальне (незаконне) перехоплення комп'ютерних даних;

– втручання у дані, включаючи навмисне пошкодження, знищення, погіршення, зміну або приховування комп’ютерної інформації без права на це;

– втручання у систему, включаючи навмисне створення серйозних перешкод функціонуванню комп’ютерної системи, наприклад, шляхом розподілених атак на ключову інформаційну інфраструктуру;

– зловживання пристроями, тобто виготовлення, продаж, придбання для використання, розповсюдження пристроїв, комп’ютерних програм, комп’ютерних паролів або кодів доступу з метою вчинення «CIA-злочинів»;

2) правопорушення, пов’язані з комп’ютерами, включаючи підробку і шахрайство, вчинені з використанням комп’ютерів. Тобто це правопорушення, пов’язані з використанням комп’ютерів як засобу вчинення протизаконних дій, тобто засобу маніпуляції з інформацією;

3) правопорушення, пов’язані зі змістом інформації (з контентом, тобто змістом даних, що розміщені в комп’ютерних мережах), зокрема правопорушення, пов’язані з дитячою порнографією;

4) правопорушення, пов’язані з порушенням авторських та суміжних прав, наприклад, незаконне відтворення і використання комп’ютерних програм, аудіо/відео та інших видів цифрової продукції, а також баз даних і книг;

5) дії расистського та ксенофобного характеру, вчинені через комп’ютерні системи: поширення расистського та ксенофобного матеріалу через комп’ютерні системи; погроза з расистських та ксенофобних мотивів; образа з расистських та ксенофобних мотивів; заперечення, значна мінімізація, схвалення або виправдання геноциду чи злочинів проти людства.

Таким чином, хоча на сьогодні немає загальноприйнятого визначення терміна «кіберзлочин», серед наукової спільноти та експертів у сфері кібербезпеки сформувалося достатньо ґрунтовне уявлення про його сутність, механізми здійснення, а також пов’язані з ним загрози та ризики. Це створює основу для розроблення та впровадження заходів протидії кіберзлочинності як суспільно небезпечному явищу.

З урахуванням практики протидії злочинам, які вчиняються з використанням кіберпростору зазначаємо те, що до виявлення, розкриття та розслідування кіберзлочинів залучаються представники різних правоохоронних органів України. Тому пропонуємо авторське бачення щодо класифікації кіберзлочинів та визначити за основу функціональну відомчу належність розкриття та розслідування кіберзлочину залежно від компетенції правоохоронного органу [12].

Функціональна відомча належність розкриття та розслідування злочинів дозволяє нам зазначити те, що Служба безпеки України (далі – СБУ) комплексно забезпечує контррозвідувальний захист інформаційної та кібернетичної безпеки держави [13]. Відповідно до пріоритетних завдань на цьому напрямі діяльності СБУ відноситься:

– запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства у кіберпросторі;

– здійснення контррозвідувальних та оперативно-розшукових заходів, спрямованих на боротьбу з кібертероризмом і кібершпигунством. При цьому під кібертероризмом чинним законодавством визнається терористична діяльність, що здійснюється у кіберпросторі або з його використанням, а під кібершпигунством – шпигунство, що здійснюється у кіберпросторі або з його використанням [4];

– протидія кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави;

– розслідування кіберінцидентів і кібератак на державні електронні інформаційні ресурси, критичну інформаційну інфраструктуру;

– протидія проведенню проти України спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуації [13].

Для прикладу зазначаємо те, що в умовах повномасштабної агресії росії проти України наша держава зазнає не лише обстрілів чи ракетно-дронові акати на об'єкти критичної інфраструктури, а і кіберзагрози та кібератаки. Відповідно Законом України «Про критичну інфраструктуру» від 16 листопада 2021 року № 1882-IX [14] під охороною об'єктів критичної інфраструктури необхідно розуміти комплекс режимних, інженерних, інженерно-технічних та інших заходів (крім заходів із захисту інформації та кіберзахисту об'єктів критичної інформаційної інфраструктури), які організовуються і проводяться суб'єктами національної системи захисту критичної інфраструктури з метою запобігання та/або недопущення чи припинення протиправних дій (актів несанкціонованого втручання) на об'єктах критичної інфраструктури [14].

Своєю чергою функціональна відомча належність розкриття та розслідування злочинів дозволяє констатувати те, що підрозділи кримінальної поліції, здійснюючи оперативно-розшукову діяльність та пошук інформації з відкритих джерел, спільно з органами досудового розслідування Національної поліції України [15] (далі – НПУ) ведуть боротьбу з цілою низкою кримінальних правопорушень, які можуть бути віднесені до категорії кіберзлочинів. Так підрозділи Департаменту карного розшуку НПУ спрямовують свої зусилля на протидію злочинам проти життя та здоров'я, майновим злочинам, злочинам у сфері моральності, які вчиняються з використанням за допомогою кіберпростору. Підрозділи Департаменту міграційної поліції НПУ спрямовують свої зусилля на протидії торгівлі людьми, нелегальній міграції, злочинам у сфері моральності, які вчиняються проти дітей тощо. Актуалізувалися проблемні питання не законних послуг щодо працевлаштування за кордоном, шлюбних агентств трансплантології, секс-бізнесу та порнографії тощо. Як приклад працівники поліції спільно з прикордонниками та СБУ постійно виявляють канали нелегальної міграції чоловіків.

Підрозділи Департаменту боротьби з наркозлочинністю НПУ спрямовують свою діяльність щодо виявлення механізмів незаконного обігу наркотиків, що вчиняється з використанням сучасних інформаційно-комунікаційних та інших технологій.

Особливої уваги потребує діяльність співробітників Департаменту кіберполіції НПУ. До основних засад діяльності кіберполіції відноситься:

– реалізація державної політики у сфері протидії кіберзлочинності;

– завчасне інформування населення про появу нових кіберзлочинців;

– впровадження програмних засобів для систематизації кіберінцидентів;

– реагування на запити закордонних партнерів, які будуть надходити по каналах Національної Цілодобової мережі контактних пунктів [16].

Отже, функціональна відомча належність розкриття та розслідування злочинів дозволяє нам зазначити висновок про те, що протидія кіберзлочинам належить до повноважень різних правоохоронних органів. Відповідно правоохоронці окрім традиційних слідів вчинення даних видів злочинів виявляють та документують так звані «віртуальні» (або «цифрові» чи «комп'ютерні») сліди. При цьому зазначені обставини значно ускладнюють процес розслідування та фіксації обставин підготовки й вчинення злочинів, зокрема шахрайств, унеможливлюють свідчення підозрюваних або свідків про особливості зовнішності злочинців, а також їх впізнання. До того ж використання злочинцями сучасних телекомунікаційних та інших технологій, комп'ютерно-технічних засобів та мережі Інтернет в якості способу вчинення злочину вимагає від слідчого, детектива і працівника оперативного підрозділу не лише якісного володіння навичками поводження з комп'ютерною технікою та програмами, але й навичками пошуку, виявлення, фіксації та копіювання інформації, що міститься на комп'ютерах, смартфонах, різноманітних цифрових носіях інформації та телекомунікаційних засобах, на інтернет-ресурсах тощо. Зокрема зафіксувати електронний документ [17], який створений, переданий, збережений і перетворений електронними засобами у візуальну форму або провести автентифікацію, під якою законодавець розуміє електронний процес, що дає змогу підтвердити електронну ідентифікацію фізичної, юридичної особи,

інформаційної або інформаційно-комунікаційної системи та/або походження та цілісність електронних даних [18]. Відповідно електронна ідентифікація – це процес використання ідентифікаційних даних особи в електронній формі, які однозначно визначають фізичну, юридичну особу або уповноваженого представника юридичної особи [18].

Отже, на тепер кіберпростір разом з іншими фізичними просторами визнано одним з можливих театрів воєнних дій [19]. При цьому зростає технічний рівень реалізації кіберзагроз, вдосконалюються та розробляються нові інструменти та механізми кібератак на об’єкти критичної інфраструктури, реалізуються нові механізми вчинення шахрайств в кіберпросторі, як спеціальних інформаційних операцій щодо маніпулювання думкою чи введення в оману особи, яка може стати жертвою кіберзлочинців. Саме тому, згідно з положенням Стратегії кібербезпеки України, яка затверджена Указом Президента України від 26 серпня 2021 року № 447/2021: «Україна має бути здатною забезпечити свій соціально-економічний розвиток у цифровому світі, що вимагає набуття спроможності ефективно стримувати деструктивні дії в кіберпросторі, досягнення кіберстійкості на всіх рівнях та взаємодії всіх суб'єктів забезпечення кібербезпеки, яка ґрунтується на довірі». Відповідно протидія різним проявам кіберзлочинів є базисною основою забезпечення кіберстійкості в кіберпосторі.

1.2 Сутність шахрайств у кіберпросторі: види, особливості та методи здійснення

Шахрайство у кіберпросторі набуло особливої актуальності в контексті глобальних викликів, таких як пандемія COVID-19 та війна росії проти України. Злочинна діяльність у кіберсередовищі обумовлена специфікою цифрового простору та його здатністю адаптуватися до суспільно-економічних змін, створюючи нові можливості для маніпуляцій і незаконного збагачення.

Одним із ключових чинників, що сприяли поширенню кіберзлочинів, є інтенсивна цифровізація суспільства. Зростання використання Інтернету, спричинене карантинними обмеженнями, воєнним станом і переходом значної

частини соціально-економічної діяльності у цифровий формат, істотно збільшило обсяги онлайн-активності громадян. Поширення дистанційної роботи, онлайн-торгівлі та цифрових платформ для комунікації стало каталізатором розвитку шахрайських схем, спрямованих на зловживання довірою користувачів і викрадення персональних даних.

Ще одним важливим фактором є психоемоційна вразливість населення, яка виникла в умовах пандемії та воєнних дій. Масові страхи, тривожність і почуття нестабільності стали інструментами, які шахраї активно використовують для маніпуляцій. Наприклад, вони створюють фіктивні благодійні ініціативи, пропонують псевдомедичні послуги або засоби захисту від вірусу, що дозволяє їм отримувати незаконний доступ до фінансових ресурсів громадян.

Також значний вплив на зростання кіберзлочинності має економічна дестабілізація, яка спричинила фінансові труднощі у значної частини населення. Зловмисники використовують цей контекст, пропонуючи фіктивні вакансії, неправдиві обіцянки швидкого заробітку або програми «фінансової допомоги». Ці методи особливо поширені через їх здатність експлуатувати потреби громадян у кризовий період.

Дезінформація є ще одним потужним інструментом шахраїв. У період збройного конфлікту та інформаційної війни поширення фейкових новин, ланцюгових повідомлень та інших видів оманливої інформації стало важливим засобом отримання доступу до персональних даних і фінансових ресурсів. Шахраї використовують дезінформацію для створення атмосфери недовіри та хаосу, що ускладнює ідентифікацію справжніх загроз.

Не менш значущим аспектом є трансформація поведінкових моделей користувачів Інтернету. Масовий перехід до електронної комерції, зростання популярності онлайн-сервісів та соціальних платформ суттєво збільшили ризики потрапляння на шахрайські вебресурси. Зловмисники створюють фішингові вебсайти, які імітують легальні платформи, або використовують соціальну інженерію для отримання доступу до конфіденційної інформації користувачів.

Таким чином, шахрайство у кіберпросторі має комплексний характер, обумовлений взаємодією соціальних, психологічних та економічних факторів.

Злочинна діяльність у цифровому середовищі вирізняється високою адаптивністю, використанням сучасних інформаційних технологій і можливістю масштабного охоплення потенційних жертв. Усе це підкреслює необхідність розробки науково обґрунтованих підходів до виявлення та протидії шахрайству, враховуючи специфіку його методів і масштабів впливу на суспільство [20].

Проблематиці шахрайств, учинених у кіберпросторі в Україні, приділяли увагу такі вітчизняні науковці, як О. В. Бишевець, О. С. Белицький, Т. С. Вайда, В. В. Винник, В. М. Галунько, Л.П. Гринько, Н.О. Думанський, О. М. Джужа, Л. М. Івашко, О.В. Клювак, Т.В. Коршикова, О.І. Кривенко, А. Б. Мізерак, Л. М. Прудка, Д.В. Перепелиця, Т. В. Романенко, Я. П. Руденко, В. П. Сабадаш, О. А. Самойленко, І. В. Сабадаш, Н. В. Сметаніна, І. А. Федчак, І. М. Чекмарьова, С. С. Чернявський, С. В. Шапочка, О М. Юрченко та інші. У своїх дослідженнях вони розглядали загальні аспекти злочинів, що вчиняються в кіберпросторі, зокрема інтернет-шахрайства у мирний час. Вивченням шахрайств, які здійснюються в мережі Інтернет в умовах воєнного стану, займалися такі науковці, як О. М. Брисковська, М. О. Гелемей, Я. В. Левківська, М. Є. Собаченко та В. Г. Телійчук.

Шахрайство є одним із найбільш поширених видів кримінальних правопорушень проти власності в багатьох кримінально-правових системах, зокрема й в Україні. З урахуванням тенденції до зростання кількості випадків майнових посягань через шахрайські дії, протидія цим правопорушенням залишається одним із ключових завдань правоохоронних органів. Вчинення таких злочинів не лише створює загрозу для майнових прав окремих осіб, але й завдає шкоди стабільності економічної системи держави, ставлячи під загрозу її ефективне функціонування.

Згідно зі статтею 190 Кримінального кодексу України, шахрайство визначається як заволодіння чужим майном або набуття права на нього шляхом обману чи зловживання довірою [1]. Це кримінальне правопорушення характеризується особливою спрямованістю, яка може стосуватися як матеріальних цінностей, так і прав на такі цінності. Важливою ознакою шахрайства є наявність прямого умислу, що передбачає усвідомлення винною

особою протиправності своїх дій, та корисливий мотив, спрямований на отримання неправомірної вигоди.

Розвиток цифрових технологій та широке розповсюдження мережі Інтернет в Україні створили нові умови для вчинення шахрайства. Завдяки доступності Інтернету для громадян різних вікових категорій злочинці отримали нові інструменти для реалізації своїх протиправних намірів. Особливість інтернет-шахрайства полягає у відсутності прямого контакту між злочинцем і жертвою, що не лише полегшує приховування особи злочинця, але й стимулює його до розробки більш складних і витончених схем заволодіння чужим майном або фінансовими ресурсами.

До шахрайств, учинених у кіберпросторі, належать численні види злочинів, які використовують цифрові технології для маніпуляцій, обману та незаконного отримання вигоди.

Основна підкатегорія, що спостерігається в даному контексті, полягає у недоставленні замовлень, оформлених через інтернет-ресурси. Це явище охоплює операції з купівлі-продажу товарів у цифрових торгівельних майданчиках, розміщення оголошень про надання певних послуг та отримання попередньої часткової або повної оплати за такі послуги чи товари. Подібні випадки демонструють значну загрозу у сфері електронної комерції та створюють ризики для фінансової безпеки користувачів, оскільки недобросовісні дії можуть супроводжуватися як навмисними шахрайськими схемами, так і порушенням договірних зобов’язань. Зростання активності подібних схем зумовлене широкомасштабним переходом суб’єктів підприємницької діяльності на онлайн-платформи. Такий формат дозволяє оптимізувати операційні витрати, зокрема, усунути необхідність оренди фізичних комерційних приміщень, що, своєю чергою, сприяє формуванню більш доступних і конкурентних цін на товари та послуги, підвищуючи їхню привабливість для кінцевих споживачів.

