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)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Дослідження використання методів OSINT **при росслідувані кіберінцидентів**

Виконав: студент 6 курсу, групи СБмз-61
спеціальності 125 «Кібербезпека»
(шифр і назва спеціальності)

		Серватнюк М.М.
	(підпис)	(прізвище та ініціали)
Керівник		
	(підпис)	(прізвище та ініціали)
Нормоконтроль		
	(підпис)	(прізвище та ініціали)
Завідувач кафедри		
	(підпис)	(прізвище та ініціали)
Рецензент		
	(підпис)	(прізвище та ініціали)

Тернопіль
2021

Міністерство освіти і науки України

Тернопільський національний технічний університет імені Івана Пулюя

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

Кафедра Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«21» грудня 2021 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня магістр
(назва освітнього ступеня)

за спеціальністю 125 «Кібербезпека»
(шифр і назва спеціальності)

студенту Серватнюку Максиму Миколайовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження використання методів OSINT при розслідувані кіберінцендентів

Керівник роботи Муж Валерій Вікторович
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «___» _____ 20___ року № _____

2. Термін подання студентом завершеної роботи 16 грудня 2021 року

3. Вихідні дані до роботи _____

4. Зміст роботи (перелік питань, які потрібно розробити)

1. Дослідження основних аспектів технології OSINT, її поширення, міжнародний досвід застосування і застосування
2. Здійснення аналізу можливостей методів OSINT та ефективність їх використання при розслідуванні кіберінцендентів
3. Варіанти використання методів OSINT для розслідування кіберінцендентів та можливість імплементації OSINT у системи інформаційної безпеки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

1. Титульний аркуш
2. Мета та актуальність роботи, завдання роботи
3. Джерела отримання відкритої інформації
4. Програмні інструменти OSINT
5. Схема отримання необхідної інформації
6. Етапи планування проведення розвідки з відкритих джерел
7. Практичне використання методів OSINT для збору

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г. М.		21.12
Безпека в надзвичайних ситуаціях	Кисляк В.М. ст. викладач		

7. Дата видачі завдання 18 листопада 2021

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	04.10.21	виконано
2	Аналіз міжнародних джерел	05.10.21	виконано
3	Написання 1-го розділу	20.10.21	виконано
4	Розробка та аналіз задачі	10.11.21	виконано
5	Написання 2-го розділу	16.11.21	виконано
6	Написання 3-го розділу	20.11.21	виконано
7	Отримання питань розділу 4	01.12.21	виконано
8	Оформлення роботи	04.12.21	виконано
9	Перевірка на плагіат	09.12.21	Скидала виконано
10	Попередній захист	17.12.21	
11	Захист	23.12.21	

Студент _____ (підпис) Сенатюк М. М. (прізвище та ініціали)

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

АНОТАЦІЯ

Дослідження використання методів OSINT при розслідувані кіберінцендентів // Дипломна робота ОР «Магістр» // Серватнюк Максим Миколайович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБмз-61 // Тернопіль, 2021 // С. 65 , рис. - 7 , додат. - 1.

Ключові слова: OSINT, ІНФОРМАЦІЯ З ВІДКРИТИХ ДЖЕРЕЛ, ВІДКРИТІ ДЖЕРЕЛА.

Дана магістерська робота присвячена висвітленню питання щодо застосування методів OSINT при розслідуванні кіберінцидентів. Проведено аналіз наявних методів OSINT та можливість їх використання у різних сферах діяльності. Розглянуто варіанти використання методів OSINT при розслідувані кіберінцидентів та можливість імплементації засобів OSINT в систему управління інформаційною безпекою.

У першому розділі було досліджено основні аспекти технології OSINT, її визначення, міжнародний досвід застосування та розглянуто OSINT з юридичної точки зору.

У другому розділі здійснено аналіз можливостей методів OSINT та ефективність їх використання при розслідувані кіберінцидентів.

У третьому розділі розглянуто варіанти використання методів OSINT при розслідувані кіберзлочинів та можливість імплементації OSINT у системи інформаційної безпеки у різних сферах людської діяльності.

Ключові слова: OSINT, ІНФОРМАЦІЯ З ВІДКРИТИХ ДЖЕРЕЛ, ВІДКРИТІ ДЖЕРЕЛА.

ANNOTATION

Investigation of the use of OSINT methods in the investigation of cyber-incidents // Thesis of OR "Master" // Servatnyuk Maxim Nikolaevich // Ternopil National Technical University named after Ivan Pulyuy, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, SBMZ-61 // Ternopil, 2021 // P. 65, fig. - 7, appendix. - 1.

Key words: OSINT, INFORMATION FROM OPEN SOURCES, OPEN SOURCES.

This master's thesis is devoted to the issue of the application of OSINT methods in the investigation of cyber incidents. An analysis of existing OSINT methods and the possibility of their use in various fields of activity. Options for using OSINT methods in the investigation of cyber incidents and the possibility of implementing OSINT tools in the information security management system are considered.

The first section examines the main aspects of OSINT technology, its definition, international experience and considers OSINT from a legal point of view.

The second section analyzes the possibilities of OSINT methods and the effectiveness of their use in the investigation of cyber incidents.

The third section discusses the options for using OSINT methods in the investigation of cybercrime and the possibility of implementing OSINT in information security systems in various fields of human activity.

Зміст

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ,СИМВОЛІВ ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

OSINT - Open source intelligence (Розвідка відкритих джерел)

CCIRM - Collection coordination intelligence requirements management

AIPI - Associazione Internazionale Professori d'Italiano

SSL - Secure Sockets Layer

TLS - Transport Layer Security

API - application programming interface

IP - Internet Protocol

URL - Uniform Resource Locator

IT - Інформаці́йні технолóгії

РОЗВД - Розвідка відкритих джерел

СУІБ - система управління інформаційною безпекою

ФРН - Федеральне міністерство оборони

ШПЗ - шкідливе програмне забезпечення.

ВСТУП

Кілька десятиліть тому найбільш значущі розвідувальні служби світу з величезними бюджетами не могли робити те, що ви маєте в руках сьогодні, лише маючи підключення до Інтернету.

Їм довелося використовувати екстремальні методи шпигунства, такі як прослуховування телефонних розмов, перехоплення пошти та багато соціальної інженерії, щоб просто зібрати достатньо інформації.

Ми сприймаємо це як належне, але сьогодні ми маємо такі технології, про які два-три десятиліття тому розвідувальні служби тільки мріяли.

Як і супутникові знімки всього світу з високою роздільною здатністю, вулиця, яка показує, як місце виглядає фізично, доступ до «темної мережі», де бродять злочинці, люди публікують оновлення та фотографії в соціальних мережах, і багато іншого.

Цей новий тип розвідки з відкритим кодом дав слідчим легший спосіб розв’язувати їхні справи, вони почали називати його OSINT.

OSINT або розвідка з відкритих джерел — це розвідка, яка здійснюється шляхом збору, обробки та передачі інформації з загальнодоступних джерел цільовому одержувачу з метою вирішення певних завдань розвідки. Це важлива дисципліна розвідки, яка повинна бути включена в цикл розвідки, щоб керівники, які ухвалюють рішення та розробляють політику, були повністю поінформовані. Використання та розповсюдження перевіреної інформації з відкритих джерел дає можливість вільного обміну, оскільки при вилученні не використовувалися секретні методи.

Метою даної роботи є дослідження методів OSINT при розслідувані кіберінциндентів.

Для досягнення мети в роботі поставлені наступні завдання:

1. Провести аналіз актуальної теми проблеми та підвищити рівень її значимості.

2. Вивчити стан наявних методів проведення OSINT та їх роль у проведені розслідувань кіберінцидентів.

3. Розробити власні методи проведення OSINT при здійснені розслідування кіберінцидентів та розглянути актуальність імплементація засобів OSINT в СУІП.

Головним теоретичним результатом є вивчення питання застосування методів OSINT при розслідувані кіберінцидентів.

Практичним результатом нашої роботи є реалізація використання технологій OSINT при розслідувані кіберінцидентів.

Апробація результатів роботи. Окремі результати роботи доповідались на IX науково-технічній конференції «Інформаційні моделі, системи та технології», Тернопіль, ТНТУ, 8 – 9 грудня 2021 р.

РОЗДІЛ 1. Теоретичні основи використання методів OSINT.

1.1. Дослідження наявних методів OSINT

Дослідження на основі інформації з відкритим вихідним кодом не є новим видом діяльності для провідних країн світу, і в умовах швидкого розвитку інформаційних технологій методи її використання мають стати предметом відповідних досліджень.

Open Source Intelligence (OSINT) — це концепція, методологія та технологія для отримання та використання військової, політичної, економічної та іншої інформації з відкритих джерел без порушення закону. Використовується для прийняття рішень у сфері національної оборони та безпеки, у розслідуваннях тощо. Включає: збір інформації, реєстрацію, облік та аналіз, аналітичну та синтетичну обробку первинної інформації, зберігання та поширення інформації, інформаційну безпеку та подання. результатів дослідження. Після її аналітичної та синтетичної обробки первинна інформація з відкритих джерел може стати цінним знанням, яке потім може стати таємницею – якщо вона не належить до категорії інформації, яка не може бути віднесена до державної таємниці[1].

Інформацію із відкритих джерел та публічно доступних відомостей можна отримати із:

- Всесвітньої мережі Інтернет, яка включає наступне: форуми, блоги, сайти соціальних мереж, сайти обміну відео, такі як YouTube.com, Вікіпедія, записи Whois зареєстрованих доменних імен, метадані та цифрові файли, веб-ресурси Даркнета, дані геолокації, IP-адреси, люди, пошукові системи, і все, що можна знайти в Інтернеті.

- дипломатичних місій;

- релігійні організації;

- розвідувальні організації загальнонаціонального рівня;

- академічний напрямок; - дисертації, дослідження, та ін.;

- архіви (бібліотеки) та дослідницькі центри;

- «сіра література» - наукові доповіді, економічні звіти, маркетингові дослідження тощо. Такими нерідко тлумачать як публікації, яких немає в широкому доступі, і тому їх важко отримати [25].

В окремих випадках розвідувальні дані з доступних у відкритому доступі джерел не тільки не відрізняються від таємниць, а часто за цінністю перевершують секретну інформацію. Цінність представлених розвідкою даних обумовлена низкою характеристик як-от [8]:

- оперативність, коли в певній географічній точці розгортається криза, а розвідувальні можливості у цьому регіоні невисокі, то експерти розвідувальних служб і ті фахівці, які відповідають за формування державної безпекової політики, частіше шукають інформацію в телеефірі або в мережі Інтернет.

- об’єм - блогерів, журналістів, експертів, науковців та інших експертів у тій чи іншій галузі значно більше, ніж спеціалістів-розвідників. Два або три професійних розвідники з добре налаштованою агентурною мережею зазвичай мають суттєву перевагу над сотнею журналістів щодо можливостей доступу до таємної інформації. Однак, фахово скомпоновані фрагменти інформації, які збираються фахівцями з відкритих джерел, переважно мають більшу вагу, ніж звіти розвідувальних служб.

- якість - у роботі розвідувальних служб непоодинокими є ситуації, коли звіти готуються з опорою на посилання газетних публікацій та сфабрикованої (недостовірної) інформації. Слід зазначити, що інформація з відкритих джерел, порівняно з подібними звітами, незаплямована неправдою.

- ясність - у випадку відкритої інформації надійність відкритих джерел буває зрозумілою, або незрозумілою. Ступінь надійності таємно отриманої інформації у більшості випадків є незрозумілою. - легкість використання - таємниці, приховані за грифами «секретно» та охоронювані спеціальними програмами доступу, зазвичай важко передати фахівця, які відповідальні за прийняття рішення і, навіть, колегам-розвідникам. Інформація РОЗВД є доступною для будь-якої посадової особи.

- вартість - розвідувальний супутник, розробка, запуск та утримування якого коштує дуже дороговартнісним (мільярди доларів США), фотографує дах підприємства, на якому виробляється зброя, або корпус підводної субмарини. Іноземний журнал, передплата якого вартує близько 100 дол. США, може публікувати фотографії, зроблені в цеху заводу або відсіку субмарини. Досліджуючи потенціал, роль та цінність РОЗВД, у науковців нерідко виникають певні помилкові судження. Наприклад позиція, згідно з якою інформація, отримана з джерел, які є відкритими для вільного доступу, за своєю цінністю не переважає інформацію з медійних ресурсів. У реальності OSIF отримують з різних інформаційних джерел, яка в комплексі має багато нюансів [8].

1.2. Міжнародний досвід використання методів OSINT

У 1947 році аналітик ЦРУ Кен Шерман зазначив, що держава отримує з відкритих джерел інформації майже 80 %, пізніше (генерал-лейтенант, керівник Розвідувального управління міністерства оборони США) Самуель Уілсон стверджував що 90 % всієї розвідувальної інформації надходить з відкритих джерел, а лише 10 % – з роботи агентури [6, с. 62].

Сьогодні найповніше використання «OSINT» має місце у США. Цим методом успішно користуються такі впливові організацій як-от:

- Академія відкритих джерел;
- Департамент передових систем (ASD);
- Рада із захисту відкритих джерел;
- Розвідувальне управління Міністерства оборони США;
- Командування розвідки і безпеки ЗС США;
- Дослідницька служба бібліотеки Конгресу США (Congressional Research Service) тощо.