Серед найпоширеніших методів кіберзлочинності, поряд із недоставленням товарів чи послуг, особливе місце займають техніки соціальної інженерії, які використовуються для маніпуляції свідомістю користувачів. Одним із

найнебезпечніших проявів таких технік є фішинг, який забезпечує зловмисникам доступ до конфіденційної інформації жертв за допомогою обману. Цей тип шахрайства здобув особливу популярність завдяки зростанню використання цифрових платформ і недостатньому рівню кіберграмотності серед населення.

Фішинг – це вид шахрайства, заснований на маніпулятивних прийомах, що дозволяють отримувати персональні дані користувачів, такі як паролі, номери банківських карток, логіни до облікових записів тощо. В основі фішингових атак лежить введення користувача в оману, що призводить до добровільної передачі своїх даних зловмисникам. Фішинг може бути реалізований у різних формах і націлений як на окремих осіб, так і на організації.

Основні типи фішингових атак:

Електронні листи (Email Phishing) (див. рисунок 1.1): зловмисники надсилають підроблені електронні листи, що імітують повідомлення від банків, соціальних мереж або інших легітимних організацій. У таких листах зазвичай містяться фальшиві посилання або шкідливі вкладення.

Смішинг (Smishing): атаки через текстові повідомлення на мобільні пристрої. Зазвичай зловмисники надсилають посилання, які перенаправляють на фальшиві сайти, або використовують повідомлення для збору конфіденційної інформації.

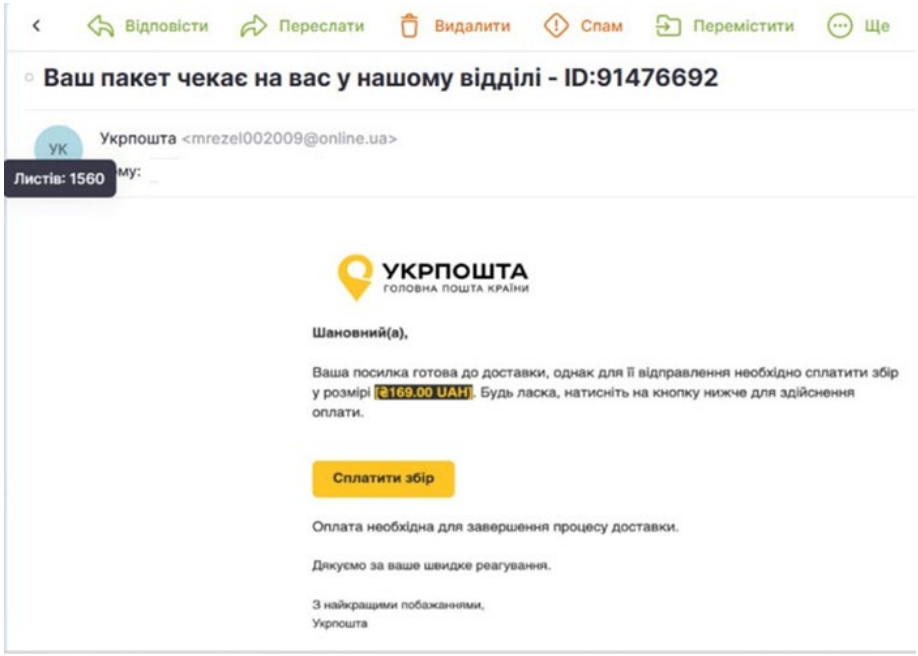

Рисунок 1.1 – Приклад фішингового електронного листа

Вішинг (Vishing): використання телефонних дзвінків, під час яких шахраї видають себе за представників банків, служб підтримки чи інших організацій, аби змусити жертв розкрити конфіденційні дані.

Фішинг через соціальні мережі: зловмисники використовують фальшиві профілі або повідомлення, які імітують спілкування з друзями чи відомими брендами, для отримання доступу до персональних даних.

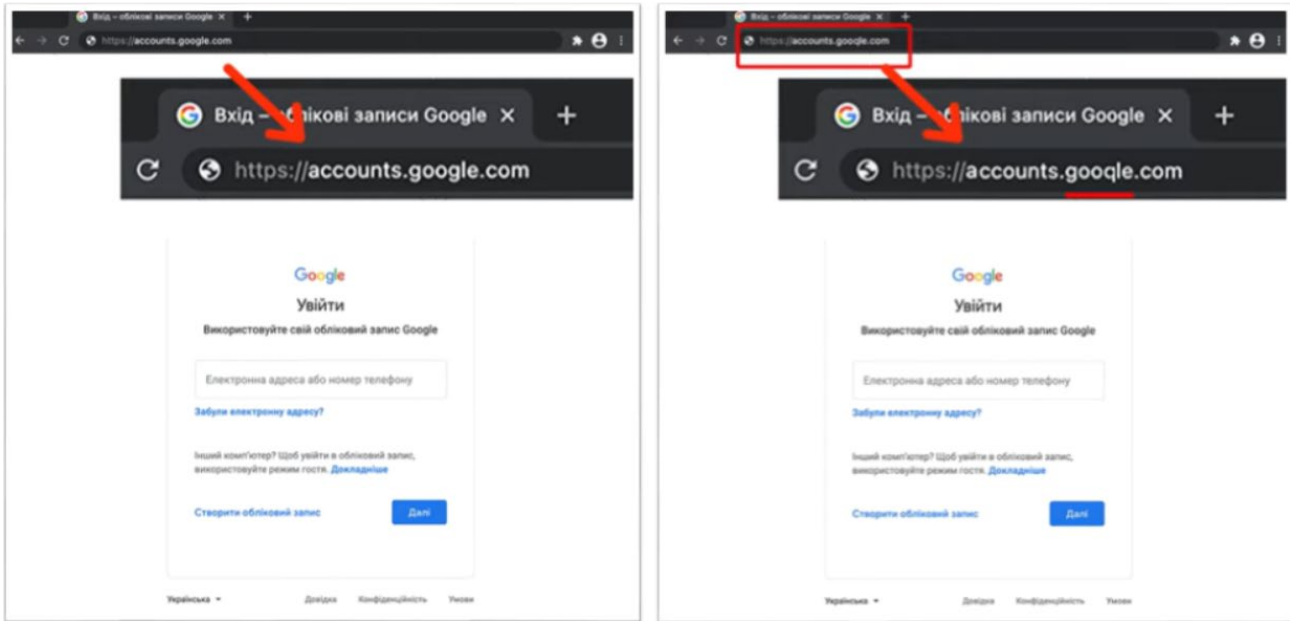

Рисунок 1.2 – Приклад фішингового сайту

Фішингові сайти (Web Phishing) (див. рисунок 1.2): створення вебсайтів, які імітують легітимні ресурси, щоб викрадати інформацію користувачів через форми для входу або оплату.

Зі зростанням використання штучного інтелекту фішинг стає дедалі складнішим для виявлення. Зловмисники використовують автоматизацію для створення персоналізованих повідомлень, які важче розпізнати як шахрайські. Це вимагає більш інтегрованого підходу до захисту, що включає технічні рішення, освітні програми та міжнародну співпрацю для боротьби з кіберзагрозами.

Фішинг залишається однією з найсерйозніших кіберзагроз сучасності, яка потребує комплексних заходів захисту та постійного вдосконалення механізмів протидії.

Також доцільно звернути увагу на шкідливе програмне забезпечення (ШПЗ), яке часто виступає невід'ємним інструментом для реалізації фішингових атак. Шкідливе програмне забезпечення (malware) є однією з найпоширеніших загроз, що використовується для досягнення різних злочинних цілей, таких як викрадення конфіденційної інформації, порушення функціонування систем або шантаж. Зазвичай ШПЗ поширюється через фішингові посилання або вкладення, що маскуються під легітимні файли або програми. У поєднанні з персоналізованими фішинговими повідомленнями, які створюються за допомогою штучного інтелекту, ШПЗ стає особливо небезпечним, оскільки може проникати у системи навіть досвідчених користувачів.

Кібербулінг є складним соціальним явищем, що виникло внаслідок стрімкого розвитку інформаційно-комунікаційних технологій та зростаючої інтеграції цифрових платформ у повсякденне життя. Він являє собою форму агресивної поведінки, яка реалізується через онлайн-середовище з метою психологічного тиску, приниження або дискредитації особи.

Ця форма агресії проявляється через використання цифрових платформ для залякування, приниження, шантажу або дискредитації особи. Характерними рисами кібербулінгу є його систематичність, публічний характер і можливість анонімності кривдників, що створює додаткові виклики для виявлення та запобігання цьому явищу.

Його наслідки можуть бути глибокими й мати серйозний вплив на жертву, включаючи емоційне виснаження, соціальну ізоляцію та зниження самооцінки. Фактори, які сприяють поширенню кібербулінгу, включають зростаючу доступність цифрових технологій, низький рівень обізнаності про основи кібербезпеки, а також недостатню ефективність законодавчих механізмів у боротьбі з подібними явищами.

Серед найбільш поширених шахрайських схем у сфері криптовалют виділяють кілька ключових видів. По-перше, це обман через соціальні мережі, де зловмисники створюють фейкові акаунти, імітуючи відомих осіб чи компанії, щоб переконати користувачів інвестувати в шахрайські проєкти. По-друге,

широко застосовується соціальна інженерія, коли злочинці маніпулюють емоціями жертв, змушуючи їх передавати доступ до своїх криптогаманців.

Особливу увагу привертають маніпуляції з первинним розміщенням монет (ICO). Зловмисники створюють фіктивні проєкти, обіцяючи високий дохід, але зникають одразу після збору коштів. Крім того, під виглядом криптоінвестиційних фондів шахраї обіцяють користувачам гарантований прибуток, що часто є частиною фінансових пірамід.

Шахрайство в хмарному майнінгу також становить серйозну загрозу, коли під приводом надання послуг із видобутку криптовалюти через хмарні платформи злочинці отримують кошти користувачів, не виконуючи жодних реальних операцій. Усі ці схеми вимагають особливої уваги та вдосконалення методів кібербезпеки для захисту криптоактивів.

В умовах воєнного конфлікту зловмисники активно використовують уразливості суспільства для реалізації специфічних шахрайських схем, які набули поширення саме через актуальні обставини. До таких схем належать фіктивні збори коштів на потреби армії, маніпуляції з оголошеннями про зниклих безвісти або полонених осіб, а також поширення підроблених повідомлень про евакуацію, що вимагають попередньої оплати або «фінансової допомоги».

Ці шахрайські дії спрямовані на експлуатацію емоційного стану жертв, викликаного страхом, тривогою або прагненням допомогти в умовах кризи. Зловмисники активно адаптують свої методи до актуальних реалій, використовуючи соціальні платформи, мобільні додатки та інші засоби цифрової комунікації для досягнення своїх цілей. Шахрайство нерідко базується на техніках соціальної інженерії, таких як створення довірливих ситуацій або вплив на почуття відповідальності, що змушує громадян передавати кошти або персональні дані.

Ключовими інструментами шахраїв є комп’ютерна техніка, мобільні пристрої, банківські рахунки, зареєстровані на підставних осіб, та спеціалізоване програмне забезпечення. Крім того, для реалізації таких схем активно використовуються інтернет-платформи, які дозволяють швидко поширювати

дезінформацію, підроблені сайти та оголошення. Ефективність шахрайства часто підкріплюється високим рівнем технологічного оснащення зловмисників, що дозволяє їм адаптувати свої дії до змінюваних умов та залишатися непомітними для правоохоронних органів.

Таким чином, шахрайство у воєнний час набуває унікальних рис, які обумовлені специфікою соціально-економічної ситуації та масштабами використання цифрових технологій. Це підкреслює необхідність удосконалення механізмів захисту громадян, зокрема через підвищення рівня цифрової грамотності, впровадження жорсткіших регуляторних норм та розробку ефективних інструментів моніторингу та протидії [21].

Узагальнюючи викладене, можна зробити висновок, що ефективна протидія шахрайству у кіберпросторі, особливо в умовах воєнного часу, потребує системного підходу. Ключовими методами боротьби є підвищення цифрової грамотності громадян, впровадження сучасних технологій для моніторингу та виявлення шахрайських схем, а також удосконалення правових механізмів, спрямованих на регулювання онлайн-діяльності. Особливу увагу слід приділити розробці інформаційних кампаній для підвищення обізнаності суспільства про загрози, пов’язані з кіберзлочинністю, і необхідності відповідальної поведінки в цифровому середовищі. Лише завдяки інтегрованим зусиллям держави, громадянського суспільства та технологічних платформ можливо забезпечити ефективний захист від загроз у кіберпросторі [22].

РОЗДІЛ 2 ОСОБЛИВОСТІ ВИКОРИСТАННЯ OSINT-ТЕХНОЛОГІЙ У РОЗКРИТТІ ШАХРАЙСТВ, УЧИНЕНИХ У КІБЕРПРОСТОРІ

2.1 OSINT-технології у боротьбі з кіберзлочинами: поняття та використання

В умовах стрімкого розвитку інформаційних технологій, коли доступ до даних із відкритих джерел стає ключовим інструментом у сфері боротьби з кіберзлочинністю, особливого значення набувають OSINT-технології (Open Source Intelligence) – розвідка на основі відкритих джерел. Цей підхід передбачає пошук, аналіз і використання інформації з публічно доступних ресурсів для виявлення кіберзагроз, розслідування злочинів та підтримки національної безпеки. Завдяки можливості обробляти значні обсяги даних і застосовувати їх для вирішення стратегічних завдань, OSINT забезпечує ефективність і оперативність у боротьбі з сучасними кіберзагрозами. Залишаючись у межах правових та етичних норм, ця методологія дозволяє отримувати критично важливу інформацію для протидії кіберзлочинам, забезпечуючи інноваційний підхід до розв'язання проблем кібербезпеки.

Розвідка на основі відкритих джерел має багатолітню історію, яка бере свій початок ще з середини XIX століття у Сполучених Штатах Америки та початку XX століття у Великій Британії. Її розвиток можна умовно поділити на кілька етапів:

Кінець 1941 року – у США була створена Служба моніторингу іноземного мовлення (Foreign Broadcast Monitoring Service – FBMS), метою якої було дослідження радіопрограм. Завдяки діяльності цієї служби вдалося виявити взаємозв’язок між цінами на апельсини в Парижі та успішністю бомбардувань залізничних мостів під час Другої світової війни.

2005-2009 роки – у Сполучених Штатах створено центр для аналізу розвідувальних матеріалів із відкритих джерел. Це стало відповіддю на значне збільшення обсягу інформації, доступної в Інтернеті.

2009-2016 роки – відбувся стрімкий розвиток Інтернету, що суттєво вплинув на життя людей, а також підвищив роль і значення відкритих джерел інформації.

З 2016 року і до сьогодні – концепція OSINT перестала обмежуватися лише оборонною сферою. Вона почала активно застосовуватися в інших галузях людської діяльності, таких як бізнес, журналістика, освіта та криміналістика.

В Україні до 2014 року технології OSINT мали обмежене застосування і були переважно інструментом журналістів-розслідувачів. Вони використовували відкриті джерела для збору інформації, викриття корупційних схем, проведення журналістських розслідувань та створення аналітичних матеріалів. У цей період їх потенціал не був широко відомий чи розвинений у сфері безпеки чи інших стратегічних напрямах.

Ситуація кардинально змінилася після початку російської збройної агресії у 2014 році. Виклики, зумовлені військовими діями, інформаційними атаками та потребою в оперативному аналізі ситуації, дали потужний імпульс для активного розвитку та розширення використання OSINT-технологій як в Україні, так і у світі. У відповідь на ці виклики були створені платформи, що стали ключовими для моніторингу та аналізу подій:

– InformNapalm [23]: міжнародна волонтерська спільнота, яка спеціалізується на використанні OSINT для збору доказів участі російських військових у конфліктах, документування порушень міжнародного права та викриття інформаційних маніпуляцій. Ця платформа об’єднує волонтерів із різних країн, які аналізують відкриті джерела, включаючи соціальні мережі, супутникові знімки, фотографії та відеоматеріали. Особлива увага приділяється розкриттю фактів агресії росії проти України, зокрема ідентифікації російських військовослужбовців, техніки та доказів їхньої присутності на окупованих територіях. Матеріали InformNapalm активно використовуються для привернення уваги міжнародної спільноти до російських злочинів, формування санкційної політики та забезпечення правосуддя.

– Molfar [24]: аналітична група, яка спеціалізується на зборі та аналізі відкритих даних, використовуючи сучасні OSINT-інструменти для розслідувань, стратегічного консалтингу та прогнозування. Основними напрямами діяльності групи є виявлення інформаційних загроз, розслідування кіберзлочинів, аналіз ринків і конкурентного середовища, а також підтримка корпоративного сектора

у виявленні ризиків. Molfar активно використовує дані з відкритих джерел, включаючи соціальні мережі, цифрові бази даних, геолокаційні сервіси та супутникові знімки, що дозволяє їм забезпечувати високу точність і релевантність аналітики.

– «Миротворець» [25]: українська платформа, яка спеціалізується на ідентифікації осіб, причетних до злочинів проти державної безпеки України, терористичної діяльності, сепаратизму та інших антидержавних дій. Платформа використовує дані з відкритих джерел, таких як соціальні мережі, офіційні заяви, фотографії та відеозаписи, для створення профілів осіб, які становлять загрозу для національної безпеки. База «Миротворця» включає інформацію про терористів, найманців, колаборантів, а також тих, хто сприяє інформаційній війні проти України. Зібрані дані використовуються правоохоронними органами, державними структурами та міжнародними організаціями для проведення розслідувань, обґрунтування санкцій та притягнення до відповідальності осіб, причетних до злочинів. Платформа також відіграє важливу роль у протидії дезінформації та підтримці інформаційної безпеки України.

Ці ініціативи не лише продемонстрували ефективність OSINT у розв’язанні нагальних завдань, але й стали символом адаптації України до умов сучасної гібридної війни.

Міжнародну увагу до можливостей OSINT привернула дослідницька група Bellingcat [26], яка стала одним із найвідоміших прикладів професійного аналізу відкритих джерел. Група здобула широку популярність завдяки своїм детальним розслідуванням, зокрема у справі збиття малайзійського рейсу MH17. Використовуючи супутникові знімки, дані соціальних мереж, геолокаційні сервіси та інші відкриті джерела, Bellingcat зуміла відтворити маршрут переміщення системи «Бук», яка була використана для атаки, та встановити причетність російських військових до цієї трагедії.

Їхній підхід продемонстрував, як OSINT може ефективно застосовуватися для встановлення фактів, навіть у контексті гібридної війни та дезінформаційних кампаній. Водночас Bellingcat наголосила на важливості прозорості, підзвітності та верифікації даних у сучасній журналістиці й аналітиці. Їхні дослідження стали

прикладом того, як можна використовувати відкриті дані для боротьби з пропагандою, розвінчання фейкових наративів і забезпечення доступу до об'єктивної інформації. Це значно підвищило довіру до OSINT як до інструмента, здатного забезпечити правду та справедливість на глобальному рівні [27].

У правоохоронній діяльності OSINT є потужним інструментом для розслідування шахрайських дій у кіберпросторі. Цей підхід дозволяє аналізувати цифрові сліди, які злочинці залишають у відкритих джерелах, таких як вебсайти, блоги, форуми та соціальні мережі. Завдяки цьому правоохоронні органи отримують змогу ідентифікувати підозрюваних, виявляти їхні зв’язки з іншими особами, досліджувати методи, які використовуються для реалізації шахрайських схем, та аналізувати фінансові транзакції, пов’язані зі злочинами. Наприклад, OSINT дозволяє відстежувати активність підозрюваних у соціальних мережах, знаходити спільників, а також виявляти вебресурси, які використовуються для координації злочинної діяльності. Це значно підвищує ефективність розслідувань, надаючи можливість уповноваженим суб’єктам отримувати важливу інформацію швидко та цілеспрямовано [28].

OSINT відіграє важливу роль у забезпеченні кібербезпеки, дозволяючи виявляти загрози на ранніх стадіях, такі як фішингові кампанії, витоки даних або атаки, пов’язані з використанням вразливостей у програмному забезпеченні. Аналітики застосовують OSINT для постійного моніторингу кіберпростору, відстежуючи підозрілу активність у реальному часі на форумах, у соціальних мережах та на спеціалізованих платформах. Це дає можливість попереджати потенційні атаки до їхнього здійснення.

У бізнес-аналітиці OSINT також має широке застосування, допомагаючи компаніям зібрати конкурентну інформацію, проаналізувати репутаційні ризики та моніторити ринкові тренди. Підприємства використовують OSINT для відстеження дій конкурентів, аналізу відгуків клієнтів, ідентифікації потенційних загроз або виявлення слабких місць у власній діяльності. Завдяки отриманій інформації компанії можуть приймати більш обґрунтовані рішення щодо стратегії розвитку, управління ризиками та адаптації до ринкових змін.

Ключовою перевагою OSINT є можливість інтеграції даних з різних джерел для створення цілісного уявлення про об’єкт дослідження або діяльність злочинців. Такий підхід дозволяє зіставляти великі обсяги інформації, виявляти закономірності, аналізувати взаємозв’язки та формувати прогнози. Наприклад, аналіз взаємодії користувачів у соціальних мережах дозволяє ідентифікувати мережі зв’язків, прогнозувати поведінку та оцінювати ризики. У сфері боротьби з шахрайством цей підхід дозволяє виявляти вразливі точки у схемах злочинців і розробляти ефективні стратегії запобігання. OSINT забезпечує не лише оперативність і точність, а й дозволяє стратегічно планувати заходи безпеки, орієнтуючись на виявлені загрози та можливості [29].

Таким чином, OSINT-технології стали багатофункціональним інструментом, який забезпечує інтеграцію різноманітних даних для вирішення комплексних завдань у різних сферах діяльності. Їх застосування дозволяє підвищити ефективність розслідувань, запобігати злочинам та приймати стратегічно важливі рішення, які відповідають викликам сучасного цифрового середовища.

2.2 Методологія використання OSINT-технологій для збору інформації в кіберпросторі

Методологія використання OSINT-технологій для збору інформації в кіберпросторі базується на системному підході, спрямованому на отримання вірогідних і релевантних даних із відкритих джерел інтернет-простору. У сучасному цифровому середовищі, де інформація є як ресурсом, так і об’єктом маніпуляцій, критично важливо дотримуватися чітких методичних принципів. Ці принципи визначають порядок дій для пошуку, вилучення, верифікації та подальшого аналізу даних, враховуючи специфіку цифрового контексту. Такий підхід забезпечує можливість вирішення практичних завдань у розслідуванні кіберзлочинів, дозволяючи ефективно працювати з неструктурованими даними, які часто є основним джерелом доказової бази.

Одним із ключових інструментів, який можна використовувати для вдосконалення цього підходу, є практичний посібник «Протокол Берклі» [30],

створений для правоохоронців, які працюють із відкритими цифровими даними під час розслідувань. У цьому документі представлено стандарти для пошуку, збору, зберігання, перевірки та аналізу контенту зі соціальних мереж та інших відкритих джерел. Він також містить міжнародні вимоги до проведення онлайн-розслідувань і детальні рекомендації щодо роботи з цифровою інформацією, із дотриманням професійних, правових і етичних норм.

У передмові до Протоколу зазначається, що «з початку 1990-х років цифрові інструменти та інтернет, як камера і телефон перед ними, докорінно змінили спосіб отримання, збирання та поширення нами інформації про порушення прав людини та інші серйозні порушення міжнародного права, включаючи міжнародні злочини.

Сьогодні уповноважені суб’єкти можуть збирати дані про потенційні порушення прав людини та інші серйозні порушення міжнародного права, включаючи міжнародні злочини, за допомогою великої кількості загальнодоступних супутникових знімків, відео та фотографій, включаючи матеріали, завантажені в інтернет зі смартфонів, та публікацій на платформах соціальних мереж. Такий розвиток подій допоміг уповноваженим суб’єктам обійти урядових та інших традиційних контролерів інформації для доступу до ключової інформації про правопорушення, навіть у режимі реального часу, яка в іншому випадку залишалася б прихованою для очей громадськості.

Однак цифрова інформація у відкритому доступі використовувалася переважно у конкретних випадках, оскільки правозахисні організації, міжурядові органи, слідчі механізми та суди часом намагалися адаптувати свою робочу практику, щоб включити нові цифрові методи встановлення фактів та аналізу. Однією з найбільших проблем, з якими вони стикаються, є розв’язання питань виявлення та перевірки відповідних матеріалів у межах збільшення обсягу онлайн-інформації, особливо фотографій та відеозаписів, знятих на смартфони та інші мобільні пристрої, деякі з яких можуть бути скомпрометовані або неправильно віднесені.

Суди та слідчі механізми мають користуватися чіткими критеріями для оцінки ваги інформації у відкритому доступі як зв’язку або як доказу

конкретного злочину. Спільні методологічні стандарти щодо автентифікації та перевірки однаково слугуватимуть місіям з виявлення фактів у сфері прав людини, які також все частіше включають цифрові матеріали у відкритому доступі у свої розслідування» [30].

Таким чином, «Протокол Берклі» виступає не лише як практичний посібник для правоохоронців, але і як універсальний методологічний інструмент, що встановлює стандарти роботи з цифровою інформацією у відкритому доступі. Він дозволяє забезпечити надійність і вірогідність даних, адаптувати сучасні цифрові методи до традиційних механізмів розслідування та впроваджувати чіткі критерії автентифікації та верифікації матеріалів. Це робить його важливим джерелом знань для слідчих, які працюють зі складними викликами сучасного інформаційного середовища, сприяючи підвищенню якості розслідувань і зміцненню довіри до отриманих доказів.

Ефективним інструментом для ідентифікації та розкриття шахрайських дій, вчинених у кіберпросторі, через аналіз відкритих джерел інформації є OSINT Framework [31]. Ця структура забезпечує систематизацію та оптимізацію процесу збору, обробки та аналізу даних із публічних джерел, що є критично важливим у цифрових розслідуваннях.

OSINT Framework побудований на основі інтеграції численних категорій інформаційних ресурсів, включаючи соціальні медіа, доменні реєстри, бази даних, онлайн-форуми та інші відкриті джерела. Його архітектура дозволяє проводити багаторівневий пошук та аналіз, спрямований на виявлення цифрових слідів злочинної діяльності, встановлення зв’язків між суб’єктами розслідування, а також визначення закономірностей і шаблонів у їхній поведінці. Важливим аспектом цього інструменту є функція пошуку інформації за іменем користувача, яка значно полегшує доступ до релевантних даних. У межах OSINT Framework цей процес організовано максимально зручно та ефективно для аналітиків.

Однією з ключових характеристик OSINT Framework є його здатність підтримувати комплексний підхід до розслідування, що дозволяє формувати цілісне уявлення про шахрайську діяльність. Завдяки високій структурованості

та гнучкості, цей інструмент є надзвичайно ефективним у розслідуванні складних злочинних схем, таких як фінансові шахрайства, викрадення персональних даних, фішингові атаки та незаконна торгівля у цифровому середовищі.

З методологічного погляду, OSINT Framework відповідає вимогам професійної етики та правових стандартів, оскільки базується на аналізі інформації з відкритих, загальнодоступних джерел. Це робить його важливим інструментом для науково обґрунтованого підходу до вирішення завдань, пов'язаних із забезпеченням кібербезпеки, проведенням кримінальних розслідувань, вивченням інформаційних загроз та протидією злочинним угрупованням у кіберпросторі.

У переважній більшості випадків OSINT-аналіз починається із введення запиту в один із доступних інструментів пошуку. Вже на цьому етапі вибір пошукової системи відіграє важливу роль, адже саме від нього залежатиме якість і релевантність отриманих даних. Не викликає сумнівів, що серед найпоширеніших пошукових платформ в Україні та у світі лідером залишається Google, завдяки своїй здатності швидко і точно обробляти величезні обсяги інформації. Його алгоритми забезпечують релевантність результатів, а додаткові функції, такі як пошук за зображеннями (Google Images), новинами (Google News) чи науковими публікаціями (Google Scholar), роблять його універсальним інструментом для OSINT-розслідувань. Проте Google активно збирає дані про користувачів, що може бути недоліком для тих, хто прагне конфіденційності.

У таких випадках альтернативою може стати DuckDuckGo [32] – пошукова система, яка зосереджується на захисті приватності. Вона не зберігає історію пошуку, не відстежує активність користувачів і не використовує персоналізовану рекламу. Це робить її особливо корисною для аналітиків, які хочуть мінімізувати свій цифровий слід під час розслідувань. Хоч DuckDuckGo не може забезпечити такого обсягу результатів, як Google, його переваги у сфері конфіденційності є важливим фактором у багатьох ситуаціях.

Ще одним цікавим інструментом є Ecosia, який вирізняється своєю екологічною спрямованістю. Використовуючи цей сервіс, кожен пошуковий

запит сприяє фінансуванню висадки дерев у різних частинах світу. Ecosia працює на базі пошукової технології Bing, але водночас пропонує унікальну можливість підтримати екологічні ініціативи. Це робить його привабливим для користувачів, які цінують соціально відповідальний підхід.

Сам Bing також є важливим інструментом для OSINT-аналітиків, адже він пропонує унікальні алгоритми пошуку, які іноді повертають результати, недоступні через Google. Bing вирізняється своїми можливостями у пошуку мультимедіа, такими як зображення, відео чи навіть академічні ресурси. Крім того, Bing активно впроваджує інструменти штучного інтелекту для вдосконалення релевантності пошукових запитів, що може бути корисним у спеціалізованих розслідуваннях. Його інтеграція з іншими продуктами Microsoft, такими як Office 365, додає зручності для професійних користувачів.

Для більшої конфіденційності можна звернутися до Startpage, який об’єднує результати Google з функціями анонімного пошуку. Startpage не збирає дані про користувачів і не використовує куки для стеження, що дозволяє отримувати переваги алгоритмів Google без ризику для приватності.

Крім того, OSINT-аналітикам можуть знадобитися спеціалізовані пошукові системи, такі як Shodan. Цей сервіс орієнтований на пошук підключених до мережі пристроїв, зокрема серверів, вебкамер чи IoT-пристроїв. Shodan є незамінним інструментом для розслідувань у сфері кібербезпеки, дозволяючи виявляти вразливі системи та пристрої.