Сьогодні багато урядових та комерційних інституцій у США широко використовують інформацію, отриману за допомогою розвідки за відкритими джерелами. Переважно таку інформацію використовують у стратегічних цілях:

планування бойових дій, організація та проведення секретних військових операцій, запобігання терористичним терактам тощо [6]. На переконання експертів розвідки США найбільшою на даний момент проблемою «OSINT» є неперевірені джерела інформації, недостовірна інформація, які нерідко провокують прийняття неефективних чи загрозливих рішень.

Експерти цінують водночас високо цінують потенціал OSINT за те, що розповсюдження та використання перевіреної інформації, яка надійшла з відкритих джерел, забезпечує можливість обміну такою інформації із іноземними партнерами, оскільки у ході її отримання фахівці не використовують приховані методи або заборонені у використанні секретні джерела [8]. Зазначене, означає, що регулятор лобістської діяльності (НРУРЛ), при потрібні, може подавати інформацію, отриману з відкритих джерел, не лише до правоохоронних органів, з метою проведення розслідування та притягнення до відповідальності потенційних правопорушників, а й до медійних структур. Подібна практика дасть можливість НРУРЛ суттєво послабити можливі інформаційні атаки на себе з боку недобросовісних суб'єктів лобіювання, звинувачення в упередженості, обмеженні їх прав тощо. Адже, як відомо, відкритість і публічність регулятора є одним з найбільш ефективних методів захисту репутації останнього від перекручування інформації та відвертої «демонізації» у громадянському суспільстві [10].

У США сформована розгалужена мережа центрів і пунктів, що ведуть OSINT - розвідку та надають відомості більш ніж 7 тис. споживачам розвідувальних даних. І це не що інше, як результат скоординованих дій законодавчої і виконавчої влади, спрямованих на проведення цілеспрямованої політики в галузі забезпечення національної безпеки. Подібні структури є на всіх рівнях.

Нині у правоохоронних органах іноземних держав організовані та успішно функціонують спеціальні підрозділи, що здійснюють кіберрозвідку з опорою на відкриті джерела інформації. Наприклад, таку діяльність за методом Open Source Intelligence здійснюють: Scotland Yard OSINT", "OSINT unit of the Los Angeles

County Sheriff's Department", "Scotland Yard OSINT", "австралійське Управління національних оцінок" та інші служби іноземних держав [9, с. 11; 7].

Зважаючи на міжнародний досвід використання «OSINT» можна зазначити, що для отримання якісної та актуальної інформації необхідно опрацьовувати велику кількість інформаційних джерел. Для правильної та продуктивної роботи цього методу не достатньо лише знаходити інформацію, її треба обробляти, аналізувати, знаходити підтвердження досліджуваних фактів, подій та явищ, адже багато інформації створюється саме для дезінформації. На сьогоднішній день в провідних країнах світу «OSINT» активно та успішно використовується інформаційно-аналітичними підрозділами; дані відсоткового співвідношення продуктивності відкритих джерел інформації підтверджують необхідність та актуальність використання досвіду США та країн Європи для вирішення оперативних, тактичних та стратегічних завдань силових структур [4].

1.3 Правові підстави використання методів OSINT

Збір та аналіз інформації із відкритих джерел як сфера діяльності повинна здійснюватися в межах нормативно-правового поля держави. Основою для цього є забезпечення конституційних прав у сфері пошуку, збору, передачу і використання інформації в усіх демократичних державах. Впровадженню у практику систем розвідки з відкритих джерел сприяють законодавство різних світових держав. Для прикладу, ще в 1996 році в США був прийнятий Закон про свободу інформації, який задекларував обов'язок стосовно спеціальних федеральних відомств забезпечити вільний доступ громадянам до своєї інформації. Закон встановив лише обмеження, які стосуються матеріалів, що стосуються до національної оборони, фінансових та особистих документів, а також документації правоохоронних органів держави. Проте варто зауважити, що в деяких країнах законодавець встановлює обмеження подібну діяльності, де факто забороняючи здійснювати розвідку зі відкритих джерел.

В Україні “кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір” (Конституція України, Розділ 2, ст. 34). В Україні правове регулювання в інформаційній сфері ґрунтується на наступних принципах:

1) Свобода законно шукати, отримувати, передавати, виробляти та поширювати інформацію;

2) встановлювати обмеження на доступ до інформації лише законами держави;

3) відкритість інформації про діяльність державних органів та органів місцевого самоврядування та вільний доступ до такої інформації, крім випадків, передбачених законодавством держави;

4) За категорією доступу інформація поділяється на відкриту (загальнодоступну) та з обмеженим доступом.

Разом з тим, узаконеного поняття “OSINT” в Україні сьогодні не існує, хоча діяльність зі збирання, зберігання, обробки та розповсюдження інформації регулюється цілою низкою законодавчих і нормативних актів:

• Закон України “Про інформацію” від 02.10.92 р. № 2657-XII (зі змінами від 13.01.11 р.), ст. 5–7[11];

• Закон України “Про друковані засоби масової інформації (пресу) в Україні” від 16.11.92 р. № 2782-XII, ст. 6, 25 [12];

• Закон України “Про охоронну діяльність” від 22.03.12 р. № 4616-VI, ст. 9, 13, 19 [13];

• Закон України “Про захист персональних даних” № 2297-VI від 01.06.10 р.[14];

• Цивільний кодекс України (ст. 505), Кримінальний кодекс України (ст. 231, 232), Кодекс України про адміністративні правопорушення (ст. 163, ст. 163); Варто зазначити, що реалізація заходів у частині забезпечення безпеки підприємництва навіть в рамках розвідки з відкритих джерел інформації в окремих випадках сприймається як проведення оперативно-розшукової діяльності, здійснювати яку, згідно із Законом України “Про оперативно-

розшукову діяльність”№ 2135-XII від 18.02.1992 р. [19] вправі тільки суб’єкти, згадані в окремих статтях означених Законів України. У затвердженій Указом Президента України “Стратегії кібербезпеки України” від 15.03.16 р. No96/2016 [18] декларуються основні завдання силовим органам, а також передбачається “створення системи своєчасного виявлення, протидії та нейтралізації кіберзагроз, в тому числі із залученням волонтерських організацій”, все це, безумовно, відноситься до застосування засобів конкурентної розвідки в цій галузі.

При цьому чинним Кримінальним кодексом України передбачена кримінальна відповідальність за незаконне збирання з метою використання або використання відомостей, що становлять комерційну таємницю, а також за розголошення комерційної таємниці. Однак така інформація виходить за рамки розвідки з відкритим джерелом.

При досить широкому та неоднозначному трактуванні законодавчих норм будь-які процедури збору, обробки та зберігання інформації про конкурентів, з одного боку, стають практично безкарними, тобто легітимними, а, з іншого боку, є важко доступними для громадян. В українській практиці фактично насправді закритий доступ до великого пласту вільно доступної в інших демократичних державах інформації, наприклад, щодо земельні ділянки, нерухомості (наявної і закладеної), наявність банківських рахунків і т.п. Більшу частину відомостей можна отримати тільки у результаті консультацій з спеціальними експертами. Нині особливо гостро назріла проблема криміналізації деяких державних служб, які у своїй діяльності використовують розвідку з відкритих джерел. Сьогодні багато підрозділів служб безпеки державної і приватної форм власності користуються базами даних з інформацією про особу (тобто, персональні дані). Подібні інформаційні бази використовуються з позитивною метою, як-от, з ціллю перевірити дані про співробітників, конкурентів чи партнерів. Ймовірно, цими базами даних бізнес-структури і окремі громадяни і надалі будуть користуватися, однак будуть змушені порушувати законодавство «йти в підпілля». Технічно можливість використання та підтримки таких баз даних

забезпечується численними системами типу «Cronos» (оболонки, які продаються легально). За допомогою таких інструментів будь-який зацікавлений користувач Інтернету має доступ до численних баз даних, які працюють під цими оболонками [19]. Сьогодні фундаментальними цінностями людства стають приватність життя особи, разом з правом на захист життя та свободою слова. Інформація про людей – персональні дані сьогодні все більше перетворюється в цінний товар, за який готові платити великі гроші. У руках зловмисника подібна інформація є потужною зброєю. Державні інститути, банківські установи, великі бізнес-корпорації не у всіх випадках спроможні забезпечити самостійно належний захист баз персональних даних, які зберігаються у них, в результаті чого, величезний потік конфіденційної інформації надходить на ринок. Тобто персональні дані важливо надійно захищати.

На сьогодні, основними європейськими правовими стандартами в галузі захисту персональних даних є Конвенція Ради Європи “Про захист осіб у зв’язку з автоматичною обробкою персональних даних” від 28 січня 1981 року (ETS №108) та “Пакет захисту даних” Європейського Парламенту та Ради від 27 червня 2016 року [24], які є обов’язковими для всіх держав-членів Європейського Союзу і які є предметом для наслідування в області законодавства, в тому числі, і нашою країною. Країни Євросоюзу мають приводити своє законодавство у відповідність зазначеним правовим стандартам. Право на приватність гарантується Конституцією України. Стаття 32 Конституції України говорить: “Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України”. Крім того в Конституції України передбачений захист ще деяких аспектів приватності. Так, стаття 30 Конституції України захищає недоторканність житла (територіальна приватність), стаття 31 – таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції (комунікаційна приватність), стаття 32 передбачає заборону збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди (інформаційна приватність), а стаття 28 передбачає заборону піддавати особу без її вільної згоди медичним, науковим чи

іншим дослідженням (захищаючи елементи фізичної приватності). Конвенція РЄ про захист осіб у зв’язку з автоматизованою обробкою персональних даних від 28 січня 1981 року (ратифікована Україною 06.07.2010 р.) визначає положення стосовно передачі через національні кордони за допомогою будь-яких засобів персональних даних, що піддаються автоматизованій обробці або зібраних з метою їхньої автоматизованої обробки. Наведені нижче дані, які зазвичай використовуються для ідентифікації особи, визначені Управлінням США з управління та бюджету як особистий:

- повне ім'я та прізвище;
- ідентифікаційний номер;
- IP-адреса (в деяких випадках);
- номер посвідчення водія;
- номери кредитних карток;
- цифрова ідентифікація (цифровий підпис);
- дата народження;
- місце народження;
- генетична інформація [27].

Українське законодавство передбачає інформаційний характер обробки персональних даних. Перед обробкою персональних даних власник або відповідальна особа (оператор) зобов’язані повідомити компетентний орган з питань захисту прав персональних даних про намір обробляти персональні дані. Далі про власника або керівника (оператора) вносяться в спеціальний реєстр операторів. Інформація, що міститься в реєстрі операторів, стає загальнодоступною.

Закони про захист персональних даних поширюються на більшість населення як учасників процесу обробки даних. А оскільки кожен є суб’єктом персональних даних, закон є загальним і поширюється на всіх. Персональні дані

часто використовуються в соціальних мережах і, зокрема, в службах електронної пошти.

Сучасна інтернет-компанія збирає та обробляє різні категорії персональних даних - своїх співробітників, своїх підрядників і деякі дані користувачів її послуг. Люди, які розміщують інформацію про себе в соціальних мережах або сервісах знайомств, свідомо роблять її доступною всім користувачам ресурсу і за законом можуть бути інтерпретовані як «публічні», тобто для цього не потрібна особлива конфіденційність, але в соціальних мережах є також інформація, яку користувач приховує і робить її доступною лише для певної групи користувачів («друзів»). У цьому випадку інтернет-ресурс повинен запропонувати спеціальні заходи захисту.

Органи, які здійснюють розвідувальну інформацію з відкритих джерел, обробляють персональні дані, які є загальнодоступними, тобто загальнодоступними, в мережі Інтернет. Для обробки згоди суб'єкта даних персональні дані не потрібні.

Проте довести, що оброблені персональні дані є загальнодоступними, є обов'язком власника або адміністратора. Це означає, що ви повинні або надати докази того, що дані були взяті з загальнодоступних джерел, або отримати згоду суб'єкта даних, а потім зберегти цей документ. Крім того, необхідно мати документ, що підтверджує публічну доступність джерел персональних даних. При цьому без відповіді залишається питання про підтвердження власником інформаційного ресурсу (веб-сайту) письмової згоди на обробку.

Висновки до першого розділу

У даному розділі було розглянуто теоретичний аспект методів OSINT. Здійснено аналіз джерел відкритої інформації та їх цінність. OSINT по своїй суті це технологія добування і використання інформації із відкритих джерел, без порушення законів.

Основним завданням розділу був загальний огляд методів OSINT, способів їх застосування та правовий аспект їх використання. Визначено чим регламентовано здійснення збору інформації із відкритих джерел в Україні.

Окремо було розглянуто міжнародний досвід використання OSINT. Як методи OSINT використовуються в інших країнах і їх роль у країнах. Міжнародний досвід використання OSINT свідчить, що методи OSINT у більшості випадків використовуються для планування бойових дій, для організації та проведення військових дій та для запобігання терористичним нападам. Використовують методи OSINT – військові, правоохоронні органи та журналісти. Таким чином OSINT виступає як незалежний і повноцінний інструмент захисту держави та суспільства. Тому методи OSINT активно та успішно використовуються у всьому світі для розслідування інцидентів та захисту громадян.