Wayback Machine, або Archive.org [33], є одним із ключових інструментів у рамках методології OSINT, який забезпечує доступ до архівних версій вебсторінок, навіть якщо вони були видалені або суттєво змінені. Цей сервіс надає унікальну можливість досліджувати історичні дані вебконтенту, дозволяючи аналізувати зміни, відновлювати видалені матеріали та документувати еволюцію контенту. Завдяки можливості відтворювати вебсторінки на конкретну дату, Wayback Machine є незамінним у розслідуванні кіберзлочинів, моніторингу інформаційних кампаній, виявленні маніпуляцій або зборі юридично значущих доказів.

Інструмент є особливо корисним для розслідування шахрайства, аналізу діяльності організацій або осіб, які намагаються приховати сліди своєї діяльності. Наприклад, він може допомогти ідентифікувати приховані маніпуляції в контенті, виявити зміни у відомостях про продукти чи послуги, а також зафіксувати видалену інформацію, яка може бути критично важливою для аналізу. Використовуючи цей сервіс, аналітики отримують доступ до архівних даних, які дозволяють відновити повну картину подій та визначити ключові етапи змін контенту.

Крім того, Wayback Machine широко використовується для документування змін у публікаціях ЗМІ, перевірки достовірності джерел, а також для відновлення інформації, яка більше не доступна через видалення сторінок або сайтів.Для європейських користувачів цікавим вибором може стати Qwant, який забезпечує конфіденційність пошуку відповідно до суворих європейських стандартів захисту даних. Qwant не відстежує користувачів і не зберігає їхні дані, що робить його схожим на DuckDuckGo, але з акцентом на європейський ринок.

Таким чином, використання різноманітних пошукових систем дає змогу OSINT-аналітикам адаптувати підхід до своїх завдань, забезпечуючи доступ до широкого спектра інформації, максимальну ефективність пошуку та належний рівень конфіденційності залежно від конкретних вимог.

Окрім цих інструментів, OSINT-розслідування передбачають систематизацію отриманої інформації за допомогою професійного програмного забезпечення, яке дозволяє ефективно організувати дані та побудувати аналітичну картину. Одним із найпоширеніших інструментів є Maltego [34] – потужне рішення для візуалізації взаємозв’язків між об’єктами дослідження, такими як доменні імена, IP-адреси, електронні адреси, соціальні профілі чи інші цифрові активи. Maltego дозволяє створювати інтерактивні графи, що надають аналітикам можливість бачити ключові зв’язки та закономірності, які можуть залишатися непомітними при традиційному аналізі. Інструмент підтримує інтеграцію з численними базами даних та зовнішніми ресурсами, що значно розширює можливості пошуку та перевірки інформації.

Іншим важливим інструментом є Hunchly [35], який автоматизує процес збереження вебконтенту для подальшого аналізу. Ця програма працює як розширення для браузера та дозволяє створювати структуровані архіви вебсторінок, включаючи знімки екранів, метадані та хронологію відвідувань. Hunchly особливо корисний для документування роботи в рамках розслідування, забезпечуючи юридичну валідність зібраних даних і можливість відтворення ходу аналізу. Це робить його незамінним для розслідувань, пов'язаних із шахрайством, кіберзлочинами або моніторингом соціальних мереж.

Крім цього, для аналізу великих масивів даних ефективним є використання інструменту Cortex XSOAR (Extended Security Orchestration, Automation, and Response), який значно спрощує обробку інформації завдяки автоматизації рутинних завдань та інтеграції різних джерел даних у єдину систему. Цей інструмент спеціально розроблений для забезпечення високого рівня координації та ефективності у сфері кібербезпеки, а також для швидкого реагування на інциденти.

Ще одним корисним інструментом є SpiderFoot [36], який спеціалізується на зборі та кореляції даних із відкритих джерел, таких як DNS-записи, соціальні мережі, бази даних зламаних облікових записів, криптовалютні транзакції та інше. SpiderFoot забезпечує автоматизацію рутинних завдань, дозволяючи аналітикам зосередитися на стратегічному аналізі отриманих результатів.

Для моніторингу соціальних медіа популярним є Social Links, інтегрований із платформою Maltego, який дозволяє швидко збирати дані про взаємодії, аудиторію та активність користувачів у популярних соціальних мережах, таких як Facebook, Twitter, Instagram, LinkedIn тощо. Social Links забезпечує глибокий аналіз соціальних графів, допомагаючи визначати ключових впливових осіб, мережі взаємозв'язків і потенційні ризики.

Сучасні OSINT-інструменти активно інтегрують технології штучного інтелекту (ШІ), відкриваючи нові можливості для ефективної обробки великих обсягів неструктурованих даних. Алгоритми ШІ дозволяють автоматизувати рутинні процеси, зокрема класифікацію інформації, виявлення аномалій та побудову прогностичних моделей. Це значно скорочує час на аналіз даних та

підвищує точність отриманих результатів. Наприклад, використовуючи ШІ, можна швидко аналізувати вміст соціальних мереж, ідентифікуючи ключові тренди, ознаки шахрайських дій або підозрілу активність окремих профілів. Такі можливості особливо важливі в умовах зростаючої кількості інформації та ускладнення цифрових загроз.

Важливою перевагою ШІ є його здатність адаптуватися до змінюваних умов і виявляти приховані закономірності в даних. Наприклад, у сфері кібербезпеки алгоритми машинного навчання можуть аналізувати мережевий трафік, визначаючи відхилення, які вказують на можливі атаки, або виявляти компрометовані облікові записи. У корпоративній розвідці ШІ допомагає оцінювати ризики, аналізувати поведінкові шаблони партнерів чи конкурентів і прогнозувати їхні дії [37].

Інтеграція інструментів, автоматизація процесів і впровадження таких технологій, як ШІ та Big Data, формують основу для створення високоефективної методології OSINT. Використання великих даних дозволяє об’єднувати різнорідні джерела інформації, виявляти ключові зв’язки між суб'єктами розслідування та створювати цілісну картину подій. Такі підходи забезпечують не лише оперативність реагування на цифрові виклики, а й можливість працювати з надскладними масивами даних, зберігаючи високу якість і достовірність аналізу.

Отже, методологія OSINT для збору інформації в кіберпросторі базується на системному підході, який поєднує використання інноваційних технологій, таких як штучний інтелект і Big Data, з перевіреними інструментами, наприклад, Wayback Machine, Maltego та OSINT Framework. Вона забезпечує можливість ефективного пошуку, верифікації, аналізу та документування даних із відкритих джерел. Ці підходи дозволяють адаптуватися до викликів сучасного цифрового середовища, працювати з великими обсягами неструктурованої інформації та вирішувати завдання різної складності, зокрема в розслідуванні кіберзлочинів, виявленні шахрайських схем і моніторингу змін у цифровому просторі. Інтеграція таких методів сприяє підвищенню достовірності аналізу, зміцненню

довіри до отриманих результатів та формуванню ефективної бази для прийняття рішень.

РОЗДІЛ 3 ПРАКТИЧНІ АСПЕКТИ ВИКОРИСТАННЯ OSINT-ТЕХНОЛОГІЙ У РОЗКРИТТІ ШАХРАЙСТВ, УЧИНЕНИХ В КІБЕРПРОСТОРІ

3.1 Методологія використання OSINT-технологій у розкритті шахрайств, учинених в кіберпросторі

Розкриття шахрайств у кіберпросторі потребує системного та методичного підходу, що враховує особливості цифрового середовища, зокрема анонімність і великий обсяг даних. Методологія використання OSINT-технологій базується на послідовному виконанні чітко визначених етапів, які охоплюють увесь процес розслідування: від збору інформації до аналізу отриманих даних і формування доказової бази. Інтеграція OSINT-інструментів у кожен етап розслідування дозволяє забезпечити високий рівень оперативності, точності та ефективності, адаптуючи розслідування до умов сучасного цифрового середовища.

Рисунок 3.1 – Етапи використання OSINT-технологій у розкритті шахрайств, учинених в кіберпросторі

Запропонована методологія передбачає поділ процесу на такі основні етапи: аналіз зв'язків, збір доказів, створення профілів підозрюваних та моніторинг активності у віртуальному просторі (див. рисунок 3.1). Кожен із цих етапів формує цілісну й логічно взаємопов'язану структуру, яка дозволяє забезпечити комплексний і системний підхід до використання OSINT-технологій у розкритті шахрайських схем у кіберпросторі, адаптуючи процес розслідування до викликів сучасного цифрового середовища. У межах кожного етапу визначено конкретні

завдання, підібрано відповідні OSINT-інструменти для їх вирішення, а також проаналізовано приклад практичного застосування, який демонструє ефективність і доцільність запропонованої методології.

Аналіз зв’язків

Завдання: Визначення зв’язків між різними людьми, подіями та локаціями для розкриття злочинної діяльності та розуміння загального контексту злочину.

Інструмент: Maltego [34].

Maltego є провідним інструментом для візуалізації даних та аналізу зв’язків. Цей інструмент дозволяє автоматизувати процес збору даних із відкритих джерел, об’єднувати їх у логічні структури та створювати графічні моделі, які демонструють взаємозв’язки між суб’єктами або об’єктами.

Приклад практичного використання. Maltego широко застосовується у розслідуваннях, пов’язаних із шахрайством, кіберзлочинністю, аналізом загроз та іншими видами злочинної діяльності. Наприклад, під час розслідування шахрайської схеми інструмент дозволяє зібрати інформацію про підозрюваних, їх контакти, фінансові транзакції та інші пов’язані дані. Maltego автоматично об’єднує ці дані в графічну модель, яка демонструє зв’язки між учасниками схеми, допомагаючи виявити ключових координаторів, виконавців і можливих спільників. Завдяки своїй потужності та гнучкості Maltego є незамінним інструментом для дослідників і аналітиків, які працюють із великими обсягами даних.

Інструмент: IBM i2 Analyst's Notebook [38].

IBM i2 Analyst's Notebook надає розширені можливості для аналізу та візуалізації складних структур і зв’язків у великих масивах даних. Завдяки інтеграції даних із різноманітних джерел, цей інструмент забезпечує створення детальних графічних моделей зв’язків між об’єктами розслідування.

Приклад практичного використання. У процесі розкриття шахрайських схем IBM i2 Analyst's Notebook може застосовуватися для збору та обробки інформації, наприклад, з митних декларацій, банківських транзакцій чи профілів у соціальних мережах. Завдяки цьому створюються детальні візуалізації зв’язків між учасниками злочинної діяльності, що дозволяє виявити ключових

організаторів, їхні ролі та зв’язки з іншими учасниками злочинної мережі. Інструмент ефективно допомагає формувати доказову базу, сприяючи подальшій юридичній оцінці отриманих даних. IBM i2 Analyst's Notebook також дозволяє проводити часовий аналіз подій, що допомагає відстежувати послідовність дій злочинців. Інструмент підтримує інтеграцію з іншими системами розслідування, що дозволяє об'єднувати дані з різних джерел для більш повного аналізу. Крім того, можливості автоматизації та використання алгоритмів машинного навчання сприяють швидшому виявленню аномалій та підозрілих активностей. Завдяки своїм потужним аналітичним можливостям, IBM i2 Analyst's Notebook значно підвищує ефективність розслідувань, дозволяючи швидше і точніше виявляти злочинні схеми. Інструмент також сприяє покращенню співпраці між різними відомствами та організаціями, забезпечуючи спільний доступ до важливої інформації та сприяючи координації дій у боротьбі з кіберзлочинністю.

Інструмент: Gephi [39].

Gephi – це дієвий інструмент для візуалізації та аналізу графів, який дає змогу ідентифікувати структури, закономірності та аномалії у великих мережах. Завдяки інтерактивному підходу до аналізу даних, Gephi дозволяє ефективно досліджувати соціальні мережі та виявляти ключові зв’язки між об’єктами.

Приклад практичного використання. Gephi можна застосувати для аналізу взаємозв’язків між фальшивими профілями у соціальних мережах. Наприклад, під час розслідування шахрайських схем Gephi дозволяє виявити, що група фальшивих профілів має спільні зв’язки, схожу активність чи взаємодії, що вказують на їхнє керування однією особою або організованою групою. Інструмент допомагає побудувати візуалізації цих взаємозв’язків, що сприяє ідентифікації координаторів, їхніх дій та мережі підконтрольних профілів.

Інструмент: Linkurious [40].

Linkurious – це спеціалізована платформа для аналізу графів, що надає можливість виявляти приховані зв’язки, шаблони та аномалії у великих наборах даних. Завдяки інтеграції з популярними базами даних графів, Linkurious забезпечує потужні інструменти для візуалізації та аналізу складних мереж.

Приклад практичного використання. Linkurious може бути використаний для аналізу транзакцій у блокчейні в межах розслідування шахрайських схем. Наприклад, інструмент допомагає ідентифікувати приховані зв’язки між криптовалютними гаманцями, які беруть участь у відмиванні грошей. Завдяки аналізу графів Linkurious дозволяє знайти аномальні транзакції з нетиповими обсягами чи частотою, які можуть бути маркером шахрайської діяльності. Інструмент також дозволяє дослідити, як ці гаманці пов’язані з іншими елементами мережі, що допомагає встановити структуру злочинної схеми. Використовуючи Linkurious, дослідники можуть не лише виявити підозрілу активність, але й представити отримані результати у вигляді чіткої графічної моделі, яка є корисною для подальшого аналізу та формування доказової бази.

Інструмент: Neo4j [41].

Neo4j – це графова база даних, яка забезпечує можливість зберігання, обробки та аналізу даних зі складними зв’язками. Вона дозволяє будувати моделі графів, досліджувати приховані шаблони та ідентифікувати залежності між об'єктами.

Приклад практичного використання. Neo4j може бути застосований для зберігання та аналізу даних, пов’язаних зі шахрайськими схемами, включаючи інформацію про організації, їхніх учасників та фінансові транзакції. Наприклад, у процесі розслідування шахрайства Neo4j допомагає ідентифікувати зв’язки між компаніями-оболонками, спільними власниками та потоками коштів. Аналіз графа дозволяє виявити ключових фігурантів злочинної організації, зрозуміти структуру їхніх дій та встановити приховані взаємозв’язки між учасниками. Крім того, Neo4j може бути використаний для відстеження транзакцій у реальному часі, що дає змогу швидко реагувати на нові загрози та попереджати незаконну діяльність. Це робить Neo4j незамінним інструментом для побудови та аналізу складних схем у розслідуваннях злочинів. Neo4j також підтримує інтеграцію з іншими інструментами та системами, що дозволяє об'єднувати дані з різних джерел для більш повного аналізу. Завдяки своїй гнучкості та потужним аналітичним можливостям, Neo4j сприяє ефективному виявленню та розкриттю

складних шахрайських схем, забезпечуючи глибоке розуміння взаємозв'язків та дій злочинців.

Інструмент: Palantir Gotham [42].

Palantir Gotham – це провідна аналітична платформа, розроблена для інтеграції, аналізу та візуалізації великих обсягів даних у реальному часі. Вона допомагає користувачам ідентифікувати приховані зв’язки, виявляти закономірності та проводити глибокий аналіз складних структур даних. Завдяки масштабованості та гнучкості, Palantir Gotham широко використовується у правоохоронних органах, розвідувальних структурах і корпоративному секторі.

Приклад практичного використання. У межах розслідування шахрайської діяльності Palantir Gotham може інтегрувати дані з різних джерел, таких як фінансові транзакції, записи телефонних розмов і активність у соціальних мережах. Інструмент дозволяє створити інтерактивну карту зв’язків, яка візуалізує стосунки між учасниками злочинної мережі, ідентифікувати ключових координаторів та відстежувати фінансові потоки. Наприклад, аналіз транзакцій може допомогти виявити незвичайні фінансові операції, які можуть бути маркерами відмивання грошей, а дослідження телефонних розмов і взаємодії у соціальних мережах – знайти зв’язки між підозрюваними та іншими учасниками схеми.

Збір доказів

Завдання: Збір загальнодоступної інформації з різних джерел для збору доказів про злочинну діяльність та підозрюваних.

Інструмент: SpiderFoot [36].

SpiderFoot – це багатофункціональний інструмент для автоматизованого збору даних із відкритих джерел з можливістю аналізу взаємозв’язків між отриманими даними.

Приклад практичного використання. SpiderFoot може бути використаний для збору інформації з соціальних мереж, форумів та вебсайтів, що підтверджує участь підозрюваного у злочині. Наприклад, у випадку кіберзлочину, SpiderFoot може зібрати дані про активність підозрюваного на форумах, де обговорюються методи шахрайства, що допоможе підтвердити його причетність. Зібрані дані

можуть включати IP-адреси, електронні пошти, домени, телефонні номери, імена користувачів та інші важливі відомості. Наприклад, якщо підозрюваний використовує певний псевдонім на різних платформах, SpiderFoot може виявити всі акаунти, пов’язані з цим псевдонімом, що допоможе створити повну картину його діяльності.

Інструмент: Recon-ng [43].

Recon-ng – це ефективний OSINT-інструмент для автоматизації збору інформації з різноманітних відкритих джерел. Завдяки модульній архітектурі інструмент дозволяє підключати додаткові модулі для збору специфічних даних, що робить його гнучким та ефективним у різних сценаріях розслідування. Recon-ng підтримує інтеграцію з багатьма API, що дозволяє розширити можливості збору даних та підвищити точність отриманих результатів.

Приклад практичного використання. У процесі розслідування кіберзлочинів, таких як шахрайство з використанням фальшивих вебсайтів для фішингу, Recon-ng може автоматично збирати інформацію про домени, пов’язані з підозрюваними. Інструмент може виявити IP-адреси, пов’язані з цими доменами, а також інші вебсайти, які використовують ті ж IP-адреси. Це дозволяє виявити мережу фальшивих вебсайтів, які використовуються для шахрайства. Recon-ng також може збирати дані про власників доменів, включаючи контактну інформацію, що допомагає встановити особи, відповідальні за створення фальшивих вебсайтів. Завдяки автоматизації збору та аналізу даних, інструмент дозволяє швидко й ефективно виявляти та розкривати складні шахрайські схеми, учинені в кіберпросторі.

Інструмент: Shodan [44].

Shodan – це пошукова система, яка спеціалізується на виявленні пристроїв, підключених до Інтернету, таких як сервери, камери спостереження, маршрутизатори, IoT-пристрої та інші мережеві компоненти. Цей інструмент використовується для збору технічних даних, що дозволяє аналізувати конфігурації пристроїв, визначати їх уразливості та досліджувати активність підозрюваних.

Приклад практичного використання. Shodan може бути використаний для ідентифікації пристроїв, які належать підозрюваному, і збору інформації про їхню технічну конфігурацію. Наприклад, під час розслідування кіберзлочину Shodan може виявити сервери, що використовуються підозрюваним для управління ботнетами або проведення атак. Інструмент надає дані про відкриті порти, активні сервіси, використовуване програмне забезпечення та можливі вразливості. Зібрана інформація допомагає уповноваженим суб'єктам визначити місцезнаходження пристроїв, встановити зв'язки між ними та виявити інші елементи інфраструктури, які можуть бути залучені до злочинної діяльності. Shodan є важливим інструментом для збору технічних доказів і проведення глибокого аналізу інтернет-інфраструктури підозрюваних.

Інструмент: Censys [45].

Censys – це платформа для пошуку, аналізу та моніторингу пристроїв, підключених до Інтернету. Вона забезпечує аналітиків інформацією про інфраструктуру мережі, вразливості пристроїв, їх конфігурації та взаємодії. Censys використовується для ідентифікації кіберзагроз, моніторингу активів і проведення розслідувань у сфері кіберзлочинності.

Приклад практичного використання. Censys може бути використаний для виявлення вразливих пристроїв, що належать підозрюваному. Наприклад, при розкритті шахрайств, учинених в кіберпросторі, платформа допомагає знайти вебсервери з уразливими конфігураціями, які використовуються підозрюваним для зберігання викрадених даних. Це дозволяє виявити точки доступу до його інфраструктури.

Фахівці можуть також використовувати Censys для аналізу відкритих портів і протоколів, пов'язаних із сервером. Наприклад, знайдений сервер може мати активні незахищені FTP- або HTTP-сервіси, що свідчать про можливу витік інформації або використання сервера в шахрайських схемах. Такі дані дозволяють створити профіль підозрюваного, оцінити його технічні ресурси та можливості.

Інструмент: TheHarvester [46].

TheHarvester – це ефективний OSINT-інструмент, розроблений для швидкого збору інформації з відкритих джерел. Він дозволяє виявляти електронні адреси, субдомени, IP-адреси, імена, конфігурації мережевих пристроїв та інші важливі дані. Інструмент широко застосовується для аналізу діяльності підозрюваних, побудови мереж зв'язків і виявлення інфраструктури, пов'язаної з кіберзлочинами.

Приклад практичного використання. У межах розслідування фішингової атаки TheHarvester може зібрати критичну інформацію, пов'язану з підозрюваним доменом. Інструмент допомагає ідентифікувати електронні адреси, які використовуються для розсилки шкідливих листів, та виявляє субдомени, на яких можуть розміщуватись фішингові сторінки або шкідливе програмне забезпечення. Крім того, зібрані IP-адреси дозволяють відстежити сервери, залучені у злочинній діяльності, такі як управління ботнетами або зберігання викрадених даних. Ця інформація допомагає побудувати карту зв'язків між підозрюваними та іншими об'єктами, виявляючи можливих спільників і додаткові елементи злочинної схеми [47].

Інструмент: Hunchly [48].

Hunchly – це інструмент для автоматичного збереження та документування вебсторінок під час розслідування. Hunchly дозволяє зберігати докази у вигляді знімків екрана та метаданих.

Приклад практичного використання. Hunchly може бути застосований для документування вебсторінок, які залучені до злочинної діяльності або відвідувані підозрюваним. Наприклад, у розслідуванні шахрайства з використанням фальшивих вебсайтів Hunchly автоматично зберігає знімки екрана таких сторінок, їхній HTML-код та метадані, зокрема URL-адреси й час доступу. Це дозволяє уповноваженим суб'єктам фіксувати важливу інформацію навіть у випадках, коли підозрювані видаляють або змінюють вміст сайтів. Збережені дані допомагають відновити вигляд і структуру вебресурсів, надаючи доказову базу для подальшого розслідування. Hunchly також полегшує аналіз великої кількості вебсторінок, впорядковуючи зібрані матеріали за категоріями та темами.

Інструмент: IntelTechniques [49].

IntelTechniques – це багатофункціональна платформа, яка забезпечує доступ до різних інструментів для збору інформації з соціальних мереж, баз даних та інших відкритих джерел. Вона надає можливість швидко знайти потрібні інструменти для збору специфічних даних, таких як контактна інформація, дані про активність у мережі та взаємозв'язки між об'єктами.

Приклад практичного використання: IntelTechniques може бути використаний для збору інформації про підозрюваного у шахрайстві з використанням фальшивих профілів у соціальних мережах. Наприклад, платформа дозволяє ідентифікувати профілі підозрюваного, зібрати публічно доступну контактну інформацію, відстежити активність у соціальних мережах та виявити зв'язки між його акаунтами. Інструменти, доступні через платформу, допомагають виявити схеми взаємодії між підозрюваними та третіми особами, а також створити детальний цифровий профіль, який можна використовувати як доказову базу в подальших розслідуваннях.

Створення профілів підозрюваних

Завдання: створення профілів підозрюваних, включаючи їх поведінку в Інтернеті, зв'язки та діяльність, для розуміння їхніх мотивів, звичок та потенційних майбутніх дій.

Інструмент: Osintgram [50].

Osintgram – це спеціалізований OSINT-інструмент, що забезпечує розширені функції збору та аналізу даних із платформи Instagram. За його допомогою можна досліджувати активність користувачів, аналізувати публікації, коментарі, хештеги, а також отримувати геолокаційні дані.

Приклад практичного використання. Osintgram може використовуватися для вивчення підозрілих акаунтів або створення профілю осіб, які є об'єктами розслідування. Інструмент дозволяє ідентифікувати ключові місця активності користувача, такі як місце проживання, роботи чи маршрути пересування. Завдяки аналізу вмісту публікацій і хештегів можна виявити основні інтереси та можливі мотиви підозрюваного.

Також Osintgram допомагає досліджувати соціальні зв’язки користувача, аналізуючи його підписників, коментарі та взаємодії. Це сприяє виявленню інших осіб, які можуть бути пов’язані зі злочинною діяльністю або входити до мережі співучасників. Наприклад, повторювані хештеги чи взаємодії з підозрілими акаунтами можуть вказувати на координацію шахрайських дій. Завдяки широкому функціоналу Osintgram забезпечує ефективний збір та систематизацію інформації, необхідної для проведення розслідувань.

Інструмент: Social-Engineer Toolkit (SET) [51].

Social-Engineer Toolkit (SET) – це дієвий інструмент для проведення соціальної інженерії, розроблений для створення різних сценаріїв атак, зокрема фішингових кампаній, які використовуються для збору інформації про поведінку користувачів в Інтернеті. Він широко використовується у сфері кібербезпеки для тестування вразливостей та розслідування кіберзлочинів.

Приклад практичного використання. Social-Engineer Toolkit може бути ефективно застосований для збору інформації про поведінку підозрюваних у розслідуваннях кіберзлочинів. Наприклад, у межах справи про шахрайство SET дозволяє створити реалістичну фішингову атаку, яка може імітувати повідомлення від банку або соціальної мережі. Підозрюваний, взаємодіючи із підробленим посиланням або формою, може ненавмисно надати критичну інформацію, таку як електронна пошта, паролі, IP-адресу або інші особисті дані. Ця інформація допоможе уповноваженим суб’єктам створити більш точний профіль підозрюваного, зрозуміти його цифрові звички, ідентифікувати використовувані пристрої або навіть знайти інші облікові записи, які можуть бути пов’язані з його діяльністю.

Інструмент: Twint [52].

Twint – це потужний OSINT-інструмент для збору даних із Twitter без використання офіційного API. Він дозволяє отримувати детальну інформацію про активність користувачів, аналізувати їхні твіти, профілі, взаємодії з іншими користувачами та використовувані хештеги. Twint ідеально підходить для розслідувань, де потрібно вивчити поведінку та активність підозрюваних у соціальних мережах.

Приклад практичного використання. Twint може бути використаний для аналізу активності підозрюваного у Twitter. Наприклад, у межах розслідування шахрайства з використанням соціальних мереж інструмент дозволяє зібрати дані про всі твіти підозрюваного, включаючи текст повідомлень, дати публікацій, використані хештеги та геолокацію. Крім цього, Twint аналізує взаємодії підозрюваного з іншими користувачами, наприклад, коментарі, ретвіти або вподобання, що дозволяє ідентифікувати осіб, із якими підозрюваний перебуває у контакті. Зібрані дані допомагають створити детальний профіль підозрюваного, зокрема, його інтереси, мережу контактів і можливі шахрайські схеми, у яких він може брати участь. Twint є ефективним інструментом для збору та аналізу даних у розслідуваннях, пов'язаних з активністю у Twitter.

Інструмент: Hootsuite [53].

Hootsuite – це платформа для управління соціальними мережами, яка дозволяє централізовано моніторити та аналізувати активність користувачів у різних соцмережах, таких як Facebook, Twitter, Instagram, LinkedIn та інші. Завдяки розширеним можливостям аналітики Hootsuite часто використовується для збору даних про поведінку підозрюваних і виявлення шаблонів їхньої активності в Інтернеті.

Приклад практичного використання. Hootsuite може бути використаний для моніторингу активності підозрюваного у різних соціальних мережах одночасно. Наприклад, у розслідуванні шахрайства з використанням фальшивих профілів платформа дозволяє відстежувати публікації підозрюваного, аналізувати їхній вміст і час публікації, а також вивчати його взаємодії з іншими користувачами, такі як коментарі, вподобання або згадки. Це допомагає ідентифікувати зв'язки підозрюваного, його можливих спільників і загальні шаблони поведінки. Зібрані дані можна використовувати для створення цифрового профілю підозрюваного та розкриття злочинної схеми. Hootsuite також дає змогу отримати оперативну інформацію про нову активність підозрюваного завдяки реальному моніторингу подій у соціальних мережах.

Інструмент: Talkwalke [54].

Talkwalker – це платформа для моніторингу соціальних мереж і аналізу публічних згадок, яка дозволяє збирати дані про активність користувачів у соціальних медіа та інших онлайн-джерелах. Завдяки розширеним аналітичним можливостям, Talkwalker є корисним інструментом для дослідження поведінки підозрюваних і виявлення зв'язків між ними.

Приклад практичного використання. Talkwalker може бути використаний для збору даних про активність підозрюваного у соціальних мережах у межах розслідування шахрайства з використанням фальшивих новин. Наприклад, інструмент дозволяє відстежувати згадки про підозрюваного в різних соцмережах, проаналізувати його публікації та взаємодії з іншими користувачами. Це може включати визначення ключових слів, пов'язаних із підозрюваним, або ідентифікацію спільноти, яка підтримує його активність. Завдяки цьому уповноважені суб'єкти можуть створити детальний профіль підозрюваного, визначити його вплив у соціальних мережах і встановити потенційних спільників. Talkwalker також дозволяє аналізувати динаміку активності, що сприяє виявленню шаблонів поведінки або ключових періодів його активності.

Інструмент: Pipl [55].

Pipl – це спеціалізована пошукова система, розроблена для збору інформації про осіб з різних джерел. Pipl дозволяє знаходити контактні дані, профілі в соціальних мережах та іншу інформацію про підозрюваних.

Приклад практичного використання. Pipl може бути використаний для пошуку додаткової інформації про підозрюваного у розслідуванні шахрайства. Наприклад, у справі, пов'язаній з використанням фальшивих ідентифікаційних документів, Pipl може допомогти виявити реальні профілі підозрюваного в соціальних мережах, його контактні дані, такі як електронні адреси чи номери телефонів, а також інші цифрові сліди. Ця інформація дозволяє уповноваженим суб'єктам підтвердити справжню особу підозрюваного, виявити зв'язки з іншими особами чи організаціями, а також створити більш детальний профіль для подальшого аналізу. Наприклад, якщо підозрюваний використовує кілька псевдонімів або має профілі на різних платформах, Pipl може зібрати всі ці дані

в одному місці, що допоможе уповноваженим суб’єктам побачити повну картину його діяльності. Крім того, Pipl може виявити історію роботи підозрюваного, його освіту та інші важливі деталі, які можуть бути корисними для розслідування. Pipl також корисний для верифікації отриманих даних з інших джерел, забезпечуючи повноту інформації. Наприклад, якщо уповноважені суб’єкти отримали електронну адресу підозрюваного із іншого джерела, вони можуть використовувати Pipl для перевірки цієї інформації та отримання додаткових даних, таких як повне ім’я, місцезнаходження та профілі в соціальних мережах.