Розділ 2. Ефективність використання методів OSINT при розслідувані кіберінциндентів

2.1. Основні джерела та можливості OSINT

Реалізація OSINT розвідки зазвичай здійснюється за трьома основними типами отримання інформації: пасивного, напівпасивного та активного. Вибір максимально ефективного типу великою мірою залежить від сценарію, за яким здійснюється процес збору інформації, а також від типу даних, які цікавлять суб'єкта збору інформації.

Пасивний збір інформації тлумачать як тип збору та обробки даних, який використовується найчастіше. Такий тип акумуляції інформації використовується лише шляхом використання загальнодоступних ресурсів.

У процесі застосування напівпасивного типу збору даних з технічного боку даний тип збору інформації направляє обмежений трафік на цільові сервери з метою отримання про них найбільш загальної інформації. Даний трафік служить для нагадування типового інтернет-трафіку, і не має привертати уваги до розвідувальної діяльності відповідних структур з боку громадськості.

Активний тип отримання інформації полягає у втіленні безпосередньої взаємодії із системою, про інформація яку збирається розвідувальними службами. Власник має змогу дізнатися про те, що стосовно нього ведеться інформаційна розвідка, оскільки фізична особа чи організація, яка акумулює інформацію, використовує новітні методи збору технічних даних про цільову IT-інфраструктуру, як-от сканування вразливостей (наприклад, неліцензійний Windows), сканування додатків веб-сервера, доступ до відкритих портів та ін. д. Такий трафік буде викликати підозру або тлумачитися як зловмисна поведінка і залишить сліди у системі виявлення вторгнень (IDS) чи системі запобігання таких вторгнень (IPS). Здійснення атак з боку соціальної інженерії тлумачиться як один із видів активного збору інформаційних даних [11].

Для здійснення подібної розвідки необхідно використовувати відповідні інструменти, для яких надано доступ до відкритих джерел інформації. До

найбільш популярними інструментами збору інформації з відкритих джерел та стеку програмних продуктів відносяться: Google Dorks, Foca, Shodan, Maltego, Spyse.

Shodan – пошуковик по пристроях, підключених до мережі (в т.ч. інтернет і веб-додатки). За допомогою даного веб ресурса можна побачити можливі вразливості того чи іншого пристрою, який наявний на даному ресурсі.Результати пошуку можна фільтрувати за допомогою таких конструкцій:

• country: країна в форматі UK, RU, US і тощо, наприклад: nginx country: UA

• city: місто, наприклад: nginx city:«Ternopil» country:UA

• os: операційна система, наприклад: microsoft-iis os:«windows 2003»

Для доступу до розширеного пошуку необхідно зареєструватися. Платні версії пропонують доступ до більшої кількості пристроїв і необмежену кількість пошуків на день.

Maltego – програмне забезпечення для пошуку, аналізу інформації та її побудови у схеми зав'язків. Його особливості: візуалізація отриманих даних, уточнення на основі відкритих джерел, комбінація для глибокого аналізу отриманих даних із закритих і відкритих джерел, автоматичний аналіз відкритих джерел і автоматична побудова зв'язків між виявленими об'єктами. Maltego дозволяє компілювати інформацію з відкритих і закритих джерел і візуалізувати агреговані дані.

Google Dork – це запити до Google, які використовують спеціальні оператори. Щоб знайти точний вираз, потрібно взяти слова в лапки, а щоб виключити всі дані з виводу, поставте перед ними «-». Dorking можна використовувати в багатьох пошукових системах, а не тільки в Google. У повсякденному використанні такі пошукові системи, як Google, Bing, Yahoo і DuckDuckGo, приймають пошуковий запит або пошуковий рядок і надають релевантні результати. Крім того, ті самі системи запрограмовані на прийом більш просунутих і складних операторів, що значно обмежує ці умови пошуку.

Оператор – це ключове слово або фраза, яка особливо актуальна для пошукової системи.

Крім того, Google Dorking також може знаходити приховані сторінки входу, повідомлення про помилки, які розкривають інформацію про доступні вразливості безпеки та спільні файли. Основна причина в тому, що адміністратор веб-сайту міг просто забути виключити з загального доступу. Найпрактичнішим і водночас найцікавішим сервісом Google є можливість пошуку віддалених або заархівованих сторінок. Це можна зробити за допомогою оператора Cache:. Оператор працює таким чином, що показує збережену (віддалену) версію сайту, яка зберігається в кеші Google.

Крім цих інструментів існує і інші не менш корисні ресурси для розвідки з відкритих джерел інформації. Серед таких інструментів ресурсів можна виділити:

Lampyr - це програмне забезпечення яке дає змогу здійснювати пошук за багатьма критеріями. Крім цього, данний ресурс має веб-версію яка є обмеженою десктоп версії. За допомогою Lampyr можна візуалізувати інформацію та зв'язки за допомогою таблиці, карти, графіка та все разом. Також присутня функція імпорту даних для її візуалізації та можливого подальшого пошуку зав'язків чи іншої інформації з відкритих джерел.

OSINT Framework що знаходиться за адресою: https://osintframework.com/. Даний ресурс по суті являє собою збірник ресурсів для пошуку інформації по категоріям. Аналогом до цього ресурсу можна вважати osint.link де зібрано більший об'єм ресурсів для здійснення пошуку інформації.

Nmap ("Network Mapper") — це програма з відкритим кодом для дослідження мережі та тестування безпеки. Він призначений для швидкого сканування великих мереж, хоча добре працює і для окремих цілей.

Це класика, що не старіє, і перший інструмент, який використовують при проведенні тесту на проникнення. Його функціонал досить великий, але в нашому випадку цікавите буде лише визначення відкритих портів, назви запущених сервісів та їх версій.

SpiderFoot – інструмент розвідки з відкритим вихідним кодом, доступний на Linux і Windows. Він розроблений мовою Python з високою конфігурацією та працює практично на будь-якій платформі. Утиліта інтегрується з простим та інтерактивним графічним інтерфейсом командного рядка. Цей інструмент автоматично дозволив надсилати запити більш ніж до 100 джерел OSINT для отримання інформації про електронні листи, імена, IP-адреси, доменні імена. Він збирає широкий спектр інформації про мету, таку як мережеві блоки, електронна пошта, веб-сервери.

Creepy – інструмент геолокаційної розвідки з відкритим вихідним кодом. Він збирає інформацію про геолокацію за допомогою різних платформ (соціальних мереж та сервісів розміщення зображень). Creepy представляє звіти на карті, використовуючи фільтр пошуку, заснований на точному місці та даті. Ці звіти доступні у форматі CSV або KML для експорту та додаткового аналізу.

Використання інструментів OSINT не є затратною процедурою для організацій. Навіть, якщо той чи інший інструмент вартує досить багато то можливо знайти схоже рішення по функціоналу за більш прийнятну суму або взагалі, яке є безкоштовним. Наприклад програмне забезпечення Maltego у використанні є умовно безкоштовним, де в безкоштовній версії користувач може познайомити із функціоналом та спробувати деякі функції програми, а платних тарифах відкривається повноформатний функціонал програмного забезпечення. Пошук інформації здійснюється з “перетворювачі”, так званими перетворювачами, які налаштовані через API з різними веб-ресурсами для пошуку інформації. Проте, функціонал Maltego дозволяє додавати власні “перетворювачі”, що дає можливість користуватися програмним забезпеченням при правильному налаштуванні, без лишніх затрат.

Також, не будем забувати про програмне забезпечення для здійснення розвідки із відкритих джерел, з відкритим кодом, яке знаходиться на веб-ресурсі “github.com”. Кожен бажаючи може скопіювати репозиторій та спробувати програмне забезпечення самостійно. Пошук такого програмного забезпечення

можна зробити за запитом “github osint”, що покаже можливі інструменти для здійснення OSINT.

2.2 OSINT як превентивні заходи

Фахівці структур, які займаються безпекою, використання методу OSINT допомагає максимально швидко знайти загальнодоступну інформацію про внутрішню діяльність фізичної особи чи підприємства/компанії, а також дані поза їх межами. Нерідко конфіденційна інформація міститься в метаданих, які фізична чи юридична особа опублікувала випадково. До таких даних відносять:

- незахищені підключені та пристрої відкриті порти;
- неоновлене програмне забезпечення;
- назви пристроїв, версії програмного забезпечення, мережі та IP-адреси;
- витік таких даних, як власний код на GitHub.

Від багатьох точок входу в корпоративну мережу залежить безліч векторів атак, доступних зловмиснику. Можна формально класифікувати точки входу:

- інформаційні системи, розташовані на периметрі та мають доступ до інтернету (сервери, робочі станції, адміністративні панелі спеціального обладнання тощо);
- мобільні пристрої, які використовуються співробітниками всередині периметра та за його межами;
- облікові записи у хмарних сервісах співробітників (зокрема які у особистих цілях).

Останній пункт часто вимагає від атакуючого інтерактиву з жертвою (наприклад, комунікацію з об'єктом фішингової атаки), що підвищує ризик виявлення атаки. Тому в деяких випадках пріоритет надається експлуатабельним точкам входу, розташованим на периметрі.

Мережевий периметр - поняття, яке з розвитком технологій та повсюдним впровадженням хмар поступово зникає. Концепція Bring your own device

(BYOD), що дозволяє співробітникам компаній використовувати особисті пристрої для бізнес-процесів, а також появу хмарного середовища розмивають периметр. Контролювати потоки даних між корпоративною мережею та зовнішнім світом стає неймовірно важко. І це полегшує життя зловмисникам — різноманіття варіантів проникнення зростає.

Слід також зазначити, що соціальні мережі та веб-сайти слугують в якості джерелі інформації, особливо про співробітників компанії. Постачальники та партнери фірми нерідко надають відкритий доступ до певних деталей IT-середовища компанії, які краще було б тримати в обмеженому доступі. Крім цього, існує велика кількість неіндексованих файлів та веб-сайтів, які іменують «невидимою мережею». Невидима мережа чи прихована мережа (з англ. deep web), невидима мережа (invisible web) чи прихована мережа (hidden web) технічно залишається загальнодоступними.

Тому методи OSINT можна використовувати для здійснення превентивних заходів реагування на кіберінциденти. Так, заздалегідь провівши розвідку із відкритих джерел інформації про підприємство можна запобігти витоку інформації або запобігти повноцінній кібератаці на організацію. Тобто, подивившись очима хакера на свою компанію, можна дізнатися, яка інформація знаходиться у відкритому доступі. Крім цього, використання методів OSINT є не затратною процедурою для грошового забезпечення компанії та вимагає мінімум таких затрат. Проте результат проведення розвідки із відкритих джерел про організацію та її працівників дозволить захистити бюджет компанії та зберегти конференційну інформацію, через яку організація понесла б великі матеріальні втрати.

Методи та інструменти OSINT дозволяють здійснювати пошук та аналіз інформації. При використані у роботі OSINT, як превентивного заходу можна запобігти повноцінній атаці на організацію чи компанію.

2.3. OSINT як першочергові заходи при розслідувані кіберінциндентів

Досить частими сьогодні є випадки несанкціонованого втручання у роботу будь-якої системи, крадіжки інформації тощо через комп'ютерні мережі. У цьому контексті важливо визначити, що таке кіберінцидент (Cyber incident).

Законом України «Про основні засади кібербезпеки України» кіберінцидент визначено, що інцидент кібербезпеки (далі - кіберінцидент) - це подія або низка небажаних подій ненавмисного характеру (природного, технічного, технологічного), дефектного, також через людський фактор) та/або такі, що мають ознаки можливої (потенційної) кібератаки, що загрожує безпеці систем електронного зв’язку, систем управління процесами, обґрунтовує ймовірність порушення нормальної роботи таких систем (у тому числі виходу з ладу). та/або блокування системи та/або несанкціоноване управління її ресурсами) загрожують безпеці (безпеці) електронних інформаційних ресурсів[21].

Використовуючи методи та інструменти OSINT, які були раніше згадані у роботі, можна здійснити оперативне реагування на любий із видів кіберінциндентів.

Список категорій кіберінцидентів в Україні склав Урядова група реагування на надзвичайні комп’ютерні системи України «CERT-UA», яка виділила 10 категорій:

1. Образливий вміст
2. Шкідливий код
3. Збір інформації зловмисником (збір інформації)
4. Спроби злому
5. Проникнення
6. Порушення доступності
7. Порушення властивостей інформації (безпека інформаційного вмісту)
8. Шахрайство
9. Відома вразливість безпеки

10. Інше

Цей перелік складено на підставі переліку категорій кіберінцидентів, затвердженого Національним координаційним центром з питань кібербезпеки при РНБО України (Протокол № 18 засідання Національної координації кібернетики). Центр безпеки Ради національної безпеки і оборони України 320/21дск)[22].

Процес управління інцидентами – це процес реєстрації інформації про безпеку та збалансованість телекомунікаційних систем (ТКС), передачі інформації до пунктів збору, обробки та аналізу з узгодженням прийняття рішень та формуванням певного управлінського впливу на Об’єкт. адміністрація. Інша класифікація таких дій визначає сім основних груп, які в основному характеризують методи, які зловмисники використовують для здійснення атаки, а саме: підслуховування паролів інших користувачів; «Соціальний розвиток»; Використання програмних помилок і закладок, а також помилок в механізмах ідентифікації користувачів і недосконалості протоколів передачі даних; Отримання інформації про користувачів стандартними засобами операційної системи; Блокування сервісних функцій атакуваної системи.