Інструмент: Clearview AI [56].

Clearview AI – це інструмент для розпізнавання облич, який дозволяє знайти інформацію про підозрюваних за допомогою аналізу зображень. Clearview AI може використовуватися для ідентифікації підозрюваних за їхніми фотографіями.

Приклад практичного використання. Clearview AI може бути використаний для ідентифікації підозрюваного за його фотографіями. Наприклад, у розслідуванні шахрайства з використанням фальшивих профілів, система може знайти зображення підозрюваного в різних базах даних та соціальних мережах. Це допоможе підтвердити, чи фотографії, використані у фальшивих акаунтах, належать підозрюваному. Clearview AI також може виявити додаткові фотографії тієї ж особи, які були завантажені на різні платформи, що дозволяє встановити зв’язки між акаунтами та ідентифікувати реальні особисті дані підозрюваного. Наприклад, якщо підозрюваний використовує різні псевдоніми на різних платформах, Clearview AI може знайти всі фотографії, пов'язані з цими псевдонімами, що допоможе уповноваженим суб’єктам побачити повну картину його діяльності. Крім того, Clearview AI може бути використаний для виявлення додаткових фотографій тієї ж особи, які були завантажені на різні платформи, що дозволяє встановити зв’язки між акаунтами та ідентифікувати реальні особисті дані підозрюваного. Наприклад, у випадку розслідування шахрайства з використанням фальшивих профілів у соціальних мережах, Clearview AI може знайти фотографії підозрюваного на різних платформах, таких як Facebook,

Instagram та LinkedIn, що допоможе підтвердити його особу та виявити його зв’язки з іншими підозрюваними. Зібрані дані сприяють формуванню детального профілю підозрюваного та підтвердженню його участі у злочинній діяльності. Clearview AI також може допомогти у вирішенні холодних справ, порівнюючи старі фотографії з сучасними базами даних, що дозволяє зробити проривні ідентифікації, які раніше були недосяжними.

Інструмент: Social Mention [57].

Social Mention – це інструмент для моніторингу соціальних медіа, який дозволяє відстежувати згадки про певні ключові слова, теми чи осіб у реальному часі. Інструмент також аналізує тональність згадок (позитивна, негативна чи нейтральна) та допомагає визначити ключові теми й тренди, пов’язані з активністю підозрюваних.

Приклад практичного використання. Social Mention може бути використаний для моніторингу згадок про підозрюваного у соціальних медіа в межах розслідування шахрайства. Наприклад, у справі, пов’язаній із поширенням фальшивих новин, інструмент може відстежувати, як часто та в якому контексті згадуються підозрюваний або пов’язані з ним ключові слова. Social Mention аналізує тональність згадок, допомагаючи визначити, чи сприймається підозрюваний як авторитетна особа або як об’єкт критики. Крім того, інструмент ідентифікує ключові теми, які обговорюються навколо підозрюваного, що може вказати на його методи роботи або вплив у соціальних мережах. Ці дані допомагають створити профіль підозрюваного, зрозуміти його роль у схемі та знайти потенційні зв’язки з іншими особами.

Моніторинг активності

Завдання: Моніторинг активності в Інтернеті в режимі реального часу для відстеження переміщень і комунікації між підозрюваними, а також для виявлення нових загроз.

Інструмент: Holehe [58].

Holehe – це інструмент для сканування облікових даних, який визначає витік інформації з різних джерел, що допомагає виявити потенційні ризики безпеці. Holehe перевіряє, чи пов’язана електронна адреса з обліковими записами на

різних вебсайтах, включаючи популярні платформи, такі як Twitter, Instagram, Imgur та понад 120 інших. Інструмент використовує функції відновлення паролів, реєстрації та входу для отримання інформації, не сповіщаючи власника електронної адреси.

Приклад практичного використання. Holehe може бути використаний для виявлення скомпрометованих облікових даних підозрюваного. Наприклад, у розслідуванні кіберзлочину, Holehe може знайти облікові дані підозрюваного, які були викрадені та опубліковані на форумах або в темних вебресурсах. Це дозволяє уповноваженим суб’єктам вчасно вжити заходів для запобігання подальшим злочинам, а також відстежувати активність підозрюваного у реальному часі. Зібрані дані можуть включати електронні адреси, пов’язані з різними обліковими записами, частково приховані електронні адреси для відновлення, номери телефонів та іншу важливу інформацію. Наприклад, якщо підозрюваний використовує певну електронну адресу на кількох платформах, Holehe може виявити всі облікові записи, пов'язані з цією адресою, що допоможе уповноваженим суб’єктам створити повну картину його діяльності. До того ж Holehe підтримує інтеграцію з іншими сервісами, що дає змогу отримувати додаткові дані про підозрюваного, оперативно реагувати на нові загрози та моніторити його активність у режимі реального часу.

Інструмент: Spyderlab Darknet Forensic [59].

Spyderlab Darknet Forensic – інструмент для моніторингу прихованих вебресурсів, який дозволяє виявляти потенційні загрози та витоки даних. Spyderlab Darknet Forensic використовує передові алгоритми та машинне навчання для аналізу даних з прихованих вебфорумів, ринків та сервісів. Інструмент забезпечує безперервний моніторинг прихованого вебу, надаючи реальну інформацію про нові вразливості, вектори атак та загрози.

Приклад практичного використання. Spyderlab Darknet Forensic використовується для відстеження активності підозрюваних на прихованих вебфорумах та ринках. У межах розслідування кіберзлочинів цей інструмент дозволяє виявляти обговорення, пов’язані з продажем викрадених даних чи плануванням атак, що забезпечує уповноваженим суб’єктам можливість

оперативно реагувати на потенційні загрози. Зібрана інформація може включати деталі про облікові записи підозрюваного, його спілкування з іншими користувачами, а також дані про товари чи послуги, які він пропонує. Наприклад, якщо підозрюваний здійснює продаж викрадених даних через приховані вебринки, Spyderlab Darknet Forensic здатний виявити відповідні оголошення, зібрати інформацію про покупців і продавців, а також простежити транзакції, створюючи повну картину злочинної діяльності.

Крім цього, інструмент аналізує дані з різних джерел, таких як форуми, блоги та соціальні медіа, для виявлення нових вразливостей та потенційних атак. Це дозволяє уповноваженим суб'єктам своєчасно отримувати інформацію про загрози, які плануються, і вживати необхідних заходів для їхнього попередження.

Інструмент: ZeroFOX [60].

ZeroFOX – платформа для моніторингу соціальних медіа та захисту бренду, яка дозволяє виявляти фішингові атаки, шахрайські акаунти та інші загрози. ZeroFOX забезпечує безперервний моніторинг соціальних медіа, мобільних додатків, доменів та інших цифрових активів, використовуючи машинне навчання та штучний інтелект для виявлення та нейтралізації загроз. Платформа також пропонує функції автоматичного видалення шкідливого контенту та акаунтів.

Приклад практичного використання. ZeroFOX може бути використаний для моніторингу соціальних медіа на предмет фішингових атак та шахрайських акаунтів. Наприклад, у розслідуванні шахрайства з використанням фальшивих профілів, ZeroFOX може виявити акаунти, які видають себе за відомі бренди або осіб. Зібрані дані можуть включати інформацію про акаунти, які використовують логотипи та назви відомих брендів для обману користувачів, а також деталі про фішингові посилання та шкідливі вебсайти. Наприклад, якщо підозрюваний створює фальшиві акаунти для проведення фішингових атак, ZeroFOX може виявити ці акаунти, зібрати інформацію про їхню активність та автоматично подати запити на їх видалення. Крім того, ZeroFOX може виявити шахрайські акаунти, які використовують імена та фотографії відомих осіб для обману

користувачів, що дозволяє уповноваженим суб'єктам швидко реагувати та запобігати подальшим атакам. Платформа також може інтегруватися з іншими системами безпеки для забезпечення комплексного захисту від цифрових загроз.

Інструмент: Recorded Future [61].

Recorded Future – це платформа для аналізу загроз, яка використовує технології машинного навчання для моніторингу Інтернету та ідентифікації нових загроз у режимі реального часу. Recorded Future об'єднує та обробляє дані з різноманітних джерел, включаючи прихований веб, відкриті джерела, технічну інформацію та соціальні медіа, забезпечуючи повну картину загроз. Платформа надає актуальну та своєчасну інформацію, що дозволяє організаціям ухвалювати обґрунтовані рішення та оперативно реагувати на потенційні ризики.

Приклад практичного використання. Recorded Future може бути використаний для моніторингу загроз у реальному часі. Наприклад, у розслідуванні кіберзлочину, цей інструмент може виявити нові вразливості або атаки, що плануються, аналізуючи дані з різних джерел, таких як форуми, блоги та соціальні медіа. Зібрані дані можуть включати інформацію про тактики, техніки та процедури (TTP) зловмисників, індикатори компрометації (IOC), такі як IP-адреси, доменні імена, хеші файлів та сигнатури шкідливого програмного забезпечення. Наприклад, якщо підозрюваний планує атаку на конкретну організацію, Recorded Future може виявити обговорення цієї атаки на форумах або в соціальних медіа, що дозволяє уповноваженим суб'єктам вчасно вжити заходів для запобігання атаці. Крім того, платформа може допомогти виявити нові вразливості в програмному забезпеченні, які можуть бути використані зловмисниками, що дозволяє організаціям своєчасно оновлювати свої системи та захищати їх від потенційних атак.

Інструмент: DarkOwl [62].

DarkOwl – це інструмент для моніторингу тіньового цифрового простору, який дозволяє виявляти витоки даних, обговорення злочинної діяльності та інші загрози. DarkOwl використовує передові алгоритми для аналізу даних із закритих форумів, ринків та анонімних сервісів. Інструмент забезпечує безперервний

моніторинг тіньового цифрового простору, надаючи актуальну інформацію про нові вразливості, вектори атак та загрози.

Приклад практичного використання. DarkOwl може бути застосований для моніторингу тіньового цифрового простору з метою виявлення витоків даних та обговорення злочинної діяльності. Наприклад, під час розслідування шахрайства цей інструмент здатний виявити, що підозрюваний продає викрадені дані на закритих онлайн-ринках, що дає змогу уповноваженим суб'єктам оперативно реагувати та запобігати подальшим злочинам.

Зібрана інформація може містити деталі облікових записів підозрюваного, його спілкування з іншими користувачами, а також дані про товари чи послуги, які він пропонує. Наприклад, якщо підозрюваний продає викрадені дані в анонімних мережах, DarkOwl може виявити відповідні оголошення, зібрати інформацію про покупців і продавців, а також відстежити транзакції, що сприяє створенню повної картини злочинної діяльності.

Інструмент: Cybersixgill [63].

Cybersixgill – це платформа для моніторингу прихованого вебу та глибокого вебу, яка дозволяє виявляти загрози та витоки даних у реальному часі. Cybersixgill збирає та аналізує дані з прихованого вебу, глибокого вебу та відкритих джерел, використовуючи машинне навчання та штучний інтелект для виявлення загроз. Платформа забезпечує своєчасну та релевантну інформацію, що дозволяє організаціям приймати обґрунтовані рішення та швидко реагувати на загрози.

Приклад практичного використання. Cybersixgill може бути використаний для моніторингу прихованого вебу та глибокого вебу на предмет загроз та витоків даних. Наприклад, у розслідуванні кіберзлочину, Cybersixgill може виявити обговорення підозрюваного про продаж викрадених даних або планування атак, що дозволяє уповноваженим суб'єктам вчасно реагувати на нові загрози. Зібрані дані можуть включати інформацію про тактики, техніки та процедури (TTP) зловмисників, індикатори компрометації (IOC), такі як IP-адреси, доменні імена, хеші файлів та сигнатури шкідливого програмного забезпечення. Наприклад, якщо підозрюваний планує атаку на конкретну

організацію, Cybersixgill може виявити обговорення цієї атаки на форумах або в соціальних медіа, що дозволяє уповноваженим суб'єктам вчасно вжити заходів для запобігання атаці. Крім того, платформа може допомогти виявити нові вразливості в програмному забезпеченні, які можуть бути використані зловмисниками, що дозволяє організаціям своєчасно оновлювати свої системи та захищати їх від потенційних атак.

Інструмент: LogRhythm [64].

LogRhythm – це платформа для моніторингу та аналізу безпеки, яка дозволяє виявляти аномалії та загрози у реальному часі. LogRhythm забезпечує безперервний моніторинг мережевої та системної активності, аналізуючи журнали та події для виявлення підозрілої або шкідливої поведінки. Платформа використовує машинне навчання та поведінкову аналітику для виявлення аномалій, що дозволяє організаціям швидко реагувати на загрози.

Приклад практичного використання. LogRhythm може бути використаний для моніторингу активності підозрюваного у корпоративних мережах. Наприклад, у розслідуванні внутрішнього шахрайства, LogRhythm може виявити аномальні дії підозрюваного, такі як несанкціонований доступ до конфіденційних даних або спроби видалення журналів активності, що дозволяє уповноваженим суб'єктам швидко реагувати та запобігати подальшим злочинам. Зібрані дані можуть включати інформацію про підозрілі входи в систему, зміни конфігурацій, спроби доступу до захищених ресурсів та інші аномальні дії. Наприклад, якщо підозрюваний намагається отримати доступ до конфіденційних даних без відповідних прав, LogRhythm може виявити цю спробу та згенерувати попередження для уповноважених суб'єктів. Крім того, платформа може допомогти виявити спроби видалення журналів активності, що може свідчити про спробу приховати сліди злочинної діяльності.

Отже, послідовне виконання цих етапів забезпечує цілісний підхід до розкриття шахрайств, учинених у кіберпросторі, дозволяючи ефективно працювати з великими обсягами даних, створювати чіткі зв'язки між отриманою інформацією та формувати доказову базу, яка відповідає сучасним юридичним вимогам. Використання OSINT-технологій не лише підвищує ефективність

розслідувань, а й оптимізує процеси збору та аналізу інформації в умовах динамічного цифрового середовища. Завдяки потужним аналітичним можливостям, ці інструменти сприяють швидшому та точнішому розслідуванню, підвищуючи якість та швидкість виявлення кіберзлочинів.

РОЗДІЛ 4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Магістерська робота присвячена дослідженню використання OSINT-технологій при розкритті шахрайств, учинених у кіберпросторі. Використання цих технологій передбачає значні навантаження на уповноважених суб'єктів, які працюють з комп'ютерами та іншими цифровими пристроями протягом тривалого часу. У зв'язку з цим, дотримання вимог охорони праці стає необхідною умовою для забезпечення продуктивності досліджень, мінімізації ризиків для здоров'я та запобігання розвитку професійних захворювань.

Тривале використання комп'ютерів створює специфічні ризики для фізичного, психоемоційного та когнітивного стану працівників, що робить організацію робочого процесу важливим компонентом професійної діяльності.

Організація робочого місця

Робоче місце повинно відповідати ергономічним та санітарно-гігієнічним вимогам:

– Освітлення: рівномірне освітлення, що унеможливлює відблиски на моніторі, із використанням як природного, так і штучного світла.

– Мікроклімат: підтримання комфортної температури (18-22 °C) та вологості (40–60%) разом із регулярним провітрюванням.

– Ергономіка меблів: стілець із регулюванням висоти та підтримкою попереку, стіл, який дозволяє правильно розташувати монітор та клавіатуру. Монітор повинен розташовуватись на відстані 50–70 см від очей, а його центр – на рівні або трохи нижче рівня очей.

Режим роботи

Регламент роботи за комп'ютером має знижувати ризики перенапруження:

– Перерви: кожні 50–60 хвилин роботи необхідно робити 5–10-хвилинну перерву для виконання фізичних вправ та гімнастики для очей.

– Чергування діяльності: зміна характеру роботи (наприклад, аналітична діяльність, виконання документів) сприяє рівномірному розподілу навантаження на організм.

– Обмеження тривалості: безперервна робота за комп’ютером не повинна перевищувати двох годин, після чого доцільна більш тривала пауза.

Профілактика професійних захворювань

Тривала робота за комп’ютером може призводити до порушень постави, зорових розладів та розвитку тунельного синдрому. Запобігання таким проблемам включає:

– Фізичну активність: вправи для м’язів шиї, спини, зап’ясть. Наприклад, розминка плечей, нахили голови та обертання кистями.

– Зорову гімнастику: правило «20-20-20» (кожні 20 хвилин дивитися на об’єкт на відстані 20 футів протягом 20 секунд) для зняття напруження з очей.

– Технічні засоби: налаштування яскравості та контрастності екрана відповідно до освітлення, використання антирефлексних екранів або окулярів.

Таким чином, раціональна організація робочого процесу з дотриманням правил охорони праці дозволяє мінімізувати негативний вплив на здоров’я працівників, запобігти професійним захворюванням та забезпечити ефективність діяльності. Створення безпечного середовища є важливим компонентом роботи з цифровими технологіями.

4.2 Фактори, що впливають на функціональний стан користувачів комп’ютерів

Функціональний стан користувачів комп’ютерів визначається низкою взаємопов’язаних чинників, які впливають на фізичне, психоемоційне та когнітивне здоров’я. У сучасних умовах, коли цифрові технології займають ключову роль у професійній діяльності, необхідно враховувати специфічні особливості, які можуть як позитивно, так і негативно впливати на працездатність працівників. Важливо створити умови, які мінімізують вплив негативних факторів та забезпечують оптимальну ефективність роботи.

Фізичні фактори

Вплив статичної позиції:

– Тривале сидіння в одній позі викликає застійні явища у кровоносній системі, особливо в нижніх кінцівках, що підвищує ризик варикозного розширення вен.

– Надмірне навантаження на певні групи м’язів (спина, шия, кисті рук) спричиняє розвиток м’язових спазмів і хронічного болю.

Робоче середовище:

– Робота в приміщеннях із недостатнім рівнем природного освітлення або вентиляції призводить до зниження рівня кисню в крові, що впливає на загальне самопочуття.

– Шумове забруднення, навіть незначне, може викликати підвищену стомлюваність, оскільки організм витрачає ресурси на адаптацію до сторонніх звуків.

Вплив електромагнітного випромінювання:

– Постійне перебування біля комп’ютерної техніки створює вплив низькочастотного електромагнітного випромінювання, що може негативно позначатися на функціях нервової та ендокринної системи.

Контакт із периферійними пристроями:

– Використання комп’ютерної миші, клавіатури та інших периферійних пристроїв без належного дизайну може спричинити мікротравми суглобів, такі як тендиніт.

Психоемоційні фактори

– Інформаційний стрес. Робота з великими обсягами інформації, дедлайни та необхідність швидкого прийняття рішень викликають перевантаження психіки. Постійне напруження може призводити до хронічної втоми.

– Монотонність діяльності. Виконання одноманітних завдань знижує мотивацію та викликає емоційне виснаження.

– Соціальна ізоляція. Тривала робота за комп’ютером може знижувати рівень живого спілкування, викликати почуття самотності та впливати на загальний психоемоційний стан.

– Робота під тиском. Наявність суворих дедлайнів або складних завдань підвищує рівень тривожності, провокує зниження емоційного балансу та професійне вигорання.

Когнітивні фактори

– Багатозадачність. Робота у цифровому середовищі часто потребує виконання кількох завдань одночасно. Це створює перевантаження когнітивних ресурсів, що знижує ефективність і збільшує ризик помилок.

– Складність завдань. Виконання аналітичних завдань із високим рівнем складності потребує значних розумових зусиль, що може викликати когнітивне виснаження.

– Технічні проблеми. Збої в роботі програмного забезпечення чи обладнання створюють перешкоди для виконання завдань, викликають фрустрацію та знижують продуктивність.

– Навчання новим технологіям. Постійна необхідність адаптуватися до змін у програмному забезпеченні чи технологіях створює додатковий когнітивний тиск.

Організаційні фактори

– Нечіткість робочого процесу. Відсутність зрозумілих регламентів чи процедур викликає плутанину, збільшує ймовірність помилок і знижує продуктивність.

– Нерівномірний розподіл обов’язків. Надмірне навантаження на окремих працівників спричиняє перевтому, тоді як недостатнє завантаження інших знижує їхню залученість.

– Недостатнє технічне забезпечення. Використання застарілого обладнання чи програмного забезпечення уповільнює роботу, створює перешкоди та додатковий стрес.

– Відсутність належного режиму роботи. Неврахування необхідності регулярних перерв та неправильно організований графік збільшують ризик професійного вигорання.

Рекомендації для покращення функціонального стану

Організація робочого середовища:

– Забезпечення комфортного мікроклімату (температура, вологість, вентиляція).

– Налаштування освітлення для уникнення перенапруження зору.

Підтримка фізичного стану:

– Виконання регулярних фізичних вправ для розминки м’язів спини, шиї та кистей рук.

– Впровадження правил гігієни зору, таких як правило «20-20-20».

Психологічна підтримка:

– Організація можливостей для живого спілкування між працівниками.

– Проведення тренінгів із подолання стресу та управління часом.

Оптимізація робочих процесів:

– Впровадження автоматизації рутинних завдань.

– Чітке регламентування робочих процедур і справедливий розподіл обов’язків.

Навчання та підтримка:

– Регулярне підвищення кваліфікації працівників із освоєння нових технологій.

– Забезпечення оперативної технічної підтримки.

Отже, розуміння та врахування фізичних, психоемоційних, когнітивних і організаційних чинників дозволяє мінімізувати їхній негативний вплив на функціональний стан користувачів комп’ютерів. Комплексний підхід до організації роботи сприяє покращенню здоров’я, підвищенню ефективності працівників та загальній продуктивності.

ВИСНОВКИ

У рамках виконання кваліфікаційної роботи на тему «Використання OSINT-технологій при розкритті шахрайств, учинених в кіберпросторі» реалізовано комплексний підхід до дослідження і вирішення поставлених завдань, що дозволило досягти основної мети роботи.

У першому розділі детально розглянуто теоретичні основи шахрайств у кіберпросторі, наведено дефініцію поняття кіберзлочинів, охарактеризовано їх класифікацію відповідно до нормативно-правових баз, які регулюють боротьбу з кіберзлочинністю в Україні та світі, включно з аналізом Будапештської конвенції, а також визначено ключові особливості шахрайських схем, які базуються на використанні сучасних інформаційних технологій. Закцентовано на проблемах ідентифікації цифрових слідів, зумовлених високим рівнем анонімності злочинців, і надає детальну характеристику сучасних методів здійснення шахрайств, таких як фішинг, соціальна інженерія, використання шкідливого програмного забезпечення та маніпуляції через криптовалютні транзакції.

Другий розділ присвячено аналізу методологічних підходів і особливостей застосування OSINT-технологій. У ньому досліджено функціональні можливості сучасних інструментів, таких як Maltego, Recon-ng, SpiderFoot, Shodan та The Harvester, які забезпечують автоматизоване отримання, структурування та аналіз даних із відкритих джерел.

Значну увагу приділено аналізу соціальних платформ (зокрема, Facebook, Twitter, LinkedIn), які є основними середовищами поширення шахрайських схем. Використання OSINT дає змогу ідентифікувати підозрілі облікові записи, встановлювати мережеві зв’язки між ними та вивчати поведінкові моделі.

Окремо розглянуто методи обробки даних із публічних реєстрів, таких як WHOIS і OpenCorporates, які містять інформацію про реєстрацію доменів, юридичних осіб і фінансових установ, що активно використовуються у шахрайських операціях.

Особливий акцент зроблено на застосуванні OSINT-технологій для аналізу криптовалютних транзакцій за допомогою таких платформ, як Chainalysis. Ці платформи дозволяють відстежувати анонімні фінансові потоки та встановлювати джерела фінансування шахрайських схем.

Також розглянуто можливості OSINT Framework, інтерактивної платформи, що інтегрує різноманітні інструменти й методики OSINT для пошуку та аналізу інформації. OSINT Framework є універсальним інструментом, який дозволяє адаптувати роботу до специфіки конкретних шахрайських схем завдяки інтеграції засобів роботи із соціальними мережами, криптовалютними платформами, реєстраційними базами та геолокаційними даними.

Крім того, у розділі проаналізовано застосування протоколу Берклі, який є ефективним інструментом для оптимізації роботи з великими обсягами даних, отриманими з відкритих джерел. Протокол дозволяє швидко сортувати й відбирати релевантну інформацію, що значно скорочує час на її обробку та підвищує ефективність аналітичних систем.

Особливу увагу приділено аналізу метаданих, які використовуються для відновлення часових і просторових характеристик цифрових слідів. Це має вирішальне значення для формування доказової бази, необхідної під час розслідування кіберзлочинів.

Третій розділ дослідження зосереджений на розробці методології застосування OSINT-технологій для ідентифікації та розкриття шахрайських дій у кіберпросторі, що ґрунтується на науково обґрунтованих підходах та сучасних технічних рішеннях. У цьому розділі представлено структурований підхід до впровадження технологій OSINT у правоохоронну практику, де кожен етап має чітко окреслені завдання, алгоритми реалізації та рекомендовані інструменти, які забезпечують підвищення ефективності розслідувань.

Ключові етапи методології описано з урахуванням специфіки кіберзлочинів. Зокрема, етап збору інформації включає використання відкритих джерел, таких як соціальні мережі, онлайн-форуми, публічні бази даних та цифрові платформи. Для забезпечення всебічності дослідження запропоновано застосування низки OSINT-інструментів, серед яких Maltego, Shodan, SpiderFoot, а також

спеціалізовані сервіси для аналізу метаданих та геолокаційної інформації. Ці інструменти забезпечують високий рівень автоматизації процесів збору даних та підвищують точність аналізу.

Особлива увага приділяється етапу аналізу зібраної інформації, що включає ідентифікацію цифрових слідів, встановлення зв'язків між суб'єктами шахрайської діяльності та формування доказової бази. Для кожного етапу запропоновано практичні кейси, які ілюструють дієвість розробленого підходу. Наприклад, розглянуто конкретний випадок розкриття фішингових атак, де за допомогою OSINT-методів було виявлено інфраструктуру зловмисників та заблоковано їх діяльність.

Крім того, розділ акцентує увагу на процедурі документування електронних доказів, яка є важливим компонентом будь-якого розслідування у цифровому середовищі. Описані методи автентифікації зібраних даних та представлені рекомендації щодо використання спеціалізованих програмних засобів для забезпечення їх достовірності.

Висновки роботи підкреслюють актуальність і значущість проведеного дослідження, особливо в умовах зростання кількості кіберзлочинів у сучасному суспільстві. Доведено, що використання OSINT-технологій є не лише ефективним, але й необхідним інструментом у боротьбі з шахрайствами, учиненими в кіберпросторі. Результати дослідження мають як теоретичну, так і практичну цінність, оскільки були впроваджені в освітній процес Донецького державного університету внутрішніх справ (відповідно до Акту впровадження результатів науково-дослідної роботи в освітній процес від 18.12.2024 року), зокрема під час викладання таких освітніх компонентів, як «Пошук інформації з відкритих джерел (OSINT) працівниками кримінальної поліції» та «Інформаційно-аналітичне забезпечення підрозділів кримінальної поліції». Крім того, отримані результати впроваджено в науково-дослідну діяльність університету (згідно з Актом впровадження результатів науково-дослідної роботи в науково-дослідну діяльність від 18.12.2024 року).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кримінальний процесуальний кодексу України від 13 квітня 2012 року № 4651-VI. Дата оновлення: 21 листопада 2024 року. Вебпортал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text

2. Цивільний процесуальний кодекс України від 18 березня 2004 року № 1618-IV. Дата оновлення: 19 жовтня 2024 року. Вебпортал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/1618-15#Text

3. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. Сайт офісу Генерального прокурора. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2

4. Про основні засади забезпечення кібербезпеки України : закон України від 17.08.2022 № 2163-VIII. Вебпортал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

5. Білобров Т.В. Адміністративно-правовий статус Департаменту кіберполіції Національної поліції України : дис. … канд. юр. наук. Київ, 2020. 209 с.

6. Кравцова М.О. Сучасний стан і напрями протидії кіберзлочинності в Україні. Вісник кримінологічної асоціації України. 2018. №2 (19). С. 155-166.

7. Гавловський В.Д. Аналіз стану кіберзлочинності в Україні. Інформація і право. 2019. №1 (28). С. 108-117.

8. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. Дата оновлення: 28 червня 2024 року. Вебпортал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

9. Конвенція про кіберзлочинність: Міжнародний документ Ради Європи від 23.11.2001, ETS №185. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

10. Про ратифікацію Конвенції Ради Європи про кіберзлочинність: Закон України від 07.09.2005 № 2824-IV. URL: https://zakon.rada.gov.ua/laws/show/2824-15#Text

11. Про затвердження Типологій легалізації (відмивання) доходів, одержаних злочинним шляхом, у 2013 році : наказ Державної служби фінансового

моніторингу України від 25.12.2013 № 157. URL: https://zakon.rada.gov.ua/laws/show/v0157827-13#Text

12. Когут Ю.І. Кібервійни, кібертеторизм, кіберзлочинність (концепції, стратегії, технології) : практичний посібник / Ю.І. Когут. – Київ : Консалтингова компанія «СІДКОН» ; ВД «Дакор» 2023. – 284 с.