У Конвенції Ради Європи 2001 року, що спрямована на боротьбу з кіберзлочинністю, йдеться про чотири можливі групи таких дій [2]:

1. інциденти, які мають на меті порушити конфіденційність, цілісність і доступність комп'ютерних даних і систем і вчинені:

- несанкціонований доступ до інформаційного середовища (незаконний навмисний доступ до комп'ютерної системи або її частин та до Інтернет-протоколу (IP) іншої сторони в обхід систем безпеки);

- втручання в дані (незаконна зміна, пошкодження, видалення, фальсифікація або блокування комп'ютерних даних і команд управління шляхом кібератак на інформаційні системи, ресурси та мережі державного та військового управління);

- порушення роботи системи (незаконне порушення або перешкоджання роботі комп'ютерної системи шляхом розробки та розповсюдження вірусних

SPZ, використання апаратних закладок, електронних та інших впливів на технічні засоби та системи телекомунікацій і зв'язку, обробки та передачі інформації, системи захисту IP , системи та мережі, програмне та математичне програмне забезпечення, протоколи передачі даних, алгоритми адресації та маршрутизації);

- незаконне прослуховування (незаконне, навмисне аудіовізуальне та/або електромагнітне прослуховування комп'ютерних даних, не призначених для загального доступу);

- незаконне використання комп'ютерної та телекомунікаційної техніки або повна їх конфіскація.

2. Комп'ютерне шахрайство та підробка:

- підробка документів за допомогою комп'ютерних засобів (незаконне навмисне введення, зміна, видалення або блокування комп'ютерних даних, що знижує достовірність документів);

- шахрайство у використанні комп'ютерних засобів (втручання у функціонування комп'ютерної системи з метою умисного неправомірного отримання економічної вигоди).

3. Інциденти, пов'язані з розміщенням нелегальної інформації в мережах.

4. Інциденти, пов’язані з авторськими та суміжними правами.

Найпоширеніші інциденти такого типу включають витік конфіденційної інформації; незаконний доступ до інформації; Відновлення інформації; компрометуюча інформація; саботаж; IT-шахрайство; ненормальна мережева активність; ненормальна поведінка бізнес-додатків; використання активів установи в особистих цілях або шахрайські операції.

Законодавство України визначає кібератаки як цілеспрямовані (навмисні) дії у кіберпросторі, що здійснюються засобами електронного зв’язку (включаючи інформаційно-комунікаційні технології, програмне забезпечення, програмно-апаратне забезпечення, інші техніко-технологічні засоби та обладнання), спрямовані на одну або поєднання таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів,

що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, несанкціонований доступ до цих ресурсів; порушення безпеки, сталого, надійного та нормального функціонування комунікаційних та/або технологічних систем; використання системи зв'язку, її ресурсів та електронних засобів зв'язку для здійснення кібератак на інші об'єкти кіберзахисту.

Зовнішній кіберінцидент – це той, який походить від зловмисника, який не має прямого відношення до жертви. Системні події такого типу включають шахрайство в системах електронного документообігу; атаки відмови в обслуговуванні (DoS), включаючи розподілені (DDoS) атаки; Перехоплення та заміна трафіку; неналежне використання бренду закладу в мережі Інтернет; фішинг; публікація конфіденційної (провокаційної) інформації в мережі Інтернет; злом або спроба зламати мережеві вузли; сканування порталу закладу чи мережі, вірусні атаки; незаконний доступ до конфіденційної інформації; анонімні листи (листи з погрозами) тощо [24].

Розвиток кібератак за останні роки свідчить про те, що докорінно змінюються не лише суб'єкти та об'єкти кібервпливу, а й їх цілі та завдання – від примітивних кібератак на компанію-конкурента до міжнародних протистоянь у кіберпросторі. Різкі зміни, викликані найвідомішими інцидентами в кіберпросторі та навколо нього за останні роки, ставлять нетривіальний виклик для військового та політичного керівництва провідних держав світу, ефективність якого визначатиме найближчі перспективи людської цивілізації. Кіберпростір та пов'язані з ним нові виклики та загрози, які створили нове поле конфронтації для розробки єдиної стратегії контрзаходів, потребують ретельного аналізу найвідоміших кіберінцидентів останніх років.

Єдиного робочого шаблону для розслідування кіберінциденту не існує, але є деякі загальні контрольні точки, які слід пам'ятати під час розслідування.

Серед них: збір всієї інформації по факту вчинення кіберінциденту та перетворення, її, на прийнятний для аналізу вид, зіставлення отриманих відомостей із вже відомими даними, а також збагачення інформації про інцидент

новими знахідками з IT-інфраструктури та відкритих джерел. Цей процес ітеративний і припиняється лише тоді, коли проведений всебічний аналіз усієї отриманої інформації.

Збір інформації, якщо говорити загалом, здійснюється з жорстких дисків, оперативної пам'яті, трафіку. Для нас цікавить будь-яка структурована інформація, сформована будь-якими програмними засобами: компонентами операційної системи, системними додатками, спеціалізованим програмним забезпеченням, засобами захисту та іншим програмним забезпеченням.

Перетворення інформації проводиться як загальнодоступними засобами, так і з використанням внутрішніх розробок.

Коли стоїть завдання розібратися в тому, як стався конкретний інцидент, насамперед здійснюється детальне вивчення компанії, знайомство з її керівництвом, співробітниками, збереженням всіх можливих даних. Дуже часто люди діляться деталями, що суперечать одна одній: плутаються у показаннях, дають різну інформацію, дуже специфічно описують інциденти.

Дальше іде вивчення даних, образів, лог файлів, зібраних з технічних засобів, які були в організації. З великого масиву інформації можна виділити дані, важливі для розслідування, посортувати їх за часом, провести статистичний аналіз, дослідити та відновити ланцюжок подій у хронологічному порядку: від фактів проникнення в інфраструктуру до виведення даних чи інших дій, що порушують цілісність, конфіденційність чи доступність інформації.

Це все дії зазвичай виконуються при втручанні у систему чи інфраструктуру компанії. Але це займає досить багато часу та ресурсів. Для оперативного розслідування кіберінцидентів доцільно було б використовувати методи OSINT, паралельно стандартним методам розслідування кібератак, в комплексі із іншими заходами розслідування інцидентів та чим, добитися найкращого результату.

Висновки до другого розділу

В розділі висвітлюються основині джерела OSINT та способи отримання інформації із таких джерел. На даний час існує безліч інструментів для здійснення OSINT. Було згадано декілька основних інструментів OSINT. Здійснено короткий аналіз їх можливостей та ефективність їх використання при здійсненні розвідки із відкритих джерел.

Крім цього, ми розглянули типи здобування інформації, яких є три: пасивний, напівпасивний і активний. Проаналізувавши поняття типів здобування інформації, визначили чим вони відрізняються.

Також визначили, що методи OSINT допомагають спеціалістів з безпеки запобігти витоку інформації про їх компанії. Розібрали, яку саме конференційну інформацію можливо втрати не використавши методи OSINT для перевірки своєї організації на факти можливих витоків інформації та спроможність здійснення атаки на неї, використавши розвідки із відкритих джерел. Крім цього, з'ясували яким чином можна знаходити безкоштовні інструменти OSINT.

Також ми визначили, що проведення такої розвідки не є затратною процедурою для капіталу компанії. Що буде актуально, як в малих , так і у великих компаніях.

Розділ 3. Практичні рекомендації при розслідувані кіберінциндента за допомогою методів OSINT

3.1. Способи використання OSINT при розслідувані кіберінциндентів

Безумовно OSINT – це технологія сьогодення та майбутнього і ті, хто розуміє її інструменти та принципи роботи, завжди будуть на крок попереду у питаннях, пов’язаних з конкуренцією, особистою, корпоративною та національною безпекою.

В Україні з 2014 р. робляться спроби використовувати OSINT у військових операціях, але застосування цього інструменту в державному управлінні та політиці захисту національних інтересів досі перебувають на стадії наукового пошуку.

Розслідування кіберінцидентів це трудозатратний по часу процес, який вимагає врахування всіх деталей. Для початку потрібно з'ясувати якого типу інцидент відбувся, як довго він тривав та які дії відбулися за той період часу. Знаючи ці першочергові фактори ми зможемо провести аналіз ситуації та у подальшому вибрати засоби та методи для розслідування. Адже немає єдиного шаблону який би слугував прикладом для тої чи іншої інциденту. Проте завжди присутні точки від яких ми можемо відштовхуватися при розслідуванні.

Так, коли відбувається кіберінцидент чи повноцінна кібератака то в будь-якому випадку залишається інформація про подію яка відбулася.

Зібрати першочергову інформацію про подію є відправною точкою для подальшого розслідування та використання системи OSINT.

3.1.1. Пошук інформації за деталями електронного листа

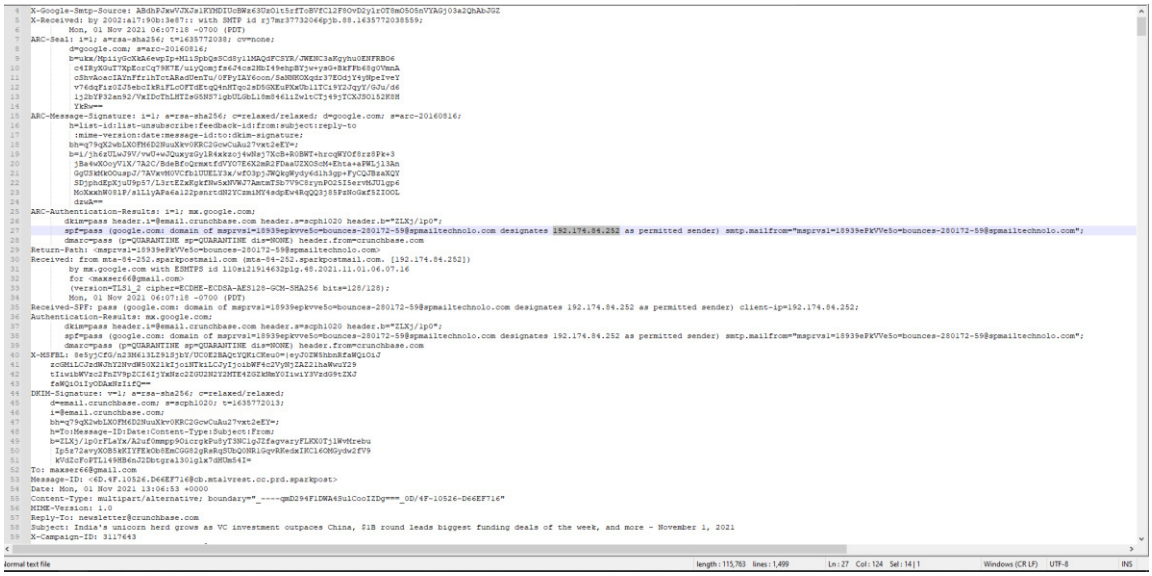
Яскравим прикладом може слугувати така подія, як отримання листа на електрону скриньку із прикріпленим файлом, де прикріпленим файлом виступає архів із шкідливим програмним забезпеченням. При розархівуванні здійснює

збирання заданих йому файлів та передає на сторонній сервер. На даний час такі випадки не є поодинокими. Відправниками таких листів можуть бути як новачки, які тільки пробують та тестують такі засоби, так і особи, які бажають здійснити хакерську атаку на організацію та заволодіти її даними.

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

Скачавши лист на свій персональний комп'ютер та відкривши його у текстовому редакторі, можна побачити Ip-адресу відправника або сервісу через який здійснювалась пересилки. Приклад відкритого листа можна побачити на рис. 3.1.1.

Рис. 3.1.1.



Для відкриття листа було використано програмне забезпечення “Notepad++”. У 27 рядку файлу листа, що рис. 3.1 можна замітити Ip-адресу сервісу відправника: 192.174.84.252. Використавши інструмент “whois”, а точніше скориставшись веб-ресурсом “https://whoer.net/ru/checkwhois” ми можемо дізнатися інформацію про хостинг-провайдера, який надає послуги по

цьому Ip-адресу. На рис. 3.2 ми спостерігаємо, що інформація про відправника зберігатися фізично у компанії “SparkPost”, яка розміщує свої сервери на території Сполучених Штатів Америки у Штаті Огáйо (англ. Ohio), місто Дублін, індекс міста 43017.

Рис. 3.1.2

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

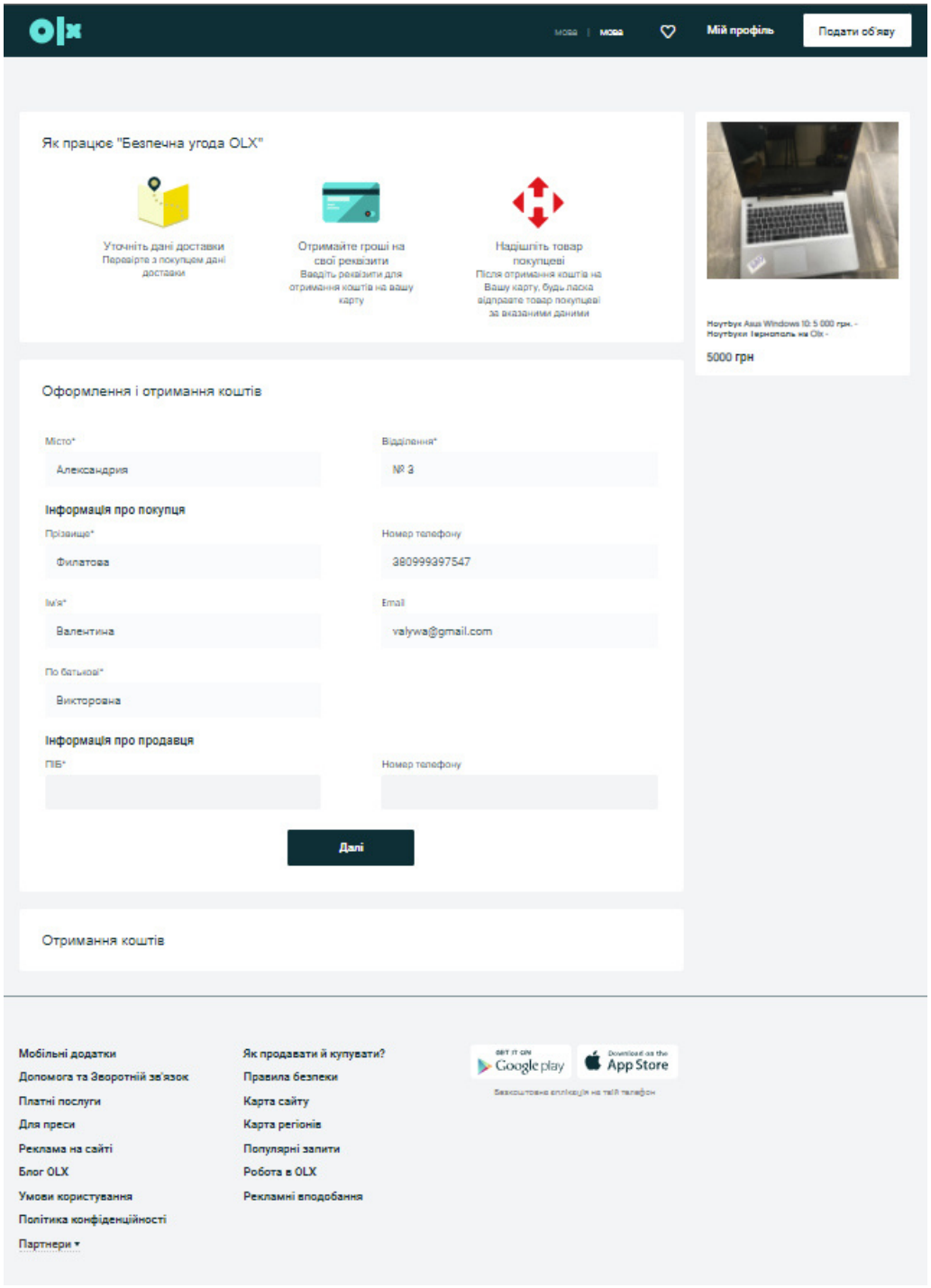
Так, не беручи до уваги те, що до повідомлення було прикріплений файл та без його аналізу, ми дізналися багато інформації від якої можна відштовхнутися при дослідженні. Звісно, без детального аналізу файлу та принципу його дії не можна скласти повної картини кіберінциденту.

Крім цього, існує безліч інших випадків кіберінцидентів де є доцільність використання методів OSINT. Приклади таких інцидентів ми розглянемо нижче.

3.1.2. Пошук інформації по url адресі

Отримання посилання на фішинг веб-ресурс, як кіберінцидент, характеризується самим посиланням. Тобто ми маємо url від якої будемо відштовхуватися не беручу до уваги джерело отримання такого посилання. Найпопулярнішим фішинг посиланням в Україні можна рахувати це посилання на “OLX доставку” або самий веб-ресурс. Для дослідження ми будемо використовувати реальне фішинг посилання “https://olx.ua-pocchta.xyz/delivery.php?pay=1&q=4624029673”, яке було використане для отримання грошей від продавця. Вигляд веб-ресурс мав такий, як на рис. 3.1.3. Серед то, за що ми можемо зачепитися при розслідуванні такого типу кіберінциденту, насамперед, так це url посилання. Оскільки реквізити отримувача є вигаданими та не має змісту їх перевіряти. Тільки в кінці такого розслідування для повноти інформації можливо здійснити таку перевірку.

Рис. 3.1.3



Тому, для початку скористаємося веб-ресурсом ”https://www.whoer.net/checkwhois” для перевірки фізичного розташування інформації про веб-ресурс. Із рис. 3.1.4 ми бачимо, що даний фішинговий сайт має Ip-адресу 135.125.21.210, що належить діапазону Ip-адрес, які обслуговує

cloud.4host.su, який в свою чергу орендує сервери в “OVH SAS”, яка є французькою компанією та фізично розміщення серверів має у Франції.

Рис. 3.1.4

3.1.3 Пошук інформації за адресою крипто-гаманця

При розслідувані кіберінцидента, в якому фігурує крипто гаманець можливо здійснити ідентифікацію особи власника гаманця. Засоби OSINT дозволяють здійснити аналіз інформації по крипто гаманцю. Крім цього, технологія Блокчейн дозволяє всім бажаючим переглянути стан гаманця та транзакції, які відбувалися із його використанням, знаючи лише адресу гаманця. Технології OSINT дозволяють більш комплексно підійти до питання пошуку такої інформації. Данні про власника крипто-гаманця стали не виключенням. Один із інструментів OSINT для здійснення пошуку інформації є Maltego, який був раніше згаданий в роботі, дає змогу здійснювати аналіз крипто-гаманців та встановлювати зв'язки між ними, як це показано на рис. 3.1.5 та рис. 3.1.6

Рис. 3.1.5

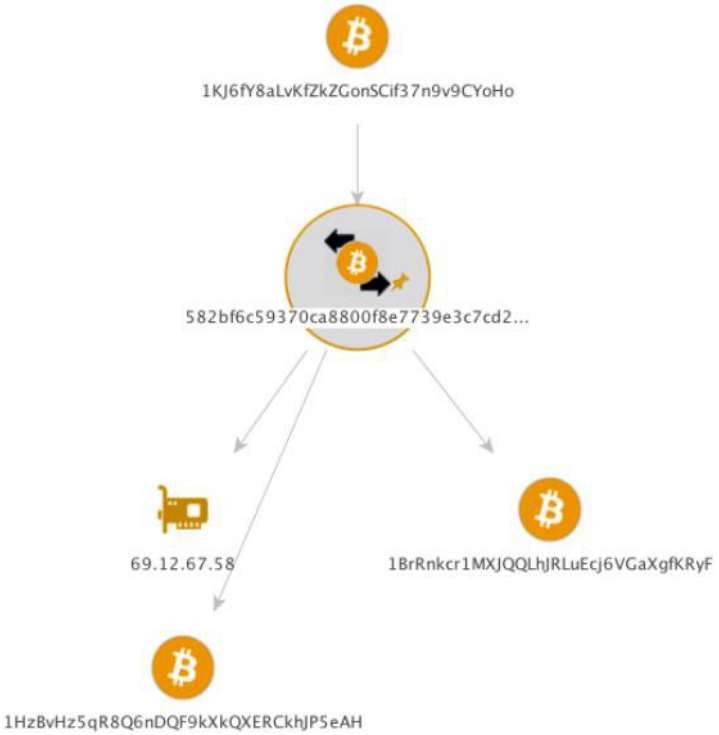
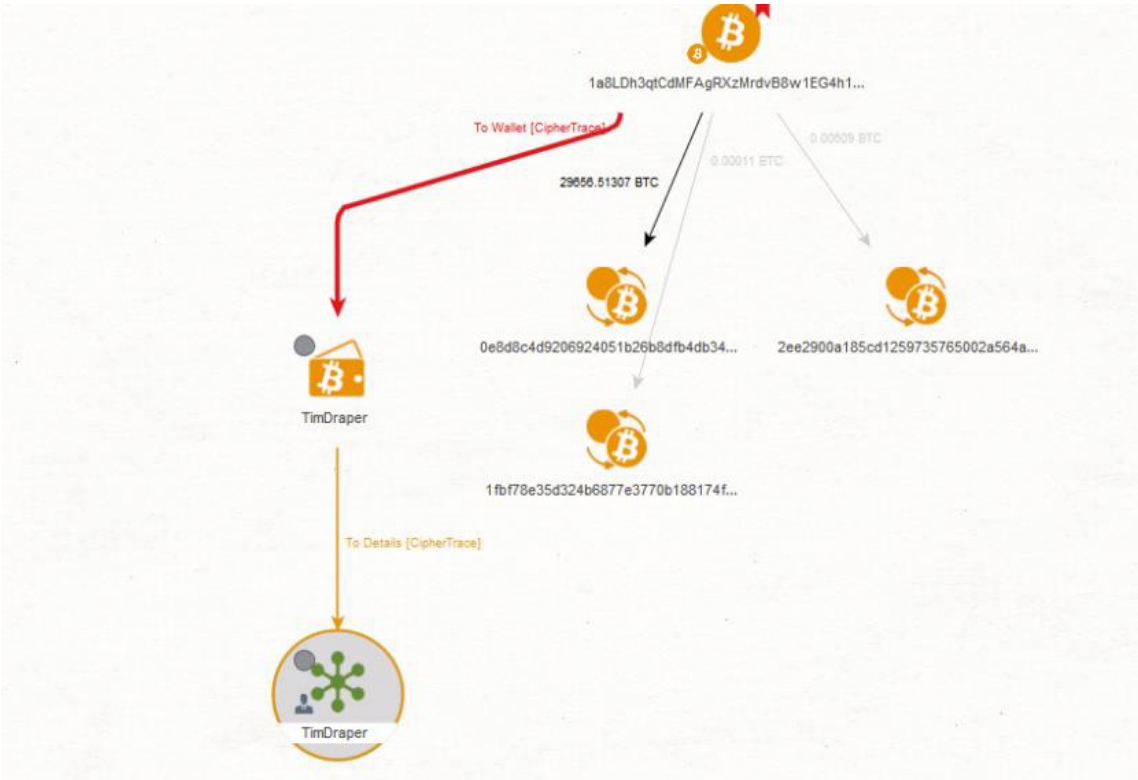

1KJ6fY8aLvKfZkZGonSCif37n9v9CYoHo
582bf6c59370ca8800f8e7739e3c7cd2...
69.12.67.58
1BrRnkcr1MXJQQLhJRLuEcj6VGaXgfKRyF
1HzBvHz5qR8Q6nDQF9kXkQXERCkhJP5eAH

Рис. 3.1.6


1a8LDh3qtCdMFAgRXzMrdvB8w1EG4h1...
To Wallet [CipherTrace]
29656.51307 BTC
0.00011 BTC
0.00609 BTC
0e8d8c4d9206924051b26b8dfb4db34...
2ee2900a185cd1259735765002a564a...
TimDraper
1fbf78e35d324b6877e3770b188174f...
To Details [CipherTrace]
TimDraper

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

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

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

3.2. Імплементація засобів OSINT в СУІП

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

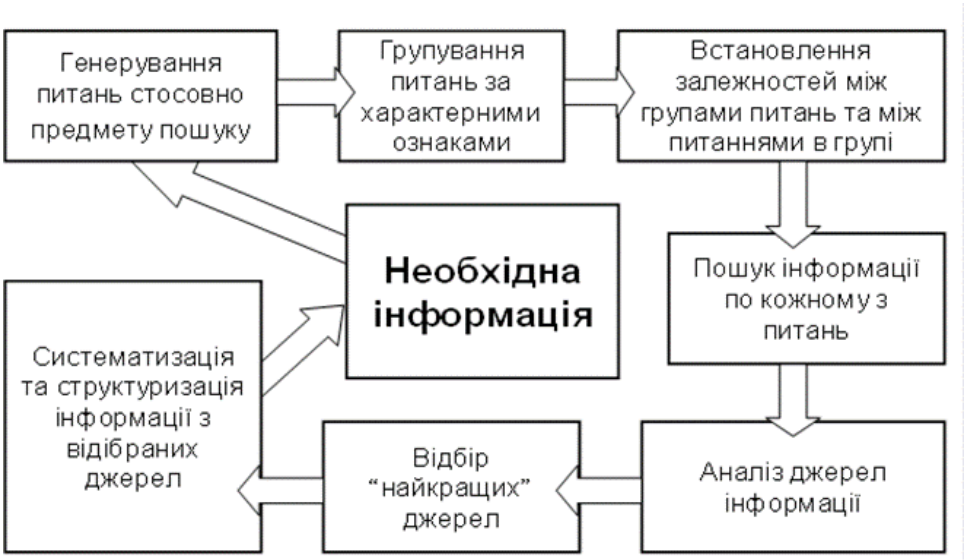
Розвідка з відкритим кодом (OSINT) є однією з дисциплін розвідки. Включає пошук, відбір і збір данних з загальнодоступних джерел та їх аналіз. У розвідувальному співтоваристві термін «відкритий» відноситься до загальнодоступного джерела (на відміну від засекречених джерел та джерел обмеженого використання),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

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

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

Непоганий метод пошуку інформації із відкритих джерел інформаці наведено на рис. 3.2.1.