13. Захист інформаційного та кіберпростору [сайт]. URL: https://ssu.gov.ua/zabezpechennia-informatsiinoi-bezpeky

14. Про критичну інфраструктуру: Закон України від 16 листопада 2021 року № 1882-IX. Дата оновлення: 21 вересня 2024 року. Вебпортал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

15. Структура та функції органів (підрозділів) Національної поліції України. Сайт Національної поліції України. URL: https://www.npu.gov.ua/pro-policiyu/struktura-nacionalnoyi-policiyi

16. Кіберполіція України. Офіційний сайт кіберполії Національної поліції України. URL: https://cyberpolice.gov.ua/

17. Про електронні документи та електронний документообіг: Закон України від 22 травня 2003 року № 851-IV. Дата оновлення: 31 грудня 2023 року. Вебпортал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text

18. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 5 жовтня 2017 року № 2155-VIII. Дата оновлення: 15 листопада 2024 року. Вебпортал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2155-19#n3

19. Стратегія кібербезпеки України: затв. Указом Президента України від 26 серпня 2021 року № 447/2021. Вебпортал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

20. Організація розкриття шахрайств, учинених в кіберпросторі / Шевчишен А. В., Романов М. Ю., Волобоєв А. О., Лунгол О. М., Габорець О. А., Головкін С. В.; за заг. ред С. С. Вітвіцького. Київ : Алерта, 2023. – 200 с.

21. Haborets O. The impact of cyber threats on community and citizen security: analysis and perspectives on resolution. Взаємодія державних органів та громадськості у сфері протидії кримінальним правопорушенням у центральних

регіонах України : матеріали круглого столу (17 квітня 2024 року, м. Кропивницький). Кропивницький : ДонДУВС, 2024. С. 36–37.

22. Muzh V. Computer technologies as an object and source of forensic knowledge: challenges and prospects of development / Valerii Muzh, Taras Lechachenko // Scientific Journal of TNTU. – Tern. : TNTU, 2024. – Vol 115. – № 3. – P. 17-22.

23. InformNapalm. International Volunteer Community. URL: https://informnapalm.rocks/

24. Molfar – OSINT. URL: https://molfar.com/

25. Центр дослідження ознак злочинів проти національної безпеки України, миру, безпеки людства та міжнародного правопорядку «Миротворець». URL: https://myrotvorets.center/

26. Беллінгкет українською мовою. URL: https://uk.bellingcat.com/

27. Haborets O.A. The role of open sources of information (OSINT) in detecting and countering disinformation in the modern information space. Цифровізація вищої освіти та цифрова грамотність: матеріали науково-педагогічного підвищення кваліфікації, 29 січня – 10 березня 2024 року. – Львів – Торунь : Liha-Pres, 2024. С. 44-45.

28. Haborets O. A. OSINT: a scientific approach to informed decision-making. Актуальні проблеми кібербезпеки в Україні в умовах воєнного стану: матеріали міжвідомчого науково-практичного круглого столу (м. Київ, НАВС, 25 квітня 2024 р.).: Нац. акад. внутр. справ, 2024. 144 с.. НАВС, Київ – 25.04.2024. С.32-33.

29. Торбас О. О. OSINT при розслідуванні кримінальних правопорушень : підручник / О. О. Торбас. – Одеса : Видавництво «Юридика», 2024. – 180 с.

30. Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних. Berkeley Law : website. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf

31. OSINT Framework. URL: https://osintframework.com

32. Tymoshchuk, D., Yasniy, O., Mytnyk, M., Zagorodna, N., Tymoshchuk, V., (2024). Detection and classification of DDoS flooding attacks by machine learning methods. CEUR Workshop Proceedings, 3842, pp. 184 - 195.

33. Wayback Machine. URL: https://web.archive.org/

34. Maltego. URL: https://www.maltego.com

35. Lypa, B., Horyn, I., Zagorodna, N., Tymoshchuk, D., Lechachenko T., (2024). Comparison of feature extraction tools for network traffic data. CEUR Workshop Proceedings, 3896, pp. 1-11.

36. SpiderFoot. URL: https://github.com/smicallef/spiderfoot

37. Габорець О., Шаєц Є. Використання OSINT: інноваційні підходи до збору та аналізу відкритих даних для забезпечення безпеки та розвідувальної діяльності. Теоретико-прикладні проблеми кримінального процесу та криміналістики в умовах воєнного стану : тези доп. Між-народ. наук.-практ. конф. (м. Кам'янець-Подільський, 24 листоп. 2023 р.) / МВС України, Харків. нац. ун-т внутр. справ, Наук. парк «Наука та безпека», ф-т № 1. – Кам'янець-Подільський : ХНУВС, 2023. С. 82-83.

38. IBM i2 Analyst's Notebook. URL: https://www.ibm.com/support/pages/download-ibm-i2-analysts-notebook-931

39. ТИМОЩУК, Д., ЯЦКІВ, В., ТИМОЩУК, В., & ЯЦКІВ, Н. (2024). INTERACTIVE CYBERSECURITY TRAINING SYSTEM BASED ON SIMULATION ENVIRONMENTS. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (4), 215-220.

40. Linkurious. URL: https://linkurious.com

41. ТИМОЩУК, Д., & ЯЦКІВ, В. (2024). USING HYPERVISORS TO CREATE A CYBER POLYGON. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (3), 52-56.

42. Tymoshchuk, D., & Yatskiv, V. (2024). Slowloris ddos detection and prevention in real-time. Collection of scientific papers «ΛΌГОΣ», (August 16, 2024; Oxford, UK), 171-176.

43. Muzh, V., & Lechachenko, T. (2024). Computer technologies as an object and source of forensic knowledge: challenges and prospects of development. Вісник Тернопільського національного технічного університету, 115(3), 17-22.

44. Shodan. URL: https://www.shodan.io

45. Tymoshchuk, V., Vorona, M., Dolinskyi, A., Shymanska, V., & Tymoshchuk, D. (2024). SECURITY ONION PLATFORM AS A TOOL FOR DETECTING AND ANALYSING CYBER THREATS. Collection of scientific papers «ΛΌГОΣ», (December 13, 2024; Zurich, Switzerland), 232-237.

46. TheHarvester. URL: https://github.com/laramies/theHarvester

47. Лунгол О.М., Габорець О.А. OSINT-технології в правоохоронній діяльності: навчальний посібник. Мультимедійне видання. Кропивницький: Book Creator, 2023. 107 с.

48. Hunchly. URL: https://hunch.ly

49. Tymoshchuk, V., Vantsa, V., Karnaukhov, A., Orlovska, A., & Tymoshchuk, D. (2024). COMPARATIVE ANALYSIS OF INTRUSION DETECTION APPROACHES BASED ON SIGNATURES AND ANOMALIES. Матеріали конференцій МЦНД, (29.11. 2024; Житомир, Україна), 328-332.

50. Tymoshchuk, V., Mykhailovskyi, O., Dolinskyi, A., Orlovska, A., & Tymoshchuk, D. (2024). OPTIMISING IPS RULES FOR EFFECTIVE DETECTION OF MULTI-VECTOR DDOS ATTACKS. Матеріали конференцій МЦНД, (22.11. 2024; Біла Церква, Україна), 295-300.

51. Social-Engineer Toolkit. URL: https://github.com/trustedsec/social-engineer-toolkit

52. Tymoshchuk, V., Pakhoda, V., Dolinskyi, A., Karnaukhov, A., & Tymoshchuk, D. (2024). MODELLING CYBER THREATS AND EVALUATING THE PERFORMANCE OF INTRUSION DETECTION SYSTEMS. Grail of Science, (46), 636–641. https://doi.org/10.36074/grail-of-science.29.11.2024.081

53. Stanko, A., Wieczorek, W., Mykytyshyn, A., Holotenko, O., & Lechachenko, T. (2024). Realtime air quality management: Integrating IoT and Fog computing for effective urban monitoring. CITI, 2024, 2nd.

54. Talkwalker. URL: https://www.talkwalker.com

55. Derkach, M., Skarga-Bandurova, I., Matiuk, D., & Zagorodna, N. (2022, December). Autonomous quadrotor flight stabilisation based on a complementary filter and a PID controller. In 2022 12th International Conference on Dependable Systems, Services and Technologies (DESSERT) (pp. 1-7). IEEE.

56. Mishko, O., Matiuk, D., & Derkach, M. (2024). Security of remote iot system management by integrating firewall configuration into tunneled traffic. Вісник Тернопільського національного технічного університету, 115(3), 122-129.

57. Social Mention. URL: https://www.socialmention.com

58. Муж, В. В. (2015). Правова свідомість як мотив правомірної поведінки. Вісник Національного університету Львівська політехніка. Серія: Юридичні науки, (824), 278-282.

59. Муж, В. В., & Гарасимів, Т. З. (2015). Юридичне моделювання правової свідомості у контексті юридичної доктрини. Вісник Національного університету Львівська політехніка. Серія: Юридичні науки, (824), 283-289.

60. ZeroFOX. URL: https://www.zerofox.com

61. Stadnyk, M. (2016, February). The informative parameters determination for a visual system diagnostics by using the steady state visual evoked potentials. In 2016 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET) (pp. 800-803). IEEE.

62. DarkOwl. URL: https://www.darkowl.com

63. Cybersixgill. URL: https://cybersixgill.com

64. LogRhythm. URL: https://logrhythm.com

Додаток А Публікація

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

Кафедра інформаційних технологій

та кібербезпеки ННІ № 1

Присвячується
35-річчю кафедри інформаційних технологій та кібербезпеки

МАТЕРІАЛИ

міжвідомчого науково-практичного круглого столу на тему:

«АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ В УКРАЇНІ В УМОВАХ ВОЄННОГО СТАНУ»

(м. Київ, НАВС, 25 квітня 2024 року)

Київ – 2024

Список використаних джерел:

1. Боднар І. Р. Інформаційна безпека як основа національної безпеки. Механізм регулювання економіки. 2014. № 1. С. 68–75.
2. Панченко О. Інформаційна складова національної безпеки. Вісник Національної академії Державної прикордонної служби України. 2019. Випуск 3. URL: https://www.rdc.org.ua/download/stati/Informational-warehouse.pdf (дата звернення: 15.04.2024).
3. Паш Б. В. Складові інформаційної безпеки держави: постановка питання. Закарпатські правові читання. 2017. Том 1. С. 509–512.
4. Кобко Є. В. Інформаційна безпека в системі національної безпеки: сучасність і перспективи. National law journal: teory and practice. 2019. March. С. 46–50.
5. Гаврильців М. Т. Інформаційна безпека держави в системі національної безпеки України. Юридичний науковий електронний журнал. 2020. № 2. С. 200–203.
6. Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС і навчальному процесі : збірник наукових статей за матеріалами доповідей Всеукраїнської науково-практичної конференції 23 грудня 2016 року / упорядник Т. В. Магеровська /. Львів : ЛьвДУВС, 2017. 313 с.

Haborets Olha Andriivna
PhD, Associate Professor of the Department of Operational-search Activities and Information Security of Donetsk State University of Internal Affairs

OSINT: A SCIENTIFIC APPROACH TO INFORMED DECISION-MAKING

In the current era of rapid technological progress and widespread internet availability, Open Source Intelligence (OSINT) technologies demonstrate substantial authority in the processes of sourcing, analyzing, and utilizing information. This dominance stems from their capacity to systematically navigate the vast expanse of digital data, extracting valuable insights crucial for informed decision-making across various domains.

OSINT entails the systematic gathering, examination, and utilization of publicly available information from diverse sources to draw meaningful conclusions and comprehend various situations. This methodology finds application across intelligence, cybersecurity, competitive analysis, law enforcement, and other sectors where access to open information enhances decision-making processes. It relies on sources like social media, public databases, websites, and forums.

Within the domain of OSINT, researchers and analysts harness specialized tools and techniques to collect, assess, and interpret vast amounts of data, thereby extracting valuable insights [1, p. 92]. This process encompasses revealing information about individuals, companies, organizations, events, technologies, and other pertinent subjects.

However, due to the multifaceted nature of OSINT and the array of associated tools, our focus narrows to a specific aspect within this expansive field - the OSINT Framework. This framework comprises tools and resources tailored to gather and analyze information from publicly available internet sources, facilitating exploration, monitoring, and analysis of various data types to identify patterns, trends, and potential threats. Leveraging OSINT proves indispensable across diverse domains such as cybersecurity, fraud prevention, criminal investigations, incident analysis, and intelligence operations. The abundance of openly accessible internet data provides valuable insights into pinpointing threats, vulnerabilities, suspicious activities, and emerging trends, benefiting both commercial and public sectors by supporting decision-making, compiling statistics, monitoring social media, and gauging public sentiment.

Effectively employing OSINT requires adept skills in information searching, filtering, and analysis, alongside adherence to legal and ethical considerations regarding open information access. This article serves as a valuable resource compilation for newcomers to the OSINT and infosec fields, while seasoned professionals will find it enriching with useful information and unique materials.

Open Source Intelligence involves utilizing publicly available sources to acquire and assess information accessible to the general public, with the primary aim of comprehending given situations or entities through processing and analyzing openly accessible data. With technological advancements and data proliferation, OSINT offers extensive application opportunities across various domains.

In the realm of social networks and media, OSINT encompasses activities such as monitoring social media platforms for interactions, community dynamics, and key individuals, as well as tracking news and content from diverse sources to grasp the prevailing situation.

In geospatial analysis, OSINT utilizes geodata including satellite imagery and geographic information systems to locate objects and scrutinize spatial relationships, while textual and visual information analysis involves employing natural language processing (NLP) algorithms and computer vision technologies.

Integral to OSINT are data analysis platforms like Maltego and Recorded Future, along with ethnographic analysis focusing on sociocultural learning to understand behavioral patterns and cultural differences for effective information contextualization.

The aforementioned OSINT tools are extensively applied in the fields of security, intelligence, business intelligence, and beyond, integrating scientific methodologies and cutting-edge technologies to optimize data collection and analysis, thereby enabling informed and strategic decision-making processes.

References:

1. Zhmur N.V. Mezhdunarodno-pravovye standarty zashhity informacii: otdelnye aspekty. Legeasi Viata. 2014. № 2/2 (266). S. 90-93.

Глущенко Іван Олександрович
курсант 2 курсу факультету № 4 Харківського національного університету внутрішніх справ, рядовий поліції

Науковий керівник:
Світличний Віталій Анатолійович *кандидат технічних наук, доцент, доцент кафедри протидії кіберзлочинності факультету № 4 Харківського національного університету внутрішніх справ*

ДЕЯКІ ОСОБЛИВОСТІ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В ДІЯЛЬНОСТІ ПОЛІЦІЇ УКРАЇНИ

Вступ. Штучний інтелект, впроваджений в різноманітні сфери життя в умовах цифрової революції, дозволяє вирішувати складні завдання за допомогою наукових методів досліджень та обробки інформації. Ця технологія дозволяє створювати та використовувати бази знань, моделі ухвалення рішень і алгоритми роботи з інформацією, щоб досягти поставлених цілей.

Виклад основного матеріалу. Принципи та завдання розвитку технологій штучного інтелекту в Україні законодавчо визнано одним із пріоритетних напрямів у сфері науково-технологічних досліджень. Україна, яка є членом Спеціального комітету із штучного інтелекту при Раді Європи, у жовтні 2019 року приєдналася до Рекомендацій Організації економічного співробітництва і розвитку з питань штучного інтелекту (Organization for Economic Cooperation and Development, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449) [1].

Використання можливостей ШІ у роботі правоохоронних органів, зокрема у напрямі протидії злочинності, є практично затребуваним та актуальним. Можливості програмного забезпечення в частині підтримання правопорядку дають значну перевагу людському потенціалу щодо фіксації, попередження та завчасного реагування на правопорушення. Однією з головних можливостей є використання аналітики даних і машинного навчання для прогнозування злочинів, виявлення злочинців та аналізу моделей злочинності. Це дозволяє