Рис. 3.2.1



Його суть полягає в наступному: для отримання необхідної інформації про проблему необхідно сформувати якнайбільше питань, згрупувати питання за характеристиками, встановити взаємозв'язки між групами та окремими проблемами, шукати інформацію з кожної проблеми, аналізувати джерела інформації. для об'єктивності, новизни, достовірності і т. д. відбирати найкращі джерела, систематизувати та упорядкувати інформацію.

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

Для створення єдиного автоматизованого засобу СУІР спочатку необхідно визначити основні напрямки автоматизації процесів управління інформаційною безпекою на всіх фазах циклу управління: планування, впровадження, перевірка, удосконалення стандартів серії ДСТУ[39].

Процес планування повинен включати наступні етапи:

1. Визначте перелік інформаційних ресурсів підприємства. Автоматизований інструмент допомагає зберегти дані про інформаційні ресурси та їх зміни, а також може спростити процес збору даних.

2. Оцінка критичності інформації. Тут автоматизований інструмент може зберігати лише дані опитування.

3. Оцінка безпеки інформаційних ресурсів. Інтеграція з базами даних про вразливості та інтегрованими базами даних загроз допомагає оптимізувати цей процес і забезпечити його повноту.

Також можлива інтеграція з різними сканерами уразливостей.

4. Виявлення інформаційних ризиків. Вбудоване алгоритмічне рішення розраховує інформаційні ризики на основі введених даних. Результат виводиться у вигляді звіту.

5. Обрання стратегії управління ризиками, визначення способів зниження ризиків. За допомогою автоматизованої технології ви можете гнучко та зручно моделювати різні варіанти реалізації захисту, оцінювати ефективність запланованих засобів та вибирати найкращу стратегію захисту[40].

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

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

- нормативні документи (методичні вказівки, положення, інструкції);

- записи, що підтверджують виконання існуючих процедур в організації.

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

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

Статистика та аналіз подій. Аналіз подій є основним критерієм ефективності та адекватності інформаційної безпеки організації, а також ефективності ЗМІР загалом. Заходи щодо покращення відновлювальних заходів визначаються на основі інформації про інциденти[40].

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

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

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

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

У кінці заключного етапу, весь прогрес повертається до етапу планування та циклічно повторюється впродовж усього життєвого циклу системи управління інтелектуальною власністю[41].

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

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

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

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

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

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

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

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

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

Безперервність бізнесу: на безперервність бізнес-операцій можуть вплинути різноманітні природні та техногенні катастрофи. Ці катастрофи можуть легко вивести підприємства з ладу без належних запобіжних заходів. Методи OSINT

дозволяють командам використовувати інформацію з надійних глобальних джерел для покращення обізнаності та прозорості ситуації.

Безпека критичної інфраструктури: Критична інфраструктура підтримує підприємства та країни; тому розуміння будь-яких потенційних збоїв є критичним. Методи OSINT забезпечують систему раннього попередження, щоб передбачити та пом’якшити ризики, які можуть вплинути на інфраструктуру.

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

Висновки до третього розділу

У процесі аналізу існуючих підходів до визначення OSINT ми запропонували власне визначення OSINT як форми розвідувальної роботи, яка включає їх пошук та вибір з відкритих джерел, подальшу класифікацію та аналіз інформації, висновки, що надаються керівництву, та може бути основою для управлінських рішень.

Актуальність використання OSINT як інструменту контролю та моніторингу NRURL, обумовлена рядом специфічних переваг цього методу розвідки.

По-перше, використання OSINT як основний інструмент моніторингу діяльності лобістських структур дозволить скоротити час та ресурси суб'єкта контролю, виключивши незначні моменти, або навпаки – виявити найбільш спірні, потенційно потенційно суперечливі моменти. Суб'єкти лобіювання, що загрожують національній безпеці, вже знаходяться на початковій стадії спостереження.

По-друге, активне застосування OSINT NRURL не лише своєчасно визначить підстави для застосування тих чи інших санкцій до лобістів, які порушують правила гри, а й своєчасно проінформує Президента України, Прем'єр-міністра України та інших офіційних осіб про це. спроби непрямого лобіювання та можливі наслідки цих спроб.

По-третє, NRRL може за необхідності надавати інформацію, отриману з відкритих джерел, як правоохоронним органам для розслідування і переслідування потенційних злочинців, а й у засобах масової інформації. Це дозволить NRURL істотно знизити можливі інформаційні атаки недобросовісних лобістів, звинувачення у упередженості, обмеження їхніх прав та ін.

РОЗДІЛ 4. ОХОРОНА ПРАЦІ ТА БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

4.1 Фактори, що впливають на функціональний стан користувачів комп'ютерів

Темпи зростання числа користувачів ПЕОМ неухильно зростають. Одночасно з цим стає все більш очевидною можлива небезпека для здоров'я працюючих на ПЕОМ.

Дисплей - головне джерело небезпеки. Він випускає випромінювання декількох видів: рентгенівське, ультрафіолетове, інфрачервоне, електромагнітне. Для кожного з цих випромінювань розроблені гранично допустимі норми, проте вони досить умовні й різняться у кожній країні. Норми передбачають, що опромінюється весь організм людини, тоді як на ділі впливу піддається лише верхня частина тулуба. Згадані норми встановлені з розрахунку на кожен вид опромінення в окремо, хоча реально всі поля діють одночасно, а їх комплексний вплив досі не досліджено [28, С.115].

Крім того, відеодисплейний термінал порушує рівновагу між позитивно і негативно зарядженими іонами в повітрі. Електростатичне поле дисплея притягає негативні іони, порушуючи тим самим загальний баланс атмосфери. Це також шкодить здоров’ю. Вже через годину роботи біля монітора спостерігається майже повне зникнення негативних іонів. Ось чому необхідно, щоб до робочого місця за комп’ютером проникав свіже повітря. У зв’язку з усіма цими небезпеками досить чітко регламентовані розміри столу і стільця для роботи з комп’ютером. Адже "закам’яніли" постава шкідливо впливає на скелетно-м’язову систему. Стіл повинен бути просторим, із спеціальною підставкою для ніг, а робочий стілець - мати відрегульовану висоту, певний кут нахилу сидіння і спинки [29, С.86].

За правилами, світло при роботі з комп’ютером повинен падати зліва, а відстань від очей до екрана повинна бути близько 50 сантиметрів. Крім того, крісло слід відрегулювати так, щоб очі були на одному рівні з центром монітора. Фахівці говорять, що саме очі найбільш страждають при роботі з комп’ютером.

Виявляється, коли довго дивишся на екран, перестаєш моргати. Тому очі червоніють, сльозяться, а значить, знижується зір.

Системний блок створює тільки електромагнітне поле (випромінювання). Правда є ще й шум від вентиляторів, але ця тема всім зрозуміла і не вимагає знань електроніки. Шкода від електромагнітного поля однозначно є при високому рівні поля. Однак поле комп'ютер створює набагато менше, ніж мобільний телефон. Тобто йому далеко до мікрохвильової печі по потужності.

Монітор має два основних шкідливих фактора. Бета-випромінювання (а простіше, потік електронів), яке власне кажучи і створює картинку на екрані, і висока напруга (як і в будь-якому телевізорі, воно досягає 16-20 кіловольт), що викликає іонізацію повітря [30, С.34].

Бета-випромінювання поширюється монітором у двох напрямках - вперед і назад. У старих телевізорах і моніторах випромінювання досягало одного або двох метрів від екрану. По дорозі вибиваючи електрони з молекул повітря, перетворюючи їх у позитивні іони, шкідливі для людини. На даний момент монітори мають дуже низький рівень бета-випромінювання, тобто електрони вилітають за межі екрану на кілька сантиметрів. Основне випромінювання монітора направлено тому, там «зона ураження» поширюється на метр-півтора. От її і слід уникати. Висока напруга відхоплючи у молекул повітря електрони, також перетворює молекули на шкідливі позитивні іони. Так що ж робити і чого уникати? уникати в першу чергу крайнощів.

Будь-яка поза при тривалій фіксації шкідлива для опорно-рухового апарату, веде до застою крові в органах. Це особливо проявляється при фізіологічному положенні різних частин тіла і тривало повторюваних одноманітних рухах. Небезпеку для здоров'я представляє не тільки втома тих груп м'язів, які ці рухи виконують, але і психологічна фіксація на них (утворення стійких вогнищ збудження ЦНС з компенсаторним гальмуванням інших її ділянок). Хоча найбільш шкідливі саме повторювані одноманітні навантаження. Під час роботи за комп'ютером людина сидить кілька годин поспіль в незручному становищі. Це не тільки загрожує втомою і загальною втомою, а й може призвести до

розвитку остеохондрозу різних ділянок хребта - шийного, грудного, попереково-крижового [31, С.89].

У зв'язку з цим лікарі надають великого значення підтримці правильної пози під час роботи за комп'ютером. Дотримання цього правила - важливий елемент профілактики захворювань. Щоб робота за комп'ютером не шкодила здоров'ю, необхідно постійно стежити за своєю поставою. Правильна постава максимально розвантажує м'язи і дозволяє працювати довше, менше втомлюючись.

Вважається, що при правильній поставі вуха повинні розташовуватися точно в площині плечей, а плечі - точно над стегнами. Голову слід тримати рівно по відношенню до плеча. При погляді вниз, голова не повинна нахилятися вперед.

Якщо в процесі роботи в згорбленому стані, навантаження на хребет збільшується, то це приводить до надмірного розтягування м'язів. Згорблене положення може стати причиною синдрому зап'ястного каналу, грижі міжхребцевих дисків поперекового і шийного відділів.

Багато хто, дивлячись на екран монітора, витягує шию вперед. Часто це пов'язано з тим, що монітор відсунутий занадто далеко. У результаті навантаження на м'язи голови і шиї зростає приблизно в три рази, судини шиї стискуються, погіршуючи кровопостачання голови. Крім того, людині, що сидить у такій позі, доводиться щоразу відкидати голову назад, щоб розгледіти, наприклад, чи лежить прямо перед нею паперовий документ. Це посилює прогин шийного відділу хребта. Згодом це може привести до головного болю і болю у руках, оскільки нерви, що відходять від спинного мозку в області шиї, простягаються до кінчиків пальців [32, С.156].

Сутулість викликає надмірне навантаження на плечові сухожилки і м'язи плеча. Тривала робота в такій позі може призвести до розвитку синдрому зап'ястного каналу і защемлення плеча.

Піднімаючись з стільця або крісла, на яких багатьом доводиться проводити значну частину часу на роботі і вдома, хребет, суглоби разом з навколишніми

м’язами і зв’язками "звикають" до даної пози, тому перехід у вертикальне положення вимагає плавності і точності рухів, щоб "застояні" структури опорно-рухового апарату встигли включитися в новий режим роботи. Спочатку треба пересунутися у кріслі, сівши на передню його частину. Стійко поставивши ступні на ширину плечей, нахилити тулуб вперед приблизно до кута 70 градусів по відношенню до підлоги, намагаючись не згинати поперек. У досягнутій позиції можна вважати, що колінні суглоби зігнуті під кутом 90 градусів, а тазостегнові знаходяться в оптимальному стані. Далі не важко відірвати від сидіння сідниці і плавно встати, стежачи за синхронністю руху міжколінних і тазостегнових суглобів і випрямленням тулуба. При дотриманні цієї умови можна зупинитися в будь-якій точці даної траєкторії, відчуваючи себе відносно комфортно і стійко, без надмірного напруження в ділянці нирок, чим забезпечується хребет від ушкоджень, якщо навчитеся сідати з вертикального положення, дотримуючись зворотної послідовності дій, рекомендованих для підйому з положення сидячи [33, с.413].

Пропонований спосіб підйому з крісла є навчальним і вимагає наполегливості в оволодінні цим навиком. У період виражених болів в спині він може бути складним. Найбільш поширеною помилкою є випереджаюче випрямлення колінних суглобів з подальшим випрямленням тулуба, що загрожує пошкодженню поперекових сегментів хребта.

Якщо крісло з підлокітниками, то можна допомогти собі встати, впираючись у них долонями. При відсутності підлокітників можливий підйом, при якому треба зробити вихідний упор долонями у власні коліна і по черзі перемістити кисті рук вгору по стегнах, щоб допомогти випрямленню тулуба. Цей спосіб допомагає в період гострих болів у спині, але навчитися його виконання можна і в спокійний період.

Для сором’язливих людей, які не бажають звертати на себе увагу оточуючих своїми зосередженими діями при підйомі з стільця, пропонується інший спосіб. На відміну від попередніх методів він характеризується витонченістю і стрімкістю при збереженні безпеки [34, с.147]. При цьому не

треба широко розставляти ступні - досить одну ногу поставити на носок на 10 см назад під стілець, використовуючи її при підйомі зі стільця в якості стартової опори. Цей спосіб дозволяє при мінімальних зусиллях швидко опинитися у вертикальному положенні.

Персонал, що працює на комп'ютері зобов'язаний дотримуватися вимог інструкції, розробленої на підставі Санітарних норм і правил СанПіН 2.2.2.542-96 «Гігієнічні вимоги до відео - дисплейним терміналів, персональним електронно-обчислювальних машин і організації робіт», а також нести особисту відповідальність за дотримання вимог безпеки своєї праці і за створення небезпечного чи шкідливого виробничого фактора для інших працюючих і поломку комп'ютера.

Для підвищення вологості повітря слід використовувати зволожувачі. У кабінеті повинно бути штучне і природне освітлення. Основний потік природного світла повинен бути ліворуч. На вікнах повинні бути завіси в два рази більші ширини вікна. Забороняється застосовувати для вікон чорні завіси [35, С.93].

Кабінет, де знаходяться комп'ютери відноситься до пожежонебезпечного приміщення категорії «Б», тому необхідно мати вуглекислотний вогнегасник типу ВУ-5 і вміти ним користуватися.

Необхідно звертати увагу на заземлення, тому що в комп'ютері використовуються мікросхеми, чутливі до статичної електрики. Особливу увагу звертають на цілісність ізоляції всіх кабелів та роз'ємів, щоб не виявитися несподівано під напругою щодо землі. Забороняється самостійно відкривати комп'ютер, з-за високої напруги всередині. Виключається робота з комп'ютером і його периферійними пристроями з відкритим корпусом. Не дозволяється самостійно перемикати силові та інтерфейсні кабелі, проливати рідини і т.ін.

Робоче місце на комп'ютері необхідно обладнати спеціальними меблями: обертовим стільцем із змінною висотою сидіння і кута нахилу спинки.

При роботі на комп'ютері працюючий повинен бути уважним, не відволікатися на побутові справи.

Під час роботи комп'ютера забороняється:

- залишати комп'ютер без нагляду;
- проводити ремонт;
- знімати корпус з комп'ютера.

Тривалість безперервної роботи з комп'ютером без регламентованої перерви не повинна перевищувати 2 годин.

Під час регламентної перерви з метою зниження нервово-емоційного напруження, стомлення зорового аналізатора, усунення впливу гіподинамії та гіпокінезії, запобігання розвитку познотопічної втоми доцільно виконувати комплекси вправ. Рівень шуму в приміщенні під час роботи комп'ютерів не повинен перевищувати 50 дБА [36, с.178].

Конструкція відеомонітора повинна передбачати заходи, що забезпечують добру розбірливість зображення, незалежну від зовнішнього освітлення.

У залежності від призначення і області застосування відео-термінали можуть бути розділені на наступні групи:

- група А - кольорові монітори тільки для демонстраційних цілей.
- група Б - кольорові монітори для персональної роботи;
- група В - монохромні монітори.

Категорично забороняється використання на робочому місці електронагрівальних приладів з відкритим елементом, відкритим вогнем.

Користування електронагрівальними приладами з закритими нагрівальними елементами дозволяється тільки у спеціально відведених для цього місцях.

Недотримання вимог до мікроклімату приміщення може не тільки різко знижувати продуктивність праці, викликати втрати робочого часу через збільшеного числа помилок у роботі, але і приводити до функціональних

розладів або хронічних захворювань органів дихання, нервової системи, імунної системи.

У аварійних ситуаціях комп'ютер необхідно негайно відключити від мережі: при відключенні електричної енергії; при пожежі; при появі запаху диму [37, С.89].

Людину, що потрапила під напругу, необхідно негайно звільнити від дії струму, відключивши комп'ютер або відкинувши електродріт . Якщо це неможливо зробити швидко, потерпілого необхідно відтягнути від струмоведучих частин, діючи однією рукою, ізольованою гумовою рукавичкою (сухим одягом) торкаючись лише одягу потерпілого. До прибуття лікаря потерпілому надати першу допомогу. У перші хвилини з моменту ураження необхідно почати штучне дихання, закритий масаж серця. Під час пожежі приступити до гасіння пожежі вуглекислотним вогнегасником і викликати пожежну команду за тел. 101.

Після закінчення роботи відключити комп'ютер від мережі.

4.2 Охорона праці при надзвичайній ситуації

Єдина державна система запобігання і реагування на надзвичайні ситуації техногенного та природного характеру та захист інформації в сучасному інформаційному суспільстві.

Єдина державна система запобігання і реагування на надзвичайні ситуації техногенного та природного характеру створена в Україні згідно з постановою Кабінету Міністрів України від 3 серпня 1998 р. № 1198.

Єдина державна система запобігання і реагування на надзвичайні ситуації техногенного та природного характеру (далі ЄДС НС), центральні та місцеві органи виконавчої влади, виконавчі органи рад, державні підприємства, установи та організації з відповідними силами і засобами, які здійснюють нагляд за забезпеченням техногенної та природної безпеки, організовують проведення

роботи із запобігання надзвичайним ситуаціям (НС) техногенного та природного походження і реагування у разі їх виникнення з метою захисту населення і довкілля, зменшення матеріальних втрат.

ЄДС НС складається з постійно діючих функціональних і територіальних підсистем і має чотири рівні – загальнодержавний, регіональний, місцевий та об'єктовий. Функціональні підсистеми (ФП) створюються міністерствами та іншими центральними органами виконавчої влади для організації роботи пов'язаної із запобіганням НС та захистом населення і територій від їх наслідків. У НС сили і засоби ФП регіонального, місцевого та об'єктового рівня підпорядковуються в межах, що не суперечать законодавству, органам управління відповідних територіальних підсистем ЄДС НС. Територіальні підсистеми (ТП) створюються в АР Крим, областях, мм. Києві та Севастополь для запобігання і реагування на НС у межах відповідних регіонів. Організаційна структура та порядок діяльності ФП і ТП визначаються в положеннях про них [43, С.170].

Кожен рівень ЄДС НС має координуючі та постійні органи управління, систему повсякденного управління, сили і засоби, резерви матеріальних та фінансових ресурсів, системи зв'язку та інформаційного забезпечення.

Координуючими органами ЄДС НС є:

- на загальнодержавному рівні – Державна комісія з питань техногенно-екологічної безпеки та надзвичайних ситуацій; Національна рада з питань безпечної життєдіяльності населення;

-на інших рівнях – відповідні комісії з питань техногенно-екологічної безпеки та надзвичайних ситуацій.

Постійними органами управління ЄДС НС є:

-на загальнодержавному рівні – Кабінет Міністрів України, міністерства та інші органи виконавчої влади;

-на регіональному та місцевому рівнях – відповідні органи виконавчої влади, уповноважені органи з питань НС та цивільного захисту населення;

-на об’єктовому рівні – структурні підрозділи підприємств, установ та організацій або спеціально призначені особи з питань НС.

До системи повсякденного управління ЄДС НС входять оснащення необхідними засобами зв’язку, оповіщення, збирання, аналіз і передача інформації:

-центри управління в НС, оперативно-чергові служби уповноважених органів з питань НС та цивільного захисту населення усіх рівнів;

-диспетчерські служби центральних і місцевих органів виконавчої влади, державних підприємств, установ та організацій.

До складу сил і засобів ЄДС НС входять відповідні сили і засоби ФП і ТП, а також недержавні (добровільні) рятувальні формування, які залучаються для виконання відповідних робіт.

Залежно від масштабів і особливостей НС, що прогнозується або виникла, рішенням відповідних органів влади, у межах конкретної території може існувати один з таких режимів функціонування ЄДС НС: режим повсякденної діяльності (при нормальній обстановці); режим підвищеної готовності (при істотному погіршенні обстановки та з одержанням прогнозної інформації щодо можливості виникнення НС); режим діяльності у надзвичайній ситуації (при реальній загрозі виникнення НС і реагуванні на них); режим діяльності у надзвичайному стані (запроваджується в Україні або на окремих її територіях в порядку, визначеному Конституцією України та Законом України “Про надзвичайний стан” [44, С.54].

ЄДС НС фінансується за рахунок державного та місцевого бюджетів, позабюджетних коштів Ради міністрів АК Крим, центральних органів виконавчої влади, коштів державних підприємств, установ та організацій, страхових фондів та інших джерел. Для ліквідації наслідків НС створюються на усіх рівнях функціонування ЄДС НС запаси матеріальних та фінансових ресурсів.

Цивільна оборона України побудована за територіально–виробничим принципом. Загальне керівництво Цивільною обороною України відповідно до її побудови покладається на: Кабінет Міністрів України, міністерства, інші

центральні органи виконавчої влади, Раду Міністрів АР Крим, місцеві державні адміністрації, керівників підприємств, установ і організацій незалежно від форм власності і підпорядкування. Начальником Цивільної оборони України є прем'єр-міністр України, а його заступником керівник центрального органу виконавчої влади з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи; начальником Цивільної оборони Автономної Республіки Крим є Голова Ради Міністрів АР Крим; начальниками Цивільної оборони згідно з адміністративно-територіальним устроєм України є голови місцевих державних адміністрацій; начальниками цивільної оборони в міністерствах, інших центральних органах виконавча влада, на підприємствах, в установах та організаціях є їх керівники.

Безпосереднє виконання завдань Цивільної оборони здійснюється постійно діючими органами управління у справах цивільної оборони, у тому числі створеними у складі підприємств, установ і організацій та службами ЦО.

Завдання, функції та повноваження органів управління у справах цивільної оборони визначаються Законом України "Про Цивільну оборону України" і Положенням про органи управління у справах Цивільної оборони, яке затверджується Кабінетом Міністрів України.

Органи управління, у. справах цивільної оборони, які входять до складу місцевих державних адміністрацій, є підрозділами подвійного підпорядкування. Закон та Положення про цивільну оборону визначають повноваження органів державної виконавчої влади та управління, керівництва підприємств установ та організацій незалежно від форм власності і підпорядкування та обов'язки посадових осіб з питань Цивільної оборони [45, С.31].

Міністерства, інші центральні органи виконавчої влади, Рада Міністрів АР Крим, місцеві державні адміністрації, виконавчі органи сільських, селищних, міських рад у межах своїх повноважень забезпечують вирішення питань цивільної оборони, здійснення заходів щодо захисту населення і місцевостей під час надзвичайних ситуацій, сприяють органам управління у справах цивільної оборони у виконанні покладених на них завдань. Керівництво підприємств,

установ і організацій незалежно від форм власності і підпорядкування забезпечує своїх працівників засобами індивідуального та колективного захисту, організовує здійснення евакуаційних заходів, створює сили для ліквідації наслідків надзвичайних ситуацій та забезпечує їх готовність до практичних дій, виконує інші заходи Цивільної оборони і несе, пов'язані з цим, матеріальні та фінансові витрати в порядку та обсягах, які передбачені законодавством України.

Радіаційні, хімічні і вибухонебезпечні підприємства додатково створюють локальні системи виявлення загрози виникнення надзвичайних ситуацій та оповіщення персоналу і населення, що проживає в зонах можливого ураження, а також запроваджують інженерно-технічні заходи, що зменшують ступінь ризику виникнення аварій, пожеж та вибухів, і несуть витрати щодо їх здійснення в обсягах, передбачених відповідними нормативно-правовими актами.

Власники потенційно небезпечних об'єктів відповідають за захист населення, що проживає в зонах можливого ураження від наслідків аварій на цих об'єктах [45, С.23].

Організація цивільної оборони НЕК "Укренерго".

Начальником цивільної оборони НЕК "Укренерго" являється її директор. Начальниками ЦО відособлених структурних одиниць є їх директора.

Функції координуючих органів управління виконують комісії з питань НС, які створено в апараті Компанії та в відособлених структурних одиницях.

Безпосередня організація виконання завдань ЦО покладена на групи ЦО і моброботи. Повсякденними органами управління є чергові зміни диспетчерських служб та служб зв'язку на які покладено функція збирання первинної інформації про виникнення НС та оповіщення керівного складу.

Силами ЦО НЕК "Укренерго" є невоєнізовані формування, які створено в апараті Компанії та в відособлених структурних одиницях.

Захист інформації — сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до

завдання шкоди власникам і користувачам інформації. Термін вживається в Україні для опису комплексу заходів по забезпеченню інформаційної безпеки.

Захист інформації ведеться для підтримки таких властивостей інформації як:

- Цілісність — неможливість модифікації інформації неавторизованим користувачем.
- Конфіденційність — інформація не може бути отримана неавторизованим користувачем.
- Доступність — полягає в тому, що авторизований користувач може використовувати інформацію відповідно до правил, встановлених політикою безпеки не очікуючи довше заданого (прийнятного) інтервалу часу.
- Спостережливість — властивість системи, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об'єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії.

Аспекти захисту інформації:

Конфіденційність — захист від несанкціонованого ознайомлення з інформацією.

Цілісність — захист інформації від несанкціонованої модифікації.

Доступність — захист (забезпечення) доступу до інформації, а також можливості її використання. Доступність забезпечується як підтриманням систем в робочому стані так і завдяки способам, які дозволяють швидко відновити втрачену чи пошкоджену інформацію [46, С.103].

Висновки до четвертого розділу

- Дисплей - головне джерело небезпеки в персональному комп'ютері. Він випускає випромінювання декількох видів: рентгенівське, ультрафіолетове, інфрачервоне, електромагнітне.

- Під час роботи з комп’ютером найбільшому ризику піддаються зорова, опорно-рухова, нервово-психічна системи і репродуктивна функція у жінок.

- При роботі з комп’ютером шкідливими і небезпечними чинниками є: електростатичні поля; електромагнітне випромінювання; наявність потужних іонізуючих випромінювань; локальне стомлення, загальна втома; стомлюваність очей; небезпека ураження електричним струмом; пожежонебезпека.

- В аварійних ситуаціях комп’ютер повинен негайно відключений від мережі.

- ЄДС НС складається з постійно діючих функціональних і територіальних підсистем і має чотири рівні – загальнодержавний, регіональний, місцевий та об’єктовий.

- Кожний рівень ЄДС НС має координуючі та постійні органи управління, систему повсякденного управління, сили і засоби, резерви матеріальних та фінансових ресурсів, системи зв’язку та інформаційного забезпечення.

- Захист інформації — сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації.

ВИСНОВКИ

В даній дипломній роботі було розглянуто методи OSINT, а також питання інтеграції методів OSINT при розслідування кіберінцидентів. Основним завданням роботи було висвітлити методи OSINT при розслідувані кіберінцидентів.

Використання технологій OSINT іншими державами, дає нам поняття про їх дієвість та ефективність у різних галузях. Було розглянуто міжнародні органи, які суто спеціалізуються на розвідці із відкритих джерел (OSINT). Частково була піднята тема використання технологій OSINT в Україні та правові основи застосування методів розвідки з відкритих джерел інформації (OSINT).

В ході виконання роботи були розглянуті основні типи методів розвідки із відкритих джерел (OSINT). Та досліджено способи використання методів OSINT при розслідувані кіберінцидентів. Крім цього, було змодельована декілька ситуацій де на практичному прикладі відображено способи використання технологій OSINT та їх можливості.

Список використаних джерел:

1. Електронна енциклопедія Wikipedia. Українськомовна версія // https://uk.wikipedia.org/w/index.php?title=Розвідка_на_основі_відкритих_джерел&stable=0

2. Модель_OSINT//https://web.archive.org/web/20090412164950/http://www.computerra.ru/think/kiwi/324966/6

3. Жарков Я.М. Наукові підходи щодо визначення суті розвідки з відкритих джерел / Я.М. Жарков, А.О. Васильєв // Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки. - 2013. - Вип. 30. - С. 38-41. - // http://nbuv.gov.ua/UJRN/VKNU_vsn_2013_30_12.

4. Використання технологій OSINT для отримання розвідувальної інформації / О.В. Минько, О. Ю. Іохов, В.Т. Оленченко, К.В. Власов. // http://webcache.googleusercontent.com/search?q=cache:pNCIFjnKvnEJ:irbisnbuv.gov.ua/cgibin/irbis_nbuv/cgiirbis_64.exe%3FC21COM%3D2%26I21DBN%3DUJRN%26P21DBN%3DUJRN%26IMAGE_FILE_DOWNLOAD%3D1%26Image_file_name%3DPDF/suntz_2016_4_22.pdf+&cd=11&hl=uk&ct=clnk&gl=ua.

5. Актуальні питання протидії кіберзлочинності та торгівлі людьми. Харків, 2018 // http://univd.edu.ua/science-issue/issue/3329

6. Распознавание информационных операций / А. Г. Додонов, Д. В. Ландэ, В. В. Цыганок, О. В. Андрейчук, С. В. Каденко, А. Н. Грайворонская. К. : ООО «Инжиниринг», 2017. 282 с

7. NATO Open Source Intelligence Reader (2002). // http://information-retrieval.info/docs/NATO-OSINT.html–

8. Розвідка Відкритих Джерел (OPEN SOURCE INTELLIGENCE) Ржевська Н.Ф., Кожушко О.О. // http://ena.lp.edu.ua/bitstream/ntb/19232/1/53-Rzhevska-257-261.pdf

9. Албул С.В. До питання концептуалізації напрямів вдосконалення інформаційно-аналітичного забезпечення негласної роботи суб'єктів оперативно-розшукової діяльності в Україні. Правові та організаційно-тактичні

засади оперативно-розшукової діяльності Національної поліції України: Матеріали Всеукраїнської науково- практичної інтернет-конференції (м. Одеса, 30 жовтня 2020р.). Одеса: ОДУВС, 2020. С. 9–12.

10. Open Source Intelligence (OSINT): Issues for Congress, December 5, 2007. // www.fas.org/sgp/crs/intel/RL34270.pdf

11. Про інформацію: Закон України від 02.10.92 р. № 2657-XII.

12. Про друковані засоби масової інформації (пресу) в Україні: Закон України від 16.11.92 р. № 2782-XII.

13. Про охоронну діяльність: Закон України від 22.03.12 р. № 4616-VI.

14. Про захист персональних даних: Закон України від 01.06.10 р. № 2297-VI.

15. Питання європейської та євроатлантичної інтеграції: Указ Президента України від 20.04.19р. №155/2019.

16. Про Національний координаційний центр кібербезпеки: Указ Президента України від 07.06.16р. №242/2016.

17. Про оперативно-розшукову діяльність: Закон України від 18.02.92 р. № 2135-XII

18. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “Про Стратегію кібербезпеки України”: Указ Президента України від 15.03.16 р. № 96/2016.

19. Ланде Д.В. Правові питання конкурентної розвідки // http://ippi.org.ua/sites/default/files/7_16.pdf

20. Сучасні інформаційні технології у сфері безпеки та оборони №1 (40)/2021 // https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjqwcyMgaf0AhUshv0HHYsXBsQ4ChAWegQIAhAB&url=http%3A%2F%2Fsit.nuou.org.ua%2Farticle%2Fview%2F232327%2F232579&usg=AOvVaw1CBdAprnoHDWl2VuC3OUbQ

21. Законі України “Про основні засади забезпечення кібербезпеки України”

22. ПЕРЕЛІК категорій кіберінцидентів // https://cert.gov.ua/recommendation/16904

23. Журнал “Юридичний бюлетень”. випуск 11. ч. 1. 2019, організаційно-правові засади використання розвідки з відкритих джерел інформації (osint) в діяльності розвідувальних служб європейських країн / Бурба Василь Васильович // http://www.lawbulletin.oduvs.od.ua/archive/2019/11/part_1/3.pdf

24. Розробка системи управління кіберінцидентами в мережах LTE // https://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/13036/18086

25. Розвідка відкритих джерел інформації (osint) у розвідувальній практиці США / Кожушко Ольга Олегівна // http://jrnl.nau.edu.ua/index.php/IMV/article/viewFile/3264/321

26. Журнал «Юридичний бюлетень» випуск 11. ч. 1. 2019 // http://www.lawbulletin.oduvs.od.ua/archive/2019/11/part_1/11-1.pdf

27. Електронна енциклопедія Wikipedia. Українськомовна версія // https://uk.m.wikipedia.org/wiki/Персональні_дані/

28. Жидецький, В. І. Основи охорони праці / В. І. Жидецький – Л. : Афіша, 2005. – 349 с

29. Гандзюк, М. П. Основи охорони праці: підруч. / М. П. Гандзюк, Е. П. Желібо, М. О. Халимовський – К. : Каравела, 2005. – 393 с.

30. Григорьев, М. Кто выигрывает в масс-медиа войнах / М. Григорьев // Открытая политика. – 1999. – №3-4 (34). – С. 2-7.

31. Бедрій, Я. І. Охорона праці : навч. посіб. / Я. І. Бедрій. – Львів : Афіша, 1997. – 258 с.

32. Дурдинця, В. В. Збірник нормативно-правових актів з питань надзвичайних ситуацій техногенного та природного характеру / В. В. Дурдинця. – К. : Чорнобиль інтерінформ, 2001. – 532 с.

33. Ткачук, К. Н. Охорона праці та промислова безпека / Ткачук К. Н., Зацарний В. В., Сабарно Р. В. – К. : Лібра, 2010. – 560 с.

34. Ткачук, К. Н. Основи охорони праці / К. Н. Ткачук, М. О. Халімовський, В. В. Зацарний. – К. : Основа, 2006. – 448 с.

35. Рожков, А. П. Пожежна безпека : навч. довід. / А. П. Рожков. – К., 1999. – 256 с.

36. Теличко, Е. М. Міжнародне законодавство про охорону праці. Конвенції та рекомендації МОП у 3-х томах. Том 1 / Е. М. Теличко. – К. : «Основа», 1997. – 672 с.

37. Москальова, В. М. Основи охорони праці : підруч./ В. М. Москальова. – К., 2005. – 208 с.

38. Антонюк В. В. Організаційно-правові засади формування та реалізації державної політики інформаційної безпеки України: // http://academy.gov.ua/pages/dop/138/files/8de62817-e4bf-40d8-acb0-96384ec79f34.pdf

39. ДСТУ ISO/IEC 27000:2015 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник (ISO/IEC 27000:2014, IDT).

40. Заєць П.М., Іванова О.С. Визначення підходів щодо впровадження засобів і систем автоматизації процесів управління інформаційною безпекою організації // https://academy.ssu.gov.ua/uploads/p_57_35588992.pdf

41. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).

42. Серватнюк М. Інтеграція методів OSINT в систему управління інформаційним ризиками. ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ : IX науково-техн. конф., м. Тернопіль, 8–9 груд. 2021 р. 2021. с. 76.

43. Купчик, М. П. Основи охорони праці / М. П. Купчик. – К. : Основа, 2000. – 416 с.

44. Керб, л. П. Основи охорони праці : навч. Посіб. / л. П. Керб. – к. : кнеу, 2003. – 215 с.

45. Гончарук, В. Є. Оцінка обстановки у надзвичайних ситуаціях : навч. посіб. / В. Є. Гончарук. – Львів, Видавництво НУ “Львівська політехніка”, 2004. – 136 с.

46. Сєріков, Я. О. Основи охорони праці : навч. посіб. / Я. О. Сєріков. – Харків, ХНАМГ, 2007. – 227с.

47. Васюк К. В. Автоматизація збору корпоративної та особистої інформації з відкритих джерел : кваліфікаційна робота бакалавра за спеціальністю „125 — кібербезпека“ / К. В. Васюк — Тернопіль : ТНТУ, 2021. — 73 с.

48. Пех С. Конкурентна розвідка / Пех С. // Матеріали IX Всеукраїнської студентської науково-технічної конференції „Природничі та гуманітарні науки. Актуальні питання“, 20-21 квітня 2016 року — Т. : ТНТУ, 2016 — Том 1. — С. 114. — (Секція: Інформаційні технології).

49. Федорчук С. Цілі і завдання інтернет-розвідки / Федорчук С. // Матеріали IX Всеукраїнської студентської науково-технічної конференції “Природничі та гуманітарні науки. Актуальні питання”, 20-21 квітня 2016 року — Т. : ТНТУ, 2016 — Том 1. — С. 116-117. — (Секція: Інформаційні технології).

ДОДАТКИ

Додаток А

Тези конференції

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

МАТЕРІАЛИ

IX НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ,
СИСТЕМИ ТА ТЕХНОЛОГІЇ»

8–9 грудня 2021 року

ТЕРНОПІЛЬ
2021

УДК 004.056
М.М. Серватнюк
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ІНТЕГРАЦІЯ МЕТОДІВ OSINT В СИСТЕМУ УПРАВЛІННЯ ІНФОРМАЦІЙНИМ РИЗИКАМИ

UDC 004.056
M.M. Servatniuk

INTEGRATION OF OSINT METHODS INTO THE INFORMATION RISK MANAGEMENT SYSTEM

В сучасних умовах розвитку інформаційних технологій та всесвітньою мережі Інтернет постає питання здійснення ефективного пошуку інформації. Одним з таких засобів пошуку інформації є розвідка із відкритих джерел інформації (OSINT), яка являє собою концепцію, методологію і технологію пошуку та використання військової, політичної, економічної та іншої інформації з відкритих джерел, без порушення законів. [1]

У сферу інтересів OSINT входить пошук та аналіз відкритих баз даних, офіційних документів, комерційних та не комерційних ресурсів в і багато іншого. Таким чином систем OSINT дозволяє отримати відповідь на багато питань, що виникають, як у рядового користувача мережі Інтернет, так і в працівників сфери безпеки та спецслужб.

У теперішній час, за різними оцінками експертів, американські спецслужби отримують від 35% до 95% своїх розвідувальних даних із відкритих джерел. Частка витрат OSINT у розвідувальному бюджеті США складає лише 1% [2]. В Україні з 2014 р. робляться спроби використовувати OSINT у військових операціях, але застосування цього інструменту в державному управлінні та політиці захисту національних інтересів досі перебувають на стадії наукового пошуку [3].

Системи OSINT дає змогу систематизувати та узагальнити великі масиви інформації з відкритих джерел для проведення розгорнутого аналізу. Використовуючи інструменти OSINT, такі як Shodan, Google Dorks, Maltego, The Harvester, здійснювати пошук та аналіз інформації стає набагато швидше та простіше.

Веб-сайти та соціальні мережі можуть бути джерелом інформації, особливо про співробітників. Постачальники та партнери можуть також надавати доступ до певних деталей організації, які краще було б тримати в обмеженому доступі. Крім цього, існує велика кількість неіндексованих веб-сайтів та файлів, відомих під назвою «глибинна мережа», які залишаються технічно загальнодоступними.

Таким чином, при проведені ряду заходів, при перевірці інформації, яка знаходиться у вільному доступі за допомогою технологій OSINT можна запобігти витоку конференційної інформації.

Література.

1. Розвідка на основі відкритих джерел. URL: https://en.wikipedia.org/wiki/Open-source_intelligence.
2. Яровой Т. С. OSINT як перспективний інструмент контролю за лобістською діяльністю в контексті державної безпеки. URL: 18.pdf (maup.com.ua).
3. Heather J. Williams, Ilana Blum. Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise. URL: https://www.rand.org/pubs/ research_reports/RR1964.html.